



**FACULTAD DE INGENIERIA, ARQUITECTURA Y
URBANISMO**

**ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA
DE SISTEMAS**

TESIS

**DESARROLLAR LA PROPUESTA DE VIRTUALIZACIÓN DE
DISPOSITIVOS DE CONMUTACIÓN PARA OPTIMIZAR
LOS SERVICIOS DE LA RED LAN EN EL HOSPITAL
NACIONAL EDGARDO REBAGLIATI MARTINS – EsSALUD**

**PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO
DE SISTEMAS**

Autor:

Bach. Sánchez Arias Raúl Lian

Asesor:

Ing. Vidaurre Flores Miguel Ángel

Línea de Investigación:

**Tecnologías de la información, Redes y
Comunicaciones y Seguridad Informática.**

Lima – Perú

2018



Aprobación de la Tesis

Mg. CARRION BARCO GILBERTO
Presidente del jurado de tesis

Mg. BRAVO RUIZ JAIME ARTURO
Secretario del jurado de tesis

Ing. MEJIA CABRERA HEBER IVAN
Vocal del jurado de tesis

DEDICATORIA

A mi muy amada y admirable madre Elvira Arias Pillpe,
a mi muy querido padre Camilo Raúl Sánchez Chau,
a mi amada esposa Marycielo Katlin Casana Linares,
y a mis dos adoradas hijas Dafne y Hayami Sánchez,
gracias por su gran apoyo moral e incondicional día a
día, inculcándome los buenos valores para poder ser
un profesional competente, honesto y ajeno de toda
corrupción.

A Dios, por darme fuerzas y guiar mis pasos, a la
Institución donde laboro en el HNERM-EsSALUD,
por poner en mi camino a excelentes profesionales de
buenos sentimientos como el Ing. Josué Gutiérrez y el
Ing. Richard Rodríguez que contribuyeron en formarme
como persona con sus acertados y sabios consejos.

AGRADECIMIENTO

Al Ing. Vidaurre Flores Miguel Ángel y al Ing. Heber Mejía quienes estuvieron asesorándome en el desarrollo del proyecto de tesis.

A mi familia Sánchez Arias y también a mis amigos quienes me brindaron su apoyo moral en cada instante cuando más los necesitaba.

RESUMEN

En la presente investigación se desarrollará la propuesta de virtualización de dispositivos de conmutación que permitirán mejorar el performance de la Red LAN, desarrollando una propuesta de diseño de arquitectura de Red de Alto Nivel, así como también el plan de Segmentación de la Red LAN a través de la implementación de Redes de Area Local Virtual (Virtual Local Area Network – VLAN) por tipo de servicio (Voz, Datos, Video, Impresión, Imágenes, Pac's y WiFi); asimismo se propondrá los niveles de seguridad de la Red LAN a través de reglas, regulaciones y políticas por puerto, Vlans y protocolos a fin de mitigar las vulnerabilidades a posibles ataques en la Red, cabe indicar que en el presente proyecto de investigación permitirá mejorar significativamente el desempeño de la Red LAN, los sistemas institucionales y la calidad de los servicios logrando satisfacer a los usuarios asistenciales, administrativos y a la población asegurada.

En la presente investigación se hará uso de los conocimientos teóricos de TI, para optimizar los servicios de la Red LAN, por ende, los usuarios administrativos y asistenciales tendrán mejoras en los flujos de información y las transacciones de los registros serán oportunas para las atenciones de los pacientes asegurados mediante los aplicativos institucionales, aplicando los procesos de planificación de Gestión vigentes para dar solución a la realidad problemática del HNERM-EsSALUD en estudio.

Por otro lado, se justifica metodológicamente, como se aborda la investigación la misma que servirán como referencia para los Hospitales de Alto nivel III, donde la criticidad de los servicios es absoluta, por último, presenta relevancia social, pues al mejorar los servicios brindados a la población asegurada se contribuye a la humanización de los servicios de salud, a la consolidación de una organización sólida, con una buena gestión que logrará fidelizar al paciente que se convertirá en un cliente frecuente.

Palabras Claves: Virtualización, Dispositivos de Conmutación, Red LAN, Diseño de Arquitectura de Red de Alto Nivel, Segmentación y Niveles de Seguridad.

ABSTRACT

In the present investigation the proposal of virtualization of switching devices will be developed that will improve the performance of the LAN Network, developing a high-level network architecture design proposal, as well as the segmentation plan of the LAN Network through of the implementation of Virtual Local Area Networks (VLAN) by type of service (Voice, Data, Video, Printing, Images, Pac's and WiFi); the security levels of the LAN Network will be proposed through rules, regulations and policies by port, Vlans and protocols in order to mitigate the vulnerabilities to possible attacks on the Net, it should be noted that in this research project will significantly improve the performance of the LAN Network, institutional systems and the quality of the services, satisfying the care users, administrative users and the insured population.

In the present research the theoretical knowledge of IT will be used to optimize the LAN Network services, therefore, the administrative and assistance users will have improvements in the information flows and the transactions of the records will be opportune for the attention of the patients insured through the institutional applications, applying the current management planning processes to solve the problematic reality of the HNERM-EsSALUD under study.

On the other hand, it is methodologically justified, as the research is addressed, which will serve as a reference for High Level III Hospitals, where the criticality of the services is absolute, and finally, it has social relevance, since by improving the services provided to the insured population contributes to the humanization of health services, to the consolidation of a solid organization, with good management that will achieve loyalty to the patient who will become a frequent client.

Keywords: Virtualization, Switching Devices, LAN Network, High Level Network Architecture Design, Segmentation and Security Levels.

INTRODUCCIÓN

En la presente investigación se plasmará cómo se encuentra en la actualidad el avance de TI en el HNERM-EsSALUD y la realidad del lugar donde trabajamos y cuántos usuarios somos tanto en la parte administrativa como asistencial, asimismo cabe indicar que se ha demostrado que una Organización, Empresa y/o Institución orientada a brindar servicios de salud bien gestionada y responsable en cuanto al manejo de la información, los recursos tecnológicos, equipamiento quirúrgicos, recursos humanos y materiales médicos, además de una constante comunicación entre las diferentes áreas, tienden a ser más eficientes, mejorando en los procesos de los servicios de prestaciones de salud que se brinda, además mediante estos procesos de gestión son capaces de reducir sus gastos, por ello podemos decir que por lo general este tipo de Organizaciones, Empresas e Instituciones orientados a la salud buscan invertir para consolidar el trabajo en equipo e interactuar para un objetivo en común ofrecer más y mejores servicios de prestaciones de salud a nivel local, regional, nacional y brindar un servicio de salud de primer nivel.

Actualmente, gracias a los grandes avances tecnológicos a nivel de hardware y software podemos contar con una gama de herramientas en el HNERM-EsSALUD como Equipos Biomédicos, Telemedicina, Equipos Autoanalizadores de Laboratorio, los PAC'S, Equipos de Radiografías, Ecografías, Tomografías, PET/CT y Resonancia Magnética, cabe indicar que estas herramientas nos facilitan en tener los resultados en tiempo real, en la presente investigación se justifica técnicamente porque pretende proponer la virtualización de dispositivos de conmutación que permitirán mejorar el performance de los servicios de la Red LAN, desarrollando una propuesta de diseño de arquitectura de Red de Alto Nivel, así como también desarrollar el plan de segmentación de la Red LAN a través de la implementación de Redes de Área Local Virtual (Virtual Local Area Network – VLAN) por tipo de servicio (Voz, Datos, Video, Impresión, Imágenes, Pac's y WiFi); y proponer los niveles de seguridad de la Red LAN a través de reglas, regulaciones y políticas por puerto, Vlans y protocolos a fin de mitigar las vulnerabilidades a posibles ataques en la Red, como solución y respuesta a la problemática existente de la Red LAN en el HNERM-EsSALUD.



INDICE

Contenido

DEDICATORIA.....2
AGRADECIMIENTO.....4
RESUMEN.....5
ABSTRACT.....6
INTRODUCCION.....7

CAPITULO I: PROBLEMA DE LA INVESTIGACIÓN17

1.1. Situación problemática..... 17
 1.2. Formulación del problema..... 30
 1.3. Delimitación de la Investigación..... 30
 1.4. Justificación e importancia de la Investigación..... 31
 1.5. Limitaciones de la Investigación.....31
 1.6. Objetivos.....32
 Objetivo general.....32
 Objetivos específicos.....32

CAPITULO II. MARCO TEÓRICO.....33

2.1. Antecedentes de la Investigación.....33
 2.2. Estado del arte.....39
 2.3. Bases teórico científicas..... 43
 2.3.1 Virtualización.....43
 2.3.1.1 ¿Qué es lo Virtual?:.....43
 2.3.2 Virtualización y Estetización de La Arquitectura Actual .. 46
 2.3.2.1 La hipótesis de la an-estetica de la Arquitectura..... 46
 2.3.3 Concentradores de cableado (Nivel Físico): HUB Y MAU..... 48
 2.3.3.1 Puente o Bridge (Nivel Enlace)..... 48
 2.4. Definición de términos básicos..... 59

CAPITULO III: MARCO METODOLÓGICO..... 66

3.1. Marco metodológico..... .66



3.1.1. Tipo y diseño de la investigación.....	66
3.1.2. Tipo de investigación.....	66
3.1.3. Diseño de la investigación.....	66
3.2. Población y muestra.....	67
3.2.1. Población los Dispositivos de Conmutacion a virtualizar del HNERM-EsSALUD.....	67
3.2.2. Muestra.....	67
3.2.3. Metodos de Investigacion.....	68
3.2.4. Beneficios de LifeCycle.....	69
3.3. Hipótesis.....	74
3.3.1. Variables.....	74
3.3.1.1. Variable Independiente	74
3.3.1.2. Variable Dependiente.....	74
3.3.1.3. Variable Interviniente.....	74
3.4. Operacionalización.....	74
3.5. Métodos, Técnicas e instrumentos de recolección de datos.....	77
3.5.1. El Test.....	77
3.5.2. Ficha de Evaluación.....	77
3.5.3. Encuesta.....	77
3.5.4. Observación.....	78
3.6. Procedimiento para la recolección de datos.....	78
3.6.1. Procedimiento de la Técnica de Recolección de Datos.....	78
3.6.2. Procedimiento de la Ficha de evaluación.....	79
3.6.3. Procedimiento de la Encuesta.....	79
3.6.4. Procedimiento de la Observación.....	79
3.7. Análisis estadístico e interpretación de datos.....	80
3.8. Criterios Eticos.....	83
3.9. Criterios de Rigor Científico.....	83
CAPITULOIV: ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS.....	84
4.1. Resultados en tablas y Graficos.....	84
4.2. Discusión de Resultados.....	106



CAPITULO V: DESARROLLO DE PROPUESTA DE INVESTIGACIÓN.....	113
5.1. Fase 1-Preparación (LifeCycle Services).....	113
5.2. Fase 2-Planificación (LifeCycle Services).....	135
5.3. Fase 3-Diseño (LifeCycle Services)	199
5.4. Fase 4-Implementacion (LifeCycle Services).....	317
5.5. Fase 5-Operación (LifeCycle Services).....	324
5.6. Fase 6-Optimización (LifeCycle Services)	346
CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES.....	367
6.1. Conclusiones.....	367
6.2. Recomendaciones.....	368
REFERENCIAS	369
ANEXOS.....	371
Anexo 1 Conmutadores.....	372
Anexo 2 Gabinetes.....	394
Anexo 3 Telefonía.....	430
Anexo 4 Cámara y Video Vigilancia.....	442
Anexo 5 Backbone-Canalización de Acometida-HNERM	451



INDICE DE FIGURAS

Contenido

Figura 1. Datos Estadísticos de Virtualización.	18
Figura 2. Mapa Territorial	20
Figura 3. Cableado Estructurado Renovado del HNERM-ESSALUD.....	21
Figura 4. Core Principal OmniSwitch 9700 y OmniSwitch 9800	22
Figura 5. Centro de Datos y Backbone Actual del HNERM-ESSALUD.....	24
Figura 6. Esquema Diseño Cableado Estructurado del HNERM-ESSALUD.....	25
Figura 7. Equipos Telefónicos Analógicos y Digitales Alcatel del HNERM.....	25
Figura 8. Diseño Data Center Actual del HNERM-ESSALUD.....	26
Figura 9. Trabajos Realizados en el Data Center del HNERM.....	27
Figura 10. Requerimientos Data Center – Norma TIA 942.....	27
Figura 11. Diseño de Subredes.....	28
Figura 12. Plano del HNERM-Essalud.....	29
Figura 13. Caso de Éxito.....	38
Figura 14. Virtualizando Servidores.....	40
Figura 15. Etapas de La Virtualización.....	41
Figura 16. IBM – VMS.....	42
Figura 17. Soporte De Rstp En Switches Catalyst.....	52
Figura 18. Fases De La Metodología Lifecycle Services – Cisco.....	73
Figura 19. Números de Contextos Virtuales a implementar	84
Figura 20. Device Virtualization	84
Figura 21. Conmutador Cisco Nexus 7000	85
Figura 22. Products Specifications	86
Figura 23. Soluciones Integrales para Centros de Datos	87
Figura 24. Sistema independiente de aire acondicionado de precisión	88
Figura 25. Servicios por Subredes	90
Figura 26. Trafico Protocolo IPV4.....	91
Figura 27. Porcentaje % of Bandwidth	91
Figura 28. IP-V4 Protocol Distribution	92
Figura 29. Tráfico por Mac all Protocols.....	92
Figura 30. Porcentaje % Bandwidth Distribution by VLAN	93



Figura 31. Bandwidth Distribution by Vlan Statistics	93
Figura 32. Porcentaje % Bandwidth Distribution by Vlan Statistics	94
Figura 33. VLAN Type TRT-PORT IP Interface.....	95
Figura 34. Número de Redes virtuales Existentes	96
Figura 35. Número de Listas de Acceso ACL, por Subredes	98
Figura 36. Consolidado de Inactividad Producidos por Unicast, Multicast y Broadcast.....	99
Figura 37. Consolidado de Cargas del Core Principal de La Red LAN.....	100
Figura 38. Consolidado del Ancho de Banda del Core Principal.....	101
Figura 39. Consolidado del Ancho de Banda del Core Principal	102
Figura 40. Consolidado del Ancho de Banda del Core Principal	103
Figura 41. Consolidado Usuarios Afectados por el Consumo del Ancho de Banda	104
Figura 42. Número de Enlaces Redundantes Existentes	105
Figura 43. Generación de Inactividad Core Principal	107
Figura 44. Generación de Inactividad Core Principal	107
Figura 45. Generación de Inactividad Core Principal	108
Figura 46. Generación de Inactividad Core Principal	108
Figura 47. Generación de Inactividad Core Principal	109
Figura 48. Generación de Inactividad Core Principal	109
Figura 49. Generación de Inactividad Core Principal	110
Figura 50. Generación de Inactividad Core Principal	110
Figura 51. Consolidado de uso Hosts en Packets del Core Principal	111
Figura 52. Estadística de Protocolos en Packets del Core Principal	112
Figura 53. Diseño Actual de Estructuración de la Red Informática	115
Figura 54. Diseño Propuesto de la Topología Estrella Jerárquica	116
Figura 55. Switches Nexus de Cisco serie 7000.....	121
Figura 56. Módulo Fabric 2 Cisco Nexus 7000.....	123
Figura 57. Módulo de E/S de 1/10 GE con 48 puertos Nexus de Cisco serie 7000	124
Figura 58. Conmutador Cisco Nexus 7000.....	126
Figura 59. Topología en Estrella Jerárquico	136
Figura 60. Cuadro de Evolución de MySql	139
Figura 61. Optiview Analizador de Red	140
Figura 62. Migración del CORE OmniSwitch 9700 al 9800	150



Figura 63. Gabinetes K Antes y Gabinetes K Después	151
Figura 64. Migración del Core OmniSwitch 9800 al Core Nexus 7000.....	154
Figura 65. Diseño de Arquitectura Propuesta Seguridad a Través de Firewalls.....	199
Figura 66. Seguridad Informática Actual en una PC	226
Figura 67. Seguridad a Nivel de Capa 2 en la Red Local	227
Figura 68. Acceso por PUTTY a través de S.O. Linux y Acceso por WinSCP	228
Figura 69. Seguridad a través de FIREWALL de la PC	229
Figura 70. Las Propiedades de Protocolo TCP/IP de la PC	230
Figura 71. Seguridad por FIREWALL y protección de la RED	231
Figura 72. Seguridad de Protección contra Virus y Amenazas	232
Figura 73. Rendimiento y estado de la PC	233
Figura 74. Diagnóstico de Gabinetes y Equipos Intermedios	284
Figura 75. Diseño Diagrama de Red Alto Nivel	287
Figura 76. Bloque Campus	290
Figura 77. Diseño de Arquitectura del Conmutador	292
Figura 78. Enlaces Redundantes	293
Figura 79. Conectividad de Red Inalámbrica para el Bloque de Campus	295
Figura 80. Bloque Data Center	297
Figura 81. Arquitectura VDC Propuesto	299
Figura 82. VDC	301
Figura 83. Aislamiento de Fallas VDC	303
Figura 84. Device Virtualization VDC'S.....	303
Figura 85. Traditional Firewall Separation with VDC'S	314
Figura 86. Enhanced Firewall Separation with VDC'S	314
Figura 87. Typical Physical Topology	315
Figura 88. Horizontal Consolidation With VDC'S	315
Figura 89. Both Typical and Vertical with VDC'S	316
Figura 90. Arquitectura de los VDC'S de los Switches Nexus 7000.....	317
Figura 91. Virtualizando los Conmutadores Nexus 7000 en Emulador GNS3.....	318
Figura 92. Generación de Inactividad Core Principal	319
Figura 93. Generación de Inactividad Core Principal	319
Figura 94. Emulador GNS3.....	320

Figura 95. Requerimientos Mínimos para uso del Emulador GNS3.....	321
Figura 96. Instalación del Emulador GNS3.....	322
Figura 97. Instalación del Emulador GNS3.....	322
Figura 98. Instalación del Emulador GNS3.....	323
Figura 99. Instalación del Emulador GNS3.....	323
Figura 100. Chassis del Switch Nexus 7000.....	326
Figura 101. Reporte del Performance de la Red LAN	327
Figura 102. Gráfico del Performance de la Red LAN	327
Figura 103. Reporte del Performance de la Red LAN	328
Figura 104. Gráfico del Performance de la Red LAN	328
Figura 105. Mapa Ubicación Actual del Data Center y Gabinetes.....	348
Figura 106. Mapa Ubicación Propuesto del Data Center y Gabinetes.....	349
Figura 107. Plano de Ubicación Actual de la 1era. Planta	350
Figura 108. Topología Estrella Jerárquica Propuesta	351
Figura 109. Comandos de la Virtualización de los VDC'S	351
Figura 110. Comandos de la Virtualización de los VDC'S.....	352
Figura 111. Comandos de la Virtualización de los VDC'S	352
Figura 112. Comandos de la Virtualización de los VDC'S	353
Figura 113. Comandos de la Virtualización de los VDC'S	353
Figura 114. Comandos de la Virtualización de los VDC'S	354
Figura 115. Comandos de la Virtualización de los VDC'S	354
Figura 116. Comandos de la Virtualización de los VDC'S	355
Figura 117. Comandos de la Virtualización de los VDC'S	355
Figura 118. Demostración de la Virtualización de los Conmutadores Nexus.....	356
Figura 119. Reporte en S.O. Linux de las VLAN'S del VDC1	357
Figura 120. Reporte de Trafico por MAC de todos los Protocolos	359
Figura 121. Cuadro Estadístico del Reporte de Trafico por MAC	360
Figura 122. Cuadro Estadístico del Reporte de Trafico por VLAN'S.....	361
Figura 123. Funcionamiento de los Sistemas y Aplicativos en Diferentes Servicios.....	362
Figura 124. Funcionamiento de los Sistemas y Aplicativos en Diferentes Servicios	363
Figura 125. Razones porque usar Tecnología Cisco Switch Nexus 7000.....	364
Figura 126. Razones porque usar Tecnología Cisco Switch Nexus 7000.....	364



Figura 127. Razones porque usar Tecnología Cisco Switch Nexus 7000.....	365
Figura 128. Razones porque usar Tecnología Cisco Switch Nexus 7000.....	365
Figura 129. Cisco Líder en Tecnología	366
Figura 100. Cisco Líder en Integrar Tecnología	366

INDICE DE TABLAS

Contenido

Tabla 1. Cuadro General de los Dispositivos de Conmutación	23
Tabla 2. Población y Muestra.....	67
Tabla 3. Calculo con Formula de Muestreo con población Finita.....	68
Tabla 4. Variable Independiente.....	75
Tabla 5. Variable Dependiente.....	76
Tabla 6. Tiempo de Inactividad del Core Principal	81
Tabla 7. Cuadro de Conmutadores a Virtualizar.....	89
Tabla 8. Cuadro Consolidado de Inactividad del Dispositivo Conmutador	97
Tabla 9. Product Specifications.....	127
Tabla 10. Cuadro de Equipos Intermedios de la OSI HNERM EsSALUD.....	147
Tabla 11. Formato Actual de Diagnóstico de la Red LAN	148
Tabla 12. Cuadro de servidores en el cuarto de Telecomunicaciones	149
Tabla 13. Plan Direccionamiento Ip	153
Tabla 14. Presupuesto Consolidado	156
Tabla 15. Análisis Interno de FODA HNERM EsSALUD	235
Tabla 16. Análisis Externo de FODA HNERM EsSALUD	237
Tabla 17. Análisis Prevención y Mitigación de Riesgos.....	240
Tabla 18. Cuadro de Niveles de Atención por tipo de Riesgo.....	242
Tabla 19. Niveles de Atención de los Aplicativos Informáticos.....	243
Tabla 20. Servidores de la Oficina de Soporte Informático	244
Tabla 21. Dispositivos conmutadores en General	246
Tabla 22. Dispositivos conmutadores Administrables	247
Tabla 23. Cuadro de Aplicativos Informáticos Actuales	249
Tabla 24. <i>Cuadro de Usuarios en el HNERM EsSALUD</i>	251



Tabla 25. Cuadro de Accesos en el HNERM EsSALUD	251
Tabla 26. Cuadro de solicitud de requerimiento	253
Tabla 27. Bitácora de las Caidas de los servicios de la Red LAN	275
Tabla 28. Mantenimiento preventivo equipos de cómputo Red Rebagliati	281
Tabla 29. Inventario Impresoras Láser de la Red Rebagliati	282
Tabla 30. Inventario Impresoras Matriciales Red Rebagliati	283
Tabla 31. Resumen simplificado mantenimiento preventivo para data center	285
Tabla 32. Equipos Intermedios Swithes de la Red de Telecomunicaciones	286
Tabla 33. Cuadro de Cronograma de las Fases, Actividades, Avances y Fechas	326
Tabla 34. Personal de la Oficina de Soporte Informático	329
Tabla 35. Consolidado del Ancho de Banda y Trafico del Performance de la Red	358

CAPÍTULO I: PROBLEMA DE LA INVESTIGACIÓN.

1.1. Situación problemática

En la actualidad hay Instituciones, Empresas y Organizaciones del estado como el sector salud EsSALUD y como el sector privado las Clínicas Particulares que brindan servicios de Salud que se ubican en las diferentes localidades de nuestro País, que tienen diversos inconvenientes como gastos innecesarios en la contratación de servicios en gestión de recursos en Redes y Comunicaciones, contratación de profesionales que no logran diagnosticar con veracidad la lentitud y caídas de la Red LAN, informes de costos sobre elevados para implementar, reestructurar y segmentar la Red LAN. Así mismo cabe mencionar que de la información obtenida de las realidades de los Centros Asistenciales de EsSALUD se ha coincidido en la búsqueda de una nueva herramienta de solución como es el desarrollo de una propuesta de la virtualización de dispositivos de conmutación que logrará beneficios en cuanto a agilidad empresarial, calidad de servicios y gestión de la Red LAN en el HNERM-EsSALUD.

Análisis de la Problemática a nivel Local, Regional y Nacional de los Hospitales de EsSALUD.

Actualmente EsSALUD cuenta con 390 centros asistenciales a nivel local, regional y nacional: nivel III (9 hospitales nacionales 3 institutos), nivel II (76 hospitales de mediana complejidad) y nivel I (302 centros asistenciales del primer nivel de atención). Cabe mencionar en lo que respecta a ciudad de Lima se ha recogido la documentación solicitada y se ha realizado el levantamiento de información técnico sobre las gestiones en redes y comunicaciones y casi el 50% de los referidos CAP de la Red Asistencial del Hospital Nacional Edgardo Rebagliati Martins–EsSALUD no cuentan con una buena performance de la Red LAN, segmentación de la Red LAN y niveles de seguridad.

El HNERM-EsSALUD, actualmente está inmerso a la constante evolución tecnológica de los dispositivos de electromedicina, los mismos que están evolucionando con la tecnología IP, esto conlleva al área de tecnología de información y comunicaciones en tener una infraestructura confiable, que garantice el óptimo servicio, con escalabilidad, seguridad y la funcionalidad 24 x 7 x 365.



Por ello la alta dirección de EsSALUD ha creído conveniente encargar a la Oficina de Soporte Informático del Hospital Nacional Edgardo Rebagliati Martins-EsSALUD considerado el Hospital Emblema por ser de Alto Nivel III, elaboren las propuestas de solución necesarias para abordar esta problemática.

Finalmente, cabe mencionar que un conmutador virtual (vSwitch) nos permitirá que las máquinas virtuales (VM) se comuniquen entre sí que será parte de la solución a la propuesta planteada, los vSwitches gestionan y dirigen el tráfico en un entorno virtual, donde cada host virtual debe conectarse a un switch virtual de la misma manera un host físico debe estar conectado a un conmutador físico, así mismo la virtualización de red está destinada a mejorar la productividad y la eficiencia mediante la realización de tareas de forma automática, permitiendo que los archivos, imágenes y programas que se gestionen de forma centralizada desde un único sitio físico., *Figura 1.*

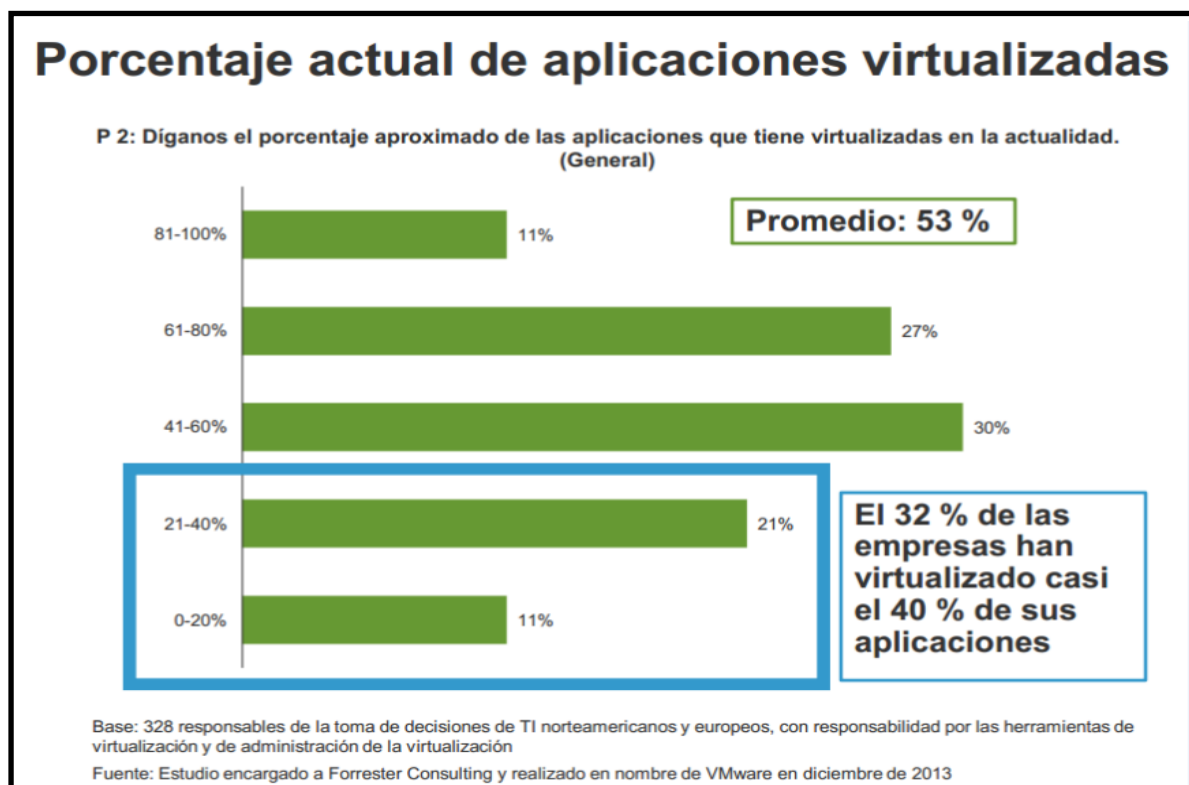


Figura 1. Datos Estadísticos de Virtualización. Fuente: Estudio encargado a Forester Consulting y realizado en el nombre de Vmware diciembre (2013).



Red asistencial Rebagliati:

Los siguientes establecimientos de salud pertenecen a la Red Desconcentrada III Rebagliati:

- a. Hospital III Suárez Angamos
- b. Hospital II Cañete
- c. Hospital I Uldarico Rocca Fernández
- d. Hospital I Carlos Alcántara Butterfield
- e. Clínica Central de Prevención
- f. Policlínico Pablo Bermúdez
- g. Policlínico Chincha
- h. Policlínico Próceres
- i. Policlínico Juan José Rodríguez Lazo
- j. Policlínico Santa Cruz
- k. Centro de Atención Primaria III San Isidro
- l. Centro de Atención Primaria III San Juan de Miraflores
- m. Centro de Atención Primaria III Surquillo
- n. Centro de Atención Primaria II Lurín
- o. Centro Médico Mala
- p. Centro de Urgencias “Playas del Sur”
- q. CEDHI
- r. Posta Médica La Quebrada
- s. Posta Médica San Isidro

IPRESS

- a. Magdalena
- b. Jesús María
- c. Suiza Lab.
- d. Hospital Villa Salud
- e. Soluciones Médico Quirúrgico del Perú SAC

APP

- a. Hospital II Guillermo Kaelin de La Fuente
- b. Policlínico Guillermo Kaelin de La Fuente





Figura 2. Mapa Territorial de las Redes Asistenciales a Nivel Nacional, Regional y Local. Fuente: Nuestras Redes Asistenciales EsSALUD (2018).

El presente trabajo de investigación se ha realizado en unos de los hospitales emblemáticos del Seguro Social como es el Hospital Nacional Edgardo Rebagliati Martins – EsSALUD, ubicado en el Distrito de Jesús María, Departamento de Lima, país Perú.

A continuación, se describe a detalle la problemática actual de cada uno de los Sistemas de la Red LAN del HNERM-EsSALUD:

Sistema de Cableado Estructurado:

El cableado estructurado existente en el HNERM-EsSALUD, es de Cat. 5 y la gran mayoría es de Cat. 6 de los cuales 2,000 puntos de red, han sido instalados y certificados el año 2008 de acuerdo a lo establecido por los estándares de la industria, a la fecha ha crecido en un 150% del total de puntos instalados el año 2008 el mismo que cubre la demanda de nuevos Puntos de Red de manera improvisada, que en muchos casos no tienen las especificaciones necesarias para una mejor viabilidad y protección de los dispositivos conmutadores del mencionado hospital.



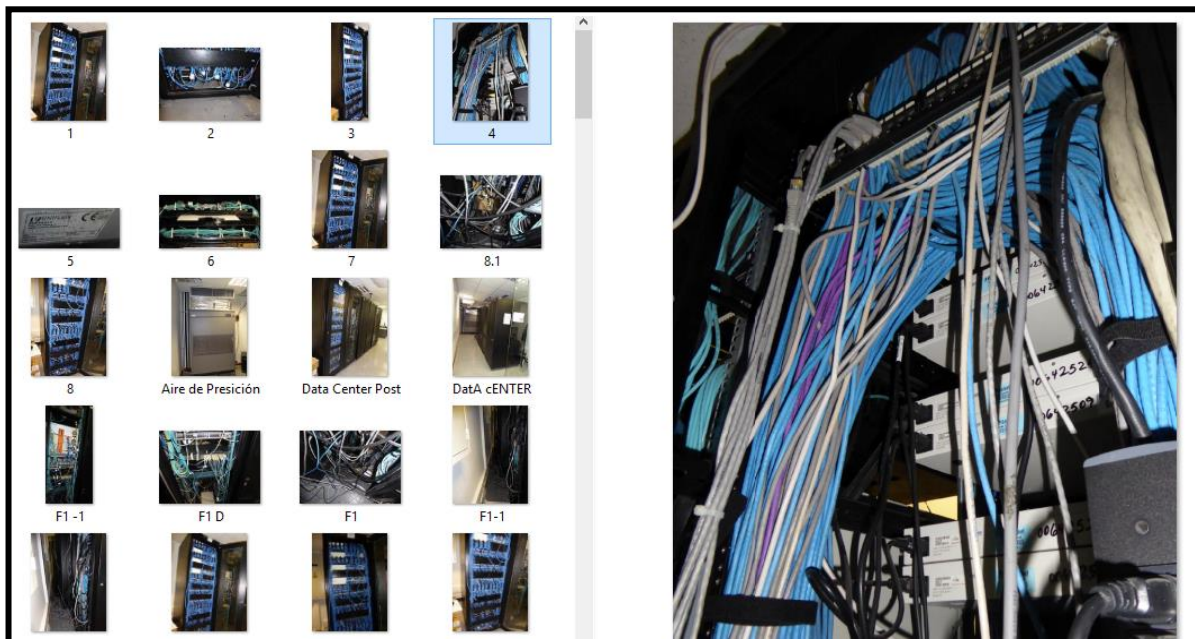


Figura 3. Cableado Estructurado Renovado del HNERM EsSALUD. Fuente: Oficina de Soporte Informático del HNERM EsSALUD (2017).

Debido al crecimiento no planificado por factores como (Avance tecnológico de la Telemedicina, Informática, la dinámica de los cambios funcionales de las oficinas) todo ello ha llevado a realizar instalaciones de puntos de red sin certificar un 30% cat. 5e y 120% cat. 6.

El sistema de canalización ha excedido la capacidad máxima establecida por el fabricante y estándares de la industria.

No existe sistema eléctrico exclusivo para el sistema de cableado estructurado.

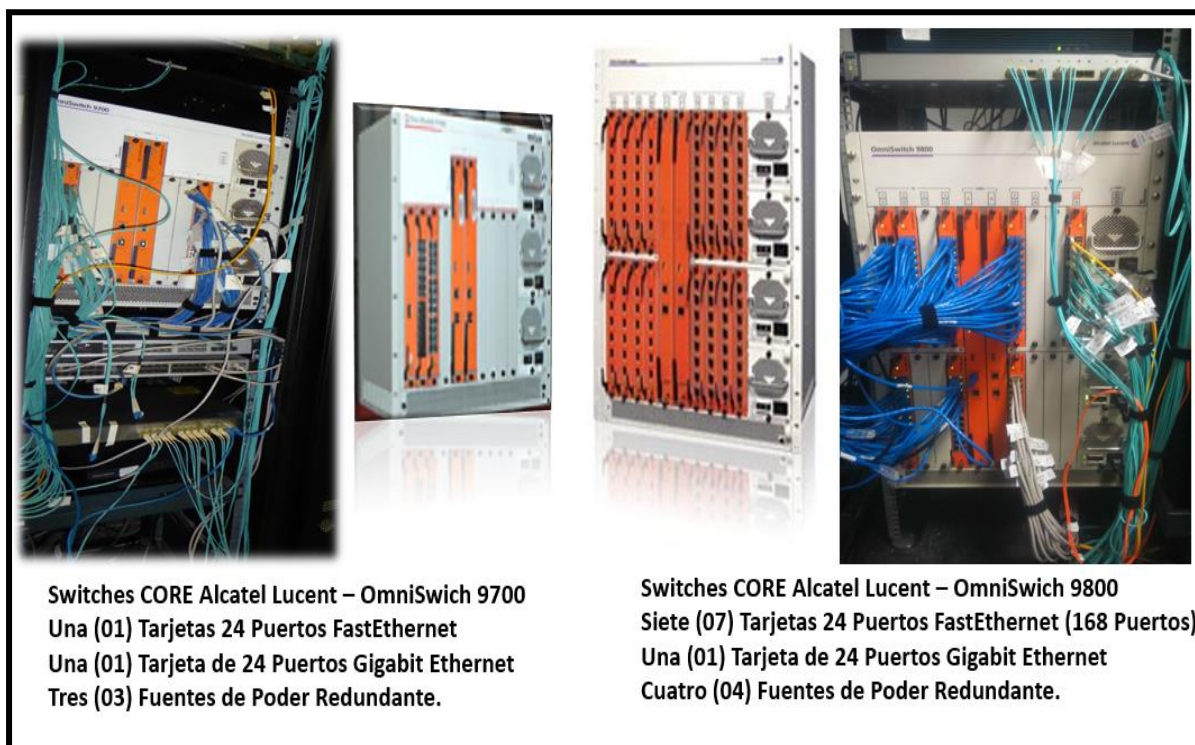
No existe un plan de contingencia actualizado para la continuidad del servicio.



Equipos de Comunicación:

Los equipamientos de comunicaciones el 100 % han cumplido su vida útil, (12 años de vida útil), de los cuales 32% son administrables y el 68% son Standalone (hub), así mismo existen diversidad de marcas (07 marcas) lo que dificulta la administración.

El 70 % de equipos de comunicaciones presenta errores lógicos a nivel de interfaces de red tales como desbordamiento de base de datos, apagado de puertos, falla de fuente de poder, lo que genera intermitencia en la red y caída de los sistemas afectando la atención al asegurado.



Switches CORE Alcatel Lucent – OmniSwich 9700
 Una (01) Tarjetas 24 Puertos FastEthernet
 Una (01) Tarjeta de 24 Puertos Gigabit Ethernet
 Tres (03) Fuentes de Poder Redundante.

Switches CORE Alcatel Lucent – OmniSwich 9800
 Siete (07) Tarjetas 24 Puertos FastEthernet (168 Puertos)
 Una (01) Tarjeta de 24 Puertos Gigabit Ethernet
 Cuatro (04) Fuentes de Poder Redundante.

Figura 4. Core Renovado Omniswitch 9800 en el HNERM EsSALUD. Fuente: Oficina de Soporte Informático del HNERM EsSALUD (2017).

Actualmente la infraestructura de comunicaciones no cuenta con redundancia lo que no garantiza la continuidad operativa del servicio en caso de emergencias o desastres.

La centralización de compras de equipos activos (Parque informático) por parte de GCTIC sede central no permite atender los nuevos requerimientos de los proyectos contemplados con los avances de la telemedicina.



Tabla 1
Cuadro General de los Dispositivos de Conmutación del HNERM EsSALUD

Nº	MARCA	MODELO	CONFIGURACION	TIPO	VELOCIDAD	POE	VLAN	CAPA	SFP	GE	ETH	UR	CANT.	
1	ALCATEL-LUCENT	OmniSwitch 9800	CORE PRINCIPAL	MODULAR	10/100/1000	NO	Administrables	SI	L3	48	168	-	18	1
2	ALCATEL-LUCENT	OmniStack LS 6224P	BORDE DATOS	FUO	10/100	SI	Administrables	SI	L2	2	4	24	1	31
3	ALCATEL-LUCENT	OmniStack LS 6450P	BORDE DATOS	FUO	10/100/1000	SI	Administrables	SI	L2/L3	2	2	24	1	4
4	CISCO	Catalyst 3750	CORE CAMARAS	FUO	10/100/1000	NO	Administrables	SI	L2/L3	12			1	1
5	CISCO	Router BEFSR81		FUO		NO						8	1	1
6	CISCO	Catalyst 3560 Series	BORDE CAMARAS	FUO	10/100	NO	Administrables	SI	L2	1	1	8	1	7
7	ALIED TELESIS	AT 8000S/24POE	BORDE DATOS	FUO	10/100	NO	Administrables	SI	L2	2	2	24	1	1
8	ALIED TELESIS	AT- GS950	DISTRIBUCION	FUO	10/100/1000	NO	Administrables	SI	L2	2	2	8	1	1
9	3COM	Super Stack 5500G -EL	DISTRIBUCION	FUO	10/100	NO	Administrables	SI	L2	2	2	24	1	6
10	3COM	Baseline Switch 2824	DISTRIBUCION	FUO	10/100	NO	Administrables	SI	L2	2	2	24	1	3
11	HP	V1905-24-POE	DISTRIBUCION	FUO	10/100	NO	Administrables	SI	L2	2	2	24	1	3
12	HP	V1920-24	DISTRIBUCION	FUO	10/100/1000	NO	Administrables	SI	L2	2	2	24	1	1
13	D - LINK	DGS - 3100	DISTRIBUCION	FUO	10/100/1000	NO	Administrables	SI	L2	4	24		1	1
14	D - LINK	DGS - 3024	DISTRIBUCION	FUO	10/100/1000	NO	Administrables	SI	L2	4	24		1	5
15	D - LINK	DGS - 3120	DISTRIBUCION	FUO	10/100/1000	NO	Administrables	SI	L2/L3	4	24		1	1
16	D - LINK	DGS - 1510-28	DISTRIBUCION	FUO	10/100/1000	NO	Administrables	SI	L2/L3	4	24		1	12
17	D - LINK	DGS - 1210-28P	DISTRIBUCION	FUO	10/100/1000	SI	Administrables	SI	L2	4	24		1	1
18	D - LINK	DGS - 1210-28	DISTRIBUCION	FUO	10/100/1000	NO	Administrables	SI	L2	4	24		1	10
19	D - LINK	DGS - 1210-48	DISTRIBUCION	FUO	10/100/1000	NO	Administrables	SI	L2	4	48		1	4
20	D - LINK	DES - 1024A	DISTRIBUCION	FUO	10/100	NO	Stand-alone	NO				24	1	10
21	D - LINK	DES - 1024D	DISTRIBUCION	FUO	10/100	NO	Stand-alone	NO				24	1	25
22	D - LINK	DES - 1016D	DISTRIBUCION	FUO	10/100	NO	Stand-alone	NO				16	1	2
23	D - LINK	DES - 1060D	DISTRIBUCION	FUO	10/100	NO	Stand-alone	NO				16	1	1
24	D - LINK	DXS - 3326GSR	CORE BACKUP	FUO	10/100/1000	NO	Administrables	SI	L2/L3	24	4		1	1
25	D - LINK	DIR-400 ROUTER		FUO		NO						24	1	1
26	TRENDnet	TEG - 516DG	DISTRIBUCION	FUO	10/100	NO	Stand-alone	NO				16	1	1
													135	

Fuente: Oficina de Soporte Informático del HNERM EsSALUD (2017).

La renovación de equipos de comunicaciones será planificada cumpliendo estrictamente lo establecido por el fabricante (vida útil) toda vez que el hospital de nivel IV, donde las disponibilidades de los sistemas de información deberán estar activos 24x7x365 de manera ininterrumpida.

Así como también La obsolescencia tecnológica de los equipos activos, en los diferentes servicios de las Áreas Administrativas y Asistenciales no ha sido renovada en su totalidad el parque informático, por lo que se ha levantado observaciones y se está presupuestando para el requerimiento de nuevos equipos informáticos.



Backbone:

Cabe mencionar que el Backbone existente es de fibra óptica multimodo de 50/125um., om3 de 6 hilos que garantiza una velocidad de 10 GB, para un óptimo funcionamiento del cableado troncal (Backbone) del HNERM-EsSALUD, se recomienda realizar una nueva distribución de los Gabinetes de comunicaciones los mismos que deben considerar la instalación del cableado de Fibra Óptica desde nuestro Data Center.

La topología de la red debe ser tipo estrella jerárquica con redundancia que interconecte el Gabinete de Distribución Principal (GDP) que se encuentra ubicado en el Data Center hasta los Gabinetes de Distribución Secundarios (GDS), logrando velocidades iniciales a 1 Gbps y soporten transmisiones futuras de 10/40/100Gbps.



Figura 5. Centro de Datos Actual y Backbone Actual del HNERM EsSALUD. Fuente: Oficina de Soporte Informático del HNERM EsSALUD (2017).

Los ductos actualmente no cumplen con las especificaciones técnicas requeridas, así mismo teniendo en cuenta una ocupación máxima inicial del 50%. La estructura general del cableado estructurado se basa en una distribución jerárquica del tipo "estrella", con un nivel de interconexión.

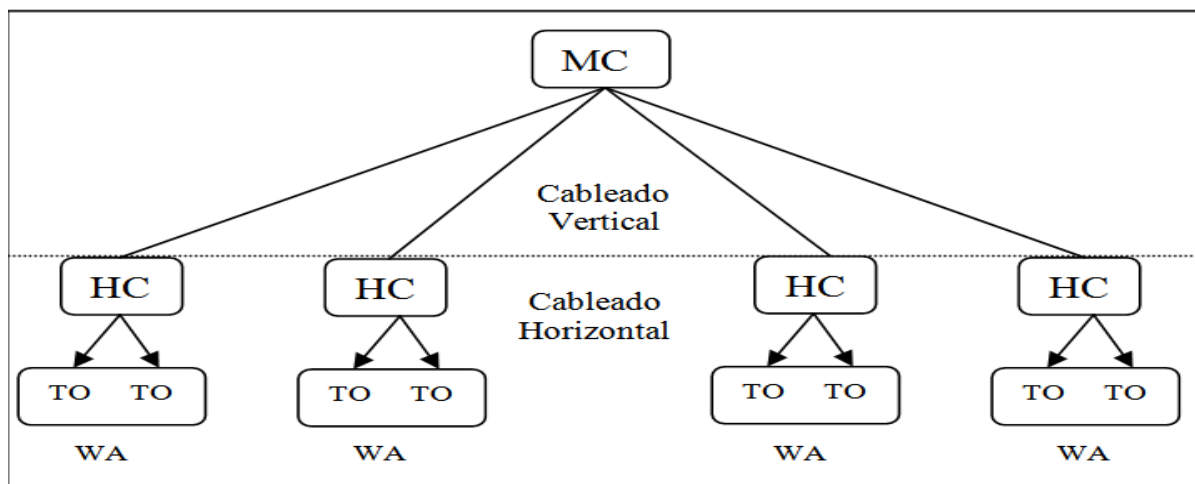


Figura 6. Esquema Diseño Cableado Estructurado del HNERM EsSALUD. Fuente: Oficina de Soporte Informático del HNERM EsSALUD (2017).

Sistema de Telefonía:

La central Telefónica existente es un espejo de sede central la misma que es obsoleta y es administrada por sede central, actualmente el HNERM-EsSALUD tiene asignados 1088 anexos de los cuales el 87% son equipos analógicos, el 8% son IP y el 5% son Digitales.



Figura 7. Equipos Telefónicos Analógicos y Digitales Alcatel del HHNERM EsSALUD. Fuente: Oficina de Soporte Informático del HNERM EsSALUD (2017).

Los 1,096 números de anexos que han sido asignados al HNERM-EsSALUD no cubre la demanda del hospital debido al agotamiento de números de anexos (4 dígitos), teniendo una demanda de 1,500 números de anexos más, existen 1,500 equipos de telefonía IP que no se instalan debido que la infraestructura de red no es la adecuada, no disponibilidad de números de anexo, donde existen áreas que comparte el anexo a través de puentes.



Data Center:

El Data center del HNERM-EsSALUD, actualmente no cumple con los estándares establecidos por la norma ANSI/TIA 942.

El área física asignada es 10 m², de los cuales se alojan 6 gabinetes de comunicaciones de los cuales 2 están asignados a equipos de comunicaciones (Switch CORE modular OS 9800, OptiView XG, Bandejas de Fibra Óptica, Telefonía IP), los cuatro gabinetes restantes alojan 32 Servidores donde están instalados los distintos aplicativos institucionales y gran parte aplicativos de las casas comerciales sesión en uso), 01 aire acondicionado de precisión y uno de confort, 02 UPS de 10 kva.

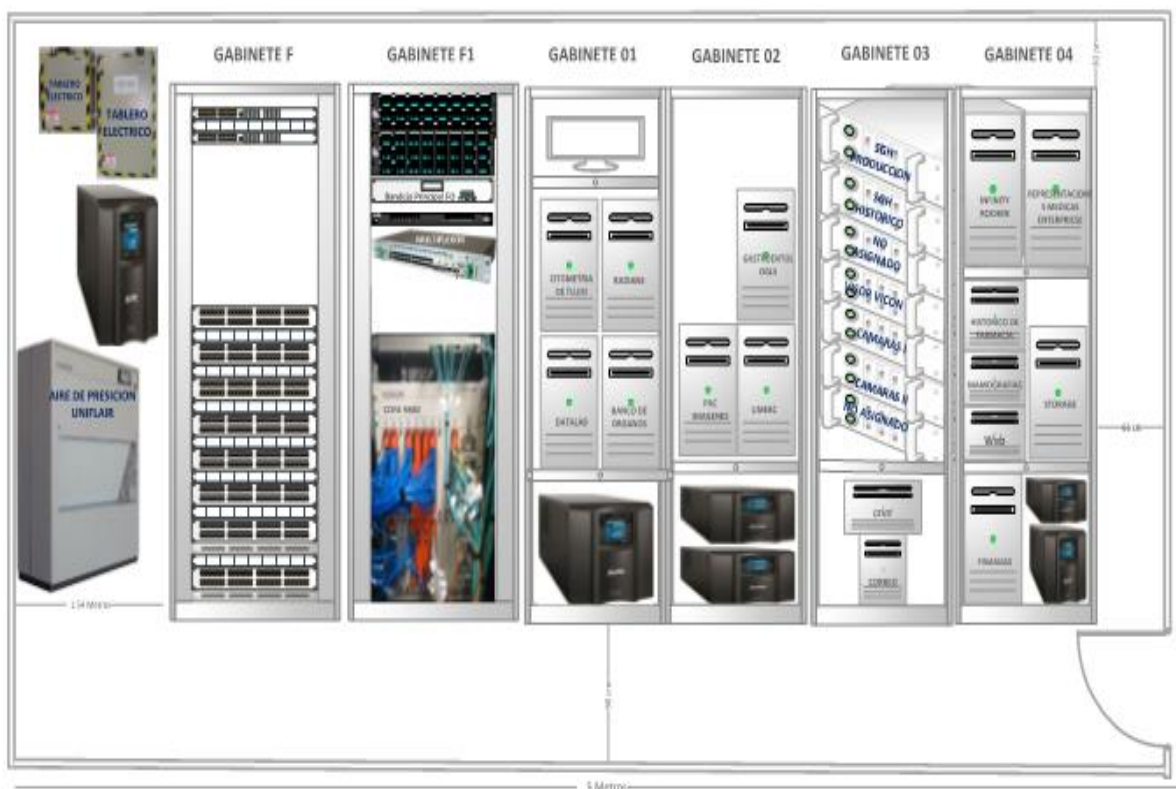


Figura 8. Diseño Data Center Actual del HNERM EsSALUD. Fuente: Oficina de Soporte Informático del HNERM EsSALUD (2017).





Figura 9. Trabajos Realizados en el Data Center del HNERM EsSALUD. Fuente: Oficina de Soporte Informático del HNERM EsSALUD (2017).

REQUERIMIENTOS GENERALES		
LOCALIZACIÓN	DISEÑO DE ARQUITECTURA	DISEÑO ELECTRICO
<p>Evitar cercanía fuentes EMI Evitar ventanas exteriores Accesibilidad para grandes equipos.</p>	<p>Dimensión física (proyección de crecimiento). Considerar tableros eléctricos y UPS. Altura de techo: mínimo 8.5 pies (2.59 m). La iluminación no debe de ser provista del mismo panel de equipos. La puerta debe ser por lo menos de 3 pies x 7 pies (0.90 m x 2.10 m) La carga del piso debe ser: Mínimo carga distribuida: 150 lbf/ft² (224 kg/m²) Recomendado: 250 lbf/ft² (373 kg/m²)</p>	<p>Energía: - Definir cantidades apropiadas de tomas eléctricas y tableros. Puesta a tierra y cableado. Cumplimiento de especificaciones de ANSI-J-STD-607-A</p>
ACCESO	CONDICIONES AMBIENTALES	OTRAS CONSIDERACIONES
<p>Limitado a personal autorizado.</p>	<p>Cuarto protegido de contaminantes Operación continua 24/7/365 Requerimiento de Temp/Humedad 20 °C – 25 °C 40% - 55% de humedad relativa Medición de los equipos en operación Mantener presión positiva Adecuada ventilación de baterías Vibración. Puede generar acoplamiento al cableado o equipos.</p>	<p>Protección de fuego: - Detección temprana Extinción Infiltración de agua: - reducir donde exista riesgo Drenaje en el piso. No tubos o drenajes sobre piso.</p>

Figura 10. Requerimientos Generales que debe Cumplir un Data Center Norma TIA 942. Fuente: Oficina de Soporte Informático del HNERM EsSALUD (2017).



El cableado Horizontal establecido para los Servidores no está certificado, no cuenta con pozo a tierra exclusivo para el Data center, grupo electrógeno, sistema contra incendios, espacios físicos para el aire frío y caliente, sistema de aire acondicionado de precisión de contingencia.

No cuenta con un Plan de Contingencia.

Sistema de Seguridad Inoperativo.

Segmentación De La Red LAN:

Actualmente el HNERM – ESSALUD cuenta con 09 subredes asignadas al servicio de datos comprendidas en los rangos 172.22.40.0 /24, 172.22.41.0 /24, 172.22.42.0 /24, 172.22.43.0 /24, 172.22.44.0 /24, 172.22.46.0 /24, 172.22.47.0 /24, 172.22.48.0 /24, 172.22.49.0 /24 haciendo un total de 2,783 direcciones IP, las mismas que se encuentra en VLAN 1 por default, teniendo en cuenta que el HNERM – ESSALUD cuenta con servicios de video a través de cámaras IP, Imágenes PACS las mismas que se transfieren desde los equipos biomédicos a los distintos servidores, telefonía IP, Servicio de Datos e Impresión, donde el mayor ancho de banda lo consumen las cámaras IP 45%, Imágenes PACS 25%, Datos e Impresión 25 y Voz sobre IP 5% respectivamente.

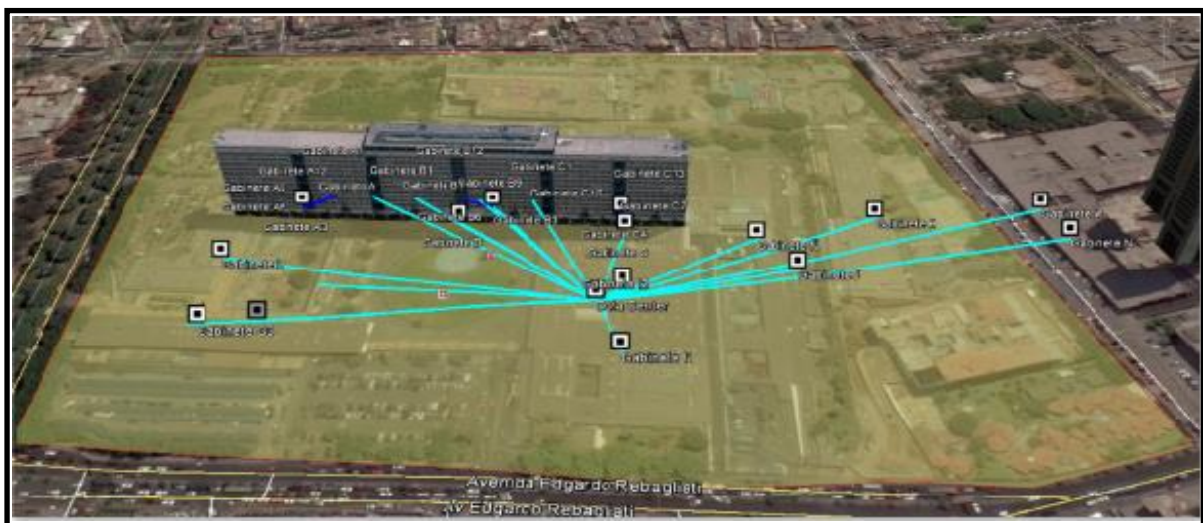


Figura 11. Diseño de Subredes. Fuente: Oficina de Soporte Informático del HNERM EsSALUD (2017).



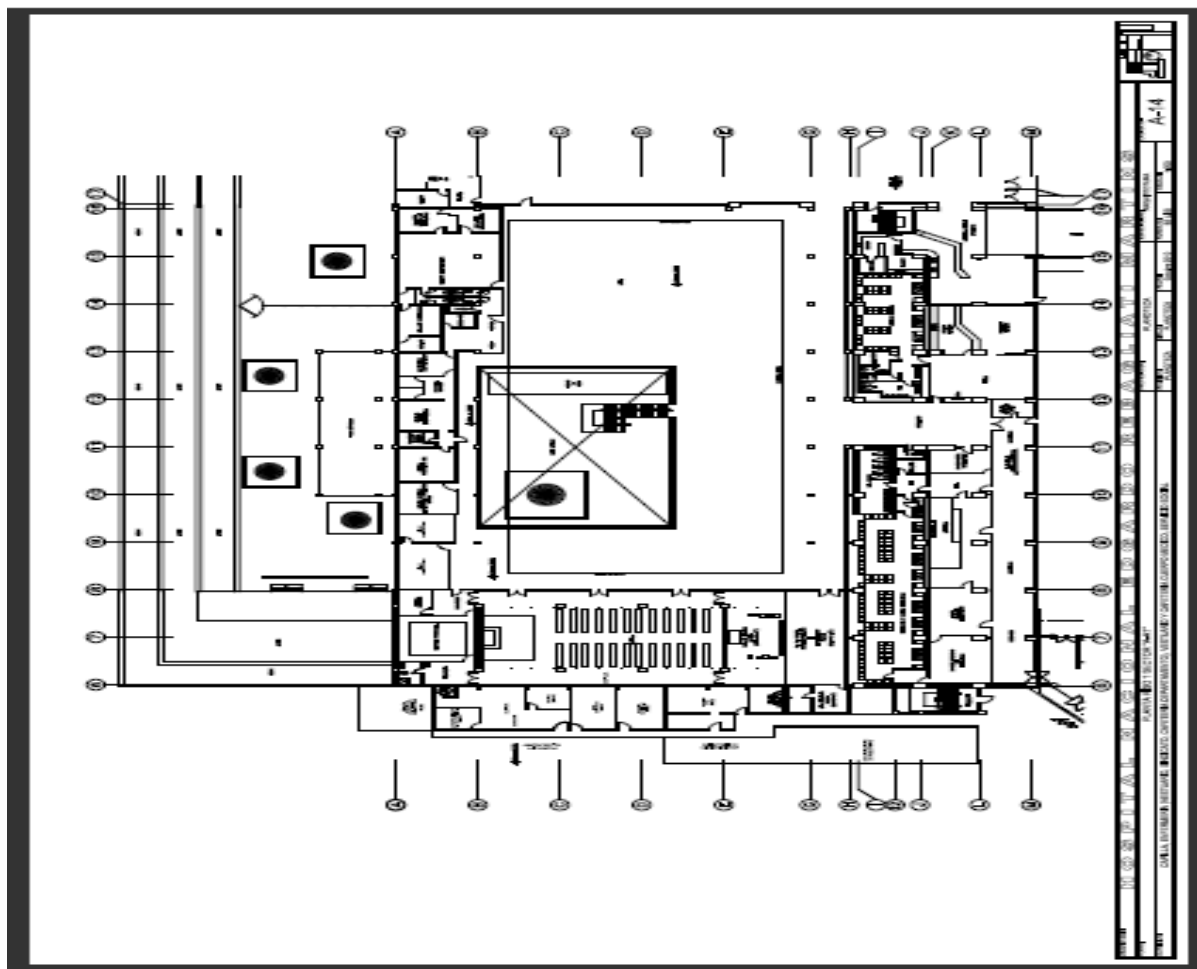


Figura 12. Plano del HNERM EsSALUD. Fuente: Oficina de Soporte Informático del HNERM EsSALUD (2017).

Como podemos apreciar existen 3,036 direcciones IP, las mismas que son insuficiente para un parque informático de 6,000 equipos, al respecto el direccionamiento IP lo asigna la GCTIC–ESSALUD, donde estarán parametrizados los rangos a nivel nacional limitándonos a utilizar las direcciones IP asignadas.

Las Redes Virtuales (Virtual LANs) separan de forma ordenada y lógica el tráfico total que puede circular por una misma red. En general el tráfico asociado a una VLAN no debe circular por ninguna otra VLAN configurada.

El rendimiento de la red es un factor importante en la productividad de los servicios del Hospital. Una de las tecnologías que contribuyen a mejorar el rendimiento de la Red es la división de los grandes dominios de difusión en dominios más pequeños.



Así mismo el crecimiento de las áreas de trabajo no planificado, ha afectado el rendimiento de la Red LAN, lo que ha conllevado que se realicen instalaciones inadecuadas en todos los segmentos de red.

Actualmente cubren las demandas del servicio en un 33.03 %, con limitaciones en la transferencia de información debido a la velocidad de los equipos intermedios instalados como cascada (10/100 Mbps) en su mayoría son de uso doméstico.

1.2. Formulación del problema.

¿Cuál será los resultados esperados desarrollando la propuesta de virtualización de dispositivos de conmutación y de qué manera resolverá los problemas que se vienen suscitando por las caídas frecuentes de los servicios de la Red LAN, que afectan la comunicación, generando malestar a los usuarios asistenciales y administrativos, población asegurada, seguridad, procesos de análisis y procedimientos que se brindan en los diferentes servicios del HNERM-EsSALUD, incrementando el recurso humano y costos innecesarios para la Institución?

1.3. Delimitación de la Investigación

Sobre el desarrollo de la propuesta de Virtualizar los Dispositivos conmutadores, se tuvo todas las facilidades para la realización de la toma de la información y documentación correspondiente a la Oficina de Soporte Informático del Hospital Nacional Edgardo Rebagliati Martins – EsSALUD. Así mismo, de las diferentes áreas involucradas y los coordinadores comprometidos, cabe precisar que el jefe de la OSI-HNERM-EsSALUD Ing. Ángelo Gregorio D'uniam D'uniam y los demás profesionales de cada Área funcional aportaron sin ningún inconveniente al presente trabajo de investigación por el periodo de octubre del 2015 a enero del año 2017.

1.4. Justificación e importancia de la Investigación.

Se justifica técnicamente porque pretende desarrollar la propuesta de virtualización de dispositivos de conmutación que permitirán mejorar el performance de los servicios de la Red LAN, a través de la convergencia de redes, calidad de servicio, seguridad, escalabilidad y alta disponibilidad.

Como respuesta a la problemática existente de la red LAN en el HNERM–EsSALUD, cabe indicar que la investigación pretende proponer una alternativa de solución que permitirá mejorar significativamente el desempeño de los servicios de la Red LAN y los sistemas institucionales, mejorando la atención logrando satisfacer a los usuarios asistenciales y administrativos, población asegurada, optimizando costos y recursos humanos.

Por otro lado, se justifica metodológicamente, cómo se aborda la investigación la misma que servirán como referencia para hospitales de salud de alto nivel, donde la criticidad de los servicios es absoluta, por último, presenta relevancia social, pues al mejorar los servicios de la Red LAN, tanto los usuarios y la población asegurada contribuye a la humanización de las prestaciones servicios de salud, a la consolidación de una organización sólida, con una buena gestión que logrará fidelizar al paciente que se convertirá en un cliente frecuente.

1.5. Limitaciones de la Investigación

En la presente investigación se tuvo algunos inconvenientes con respecto a que no todas las Empresas que se visitaron no dan información presencialmente y no todos aplican la virtualización a los dispositivos conmutadores, las informaciones que brindan es relacionado a las ventas que generan con el tipo de virtualización de nuevas soluciones que cada Empresa lanza al mercado y que cada empresa interesada de acuerdo a su realidad adquiere dicha solución, el otro inconveniente que los procesos de compra o para adquirir el servicio tarda porque se hace todo un proceso burocrático de sustento para que se pueda concretar el equipo o servicio solicitado por la Empresa.



1.6. Objetivos.

Objetivo general.

Desarrollar la propuesta de virtualización de dispositivos de conmutación para optimizar los servicios de la Red LAN del HNERM-EsSALUD.

Objetivos específicos:

- a. Desarrollar una propuesta de diseño de arquitectura de Red de Alto Nivel haciendo uso de Virtualización de Dispositivos de Conmutación de la Red LAN en el HNERM-EsSALUD.
- b. Desarrollar un plan de segmentación la Red LAN a través de la implementación de Redes de Área Local Virtual (Virtual Local Area Network) por tipo de servicio (Voz, Datos, Video, Impresión, Imágenes Pac's, WIFI).
- c. Proponer niveles de Seguridad de la Red LAN a través de reglas, regulaciones y políticas por puerto, Vlans y protocolos a fin de mitigar las vulnerabilidades a posibles ataques en la Red.

CAPÍTULO II. MARCO TEÓRICO

2.1. Antecedentes de la Investigación

En la presente investigación se realizó el estudio de Investigación sobre el “Diseño e Implementación de una red Privada Virtual para la empresa Eléctrica Quito S.A., Matriz las Casas para la transmisión de Datos y Voz sobre IP”.

Esto significa que este proyecto contempla una solución para las necesidades más urgentes en el aspecto de comunicación-seguridad, orientadas específicamente a la red de datos de la Empresa Eléctrica Quito S.A. (E.E.Q.S.A.), implementada en su mayoría dentro del modelo de referencia TCP/IP. Además de solucionar las necesidades, se ha planificado también, el proyectar soluciones a las futuras necesidades y aplicaciones que ingresen y sean parte de la red de datos, como por ejemplo las aplicaciones multimedia: VoIP, Telefonía IP, Videoconferencia, etc. (Díaz, 2010, p. 93)

Los anexos los puedes solicitar al personal autorizado de la biblioteca.

El propósito de la investigación de la presente tesis fue realizar un “Análisis de tráfico de red del servicio de la administración aduanera del estado Zulia”.

Tiene como finalidad de proporcionar a los investigadores una herramienta teórica que permita determinar el comportamiento bajo ciertos parámetros de cualquier red (velocidad de conexión, ancho de banda, tasa de transmisión, entre otros), a fin de proponer recomendaciones que permitan incrementar la calidad de servicio. El estudio fue descriptivo y de campo, con diseño no experimental transeccional descriptivo. Se utilizó una población conformada por 108 computadoras del Servicio de la Administración Aduanera de la región zuliana. (Rivero, 2010, p. 23)

Para realizar el análisis de tráfico se seleccionaron 64 computadores (con las mismas especificaciones) y se utilizó un (1) software denominado Analyzer Enterprise Versión 6.0, el cual permitió medir la tasa de transmisión e identificar y evaluar los puntos críticos que afectan el rendimiento de la red de aduanas.



La base teórica manejada para la investigación estuvo conformada por documentos y publicaciones obtenidas de tesis, artículos y libros de tráfico y calidad de servicio de redes. Ahora bien, en relación con los resultados obtenidos, se encontró un 53% del nivel de congestamiento de tráfico en la red de la Aduana Subalterna Aérea de la Chinita y un 41% en Paraguachón, por lo que se realizaron las respectivas recomendaciones que permitieran mejorar la calidad de servicio de la red de aduanas.

En lo relacionado con las recomendaciones aportadas a tal situación se logra mencionar que se debe evaluar constantemente el nivel de tráfico existente en la red, adquirir tecnologías de software analizadores de red de última generación, los routers de las Aduanas Subalternas deberían estar configurados para dos rutas. Una ruta con la Sede SENIAT-Caracas y otra ruta virtual que les permita conectarse con la Sede Principal de Maracaibo, se recomienda el análisis de otros parámetros para la medición del tráfico, valorar constantemente la plataforma tecnológica en cuanto a su configuración, instalación, modernización y aplicación para optimizar el funcionamiento de la red del servicio de la administración aduanera del estado Zulia.

El presente trabajo de tesis es sobre un “Rediseño de la red de voz y datos del Centro de Convenciones Eugenio Espejo”, mediante una estructura de VLANS permitiendo conceptualizar sus beneficios y ventajas de ser implementadas sobre cualquier marca de equipo, optimizando los recursos que tiene este espacio patrimonial y contribuyendo a un ahorro económico para la Empresa Pública Metropolitana de Gestión de Destino Turístico encargada de administrar este lugar como parte de su contribución con el desarrollo turístico de la ciudad de Quito.

El prototipo implementado en este proyecto de titulación une dos marcas conocidas de Switchs con servidores basados en Linux demostrando que al trabajar en conjunto se puede obtener muy buenos resultados y este diseño se constituye en una base para que se pueda en un futuro tomar la decisión de replicar el diseño en todo el Centro de Convenciones Eugenio Espejo. (Puga, 2015, p. 30)

El presente trabajo de tesis plantea una propuesta de “Segmentación con Redes de Áreas Locales Virtuales (VLANS) y priorización del Ancho de Banda con Calidad de Servicio (QoS) para la mejora del Rendimiento y Seguridad de la Red de Área Local (LAN) en la Empresa Editora El Comercio Planta Norte”.

La empresa Editora El Comercio Planta Norte posee una red plana en su diseño lo cual dificulta la administración del tráfico de la Red, debido a la ausencia de estándares de calidad en gestión de tráfico LAN, políticas de seguridad no alineadas a las necesidades de la empresa y desaprovechamiento de la performance de los equipos de comunicación instalados. Esto ha ocasionado la latencia de la red en horas pico, degradándose la velocidad de transferencia por el tráfico desmedido de la información y perjudicando o retardando los procesos más importantes en la empresa en intervalos de 60 a 90 minutos. (Molina, 2012, p. 67)

Asimismo, la información periodística enviada por los corresponsales hacia la Planta, ocasiona pérdida de tiempo en acciones de subida y descarga de archivos (Fotos, videos, infografías, avisos publicitarios, etc.). Adicionalmente, los parámetros de seguridad de la Red no garantizan la inviolabilidad de los equipos y la manipulación de la información, lo cual representa un riesgo para la integridad y desarrollo de los procesos. Por ello, se rediseñó la red para el soporte de redes LAN Virtuales y de esta manera, segmentar las áreas en subredes para un mayor nivel de protección; brindar seguridad (Listas de Control de Acceso ACLS, Tecnologías emergentes en Seguridad Windows Server 2008, Nivel de autenticación Radius); mejorar el consumo de Ancho de Banda (Calidad de Servicio QoS, Protocolo de Agregación de Enlaces de Control LACP, Troncales, etc.).

Implementar nuevos protocolos en tecnología CISCO; instalar redes inalámbricas y nuevos Servicios de transferencia de archivos (Protocolo de Transferencia de Archivos FTP) Todo ello, con el propósito de disminuir costos y elevar la productividad de la Planta Norte, haciéndola más robusta y escalable ante un crecimiento tecnológico a mediano y largo plazo.

Palabras Clave: Red de Área Local, Redes de Áreas Locales Virtuales, Protocolo de Agregación de Enlaces de Control, Listas de Control de Acceso, Radius, Calidad de Servicio, Protocolo de Transferencia de Archivos.

La presente tesis de investigación, pretende realizar la “Segmentación de la red y priorización del uso del ancho de banda, debido a que el diseño actual de la red de la Ciudad Universitaria de la Universidad Nacional de San Martín – Tarapoto”.

Es una red plana con la VLAN por defecto, en consecuencia, no existe una adecuada segmentación del dominio de colisión y dominio de broadcast, lo que repercute drásticamente en el rendimiento de la misma a nivel de transmisión de paquetes entre los edificios que son extremos de la estrella y el nodo concentrador. Esto ocasiona la latencia de la red en fechas y horas pico, degradándose la velocidad de transferencia por el tráfico desmedido y no segmentado de los datos y perjudicando o retardando los procesos académicos y administrativos. (Ramirez, 2015, p. 104)

Por ello, como parte de la solución a las necesidades identificadas en la presente investigación, se plantea el rediseño de la red para el soporte de redes LAN Virtuales, y de esta manera segmentar las áreas en subredes para un mayor nivel de protección; brindar seguridad (Listas de control de acceso ACLS, tecnologías emergentes en seguridad de Windows).

Posteriormente a la segmentación de la red, se realiza la priorización del ancho de banda de acuerdo a los segmentos VLAN creados, identificando qué edificios necesitan de un mayor ancho de banda discriminando adecuadamente su acceso en función a su prioridad, permitiendo esto mejorar el consumo de ancho de banda (Calidad de servicio QoS), implementando protocolos para mejorar la administración de la red, permitiendo disminuir costos y elevar la productividad de la UNSM).

Este proyecto de tesis propone una estrategia para la “Implementación de Virtualización en el centro de cómputo de la Oficina de tecnología de información del

Ministerio de Transporte y Comunicaciones”. Con la virtualización de equipos físicos se logra la reducción de costos en rubros como el mantenimiento, energía, espacio físico y personal necesario para la administración del equipo.

En conjunto las reducciones producen ahorros muy atractivos para las empresas que buscan la optimización de sus recursos, pero manteniendo o incrementando el nivel de los servicios de tecnologías de la información existentes. Para la ejecución del proyecto se realizó la planeación e implementación de toda una arquitectura de virtualización, la cual estuvo conformada de servidores blade y storage de la marca DELL, manejados por VMware líder en el rubro de la virtualización. (Espinoza & Lobaton, 2014, p. 49)

Como resultado, se consiguió implementar una plataforma de virtualización que sea capaz de soportar todos los servicios informáticos que se brindan, reduciendo esfuerzos en la gestión como en el área económica, e incrementando la fuerza de la solución para soportar proyectos nuevos a futuro.

La presente tesis de investigación tiene por objetivo el “Desarrollar la propuesta de Virtualización de escritorios dirigido a instituciones educativas”.

El presente trabajo de investigación tiene por objetivo analizar las diferentes soluciones de virtualización del mercado informático y a partir de ello lanzar una propuesta el cuál priorice el principal beneficio de esta tecnología, el de reducir los costos de hardware. Es conveniente encontrar la solución de este problema porque al igual que la I.E.E. “Antonio Raymondi” y el C.E.E. “Rafael Narváez Cadenillas” otras instituciones educativas se encuentran en la misma situación y encontrar una solución que haga frente a dichas necesidades sin duda permitirá tener una perspectiva diferente sobre las distintas formas en el que se puede gestionar el laboratorio de cómputo a fin de reducir la inversión de adquirir, operar y mantener su infraestructura tecnológica. (Grimson, 2015, pág. 83)

Por ello, la presente investigación plantea solucionar estos problemas a través de la virtualización de escritorios. Sin lugar a duda el tema de la virtualización es muy amplio, así como las diferentes alternativas que ofrece el mercado informático, bajo este contexto la presente investigación se centra en analizar dichas alternativas y lanzar la propuesta, es decir, proponiendo el plan de implementación, la solución software, el método de virtualización, los modelos de virtualización y el ahorro generado por cada uno de ellos.

Caso de Éxito: VMware y SOS presentan SAP en Hierro Barquisimeto:

Dedicados a comercializar productos siderúrgicos y ferreteros en la región occidental y andina de Venezuela, Hierro Barquisimeto emprendió la incorporación de la plataforma SAP, tras la evaluación junto a Suministros Obras y Sistemas (SOS) se decidió ejecutar la virtualización de su plataforma hecho que les permitió integrar tres servidores Cisco UCS 200 M1 con doble procesador Intel Xeon, Quad Core con 48 GB de memoria cada uno, 144 GB de disco en cada unidad y una SAN de 7,2 TB en almacenamiento crudo.

Resultado: En la actualidad la compañía está virtualizada en un 95% de sus operaciones en sistemas de información asimismo a comenzado a migrar sus servicios de IT a modelos más ágiles y productivos como lo es cloud computing preparándose así para su transición a la nube pública., *Figura 13.*



Figura 13. Caso de Éxito. Fuente: (Jhoanna Terán, 2011).

2.2. Estado del arte

De acuerdo con la revista en su investigación refiere.

Que la virtualización es un término que se refiere a la abstracción de los recursos de una computadora llamada Hypervisor o VMM (Virtual Machine Monitor) Crea una capa de la abstracción entre el hardware de la máquina física (host) y el sistema operativo de la máquina virtual (virtual machine, guest). (El Magazine de la Virtualizacion & Cloud Computing, 2004, p. 18)

El VMM maneja los recursos de las maquinas físicas subyacentes (designadas por el computador central) de una manera que el usuario pueda crear varias máquinas virtuales presentando a cada una de ellas una interfaz del hardware que sea compatible con el sistema operativo elegido.

En esta investigación refiere que la virtualización es una tecnología que fue desarrollada por IBM en los años 60.

La primera computadora diseñada específicamente para virtualización fue el mainframe IBM S/360 Modelo 67. Esta característica de virtualización ha sido un Standard de la línea que siguió (IBM S/370) y sus sucesoras, incluyendo la serie actual. Durante los 60s y los 70s fueron muy populares, pero las máquinas virtuales desaparecieron prácticamente durante los 80s y los 90s. (IBM System, 2009, pág. 5)

No era hasta el final de los 90s que volvió a resurgir la tecnología de las máquinas virtuales y no solamente en el área tradicional de servidores sino también en muchas otras áreas del mundo de la computación: “En la actualidad asistimos a su eclosión gracias al fuerte descenso del coste total de propiedad (TCO) atribuible a tecnologías vía hardware como Intel VT, AMD-V Pacífica, NPIV y vía software VMWare, XEN, Microsoft Hyper-V, VirtualIron.



De acuerdo con su investigación nos refiere sobre la Virtualización, ya para la década de los 80 y con la llegada de las relativamente económicas maquinas x86, comenzó una nueva era de microcomputadoras, aplicaciones cliente-servidor, y “computación distribuida”; en donde los enormes y potentes “mainframes” con mil y una tareas y utilidades en una sola caja gigantesca se comenzaron a cambiar por relativamente pequeños servidores y computadoras personales de arquitectura x86, con “una caja diferente para cada uso”, lo que se convirtió rápidamente en el estándar de la industria.

Debido a esto, una vez más, el tema de la virtualización vuelve a quedar prácticamente en el olvido y no es hasta finales de la década de los 90 que gracias al alto desarrollo del hardware volvemos a caer en un predicamento similar al que estábamos en los años 60: el hardware existente es altamente eficiente, y utilizar cada “caja” para una sola aplicación sería un desperdicio de recursos, espacio, energía y dinero; y tampoco es conveniente asignarle múltiples usos o instalar varias aplicaciones en un solo servidor convencional, por más de una razón: ej. estas aplicaciones podrían ser conflictivas entre sí, o podrían requerir diferentes configuraciones e inclusive diferentes sistemas operativos, o tener diferentes requerimientos de seguridad, entre otras variables que podrían causar problemas al ejecutar estas funciones simultáneamente. (Lopez, 2009, p. 10)

Es por esto que vuelve a resurgir la idea de dividir el hardware, de manera tal que funcione como múltiples servidores independientes, pero compartiendo los recursos de un mismo servidor físico. Y es de aquí que nace lo que hoy todos conocemos como “Virtualización”, *Figura 14*.

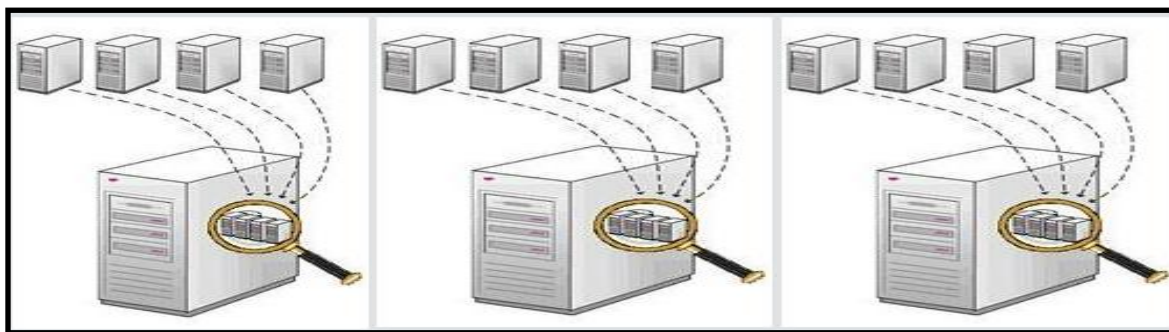


Figura 14. Virtualizando Servidores. Fuente: Eddie López (2009).



De acuerdo con su investigación refiere que la Virtualización no es nada nuevo.

Que durante la década de los 60 los equipos de informática de muchas empresas y entidades tenían un problema similar: contaban con super-computadoras o “mainframes” de alto rendimiento que deseaban “particionar lógicamente”, o utilizar para múltiples tareas simultáneas; lo que hoy conocemos como “multitasking”, trabajar más de una aplicación o proceso simultáneamente. (Buitrago, 2013, p. 4)

Es por esto que IBM desarrolló un método para crear múltiples “particiones lógicas” (similar a lo que conocemos hoy como “máquinas virtuales”) las cuales trabajaban independientemente una de las otras, y cada una utilizando los recursos provistos por el “mainframe”, *Figura 15*.

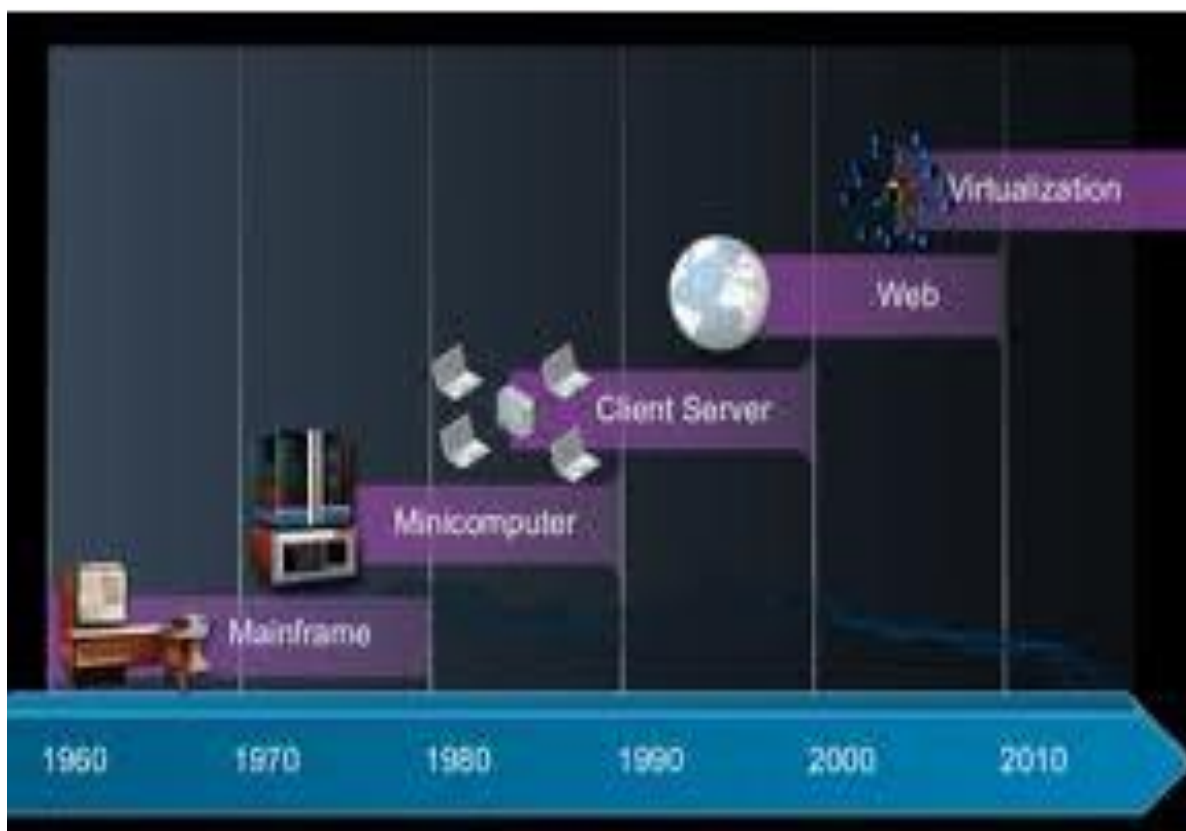


Figura 15. Etapas de la Virtualización. Fuente: Osley Antonio Buitrago Cardona (2013).

Refiere en su investigación que la Virtualización “Es una de las tecnologías más importantes de los últimos años que supone un antes y un después en la infraestructura TI de las empresas” Virtualización “Ha provocado un cambio fundamental en la forma en que se consideran y administran las infraestructuras TI de las empresas” “Según los últimos datos IDC la base de instalada de servidores se ha multiplicado por 9 en los últimos 15 años”, nos encontramos con un parque infrautilizado y con dificultades de mantenimiento.

Fue sobre los años 60 cuando IBM empezó a tener unos Hosts que ya tenían importante capacidad de computación, por lo que empezaron a pensar en que el host tuviera unas particiones lógicas, las cuales, en el año 80 personalmente empecé a escuchar con la denominación “VMs” en un CPD con un 4381 de una gran empresa española. (Gris, 2016, p. 7)

De tener un concepto de unidad física con mucha potencia, se aplicaba el tener varias unidades lógicas utilizando mejor los recursos. (Gráfico N°16).

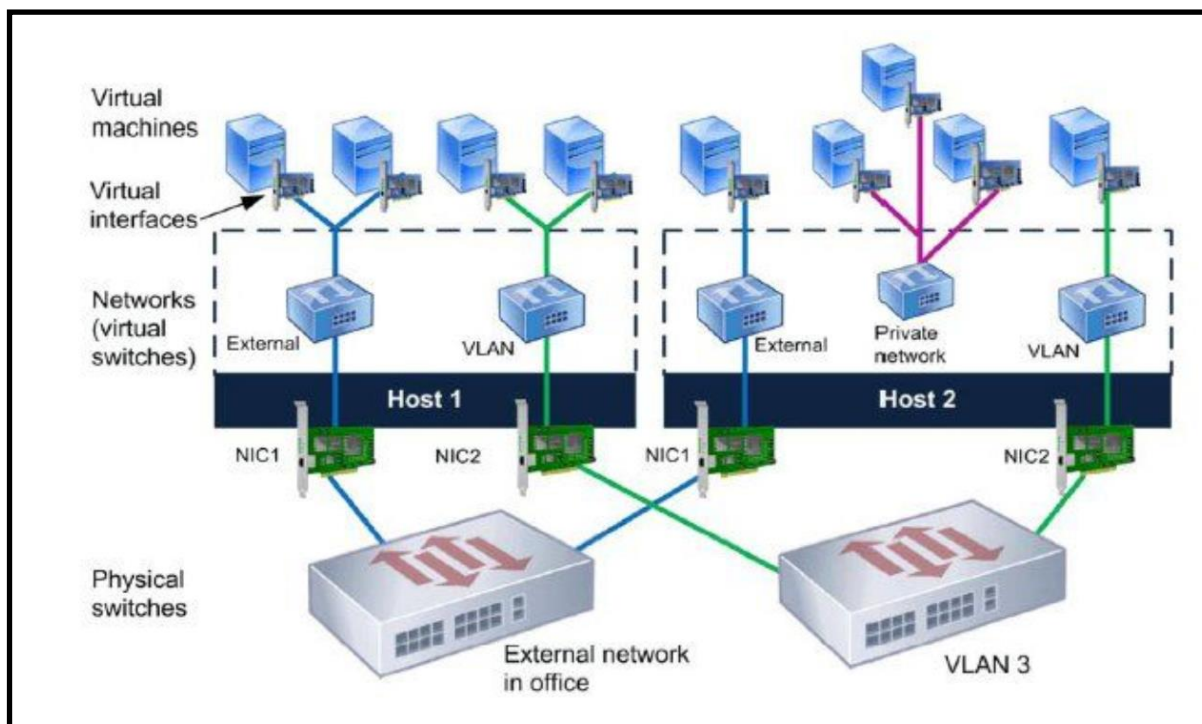


Figura 16. IBM – VMS. Fuente: José María Gris (2016).



2.3. Bases teórico científicas

2.3.1 Virtualización.

2.3.1.1 ¿Qué es lo Virtual?:

El reciente mundo del ciberespacio ha abierto nuevamente el debate acerca de lo “real” y lo “virtual”.

¿Hasta dónde una identidad creada para un juego de Internet tiene correlación con la identidad cotidiana de una persona? ¿En qué medida lo que yo pueda hacer o dejar de hacer en la red es irreal? O en todo caso, ¿es irreal? En este contexto, analicemos algunas características de la virtualización que trabaja el matemático francés Paul Pierre Levy. (Levy, 1998, p. 35)

Como primera medida hace la distinción entre la “actualización” y la “virtualización”.

Para comprender la primera hay que partir de los supuestos filosóficos que hablan de las potencialidades del ser: una persona o cosa tiene múltiples posibilidades de ser a futuro y su materialización posterior no será más que una de las resoluciones posibles para esa potencialidad.

Es básicamente uno de los principios aristotélicos, como podemos ver a continuación: “...la producción y “el llegar a ser” de los seres naturales es interna (inmanente) a ellos mismos: cada ser se realiza, opera y se desarrolla desde sí mismo y por sí mismo.

Nada externo a la semilla hace que ésta se desarrolle y convierta en un árbol. Por eso, un árbol o una semilla es un ser natural y una mesa, hecha de la madera de ese árbol no lo es sino accidentalmente: sólo en tanto en que es madera y no en tanto que es mesa.”

Por eso, y siguiendo el ejemplo, podemos decir que la mesa es una actualización de la semilla, ya que, si bien terminó siendo una mesa, también podría haber sido simplemente un árbol, una hoja de papel, etc.

Ahora bien, la virtualización se trata de una modificación en las identidades, de un cambio ontológico donde ya no hay una sola forma de resolver las potencialidades, no hay actualidad, sino que es una complejización de la realidad (no se opone a ella).

Aquí estamos hablando de múltiples formas, múltiples resoluciones a las potencialidades, de un convivir con esa variedad y mutar constantemente.

Las novedades de la virtualización:

¿Qué fue lo que hizo que haya un cambio en la percepción de la realidad? ¿Qué tiene lo virtual que no tenía lo actual?

Pues bien, Levy presenta tres características principales:

1. Desterritorialización: Lo virtual rompe con las barreras geográficas y temporales. Nos permite transitar por lugares lejanos simplemente con entrar al Google Earth, leer diarios de España, Sudáfrica, Australia, etc. etc. Pero, además, la virtualidad crea sus propios espacios, sus propios mundos si se quiere.

Juegos como el Second Life permiten que los usuarios construyan sus casas, sus ciudades, sus vidas en última instancia; y si bien no hay una materialización de esos lugares, no por eso dejan de ser reales, más bien existen en esa realidad virtual (haciendo Control+clic en la imagen del Second Life se podrá ver un breve video del juego en YouTube).

A su vez, el tiempo también se modifica. Ahora, paradójicamente, el ahora convive (paradójicamente) con muchos tiempos pasados y futuros.



Por ejemplo, el sencillo acto de mandar un mail supone una interacción entre dos personas que puede no ser en simultáneo: yo le escribo un correo electrónico ahora a mi mamá y ella recién lo lee mañana a la tarde, pero lo lee, y allí está la recepción de mi mensaje. El software de chat Messenger presenta en sus últimas versiones la posibilidad de que varios usuarios le dejen un mensaje escrito a una persona y ésta los lea recién cuando abre su Messenger, así sea un mes después y en una computadora ajena. Estas y otras situaciones más dan cuenta de esta desterritorialización en la que el aquí y él ahora se han separado.

- 2. Efecto Moebius:** La cinta de Moebius es una superficie de dos dimensiones con un solo lado por la cual, por ejemplo, se puede desplazar un objeto infinitamente. Esta concepción física es trabajada en la virtualidad para dar cuenta de la constante ir y venir entre lo público y lo privado que se produce allí. Al conectarse a la red un sujeto se pone inmediatamente en contacto con millones y millones de computadoras en el mundo que tienen tanto acceso a los distintos lugares del ciberespacio como él y con las que incluso puede compartir archivos, dialogar (mediante chat, por ejemplo) y demás.

Pero a la vez, esa misma persona tiene la posibilidad de construir un espacio privado donde recibe correos electrónicos, guarda sus fotos, sube videos, etc. En esos casos, utiliza una cuenta propia y una contraseña que le permite (en teoría) ser el único en poder ingresar allí. Ahora bien, el efecto Moebius vuelve una vez más cuando esa persona puede, al mismo tiempo, compartir ese espacio con los demás, y así tenemos ejemplos como los de los floggers que hacen cuentas en páginas donde pueden “colgar” sus fotos y mostrárselas a sus contactos. A la vez, mientras que se pasa de lo público a lo privado, también se puede pasar de un mundo “real” a uno virtual. Y entendamos en este caso lo real como lo cotidiano, lo materializado fuera del ciberespacio.

Así, podemos ver por ejemplo que mientras una persona está navegando y revisando su cuenta de correo electrónico, puede al mismo tiempo estar jugando un juego de simulación donde tiene una vida completamente diferente, incluso hasta con otro sexo.

- 3. Colectivización:** Tiene que ver con los dos aspectos señalados anteriormente y con una convivencia permanente con millones y millones de personas en el mundo con las que además interaccionamos de una u otra forma.

En Internet casi todo es compartido e incluso en el ámbito informativo el conocido paradigma de que “me copien lo menos posible”, de la originalidad, ha dado lugar a una concepción de multiplicación y de “aparecer citado en muchos lugares”. Se relaciona precisamente con fluir dentro de ese enmarañado mundo virtual.

2.3.2 Virtualización y Estetización de La Arquitectura Actual

2.3.2.1 La hipótesis de la an-estética de la Arquitectura.

De acuerdo con (Leach, 2001) la hipótesis del libro es simple, verifica la disolución de la esencia arquitectónica por su comercialización y virtualización. Al inicio de la argumentación, Leach se basa en los escritos ampliamente conocidos de Jean Baudrillard; este filósofo francés, quien a lo largo de su desarrollo intelectual en el mercado internacional de ideas se convirtió en el teólogo de la virtualización, diagnosticó la desaparición de la cultura material en sus fotocopias y simulacros digitales.

El resumen de esta hipótesis, bastante conocida y criticada, enmarca la argumentación de Leach.

No sólo estructura el desarrollo de ideas, sino también caracteriza –involuntariamente– el concepto intelectual del autor: su libro es un montaje interminable de fotocopias de textos ya conocidos, incluso anacrónicos. Así, retomar y refritear a Baudrillard es el hilo conductor del libro de Leach, y una confirmación posterior del refutable filósofo francés. Un recorrido por el montaje de ideas sueltas demuestra la disciplina intelectual de Leach.

Su mayor logro fue la invención del título que en el original inglés –anaesthetics– combina anestésica y anestesia (p. 8). Tal proceso de abolición de la arquitectura, que "se reduce a un juego de formas vacías y seductoras" (p. 9), está explicado en cinco capítulos.

- a. El primer capítulo, llamado "La saturación de la imagen" (pp. 13-35). reincide en el lamento por la pérdida de los significados culturales en los tiempos de la sobreproducción de imágenes en un nivel global (pp. 16-18).
- b. En el segundo capítulo, "El arquitecto como fascista" (pp. 37-60), continúa la argumentación sumamente banal. Tal título sugiere un análisis del concepto político del fascismo, y la relación del arquitecto con un sistema de represión dictatorial.
- c. En el tercer capítulo, "La estética de la embriaguez" (pp. 61-92), Leach presenta exactamente esta misma selección de pensadores urbanos, que desde hace más de veinte años no faltan en cualquier libro sobre cultura urbana.
- d. El penúltimo capítulo, "La arquitectura de la pasarela" (pp. 93-118), además de repetir las débiles ideas del autor, introduce el movimiento situacionista alrededor del artista Guy Debord, que contiene gran potencial reflexivo sobre el tema general de la anestésica arquitectónica.



- e. Agotado por tanta desesperación con la lectura del libro, es casi imposible soportar el último capítulo, "Seducción, el último refugio" (pp. 119-144), que concluye la débil argumentación con otra exégesis de Baudrillard, muy lejos del objeto de estudio, la arquitectura.

En este último paso de un aburrido camino por las 144 páginas, el autor utiliza la tesis equivocada de que la seducción visual de la arquitectura "nunca puede ser crítica" (p. 132), para desprestigiar a sus colegas académicos de la escuela londinense de arquitectura.

Casi es el tono de una secta fundamentalista que tiene prohibido percibir y crear imágenes, el que Leach usa para criticar las tendencias arquitectónicas actuales que se fijan en la superficie (p. 140); en lugar del complejo análisis de este fenómeno, prevalece la reducción moral al vituperar el "juego vacío y persuasivo de las apariencias, donde la crítica pierde su fuerza y la complacencia y la fascinación se le adelantan" (p. 143).

2.3.3 Concentradores de cableado (Nivel Físico): HUB Y MAU.

2.3.3.1 Puente o Bridge (Nivel Enlace)

Los puentes, tal como su nombre lo indica, proporcionan las conexiones entre LAN. Los puentes no sólo conectan las LAN, sino que además verifican los datos para determinar si les corresponde o no cruzar el puente. Esto aumenta la eficiencia de cada parte de la red. (Ordoñez, 2014, p. 265)

Conmutadores o switch (Nivel Enlace):

Los SWITCH son otros equipos más actuales que centralizan el cableado y mejoran la velocidad de la red evitando colisiones en lo posible. Muy usados en redes de área local Ethernet.

Diferencias entre: HUB o Concentrador, Switch o Conmutador.

HUB o Concentrador

- a. Tecnología compartida
- b. Ancho de banda repartido entre puertos
- c. Manda lo que recibe a todos los puertos
- d. Produce colisiones
- e. Solo permite una comunicación en un instante determinado.
- f. Trabaja en modo Simplex o half duplex

Switch o Conmutador

- a. Tecnología conmutada
- b. Ancho de banda completo para cada puerto
- c. Aprende dónde está cada uno y solo lo envía al destinatario.
- d. Produce menos colisiones
- e. Permite hasta N.º puertos/2 comunicaciones instantáneas
- f. Trabaja en modo half o full Duplex
- g. Permite a switch avanzados Port Trunking y VLAN

Características de un Switch:

- a. **Opera con funciones de bridge, interconectando segmentos de la red.**
- b. **Realiza la conmutación trabajando a nivel MAC (Ethernet), necesita aprender las direcciones MAC: control de errores y lectura de las cabeceras MAC (direccionamiento).**

- c. **No son dispositivos de medio compartido, disminuyendo la probabilidad de colisiones.** Permite que haya diferentes tramas, en diferentes puertos, fluyendo simultáneamente.
- d. **Pueden ser half o full duplex.**
- e. **Proporciona mayor ancho de banda.** El cálculo del mismo depende de la velocidad y el tipo de puertos existentes.

Tipos de Switch. Existen diferentes técnicas de conmutación:

- a. **Fast forward (cut-through):** La trama se conmuta al puerto de salida nada más conocer la dirección MAC. Sólo es necesaria la cola de salida.
 - a.1. **Ventaja:** Disminuye la latencia.
 - a.2. **Inconvenientes:** Requiere la misma velocidad en ambos puertos y no implementa control de errores.
- b. **Store and forward:** Espera hasta que recibe completamente la trama para conmutarla.
 - b.1. **Ventajas:** Almacena la trama completa, por lo que puede realizar control de errores o incluso filtrado de la misma.
 - b.2. **Inconvenientes:** Aumenta la latencia.

Otras clasificaciones de Switches:

1. Por velocidad: 10, 100, 1000, 10000 Mbps.
2. Aislados, apilables y tipo chasis.
3. Según las diferentes posibilidades ofrecidas a nivel superior (conmutación nivel 3).
4. Según el sistema de gestión.

Características Adicionales:

1. Agrupación de puertos (**port trunk**), es un medio para unir dos Switchs mediante dos o más puertos y por lo tanto aumentar el ancho de banda de la conexión entre los Switchs.
2. Protocolo de encaminamiento: **Spanning tree. Spanning Tree Protocol (STP)** es un protocolo de red de la segunda capa. 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 que la topología está libre de lazos. STP es transparente a las estaciones de usuario.
3. Norma 802.1D en este documento, se proporciona información sobre las mejoras agregadas por RSTP al estándar 802.1D anterior. **El estándar Spanning Tree Protocol (STP) 802.1D** fue diseñado en un momento en que la recuperación de la conectividad después de una interrupción de un minuto más o menos se consideraba un rendimiento adecuado.

Con la llegada del switching de capa 3 en entornos de LAN, el bridging ahora compite con soluciones ruteadas donde los protocolos, como Open Shortest Path First (OSPF) y Enhanced Interior Gateway Routing Protocol (EIGRP), pueden proporcionar una trayectoria alternativa en menos tiempo. Cisco mejoró la especificación 802.1D original con funciones como UplinkFast, BackboneFast y PortFast para acelerar el tiempo de convergencia de una red puenteada. La desventaja es que estos mecanismos son de propiedad exclusiva y requieren configuración adicional.

Rapid Spanning Tree Protocol (RSTP; IEEE 802.1w) se puede considerar una evolución del estándar 802.1D, más que una revolución. La terminología de 802.1D sigue siendo fundamentalmente la misma. La mayoría de los parámetros no se han modificado para que los usuarios familiarizados con 802.1D pueden configurar rápidamente el nuevo protocolo sin problemas.

En la mayoría de los casos, RSTP se desempeña mejor que las extensiones de propiedad exclusiva de Cisco sin ninguna configuración adicional. 802.1w también se puede invertir nuevamente a 802.1D para interoperar con bridges heredados por puerto.

Esto descarta los beneficios que presenta. La nueva edición del estándar 802.1D, IEEE 802.1D-2004, incorpora los estándares IEEE 802.1t-2001 e IEEE 802.1w.

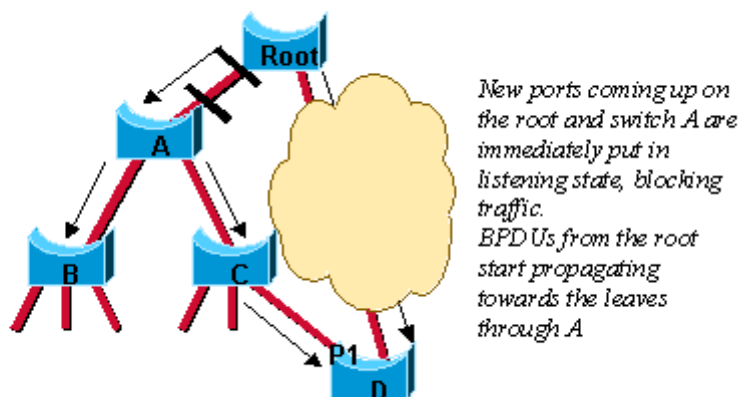
Plataforma Catalyst	MST con RSTP	RPVST+ (también conocido como PVRST+)
Catalyst 2900XL/3500XL	No disponible	No disponible
Catalyst 2940	12.1(20)EA2	12.1(20)EA2
Catalyst 2950/2955/3550	12.1(9)EA1	12.1(13)EA1
Catalyst 2970/3750	12.1(14)EA1	12.1(14)EA1
Catalyst 3560	12.1(19)EA1	12.1(19)EA1
Catalyst 3750 Metro	12.1(14)AX	12.1(14)AX
Catalyst 2948G-L3/4908G-L3	No disponible	No disponible
Catalyst 4000/2948G/2980G (CatOS)	7.1	7.5
Catalyst 4000/4500 (IOS)	12.1(12c)EW	12.1(19)EW
Catalyst 5000/5500	No disponible	No disponible
Catalyst 6000/6500	7.1	7.5
Catalyst 6000/6500 (IOS)	12.1(11b)EX, 12.1(13)E, 12.2(14)SX	12.1(13)E
Catalyst 8500	No disponible	No disponible

Figura 17. Soporte de RSTP en Switches Catalyst. Fuente: Introducción al Rapid Spanning Tree Protocol Cisco (2017).



Convergencia con 802.1d

En este diagrama, se ilustra cómo 802.1D se ocupa de un nuevo link que se agrega a una red puentada:



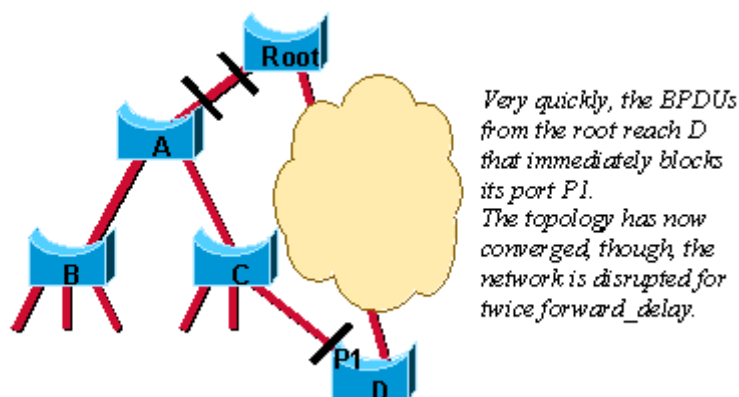
En esta situación, se agrega un link entre el bridge root y el Bridge A. Suponga que ya hay una conexión indirecta entre el Bridge A y el bridge root (a través de C-D en el diagrama).

El STA bloquea un puerto e inhabilita el loop de bridging. Primero, cuando aparecen, ambos puertos en el link entre la root y el Bridge A se ponen en el estado de escucha.

El Bridge A ahora puede escuchar a la root directamente. Propaga inmediatamente sus BPDUs en los puertos designados, hacia las hojas del árbol de spanning tree.

Tan pronto como los Bridges B y C reciben esta nueva información superior del Bridge A, retransmiten inmediatamente la información hacia las hojas. En unos pocos segundos, el Bridge D recibe una BPDUs de la root y bloquea de forma instantánea el puerto P1.





El spanning tree es muy eficiente en la manera en que calcula la nueva topología de la red. El único problema ahora es que debe transcurrir el doble de demora de reenvío antes de que el link entre la root y el Bridge A terminen finalmente en el estado de reenvío.

Esto significa 30 segundos de interrupción del tráfico (se aíslan las partes enteras A, B y C la red) porque el algoritmo de 802.1D no tiene un mecanismo de retroalimentación para anunciar claramente que la red converge en cuestión de segundos.

Convergencia con 802.1w

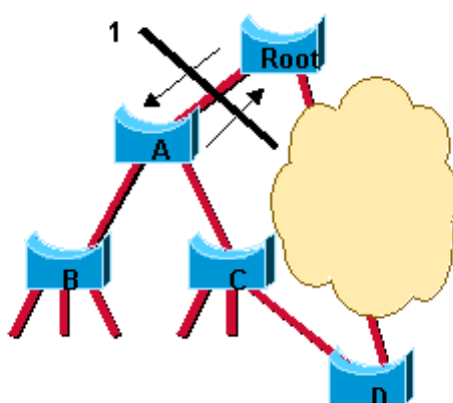
Ahora, usted puede ver cómo RSTP se ocupa de una situación similar. Recuerde que la topología final es exactamente la misma que la calculada por 802.1D (es decir, un puerto bloqueado en el mismo lugar que antes). Solamente los pasos utilizados para llegar a esta topología han cambiado.

Se ponen ambos puertos en el link entre A y la raíz en estado de bloqueo designado en cuanto aparecen.

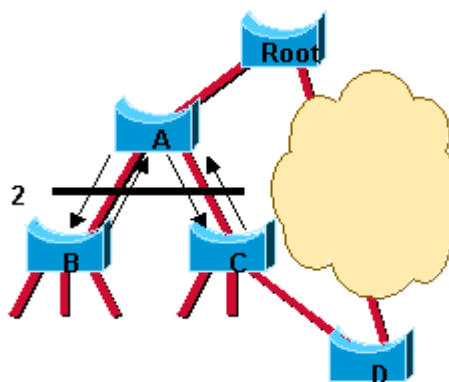
Hasta el momento, todo se comporta como en un entorno puro de 802.1D. Sin embargo, en esta etapa, ocurre una negociación entre el Switch A y el root.

Tan pronto como A recibe la BPDU del root, bloquea los puertos designados que no son de borde. Esta operación se denomina sincronización.

Una vez realizado esto, el Bridge A autoriza explícitamente al bridge root para poner su puerto en el estado de reenvío. En este diagrama, se ilustra el resultado de este proceso en la red. El link entre el Switch A y el bridge root se bloquea y ambos bridges intercambian BPDU.



Una vez que el Switch A haya bloqueado sus puertos designados que no son de borde, el link entre el Switch A y la root se pondrá en el estado de reenvío y usted llegará a la situación:



Todavía no puede haber un loop. En lugar de bloquear *arriba* del Switch A, la red ahora bloquea *debajo* del Switch A. Sin embargo, el posible loop de bridging se corta en una ubicación diferente. Este corte viaja hacia abajo del árbol junto con las nuevas BPDU originadas por la root a través del Switch A.

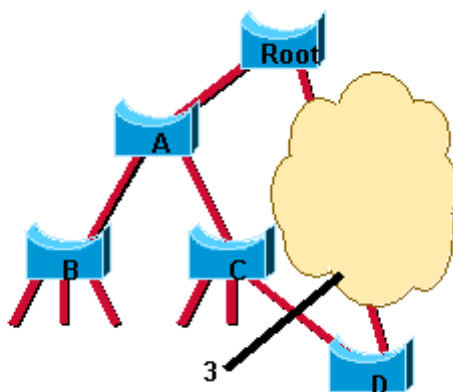


En esta etapa, los puertos recientemente bloqueados en el Switch A también negocian una transición rápida al estado de reenvío con sus puertos vecinos en el Switch B y el Switch C que ambos inician una operación de sincronización.

Con excepción del puerto root hacia A, el Switch B tiene solamente puertos designados de borde.

Por lo tanto, no tiene ningún puerto para bloquearlo a fin de autorizar al Switch A para pasar al estado de reenvío.

Del mismo modo, el Switch C debe bloquear su puerto designado para D. Ahora se llega al estado que se muestra en este diagrama:



Recuerde que la topología final es exactamente la misma que la que se muestra en el ejemplo de 802.1D, lo que significa que el puerto P1 en D termina en bloqueo.

Esto significa que se llega a la topología de red final, justo a tiempo para que las nuevas BPDUs viajen hacia abajo del árbol.

No participa ningún temporizador en esta convergencia rápida.

El único nuevo mecanismo introducido por RSTP es el reconocimiento de que un switch puede enviar en su nuevo puerto root para autorizar la transición inmediata al estado de reenvío y omite las etapas de escucha y aprendizaje largas del doble de demora de reenvío.

El administrador solo debe recordar esto para beneficiarse de la convergencia rápida:

- a. Esta negociación entre los bridges es solo posible cuando los bridges están conectados por links punto a punto (es decir, links de dúplex completo, a menos que haya una configuración de puerto explícita).
- b. Los puertos de borde tienen una función aún más importante ahora que PortFast se habilita en puertos en 802.1D. Por ejemplo, si el administrador de la red no puede configurar correctamente los puertos de borde en B, su conectividad es afectada por el link entre A y la root que aparece.
- c. Busca el camino más eficiente. Coste de enlace
- d. Robustez frente a fallos de enlace
- e. Evita bucles infinitos
- f. **VLAN LAN Virtuales** (Virtual LAN). 802.1Q, VLT, Pág. 146-147
Libro Texto.
- g. **Fast IP**
 1. Opera con funciones de router, interconectando VLAN.
 2. Realiza la conmutación trabajando a nivel IP o superior.



Métodos de gestión del switch:

Al igual que en el hub, se puede establecer dos clasificaciones posibles para la gestión del switch:

- a. La primera de ellas se basa en el tipo de puerto al cual se conecta el equipo de gestión.
- b. La segunda clasificación está en función del servidor utilizado para la gestión:

Equipos nivel (1 y 2) para WLAN (Redes locales inalámbricas).

Wi-Fi es una marca de la **Wi-Fi Alliance** (anteriormente la WECA: Wireless Ethernet Compatibility Alliance), la organización comercial que adopta, prueba y certifica que los equipos cumplen **los estándares 802.11**.

2.4. Definición de términos básicos

- a. **ADAPTADOR**, Dispositivo que añade funcionalidad de red a su equipo.
- b. **ANCHO DE BANDA**, Capacidad de transmisión de un dispositivo o red determinado.
- c. **BALANCEO DE PETICIONES ENTRANTES**, Forma de procesamiento de la información proveniente de Internet (Tráfico entrante) la cuál es distribuida ordenadamente a través de la red local (LAN).
- d. **BPS**, Bits Por Segundo; se refiere a la velocidad a la que la información es enviada sobre una conexión lógica ("data link")
- e. **BROADCAST**, Se refiere al mensaje que se envía a todas las estaciones en una conexión lógica ("data link") multipunto.
- f. **CHANNEL (CANAL)**, También se le denomina circuito, línea, "Path". Es un medio, físico o lógico, para mover datos en una dirección. Un canal puede ser **SIMPLEX** si los datos se envían siempre en una sola dirección o **HALF DUPLEX** si se envía información en ambas direcciones alternadamente. Dos canales se pueden combinar para proveer transmisión **FULL DUPLEX**. Frecuentemente nos referimos a estos dos canales como un canal **FULL DUPLEX**.
- g. **CHECKPOINT**, Es la manera en que IBM llama la operación continua de ARQ de su protocolo SDLC.
- h. **CONMUTADOR**, es un Dispositivo que es el punto central de conexión de equipos y otros dispositivos de una red, de forma que los datos puedan transmitirse a velocidad de transmisión completa.
- i. **CONVERGENCIA**, velocidad y capacidad de un grupo de dispositivos de internetwork que ejecutan un protocolo de enrutamiento específico para coincidir con la topología de una internetwork después de un cambio en esa topología.
- j. **DATA NETWORKING**: Estado al que se llega después de haber implementado una red de dispositivos de cómputo comúnmente denominada Red LAN, se dice que al estar conectados todos estos dispositivos se conforma una red de datos.
- k. **DHCP** (Protocolo de configuración dinámica de host), protocolo que permite a un dispositivo de una red, conocido como servidor DHCP.
- l. **DESCARGAR**, Recibir un archivo transmitido a través de una red.



- m. **DIRECCIÓN IP**, dirección que se utiliza para identificar un equipo o dispositivo en una red.
- n. **DDNS (SISTEMA DINÁMICO DE NOMBRES DE DOMINIO)**, Permite albergar un sitio Web, servidor FTP o servidor de correo electrónico con un nombre de dominio fijo (por ejemplo, www.xyz.com) y una dirección IP dinámica.
- o. **DNS (SERVIDOR DE NOMBRES DE DOMINIO)**, La dirección IP de su servidor ISP, traduce nombres de los sitios Web a direcciones IP.
- p. **DOMAINKEYS**: Sistema de autenticación de correo electrónico designado a verificar el dominio DNS de un emisor de correo electrónico y la integridad del mensaje.
- q. **DSL (LÍNEA DE SUSCRIPTOR DIGITAL)**, Conexión de banda ancha permanente a través de las líneas de teléfono tradicionales.
- r. **DSSS (ESPECTRO DE DISPERSIÓN DE SECUENCIA DIRECTA)**, Transmisión de la frecuencia con un patrón de bit redundante que se traduce en una menor probabilidad de que la información se pierda durante dicha transmisión.
- s. **DTIM (MENSAJE DE INDICACIÓN DE TRÁFICO DE ENTREGA)**, Mensaje incluido en paquetes de datos que puede aumentar la eficacia inalámbrica.
- t. **DÚPLEX COMPLETO**, La disponibilidad de un dispositivo de red para recibir y transmitir datos de forma simultánea.
- u. **DÚPLEX MEDIO**, Transmisión de datos que puede producirse en dos direcciones a través de una única línea, sólo en una dirección cada vez.
- v. **EAP (PROTOCOLO DE AUTENTICACIÓN EXTENSIBLE)**, Protocolo general de autenticación que se utiliza para controlar el acceso a redes. Muchos métodos de autenticación específicos trabajan dentro de este marco.
- w. **EAP-PEAP** (Protocolo autenticación extensible-Protocolo autenticación extensible protegido).
- x. **EAP-TLS** (Protocolo de autenticación extensible-Seguridad de la capa de transporte)
- y. **EL PROTOCOLO DE DESCUBRIMIENTO DE CISCO (CDP, CISCO DISCOVERY PROTOCOL)**, es un protocolo propiedad de Cisco que puede configurarse en todos los dispositivos de Cisco.

- z. **ENRUTADOR**, dispositivo de red que conecta redes múltiples, tales como una red local e Internet.
- aa. **ETHERNET**, protocolo de red estándar de IEEE que especifica la forma en que se colocan los datos y se recuperan de un medio de transmisión común.
- bb. **FIBRA ÓPTICA**, medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir.
- cc. **FIREWALL**, elemento utilizado en redes de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas.
- dd. **GATEWAYS**, Dispositivo de una red que sirve como punto de acceso a otra red.
- ee. **GBPS**, Giga Bits Por Segundo; se refiere a billones americanos (miles de millones) de bits por segundo.
- ff. **HALF DUPLEX TRANSMISIÓN**, Se refiere a el diálogo entre dos estaciones donde ninguna estación enviará datos mientras la otra está enviando datos.
- gg. **HOSTS**, sistema de computación en una red.
- hh. **HTTP** (Protocolo de transferencia de hipertexto), protocolo de comunicaciones utilizado para conectarse a servidores de la World Wide Web.
- ii. **IP**, protocolo de Internet. Protocolo de capa de red en el stack TCP/IP que brinda un servicio de internetworking sin conexión.
- jj. **IPv6**, protocolo de capa de red para trabajos de Internet conmutados por paquetes. Sucesor de IPv4 para uso general en Internet.
- kk. **LAN**, el término Red de área local (LAN) hace referencia a una red local, o a un grupo de redes locales interconectadas, que están bajo el mismo control administrativo.
- ll. **LOOP**, Arreglo de comunicaciones multipunto donde las estaciones se conectan en forma de anillo o "loop". Todas las estaciones llevan a cabo la función de almacenaje y envío de datos. La estación anfitriona o "host" envía datos en una dirección "downlink direction" y recibe datos en otra dirección "uplink direction".
- mm. **LRC**, Siglas en inglés para "Longitudinal Redundancy Checking". Este es el proceso de verificación de errores cuando se envían datos sobre un "data link"
- nn. **LOOPBACK**: 127.0.0.1 es una dirección IP disponible en todos los dispositivos para ver si la tarjeta NIC de ese dispositivo funciona.

- oo. **MAP**, Siglas en inglés para "Manufacturing Automation Protocol". Protocolo diseñado por la compañía General Motors, como un esfuerzo para definir ciertos estándares del modelo OSI que aplican a este tipo de compañía de manufactura automatizada.
- pp. **MÁSCARA DE SUBRED**, Código de dirección que determina el tamaño de la red.
- qq. **MBPS (MEGABITS POR SEGUNDO)**, Un millón de bits por segundo, unidad de medida de transmisión de datos.
- rr. **MHZ**, Equivale a 106 hercios (1 millón). Se utiliza muy frecuentemente como unidad de medida de la frecuencia de trabajo de un dispositivo de hardware.
- ss. **MIRC**, Programa de Internet Relay Chat que se ejecuta bajo Windows.
- tt. **MÓDEM DE CABLE**, un dispositivo que conecta un equipo a la red de la televisión por cable que a su vez se conecta a Internet.
- uu. **MODEM FULL DUPLEX**, Provee un canal para el envío de información en cualquier dirección. Se requiere este tipo de modem para que dos estaciones puedan enviarse información a la misma vez.
- vv. **MODEM HALF DUPLEX**, Este modem permite el envío de información en una dirección en algún momento. Este tipo de módem no puede enviar información mientras otro modem al final del "data link" está enviando información.
- ww. **MULTICAST MULTIDIFUSIÓN**, Técnica que permite que copias de un solo paquete se transfieran a un subconjunto seleccionado de todos los posibles destinos.
- xx. **NVRAM**, memoria de acceso aleatorio no volátil. Memoria de acceso aleatorio que, cuando la computadora se apaga, el contenido de la NVRAM permanece allí.
- yy. **PoE**, (Alimentación a través de Ethernet), tecnología que permite a un cable de red Ethernet transmitir tanto datos como corriente.
- zz. **PPTP** (Protocolo de túnel punto a punto), protocolo VPN que permite tunelar el protocolo Punto a punto (PPP) a través de una red IP.
- aaa. **PUERTA DE ENLACE**, un dispositivo que interconecta redes con protocolos de comunicaciones diferentes e incompatibles.
- bbb. **PUERTO**, punto de conexión en un equipo o dispositivo de red utilizado para conectar un cable o adaptador.

- ccc. **PUNTO DE ACCESO**, dispositivo que permite a los equipos y a otros dispositivos equipados con función inalámbrica comunicarse con una red con cable.
- ddd. **RAPID SPANNING TREE PROTOCOL (RSTP)**, es un protocolo de red de la segunda capa OSI, (nivel de enlace de datos), que gestiona enlaces redundantes
- eee. **RED TRONCAL**, parte de una red que conecta la mayoría de los sistemas y los une en red, así como controla la mayoría de datos.
- fff. **RED**, serie de equipos o dispositivos conectados con el fin de compartir datos, almacenamiento y la transmisión entre usuarios.
- ggg. **ROUTER**: Dispositivo de capa de red que usa una o más métricas para determinar la ruta óptima a través de la cual se debe enviar el tráfico de red.
- hhh. **ROUTING**, el proceso de mover un paquete de datos de fuente a destino, normalmente se usa un Router.
- iii. **RUTA SUMARIZADA**, la sumarización de ruta reduce el número de rutas que el router debe mantener.
- jjj. **SERVIDOR**, cualquier equipo cuya función en una red sea proporcionar acceso al usuario a archivos, impresión, comunicaciones y otros servicios.
- kkk. **SHELL SEGURO (SSH)**, es un protocolo que proporciona una conexión de administración segura (cifrada) a un dispositivo remoto.
- lll. **SMTP (Simple Mail Transfer Protocol)**, protocolo de correo electrónico estándar de Internet.
- mmm. **SPANNING TREE PROTOCOL (STP)**, es un protocolo de capa 2 que se ejecuta en bridges y switches.
- nnn. **SSID (Service Set Identifier)**, nombre de su red inalámbrica. Tasa TX Tasa de transferencia.
- ooo. **SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)**, Protocolo de control y supervisión de redes ampliamente extendido.
- ppp. **STDM, Statistical Time Division Multiplexing Multiplexado por división estadística de tiempo.** Tecnología de multiplexado que ofrece un ancho de banda variable de acuerdo a los requerimientos.
- qqq. **TCP (Transport Control Protocol)**, un protocolo de red para la transmisión de datos que requiere la confirmación del destinatario de los datos enviados.



- rrr. **TCP/IP** (Transport Control Protocol / Internet Protocol), protocolo de red para la transmisión de datos que requiere la confirmación del destinatario de los datos enviados.
- sss. **TELNET**, comando de usuario y protocolo TCP/IP que se utiliza para acceder a equipos remotos.
- ttt. **Topología**, distribución física de una red.
- uuu. **TZ, PRO y E-Class NSA**, modelos de “Firewalls” comercializados por la firma Sonicwall.
- vvv. **UNICAST (LA UNIDIFUSIÓN O DIFUSIÓN ÚNICA)**, Es el envío de información desde un único emisor a un único receptor.
- www. **VDC (VIRTUAL DEVICE CONTEXTS)**, se puede utilizar para virtualizar el propio dispositivo, presentando el switch físico como múltiples dispositivos lógicos
- xxx. **VPN** (Red privada virtual), Medida de seguridad para proteger los datos a medida que abandona una red y pasa otra a través de Internet.
- yyy. **WAN** (Wide Area Network), Grupo de equipos conectados en red en un área geográfica extensa.
- zzz. **WEP** (Wired Equivalent Privacy), Protocolo de seguridad para redes inalámbricas.

- aaaa. **Wireless**, tipo de comunicación en la que no se utiliza un medio de propagación físico alguno esto quiere decir que se utiliza la modulación de ondas electromagnéticas.
- bbbb. **WLAN** (Wireless Local Area Network), grupo de equipos y dispositivos asociados que se comunican entre sí de forma inalámbrica.
- cccc. **WPA** (WiFi Protected Access), Es un protocolo de seguridad para redes inalámbricas que se fundamenta en los cimientos básicos de WEP.
- dddd. **802.11^a**: Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 54 Mbps y una frecuencia de funcionamiento de 5 GHz.
- eeee. **802.11b**: Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 11 Mbps y una frecuencia de funcionamiento de 2,4 GHz.
- ffff. **802.11g**: Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 54 Mbps y una frecuencia de funcionamiento de 2,4 GHz y con compatibilidad con versiones anteriores con dispositivos 802.11b.



- gggg. **IEEE 802.1D**, Estándar de la IEEE para el nivel de acceso de control para puentes o "bridges" inter LAN, entrelazando redes IEEE 802.3, 802.4 y 802.5.
- hhhh. **IEEE 802.1Q**, Estándar IEEE que evolucionó a partir del protocolo ISL (enlace entre conmutadores) de Cisco Systems. Sin embargo, ISL y 802.1Q no son intercambiables. La referencia 802.1Q se conoce también como red local virtual (VLAN) o estándar de conmutación por marcado.
- iiii. **IEEE 802.1w**, Es una evolución del Spanning Tree Protocol (STP), reemplazándolo en la edición 2004 del 802.1d.

CAPÍTULO III: MARCO METODOLÓGICO

3.1. Metodología Lifecycle Services de Cisco

De acuerdo con (Cisco, 2006) el enfoque de Lifecycle Services de Cisco define el conjunto mínimo de actividades necesarias, por tecnología y por nivel de complejidad de la Red, para ayudar a los clientes a instalar y operar exitosamente tecnologías de Cisco, y optimizar su desempeño a través del ciclo de vida de la red.

3.1.1. Tipo y diseño de la investigación.

Por las características la presente espera poder caracterizar al fenómeno a estudiar, esta investigación es de tipo **Aplicada y diseño Cuasi Experimental**.

3.1.2. Tipo de investigación.

Aplicada: En la presente investigación se hará uso de los conocimientos teóricos de TI, para desarrollar la propuesta de virtualización de dispositivos de conmutación para optimizar los servicios de la Red LAN, asimismo los usuarios tendrán mejoras en los flujos de información y las transacciones de registros serán oportunas mediante el uso de los aplicativos institucionales, aplicando los procesos de planificación vigentes para dar solución a la realidad problemática del HNERM-EsSALUD en estudio.

3.1.3. Diseño de la investigación.

Cuasi Experimental:

En el presente estudio de investigación es cuasi experimental porque a través de la investigación se puede realizar la virtualización de dispositivos de conmutación con el fin de Optimizar los servicios de la Red LAN en el HNERM.

3.2. Población y muestra.

3.2.1. Población.

La Población está definida por los dispositivos de conmutación a virtualizar en el HNERM-EsSALUD y será finita y tendrá un tamaño universal de 135.

3.2.2. Muestra.

El instrumento se aplicará a los dispositivos de conmutación a virtualizar de tal manera que los valores de la probabilidad de la ocurrencia serán operados de forma porcentual.

Tabla 2
Población y Muestra

Descripción	Población	Tamaño Muestra
Los dispositivos de conmutación a virtualizar	Finita	135

Fuente: Elaboración Propia (2017).

Resultado de Formula de Muestreo con población Finita.

$$n = \frac{n_0}{1 + \frac{n_0}{N}}$$

donde: $n_0 = p * (1 - p) * [Z(1 - \frac{\alpha}{2})]^2$



Tabla 3
 Calculo con Formula de Muestreo con poblacion Finita

N [tamaño del universo]	135	← Escriba aquí el tamaño del universo
p [probabilidad de ocurrencia]	0.5	← Escriba aquí el valor de p
Nivel de Confianza (alfa)	1-alfa/2	z (1-alfa/2)
90%	0.05	1.64
95%	0.025	1.96
97%	0.015	2.17
99%	0.005	2.58

Fórmula empleada

$$n = \frac{n_o}{1 + \frac{n_o}{N}} \quad \text{donde:} \quad n_o = p^*(1-p)^* \left[\frac{z (1-\frac{\alpha}{2})}{d} \right]^2$$

Matriz de Tamaños muestrales para un universo de 135 con una p de 0.5										
Nivel de Confianza	d [error máximo de estimación]									
	10.0%	9.0%	8.0%	7.0%	6.0%	5.0%	4.0%	3.0%	2.0%	1.0%
90%	45	51	59	68	78	90	102	114	125	132
95%	56	63	71	80	90	100	110	120	128	133
97%	63	70	78	86	96	105	114	122	129	133
99%	75	81	89	97	104	112	119	126	131	134

Fuente: Elaboración Propia (2017).

3.2.3. Métodos de investigación

Lifecycle Services de Cisco (servicios del ciclo de vida de la red)
 Hemos elegido esta metodología:

- Porque Lifecycle Services son metodologías y prácticas que soportan la evolución de la red y ayuda a las empresas a incrementar el retorno de inversión en estas tecnologías.
- Mejora la disponibilidad, estabilidad, seguridad y escalabilidad de la red a través del sistema de planeación, diseño, mantenimiento y optimización.
- Define el conjunto mínimo de actividades necesarias, según la tecnología y la complejidad de la red, así como para optimizar el rendimiento de las mismas durante el Ciclo Vital de la red.
- Este enfoque, y la venta de Servicios (TSS – Technical Support Services) te puede ayudar a desplegar una red de alto rendimiento y un plan de apoyo de red, integrar tecnologías avanzadas, reducir el coste total de mantenimiento de red (TCO) y mantener una red en buen estado mediante rutinas diarias, asegurando el acceso a los recursos técnicos adecuados.



- Acelerar el acceso a aplicaciones y servicios ayuda a obtener agilidad empresarial.
- Ayuda a proteger, optimizar y hace crecer las plataformas de Red utilizando un planteamiento de ciclo de vida, el cual crea valor de negocios y excelencia operacional.

Según Cisco Systems (2006), el enfoque de Lifecycle Services de Cisco define el conjunto mínimo de actividades necesarias, por tecnología y por nivel de complejidad de la red, para ayudar a los clientes a instalar y operar exitosamente tecnologías de Cisco, y optimizar su desempeño.

3.2.4. Beneficios de Lifecycle Services

- Incrementa el valor de la red en la gestión de negocios y el retorno de inversión y coloca al cliente en una posición ventajosa al disminuir el costo total de propiedad de la red, mejorando ambos: la agilidad del negocio y la disponibilidad de la red.
- Acelera la estrategia.
- de penetración del mercado (go-to-market) al entregar soluciones a tiempo, dentro del presupuesto, y a un precio competitivo a través de una metodología comprobada y consistente que enfatiza la coordinación entre Cisco, sus socios de negocios y las capacidades de los clientes.
- Mejora la disponibilidad, estabilidad, seguridad y escalabilidad de la red a través del sistema de planeación, diseño, mantenimiento y optimización.
- Maneja la complejidad creciente de la red al proveer consistencia en los procesos para instalar y mantener la tecnología de Cisco Systems.

Fases de Lifecycle Services

1. Fase de Preparación

Se establece los requerimientos del negocio y la visión tecnológica correspondiente.

También desarrolla la estrategia técnica e identifica las tecnologías que mejor pueden soportar los planes de crecimiento. Esta fase inicial es clave para la fase de Planeación.

2. Fase de Planeación

En la fase de planeación del ciclo de vida de la red, una empresa evalúa su red para determinar si la infraestructura de sistema existente, las localidades y el ambiente operativo pueden soportar el sistema propuesto.

La organización trata de asegurar la disponibilidad de los recursos adecuados para administrar el proyecto de despliegue de tecnología, desde la planeación hasta el diseño e implementación.

Para planear la seguridad de la red, la empresa evalúa su sistema, redes e información contra intrusos, así como también evalúa la red para detectar la factibilidad de que redes externas y no confiables obtengan acceso a redes y sistemas internos y confiables.

Se crea un plan de proyecto para ayudar a administrar las tareas, riesgos, problemas, responsabilidades, hitos críticos y recursos requeridos para implementar cambios en la red.

El plan de proyecto se alinea con el campo de acción, el costo y los parámetros de recursos establecidos en los requerimientos de negocio originales.



3. Fase de Diseño

Durante la fase de diseño del ciclo de vida de la red, una empresa desarrolla un plan detallado completo que cumple con los requerimientos técnicos y de negocios actuales e incorpora especificaciones para soportar la disponibilidad, confiabilidad, seguridad, escalabilidad y desempeño. Adicionalmente, la empresa desarrolla un diseño específico amplio para las operaciones del sistema tecnológico y los procesos y herramientas de administración de la red.

Donde sea relevante, se crean aplicaciones hechas a la medida para que la tecnología pueda cumplir con los requerimientos de la organización y le permita la integración con la infraestructura de red existente.

Durante la fase de diseño se desarrollan una variedad de planes para guiar actividades tales como configuración y prueba de conectividad, despliegue y comisionar el sistema propuesto, migración de servicios de la red, demostración de funcionalidad de la red y validación de la operación de la red.

4. Fase de Implementación

En la fase de implementación, la empresa trabaja para integrar dispositivos sin interrumpir a la red existente o crear puntos de vulnerabilidad.

La empresa puede montar y probar el sistema propuesto antes de desplegarlo. Después de identificar y resolver cualquier problema de implementación del sistema, la empresa instala, configura e integra los componentes del sistema e instala, configura, prueba y comisiona el sistema de operaciones y administración de la red.

Una vez que se han migrado los servicios de red, la empresa valida que su red operativa esté funcionando como se había planeado, valida las operaciones del sistema y trabaja para cerrar las brechas en las habilidades del personal.

5. Fase de Operación

Las operaciones de la red representan una gran parte del presupuesto de TI de una empresa. Una organización gasta tiempo considerable en esta fase, viviendo con la tecnología dentro del ambiente de la empresa. A través de la fase de operación, la empresa mantiene la salud continua del sistema, monitoreando y administrándola proactivamente para maximizar su desempeño, capacidad, disponibilidad, confiabilidad y seguridad.

La empresa administra y resuelve problemas o cambios que afecten al sistema, reemplazando o reparando hardware conforme sea necesario.

Realiza movimientos físicos y lógicos, añade y cambia y mantiene actualizados el software y aplicaciones del sistema y administra a los proveedores de hardware y software para ayudar a asegurar la entrega eficiente de productos o servicios.

6. Fase de Optimización

El objetivo máximo de la fase de optimización es alcanzar la excelencia operativa a través de esfuerzos continuos para mejorar el desempeño y funcionalidad del sistema.

Una empresa trata de asegurar que su sistema operacional está cumpliendo con los objetivos y requerimientos establecidos en el caso de negocio de la empresa y trabaja para mejorar el desempeño y seguridad del sistema.

Las prácticas de administración se mejoran al perfeccionar la habilidad de despliegue de la red y las eficiencias operativas a través de un sistema de administración de la red que automatiza, integra y simplifica los procesos y herramientas de administración.

Los requerimientos del negocio se actualizan y contrastan regularmente con la estrategia de tecnología, desempeño y operaciones de la red. La red debe ser adaptable y debe estar preparada para lidiar con requerimientos nuevos o cambiantes.

Conforme se modifica para soportar nuevos requerimientos empresariales o para mejorar el desempeño, la red reingresa a la fase de preparación de su ciclo de vida.

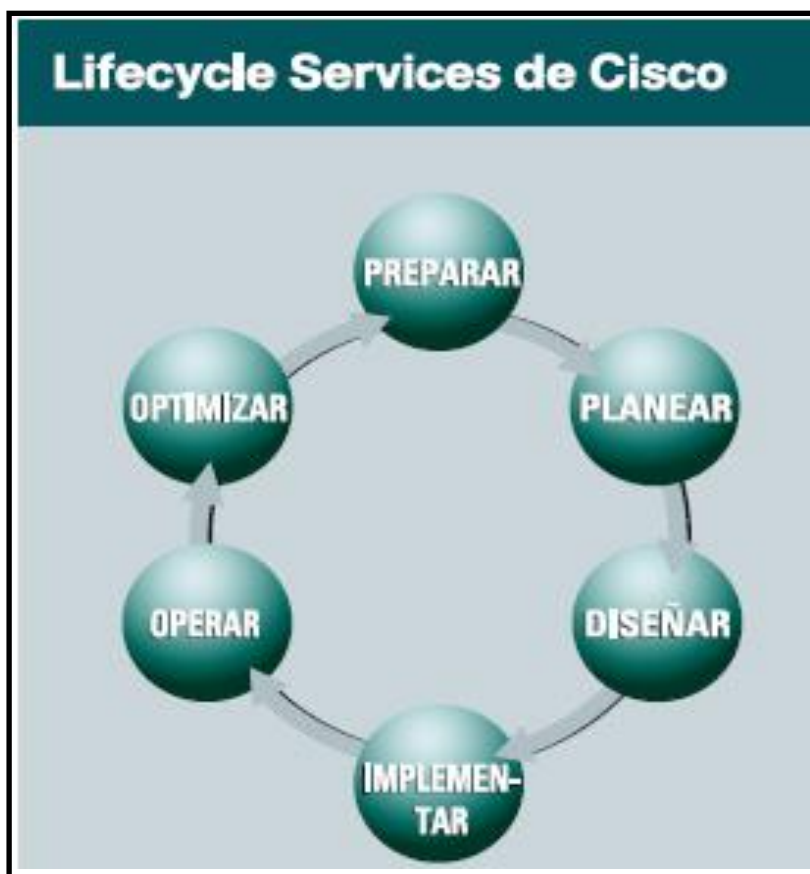


Figura 18. Fases de la Metodología Lifecycle Services de Cisco. Fuente: Cisco System (2006).



3.3. Hipótesis.

El Desarrollo de la propuesta de virtualización de dispositivos de conmutación permitirá mejorar el performance de la Red LAN, a través de la convergencia de redes, calidad de servicio, seguridad, escalabilidad y alta disponibilidad, como respuesta a la problemática existente de la Red LAN en el HNERM–EsSALUD.

3.3.1. Variables.

3.3.1.1. Variable Independiente

Desarrollar la propuesta de Virtualización de Dispositivos de Conmutación.

3.3.1.2. Variable Dependiente

Optimizará los servicios de la Red LAN en el Hospital Nacional Edgardo Rebagliati Martins–EsSALUD se obtendrá una mejor performance para facilitar la gestión.

3.3.1.3. Variable Interviniente

Metodología LifeCycle Services de Cisco.

3.4. Operacionalización.

En el presente trabajo de investigación se diseñará el esquema de las dos variables independiente dependiente que a continuación detallamos:

Tabla 4
Variable Independiente

Variable Independiente	Dimensiones	Indicadores	Técnicas e instrumentos de recolección de datos
<p>Desarrollar la propuesta de Virtualización de Dispositivos de Conmutación.</p>	<p>Convergencia de redes.</p> <p>Eficiencia energética.</p> <p>Optimización de recursos en data center</p>	<p>a. Número de contextos virtuales a implementar.</p> <p>b. Número de CORE virtuales interconectados.</p> <p>c. Consumo de energía en equipos de conmutación y servidores.</p> <p>d. consumo de energía en equipos de aire acondicionado.</p> <p>e. Número de equipos servidores a virtualizar.</p> <p>f. Número de Conmutadores a virtualizar.</p>	<p>a. Ficha de Evaluación</p> <p>b. Observación.</p> <p>c. Observación</p> <p>d. Test</p> <p>e. Observación</p> <p>f. Observación</p>

Fuente: Elaboración Propia (2017).



Tabla 5
Variable Dependiente

Variable Dependiente	Dimensiones	Indicadores	Ítems o Respuestas	Técnicas e instrumentos De recolección de datos	
<p>Optimizará los servicios de la Red LAN en el Hospital Nacional Edgardo Rebagliati Martins–EsSALUD se obtendrá una mejor performance para facilitar la gestión.</p>	<p>1. Calidad de Servicio</p>	1.1. Número de reportes de análisis de calidad de servicio por sub redes.	¿Las subredes existentes se aplica calidad de servicio?	a. Ficha de Evaluación	
		1.2. Tiempo de transferencia de datos.	¿La transferencia de datos cumple la demanda de los servicios?	b. Observación	
		1.3. Número de Redes virtuales existentes.	¿Se encuentra segmentada la red?	c. Observación.	
	<p>2. Escalabilidad de la red</p>	2.1. Porcentaje de escalamiento Horizontal y Vertical de la red al año.	¿Él verá el porcentaje de escalamiento horizontal y vertical?	d. Ficha de Evaluación	
		<p>3. Seguridad en la Red</p>	3.1. Número de Listas de Control de Acceso – ACL, por sub redes.	¿Cada sub red contará con listas de control de acceso necesarias?	e. Observación
	3.2. Número de métodos de autenticación configurados.		¿Estarán configurados los métodos de autenticación en todos los equipos?	f. Observación	
	<p>4. Disponibilidad de la Red.</p>		4.1. Porcentajes de disponibilidad y tiempo de inactividad de la red mes y año.	¿El servicio de red se encuentra disponible?	g. Encuesta
			4.2. Número de enlaces redundantes existentes.	¿Se cuenta con número de enlaces establecidos?	h. Observación

Fuente: Elaboración Propia (2017).



3.5. Métodos, Técnicas e instrumentos de recolección de datos.

Se tendrá como propósito obtener los datos (información) de la OSI-HNERM, válidos y confiables, para el uso de las técnicas como: Test, Ficha de evaluación, encuesta y observación para validar las variables independiente y dependiente, que a continuación se detalla de la siguiente manera:

3.5.1. El Test

Se usó esta técnica de Test porque hace referencia a las pruebas destinadas a evaluar las funciones relacionadas con la:

- a. Eficiencia Energética (OSI-HNERM)

3.5.2. Ficha de Evaluación

Se usarán las fichas de evaluación para monitorear y evaluar las variables en estudio, con el objetivo de contribuir a los sistemas relacionadas con:

- a. Calidad del Servicio (OSI-HNERM)
- b. Convergencia de Redes (OSI-HNERM)
- c. Escalabilidad de la Red (OSI-HNERM)
- d. Seguridad en la Red (OSI-HNERM)

3.5.3. Encuesta

Se realizó mediante encuestas aplicadas a usuarios asistenciales y administrativos del HNERM, con preguntas fáciles y rápidas de contestar, a la vez cortas y concisas para así; hacer que los encuestados den sus respuestas sin la necesidad de buscar muchos argumentos estos se relacionaron con:

- a. Disponibilidad de la Red. (OSI-HNERM)



3.5.4. Observación

Se usó la técnica de la Observación porque nos permite recoger información que consiste básicamente, en observar, acumular e interpretar las actuaciones, comportamientos y hechos de los servicios de la Red LAN del HNERM, tal y como las realizan habitualmente, relacionada con:

- | | |
|--------------------------------------|--------------|
| b. Convergencia de Redes | (OSI-HNERM) |
| c. Eficiencia Energética | (OSI-HNERM) |
| d. Optimización Recursos Data Center | (OSI-HNERM) |
| e. Calidad de Servicio | (OSI-HNERM). |

3.6. Procedimiento recolección de datos.

Se coordinó directamente con los jefes de cada área del HNERM para que brinden las facilidades en los tres turnos Mañana, Tarde y Noche ya que el hospital se trabaja 24x7x365.

A continuación, explicaremos los procedimientos que hemos considerado en la intervención de los métodos y/o técnicas de investigación utilizadas como: las técnicas de Test, Ficha de evaluación, encuesta y observación.

3.6.1. Procedimiento de la Técnica de Recolección de Datos

- a. Se utilizó el Dispositivo Autoanalizador OptiView - Fluke Networks para verificar el funcionamiento de Red LAN del HNERM.
- b. Se realizó los seguimientos diarios mostrando los reportes correspondientes del performance de Red LAN.
- c. Se realizó 10 preguntas al usuario sobre la Eficiencia Energética.
- d. Se realizó los reportes sobre la Eficiencia Energética.
- e. Se realizó reportes diarios sobre las caídas de la Red LAN.
- f. Se realizó los reportes de los Gabinetes que han reportado mayores inconvenientes con problemas de hardware.



3.6.2. Procedimiento de la Ficha de evaluación:

- a. Se han registrado los datos correspondientes la Red LAN.
- b. Se ha registrado en las áreas asistenciales y administrativas los datos pertinentes sobre los números de contextos virtuales a implementar de la Convergencia de Redes.
- c. Se ha registrado en las áreas asistenciales y administrativas los datos pertinentes sobre los Porcentajes de la Escabilidad de la Red.
- d. Se ha registrado en la OSI-HNERM los datos pertinentes sobre las listas de control de Acceso ACL sobre la Seguridad en la Red.
- e. Se realizó las observaciones correspondientes para saber el Número de Redes virtuales existentes para la implementación de la Calidad del Servicio.

3.6.3. Procedimiento de la Encuesta:

- a. Se han realizado las encuestas a los usuarios asistenciales y administrativas sobre el performance de la Red.
- b. Se han realizado las encuestas a los usuarios asistenciales y administrativas sobre las posibles caídas en el día de la Red LAN en el HNERM-EsSALUD.
- c. Se han realizado las encuestas en la OSI-HNERM sobre el servicio de la Red si se encuentran los números de enlaces suficientes para coberturar todos los servicios.

3.6.4. Procedimiento de la Observación:

- a. Se han realizado las observaciones en las áreas correspondientes sobre la Convergencia de Redes.

- b. Se ha registrado en la OSI-HNERM datos pertinentes sobre los números de contextos virtuales a implementar de la Convergencia de Redes.
- c. Se ha registrado en la OSI-HNERM los datos pertinentes sobre los números de Core virtuales interconectadas de la Convergencia de Redes.
- d. Se realizó las observaciones correspondientes sobre la Eficiencia Energética.
- e. Se realizó las observaciones correspondientes sobre el funcionamiento de conmutadores de la Red LAN.
- f. Se realizó las observaciones correspondientes sobre el número de equipos de servidores a virtualizar para la Optimización de Recursos en Data Center.
- g. Se realizó las observaciones correspondientes para saber el Tiempo de transferencia de datos para la Calidad del Servicio.

3.7. Análisis estadístico e interpretación de datos.

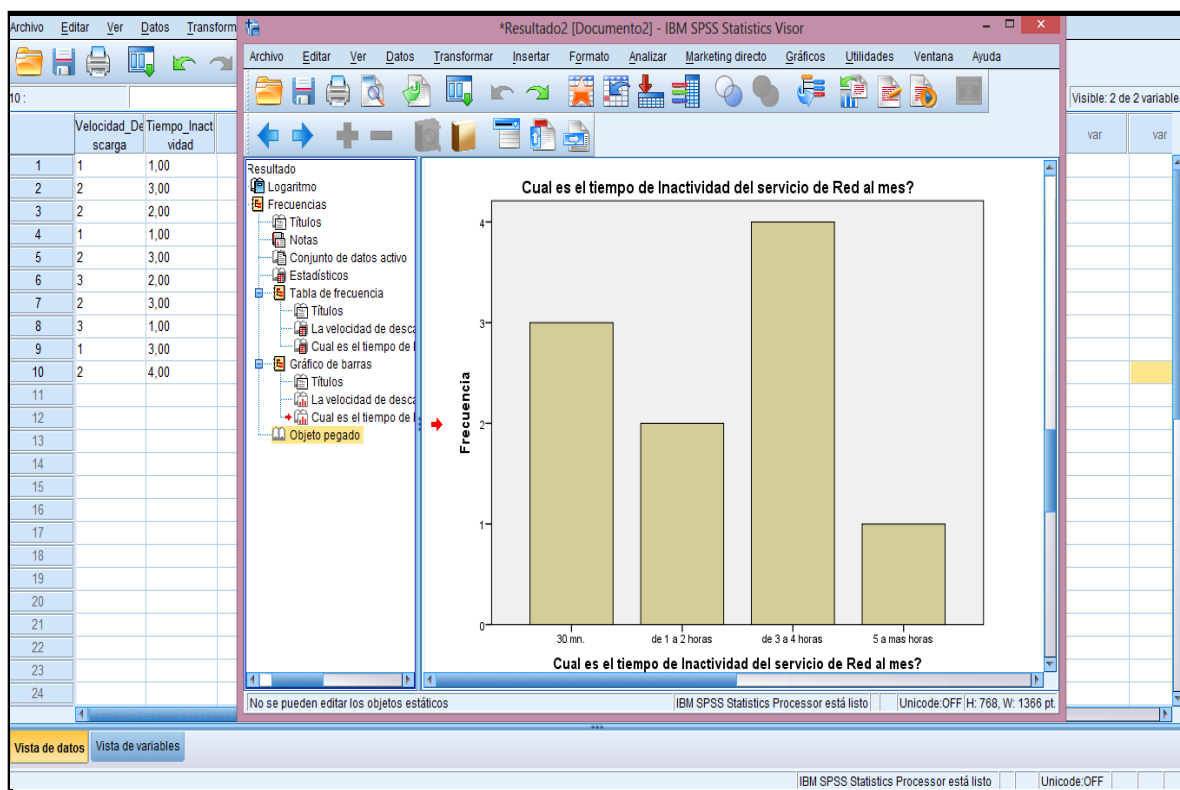
En el presente trabajo de investigación se aplicará las siguientes fórmulas para poder obtener los resultados estadísticos requeridos:

- a. **Media:** Es la suma de todos los valores dividido por su número, se calcula de la siguiente manera:

$$X = \frac{\sum X}{n}$$



Tabla 6
Tiempo de Inactividad del Core Principal del HNERM EsSALUD



Fuente: Elaboración Propia SPSS (2017).

Nota: Se obtendrá los datos estadísticos sobre el tiempo de Inactividad del dispositivo conmutador del Core Principal de la Red LAN en el HNERM-EsSALUD aplicando la media.

También se considerará las presentes formulas en caso que la población de estudio sea pequeña o muy numerosa lo detallamos de la siguiente manera:

- b. **Media Aritmética:** En aquellas situaciones en que la población de estudio es pequeña suele utilizarse la media poblacional mediante la expresión:

$$\mu = \frac{\sum_{i=1}^N Xi}{N}$$



En cambio, si la población de estudio es muy numerosa se procede a obtener la media muestral definida matemáticamente por la expresión:

$$X = \frac{\sum_{i=1}^N \bar{X}_i}{N}$$

3.8. Criterios éticos.

En el presente trabajo de investigación es de vital importancia y relevancia para el Tesista considerar los criterios éticos siguientes:

a. Ambiente

En el presente trabajo de Investigación a realizar no afectará el medio ambiente del HNERM-EsSALUD porque se tomarán en cuenta las medidas y normas correspondientes.

b. Confidencialidad

La Jefatura de la OSI-HNERM se asegurará de la protección de la identidad de la institución y de las personas que estamos participando como informantes en la presente investigación.

c. Objetividad

Cada información obtenida de la OSI-HNERM en el presente trabajo de investigación se basará en criterios técnicos e imparciales.

d. Originalidad

En el presente trabajo de investigación citaremos las fuentes bibliográficas de la información mostrada, a fin de demostrar la inexistencia de plagio intelectual.



e. Veracidad

Cabe mencionar que toda la información del presente trabajo de investigación mostrada y obtenida de la OSI-HNERM es verdadera, cuidando la confidencialidad de ésta.

f. Derechos Laborales

En el presente trabajo propuesto de solución, propiciara el respeto a los derechos laborales en la entidad de estudio.

3.9. Criterios de Rigor Científico

En el presente trabajo de investigación es de vital importancia y relevancia para el Tesista considerar los criterios de rigor científico siguientes:

a. Confiabilidad

En el presente trabajo de investigación planteado, se realizan cálculos estadísticos para la determinación del nivel de consistencia interna de los instrumentos de recolección de datos de la OSI-HNERM.

b. Validación

En el presente trabajo de Investigación, se validarán los instrumentos de recolección de datos recogidos y propuesta de solución a través de juicio de expertos.

c. Trabajo Metódico

Se usarán los métodos estructurados y rigurosos para el desarrollo de la investigación: recolección de información bibliográfica, trabajo de campo, análisis de datos, proyecciones, etc.



CAPÍTULO IV: ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

4.1. Resultados en tablas y Gráficos

Asimismo, se presentará las mediciones de los indicadores de la Variable Independiente en tablas y gráficos:

a. Números de Contextos Virtuales a implementar.

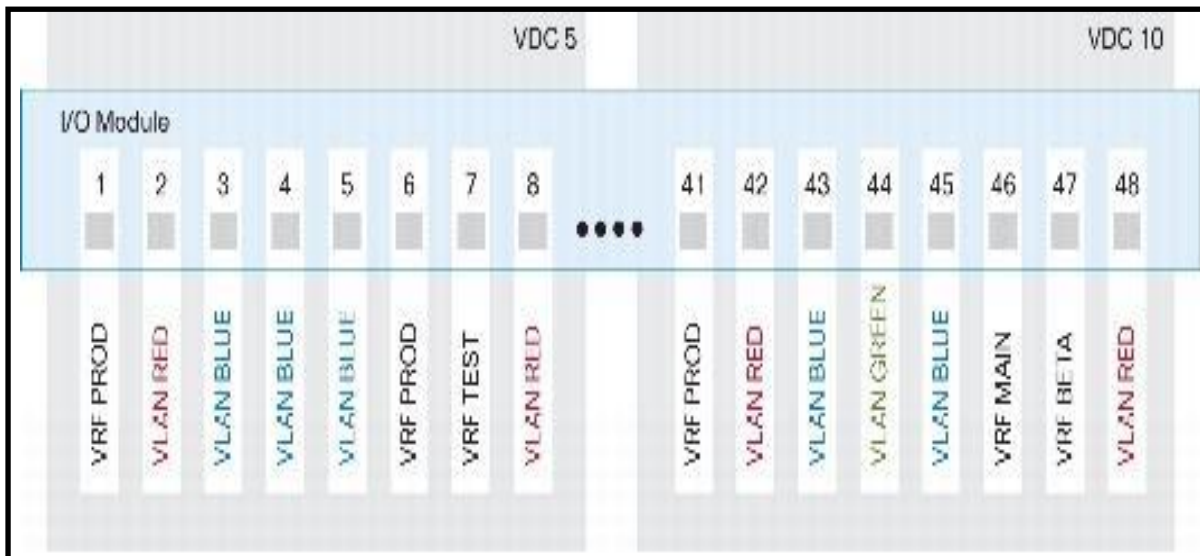


Figura 19. Números de Contextos Virtuales a implementar. Fuente: Cisco (2017).

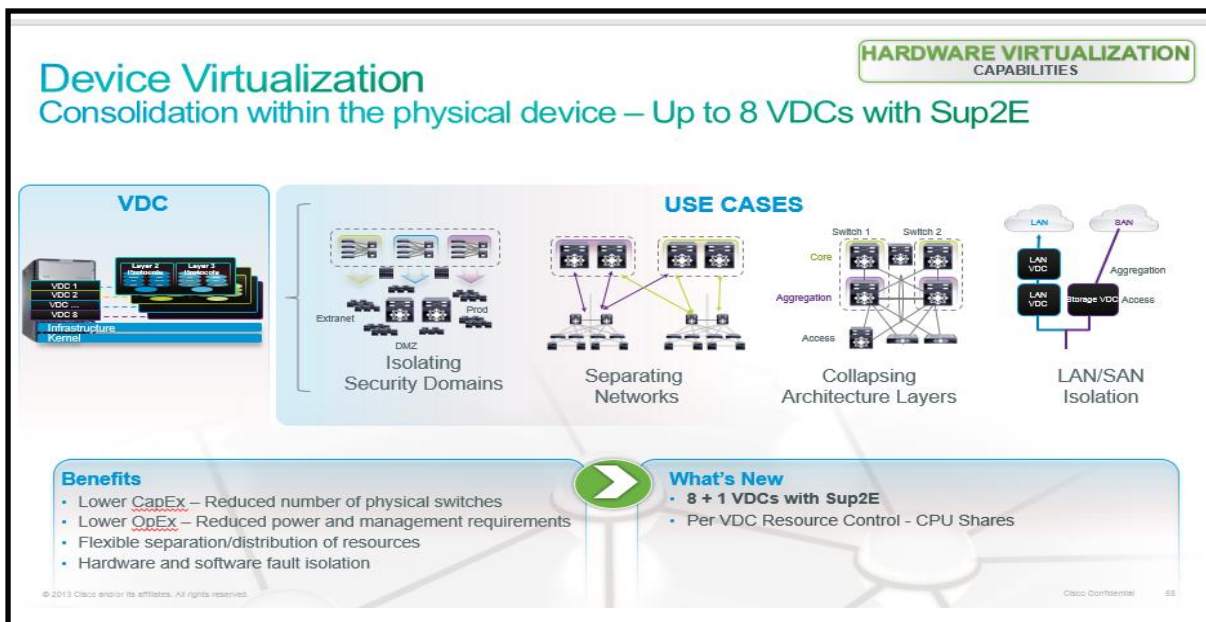


Figura 20. Device Virtualization. Fuente: Cisco (2017).

Nota: Se muestra el número contextos virtuales a implementar son (08).



b. Número de Core Virtual Interconectadas.



Figura 21. Conmutador Cisco Nexus 7000 Switch. Fuente: Cisco (2017).

Nota: Se muestra el número de Core a Virtualizar son (02).

c. Consumo de Energía en Equipos de Conmutación y Servidores.

La medición de consumo de energía será al equipo conmutador de Nexus 7000 serán (02).

1. La serie Cisco Nexus 7000 utiliza fuentes de alimentación que son eficientes hasta un 90 por ciento, por lo que se pierde menos energía como calor y se dispone de más energía para el sistema que con fuentes de alimentación típicas.
2. Los módulos del ventilador en el chasis se ajustan para compensar las características térmicas cambiantes.
3. A velocidades más bajas, utilizan menos energía. En el chasis de 9 ranuras, la bandeja del ventilador está diseñada para apagar completamente la alimentación de una fila de ventiladores cuando las ranuras correspondientes no se usan.

4. La consolidación de los conmutadores múltiples en la serie Cisco Nexus 7000 está habilitada por la combinación potente de alta densidad y rendimiento, compatibilidad con la virtualización de dispositivos y características completas de confiabilidad y disponibilidad.

5. Esta consolidación aumenta la eficiencia de la energía al reducir la energía desperdiciada de múltiples sistemas parcialmente cargados e inflexibles.

Product Specifications				
Item	Specification			
	Cisco Nexus 7000 4-Slot Switch	Cisco Nexus 7000 9-Slot Switch	Cisco Nexus 7000 10-Slot Switch	Cisco Nexus 7000 18-Slot Switch
Physical specifications	<ul style="list-style-type: none"> Usable rack space: 7RU 4-slot chassis: 2 dedicated supervisor modules and 2 I/O modules 4 power supply slots Dimensions (H x W x D): 12.2 x 17.3 x 24 in. (30.9 x 43.9 x 61 cm) Chassis depth including cable management and chassis doors is 29.6 in. (75.2 cm) Unit is rack mountable in a standard 19-inch (482.6-mm) Electronic Industries Alliance (EIA) rack Weight <ul style="list-style-type: none"> Chassis only: 45 lb. (20 kg) Fan Tray: 25 lb (11.3 kg) Supports 3-kW AC and DC and 3.5-kW HV AC/DC power supplies Supports up to 6 chassis stacked in a 42RU rack 	<ul style="list-style-type: none"> Usable rack space: 14RU 9-slot chassis: 2 dedicated supervisor modules and 7 I/O modules 5 fabric module slots 2 power supply slots Dimensions (H x W x D): 24.5 x 17.3 x 24 in. (62.2 x 43.9 x 61 cm) Chassis depth including cable management and chassis doors is 29 in. (73.7 cm) Unit is rack mountable in a standard 19-inch (482.6-mm) EIA rack Weight <ul style="list-style-type: none"> Chassis only: 100 lb. (45 kg) Fabric Module: 5 lb (2.3 kg) Fan Tray: 25 lb (11.3 kg) Supports 6-kW and 7.5-kW AC and DC power supplies Supports up to 3 chassis stacked in a 42RU rack 	<ul style="list-style-type: none"> Usable rack space: 21RU 10-slot chassis: 2 dedicated supervisor modules and 8 I/O modules 5 fabric module slots 3 power supply slots Dimensions (H x W x D): 36.5 x 17.3 x 33.1 in. (92.7 x 43.9 x 84.1 cm) Chassis depth including cable management and chassis doors is 38 in. (96.5 cm) Unit is rack mountable in a standard 19-inch (482.6-mm) EIA rack Weight <ul style="list-style-type: none"> Chassis only: 200 lb. (90 kg) Fabric Module: 4 lb (1.8 kg) System Fan Tray: 20 lb (9.1 kg) Fabric Fan Tray: 5 lb (2.3 kg) Supports 6-kW and 7.5-kW AC and DC power supplies 	<ul style="list-style-type: none"> Usable rack space: 25RU 18-slot chassis: 2 dedicated supervisor modules and 16 I/O modules 5 fabric module slots 4 power supply slots Dimensions (H x W x D): 43.5 x 17.3 x 33.1 in. (110.5 x 43.9 x 84.1 cm) Chassis depth including cable management and chassis doors is 38 in. (96.5 cm) Unit is rack mountable in a standard 19-inch (482.6-mm) EIA rack Weight <ul style="list-style-type: none"> Chassis only: 187 lb. (85 kg) Fabric Module: 7.5 lb (3.4 kg) Fan Tray: 25.8 lb (11.7 kg) Supports 6-kW and 7.5-kW AC and DC power supplies
Environmental specifications	<ul style="list-style-type: none"> Airflow direction: Side to rear Operating temperature: 32 to 104°F (0 to 40°C) Operational relative humidity: 5 to 90%, noncondensing Operating altitude: -500 to 13,123 ft. (agency certified 0 to 6500 ft.) Seismic: Zone 4 per GR63 Floor loading: 42 lb. per sq. ft. Operational vibration GR63, Section 5.4.2 ETS 300 019-1-3, Class 3.1, Section 5.5 Storage altitude: -1000 to 30,000 ft. Storage temperature: -40 to 158°F (-40 to 70°C) Storage relative humidity: 5 to 95%, noncondensing Heat dissipation: Maximum 3500W per chassis (actual dissipation will be lower, depending on the chassis configuration) 	<ul style="list-style-type: none"> Airflow direction: Side to side Operating temperature: 32 to 104°F (0 to 40°C) Operational relative humidity: 5 to 90%, noncondensing Operating altitude: -500 to 13,123 ft. (agency certified 0 to 6500 ft.) Seismic: Zone 4 per GR63 Floor loading: 104 lb. per sq. ft. Operational vibration GR63, Section 5.4.2 ETS 300 019-1-3, Class 3.1, Section 5.5 Storage altitude: -1000 to 30,000 ft. Storage temperature: -40 to 158°F (-40 to 70°C) Storage relative humidity: 5 to 95%, noncondensing Heat dissipation: Maximum 7500W per chassis (actual dissipation will be lower, depending on the chassis configuration) 	<ul style="list-style-type: none"> Airflow direction: Bottom front of chassis to top back Operating temperature: 32 to 104°F (0 to 40°C) Operational relative humidity: 5 to 90%, noncondensing Operating altitude: -500 to 13,123 ft. (agency certified 0 to 6500 ft.) Seismic: Zone 4 per GR63 Floor loading: 190 lb. per sq. ft. Operational vibration GR63, Section 5.4.2 ETS 300 019-1-3, Class 3.1, Section 5.5 Storage altitude: 1000 to 30,000 ft. Storage temperature: -40 to 158°F (-40 to 70°C) Storage relative humidity: 5 to 95%, noncondensing Heat dissipation: Maximum 12,000W per chassis (actual dissipation will be lower, depending on the chassis configuration) 	<ul style="list-style-type: none"> Airflow direction: Side to side Operating temperature: 32 to 104°F (0 to 40°C) Operational relative humidity: 5 to 90%, noncondensing Operating altitude: -500 to 13,123 ft. (agency certified 0 to 6500 ft.) Seismic: Zone 4 per GR63 Floor loading: 190 lb. per sq. ft. Operational vibration GR63, Section 5.4.2 ETS 300 019-1-3, Class 3.1, Section 5.5 Storage altitude: 1000 to 30,000 ft. Storage temperature: -40 to 158°F (-40 to 70°C) Storage relative humidity: 5 to 95%, noncondensing Heat dissipation: Maximum 18,000W per chassis (actual dissipation will be lower, depending on the chassis configuration)

Figura 22. Products Specifications. Fuente: Cisco (2017).

Nota: Se muestra el consumo de energía será a los servidores estos son (32).



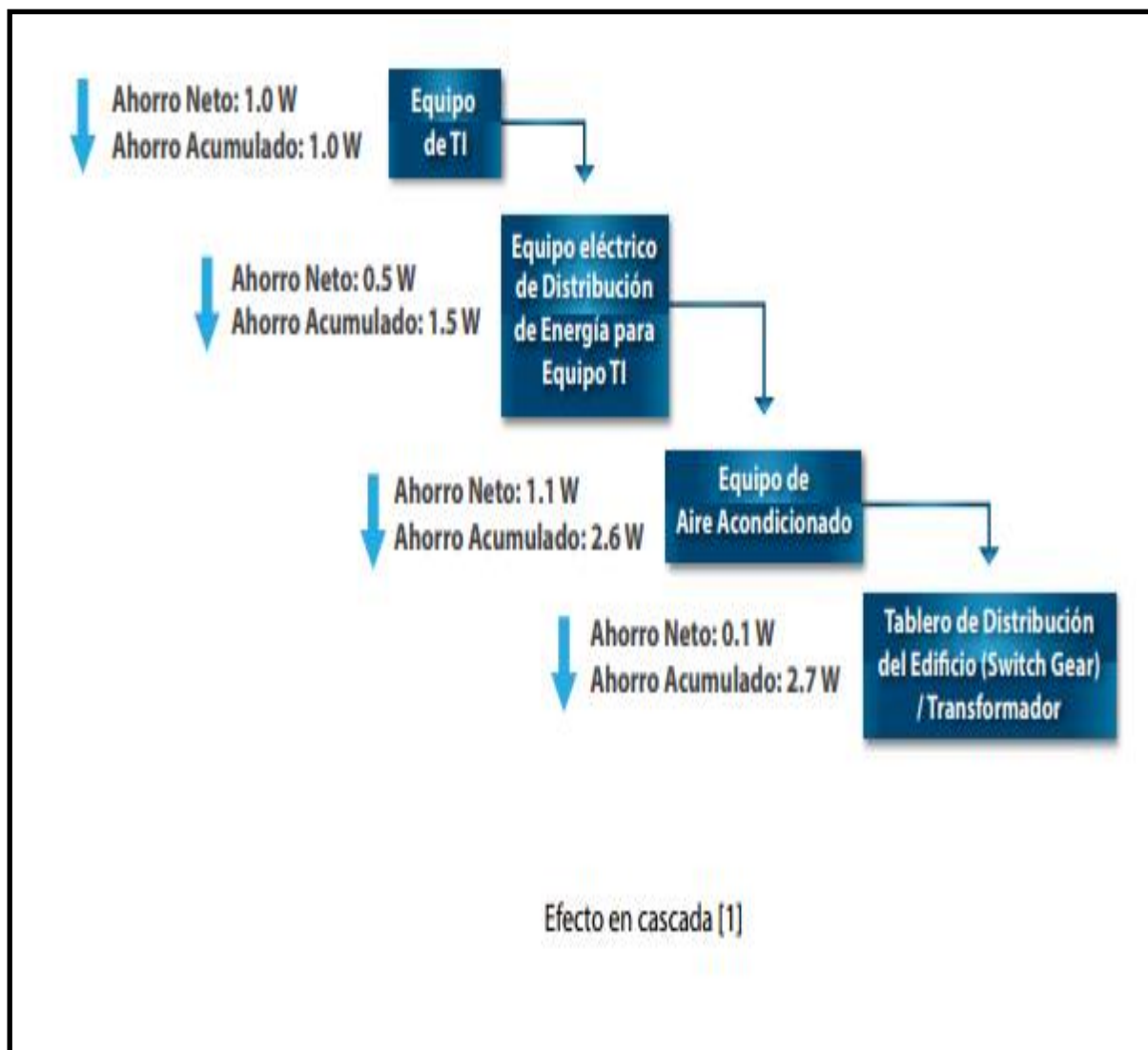


Figura 23. Soluciones Integrales para Centros de Datos. Fuente: Grupo Electrotécnica (2016).

Nota: Si los equipos de TI consumen menos, se puede generar un efecto en cascada [1] de ahorro energético, a través de las primeras 2 trayectorias.

Esto porque cuando se disminuye el consumo de los equipos de TI, estos y los de potencia generan menos calor, entonces los equipos de enfriamiento consumen menos energía, y así los equipos de potencia generan aún menos calor.

Consumo de Energía:

En la figura se muestra un ejemplo del efecto en cascada, y cómo si se reduce 1 watt de consumo en los equipos de TI, se puede obtener un ahorro total de 2,7 watts de consumo en el data center.

d. Consumo de Energía en Equipos de Aire Acondicionado.

CyberAir 3 (20 a 82 kW): Sistema independiente de aire acondicionado de precisión para aplicaciones de altas prestaciones.



Figura 24. Sistema independiente de aire acondicionado de precisión para aplicaciones de altas prestaciones.

Fuente: Empresa Editel (2016).

Nota: Se muestra el Consumo de Energía del Aire Acondicionado de Precisión es: (20 a 82 kW) y solo se aplica a (01).

- El sistema de circuito cerrado de aire CyberAir 3 de STULZ controla las condiciones del centro de datos con máxima precisión y fiabilidad, así como un uso eficiente de la energía eléctrica.
- Diseñado para el funcionamiento fiable continuo durante largos años, el CyberAir 3 de STLZ es extremadamente preciso, silencioso y excepcionalmente económico.
- Mantiene su equipo IT disponible en todo momento.



e. Número de Equipos servidores a Virtualizar.

El Número de servidores a Virtualizar son (32).

f. Número de Conmutadores a Virtualizar.

Tabla 7

Cuadro de Conmutadores a Virtualizar

EQUIPO DE COMUNICACIONES	CANTIDAD	DESCRIPCIÓN
SWITCH TIPO I	2	Switch de Core Principal
SWITCH TIPO II	1	Switch de Distribución para el Centro de Datos con puertos en fibra
SWITCH TIPO III	1	Switch de Distribución para el Centro de Datos con puertos en cobre
SWITCH TIPO IV	70	Switch de acceso de para servicios de voz, data, impresiones y Wireless corporativo
SWITCH TIPO V	36	Switch de acceso para servicios de video vigilancia. Soporte de POE+
SWITCH TIPO VI	13	Switch de acceso para comunicación con equipos médicos
SWITCH TIPO VII	28	Switch de acceso para comunicación con equipos médicos

Nota: Se muestra los Números Conmutadores a Virtualizar son (135).

Asimismo, se presentará las mediciones de los indicadores de la Variable Dependiente en tablas y gráficos.



1.1. Número de reportes de Análisis de calidad de servicios por Subredes.

Datos_Gab	0.0.0.0	0.0.0.0	DOWN	NO unbound
Datos_Gab_A	10.1.6.1	255.255.254.0	UP	YES vlan 100
Datos_Gab_A1	0.0.0.0	0.0.0.0	DOWN	NO unbound
Datos_Gab_B1	10.1.43.1	255.255.255.0	UP	YES vlan 200
Datos_Gab_B3	10.1.14.1	255.255.254.0	UP	YES vlan 120
Datos_Gab_C	10.1.10.1	255.255.254.0	UP	YES vlan 110
Datos_Gab_C1	10.1.22.1	255.255.254.0	UP	YES vlan 140
Datos_Gab_D	10.1.47.1	255.255.255.0	UP	YES vlan 220
Datos_Gab_F	10.1.37.1	255.255.255.0	UP	YES vlan 180
Datos_Gab_G3	10.1.49.1	255.255.255.0	UP	YES vlan 230
Datos_Gab_I2	10.1.30.1	255.255.254.0	UP	YES vlan 160
Datos_Gab_J	10.1.51.1	255.255.255.0	UP	YES vlan 240
Datos_Gab_K	10.1.53.1	255.255.255.0	UP	YES vlan 250
Datos_Gab_L	10.1.55.1	255.255.255.0	UP	YES vlan 260
Datos_Gab_M	10.1.40.1	255.255.255.0	UP	YES vlan 190
Datos_Gab_N	10.1.57.1	255.255.255.0	UP	YES vlan 270
EMP	192.168.1.1	255.255.255.0	DOWN	NO EMP
Enlace-Sede-Central	192.168.20.40	255.255.255.0	UP	YES vlan 10
Imagenes_Packs	10.1.3.1	255.255.255.0	UP	YES vlan 510
Impresora_Gab_L	10.1.56.129	255.255.255.224	UP	YES vlan 262
Impresoras_Gab_A1	10.1.21.1	255.255.255.192	UP	YES vlan 132
Impresoras_Gab_B1	10.1.44.129	255.255.255.224	UP	YES vlan 202
Impresoras_Gab_B3	10.1.17.1	255.255.255.192	UP	YES vlan 122
Impresoras_Gab_C	10.1.13.1	255.255.255.192	UP	YES vlan 112
Impresoras_Gab_F	10.1.39.1	255.255.255.192	UP	YES vlan 182
Impresoras_Gab_I1	0.0.0.0	0.0.0.0	DOWN	NO unbound
Impresoras_Gab_I2	10.1.33.1	255.255.255.192	UP	YES vlan 162
Impresoras_Gab_J	10.1.52.129	255.255.255.224	UP	YES vlan 242
Impresoras_Gab_K	10.1.54.129	255.255.255.224	UP	YES vlan 252
Impresoras_Gab_M	10.1.42.1	255.255.255.192	UP	YES vlan 192
Impresoras_Gab_N	10.1.58.129	255.255.255.224	UP	YES vlan 272
Loopback	127.0.0.1	255.0.0.0	UP	NO Loopback
Marcadores_biome	10.1.5.1	255.255.255.192	UP	YES vlan 530
Server	10.1.0.1	255.255.255.128	UP	YES vlan 540
Voz-0	172.29.120.4	255.255.255.0	UP	YES vlan 450
Voz-1	172.29.121.4	255.255.255.0	UP	YES vlan 451
Voz-2	172.29.122.4	255.255.255.0	UP	YES vlan 452
Voz-Oxe	172.20.46.240	255.255.255.0	UP	YES vlan 2
Voz_Gab_J	10.1.52.1	255.255.255.128	UP	YES vlan 241
Voz_Gab_K	10.1.54.1	255.255.255.128	UP	YES vlan 251
Wan-Backup-Tdp	192.168.131.190	255.255.255.248	DOWN	NO vlan 9
prueba	0.0.0.0	0.0.0.0	DOWN	NO unbound
vlan_130	10.1.18.1	255.255.254.0	UP	YES vlan 130
vlan_150	10.1.26.1	255.255.254.0	UP	YES vlan 150
vlan_151	10.1.28.1	255.255.255.0	UP	YES vlan 151
vlan_152	10.1.29.1	255.255.255.192	DOWN	NO vlan 152
vlan_170	10.1.34.1	255.255.255.0	UP	YES vlan 170
vlan_172	10.1.36.1	255.255.255.192	DOWN	NO vlan 172

Figura 25. Servicios por Subredes. Fuente: Oficina de Soporte Informatico (2017)

Nota: Se muestra los Números de reportes de las Subredes (voz, datos, video, Pacs, Wifi e impresión, estas son (06)).



1.2. Tiempo de transferencia de Datos.

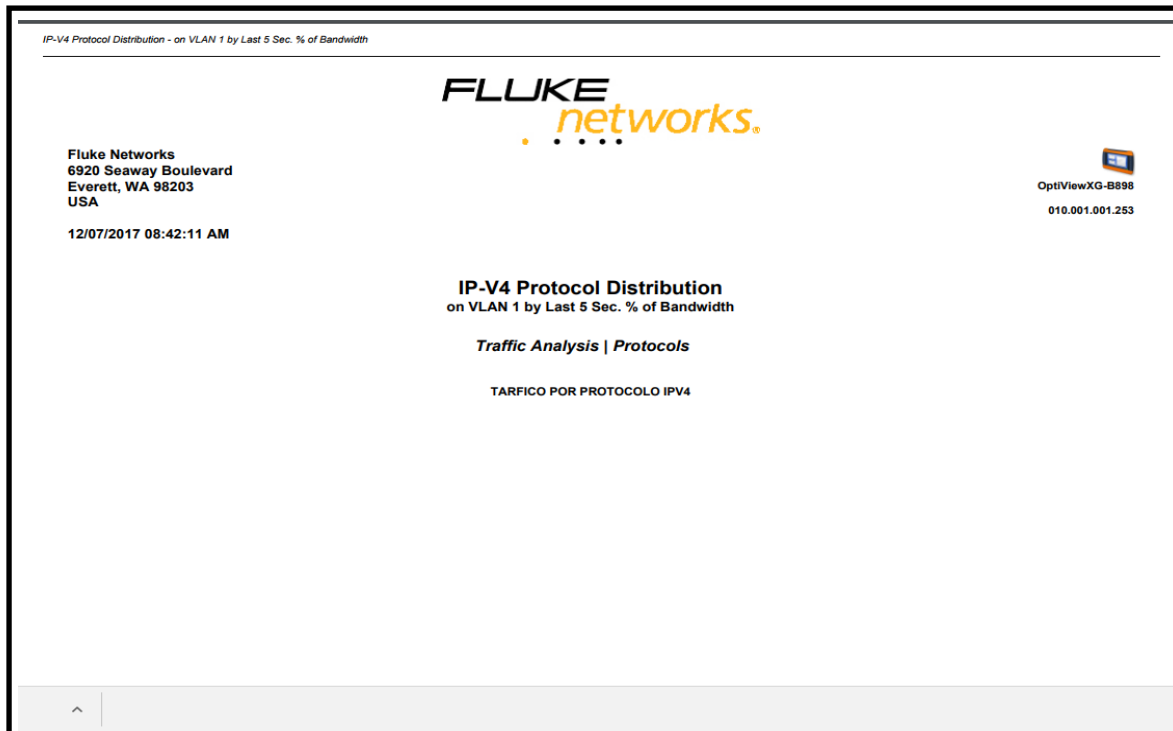


Figura 26. Trafico Protocolo IPV4 Fuente: Oficina de Soporte Informático (2017).

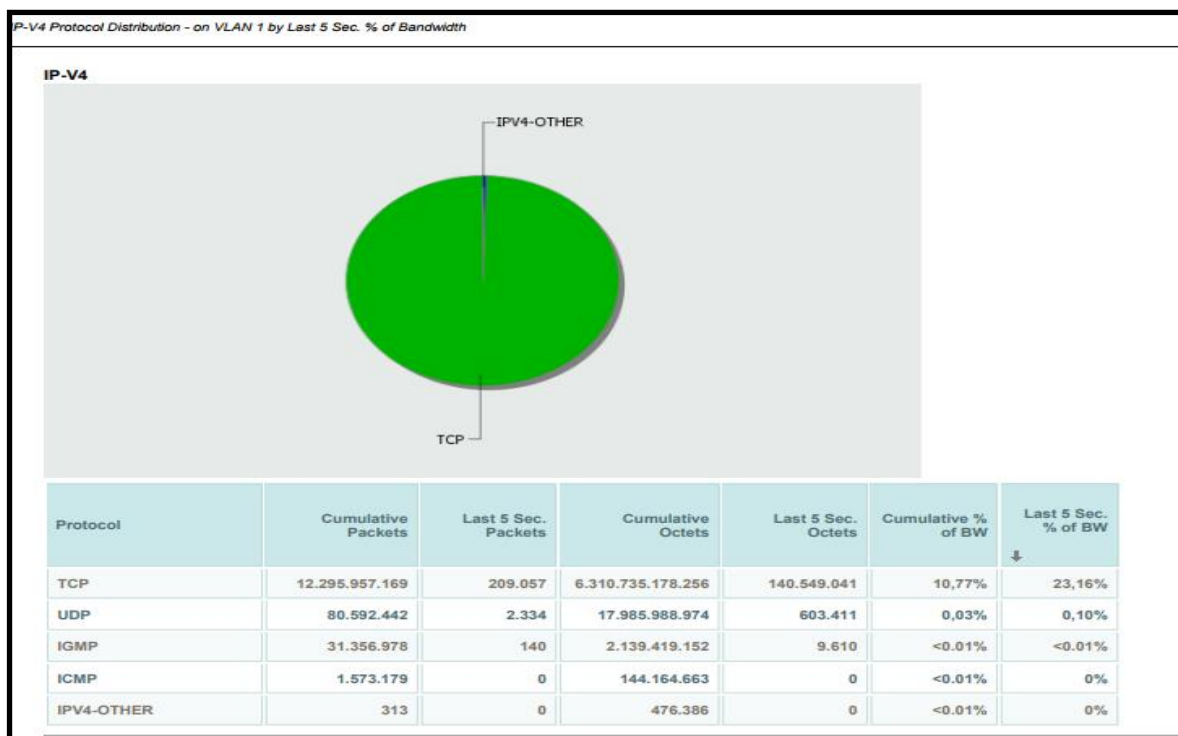


Figura 20. Porcentaje % of Bandwidth Fuente: Oficina de Soporte Informático (2017).



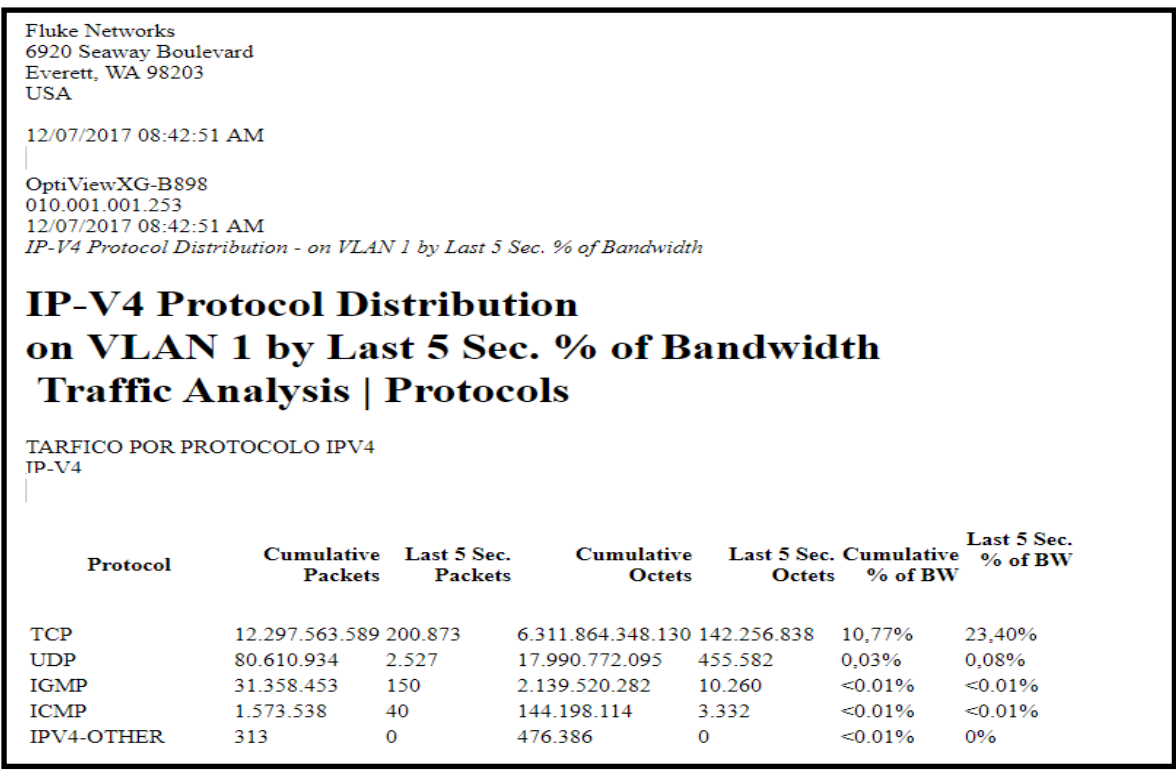


Figura 28. IP-V4 Protocol Distribution Fuente: Oficina de Soporte Informático (2017).

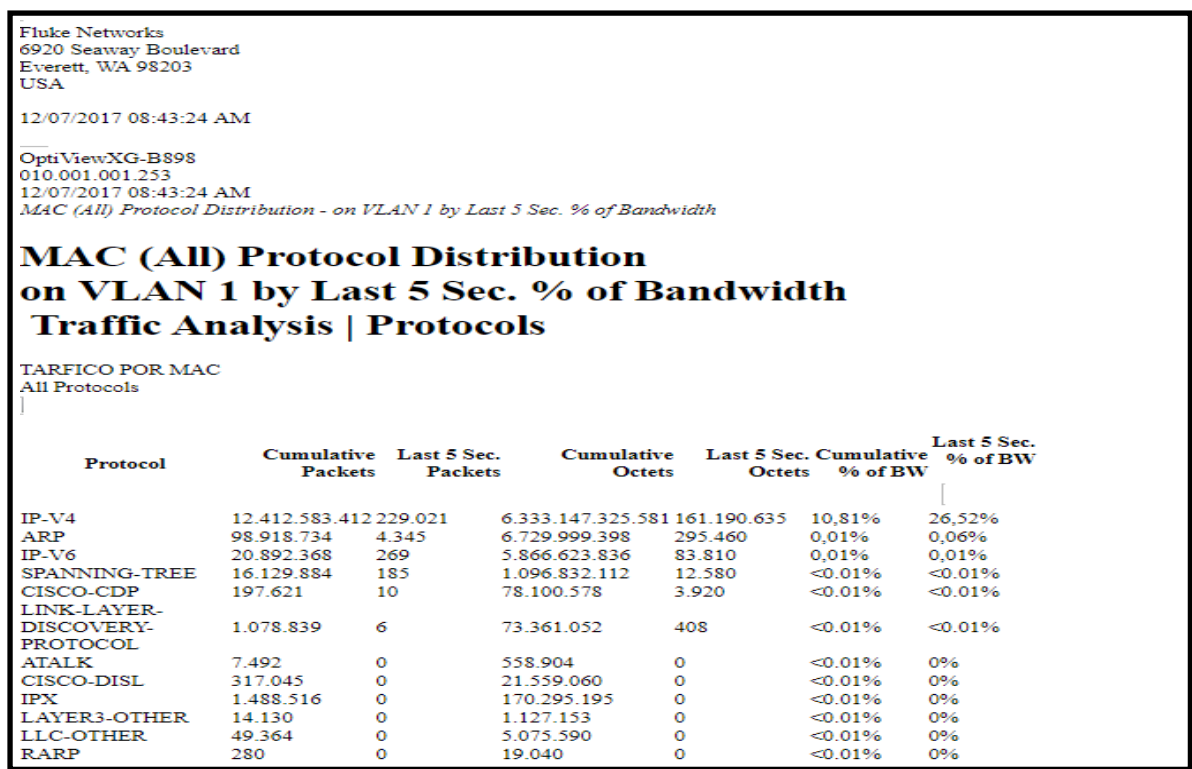


Figura 21. Tráfico por Mac all Protocols Fuente: Oficina de Soporte Informático (2017).



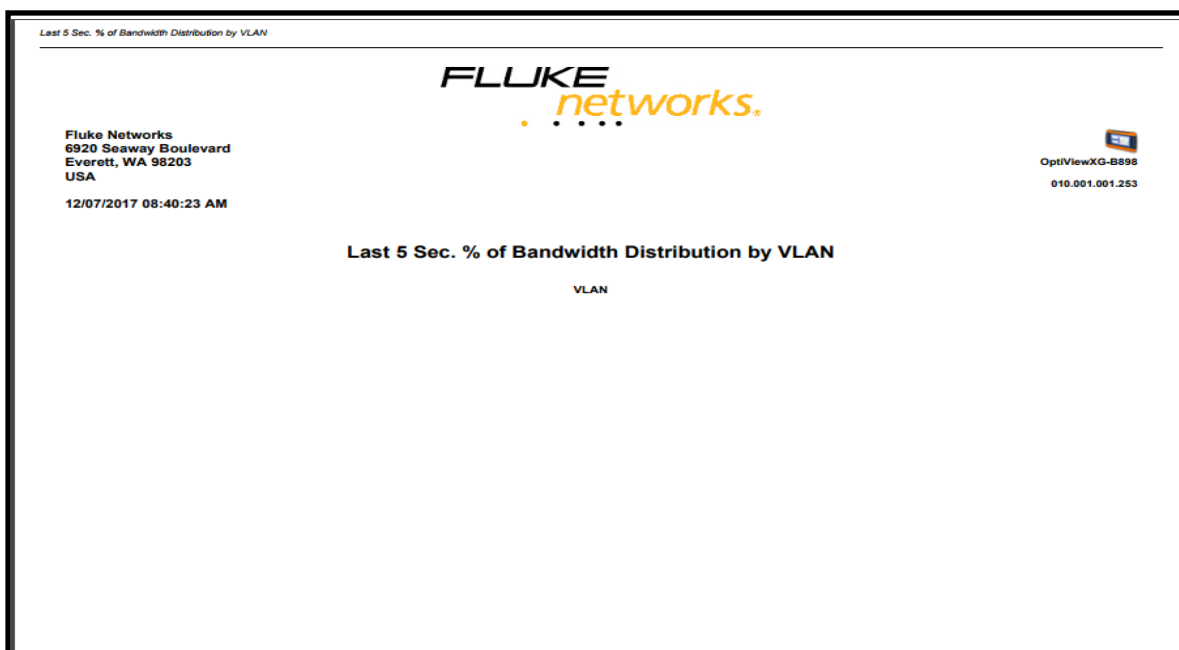


Figura 30. Porcentaje % Bandwidth Distribution by VLAN Fuente: Oficina de Soporte Informático (2017).

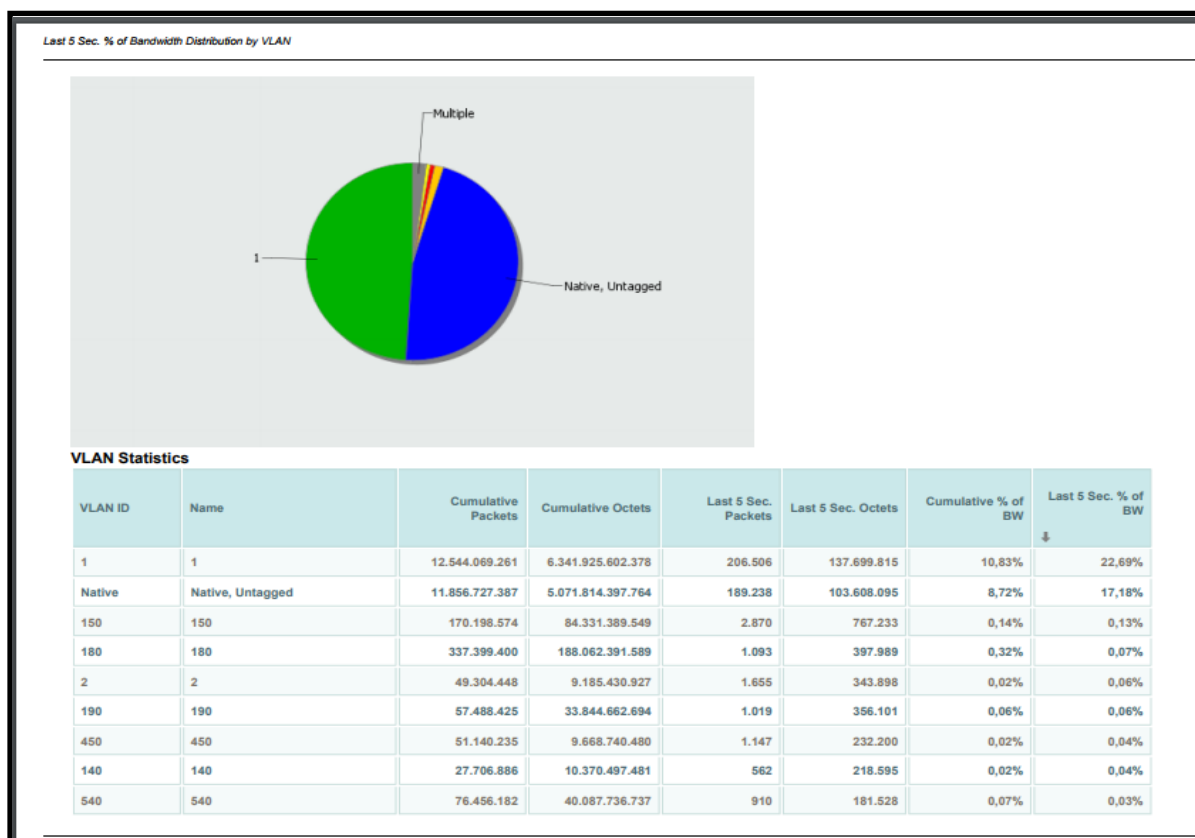


Figura 31. Bandwidth Distribution by Vlan Statistics Fuente: Oficina de Soporte Informático (2017).



Fluke Networks
6920 Seaway Boulevard
Everett, WA 98203
USA

12/07/2017 08:39:40 AM

OptiViewXG-H898
010.001.001.253
12/07/2017 08:39:40 AM
Last 5 Sec. % of Bandwidth Distribution by VLAN

Last 5 Sec. % of Bandwidth Distribution by VLAN

VLAN

VLAN Statistics

VLAN ID	Name	Cumulative Packets	Cumulative Octets	Last 5 Sec. Packets	Last 5 Sec. Octets	Cumulative % of BW	Last 5 Sec. % of BW
1	1	12.542.083.185	6.340.486.783.682	309.729	240.233.147	10,83%	37,55%
Native	Native, Untagged	11.854.867.880	5.070.590.188.090	282.336	171.549.867	8,72%	27,00%
150	150	170.175.521	84.324.825.036	4.947	2.646.233	0,14%	0,42%
190	190	57.477.250	33.840.076.424	2.830	2.241.925	0,06%	0,35%
180	180	337.390.497	188.058.903.481	1.116	455.339	0,32%	0,07%
250	250	30.302.317	15.784.252.589	1.400	415.936	0,03%	0,07%
540	540	76.449.344	40.086.506.810	1.352	262.380	0,07%	0,04%
450	450	51.133.066	9.667.285.490	876	179.571	0,02%	0,03%
2	2	49.296.176	9.183.743.224	831	164.475	0,02%	0,03%
140	140	27.703.804	10.369.439.485	409	162.343	0,02%	0,03%
270	270	19.935.295	9.046.759.916	588	99.293	0,02%	0,02%
130	130	16.512.904	8.428.790.691	139	96.398	0,01%	0,02%
240	240	176.140.323	168.045.690.968	138	68.930	0,28%	0,01%
120	120	1.086.856	182.304.435	53	28.108	<-0,01%	<-0,01%
192	192	5.472.258	2.865.223.519	89	13.236	<-0,01%	<-0,01%
170	170	1.592.028	301.789.248	38	13.368	<-0,01%	<-0,01%
999	999	34.614.163	15.537.141.947	81	5.508	0,03%	<-0,01%
510	510	129.590.817	122.376.027.541	40	5.770	0,21%	<-0,01%
260	260	4.866.334	1.466.840.735	19	5.160	<-0,01%	<-0,01%
162	162	7.732.423	6.720.881.824	5	611	0,01%	<-0,01%
200	200	1.179.386	118.230.377	7	476	<-0,01%	<-0,01%
500	500	1.034.776	84.822.673	7	476	<-0,01%	<-0,01%
182	182	2.571.811	741.938.836	5	459	<-0,01%	<-0,01%
110	110	1.164.318	234.793.938	6	422	<-0,01%	<-0,01%
132	132	636.731	517.511.564	4	272	<-0,01%	<-0,01%
141	141	241.545	16.425.060	4	272	<-0,01%	<-0,01%
122	122	477.950	32.500.600	3	204	<-0,01%	<-0,01%
160	160	1.613.518	354.828.777	3	204	<-0,01%	<-0,01%
241	241	475.983	32.366.844	3	204	<-0,01%	<-0,01%
252	252	235.081	15.985.508	3	204	<-0,01%	<-0,01%
451	451	477.376	32.461.568	3	204	<-0,01%	<-0,01%
530	530	722.209	121.957.866	3	204	<-0,01%	<-0,01%
112	112	237.937	16.179.716	2	136	<-0,01%	<-0,01%
202	202	259.494	36.769.072	2	136	<-0,01%	<-0,01%
230	230	1.043.302	298.847.528	2	136	<-0,01%	<-0,01%
262	262	236.121	16.056.228	2	136	<-0,01%	<-0,01%
100	100	788.077	53.589.236	0	0	<-0,01%	0%
131	131	240.758	16.371.544	0	0	<-0,01%	0%
151	151	239.061	16.256.148	0	0	<-0,01%	0%
220	220	510.593	34.720.324	0	0	<-0,01%	0%
242	242	266.367	18.112.956	0	0	<-0,01%	0%
251	251	239.023	16.253.564	0	0	<-0,01%	0%
272	272	239.606	16.293.208	0	0	<-0,01%	0%
452	452	240.179	16.332.172	0	0	<-0,01%	0%

Figura 32. Porcentaje % Bandwidth Distribution by Vlan Statistics. Fuente: Oficina de Soporte Informático (2017).



```
Vlan type: rtr => Router Vlan, reserved for rtr-port IP Interface
```

vlan	type	admin	oper	stree			auth	ip	ipx	mble tag	src lrn	name
				1x1	flat	auth						
1	std	on	on	on	on	off	on	NA	off	on	VLAN 1	
2	std	on	on	on	on	off	on	NA	off	on	Server-Voz	
9	std	on	off	on	on	off	on	NA	off	on	Wan-Backup-Tdp	
10	std	on	on	off	off	off	on	NA	off	on	Enlace-Sede-Central	
100	std	on	on	on	on	off	on	NA	off	on	Datos_Gab_A	
101	std	on	off	on	on	off	off	NA	off	on	Voz_Gab_A	
102	std	on	off	on	on	off	off	NA	off	on	Impresoras_Gab_A	
110	std	on	on	on	on	off	on	NA	off	on	Datos_Gab_C	
111	std	on	off	on	on	off	off	NA	off	on	Voz_Gab_C	
112	std	on	on	on	on	off	on	NA	off	on	Impresoras_Gab_C	
120	std	on	on	on	on	off	on	NA	off	on	Datos_Gab_B3	
121	std	on	off	on	on	off	off	NA	off	on	Voz_Gab_B3	
122	std	on	on	on	on	off	on	NA	off	on	Impresoras_Gab_B3	
130	std	on	on	on	on	off	on	NA	off	on	Datos_Gab_A1	
131	std	on	off	on	on	off	off	NA	off	on	Voz_Gab_A1	
132	std	on	on	on	on	off	on	NA	off	on	Impresoras_Gab_A1	
140	std	on	on	on	on	off	on	NA	off	on	Datos_Gab_C1	
141	std	on	on	on	on	off	off	NA	off	on	Voz_Gab_C1	
142	std	on	off	on	on	off	off	NA	off	on	Impresoras_Gab_C1	
150	std	on	on	on	on	off	on	NA	off	on	Datos_Gab_I1	
151	std	on	on	on	on	off	on	NA	off	on	Voz_Gab_I1	
152	std	on	off	on	on	off	on	NA	off	on	Impresoras_Gab_I1	
160	std	on	on	on	on	off	on	NA	off	on	Datos_Gab_I2	
161	std	on	off	on	on	off	off	NA	off	on	Voz_Gab_I2	
162	std	on	on	on	on	off	on	NA	off	on	Impresoras_Gab_I2	
170	std	on	on	on	on	off	on	NA	off	on	Datos_Gab_G	
171	std	on	off	on	on	off	off	NA	off	on	Voz_Gab_G	
172	std	on	off	on	on	off	on	NA	off	on	Impresoras_Gab_G	
173	std	on	off	on	on	off	off	NA	off	on	Wireless_Gab_G	
180	std	on	on	on	on	off	on	NA	off	on	Datos_Gab_F	
182	std	on	on	on	on	off	on	NA	off	on	Impresoras_Gab_F	
190	std	on	on	on	on	off	on	NA	off	on	Datos_Gab_M	
191	std	on	off	on	on	off	off	NA	off	on	Voz_Gab_M	
192	std	on	on	on	on	off	on	NA	off	on	Impresoras_Gab_M	
200	std	on	on	on	on	off	on	NA	off	on	Datos_Gab_B1	
202	std	on	on	on	on	off	on	NA	off	on	Impresoras_Gab_B1	
220	std	on	on	on	on	off	on	NA	off	on	Datos_Gab_D	
221	std	on	off	on	on	off	off	NA	off	on	Voz_Gab_D	
230	std	on	on	on	on	off	on	NA	off	on	Datos_Gab_G3	
240	std	on	on	on	on	off	on	NA	off	on	Datos_Gab_J	
241	std	on	on	on	on	off	on	NA	off	on	Voz_Gab_J	
242	std	on	on	on	on	off	on	NA	off	on	Impresoras_Gab_J	
250	std	on	on	on	on	off	on	NA	off	on	Datos_Gab_K	
251	std	on	on	on	on	off	on	NA	off	on	Voz_Gab_K	
252	std	on	on	on	on	off	on	NA	off	on	Impresoras_Gab_K	
260	std	on	on	on	on	off	on	NA	off	on	Datos_Gab_L	
262	std	on	on	on	on	off	on	NA	off	on	Impresora_Gab_L	
270	std	on	on	on	on	off	on	NA	off	on	Datos_Gab_N	
272	std	on	on	on	on	off	on	NA	off	on	Impresoras_Gab_N	
280	std	on	off	on	on	off	off	NA	off	on	Datos_Gab_N1	
282	std	on	off	on	on	off	off	NA	off	on	Impresoras_Gab_N1	
450	std	on	on	on	on	off	on	NA	off	on	Voz-0	
451	std	on	on	on	on	off	on	NA	off	on	Voz-1	
452	std	on	on	on	on	off	on	NA	off	on	Voz-2	
500	std	on	on	on	on	off	on	NA	off	on	Camaras_vigilancia	
510	std	on	on	on	on	off	on	NA	off	on	Imagenes_Packs	
530	std	on	on	on	on	off	on	NA	off	on	Marcadores_biometricos	
540	std	on	on	on	on	off	on	NA	off	on	Server	
999	std	on	on	on	on	off	on	NA	off	on	Admin_Switches	

Figura 33. VLAN Type TRT-PORT IP Interface. Fuente: Oficina De Soporte Informático (2017).

Nota: Se muestra la medición del Tiempo de transferencia de datos en 5 Sec. del Ancho de Banda, IPV4, Protocolos, Mac.



1.3. Número de redes virtuales Existentes

Datos_Gab	0.0.0.0	0.0.0.0	DOWN	NO unbound
Datos_Gab_A	10.1.6.1	255.255.254.0	UP	YES vlan 100
Datos_Gab_A1	0.0.0.0	0.0.0.0	DOWN	NO unbound
Datos_Gab_B1	10.1.43.1	255.255.255.0	UP	YES vlan 200
Datos_Gab_B3	10.1.14.1	255.255.254.0	UP	YES vlan 120
Datos_Gab_C	10.1.10.1	255.255.254.0	UP	YES vlan 110
Datos_Gab_C1	10.1.22.1	255.255.254.0	UP	YES vlan 140
Datos_Gab_D	10.1.47.1	255.255.255.0	UP	YES vlan 220
Datos_Gab_F	10.1.37.1	255.255.255.0	UP	YES vlan 180
Datos_Gab_G3	10.1.49.1	255.255.255.0	UP	YES vlan 230
Datos_Gab_I2	10.1.30.1	255.255.254.0	UP	YES vlan 160
Datos_Gab_J	10.1.51.1	255.255.255.0	UP	YES vlan 240
Datos_Gab_K	10.1.53.1	255.255.255.0	UP	YES vlan 250
Datos_Gab_L	10.1.55.1	255.255.255.0	UP	YES vlan 260
Datos_Gab_M	10.1.40.1	255.255.255.0	UP	YES vlan 190
Datos_Gab_N	10.1.57.1	255.255.255.0	UP	YES vlan 270
EMP	192.168.1.1	255.255.255.0	DOWN	NO EMP
Enlace-Sede-Central	192.168.20.40	255.255.255.0	UP	YES vlan 10
Imagenes_Packs	10.1.3.1	255.255.255.0	UP	YES vlan 510
Impresora_Gab_L	10.1.56.129	255.255.255.224	UP	YES vlan 262
Impresoras_Gab_A1	10.1.21.1	255.255.255.192	UP	YES vlan 132
Impresoras_Gab_B1	10.1.44.129	255.255.255.224	UP	YES vlan 202
Impresoras_Gab_B3	10.1.17.1	255.255.255.192	UP	YES vlan 122
Impresoras_Gab_C	10.1.13.1	255.255.255.192	UP	YES vlan 112
Impresoras_Gab_F	10.1.39.1	255.255.255.192	UP	YES vlan 182
Impresoras_Gab_I1	0.0.0.0	0.0.0.0	DOWN	NO unbound
Impresoras_Gab_I2	10.1.33.1	255.255.255.192	UP	YES vlan 162
Impresoras_Gab_J	10.1.52.129	255.255.255.224	UP	YES vlan 242
Impresoras_Gab_K	10.1.54.129	255.255.255.224	UP	YES vlan 252
Impresoras_Gab_M	10.1.42.1	255.255.255.192	UP	YES vlan 192
Impresoras_Gab_N	10.1.58.129	255.255.255.224	UP	YES vlan 272
Loopback	127.0.0.1	255.0.0.0	UP	NO Loopback
Marcadores_bicme	10.1.5.1	255.255.255.192	UP	YES vlan 530
Server	10.1.0.1	255.255.255.128	UP	YES vlan 540
Voz-0	172.29.120.4	255.255.255.0	UP	YES vlan 450
Voz-1	172.29.121.4	255.255.255.0	UP	YES vlan 451
Voz-2	172.29.122.4	255.255.255.0	UP	YES vlan 452
Voz-Oxe	172.20.46.240	255.255.255.0	UP	YES vlan 2
Voz_Gab_J	10.1.52.1	255.255.255.128	UP	YES vlan 241
Voz_Gab_K	10.1.54.1	255.255.255.128	UP	YES vlan 251
Wan-Backup-Tdp	192.168.131.190	255.255.255.248	DOWN	NO vlan 9
prueba	0.0.0.0	0.0.0.0	DOWN	NO unbound
vlan_130	10.1.18.1	255.255.254.0	UP	YES vlan 130
vlan_150	10.1.26.1	255.255.254.0	UP	YES vlan 150
vlan_151	10.1.28.1	255.255.255.0	UP	YES vlan 151
vlan_152	10.1.29.1	255.255.255.192	DOWN	NO vlan 152
vlan_170	10.1.34.1	255.255.255.0	UP	YES vlan 170
vlan_172	10.1.36.1	255.255.255.192	DOWN	NO vlan 172

Figura 34. Número de redes virtuales Existentes. Fuente: Oficina de Soporte Informático (2017).

Nota: Se muestra los números de redes existentes estos son (02) Voz 450 con 1190 anexos y Datos VLAN1 con 3000 dispositivos (Pc., impresoras, cámaras, equipos médicos, servidores y equipos de comunicaciones).

Actualmente: por las dos VLANS hay 31 * 5 +5 por cada gabinete de Voz, Datos, Impresoras y Wifi Libre, en general servidores, cámaras, administración de Switch, equipos médicos, imágenes Pacs y marcadores biométricos.



2.1. Porcentaje de Escalamiento Horizontal y Vertical de la Red al Año.

Tabla 8
Cuadro Consolidado de Inactividad del Dispositivo Conmutador Core Principal

Cuadro de Inactividad del Dispositivo de Conmutación Core Principal Año 2016 y 2017													
Fecha-Inicio	Hora-Inicio	Fecha-Fin	Hora-Fin	Tiempo (Días)	Tiempo (Hrs)	Usuarios Afectados	T.UNICAST	T.MULTICAST	T.BROADCAST	Ancho de Banda	Cargas BPS	Cargas Packets	Motivo
02/02/2016	15:45:00	02/02/2016	4:32:00 PM	0	0:47:00	1210.00	31.6%	9.8%	58.6%	2.2%	22,552Mbps	2M	Loop GDS-C1
21/04/2016	10:25:00	21/04/2016	10:48:00 AM	0	0:23:00	618.00	18.3%	9.3%	72.4%	6.3%	63,663Mbps	6M	Loop GDS-C2
22/04/2016	16:00:00	22/04/2016	4:33:00 PM	0	0:33:00	900.00	42.4%	52.0%	5.6%	51.4%	554,663Mbps	52M	Loop GDS-C1
22/04/2016	13:21:00	25/04/2016	1:25:00 PM	3	0:04:00	869.00	40.2%	50.0%	5.0%	50.2%	550,552Mbps	52M	Loop GDS-C2
16/05/2016	11:25:00	16/05/2016	12:30:00 PM	0	1:05:00	1200.00	50.6%	36.4%	13.0%	41.1%	441,668 Mbps	442K	Anomalia Trafico Multicast a consecuencia de
19/05/2016	8:25:00	19/05/2016	9:43:00 AM	0	1:18:00	950.00	3.5%	92.9%	3.6%	93.1%	993,630 Mbps	4346K	Anomalia Trafico Multicast a consecuencia de
14/07/2016	9:15:00	14/07/2016	1:02:00 PM	0	3:47:00	1250.00	42.4%	52.0%	5.6%	51.4%	554,663Mbps	52M	Anomalia Trafico Multicast a consecuencia de
04/08/2016	13:15:00	04/08/2016	2:00:00 PM	0	0:45:00	1100.00	3.3%	95.8%	0.9%	99.7%	998,740 Mbps	4586K	Anomalia Trafico Multicast a consecuencia de
16/08/2016	13:10:00	16/08/2016	2:15:00 PM	0	1:05:00	1600.00	4.9%	93.4%	1.7%	100%	1 Gbps	4609K	Anomalia Trafico Multicast a consecuencia de
17/08/2016	14:23:00	17/08/2016	2:25:00 PM	0	0:02:00	1600.00	4.1%	94.6%	1.3%	98.9%	988,687 Mbps	4557K	Anomalia Trafico Multicast a consecuencia de
22/08/2016	13:50:00	22/08/2016	2:15:00 PM	0	0:25:00	1300.00	86.6%	12.8%	0.6%	77.3%	772,557 Mbps	3394K	Anomalia Trafico Multicast a consecuencia de
29/08/2016	12:10:00	29/08/2016	1:15:00 PM	0	1:05:00	1450.00	14.1%	12.2%	73.7%	66.8%	668,084 Mbps	1846K	Trafico Broadcast en VLAN 1
01/09/2016	9:02:00	01/09/2016	9:45:00 AM	0	0:43:00	1300.00	8.9%	29.5%	3.9%	27.0%	270,334Mbps	1786K	Anomalia Trafico Multicast a consecuencia de
01/09/2016	13:52:00	01/09/2016	2:08:00 PM	0	0:16:00	1200.00	40.0%	29.5%	1.0%	76.1%	761,054Mbps	3078K	Anomalia Trafico Multicast a consecuencia de
07/09/2016	12:45:00	07/09/2016	12:48:00 PM	0	0:03:00	1300.00	42.4%	52.0%	5.6%	51.4%	554,663Mbps	52M	Loop GDS-N
28/09/2016	12:05:00	28/09/2016	12:32:00 PM	0	0:27:00	1800.00	14.1%	12.1%	73.7%	66.8%	668,084 Mbps	1846K	Trafico Broadcast en VLAN 1
28/06/2017	10:00:00	28/06/2017	11:00:00 AM	0	1:00:00	1801.00	60.0%	32.0%	8.0%	70.2%	702,020 Mbps	1886K	Trafico Broadcast en VLAN 1
30/06/2017	7:55:00	30/06/2017	8:25:00 AM	0	0:30:00	1802.00	-	-	-	-	-	-	Corte de Fluido Eléctrico

Fuente: Elaboración Propia (2017).

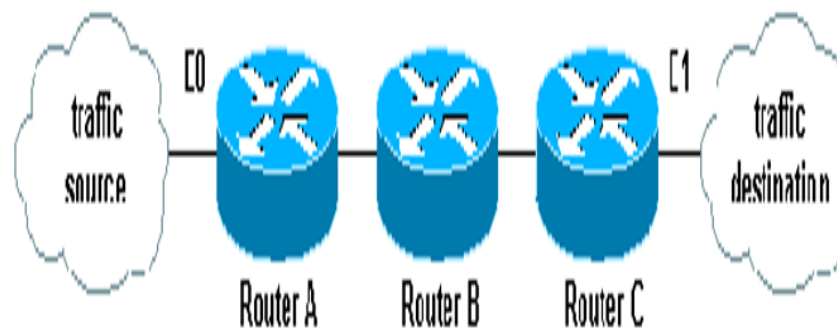
Nota: En el presente cuadro se muestra la medición del consolidado de la bitácora de caídas del conmutador (CORE Principal), donde se detalla el tiempo de inactividad en número de días, horas, ancho de banda consumido, principales cargas en Mbps y pkts. y usuarios afectados.

- El año 2016 presentó 16 caídas de red con un tiempo de inactividad de 12 horas con 48 minutos, el mismo que afectó a un promedio 1,227 usuarios.
- Para el año 2017 mes de junio se han presentado 2 caídas de red, las mismas que ocasionaron un tiempo de inactividad de 01 hora con 30 minutos afectando a un total de 1,801 usuarios.



3.1. Número de Listas de Acceso ACL, por Subredes.

Datos_Gab	0.0.0.0	0.0.0.0	DOWN	NO unbound
Datos_Gab_A	10.1.6.1	255.255.254.0	UP	YES vlan 100
Datos_Gab_A1	0.0.0.0	0.0.0.0	DOWN	NO unbound
Datos_Gab_B1	10.1.43.1	255.255.255.0	UP	YES vlan 200
Datos_Gab_B3	10.1.14.1	255.255.254.0	UP	YES vlan 120
Datos_Gab_C	10.1.10.1	255.255.254.0	UP	YES vlan 110
Datos_Gab_C1	10.1.22.1	255.255.254.0	UP	YES vlan 130
Datos_Gab_D	10.1.47.1	255.255.255.0	UP	YES vlan 220
Datos_Gab_F	10.1.37.1	255.255.255.0	UP	YES vlan 180
Datos_Gab_G3	10.1.49.1	255.255.255.0	UP	YES vlan 230
Datos_Gab_I2	10.1.30.1	255.255.254.0	UP	YES vlan 160
Datos_Gab_J	10.1.51.1	255.255.255.0	UP	YES vlan 240
Datos_Gab_K	10.1.53.1	255.255.255.0	UP	YES vlan 250
Datos_Gab_L	10.1.55.1	255.255.255.0	UP	YES vlan 260
Datos_Gab_M	10.1.40.1	255.255.255.0	UP	YES vlan 190
Datos_Gab_N	10.1.57.1	255.255.255.0	UP	YES vlan 270
EMP	192.168.1.1	255.255.255.0	DOWN	NO EMP
Enlace-Sede-Central	192.168.20.40	255.255.255.0	UP	YES vlan 10
Imagenes_Packs	10.1.3.1	255.255.255.0	UP	YES vlan 510
Impresora_Gab_L	10.1.56.129	255.255.255.224	UP	YES vlan 262
Impresoras_Gab_A1	10.1.21.1	255.255.255.192	UP	YES vlan 132
Impresoras_Gab_B1	10.1.44.129	255.255.255.224	UP	YES vlan 202
Impresoras_Gab_B3	10.1.17.1	255.255.255.192	UP	YES vlan 122
Impresoras_Gab_C	10.1.13.1	255.255.255.192	UP	YES vlan 112
Impresoras_Gab_F	10.1.39.1	255.255.255.192	UP	YES vlan 182
Impresoras_Gab_I1	0.0.0.0	0.0.0.0	DOWN	NO unbound
Impresoras_Gab_I2	10.1.33.1	255.255.255.192	UP	YES vlan 162
Impresoras_Gab_J	10.1.52.129	255.255.255.224	UP	YES vlan 242
Impresoras_Gab_K	10.1.54.129	255.255.255.224	UP	YES vlan 252
Impresoras_Gab_M	10.1.42.1	255.255.255.192	UP	YES vlan 192
Impresoras_Gab_N	10.1.58.129	255.255.255.224	UP	YES vlan 272
Loopback	127.0.0.1	255.0.0.0	UP	NO Loopback
Marcoadores_biome	10.1.5.1	255.255.255.192	UP	YES vlan 530
Server	10.1.8.1	255.255.255.128	UP	YES vlan 540
Voz-0	172.29.120.4	255.255.255.0	UP	YES vlan 450
Voz-1	172.29.121.4	255.255.255.0	UP	YES vlan 451
Voz-2	172.29.122.4	255.255.255.0	UP	YES vlan 452
Voz-Oxe	172.20.46.240	255.255.255.0	UP	YES vlan 2
Voz_Gab_J	10.1.52.1	255.255.255.128	UP	YES vlan 241
Voz_Gab_K	10.1.54.1	255.255.255.128	UP	YES vlan 251
Wan-Backup-Tdp	192.168.131.190	255.255.255.248	DOWN	NO vlan 9
prueba	0.0.0.0	0.0.0.0	DOWN	NO unbound
vlan_130	10.1.18.1	255.255.254.0	UP	YES vlan 130
vlan_150	10.1.26.1	255.255.254.0	UP	YES vlan 150
vlan_151	10.1.28.1	255.255.255.0	UP	YES vlan 151
vlan_152	10.1.29.1	255.255.255.192	DOWN	NO vlan 152
vlan_170	10.1.34.1	255.255.255.0	UP	YES vlan 170
vlan_172	10.1.36.1	255.255.255.192	DOWN	NO vlan 172



Definición de Entrada, Salida, Entrante, Saliente, Origen y Destino:

El router utiliza los términos entrada, salida, origen y destino como referencias. El tráfico en el router se puede comparar con el tráfico en una carretera.

Figura 35. Número de Listas de Acceso ACL, por Subredes. Fuente: Oficina de Soporte Informático (2017).

Nota: Se muestra el número de Listas de Acceso ACL es (01) y las Subredes (voz, datos, video, Pacs, Wifi e impresión, Estas son (06)).

3.2. Número de Métodos de Autenticación y configuración.

Nota: Se muestra los Números de métodos: TELNET, SSH, HTTP y RADIUS, Estas son (04)).

4.1. Porcentaje de Disponibilidad y Tiempo de la Inactividad de la Red por mes y Año.

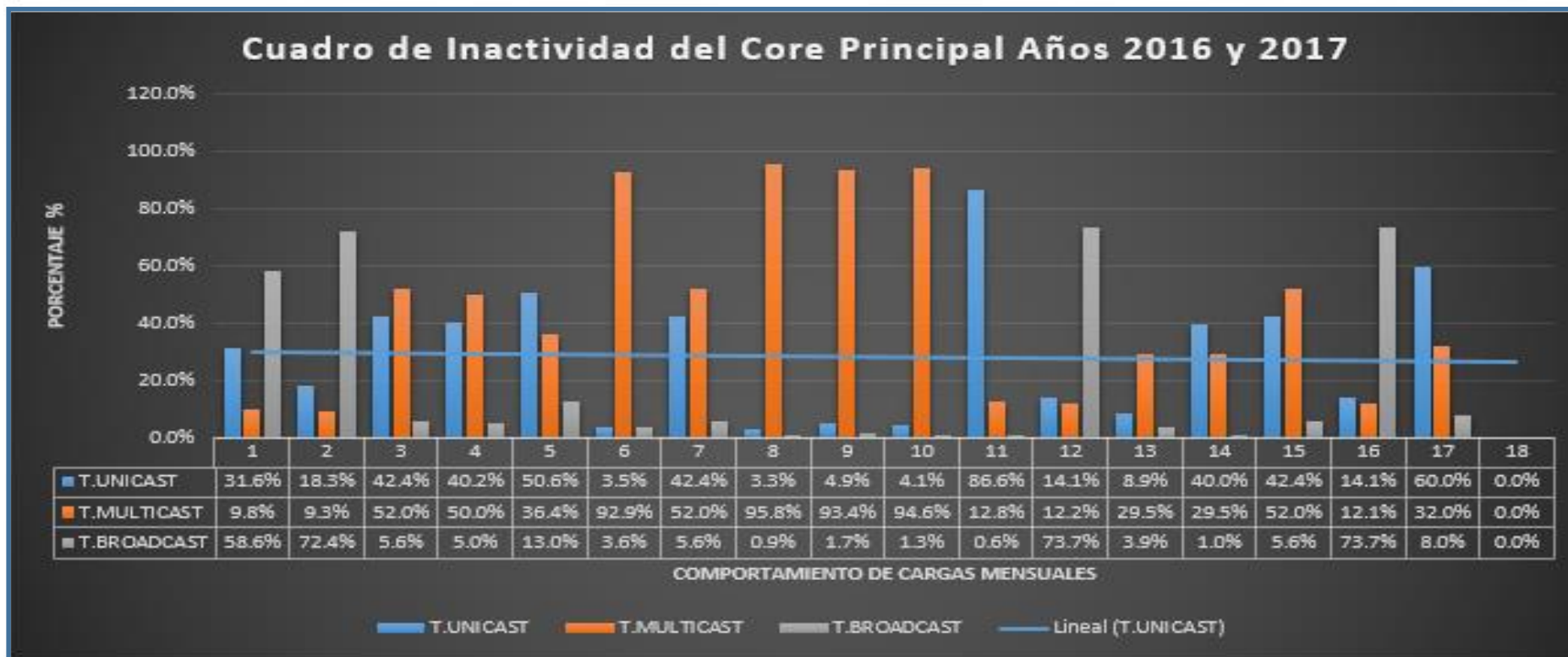


Figura 36. Consolidado de Inactividad Producidos por Unicast, Multicast y Broadcast del Core Principal de La Red LAN 2016 y 2017. Fuente: Elaboración Propia (2017).

Nota: En el presente cuadro consolidado se presenta la inactividad del conmutador (CORE Principal), por causas del multicast llegando en la referencia 8 hasta un 95.8%, así como también el Broadcast en la referencia 12 y 16 llegando hasta un 73.7% de los años 2016 y 2017.



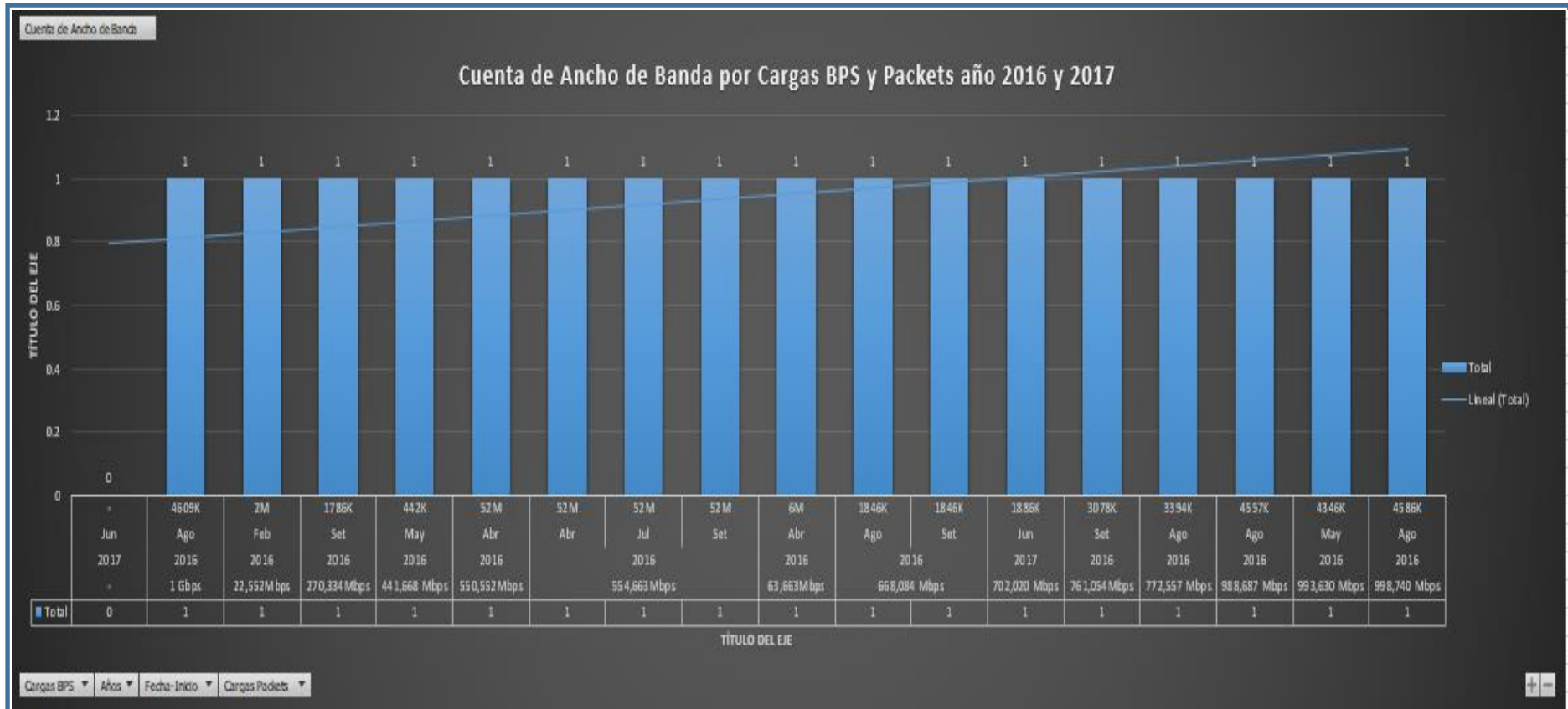


Figura 37. Consolidado de Cargas del Core Principal de La Red LAN. Fuente: Elaboración Propia (2017).

Nota: En el presente cuadro consolidado se presenta el consumo del ancho de banda producidos por las cargas en BPS y los Packets del conmutador (CORE Principal), llegando el ancho de banda al 100% el día 16/08/2016, con una carga de 1Gbps y una Carga de 4609K de Packets del 2016 a comparación del año 2017 hasta el 28/06/2017 solo se presenta un consumo de 70.2%, carga de 702,000 Mbps y 1886K de Packets, Referencia Cuadro 6 Valores del Ancho de Banda.





Figura 38. Consolidado del Ancho de Banda del Core Principal años 2016 y 2017. Fuente: Elaboración Propia (2017).

Nota: En el presente cuadro consolidado se presenta el consumo del Ancho de Banda del conmutador (CORE Principal), teniendo como referencia la fecha: 04/08/2016 con un 99.7% de consumo, el 16/08/2016 con un 100% de consumo y el 17/08/2016 con un 98.9% de los años 2016 y 2017 del HNERM-EsSALUD.



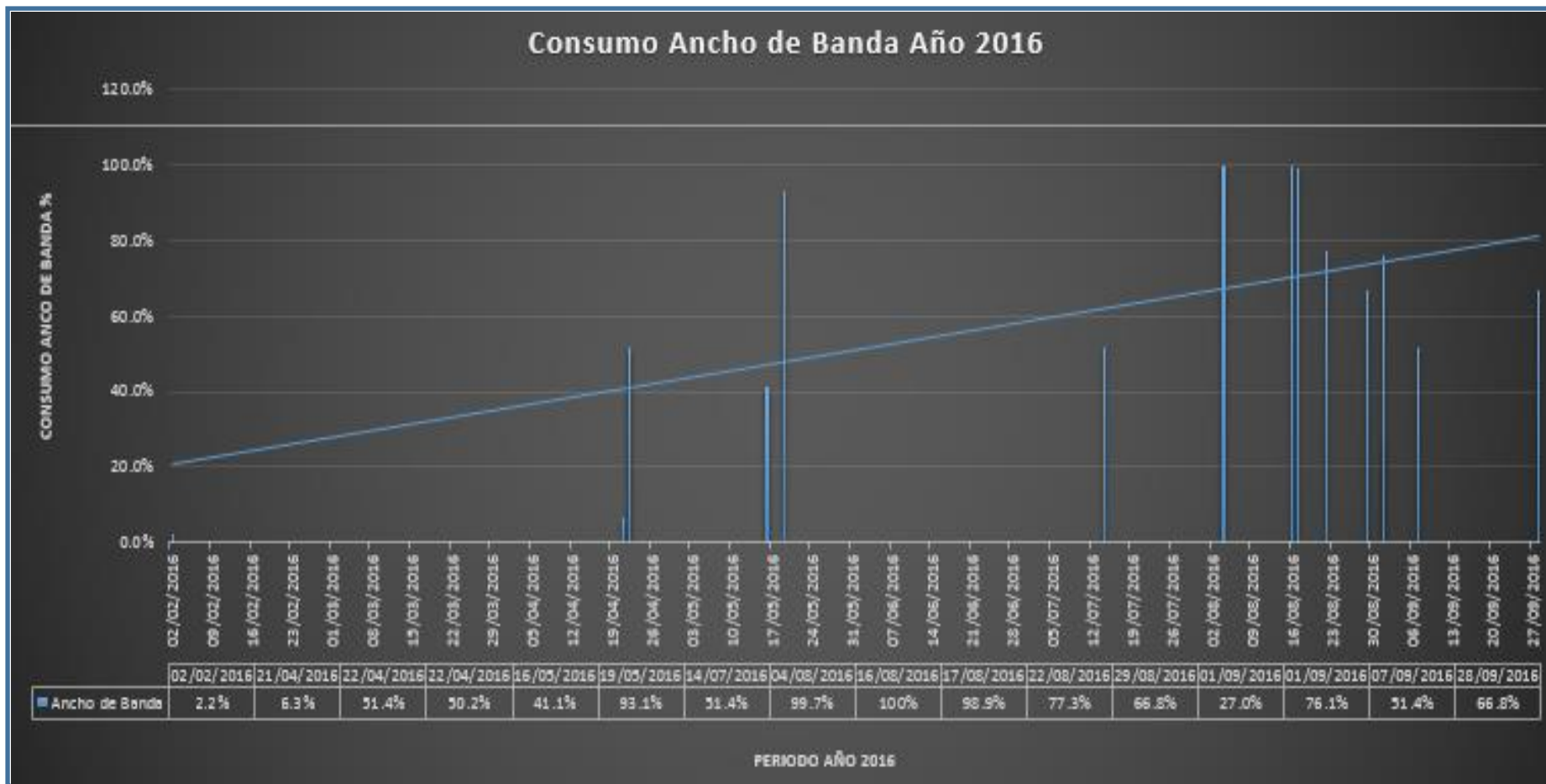


Figura 39. Consolidado del Ancho de Banda del Core Principal año 2016. Fuente: Elaboración Propia (2017).

Nota: En el presente cuadro consolidado se presenta el consumo del Ancho de Banda del conmutador (CORE Principal), teniendo como referencia la fecha: 16/08/2016 con un consumo de 100% en el año 2016 del HNERM-EsSALUD.



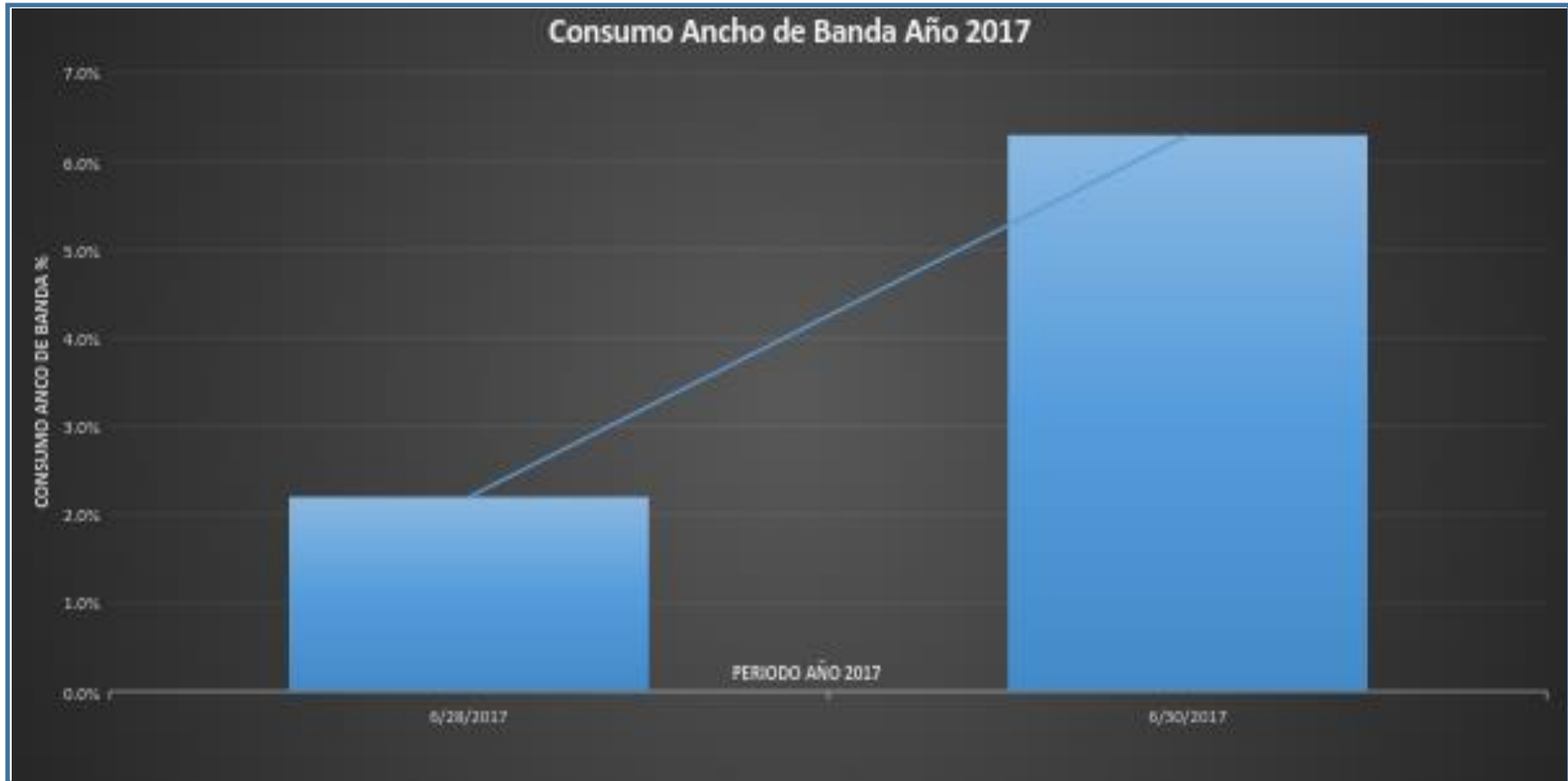


Figura 40. Consolidado del Ancho de Banda del Core Principal año 2017. Fuente: Elaboración Propia (2017).

Nota: En el presente cuadro consolidado se presenta el consumo del Ancho de Banda del conmutador (CORE Principal), teniendo como referencia la fecha: 30/06/2017 con un consumo de 70.2% en el año 2017 del HNERM-EsSALUD.



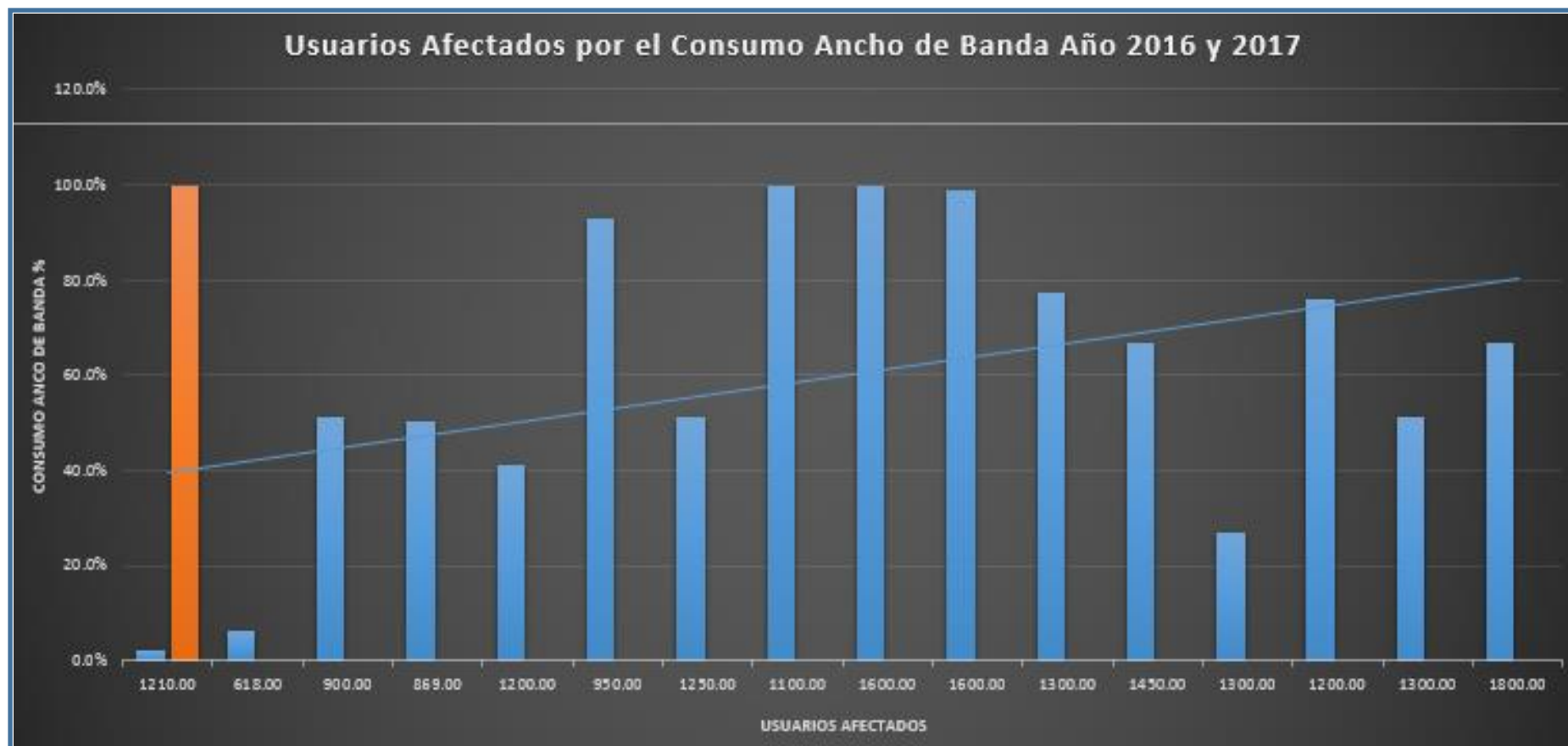


Figura 41. Consolidado Usuarios Afectados por el Consumo del Ancho de Banda del Core Principal año 2016 y 2017. Fuente: Elaboración Propia (2017).

Nota: En el presente cuadro consolidado se presenta los Usuarios afectados 1100, 1600 y 1300 por el consumo de Ancho de Banda al 100% en los años 2016 y 2017 del HNERM-EsSALUD.



4.2. Número de Enlaces Redundantes Existentes.

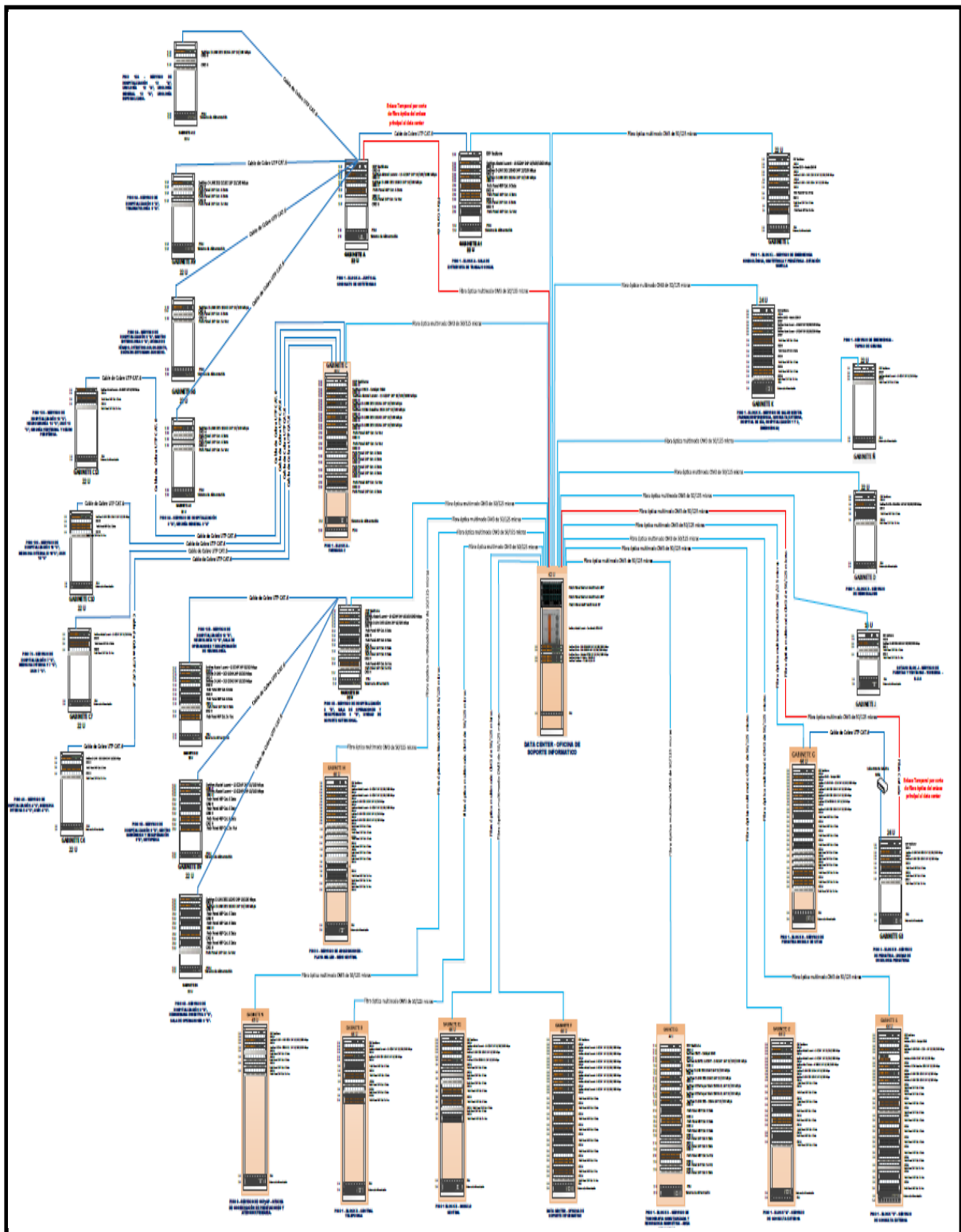


Figura 42. Número de Enlaces Redundantes Existentes. Fuente: Oficina de Soporte Informático (2017).

Nota: Se muestra los Números de Enlaces Redundantes Existentes (01), Core (135), Switches y (32) Servidores.



4.2. Discusión de los Resultados

Después de recolectar la información a través de las técnicas recolección de datos donde se han considerado la técnica de Test, la Ficha de Evaluación, la Encuesta y la Observación, se presentan los siguientes resultados: números de contextos virtuales a implementar son (08), número de Core Interconectados a virtualizar son (02) Core Nexus 7000, consumo de energía de equipos de conmutación son (135) y servidores (32) se aplicó el efecto cascada obteniendo un ahorro de 2,7 watts, consumo de energía en equipos de aire acondicionado es (20 a 82 kW) y se aplicó a (02), números de equipos servidores a virtualizar son (32), números de conmutadores a virtualizar son (135), número de reportes de análisis de calidad de servicios por subredes son (06), tiempo de transferencia de datos se muestra por 5 segundos la trama de información, número de redes virtuales existentes son (02), porcentaje de escalamiento horizontal y vertical de la red al año se muestra del año 2016 y 2017 los porcentaje hasta un 100%, números de lista de acceso ACL es (01) por las (06) subredes existentes, Se muestra los números de redes existentes estos son (02) Voz-450 con 1190 anexos y Datos VLAN1 con 3000 dispositivos (Pc., impresoras, cámaras, equipos médicos, servidores y equipos de comunicaciones. Actualmente: por las dos VLANS hay 31 * 5 +5 por cada gabinete de Voz, Datos, Impresoras y Wifi Libre, en general servidores, cámaras, administración de Switch, equipos médicos, imágenes Pacs y marcadores biométricos. números de métodos de autenticación de configuración se muestran (04) TELNET, SSH, HTTP y RADIUS, porcentaje de disponibilidad y tiempo de inactividad de la red por mes y año se muestra un tiempo de 12 horas y 48 minutos año 2016 y 1 hora y 30 minutos año 2017, consolidado se presenta los Usuarios afectados 1100, 1600 y 1300 por el consumo de Ancho de Banda al 100% en los años 2016 y 2017 y números de enlaces redundantes son (01) Core, (135) conmutadores y (32) servidores del HNERM-EsSALUD, entre las cuales los encuestados fueron todos los dispositivos de conmutación, servidores y el Core Principal del HNERM-EsSALUD

Se muestra recojo de información consolidado de la bitácora de caídas del conmutador en número de días, horas, ancho de banda consumido, principales cargas en Mbps y pkts. y usuarios afectados, en el año 2016 y año 2017.



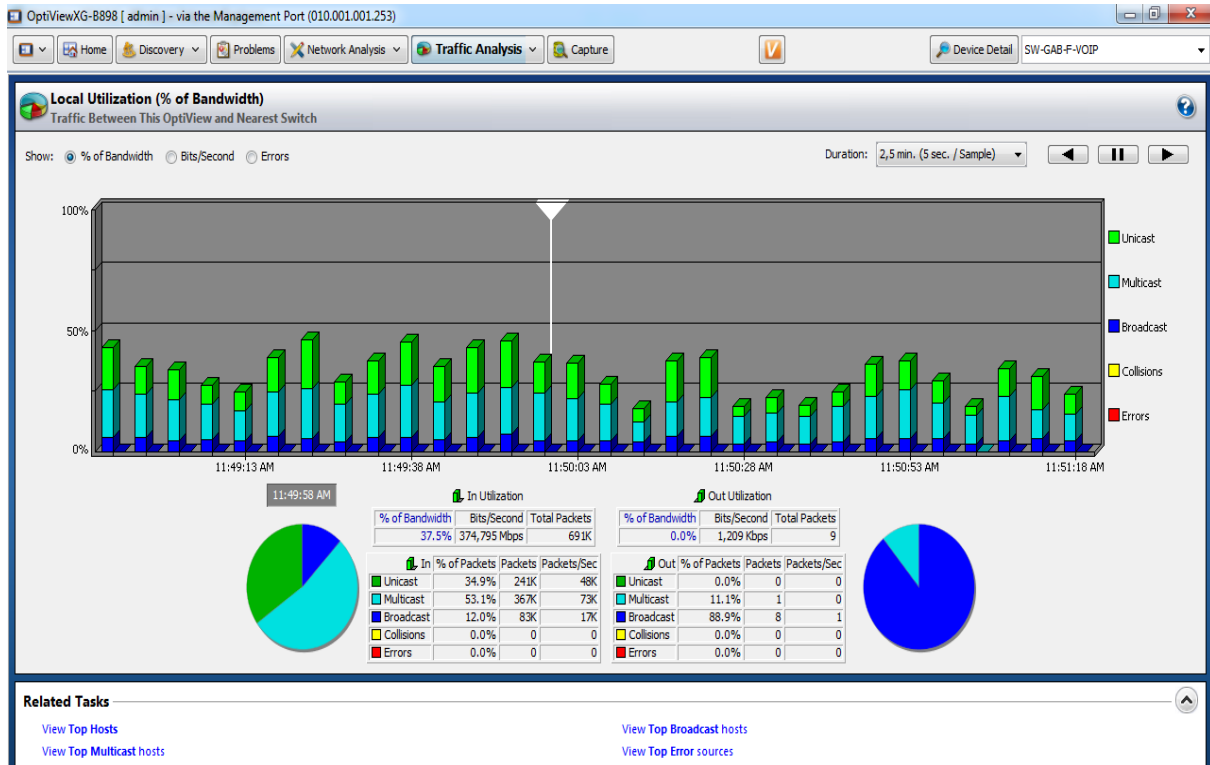


Figura 43. Generación de Inactividad Core Principal HNERM–16/05/2016 Unicast, Multicast, Broadcast, Ancho de Banda, Bps y Packets. Fuente: Oficina de Soporte Informático OptiView Fluke Networks-Ref. Tabla 8 Caída 5.

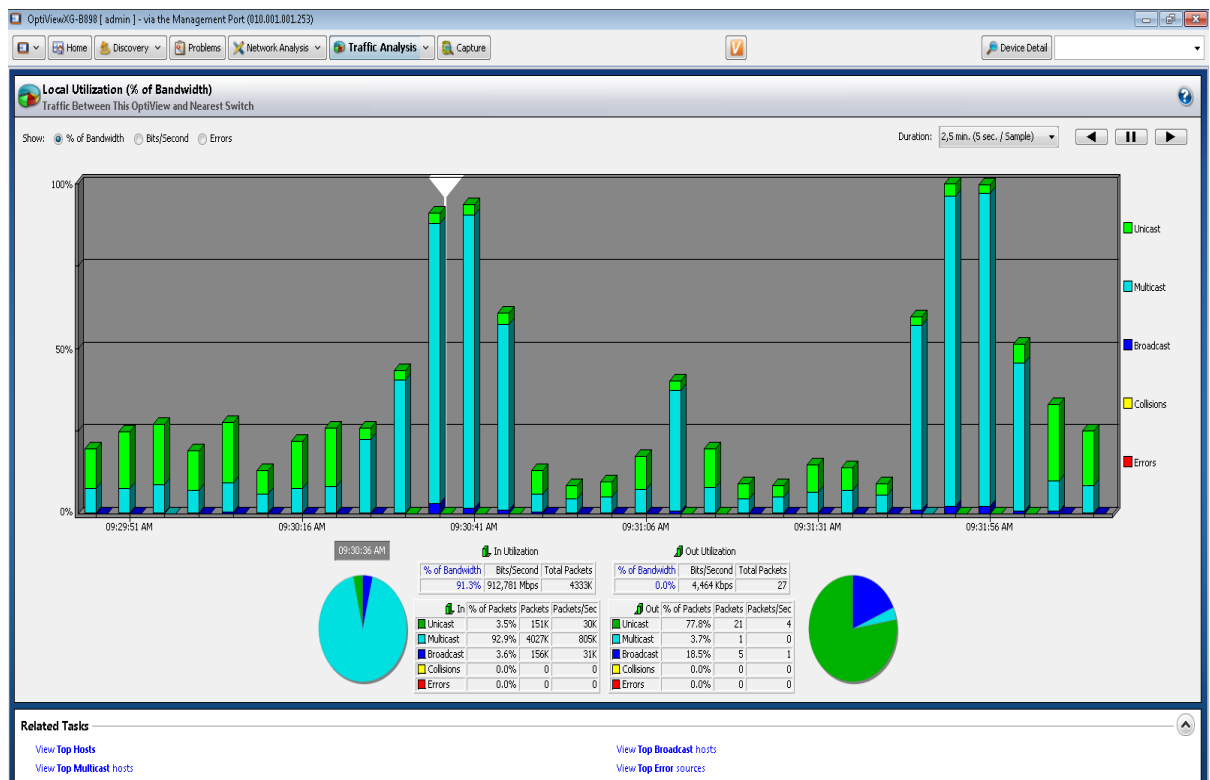


Figura 44. Generación de Inactividad Core Principal HNERM–19/05/2016 Unicast, Multicast, Broadcast, Ancho de Banda, Bps y Packets. Fuente: Oficina de Soporte Informático OptiView Fluke Networks-Ref. Tabla 8 Caída 6.



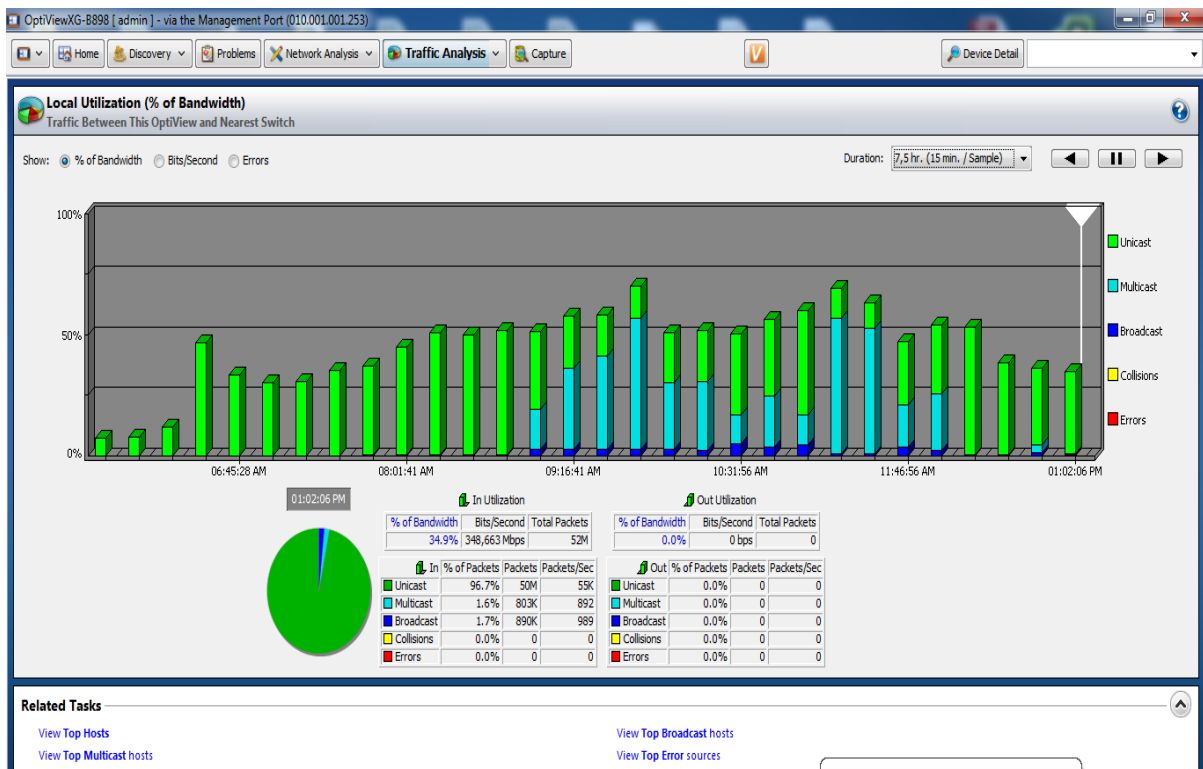


Figura 45. Generación de Inactividad Core Principal HNERM–14/07/2016 Unicast, Multicast, Broadcast, Ancho de Banda, Bps y Packets. Fuente: Oficina de Soporte Informático OptiView Fluke Networks-Ref. Tabla 8 Caída 7.

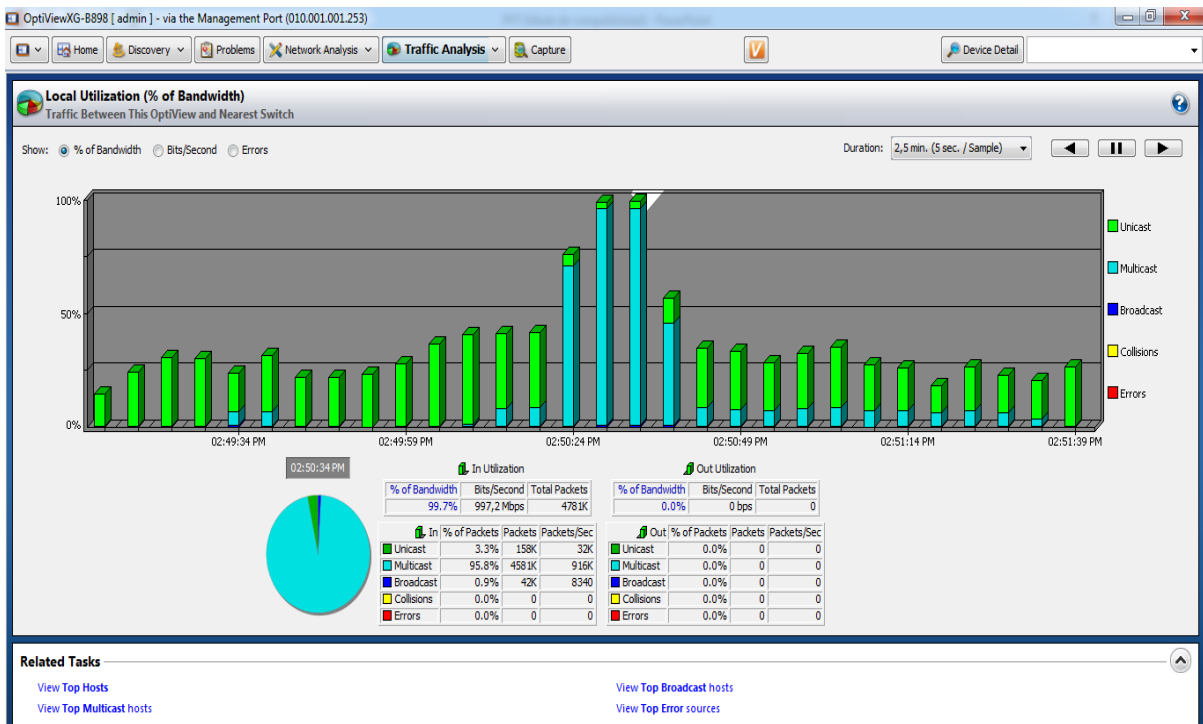


Figura 46. Generación de Inactividad Core Principal HNERM–04/08/2016 Unicast, Multicast, Broadcast, Ancho de Banda, Bps y Packets. Fuente: Oficina de Soporte Informático OptiView Fluke Networks-Ref. Tabla 8 Caída 8.



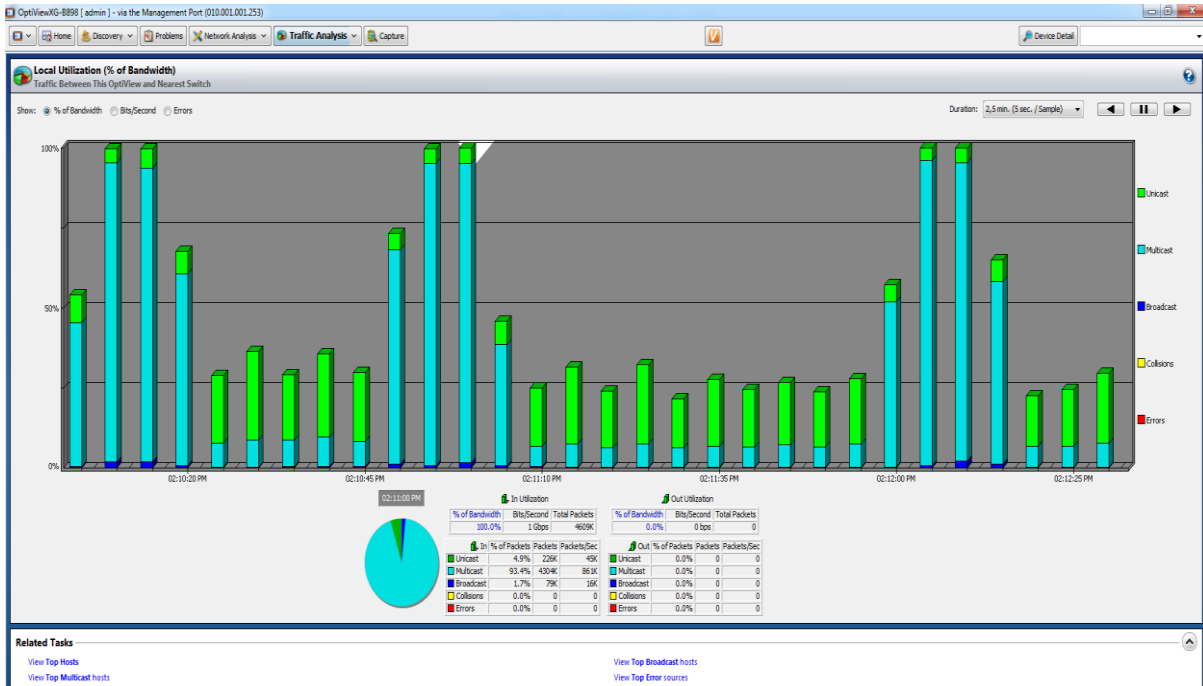


Figura 47. Generación de Inactividad Core Principal HNERM–16/08/2016 Unicast, Multicast, Broadcast, Ancho de Banda, Bps y Packets. Fuente: Oficina de Soporte Informático OptiView Fluke Networks-Ref. Tabla 8 Caída 9.

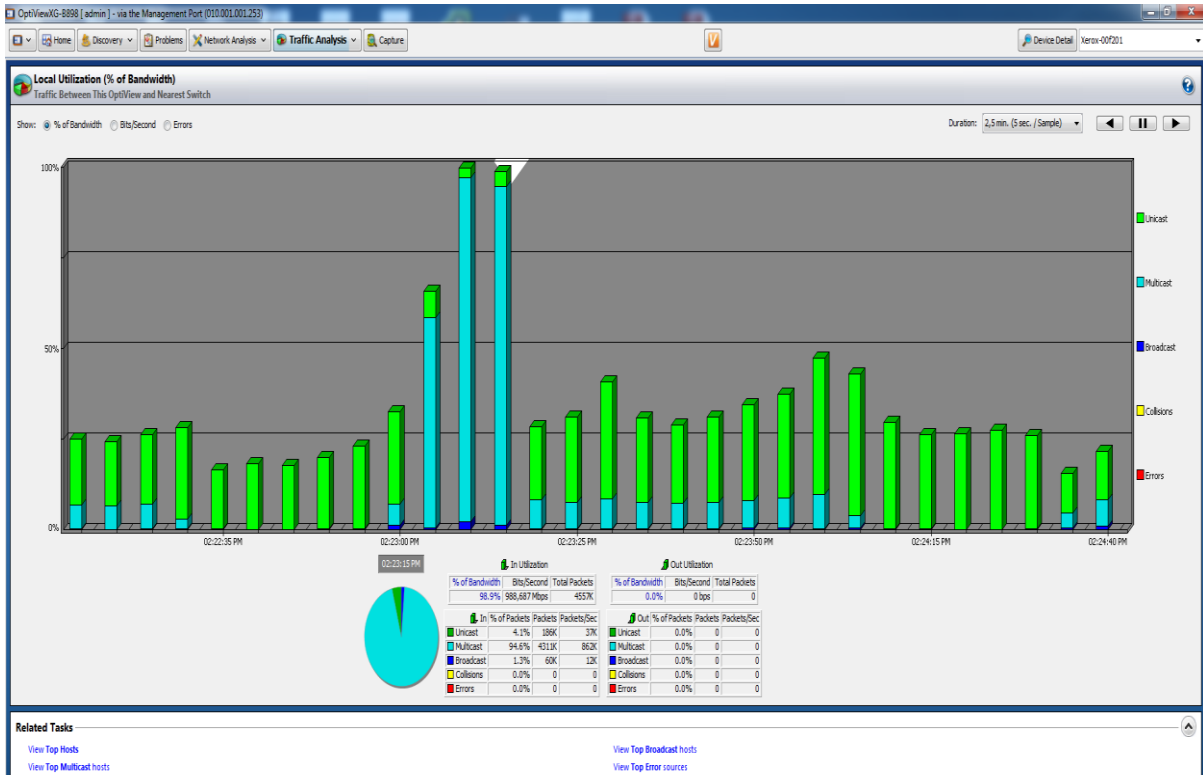


Figura 48. Generación de Inactividad Core Principal HNERM–17/08/2016 Unicast, Multicast, Broadcast, Ancho de Banda, Bps y Packets. Fuente: Oficina de Soporte Informático OptiView Fluke Networks-Ref. Tabla 8 Caída 10.



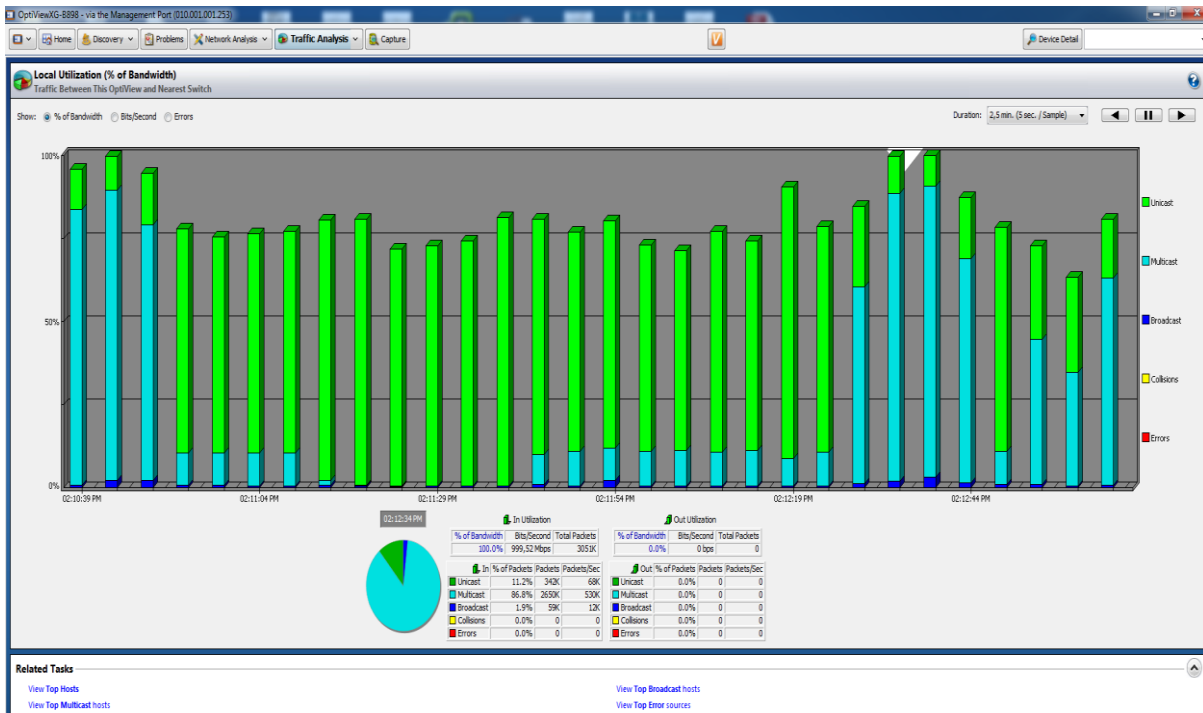


Figura 49. Generación de Inactividad Core Principal HNERM–22/08/2016 Unicast, Multicast, Broadcast, Ancho de Banda, Bps y Packets. Fuente: Oficina de Soporte Informático OptiView Fluke Networks-Ref. Tabla 8 Caída 11.

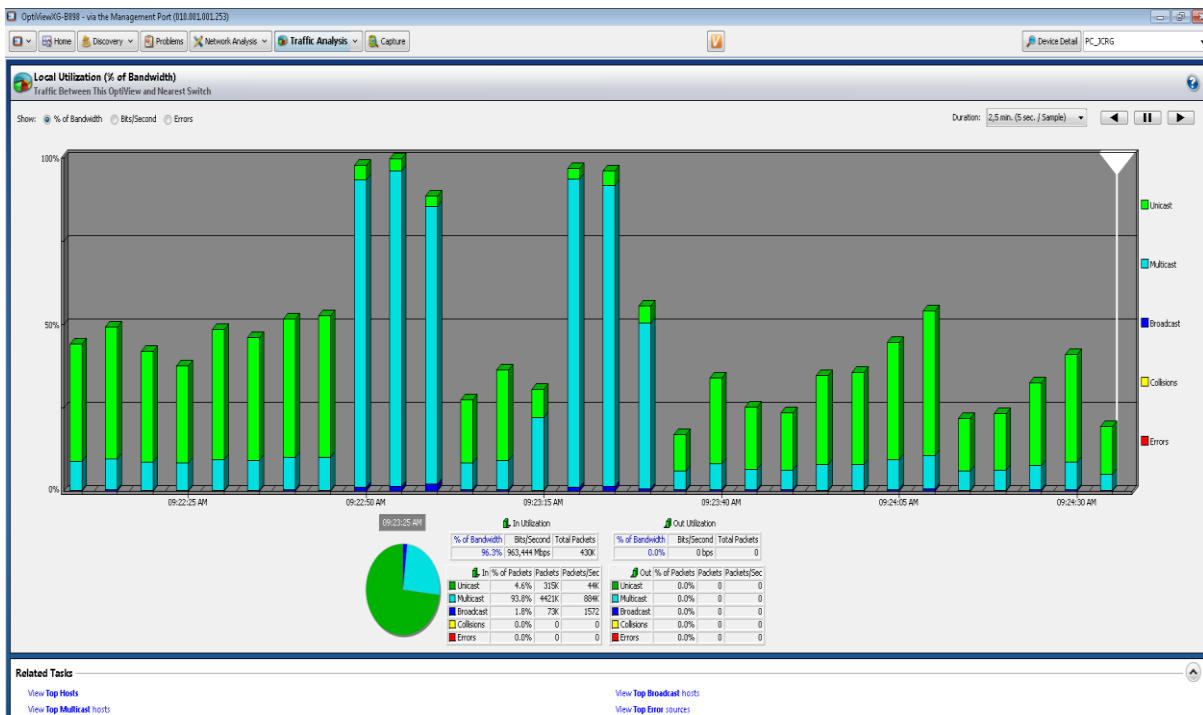


Figura 50. Generación de Inactividad Core Principal HNERM–01/09/2016 Unicast, Multicast, Broadcast, Ancho de Banda, Bps y Packets. Fuente: Oficina de Soporte Informático OptiView Fluke Networks-Ref. Tabla 8 Caída 13 y 14.



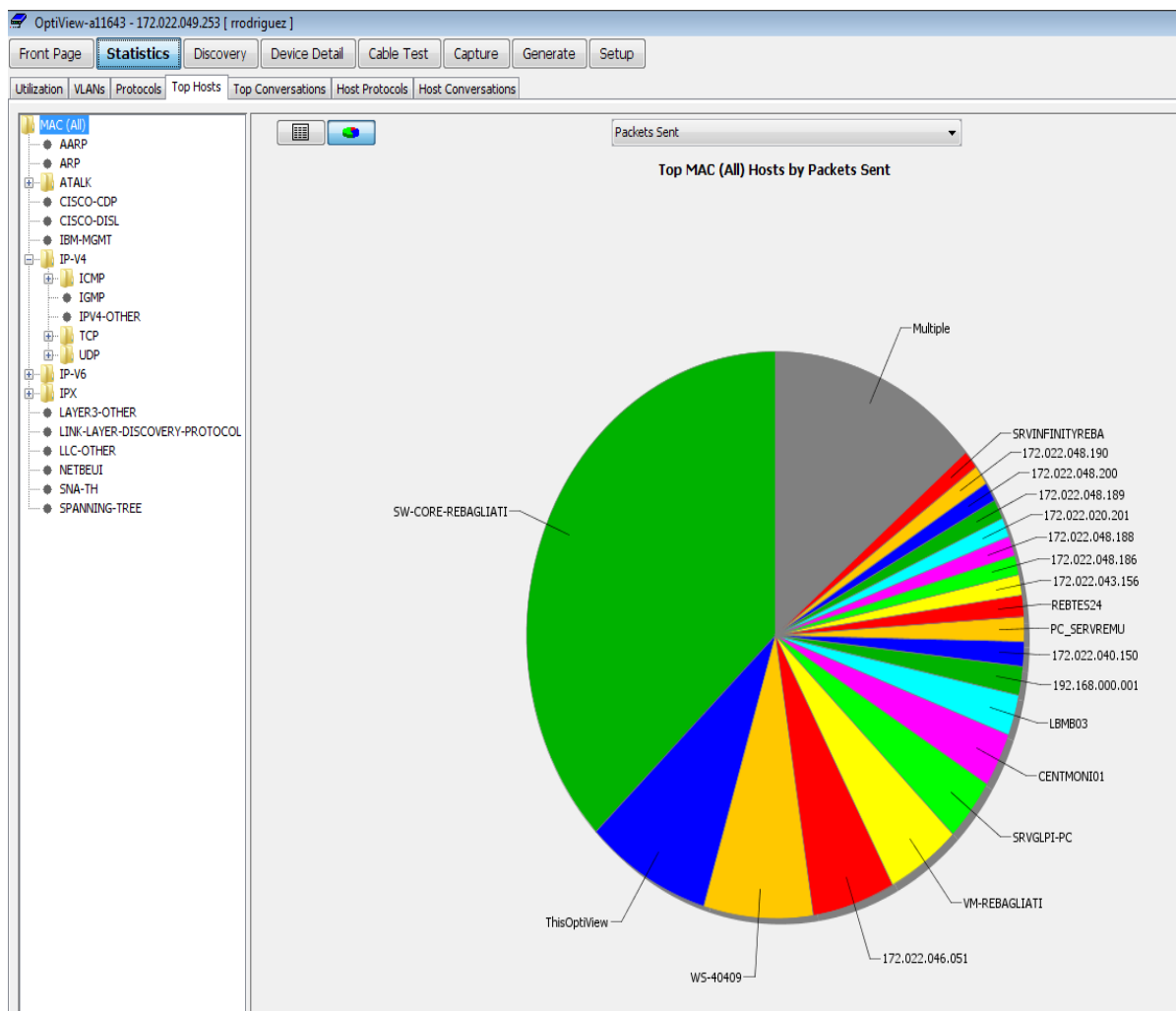


Figura 51. Consolidado de uso Hosts en Packets del Core Principal del HNERM-EsSALUD Año 2016 y 2017.
Fuente: Oficina de Soporte Informático OptiView Fluke Networks.



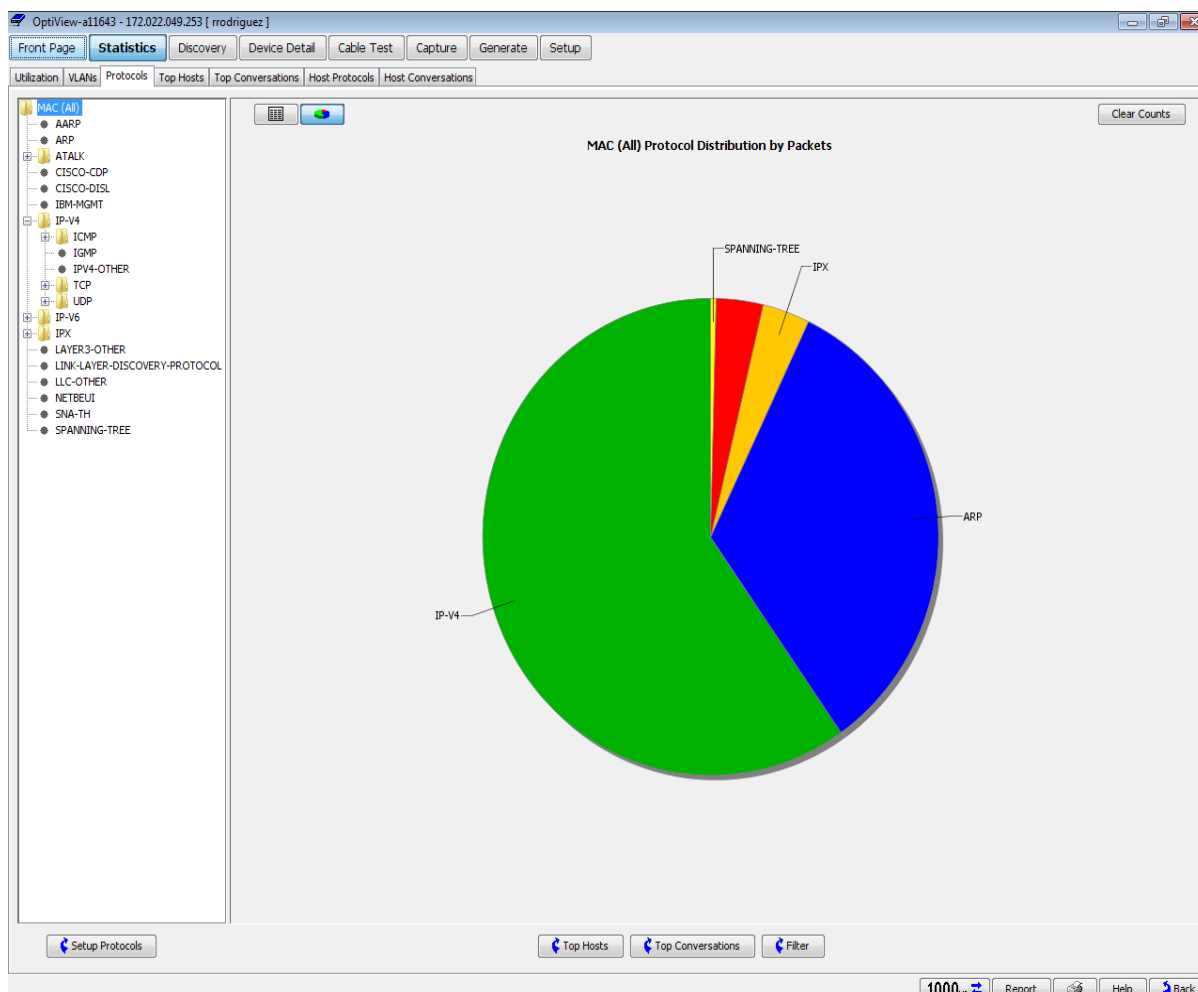


Figura 52. Estadística de Protocolos en Packets del Core Principal del HNERM EsSALUD. Fuente: Oficina de Soporte Informático OptiView Fluke Networks.

Nota: Se observa la estadística del consumo por distribución de los dispositivos de conmutación por Packets; Gráficos del N°33 al N°42 de los dispositivos existentes en el HNERM-EsSALUD, se ha obtenido dichos datos usando la herramienta del OptiView Fluke Networks que está conectado en el Core Principal OMNISWITCH 9800 de Alcatel.



CAPÍTULO V: DESARROLLO DE LA PROPUESTA DE LA INVESTIGACIÓN.

5.1.FASE I: PREPARACIÓN (LifeCycle Services)

5.1.1. Establecer los Requerimientos del Negocio en el HNERM–EsSALUD.

Requerimientos:

Que el hardware existente sea utilizado para la implementación.

Tratar de aprovechar al máximo los recursos con los que ya cuenta la institución de manera que el hardware existente sea utilizado para la investigación y con las mejoras que se le apliquen nos dé un mejor desempeño tanto para la Red LAN del HNERM-EsSALUD como para los usuarios.

Que la presencia de amenazas en la Red LAN esté controlada.

Disminuir y controlar todo tipo de ataque o amenaza que surja en los dispositivos de conmutación, la red LAN y en las computadoras, ya que al tener un intruso en estas conlleva a un mal funcionamiento de la red LAN y de los servicios del HNERM-EsSALUD.

Que la nueva implementación no genere costos de licencias de software.

Se utilizará los softwares con el que cuenta la institución, pero también se harán uso de herramientas de software libre (Open Free), así que de esa manera no habrá necesidad de costear licencias de software.

Que el hardware existente de los dispositivos de conmutación responda de manera satisfactoria en el desarrollo de las actividades de los usuarios en el HNERM-EsSALUD.

Los dispositivos de conmutación, equipos de red LAN y las computadoras que van a ser usados en la implementación cuentan con los recursos de hardware suficientes para el performance de la Red LAN y desarrollar los procesos cotidianos y las transacciones de los servicios asignados en el HNERM-EsSALUD.



Que existan políticas de seguridad informática para todos los usuarios conectados a la Red LAN del HNERM-EsSALUD.

Establecer políticas de seguridad informática en los servidores para tener un mejor control en los registros y acceso a internet, que no puedan tener acceso a información confidencial, que sólo visualicen su información personal la cual se va a encontrar en la carpeta /HOME habilitada y dentro de esta habrá una carpeta con su nombre de inicio de sesión. Asimismo, cabe precisar que cada inicio de sesión de la PC de SONDA cuenta con un Dominio propio administrado por la Sede Central de EsSALUD como medida de protección a los datos.

Que la Red LAN brinde disponibilidad y escalabilidad para el correcto funcionamiento de las estaciones de trabajo en el HNERM-EsSALUD.

Si bien la Red LAN en el HNERM-EsSALUD actual podría no presentar un funcionamiento idóneo por problemas diversos, la Red LAN que se va a trabajar tiene que estar siempre disponible en todo momento porque contamos con un servicio de 24x7 y tres turnos Mañana, tarde y noche por 365 días al año. De manera que los servidores, los dispositivos de conmutación y los equipos de cómputo respondan de manera adecuada sin entrar en un caos con el tráfico de red y se pueda ofrecer una buena calidad de servicio.

Además, que sea una Red LAN Escalable es decir que si se le implementaran más terminales por ejemplo la Red LAN siga manteniéndose en buen estado.

Que la implementación permita una respuesta inmediata ante cualquier evento.

Los problemas en la Red LAN del HNERM-EsSALUD pueden surgir en cualquier momento para ello debemos estar preparados con planes de contingencias para resolver de manera inmediata un problema, la idea es tratar de que un problema no se materialice.

5.1.2. Diseño de la estructura de la Red del HNERM–EsSALUD.

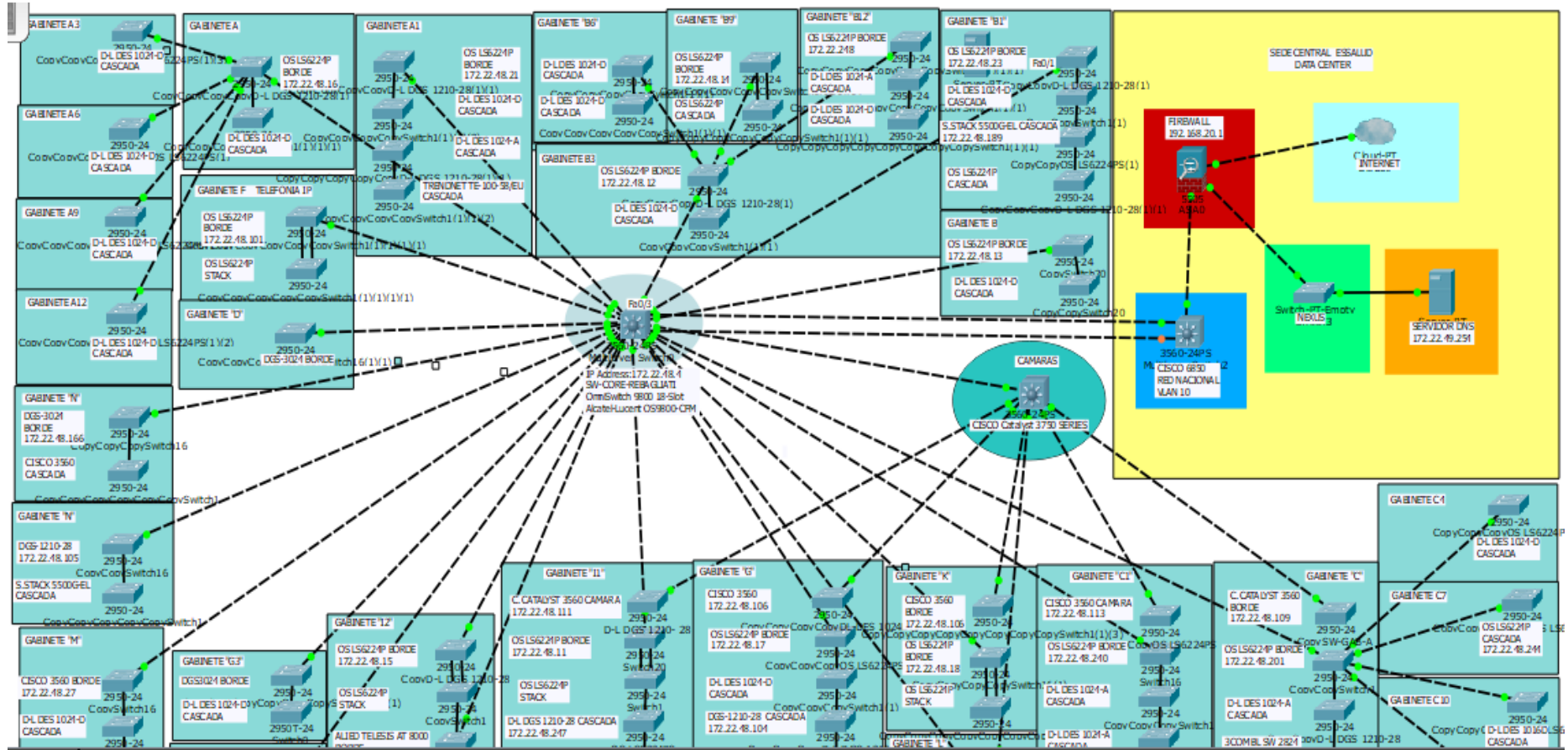


Figura 53. Diseño Actual de Estructuración de la Red Informática del HNERM EsSALUD. Fuente: Oficina de Soporte Informático del HNERM EsSALUD (2016).



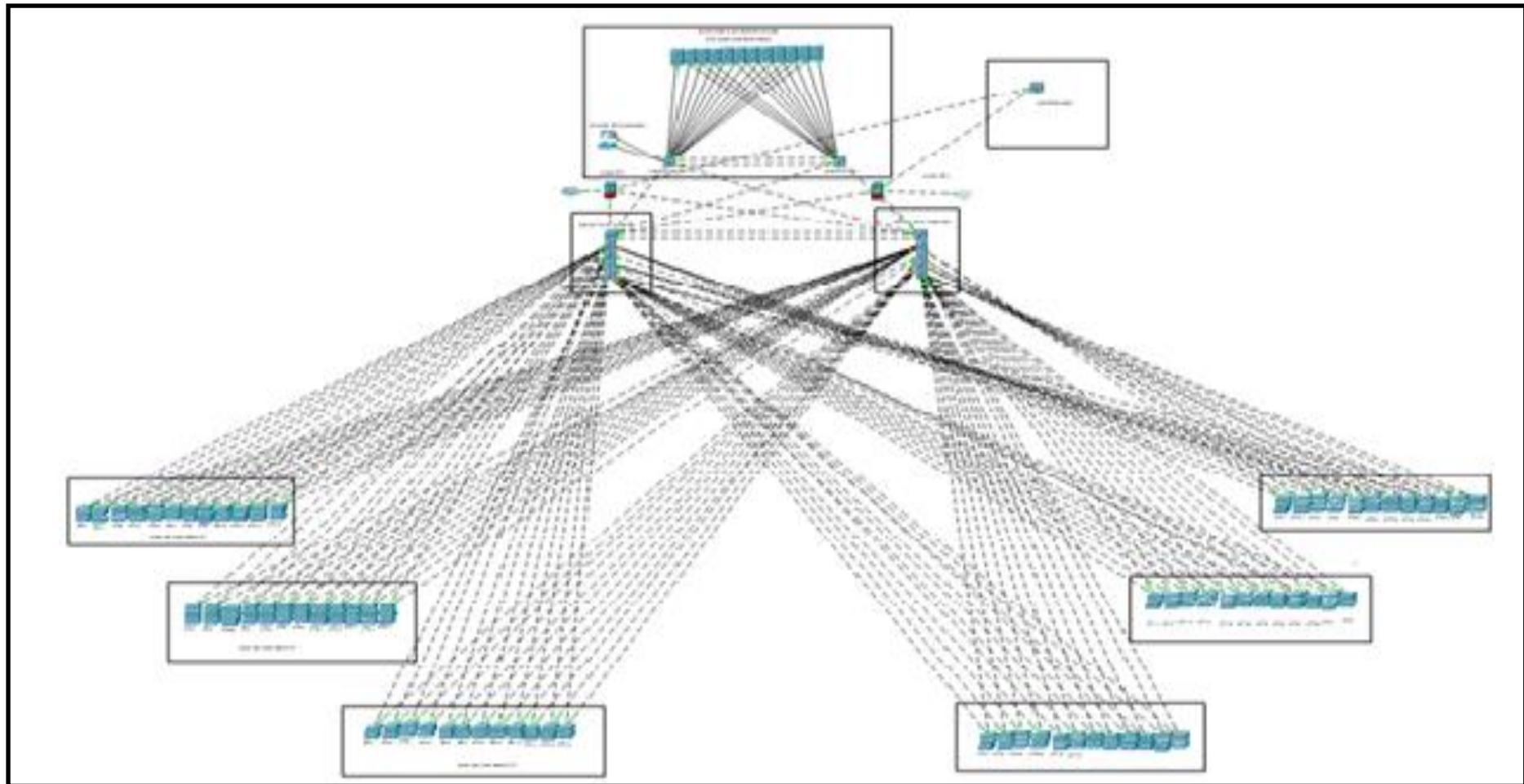


Figura 54. Diseño Propuesto de la Topología Estrella Jerárquica del HNERM EsSALUD. Fuente: Oficina De Soporte Informático (2017).

Nota: La Arquitectura De Red Jerárquica De Alto Nivel Que Se Está Proponiendo Brindará Alta Disponibilidad, Implementación De Seguridad A Través De Firewall, Redundancia Con Los Servidores Y Virtualización De Los Switchs Core Nexus.



5.1.3. Visión Tecnológica

Conmutador Cisco Nexus 7000 Switches

Descripción del producto Cisco Nexus:

La tecnología Nexus 7000 consta del siguiente hardware:

- a. Supervisor Engines
- b. I/O modules
- c. Fuentes de poder
- d. Fabric modules
- e. Fan trays.

En la parte de I/O modules tenemos los siguientes tipos de tarjetas:

- a. Tarjetas M
Tarjetas M1, M2
- b. Tarjetas F
Tarjetas F1, F2, F3

En historia, las tarjetas M fueron inicialmente fabricadas para soportar y realizar operaciones de capa 2, capa 3 y capa 4 con capacidades para manejar una gran tabla de ruteo.

Las diferencias entre M1 y M2, son el soporte de ancho de banda:

M1-XL (2008): Tarjetas con puertos GigabitEthernet (GE) de 1Gbps y 10Gbps y Throughput interno de 80Gbps/Slot

M2-XL (2012): Tarjetas con puertos GE de 10Gbps/40Gbps/100Gbps y Throughput interno de 240Gbps/slot.

En cuanto a las tarjetas F, en sus inicios las F1 (2010) solo realizaban operaciones de capa 2.



Para lograr una comunicación en capa 3 (ruteo), requerían de la tarjeta M.

Posteriormente viene la F2 (2011) que mejoró un poco dado que realizaban funcionalidades limitadas de capa 3. Sus características son de un alto performance en hardware con bajas latencias internas.

Un punto importante a considerar es que no puedes hacer un mix de tarjetas F2 con tarjetas M1/M2 y F1, ya que las F2 requieren tener dedicado un solo VDC (Contexto de dispositivo Virtual).

Todo lo demás puede ser mezclado (F1 con M1/M2)

Finalmente, durante el desarrollo de mejores tecnologías en el Nexus, se fabricó la tarjeta F3 (2013), la cual acerca en mucho la brecha entre las tarjetas M y las F (las F3 pueden realizar más funcionalidades de Capa 3.

F1.- Puertos GE de 10Gbps y throughput interno de 230Gbps/slot.

F2/F2E.- Puertos GE de 10Gbps y throughput interno de 480Gbps/slot.

F3.- Puertos GE de 10/40/100Gbps y throughput interno de 1.2Tbps/slot.

Las tarjetas Fabric corresponden a acelerar el forwarding interno del chasis.

Dependiendo el tipo de equipo (7004, 7010, 7700).

El objetivo de estas tarjetas es proveer un alto performance en la conmutación de paquetes entre los puertos de entrada y salida de los módulos I/O.

Existen 2 modelos:

FAB1.-Módulos Fabric con ancho de banda interno (throughput) de 46Gbps.

FAB2.- Módulos Fabric con ancho de banda interno (throughput) de 110Gbps.

Esta sección del Nexus es adaptable a la necesidad del cliente.

En otras palabras, puede crecer en throughput al ir incrementando la cantidad de tarjetas FAB.

Para el Nexus 7010, se tienen 5 ranuras dedicadas para tarjetas FAB. lo cual quiere decir que puedes crecer hasta 230Gbps si tu arreglo es de FAB1, o hasta 550Gbps si es FAB2.

Pueden coexistir ambas FAB en un chasis, sin embargo, FAB2 bajara su performance para adaptarse a las FAB1 por lo cual no es recomendable.

Finalmente, están las tarjetas supervisoras. Corresponden al CPU central del equipo.

Su finalidad es el plano de control y administración del sistema interno del chasis Se tienen diferentes modelos según la capacidad de performance:

SUP1.- puedes crear hasta 4VDC en el mismo equipo

SUP2.- procesador XEON, 2.13Ghz 2 Quad core, 64bit kernel, memoria hasta 32GB DDR3. Puedes crear hasta 4 + 1 VDC (1 VDC exclusivo para management).

SUP2E.- procesador XEON, 2.13Ghz Quad core, 64bit kernel, memoria hasta 12GB DDR3.

Puedes crear hasta 8+1 VDC (1 VDC exclusivo para management).

Nota: para crecer en performance (Ej: pasar de F1 a F2 o F3, de M1 a M2, de SUP1 a SUP2/SUP2E, De FAB1 a FAB2) es necesario validar el sistema operativo nexus, las licencias correspondientes y la documentación que explique paso a paso dicha migración.

En cuanto a lista de funcionalidades según el tipo de tarjeta I/O, te comparto una imagen de cómo esta distribuidas. Los interruptores de la serie 7000 son la base de la solución Cisco Unified Fabric.

Diseñado para satisfacer Los centros de datos de misión crítica, estos conmutadores ofrecen una disponibilidad excepcional, Escalabilidad y el comprobado y completo sistema de características de conmutación de centro de datos del software Cisco NX-OS.

Los Switches Cisco Nexus 7700 son la última extensión de los conmutadores modulares de la serie Cisco Nexus 7000.

Con más de 83 terabits por segundo (Tbps) de capacidad de conmutación total, el Cisco Nexus 7700 Switches ofrece los puertos Ethernet de 10, 40 y 100 puertos Gigabit de mayor capacidad en la industria, con hasta 768 puertos nativos de 10 Gbps, 384 puertos de 40 Gbps o 192 puertos de 100 Gbps.

Estándares de compatibilidad CISPR 22 Class A, BSMI CNS 13438 Class A, CISPR 24, EN 61000-3-2, VCCI Class A ITE, EN 61000-3-3, EN55024, EN55022 Class A, EN50082-1, EN 61000-6-1, AS/NZS 60950-1, ICES-003 Class A, RoHS, FCC CFR47 Part. 15, EN300-386, UL 60950-1, IEC 60950-1, EN 60950-1, CSA C22.2 No. 60950-1 MTBF (tiempo medio entre errores) 90994 sec.

Esta alta capacidad del sistema está diseñada para cumplir con los requisitos de escalabilidad De los entornos de nube más grandes.

Los conmutadores Cisco Nexus 7700 (Figura 1) tienen una consistencia operativa y de características con el Cisco Nexus existente 7000 Interruptores serie, utilizando la arquitectura del sistema común, el mismo circuito integrado específico de la aplicación (ASIC).

Y las mismas versiones de software probadas de Cisco NX-OS.



Descripción del fabricante sobre el producto



Figura 55. Switches Nexus de Cisco serie 7000 Fuente: Cisco (2017).

Cree una red de próxima generación

Cree los cimientos de la red que necesita para su centro de datos de Unified Fabric de próxima generación y núcleo de campus de alto rendimiento.

Los switches Nexus de Cisco serie 7000 ofrecen un completo conjunto de características NX-OS, con Ethernet de 10, 40 y 100 gigabits de alta densidad para el centro de datos y el núcleo de campus.

Datos Adicionales del Nexus de Cisco 7000

Más de 17 terabits de capacidad

El módulo de E/S de la serie F2 de segunda generación, los módulos Fabric 2 y el switch de formato pequeño Nexus de Cisco 7000 de 9 ranuras son las más recientes incorporaciones a los switches Nexus de Cisco serie 7000.

Más información del Nexus Cisco 7000

Una sola plataforma de extremo a extremo

Para los centros de datos, Nexus de Cisco serie 7000 ofrece una solución de extremo a extremo en una sola plataforma para el núcleo de centro de datos, agregación, y conectividad de servidor de fin de hilera y parte superior del rack de alta densidad.

Para implementaciones de núcleo de campus, proporciona una solución escalable, con gran flexibilidad y de alto rendimiento.

La plataforma Nexus de Cisco serie 7000 se ejecuta en el software Cisco NX-OS. Se diseñó específicamente para las implementaciones más críticas en el centro de datos y el campus.

Características y capacidades:

La serie 7000 de Nexus de Cisco se diseñó con tres principios en mente:

- a. Infraestructura Escalable: las capacidades de virtualización, alimentación y enfriamiento eficientes, alta densidad y alto rendimiento permiten el crecimiento de la infraestructura del centro de datos.
- b. Continuidad Operativa: el diseño de Nexus de Cisco integra hardware, características del software NX-OS y gestión para permitir entornos con cero tiempos de inactividad.



c. Flexibilidad de Transporte: Usted puede adoptar de manera progresiva y económica las más recientes innovaciones y tecnologías de red, tales como:

c.1. Virtualización de transporte superpuesto de Cisco (Overlay Transport Virtualization, OTV).

c.2. Cisco FabricPath

c.3. Fibre Channel over Ethernet (FCoE)

c.4. Cisco Locator/ID Separation Protocol (LISP)

c.5. Cisco IOS Multiprotocol Label Switching (MPLS)

Innovaciones recientes



Figura 56. Módulo Fabric 2 Cisco Nexus 7000. Fuente: Cisco (2017).

Módulo Fabric 2 Cisco Nexus 7000

El módulo Fabric 2 de segunda generación proporciona el doble del rendimiento que las generaciones anteriores.

- a. Disponible para los chasis 7009, 7010 y 7018 de Cisco Nexus
- b. Proporciona una capacidad de switching de 550 Gbps por ranura en todos los chasis Nexus de Cisco serie 7000
- c. Ofrece una capacidad de switching de hasta 17,6 Tbps en el Nexus de Cisco 7018

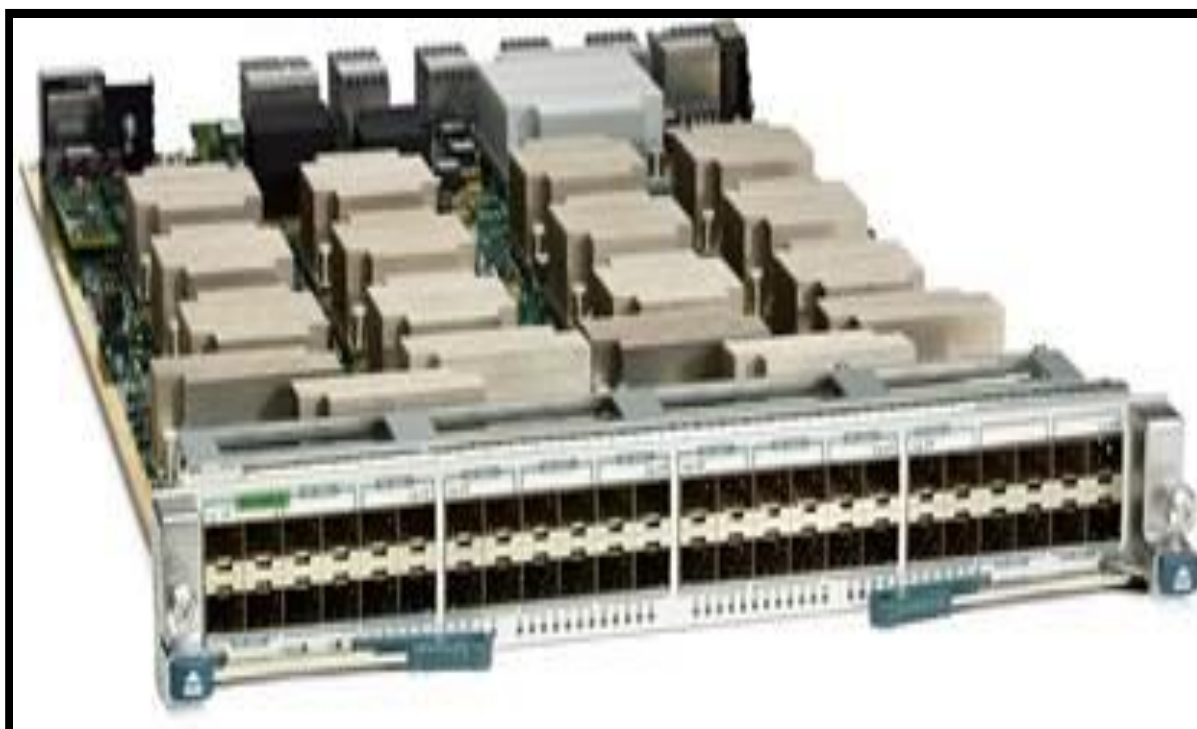


Figura 57. Módulo de E/S de 1/10 GE con 48 puertos Nexus de Cisco serie 7000 F2. Fuente: Cisco (2017).

Módulo de E/S de 1/10 GE con 48 puertos Nexus de Cisco serie 7000 F2

La segunda generación del módulo F2 ofrece funcionalidad de capa 2 y 3 de alto rendimiento para el centro de datos.

- a. Velocidad de línea en los 48 puertos con una capacidad de procesamiento de 720 Mpps y 480 Gbps.

- b. Funcionalidad de reenvío completa de capa 2 y 3.
- c. Compatibilidad con Cisco FabricPath para redes de capa 2 sumamente escalables y flexibles.
- d. Compatibilidad con Cisco Nexus 2000 para implementaciones de parte superior del rack (top-of-rack, ToR) con acceso de alta densidad.
- e. Compatibilidad con FCoE para convergencia de redes LAN y SAN sobre una sola red Ethernet.

Cisco Nexus 7009

El Cisco Nexus 7009 de formato pequeño es la más reciente incorporación a la emblemática serie 7000 de Cisco Nexus.

Este switch de alto rendimiento con 9 ranuras está diseñado para reducir el coste total de oportunidad en entornos de espacio limitado tanto de empresas como de proveedores de servicios.

- a. Uso optimizado del espacio de rack para redes de núcleo de campus y centros de datos de espacio limitado (14RU)
- b. Uniformidad operativa mediante la misma versión de NX-OS en todos los switches Nexus de Cisco serie 7000
- c. Protección de la inversión gracias a su compatibilidad con todos los módulos de E/S Nexus de Cisco serie 7000, el módulo supervisor y las fuentes de alimentación.



Figura 58. Conmutador Cisco Nexus 7000. Fuente: Cisco (2017).

Nota: Conmutador Cisco Nexus 7000 Switches Propuesto.

Tabla 9
Product Specifications

Item	Specification			
	Cisco Nexus 7000 4-Slot Switch	Cisco Nexus 7000 9-Slot Switch	Cisco Nexus 7000 10-Slot Switch	Cisco Nexus 7000 18-Slot Switch
Product compatibility	Supports all Cisco Nexus 7000 Series Supervisor and I/O modules except the following: N7K-SUP1 N7K-M132XP-12 N7K-M148GS-11 N7K-M148GT-11 N7K-F132XP-15 Does not use fabric modules	Supports all Cisco Nexus 7000 Series Supervisor and I/O modules Supports Fabric2 modules Does not support Fabric1 modules	Supports all Cisco Nexus 7000 Series Supervisor and I/O modules Supports Fabric1 and Fabric2 modules	Supports all Cisco Nexus 7000 Series Supervisor and I/O modules Supports Fabric1 and Fabric2 modules
Max local switching capacity	600 Gbps	600 Gbps	600 Gbps	600 Gbps
Max inter-slot switching capacity	440 Gbps	550 Gbps	550 Gbps	550 Gbps
Software compatibility	Cisco NX-OS Software Release 6.1(2) or later	Cisco NX-OS Software Release 5.2 or later	Cisco NX-OS Software Release 4.0 or later	Cisco NX-OS Software Release 4.1 or later
Options	Lockable front module door	Lockable front module door	<ul style="list-style-type: none"> • Air filter • Lockable front module doors 	Lockable front module door
Performance	1.44 billion packets per second (bps) (IPv4 unicast) in combination with supervisor module and built-in fabric	5.04 bpps (IPv4 unicast) in combination with supervisor and fabric modules	5.76 bpps (IPv4 unicast) in combination with supervisor and fabric modules	11.5 bpps (IPv4 unicast) in combination with supervisor and fabric modules
	Online insertion and removal (OIR) of all redundant components: supervisor modules,	OIR of all redundant components: supervisor and fabric modules,	OIR of all redundant components: Supervisor and fabric modules,	OIR of all redundant components: supervisor and fabric modules, power supplies, and fan trays



Item	Specification			
	power supplies, and fan trays	power supplies, and fan trays	power supplies, and fan trays	
MIBs	Supports Simple Network Management Protocol (SNMP) Versions 3, 2c, and 1 (see Cisco NX-OS Software release notes for details about specific MIB support)	Supports SNMPv3, v2c, and v1 (see Cisco NX-OS Software release notes for details about specific MIB support)	Supports SNMPv3, v2c, and v1 (see Cisco NX-OS Software release notes for details about specific MIB support)	Supports SNMPv3, v2c, and v1 (see Cisco NX-OS Software release notes for details about specific MIB support)
Network management	Cisco Data Center Network Manager (DCNM) 6.1(2) or later	Cisco DCNM 5.2 or later	Cisco DCNM 4.0 or later	Cisco DCNM 4.1 or later
Programming interfaces	<ul style="list-style-type: none"> • XML • Scriptable command-line interface (CLI) • Cisco DCNM 6.1(2) web services 	<ul style="list-style-type: none"> • XML • Scriptable CLI • Cisco DCNM 5.2 web services 	<ul style="list-style-type: none"> • XML • Scriptable CLI • Cisco DCNM 4.0 web services 	<ul style="list-style-type: none"> • XML • Scriptable CLI • Cisco DCNM 4.1 web services
	<ul style="list-style-type: none"> • Usable rack space: 7RU • 4-slot chassis: 2 dedicated supervisor modules and 2 I/O modules • 4 power supply slots • Dimensions (H x W x D): 12.2 x 17.3 x 24 in. (30.9 x 43.9 x 61 cm) • Chassis depth including cable management and chassis doors is 29.6 in. (75.2 cm) • Unit is rack mountable in a standard 19-inch (482.6-mm) Electronic Industries Alliance (EIA) rack • Weight <ul style="list-style-type: none"> - Chassis only: 45 lb. (20 kg) 	<ul style="list-style-type: none"> • Usable rack space: 14RU • 9-slot chassis: 2 dedicated supervisor modules and 7 I/O modules • 5 fabric module slots • 2 power supply slots • Dimensions (H x W x D): 24.5 x 17.3 x 24 in. (62.2 x 43.9 x 61 cm) • Chassis depth including cable management and chassis doors is 29 in. (73.7 cm) • Unit is rack mountable in a standard 19-inch (482.6-mm) EIA rack • Weight <ul style="list-style-type: none"> - Chassis only: 100 lb. (45 kg) 	<ul style="list-style-type: none"> • Usable rack space: 21RU • 10-slot chassis: 2 dedicated supervisor modules and 8 I/O modules • 5 fabric module slots • 3 power supply slots • Dimensions (H x W x D): 36.5 x 17.3 x 33.1 in. (92.7 x 43.9 x 84.1 cm) • Chassis depth including cable management and chassis doors is 38 in. (96.5 cm) • Unit is rack mountable in a standard 19-inch (482.6-mm) EIA 	<ul style="list-style-type: none"> • Usable rack space: 25RU • 18-slot chassis: 2 dedicated supervisor modules and 16 I/O modules • 5 fabric module slots • 4 power supply slots • Dimensions (H x W x D): 43.5 x 17.3 x 33.1 in. (110.5 x 43.9 x 84.1 cm) • Chassis depth including cable management and chassis doors is 38 in. (96.5 cm) • Unit is rack mountable in a standard 19-inch (482.6-mm) EIA rack • Weight <ul style="list-style-type: none"> - Chassis only: 187 lb. (85 kg) - Fabric Module: 7.5 lb (3.4 kg) - Fan Tray: 25.8 lb (11.7 kg) • Supports 6-kW and



Item	Specification			
	<ul style="list-style-type: none"> • Supports 3-kW AC and DC and 3.5-kW HV AC/DC power supplies • Supports up to 6 chassis stacked in a 42RU rack 	<ul style="list-style-type: none"> • Fan Tray: 25 lb (11.3 kg) • Supports 6-kW and 7.5-kW AC and DC power supplies • Supports up to 3 chassis stacked in a 42RU rack 	<ul style="list-style-type: none"> • Chassis only: 200 lb. (90 kg) • Fabric Module: 4 lb (1.8 kg) • System Fan Tray: 20 lb (9.1 kg) • Fabric Fan Tray: 5 lb (2.3 kg) • Supports 6-kW and 7.5-kW AC and DC power supplies 	
Environmental specifications	<ul style="list-style-type: none"> • Airflow direction: Side to rear • Operating temperature: 32 to 104°F (0 to 40°C) • Operational relative humidity: 5 to 90%, noncondensing • Operating altitude: -500 to 13,123 ft. (agency certified 0 to 6500 ft.) • Seismic: Zone 4 per GR63 • Floor loading: 42 lb. per sq. ft. • Operational vibration • GR63, Section 5.4.2 • ETS 300 019-1-3, Class 3.1, Section 5.5 • Storage altitude: -1000 to 30,000 ft. • Storage temperature: -40 to 158°F (-40 to 70°C) • Storage relative humidity: 5 to 95%, noncondensing • Heat dissipation: Maximum 3500W per chassis (actual dissipation will be lower, depending on the chassis configuration) 	<ul style="list-style-type: none"> • Airflow direction: Side to side • Operating temperature: 32 to 104°F (0 to 40°C) • Operational relative humidity: 5 to 90%, noncondensing • Operating altitude: -500 to 13,123 ft. (agency certified 0 to 6500 ft.) • Seismic: Zone 4 per GR63 • Floor loading: 104 lb. per sq. ft. • Operational vibration • GR63, Section 5.4.2 • ETS 300 019-1-3, Class 3.1, Section 5.5 • Storage altitude: -1000 to 30,000 ft. • Storage temperature: -40 to 158°F (-40 to 70°C) • Storage relative humidity: 5 to 95%, noncondensing • Heat dissipation: Maximum 7500W per chassis (actual dissipation will be lower, depending on the chassis configuration) 	<ul style="list-style-type: none"> • Airflow direction: Bottom front of chassis to top back • Operating temperature: 32 to 104°F (0 to 40°C) • Operational relative humidity: 5 to 90%, noncondensing • Operating altitude: -500 to 13,123 ft. (agency certified 0 to 6500 ft.) • Seismic: Zone 4 per GR63 • Floor loading: 190 lb. per sq. ft. • Operational vibration • GR63, Section 5.4.2 • ETS 300 019-1-3, Class 3.1, Section 5.5 • Storage altitude: 1000 to 30,000 ft. • Storage temperature: -40 to 158°F (-40 to 70°C) • Storage relative humidity: 5 to 95%, noncondensing 	<ul style="list-style-type: none"> • Airflow direction: Side to side • Operating temperature: 32 to 104°F (0 to 40°C) • Operational relative humidity: 5 to 90%, noncondensing • Operating altitude: -500 to 13,123 ft. (agency certified 0 to 6500 ft.) • Seismic: Zone 4 per GR63 • Floor loading: 190 lb. per sq. ft. • Operational vibration • GR63, Section 5.4.2 • ETS 300 019-1-3, Class 3.1, Section 5.5 • Storage altitude: 1000 to 30,000 ft. • Storage temperature: -40 to 158°F (-40 to 70°C) • Storage relative humidity: 5 to 95%, noncondensing • Heat dissipation: Maximum 18,000W per chassis (actual dissipation will be lower, depending on the chassis configuration)



Item	Specification
	<ul style="list-style-type: none"> • Heat dissipation: Maximum 12,000W per chassis (actual dissipation will be lower, depending on the chassis configuration)
Regulatory compliance	<ul style="list-style-type: none"> • EMC compliance • FCC Part 15 (CFR 47) (USA) Class A • ICES-003 (Canada) Class A • EN55022 (Europe) Class A • CISPR22 (International) Class A • AS/NZS CISPR22 (Australia and New Zealand) Class A • VCCI (Japan) Class A • KN22 (Korea) Class A • CNS13438 (Taiwan) Class A • CISPR24 • EN55024 • EN50082-1 • EN61000-3-2 • EN61000-3-3 • EN61000-6-1 • EN300 386
Environmental standards	<ul style="list-style-type: none"> • NEBS criteria levels • SR-3580 NEBS Level 3 (GR-63-CORE and GR-1089-CORE) • Verizon NEBS compliance VZ.TPR.9203 – Data Center • CenturyLink NEBS requirements • ATT NEBS requirements • ATT TP76200 Carrier Grade Level 1 • ETSI • ETSI 300 019-1-1, Class 1.2 Storage • ETSI 300 019-1-2, Class 2.3 Transportation • ETSI 300 019-1-3, Class 3.2 Stationary Use • Reduction of Hazardous Substances (ROHS) 5
Safety	<ul style="list-style-type: none"> • UL/CSA/IEC/EN 60950-1 • AS/NZS 60950
Warranty	Cisco Nexus 7000 Series Switches come with the standard Cisco 1-year limited hardware warranty

Fuente: Cisco (2017).

Software Requirements

All Cisco Nexus 7000 Series chassis are supported by Cisco NX-OS Software.

- The 4-slot chassis requires Cisco NX-OS Software Release 6.1(2) or later.
- The 9-slot chassis requires Cisco NX-OS Software Release 5.2 or later.
- The 10-slot chassis requires Cisco NX-OS Software Release 4.0 or later.
- The 18-slot chassis requires Cisco NX-OS Software Release 4.1 or later.



5.1.4. Planificación de una estrategia tecnológica

La estrategia tecnológica que planeamos, se basa obviamente mirando el principal problema identificado como:

La falta de un sistema de administración y seguridad en la red LAN de la institución. La complejidad de la red es ya una dificultad para la detección y corrección de los múltiples y variados problemas que van apareciendo. En toda esta variedad, han ido en aumento las acciones poco respetuosas de la privacidad y de la propiedad de recursos y sistemas.

Por otra parte, la falta de medidas de seguridad en la red es un problema que podría estar en crecimiento.

Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios.

Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización.

Además de unos planes de Continuidad de las Operaciones y Recuperación de Desastres serán muy necesarios para no materializar riesgos que puedan surgir.

5.1.4.1. Monitoreo de la red

Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.

Hacer uso eficiente de la red y utilizar mejor los recursos, como, por ejemplo, el ancho de banda.



Hacer la red más segura, protegiéndola contra el acceso no autorizado, haciendo imposible que personas ajenas puedan entender la información que circula en ella. Controlar cambios y actualizaciones en la red de modo que ocasionen las menos interrupciones posibles, en el servicio a los usuarios.

El sistema de administración de red opera bajo los siguientes pasos básicos:

- a. Colección de información acerca del estado de la red y componentes del sistema.
- b. Transformación de la información para presentarla en formatos apropiados para el entendimiento del administrador.
- c. Transportación de la información del equipo monitoreado al centro de control.
- d. Almacenamiento de los datos coleccionados en el centro de control.
- e. Análisis de parámetros para obtener conclusiones que permitan deducir rápidamente lo que pasa en la red.
- f. Actuación para generar acciones rápidas y automáticas en respuesta a una falla mayor.

5.1.5. Políticas generales de seguridad informática

Una política de seguridad informática es una forma de comunicarse con los usuarios.

Las PSI establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la organización.



No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados.

Es más bien una descripción de los que deseamos proteger y el porqué de ello.

Cada PSI es consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la compañía.

5.1.5.1. Elementos de una política de seguridad informática

Como mencionábamos en el apartado anterior, una PSI debe orientar las decisiones que se toman en relación con la seguridad.

Por tanto, requiere de una disposición por parte de cada uno de los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las PSI deben considerar entre otros, los siguientes elementos:

- a. Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica. Es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos, así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Invitación que debe concluir en una posición.
- b. Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- c. Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.

- d. Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.
- e. Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- f. Responsabilidades de los usuarios con respecto a la información a la que ella tiene acceso.

Finalmente, las PSI como documentos dinámicos de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios entre otros.



5.2. FASE 2: PLANIFICACIÓN (LifeCycle Services)

En la segunda fase del ciclo de vida de la red, una empresa, o en este caso la institución, empieza a evaluar su red para saber si la infraestructura de sistema existente, las localidades y el ambiente operativo pueden soportar el sistema propuesto. Aquí el equipo trata de asegurar la disponibilidad de los recursos adecuados para administrar el proyecto de despliegue de tecnología, desde la planeación hasta el diseño e implementación.

El tema de la seguridad es un punto importante por la cantidad de información confidencial que se maneja en instituciones de este tipo por lo tanto se tiene que planear algo para la seguridad, entonces se procede a evaluar su sistema, redes e información contra intrusos, así como también evalúa la red para detectar la factibilidad de que redes externas y no confiables obtengan acceso a redes y sistemas internos de la institución.

Se crea un plan de proyecto para ayudar a administrar las tareas, riesgos, problemas, responsabilidades, hitos críticos y recursos requeridos para implementar cambios en la red.

El plan de proyecto se alinea con el campo de acción, el costo y los parámetros de recursos establecidos en los requerimientos de negocio originales.

5.2.1. Evaluación de la red informática

5.2.1.1. Topología de la red

El término topología se refiere a la forma en que está diseñada la red, bien físicamente (rigiéndose de algunas características en su hardware) o bien lógicamente (basándose en las características internas de su software).

La topología de red es la representación geométrica de la relación entre todos los enlaces y los dispositivos que los enlazan entre sí (habitualmente denominados nodos).



Para el día de hoy, existen al menos cinco posibles topologías de red básicas: malla, estrella, árbol, bus y anillo.

A. Topología en Estrella Jerárquico

La topología de la red debe ser tipo estrella jerárquica con redundancia que interconecte el Gabinete de Distribución Principal (GDP) ubicado en el Data Center hasta los Gabinetes de Distribución Secundarios (GDS), logrando velocidades iniciales a 1 Gbps y soporten transmisiones futuras de 10/40/100Gbps.

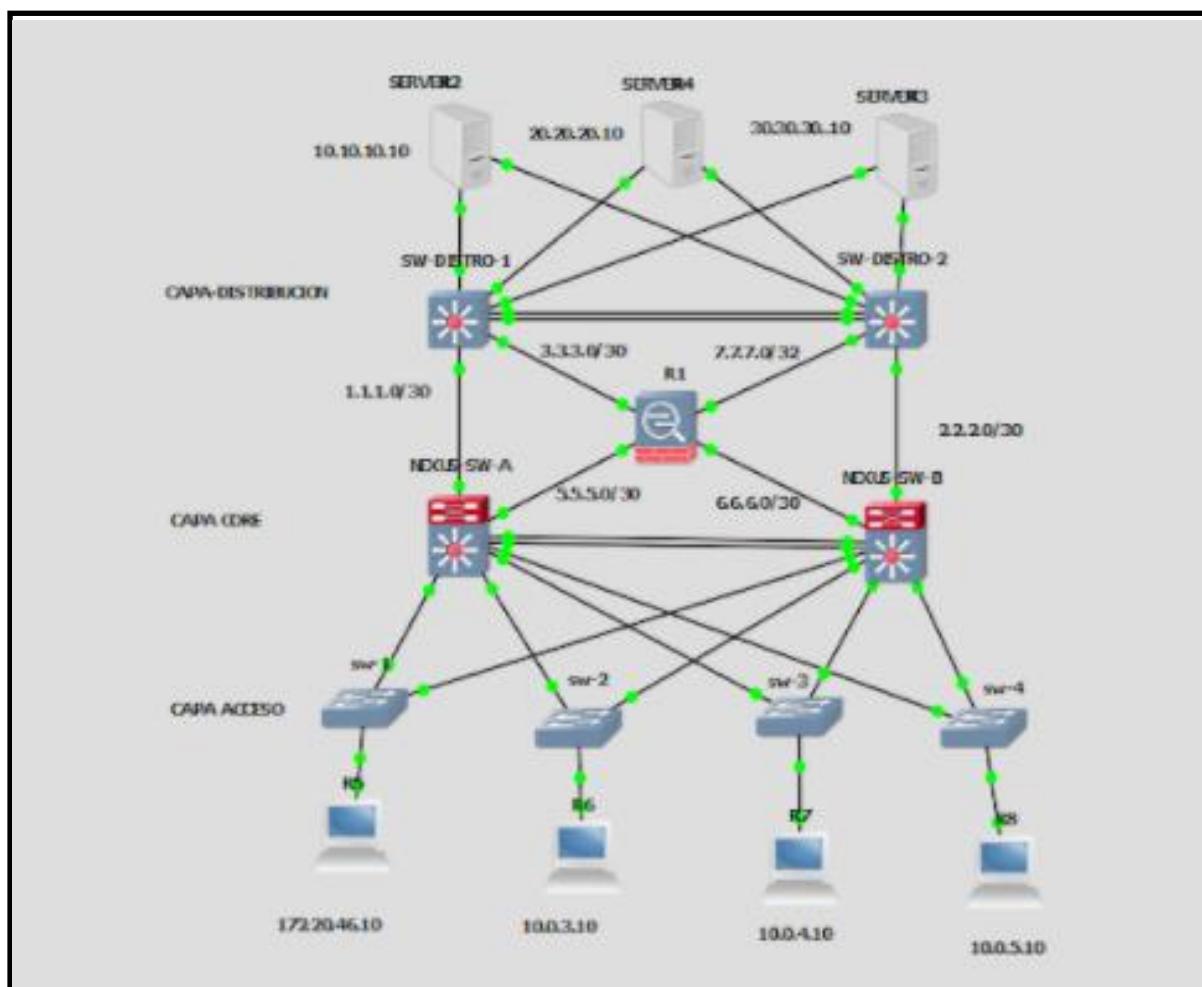


Figura 59. Topología en Estrella Jerárquico. Fuente: Elaboración Propia (2017).

Nota: La Arquitectura de Red Jerárquico de Alto Nivel que se está Proponiendo Brindara alta Disponibilidad, Implementación de Seguridad a Través de Firewall, Redundancia con los Servidores y Virtualización de los Switchs Core Nexus 7000.



B. Windows Server 2012

Windows Server 2012 tiene una función de administración de direcciones IP (IPAM) para la búsqueda, monitoreo, auditoría y administración del espacio de direcciones IP usados en una red corporativa.

IPAM provee monitoreo y gestión de servidores bajo DHCP (Dynamic Host Configuration Protocol) y DNS (Domain Name Service).

IPAM incluye componentes para:

Gestión, reporte y espacio de visualización de direcciones IP personalizadas: La pantalla de seguimiento de las direcciones IP es altamente personalizable y detallada, y se encuentran disponibles los datos de utilización.

Los espacios de direcciones IPv4 e IPv6 están organizados en bloques de direcciones IP, en rangos de direcciones IP, y en direcciones IP individualizadas.

Las direcciones IP son asignadas en campos incorporados o en campos definidos por el usuario, que pueden ser usados para organizar el espacio de direcciones IP en grupos ordenados lógicamente y jerárquicamente.

Auditoría de cambios en la configuración del servidor y seguimiento del uso de direcciones IP: Los eventos operativos se muestran por el servidor de IPAM y administrados servidores DHCP.

IPAM también permite el seguimiento de dirección IP mediante eventos de concesión DHCP y eventos de inicio de sesión de usuario, obtenidos desde Network Policy Server (NPS), controladores de dominio y de servidores DHCP.

El seguimiento está disponible por dirección IP, ID de cliente, nombre de host o nombre de usuario.



Monitoreo y manejo de servicios DHCP y DNS: IPAM permite el control automatizado de la disponibilidad de servicio para servidores DHCP y DNS Microsoft a través de la red.

Se muestra la "salud" de la zona DNS, y también está disponible una gestión detallada del alcance del servidor DHCP mediante la consola IPAM.

C. MySQL (Open Source)

MySQL es un sistema de gestión de base de datos relacional, multihilo y multiusuario con más de seis millones de instalaciones.

MySQL AB —desde enero de 2008 una subsidiaria de Sun Microsystems y ésta a su vez de Oracle Corporation desde abril de 2009— desarrolla MySQL como software libre en un esquema de licenciamiento dual.

Por un lado, se ofrece bajo la GNU GPL para cualquier uso compatible con esta licencia, pero para aquellas empresas que quieran incorporarlo en productos privativos deben comprar a la empresa una licencia específica que les permita este uso. Está desarrollado en su mayor parte en ANSI C.

Al contrario de proyectos como Apache, donde el software es desarrollado por una comunidad pública y el copyright del código está en poder del autor individual, MySQL es patrocinado por una empresa privada, que posee el copyright de la mayor parte del código.

Esto es lo que posibilita el esquema de licenciamiento anteriormente mencionado.

Además de la venta de licencias privativas, la compañía ofrece soporte y servicios.

Para sus operaciones contratan trabajadores alrededor del mundo que colaboran vía Internet.

MySQL AB fue fundado por David Axmark, Allan Larsson y Michael Widenius.

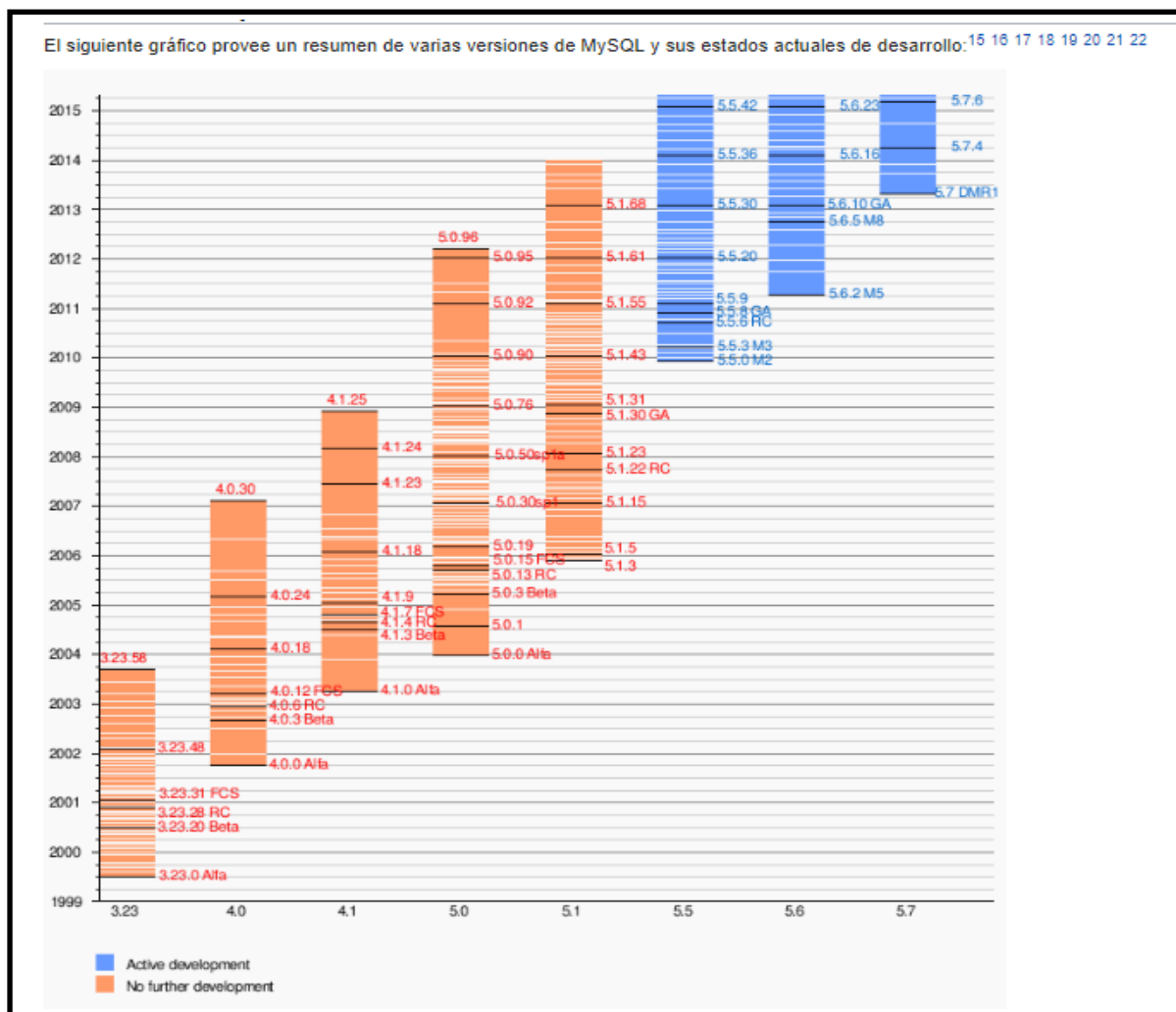


Figura 60. Cuadro de Evolución de MySQL. Fuente: Sistema de Gestión de Bases de Datos Relacionales MySQL (1995).

Nota: Se Presenta en este Gráfico de la Evolución por años las Versiones que han ido Desarrollándose el Software MySQL.



D. OptiView (Analizador de Red)

OptiView XG es una Tablet para el ingeniero de redes con hardware especializado y personalizado para el análisis automatizado de redes y aplicaciones durante la implementación y la solución de problemas de nuevas tecnologías.

Se encuentra como en casa en el centro de datos gracias a su compatibilidad para 10GbE y servidores virtualizados; en la oficina del usuario, ya que admite análisis 802.11n y de aplicaciones; y con los switches y routers que haya en medio.

Utilícelo para encontrar problemas desde su propia mesa o lléveselo, junto con los datos que haya recopilado, al lugar del problema para realizar un análisis de primera mano.

Su sistema exclusivo de solución de problemas se basa en la supervisión y el análisis proactivo, el análisis de rutas con gráficos y el análisis basado en aplicaciones, lo que ofrece una guía experta que identifica automáticamente la causa de los problemas.



Figura 61. Optiview Analizador de Red. Fuente: Oficina de Soporte Informático (2017).

Nota: La Herramienta se usa Actualmente en la Oficina de Soporte Informático del HNERM EsSALUD.

E. Políticas de seguridad de redes

Los objetivos de la política de seguridad de red son establecer políticas proteger las redes y sistemas de ordenador del uso inadecuado.

Los mecanismos de Políticas de Seguridad de Red ayudarán en la identificación y la prevención del abuso de sistemas de ordenador y redes.

Las Políticas de Seguridad de Red proporcionan un mecanismo para responder a quejas y preguntas sobre verdaderas redes y sistemas de ordenador.

Las Políticas de Seguridad de Red establecen mecanismos que protegerán y satisfarán responsabilidades legales a sus redes y conectividad de sistemas de ordenador al Internet mundial.

Los mecanismos de Políticas de Seguridad de Red apoyarán los objetivos de existir políticas.

La responsabilidad de la seguridad de los recursos de calcular descansa con los administradores de sistema que manejan aquellos recursos.

Estos riesgos que se enfrentan han llevado a que muchas desarrollen documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la empresa.



F. Planes de contingencia

Un Plan de contingencias es un instrumento de gestión para el buen gobierno de las Tecnologías de la Información y las Comunicaciones en el dominio del soporte y el desempeño.

Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones de una compañía.

Un plan de contingencias es un caso particular de plan de continuidad del negocio aplicado al departamento de informática o tecnologías.

Otros departamentos pueden tener planes de continuidad que persiguen el mismo objetivo desde otro punto de vista.

No obstante, dada la importancia de las tecnologías en las organizaciones modernas, el plan de contingencias es el más relevante.

G. Detalle de las Fases de la Planificación:

Fase I. Diagnóstico de la Red LAN (Cuarto de Equipos, Cuartos de Comunicaciones, Áreas de Trabajo y Equipos Intermedios).

Cuarto de Equipos o Data Center (ER)

Es un ambiente de propósito especial que provee espacios y mantiene condiciones ambientales apropiadas para grandes equipos de telecomunicaciones, son considerados generalmente para servir un edificio entero (o campus).



Para el diseño y su ubicación debe considerarse lo siguiente:

- a. Posibilidades de expansión, es recomendable prever el crecimiento en los equipos que irán ubicados en el ER, y prever la posibilidad de su conexión.
- b. Evitar ubicar el ER en lugar donde puede haber filtraciones de agua, ya sea por el techo o por las paredes.
- c. Facilidades de acceso para equipos de gran tamaño.

Diagnóstico:

El área destinada para el Data Center es 10 m², el cual no cumple con el estándar ANSI/TIA 942, ANSI/TIA-1179: Infraestructura de telecomunicaciones para instalaciones sanitarias, Norma Técnica de Salud N°119-MINSA/DGIEM para Data Center así mismo no se cuenta con posibilidades de expansión, el mismo que no se ha previsto el crecimiento en los equipos que irán ubicados en el ER, y prever la posibilidad de su conexión, generando un hacinamiento.

Situación de los Cuartos de Telecomunicaciones (TR)

Los cuartos de Telecomunicaciones son espacios que actúan como punto de transmisión entre las “montantes” Verticales (Backbone), y las canalizaciones de distribución horizontal, Sirven como punto de terminación del cableado horizontal y Backbone en el hardware de conexión.

Puede cumplir la función de Distribuidor Intermedio para diferentes partes del cableado.

Se debe tener en cuenta lo siguiente:

- a. El tamaño del edificio, el área útil del piso servido, los requerimientos de los usuarios, los servicios de telecomunicaciones a ser usados.
- b. Considerar la flexibilidad para futuros cambios
- c. Considerar requerimientos de iluminación, aire acondicionado, capacidad de carga de piso y requerimientos eléctricos

Diagnóstico:

- a. Los cuartos de telecomunicaciones no cuentan con un ambiente exclusivo para el funcionamiento del mismo bajo los estándares establecidos.
- b. El 75 % de los gabinetes y rack tiene poca densidad para la cantidad de puntos y equipos intermedios instalados.
- c. No se realiza limpieza y mantenimiento preventivo.
- d. Unidad de Ventilación inoperativa.
- e. Chapas de seguridad en mal estado.
- f. No se cuenta un esquema de ubicación física de los mismos.



Situación de los Equipos Intermedios

- a. Los equipos intermedios (Switches) en un 90 % ya cumplieron su vida útil (10 Años).
- b. No se cuenta con un servicio que realice el mantenimiento preventivo de los equipos (dos veces por año).
- c. Existe diversidad de marcas lo que conlleva a no tener un estándar.
- d. Los Equipos no cuentan con un sistema que estabilice la energía lo que ocasiona, subidas de tensión y las bajas conocidas como picos, estos afectan a los dispositivos electrónicos causándole grandes daños o afectando su funcionamiento.
- e. El 20 % de Switches instalados en los cuartos de comunicaciones se han quemado.
- f. La administración de los equipos depende de la OCTIC – Sede Central.
- g. No se cuenta con equipos switches como respaldo ante cualquier contingencia.

Sistema de Cableado Estructurado

- a. El 85 % del cableado estructurado Cat. 6 se encuentra certificado por el fabricante Simón de acuerdo a los estándares de la industria, representando el 15 % del cableado Cat. 5e y 6 no certificados.



- b. El Cableado no se encuentra ordenado lo que genera un desorden en su estructura. (Video, Voz, Impresoras, Equipos Biomédicos, Datos).
- c. No se cuenta con la documentación del Cableado Estructurado (Puntos existentes por tipo de servicio y área de trabajo).

Fluido Eléctrico

- a. El 75% de los cuartos de comunicaciones, cuando el fluido eléctrico se corta queda sin servicio, debido que el grupo electrógeno cobertura el 25%.
- b. No se cuenta con Sistema de pozo a tierra exclusivo para los equipos de comunicaciones.
- c. Comprende los componentes que se extienden desde el outlet hasta el equipo.
- d. La longitud máxima es de 5 metros.
- e. Cuando se requiere adaptadores (balunes, adaptadores modulares, etc.), ellos deben ser externos al outlet.

Tabla 10

Cuadro de Equipos Intermedios de la OSI HNERM EsSALUD

RELACIÓN DE EQUIPOS INTERMEDIOS								
N°	MARCA	MODELO	VELOCIDAD	CONFIGURACION	VLAN	CAPA	N° PUERTOS	CANTIDAD
1	3COM	Super Stack 5500G -EL	10/100/1000	Administrables	SI	L2	24	6
3	3COM	Baseline Switch 2824	10/100/1000	Administrables	SI	L2	24	3
4	A VAYA	P334T	10/100/1000	Administrables		L2	48	1
5	ALCATEL-LUCENT	OmniSwitch 9800	10/100/1000	Administrables	SI	L3	48	1
6	ALCATEL-LUCENT	OmniStack LS 6224P	10/100	Administrables	SI	L2	24	31
7	ALIED TELESIS	AT- GS950	10/100/1000	Administrables	SI	L2	8	1
8	ALIED TELESIS	AT 8000S/24POE					24	1
9	CISCO	Router BEFSR81					8	1
10	CISCO	Catalyst 3560	10/100/1000	Administrables	SI	L2	8	7
11	D - LINK	DIR-400 ROUTER					24	1
12	D - LINK	DES - 1024A	10/100	Puente	NO	L2	24	10
13	D - LINK	DES - 1024D	10/100	Puente	NO	L2	24	39
14	D - LINK	DGS - 3100	10/100/1000	Administrables	SI	L2	24	1
15	D - LINK	DGS - 3024	10/100/1000	Administrables	SI	L2	24	5
16	D - LINK	DGS - 3120	10/100/1000	Administrables	SI	L2/L3	24	1
17	D - LINK	DGS - 1210	10/100/1000	Administrables	SI	L2	24	3
18	D - LINK	DES - 1016D	10/100	Puente	NO	L2	16	2
19	D - LINK	DES - 1060D	10/100	Puente	NO	L2	16	1
20	TRENDnet	TEG - 516DG	10/100/1000		SI	L2	16	1

Fuente: Oficina de Soporte Informático (2017).



Tabla 11
Formato Actual de Diagnóstico de la Red LAN en el HNERM EsSALUD

FORMATO DE DIAGNOSTICO DE LA RED - HNERM														
ANEXO 001														
GABINETE														
Item	Tipo	RU	Serie	Modelo	Marca	Cod. Patrimonia	Nombre	Ubicación	Enlace	Estado	Observaciones			
1	PARED	16	N.E	SERVIDOR	N.E	07048190	Gabinete C4	FISIOLOGIA-SERVICIO DE HOSPITALIZACIÓN 4 "C", MEDICINA INTERNA II 4 "C",	Gabinete C	Bueno				
SWITCHES														
Item	Serie	Modelo	Marca	MAC	Cod. Patrimonia	Capa	Configuracion	Direccion IP	Ancho de Banda Mbp	Voltaje	Puertos	Puertos / Libre	Fecha de instalac	Enlace
1	F30H263003021	DES-1024D	D-LINK	No Aplica	00601634	2	CASCADA	N.E	10/100	50Hz/0.3A	24	4	N.E	COBRE
SISTEMA ELECTRICO									SISTEMA DE AIRE ACONDICIONADO					
SISTEMA DE ALIMENTACIÓN INNINTERRUMPIDA - UPS									AC.Precisión	AC.Confort	Extractor de Air	Cooler	Estado	
Item	Modelo	Capacidad Watts	Voltaje	Entrada Margen de Voltaje	Frecuencia	Y.Nominal	Cap.Salida	Bateria Tiempo de Respaldo				1	MALO	
1	NO HAY	NO HAY	NO HAY	NO HAY	NO HAY	NO HAY	NO HAY	NO HAY						
UNIDAD DE DISTRIBUCIÓN DE ENERGIA - PDU									SISTEMA DE POZO A TIERRA					
Item	Modelo	Tipo	Voltaje Salida	Medidor Digital	N° de Tomas	Tamaño de Rack	Marca	Estado		NO TIENE				
1	NO HAY	REGLETA	NO HAY	NO HAY	NO HAY	NO HAY	NO HAY	NO HAY						
ESTABILIZADOR								CABLEADO			PATCH CORD			
Item	Marca	Modelo	Potencia	N° Fases	Sobrecarga	Frecuencia	Tomas de	Tipo	Categoría	Certificació	Marca	Categoría	Estado	
1	NO HAY	NO HAY	NO HAY	NO HAY	NO HAY	NO HAY	NO HAY	COBRE	6	SIMON	SIMON	6	BUENO	
PATCH PANEL									OBSERVACIONES		RECOMENDACIONES			
ITEM	MARCA	CATEGORIA	TERMINAL	POTULADO	N° PUERTOS	N° P.LIBRES	TIPO	RU						
1	SIMON	6	COBRE	SI	48	15	DATA	2						
2	SIMON	5e	COBRE	SI	24	13	VOZ	1						

Fuente: Oficina de Soporte Informático del HNERM EsSALUD (2017).



Fase II. Migración del Core OmniSwitch 9700 al 9800.

Tabla 12

Cuadro de servidores en el cuarto de Telecomunicaciones del HNERM EsSALUD.

RELACIÓN DE UBICACIÓN DE CUARTOS DE TELECOMUNICACIONES						
N	TIPO	RU	MODELO	NOMBRE GABINETE	ENLACE	UBICACIÓN FÍSICA
1	PISO	45	CABLEADO	Gabinete N	Gabinete N	PISO 3 - SERVICIO DE OCPyAP - OFICINA DE COORDINACIÓN DE PRESTACIONES Y ATENCIÓN PRIMARIA.
2	PISO	44	SERVIDOR	Gabinete B1	Gabinete B1	PISO 1 BLOCK B - MODULO CENTRAL
3	PISO	44	SERVIDOR	Gabinete C	Gabinete C	PISO 1 - BLOCK A - FARMACIA 2
4	PISO	44	SERVIDOR	Gabinete C1	Gabinete C1	PISO 1 - BLOCK C - SERVICIO DE TOMOGRAFIA COMPUTARIZADA Y RESONANCIA MAGNETICA - AREA HELICOIDAD.
5	PISO	44	SERVIDOR	Gabinete G1	Gabinete G1	PISO 1 - BLOCK G - SERVICIO DE PEDIATRIA MODULO DE CITAS
6	PISO	44	SERVIDOR	Gabinete I1	Gabinete I1	PISO 1 - BLOCK "D" - SERVICIO DE CONSULTA EXTERNA
7	PISO	44	SERVIDOR	Gabinete I2	Gabinete I2	PISO 1 - BLOCK "A" - SERVICIO DE CONSULTA EXTERNA
8	PISO	45	SERVIDOR	Gabinete M	Gabinete M	PISO 3 - SERVICIO DE ADQUISICIONES - PLAYA MILLER
9	PISO	44	SERVIDORES	Gabinete B	Gabinete B	PISO 1 - BLOCK B - CENTRAL TELEFONICA
10	PISO	44	SERVIDOR	Gabinete F	Gabinete F	DATA CENTER - OFICINA DE SOPORTE INFORMÁTICO
11	PARED	22	SERVIDOR	Gabinete A3	Gabinete A3	PISO 3A - SERVICIO DE HOSPITALIZACIÓN 3 "A", CIRUGÍA GENERAL 3 "A"
12	PARED	22	SERVIDOR	Gabinete C7	Gabinete C7	PISO 7C - SERVICIO DE HOSPITALIZACIÓN 7 "C", MEDICINA INTERNA V 7 "C", UCIN 7 "C".
13	PARED	22	SERVIDOR	Gabinete C10	Gabinete C10	PISO 10C - SERVICIO DE HOSPITALIZACIÓN 10 "C", MEDICINA INTERNA III 10"C", UCIN 10 "C"
14	PARED	22	SERVIDOR	Gabinete C13	Gabinete C13	PISO 13C - SERVICIO DE HOSPITALIZACIÓN 13 "C", NEUROCIROLOGÍA 13 "C", UCIN 13 "C", CIRUGÍA VERTEBRAL Y NEURO PERIFÉRICA.
15	PARED	22	SERVIDOR	Gabinete D	Gabinete D	PISO 1 - BLOCK D - SERVICIO DE HEMODIALISIS
16	PARED	18	SERVIDOR	Gabinete Ñ	Gabinete Ñ	PISO 1 - SERVICIO DE EMERGENCIA - TOPICO DE CIRUGIA
17	PARED	22	SERVIDOR	Gabinete L	Gabinete L	PISO 1 - BLOCK L - SERVICIO DE EMERGENCIA GINECOLÓGICA, OBSTETRICIA Y PEDIÁTRICA - ESTACIÓN CAMILLA
18	PARED	22	SERVIDORES	Gabinete A	Gabinete A	PISO 1 - BLOCK A - JUNTO AL CINDICATO DE OBSTETRICIAS
19	PARED	22	SERVIDORES	Gabinete A1	Gabinete A1	PISO 1 - BLOCK A - SALA DE ENTREVISTA DE TRABAJO SOCIAL
20	PARED	22	SERVIDORES	Gabinete A6	Gabinete A6	PISO 6A - SERVICIO DE HOSPITALIZACIÓN 6 "A", GASTRO ENTEROLOGIA 6 "A", UNIDAD DE HÍGADO, INTESTINO-COLON-RECTO, ESÓFAGO-ESTOMAGO-DUODENO.
21	PARED	22	SERVIDORES	Gabinete A9	Gabinete A9	PISO 9A - SERVICIO DE HOSPITALIZACIÓN 9 "A", TRAUMATOLOGÍA 9 "A".
22	PARED	20	SERVIDORES	Gabinete A12	Gabinete A12	PISO 12A - SERVICIO DE HOSPITALIZACIÓN 12 "A", UROLOGÍA 12 "A", UROLOGÍA GENERAL 12 "A", UROLOGÍA ESPECIALIZADA.
23	PARED	22	SERVIDORES	Gabinete B3	Gabinete B3	PISO 3B - SERVICIO DE HOSPITALIZACIÓN 3 "B", SALA DE OPERACIONES Y RECUPERACIÓN 3 "B", UNIDAD DE SOPORTE NUTRICIONAL.
24	PARED	22	SERVIDORES	Gabinete B6	Gabinete B6	PISO 6B - SERVICIO DE HOSPITALIZACIÓN 6 "B", HEMORRAGIA DIGESTIVA 6 "B", SALA DE OPERACIONES 6 "B".
25	PARED	22	SERVIDORES	Gabinete B9	Gabinete B9	PISO 9B - SERVICIO DE HOSPITALIZACIÓN 9 "B", CENTRO QUIRÚRGICO Y RECUPERACIÓN 9 "B", ORTOPEDIA
26	PARED	22	SERVIDORES	Gabinete B12	Gabinete B12	PISO 12B - SERVICIO DE HOSPITALIZACIÓN 12 "B", NEUMOLOGÍA 12 "B", SALA DE OPERACIONES Y RECUPERACIÓN DE NEUMOLOGÍA.
27	PARED	24	SERVIDORES	Gabinete G3	Gabinete G3	PISO 3 - BLOCK G - SERVICIO DE PEDIATRIA - UNIDAD DE ONCOLOGIA PEDIATRICA
28	PARED	16	SERVIDORES	Gabinete J	Gabinete J	SOTANO BLOK J - SERVICIO DE PUERTAS Y VENTANAS - VIDRIERIA -B.U.C
29	PARED	24	SERVIDORES	Gabinete K	Gabinete K	PISO 1 - BLOCK K - SERVICIO DE SALUD MENTAL (FARMACODEPENDENCIA, CONSULTA EXTERNA, HOSPITAL DE DÍA, HOSPITALIZACIÓN 1 Y 2, EMERGENCIA)
30	PARED	16	SERVIDOR	Gabinete C4	Gabinete C4	PISO 4C - SERVICIO DE HOSPITALIZACIÓN 4 "C", MEDICINA INTERNA II 4 "C", UCIN 4 "C".

Fuente: Oficina de Soporte Informático del HNERM ESSALUD (2017).



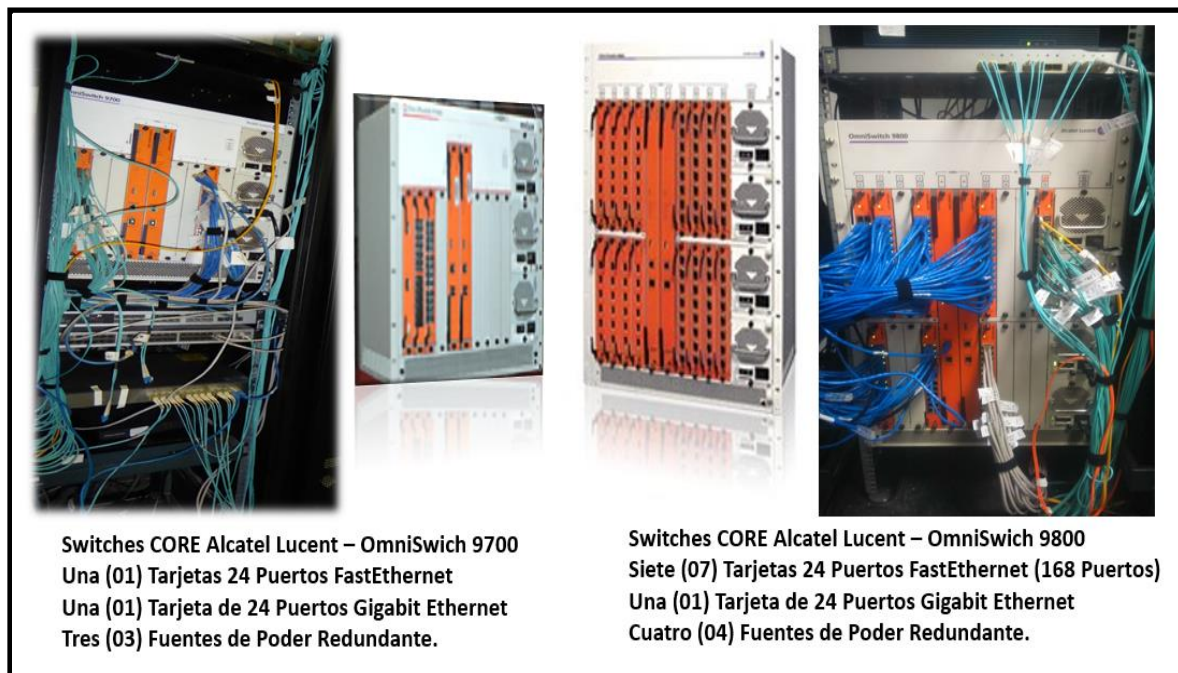


Figura 62. Migración del CORE OmniSwitch 9700 al 9800 al 100%. Fuente: Oficina de Soporte Informático (2017).

Migración del CORE OmniSwitch 9700 al 9800 al 100%.

Fase III. Capacitación Al Personal Del Área De Comunicaciones De Esta Oficina En Configuración De Equipos Intermedios, Por Parte De La Sede Central.

La Fase III se realizó en el mes de agosto del 2016.

La Oficina Central de tecnologías de Información y Comunicaciones a solicitud de la Oficina de Soporte Informático realizo la capacitación al personal de comunicaciones en Configuración de equipos Switches Alcatel 6224P y CORE 9700, segmentación de VLAN.

Logrando capacitar a seis (06) profesionales.

Fase IV. Identificación De Conexiones De Puntos De Voz, Data, Video, Equipos Biomédicos, Etc.

En la Fase IV, se encuentra en un 100% de avance, la misma que consiste en identificar los puntos de Red por tipo de servicio (Video, Voz, Data, Impresoras, Equipos Biomédicos), cobertura por área de trabajo y generar la documentación respectiva.

Fase V. Limpieza y Mantenimiento de Gabinetes y Equipos Intermedios.

En la Fase V, se encuentra en un 85% de avance, la misma que consiste en realizar la limpieza de los gabinetes, Limpieza de equipos intermedios y segmentación de VLAN.

Se ejecutado el Piloto en el Gabinete “J” y Gabinete “K”.

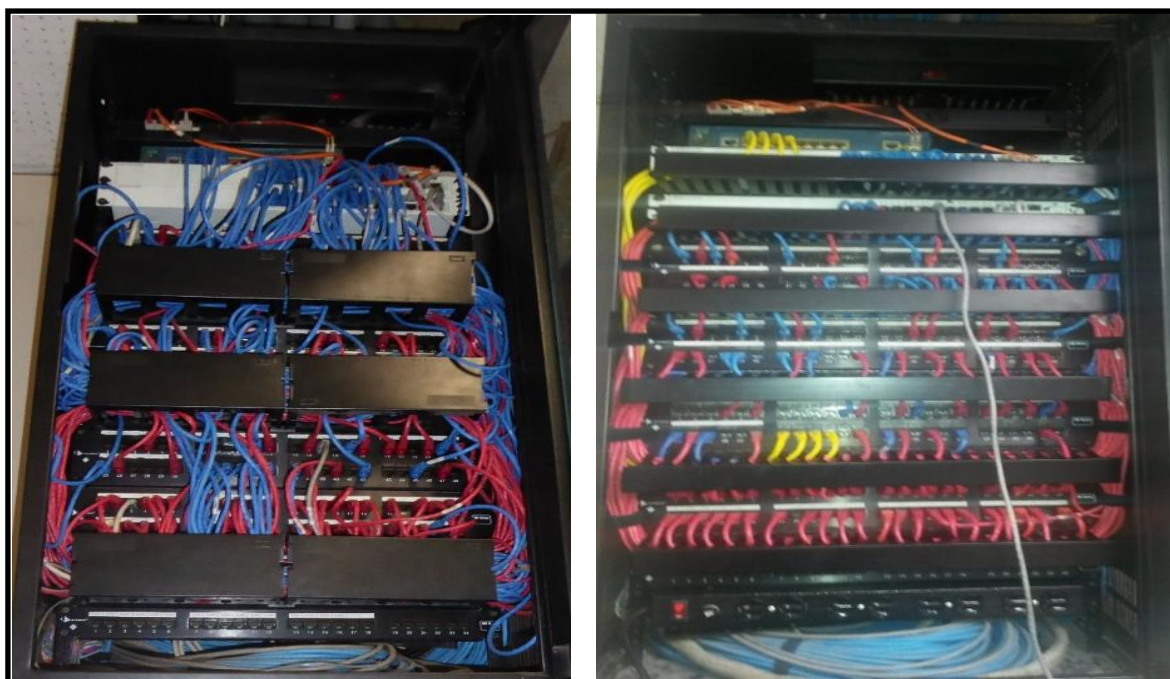


Figura 63. Gabinete K Antes y Gabinete K Después Fuente: Oficina de Soporte Informático del HNERM EsSALUD (2017).



Fase VI. Redistribución de Equipos Intermedios

En la Fase VI, se encuentra en un 50% de avance, la misma que consiste en realizar la limpieza de los equipos intermedios y redistribución.

Fase VII. Migración de Direcciones IP, y Segmentación de VLAN

La migración, surge con la necesidad del agotamiento de direcciones IP de los Rangos comprendidos en la sub red (172.22.40.0, 172.22.41.0, 172.22.42.0, 172.22.43.0, 172.22.44.0, 172.22.46.0, 172.22.47.0, 172.22.48.0, 172.22.49.0).

Actualmente tenemos problemas de conflicto de direcciones IP, tráfico de red que generan colisiones y por ende caídas de red, toda vez que no existe una segmentación de la misma.

Teniendo en cuenta que el rendimiento de la red es un factor importante en la productividad de los servicios del Hospital, se ha decidido realizar la segmentación de la Red LAN con VLAN bajo el esquema de direccionamiento de red jerárquico.

(Las direcciones IP se aplican a los segmentos de red o a las VLAN de manera ordenada, lo que permite que la red se tome en cuenta como conjunto), el mismo que garantizara la productividad de los usuarios, adaptabilidad y escalabilidad de la red.

TABLA 13
Plan Direccinamiento Ip HNERM EsSALUD

PLAN DE DIRECCIONAMIENTO IP DEL HOSPITAL EDGARDO REBAGLIATI									
DATA CENTER		OFICINA DE SOPORTE INFORMATICO							
NUM		Subnet	Mask	/	Subnet Size	Host Range	Broadcast	Puerta enlace	VLAN
	SERVIDORES DATA CENTER	10.1.0.0	255.255.255.128	/25	126	10.1.0.2 to 10.1.0.126	10.1.0.255	10.1.0.1	
VLAN GENERALES									
NUM		Subnet	Mask	/	Subnet Size	Host Range	Broadcast	Puerta enlace	VLAN
1	Admin_switches	10.1.1.0	255.255.255.0	/24	254	10.1.1.2 to 10.1.1.254	10.1.1.255	10.1.1.1	1
2	Camaras_vigilancia	10.1.2.0	255.255.255.0	/24	254	10.1.2.2 to 10.1.2.254	10.1.2.255	10.1.2.1	500
3	Imágenes_packs	10.1.3.0	255.255.255.0	/24	254	10.1.3.2 to 10.1.3.254	10.1.3.255	10.1.3.1	510
4	Equipos_medicos	10.1.4.0	255.255.255.0	/24	254	10.1.4.2 to 10.1.4.254	10.1.4.255	10.1.4.1	520
5	Marcadores_biometricos	10.1.5.0	255.255.255.192	/26	62	10.1.5.2 to 10.1.5.62	10.1.5.63	10.1.5.1	530
6	LIBRE	10.1.5.64	255.255.255.192	/26	62	10.1.5.66 to 10.1.5.126	10.1.5.127	10.1.5.65	540
GABINETE A									
PISO 1 - BLOCK A - JUNTO AL SINDICATO DE OBSTETRICES									
NUM	GABINETE A	Subnet	Mask	/	Subnet Size	Host Range	Broadcast	Puerta enlace	VLAN
1	Datos_Gab_A	10.1.6.0	255.255.254.0	/23	510	10.1.6.2 to 10.1.7.254	10.1.7.255	10.1.6.1	100
2	Voz_Gab_A	10.1.8.0	255.255.255.0	/24	254	10.1.8.2 to 10.1.8.254	10.1.8.255	10.1.8.1	101
3	Impresoras_Gab_A	10.1.9.0	255.255.255.192	/26	62	10.1.9.2 to 10.1.9.62	10.1.9.63	10.1.9.1	102
4	Wireless_Gab_A	10.1.9.64	255.255.255.192	/26	62	10.1.9.66 to 10.1.9.126	10.1.9.127	10.1.9.65	103
5	LIBRE	10.1.9.128	255.255.255.128	/25	126	10.1.9.130 to 10.1.9.254	10.1.9.255	10.1.9.129	104
GABINETE C									
PISO 1 - BLOCK A - FARMACIA 2									
NUM	GABINETE A	Subnet	Mask	/	Subnet Size	Host Range	Broadcast	Puerta enlace	VLAN
1	Datos_Gab_C	10.1.10.0	255.255.254.0	/23	510	10.1.10.2 to 10.1.11.254	10.1.11.255	10.1.10.1	110
2	Voz_Gab_C	10.1.12.0	255.255.255.0	/24	254	10.1.12.2 to 10.1.12.254	10.1.12.255	10.1.12.1	111
3	Impresoras_Gab_C	10.1.13.0	255.255.255.192	/26	62	10.1.13.2 to 10.1.13.62	10.1.13.63	10.1.13.1	112
4	Wireless_Gab_C	10.1.13.64	255.255.255.192	/26	62	10.1.13.66 to 10.1.13.126	10.1.13.127	10.1.13.65	113
5	LIBRE	10.1.13.128	255.255.255.128	/25	126	10.1.13.130 TO 10.1.13.254	10.1.13.255	10.1.13.129	114
GABINETE B3									
PISO 3B - SERVICIO DE HOSPITALIZACION									
NUM	GABINETE A	Subnet	Mask	/	Subnet Size	Host Range	Broadcast	Puerta enlace	VLAN
1	Datos_Gab_B3	10.1.14.0	255.255.254.0	/23	510	10.1.14.2 to 10.1.15.254	10.1.15.255	10.1.14.1	120
2	Voz_Gab_B3	10.1.16.0	255.255.255.0	/24	254	10.1.16.2 to 10.1.16.254	10.1.16.255	10.1.16.1	121
3	Impresoras_Gab_B3	10.1.17.0	255.255.255.192	/26	62	10.1.17.2 to 10.1.17.62	10.1.17.63	10.1.17.1	122
4	Wireless_Gab_B3	10.1.17.64	255.255.255.192	/26	62	10.1.17.66 to 10.1.17.126	10.1.17.127	10.1.17.65	123
5	LIBRE	10.1.17.128	255.255.255.128	/25	126	10.1.17.130 TO 10.1.17.254	10.1.17.255	10.1.17.129	124
GABINETE A1									
PISO 1 - BLOCK A - SALA DE ENTREVISTA DE TRABAJO SOCIAL									
NUM	GABINETE A	Subnet	Mask	/	Subnet Size	Host Range	Broadcast	Puerta enlace	VLAN
1	Datos_Gab_A1	10.1.18.0	255.255.254.0	/23	510	10.1.18.2 to 10.1.19.254	10.1.19.255	10.1.18.1	130
2	Voz_Gab_A1	10.1.20.0	255.255.255.0	/24	254	10.1.20.2 to 10.1.20.254	10.1.20.255	10.1.20.1	131
3	Impresoras_Gab_A1	10.1.21.0	255.255.255.192	/26	62	10.1.21.2 to 10.1.21.62	10.1.21.63	10.1.21.1	132
4	Wireless_Gab_A1	10.1.21.64	255.255.255.192	/26	62	10.1.21.66 to 10.1.21.126	10.1.21.127	10.1.21.65	133
5	LIBRE	10.1.21.128	255.255.255.128	/25	126	10.1.21.130 to 10.1.21.254	10.1.21.255	10.1.21.129	134
GABINETE C1									
PISO 1 - BLOCK C - SERVICIO DE TOMOGRAFIA COMPUTARIZADA Y RESONANCIA MAGNETICA									
NUM	GABINETE A	Subnet	Mask	/	Subnet Size	Host Range	Broadcast	Puerta enlace	VLAN
1	Datos_Gab_C1	10.1.22.0	255.255.254.0	/23	510	10.1.22.2 to 10.1.23.254	10.1.23.255	10.1.22.1	140
2	Voz_Gab_C1	10.1.24.0	255.255.255.0	/24	254	10.1.24.2 to 10.1.24.254	10.1.24.255	10.1.24.1	141
3	Impresoras_Gab_C1	10.1.25.0	255.255.255.192	/26	62	10.1.25.2 to 10.1.25.62	10.1.25.63	10.1.25.1	142
4	Wireless_Gab_C1	10.1.25.64	255.255.255.192	/26	62	10.1.25.66 to 10.1.25.126	10.1.25.127	10.1.25.65	143
5	LIBRE	10.1.25.128	255.255.255.128	/25	126	10.1.25.130 to 10.1.25.254	10.1.25.255	10.1.25.129	144
GABINETE I1									
PISO 1 - BLOCK D - SERVICIO DE CONSULTA EXTERNA									
NUM	GABINETE A	Subnet	Mask	/	Subnet Size	Host Range	Broadcast	Puerta enlace	VLAN
1	Datos_Gab_I1	10.1.26.0	255.255.254.0	/23	510	10.1.26.2 to 10.1.27.254	10.1.27.255	10.1.26.1	150
2	Voz_Gab_I1	10.1.28.0	255.255.255.0	/24	254	10.1.28.2 to 10.1.28.254	10.1.28.255	10.1.28.1	151
3	Impresoras_Gab_I1	10.1.29.0	255.255.255.192	/26	62	10.1.29.2 to 10.1.29.62	10.1.29.63	10.1.29.1	152
4	Wireless_Gab_I1	10.1.29.64	255.255.255.192	/26	62	10.1.29.66 to 10.1.29.126	10.1.29.127	10.1.29.65	153
5	LIBRE	10.1.29.128	255.255.255.128	/25	126	10.1.29.130 to 10.1.29.254	10.1.29.255	10.1.29.129	154
GABINETE I2									
PISO 1 - BLOCK A - SERVICIO DE CONSULTA EXTERNA									
NUM	GABINETE A	Subnet	Mask	/	Subnet Size	Host Range	Broadcast	Puerta enlace	VLAN
1	Datos_Gab_I2	10.1.30.0	255.255.254.0	/23	510	10.1.30.2 to 10.1.31.254	10.1.31.255	10.1.30.1	160
2	Voz_Gab_I2	10.1.32.0	255.255.255.0	/24	254	10.1.32.2 to 10.1.32.254	10.1.32.255	10.1.32.1	161
3	Impresoras_Gab_I2	10.1.33.0	255.255.255.192	/26	62	10.1.33.2 to 10.1.33.62	10.1.33.63	10.1.33.1	162

Fuente: Oficina de Soporte Informático del HNERM EsSALUD (2017).



Fase VIII. Migración Del Core OmniSwitch 9800 al Nexus 7000.

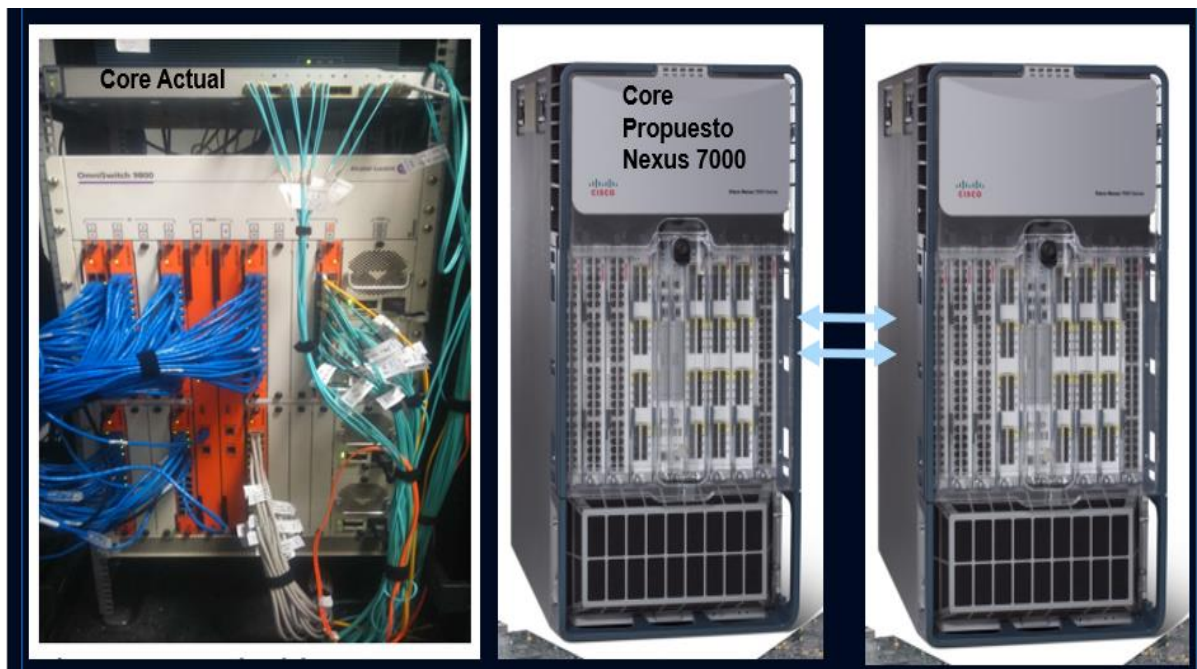


Figura 64. Migración del Core OmniSwitch 9800 al Core Nexus 7000 al 100%. Fuente: Oficina de Soporte Informático (2017).

Migración del CORE OmniSwitch 9800 al Core Nexus 7000 al 100%

Switches Cisco Nexus de la serie 7000

Cisco Nexus 7000 Series Switches crean la base de red para su próxima generación de centros de datos Unified Fabric y el núcleo del campus.

Switches modulares, incluyendo la serie Cisco Nexus 7000 y 7700, ofrecen un amplio conjunto de funciones Cisco NX-OS y herramientas de código abierto programables para despliegues de red definidos por software (SDN).

Ofrecen Ethernet Gigabit 10, 40 y 100 de alta densidad con aplicaciones concientes y análisis de rendimiento.



Cisco Nexus 7000 18-Slot Switch

- a. Diseñado para una futura escalabilidad de capacidad de conmutación de más de 15 terabits por segundo.
- b. Modular, flexible, escalable sistema operativo basado en Linux.
- c. Eficiente diseño de uso de energía y ventilación.
- d. Virtualización para la utilización eficiente de los recursos.
- e. Actualizaciones sin interrupciones ni pérdidas para evitar tiempo de inactividad del servicio.
- f. Operaciones del sistema discretas para minimizar el efecto de las actualizaciones y otras tareas de mantenimiento.
- g. API integral y abierta de Extensible Markup Language (XML) para opciones de gestión flexibles.
- h. Soporte de nuevas tecnologías sin actualizaciones totales.
- i. Plano de control y plano de datos de reenvío virtualizados para un rendimiento optimizado.
- j. Soporte a los estándares Ethernet emergentes 40 Gbps y 100 Gbps.

TABLA 14
Presupuesto Consolidado del HNERM EsSALUD

EQUIPO DE COMUNICACIONES	CANTIDAD	PRECIO \$	MONTO \$	DESCRIPCION
SWITCH TIPO I - NEXUS 7010	2	80000	160,000.00	Switch de Core Principal
SWITCH TIPO II	1	70000	70,000.00	Switch de Distribución para el Centro de Datos con puertos en fibra
SWITCH TIPO III	1	70000	70,000.00	Switch de Distribución para el Centro de Datos con puertos en cobre
SWITCH TIPO IV	70	35000	2,450,000.00	Switch de acceso de para servicios de voz, data, impresiones y wireless corporativo
SWITCH TIPO V	36	18000	648,000.00	Switch de acceso para servicios de videovigilancia. Soporte de POE+
SWITCH TIPO VI	13	35000	30,000.00	Switch de acceso para comunicación con equipos médicos
SWITCH TIPO VII	28	18000	30,000.00	Switch de acceso para comunicación con equipos médicos
CONTROLADORA DE REDES INALAMBRICAS	1	45000	45,000.00	Controlador de redes inalámbricas
PUNTOS DE ACCESO	350	2500	875,000.00	Puntos de acceso
PLATAFORMA DE GESTION	1	20000	20,000.00	Plataforma de gestión unificada de red inalámbrica y cableada
PLATAFORMA PARA EL CONTROL DE ACCESO	1	20000	20,000.00	Plataforma de control de acceso hacia la infraestructura de la .red
TRANSCIVER	450	1300	585,000.00	
			5,003,000.00	

Fuente: Oficina de Soporte Informático-HNERM EsSALUD - 2017

Nota: El Presente Cuadro muestra la Proyección de Costos para la Renovación de los Dispositivos de Conmutación del HNERM EsSALUD (2017).

ESCRIPCIÓN DE LOS TDR'S DE LOS CONMUTADORES EN GENERAL

Switch Tipo I

Cantidad de Equipos

Dos (2) Unidades

Características Generales

- El conmutador debe ser un chasis modular diseñado para soportar altas densidades de puertos gigabit Ethernet y 10-gigabit Ethernet. El equipo también soporta interfaces 40-gigabit Ethernet y 100-gigabit Ethernet.
- El conmutador debe contar con un plano de transporte de datos (tejido de conmutación) que podrá ser ampliado en demanda y en función de requerimientos de ancho de banda o redundancia. La ampliación de este tejido de conmutación se debe poder realizar durante la operación del equipo y sin interrumpir los flujos de datos existentes.



- c. El equipo deberá poseer una arquitectura de transporte de tráfico distribuida en la que las tarjetas de línea tendrán la capacidad de tomar decisiones de conmutación a nivel local con base en la información proveída por un plano de control/supervisión. Este plano de control deberá residir en un sistema redundante e independiente de tarjetas supervisoras que operarán de forma desacoplada del plano de transporte de datos mencionado en el punto anterior.
- d. Cada tarjeta de línea instalada en el chasis deberá tener conexiones múltiples a todos los diferentes módulos del tejido de conmutación existentes, de tal forma que, si algún de ellos fallara, deberá existir uno o más módulos de respaldo que provean redundancia interna de conexión en modalidad 1:1 o 2:1 como máximo. El sistema deberá dimensionarse con un mínimo de tres módulos de conmutación para así soportar la pérdida de un módulo de tejido sin perder en ningún momento la capacidad de conmutación característica de cada tarjeta de línea.
- e. El ancho de banda por ranura no debe ser inferior a 1 Tbps en full dúplex.
- f. El equipo debe tener al menos 8 ranuras para tarjetas de línea.
- g. La capacidad de conmutación total del equipo no debe ser inferior a 16 Tbps.
- h. Cada tarjeta de línea debe soportar al menos 1 millón de rutas en IPv4/IPv6.
- i. Cada puerto de 10 Gbps debe tener un buffer de ingreso no menor a 30 MB.
- j. Cada puerto de 40 Gbps debe tener un buffer de ingreso no menor a 100 MB.
- k. El equipo deberá contar con tarjetas supervisoras redundantes entre sí, las cuales deberán poder balancear las cargas a través de los módulos del tejido de conmutación. Si un módulo fallase, deberán balancear el tráfico en los restantes.
- l. Todas las tarjetas de línea, módulos de tejido de conmutación, tarjetas de control, fuentes de poder y ventiladores deberá poder ser retirados y reinsertados en el chasis durante la operación del mismo sin interrumpir el flujo de tráfico no-relacionado a través del mismo.
- m. Las fuentes de poder del equipo deben proveer redundancia N+1 y balanceo de cargas de tal forma que permitan alimentación energética completa proveniente de cualquiera de dos acometidas diferentes. El conmutador deberá poder operar al 100% de su capacidad en un escenario en el cual falle una fuente de poder física y también si una acometida eléctrica completa es interrumpida.

- n. Todos los ventiladores de enfriamiento del sistema deben ser físicamente redundantes y deben poder ser reemplazados mientras el equipo se encuentre en operación.
Si una bandeja de ventiladores fallase durante el funcionamiento del equipo, la bandeja de respaldo tendrá la capacidad de mantener el flujo de aire a través del mismo, y así mantener la temperatura a niveles nominales.
- o. La arquitectura del equipo debe soportar el estándar de fibra canal sobre Ethernet (FCoE) en todos sus puertos.
- p. Ambos conmutadores deben poder formar una instancia lógica de agregación de enlaces compartida de tal forma que otros equipos externos participando de esa instancia vean a ambos switches como un único conmutador lógico.
- q. El equipo debe incluir soporte de los protocolos de enrutamiento OSPF, BGP y IS-IS para IPv4 e IPv6.
- r. El conmutador debe soportar MPLS y LISP.
- s. Soporte de VXLAN (Virtual eXtensible Local Area Network) para la creación de topologías aisladas de tipo “overlay” de Capa 2 sobre Capa 3.
- t. Habilidad para crear fabrics basados en la tecnología de VXLAN mediante un plano de control propio del conmutador que evite el comportamiento nativo de “flooding/learning” de VXLAN. Es válido emplear algún tipo de protocolo de enrutamiento para este propósito.
- u. El conmutador debe contar con un mecanismo que permita a múltiples puertos de entrada tener acceso equitativo al ancho de banda de un único puerto de salida. Este mecanismo deberá valorar y arbitrar la utilización de las colas de entrada/salida de los puertos e impedir que el tráfico de ingreso sea bloqueado por saturación en puertos de salida. Se deberán poder definir prioridades a tipos específicos de tráfico para, así, asegurar un nivel de servicio sin pérdidas a los tipos de tráfico que lo requieran. Esta funcionalidad será indispensable para el uso de servicios de fibra canal sobre Ethernet.
- w. Todos los puertos del conmutador deben soportar el estándar de seguridad 802.1AE (AES-256) a velocidad de línea (sin bloqueo).



- x. Siguiendo el estándar 802.3ad, el conmutador debe tener capacidad de agrupación de hasta 10 puertos en un solo interface lógica para lograr una conexión de N por la velocidad máxima de la tecnología de los puertos agrupados.
La tecnología de los mismos podrá ser ethernet, fase-ethernet, gigabit-ethernet y 10/40/100 gigabit-ethernet. Esta agrupación de puertos debe poder ocurrir entre puertos de la misma tecnología pero que puedan estar en diferentes tarjetas de línea sobre el mismo chasis para lograr así conectividad de alta disponibilidad.
- y. Debe incluir soporte eficiente de tráfico de multimedios con base en multicast en la intranet por medio de Protocol Independent Multicast (en modos Sparse, Dense y Source Specific), Internet Group Management Protocol (IGMP). Debe soportar IGMP Snooping v1, v2 y v3.
- z. El conmutador debe soportar una estructura independiente de spanning-tree por vlan.
- aa. El conmutador debe tener soporte de 802.1s (MSTP) y 802.1w (RSTP)
- bb. El equipo debe soportar funcionalidades de IPv6. Estas funcionalidades deben incluir como mínimo: manejo de rutas en IPv6, OSPF, ping, telnet y tunneling de ipv4 a ipv6 y viceversa.
- cc. El conmutador debe soportar 802.1x. En particular interesa la autenticación de acceso a puertos y la asignación dinámica de vlans y políticas de calidad de servicio.
- dd. El equipo debe soportar “port mirroring” entre puertos (origen y destino) de la misma tarjeta, entre puertos de diferentes tarjetas y además entre puertos de diferentes chasis del mismo modelo del conmutador ofertado. Esto para facilitar el monitoreo de la red.
- ee. Con la finalidad de monitorear adecuadamente el uso del ancho de banda dentro de la institución el equipo debe estar en capacidad de identificar los usuarios que generan más tráfico hacia la red.
- ff. El equipo debe contar con la funcionalidad de hacer un rastreo en capa 2 (a través de la dirección MAC) y en capa 3 (a través de la dirección IP) de una estación en particular.
- gg. El equipo debe tener soporte de calidad de servicio (QoS) a través del uso de información de capas 2/3/4 tales como los bits de precedencia, frames 802.1p y puertos de capa 4.



Debe soportar colas múltiples con umbrales configurables y mecanismos de mapeo de bits ToS (Tipo de Servicio) contra bits de CoS (Clase de Servicio) para asegurar que los paquetes mantengan la calidad de servicio a la hora de traspasar las fronteras de capa 02 a capa 03 y viceversa, deberán contener las siguientes funcionalidades:

- a. Marcación de paquetes según 802.1p.
 - b. Limitación de ancho de banda por puerto.
 - c. Limitación de ancho de banda por puerto y prioridad.
 - d. Marcación de paquetes según IP TOS.
 - e. Clasificación a partir de 802.1p.
 - f. Clasificación a partir de IP TOS.
 - g. Limitación de ancho de banda por Vlan.
 - h. Limitación de ancho de banda por lista de acceso.
 - i. Weighted Round Robin
- hh. Desde el punto de vista de seguridad en capa 2, el conmutador debe estar en capacidad de realizar las siguientes funciones:
- a. Limitar la cantidad de direcciones MAC que un puerto puede tolerar.
 - b. Definir direcciones MAC específicas que un puerto va a conmutar. En caso de que una estación con una MAC diferente a las permitidas trate de acceder al puerto, el mismo debe poder bloquear la dirección específica o bloquearse completamente.
 - c. Para proteger la red de ataques de Denial of Service contra los servidores de DHCP, el conmutador deberá estar en capacidad de limitar la tasa de paquetes del tráfico de DHCP hacia estos servidores.
 - d. Para evitar que estaciones o servidores no autorizados personifiquen al servidor de DHCP, el conmutador deberá estar en capacidad de permitir únicamente el tráfico de solicitud de DHCP proveniente de puertos de acceso específicos. De la misma forma, es tráfico de respuesta de DHCP también se podrá limitar a puertos particulares.
 - e. Para evitar ataques de ARP spoofing, el conmutador debe tener algún mecanismo para permitir o denegar asociaciones IP-MAC en su tabla de



- ARP. Las asociaciones válidas se podrán introducir de forma manual en la configuración del conmutador o ser aprendidas dinámicamente a través de DHCP.
- f. El conmutador deberá contar con algún mecanismo para aislar el tráfico de broadcast y multicast entre puertos de la misma vlan.
 - g. El conmutador deberá contar con algún mecanismo para asociar direcciones IP con puertos específicos de tal forma que un usuario no pueda cambiar su dirección con la intención de obtener otros derechos de acceso. Las asociaciones válidas se podrán introducir de forma manual en la configuración del conmutador o ser aprendidas de forma dinámica a través de DHCP.
 - h. El conmutador deberá poder restringir el tráfico de uno o varios tipos de aplicaciones entre PCs o servidores que se encuentren dentro de una misma vlan y en la misma subnet sin que esto implique cambiarlos de vlan o cambiar su dirección IP.
 - i. Cada equipo debe incorporar inicialmente 02 interfaces 10 gigabit Ethernet sobre fibra. Se requiere que estos interfaces deben poder operar a velocidad de línea máxima sin bloqueo. Adicionalmente, se requiere que se provean los 24 transductores de dichos interfaces. Los transductores deben ser de la misma marca del fabricante del chasis.
 - j. El equipo debe contar con un sistema de monitoreo y administración fuera de línea del tipo “lights-out” dentro del mismo chasis. El mismo debe poder operar de forma independiente del sistema operativo principal y del procesador del conmutador. Este sistema deberá tener sus propios interfaces de red dedicados de tipo Ethernet 10/100 o 10/100/1000 (al menos dos). Estos puertos no deberán tener la opción de ser utilizados como puertos de conmutación de datos convencionales.
 - k. El equipo debe poder dar un informe completo en tiempo real sobre las sesiones establecidas a través de él. Este informe permitirá dimensionar a futuro el crecimiento de la red y debe incluir como mínimo los siguientes parámetros: direcciones ip (origen y destino), puertos tcp/udp (origen y destino), puerto físico de ingreso, puerto físico de egreso, conteo de

paquetes, conteo de bytes, estado del byte ToS, máscaras de la subnet (origen y destino) y sistemas autónomos (origen y destino). Esta información deberá poder ser enviada a algún servidor o equipo externo para ser contabilizada.

1. El conmutador deberá incluir una plataforma de administración centralizada basada en una interface gráfico tipo GUI (Graphical User Interface). Esta herramienta deberá permitir el aprovisionamiento, administración y monitoreo de procesos Local Area Network (LAN) como Storage Area Network (SAN). Adicionalmente, la plataforma de administración deberá estar en capacidad de realizar las siguientes funciones:
 - a. Realizar una validación de la configuración propuestas antes que la misma sea aplicada al sistema. Esta validación deberá realizarse contra un conjunto de reglas y atributos establecidos por el administrador.
 - b. Realizar una representación gráfica del mapa topológico de la red
 - c. Realizar la gestión de fallos del sistema.
 - d. Realizar el monitoreo del performance del equipo, mostrando como mínimo la información de la utilización de puertos, reporte del consumo de ancho de banda, reporte del conteo de errores, estadísticas de tráfico y reporte de violaciones de seguridad.
 - e. Realizar la administración de la plataforma basada en roles de usuarios.
 - f. Para propósitos de inventario, el sistema deberá tener información como el detalle de cada dispositivo.
 - g. Información de la topología de red y la configuración de la misma. Estas funcionalidades deberán brindar la flexibilidad de tener acceso a la información de los recursos físicos (chassis, supervisoras, tarjetas de puertos, ventiladores, fuentes de poder) o lógicos (direcciones IP, MAC, IDs de VLAN, listas de control de acceso, port channels) de la red.
 - h. Con la finalidad de evitar la operación deficiente del equipo o hasta una pérdida en el servicio por una configuración mal hecha, el sistema de administración deberá validar los cambios de configuración manuales antes de su puesta en operación en producción.



Este mecanismo deberá contemplar reglas para validación como por ejemplo la superposición de direcciones IP.

- i. Los mapas topológicos visuales que muestre esta herramienta deberán contener información como la configuración de los puertos, el chassis y el estado de los dispositivos físicos, así como las VLANs activas y los puertos bloqueados debido al protocolo STP (802.1d).
- j. Se deberá de permitir la configuración visual de tareas avanzadas como la creación de contextos virtuales en un switch de Core o la creación de portchannels (agregación de puertos) virtuales entre 2 chasises físicos.
- k. Con la finalidad de tener un control adecuado de los cambios de configuración en los switches, la herramienta de administración deberá mantener las últimas 50 versiones de cambios de configuración y realizar comparaciones entre versiones para entender exactamente los cambios realizados y su impacto. Los cambios de configuración también se deberán poder realizar de manera programada en algún tiempo determinado. En caso que se desee, el sistema deberá permitir regresar a una configuración pasada de manera granular en donde se decidan qué elementos de configuración pertenecen y cuáles no.
- l. Las actualizaciones de software se deberán poder hacer desde esta herramienta y deberá permitir la actualización del equipo, es decir, cambiar su software en operación de una versión a otra, sin afectar ningún tipo de servicio durante la actualización (cero paquetes perdidos o afectados). Ante un evento de actualización del sistema, la herramienta de administración deberá verificar el espacio disponible en disco para bajar la imagen, así como la compatibilidad de la configuración en operación con la nueva imagen. Las imágenes se deberán poder descargar utilizando servidores externos con servicios de TFTP, FTP o SFTP.
- m. El sistema deberá permitir la recolección de eventos de red y desplegarlos en una ventana de eventos. Cada evento deberá ser correlacionado a una funcionalidad de red. Las alarmas deberán ser mostradas con código de color dependiendo su criticidad.



Basado en esta información, la herramienta de administración deberá desplegar una calificación de la salud en general de la red.

- n. La herramienta de administración deberá permitir el control de acceso a los cambios de configuración basado en los roles de usuario. De esta manera se podrá controlar de manera granular el conjunto de tareas o cambios que un usuario puede o no realizar basado en su perfil de usuario. El acceso a la configuración del equipo puede ser vía Secure Shell SSHv2 o con SSL.
- o. La herramienta de administración deberá contar con una Interface de Programación de Aplicaciones (API, por sus siglas en inglés) basada en servicios web estándares de industria utilizando Simple Object Access Protocol (SOAP) y Extensible Markup Language (XML). De esta forma se pueden integrar tareas de monitoreo, administración y configuración del entorno de infraestructura de red del Datacenter a aplicaciones de terceros.

Administración y configuración de las siguientes funcionalidades de red:

Switcheo Ethernet:

- a. Puertos y agregación de puertos (port channel)
- b. VLANs y VLANs Privadas (PVLAN)
- c. Rapid Spanning Tree Protocol (RSTP) y Multi-Instance Spanning Tree Protocol (MISTP)

Seguridad de red:

- a. Listas de control de acceso (ACL), basadas en MAC, IP y VLAN IEEE 802.1X
- b. Autenticación, autorización, and registro de actividades (AAA)
- c. Capacidad de asegurar que los usuarios utilicen únicamente las direcciones previamente asignadas por el servidor DHCP autorizado (DHCP snooping).
- d. Capacidad de revisar que los paquetes ARP vienen de direcciones IP válidas
Prevenir el tráfico IP de direcciones IP con direcciones MAC que no correspondan a la tabla de DHCP Snooping



- e. Mecanismos para evitar que el tráfico en una red LAN sea afectado por una tormenta de tráfico broadcast, multicast o Unicast en una interface física.
- f. Limitar el número de direcciones MAC que se pueden conectar a un puerto, permitir la conexión a un puerto físico únicamente a un dispositivo basado en su dirección MAC.

- **General**

- a. Generación de contextos virtuales para un switch físico en particular
- b. Creación de un puerto lógico a partir de diferentes puertos físicos en 2 chassises distintos.
- c. Utilización de recursos de hardware con las estadísticas de la tabla de TCAM
- d. Configuración de puerto conmutado para análisis de tráfico (SPAN)
- e. Administración de imágenes del sistema operativo con actualización de software en servicio (In Service Software Upgrade – ISSU)
- f. Control de cambios de Configuraciones.

Switch Tipo II

Cantidad de Equipos

Una (1) Unidad

Características Generales

- a. Es requisito que el centro de datos incluya, dentro de su arquitectura, la capacidad de agregar alta densidad de servidores en equipos de acceso de propósito específico con capacidad de interfaces Ethernet a 1/10/25 Gbps.
- b. El conmutador de acceso para los servidores del centro de datos deberá soportar velocidades de línea de 1/10/25 Gigabit Ethernet sin bloqueo en todos sus puertos independientemente del tamaño de paquete y los servicios habilitados.
- c. Debe disponer de 48 interfaces SFP+ de 1/10/25 Gbps (las 3 velocidades deben ser soportadas) de las cuales 24 deben estar habilitadas con sus respectivos transceiver SFP+ 10GBaseSR.
- d. Debe incluir un mínimo de 06 puertos QSFP+ de 40/100 Gbps (distintos a los 48 puertos SFP+ mencionados anteriormente y sin cambio de hardware).

- e. Deberá manejar un rendimiento de hasta 3 tbps (nonblocking) con latencia no mayor a 2 microsegundos.
- f. Debe disponer de capacidad de Throughput mínimo de 2 Bpps.
- g. Ambos conmutadores deben poder formar una instancia lógica de agregación de enlaces compartida de tal forma que otros equipos externos participando de esa instancia vean a ambos switches como un único conmutador lógico.
- h. El conmutador debe soportar una cantidad mínima de 128 000 rutas IPv4.
- i. Se deben soportar hasta 8,000 rutas de multicast.
- j. Se deben soportar hasta 2,000 grupos de IGMP snooping.
- k. Se deben soportar hasta 8 puertos conformando un enlace lógico de agregación (channel). El conmutador debe permitir hasta 32 enlaces lógicos de agregación de puertos (channels).
- l. Se debe soportar hasta 2 sesiones de “port mirroring” o “span”. Se debe soportar un mínimo de 500 instancias de RPVST+.
- m. Deberá contar con mecanismo de inteligencia programable sobre la aplicación (api) que permita a los operadores administrar el switches a través de llamadas tipo rpcs, javascript o xml sobre una infraestructura http/https
- n. Deberá contar con mecanismo de acceso tipo linux shell el cual habilite la configuración del mismo a través de scripts tipo linux.
- o. Deberá contar con mecanismos de actualización e instalación de parches en línea.
- p. Soporte de VXLAN (Virtual eXtensible Local Area Network) para la creación de redes aisladas de Capa 2 sobre Capa 3 e implementación de topologías multitenant.
- q. Se debe soportar VXLAN routing y VXLAN bridging de forma nativa a velocidad de línea.
- r. Habilidad para crear fabrics basados en la tecnología de VXLAN. Se debe incluir el licenciamiento y software necesarios para proveer una interfaz gráfica intuitiva que permita administrar y monitorear el Fabric de VXLAN. El software debe permitir administrar el Fabric formado por todos los conmutadores del centro de datos como una única entidad, evitando así la necesidad de ejercer controles/comandos switch por switch. De la misma forma, la herramienta debe permitir visualizar la topología de forma gráfica y completar flujos de tareas sin



- requerirse de conocimiento de los protocolos de redes que se ejecutan en la red “underlay”. Deberá soportar rutas estáticas y dinámicas.
- s. Soporte instalado de IGMPv1, IGMPv2, IGMPv3 en IPv4, enrutamiento estático IPv4 e IPv6, RIPv2, VRRPv2, VRRPv3, OSPFv2, OPSFv3, BGP, ISIS, GRE.
 - t. Soporte de 802.1p, CoS y DiffServ (DSCP).
 - u. 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).
 - v. Soporte de ACL’s por puerto, basados en información de Capas 2, 3 y 4.
 - w. El equipo debe contar con la última versión liberada del sistema operativo con que cuente el fabricante.
 - x. El sistema operativo del conmutador debe ser de diseño modular.
 - y. El sistema operativo debe contar con mecanismos de servicio continuo con el objetivo de evitar interrupción del servicio ante operaciones de mantenimiento y actualización de software.
 - z. El sistema operativo del conmutador debe contar con mecanismos de sobrevivencia que permita correr los procesos críticos en espacios de memoria reservados independientes de cualquier otro proceso o incluso del kernel.
 - aa. El sistema operativo debe incluir como parte de él mismo, un analizador de paquetes para la función de monitoreo y la corrección del tráfico en el plano de control.
 - bb. Soportar un mínimo de 04 (cuatro) niveles de administración por consola, telnet y SSH. De no contar con el mínimo de niveles requerido, el equipo deberá contar con soporte habilitado TACACS y/o TACACS+ o protocolo similar. Además, el proveedor implementará una solución de administración centralizada que incluya el servidor o software que sean necesarios para cumplir cabalmente con el requerimiento. Administración por Interface de línea de comandos, SNMPv3 vía Software e interface Web con SSL. Soporte de métodos para exportar datos sobre flujos de tráfico a los sistemas de gestión, tales como SFLOW, NETFLOW, IPFIX o NETSTREAM (Como mínimo uno de ellos).
 - cc. Soporte de múltiples niveles de privilegios de acceso por consola para los administradores ya sea localmente o remotamente por Telnet, SSH. Soporte de los



- protocolos SNMPv1, SNMPv2c, SNMPv3, FTP, TFTP, SCP y/o SFTP, HTTP, HTTPS. Debe manejar autenticación, autorización y registro de actividades
- dd. El equipo debe tener soporte de calidad de servicio (QoS) a través del uso de información de capas 2/3/4 tales como los bits de precedencia, frames 802.1p y puertos de capa 4. Debe soportar colas múltiples con umbrales configurables y mecanismos de mapeo de bits DSCP contra bits de CoS para asegurar que los paquetes mantengan la calidad de servicio a la hora de traspasar las fronteras de capa 2 a capa 3 y viceversa.
- ee. Se debe poder definir direcciones MAC específicas que un puerto va a conmutar. En caso de que una estación con una MAC diferente a las permitidas trate de acceder al puerto, el mismo debe poder bloquear la dirección específica o bloquearse completamente.
- ff. Para evitar que estaciones o servidores no autorizados personifiquen al servidor de DHCP, el conmutador deberá estar en capacidad de permitir únicamente el tráfico de solicitud de DHCP proveniente de puertos de acceso específicos. De la misma forma, es tráfico de respuesta de DHCP también se podrá limitar a puertos particulares.
- gg. Para evitar ataques de ARP spoofing, el conmutador debe tener algún mecanismo para permitir o denegar asociaciones IP-MAC en su tabla de ARP. Las
- hh. asociaciones válidas se podrán introducir de forma manual en la configuración del conmutador o ser aprendidas dinámicamente a través de DHCP.
- ii. El conmutador deberá contar con algún mecanismo para aislar el tráfico de broadcast y multicast entre puertos de la misma vlan.
- jj. El conmutador deberá contar con algún mecanismo para asociar direcciones IP con puertos específicos de tal forma que un usuario no pueda cambiar su dirección con la intención de obtener otros derechos de acceso. Las asociaciones válidas se podrán introducir de forma manual en la configuración del conmutador o ser aprendidas de forma dinámica a través de DHCP.
- kk. El conmutador deberá poder restringir el tráfico de uno o varios tipos de aplicaciones entre PCs o servidores que se encuentren dentro de una misma vlan y en la misma subnet sin que esto implique cambiarlos de vlan o cambiar su dirección IP.



El conmutador deberá soportar los siguientes estándares:

1. IEEE 802.1w
2. IEEE 802.1s
3. IEEE 802.1x
4. IEEE 802.1ab
5. IEEE 802.1d
6. IEEE 802.1p qos/cos
7. IEEE 802.1q
8. IEEE 802.1w
9. IEEE 802.1s
10. IEEE 802.1ad
11. IEEE 802.3x
12. IEEE 802.3ab 1000base-t
13. IEEE 802.3z
14. IEEE 802.3ae 10 gigabit ethernet
15. IEEE 802.3ba 40 gigabit ethernet

El conmutador deberá soportar los siguientes RFCs:

1. RFC 2460 ipv6
2. RFC 2461 neighbor discovery (mld) para ipv6
3. RFC 2462 autoconfiguración de dirección ipv6
4. RFC 2463 icmpv6

Switch Tipo III**Cantidad de Equipos**

Una (1) Unidad

Características Generales

- a. Es requisito que el centro de datos incluya, dentro de su arquitectura, la capacidad de agregar alta densidad de servidores en equipos de acceso de propósito específico con capacidad de interfaces Ethernet a 1/10 Gbps.



- b. El conmutador de acceso para los servidores del centro de datos deberá soportar velocidades de línea de 1/10 Gigabit Ethernet sin bloqueo en todos sus puertos independientemente del tamaño de paquete y los servicios habilitados.
- c. Debe disponer de 48 interfaces de 1/10 GE en cobre.
- d. Debe incluir un mínimo de 06 puertos QSFP+ de 40/100 Gbps (distintos a los 48 puertos SFP+ mencionados anteriormente y sin cambio de hardware).
- e. Deberá manejar un rendimiento de hasta 2 tbps (nonblocking) con latencia no mayor a 2 microsegundos.
- f. Debe disponer de capacidad de Throughput mínimo de 1.5 Bpps.
- g. El conmutador debe tener buffer compartido de sistema no menor a 16 MB Ambos conmutadores deben poder formar una instancia lógica de agregación de enlaces compartida de tal forma que otros equipos externos participando de esa instancia vean a ambos switches como un único conmutador lógico.
- h. El conmutador debe soportar una cantidad mínima de 128 000 rutas IPv4.
- i. El equipo debe tener una capacidad mínima de 130,000 registros de direcciones MAC. Se deben soportar hasta 8,000 rutas de multicast.
- j. Se deben soportar hasta 2,000 grupos de IGMP snooping.
- k. Se deben soportar hasta 8 puertos conformando un enlace lógico de agregación (channel).
- l. El conmutador debe permitir hasta 32 enlaces lógicos de agregación de puertos (channels).
- m. Se debe soportar hasta 2 sesiones de “port mirroring” o “spanSe debe soportar un mínimo de 500 instancias de RPVST+.
- n. Deberá contar con mecanismo de inteligencia programable sobre la aplicación (api) que permita a los operadores administrar el switches a través de llamadas tipo rpcs, javascript o xml sobre una infraestructura http/https
- o. Deberá contar con mecanismos de acceso tipo linux shell el cual habilite la configuración del mismo a través de scripts tipo linux.
- p. Deberá contar con mecanismos de actualización e instalación de parches en línea.
- q. Soporte de VXLAN (Virtual eXtensible Local Area Network) para la creación de redes aisladas de Capa 2 sobre Capa 3 e implementación de topologías multitenant.



- r. Se debe soportar VXLAN routing y VXLAN bridging de forma nativa a velocidad de línea.
- s. Habilidad para crear fabrics basados en la tecnología de VXLAN. Se debe incluir el licenciamiento y software necesarios para proveer una interfaz gráfica intuitiva que permita administrar y monitorear el Fabric de VXLAN.
- t. El software debe permitir administrar el Fabric formado por todos los conmutadores del centro de datos como una única entidad, evitando así la necesidad de ejercer controles/comandos switch por switch. De la misma forma, la herramienta debe permitir visualizar la topología de forma gráfica y completar flujos de tareas sin requerirse de conocimiento de los protocolos de redes que se ejecutan en la red “underlay”. Deberá soportar rutas estáticas y dinámicas.
- u. Soporte instalado de IGMPv1, IGMPv2, IGMPv3 en IPv4, enrutamiento estático IPv4 e IPv6, RIPv2, VRRPv2, VRRPv3, OSPFv2, OPSFv3, BGP, ISIS, GRE.
- v. Soporte de 802.1p, CoS y DiffServ (DSCP).
- w. 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).
- x. Soporte de ACL’s por puerto, basados en información de Capas 2, 3 y 4.
- y. El equipo debe contar con la última versión liberada del sistema operativo con que cuente el fabricante.
- z. El sistema operativo del conmutador debe ser de diseño modular.
- aa. El sistema operativo debe contar con mecanismos de servicio continuo con el objetivo de evitar interrupción del servicio ante operaciones de mantenimiento y actualización de software.
- bb. El sistema operativo del conmutador debe contar con mecanismos de sobrevivencia que permita correr los procesos críticos en espacios de memoria reservados independientes de cualquier otro proceso o incluso del kernel.
- cc. El sistema operativo debe incluir como parte de él mismo, un analizador de paquetes para la función de monitoreo y la corrección del tráfico en el plano de control.
- dd. Soportar un mínimo de 04 (cuatro) niveles de administración por consola, telnet y SSH. De no contar con el mínimo de niveles requerido, el equipo deberá contar con soporte habilitado TACACS y/o TACACS+ o protocolo similar.



Además, el proveedor implementará una solución de administración centralizada que incluya el servidor o software que sean necesarios para cumplir cabalmente con el requerimiento.

- ee. Administración por Interface de línea de comandos, SNMPv3 vía Software e interface Web con SSL. Soporte de métodos para exportar datos sobre flujos de tráfico a los sistemas de gestión, tales como SFLOW, NETFLOW, IPFIX o NETSTREAM (Como mínimo uno de ellos).
- ff. Soporte de múltiples niveles de privilegios de acceso por consola para los administradores ya sea localmente o remotamente por Telnet, SSH. Soporte de los protocolos SNMPv1, SNMPv2c, SNMPv3, FTP, TFTP, SCP y/o SFTP, HTTP, HTTPS. Debe manejar autenticación, autorización y registro de actividades.
- gg. El equipo debe tener soporte de calidad de servicio (QoS) a través del uso de información de capas 2/3/4 tales como los bits de precedencia, frames 802.1p y puertos de capa 4. Debe soportar colas múltiples con umbrales configurables y mecanismos de mapeo de bits DSCP contra bits de CoS para asegurar que los paquetes mantengan la calidad de servicio a la hora de traspasar las fronteras de capa 2 a capa 3 y viceversa.
- hh. Se debe poder definir direcciones MAC específicas que un puerto va a conmutar. En caso de que una estación con una MAC diferente a las permitidas trate de acceder al puerto, el mismo debe poder bloquear la dirección específica o bloquearse completamente.
- ii. Para evitar que estaciones o servidores no autorizados personifiquen al servidor de DHCP, el conmutador deberá estar en capacidad de permitir únicamente el tráfico de solicitud de DHCP proveniente de puertos de acceso específicos. De la misma forma, es tráfico de respuesta de DHCP también se podrá limitar a puertos particulares.
- jj. Para evitar ataques de ARP spoofing, el conmutador debe tener algún mecanismo para permitir o denegar asociaciones IP-MAC en su tabla de ARP. Las asociaciones válidas se podrán introducir de forma manual en la configuración del conmutador o ser aprendidas dinámicamente a través de DHCP.
- kk. El conmutador deberá contar con algún mecanismo para aislar el tráfico de broadcast y multicast entre puertos de la misma vlan.



- ll. El conmutador deberá contar con algún mecanismo para asociar direcciones IP con puertos específicos de tal forma que un usuario no pueda cambiar su dirección con la intención de obtener otros derechos de acceso. Las asociaciones válidas se podrán introducir de forma manual en la configuración del conmutador o ser aprendidas de forma dinámica a través de DHCP.
- mm. El conmutador deberá poder restringir el tráfico de uno o varios tipos de aplicaciones entre PCs o servidores que se encuentren dentro de una misma vlan y en la misma subnet sin que esto implique cambiarlos de vlan o cambiar su dirección IP.

El conmutador deberá soportar los siguientes estándares:

1. IEEE 802.1w
2. IEEE 802.1s
3. IEEE 802.1x
4. IEEE 802.1ab
5. IEEE 802.1d
6. IEEE 802.1p qos/cos
7. IEEE 802.1q
8. IEEE 802.1w
9. IEEE 802.1s
10. IEEE 802.1ad
11. IEEE 802.3x
12. IEEE 802.3ab 1000base-t
13. IEEE 802.3z
14. IEEE 802.3ae 10 gigabit ethernet
15. IEEE 802.3ba 40 gigabit ethernet

El conmutador deberá soportar los siguientes RFCs:

1. RFC 2460 ipv6
2. RFC 2461 neighbor discovery (mld) para ipv6
3. RFC 2462 autoconfiguración de dirección ipv6
4. RFC 2463 icmpv6

Switch Tipo IV

Cantidad De Equipos

Setenta (70) Unidades

Hardware

- a. Switch capa 2 y capa 3
- b. Debe contar con al menos 48 puertos de acceso 10/100/1000 PoE/PoE+ (IEEE 802.3at) en cobre RJ45 con autonegociación
- c. Puertos uplink: Debe contar con al menos 2 puertos 10 Gigabit Ethernet tipo SFP. Estos puertos de uplink no deben bloquear puertos de acceso, maximizando así la cantidad de puertos totales por switch.
- d. Debe tener una capacidad total para entregar energía a los dispositivos conectados a sus puertos de al menos 740W, lo que permita cubrir cada uno de los 48 puertos con al menos 15W. Por lo menos la mitad de los mismos debe de poder entregar POE+.
- e. Leds indicadores de operación por puerto.
- f. Capacidad mínima de conmutación local de transmisión de 108Gbps
- g. Capacidad mínima de reenvío de 130 Mpps.
- h. Capacidad para operar con al menos 8000 direcciones MAC.
- i. El switch debe tener la capacidad de poder formar un stack de al menos 8 switches con un puerto de stack dedicado, dando como resultado del stack un plano de datos unificado, una sola configuración y una sola IP de gestión para todo el grupo de switches. Si se ofrece un módulo independiente, este debe de ser de tipo hotswap. La comunicación entre los switches dentro del stack debe ser de al menos 80Gbps full dúplex y no debe usar ningún puerto fijo mencionado en puntos anteriores.
- j. Fuente de poder hotswap con alimentación de 100 a 240VAC, 9 a 4A, 50 o 60Hz. Debe incluir fuente de poder redundante interna hotswap.
- k. Montable en rack de 19”

Software

- a. Soporte para 250 VLAN como mínimo

- b. Soporte de Spanning Tree IEEE 802.1d, así como las mejoras tales como convergencia rápida (RST 802.1w) y múltiples instancias (MST 802.1s).
- c. Capacidad de operación de puertos en half y full dúplex
- d. Soporte de NTP
- e. Soporte de DHCP para IPv4 e IPv6.
- f. Soporte de protocolos de transferencia de archivos TFTP, FTP, RCP, SCP.
- g. Procesos de debug para análisis en caso de fallas.
- h. Agregación de puertos, LACP, IEEE 802.3ad, de modo que se pueda usar cualquier puerto del mismo tipo y velocidad.
- i. Soporte embebido de mecanismos de detección de fallas en cables de cobre y conectores de fibra óptica.
- j. Soporte de Multicast IGMPv1, v2 y v3 Snooping.
- k. Soportar al menos 1000 grupos IGMP en IPv4
- l. Soporte de IGMP snooping para IPv4 e IPv6 MLD v1 y v2
- m. Software actualizable. Incluir la última versión disponible.
- n. Enrutamiento dinámico: RIP, OSPF, PBR.

Mecanismos De Gestión

- a. Puerto de Consola para gestión local con puerto RJ 45.
- b. Puerto Ethernet 10/100 dedicado para administración fuera de banda.
- c. Soporte de Telnet, HTTP y SSH para gestión remota.
- d. Registro de eventos vía Syslog
- e. Soporte de “port mirroring” por puerto y por VLAN.
- f. Soporte de SNMP v1, SNMP v2c, SNMP v3.
- g. Debe permitir Administración vía Web.
- h. Soporte del estándar IEEE 802.1AB (LLDP: Link Layer Discovery Protocol) para intercambio de información de dispositivos en redes multivendor.
- i. El equipo debe de poder soportar Netflow, sFlow o similares para el análisis de tráfico.

Mecanismo De Seguridad

- a. El switch debe tener la capacidad de limitar la cantidad de direcciones MAC aprendidas en un puerto para evitar ataques MAC address flooding que llenen la tabla de direcciones MAC del switch.



- b. Soporte de mecanismos para evitar ataques tipo DoS y MITM, basados en STP y DHCP, así como “VLAN Hopping”, “DHCP Rogue Server”.
- c. Filtros aplicables por puerto.
- d. Filtros basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP.
- e. Soporte de autenticación 802.1x con asignación dinámica de VLAN.
- f. Control de acceso centralizado por RADIUS, ya sea para los administradores del switch como para los usuarios de la red que se autentican vía 802.1x.
- g. Soporte de flexibilidad en la autenticación mediante 802.1x, que permita usar un perfil para invitados, autenticación por MAC y autenticación 1x de manera dinámica.
- h. Soporte de movilidad de MAC en esquemas 802.1x que permita la conexión a un puerto y en caso el usuario se mueva a otro dentro de la red, pueda pasar por el proceso de autenticación sin inconvenientes.

Mecanismo de Calidad de Servicio

- a. Soporte de Calidad de Servicio QoS.
- b. Manejo de prioridad a nivel de colas, cuatro colas de salida por puerto basado en hardware.
- c. IEEE 802.1p Clase de Servicio, CoS y DSCP
- d. Marcado y clasificación de paquetes basado en dirección IP origen y destino, MAC origen y destino y número de puertos TCP y UDP.
- e. Configuración automática de QoS

Mecanismo de Protocolos Estándar

- a. IEEE 802.1Q VLAN
- b. IEEE 802.3ah (100BASE-X single/multimode fiber only)
- c. IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports
- d. IEEE 802.3 10BASE-T
- e. IEEE 802.3u 100BASE-TX
- f. IEEE 802.3ab 1000BASE-T
- g. IEEE 802.3z 1000BASE-X



Switch Tipo V

Cantidad de Equipos

Treinta y Seis (36) Unidades

Características Generales

- a. Debe contar con al menos 24 puertos de acceso 10/100/1000 PoE/PoE+ (IEEE 802.3at) en cobre RJ45 con autonegociación
- b. Puertos uplink: Debe de contar con al menos 02 puertos SFP+ para el soporte de 10G. Estos puertos de uplink no deben bloquear puertos de acceso, maximizando así la cantidad de puertos totales por switch.
- c. Fuente de poder con alimentación de 100 a 240VAC, 9 a 4A, 50 o 60Hz
- d. Soporte de redundancia en fuentes internas de poder para maximizar la disponibilidad. Estas fuentes deben de ser reemplazables en caliente.
- e. Debe tener una capacidad total para entregar energía a POE a 15.4W y POE+ a 30W a todos los puertos de manera simultánea.
- f. Leds indicadores de operación por puerto.
- g. Capacidad mínima de conmutación local de transmisión de 80 Gbps.
- h. Capacidad mínima de reenvío de 65 Mpps.
- i. Capacidad para operar con al menos 32k direcciones MAC.
- j. Montable en rack de 19"
- k. El switch debe tener la capacidad de poder formar un stack de al dando como resultado del stack un plano de datos unificado, una sola configuración y una sola IP de gestión para todo el grupo de switches. Características mínimas esperadas del stack:
 1. Comunicación entre los switches dentro del stack debe ser de al menos 150Gbps.
 2. Capacidad de poder agregar o retirar miembros al stack sin impactar los servicios.
- l. El sistema operativo de la solución debe de ser modular.
- m. Soporte para 1000 VLAN como mínimo
- n. Soporte de Spanning Tree IEEE 802.1d, así como las mejoras tales como convergencia rápida (RST 802.1w) y múltiples instancias (MST 802.1s).
- o. Capacidad de operación de puertos en half y full dúplex



- p. Soporte de NTP
- q. Soporte de DHCP para IPv4 e IPv6.
- r. Soporte de protocolos de transferencia de archivos TFTP, FTP, SCP.
- s. Agregación de puertos, LACP, IEEE 802.3ad, de modo que se pueda usar cualquier puerto del mismo tipo y velocidad.
- t. Soporte embebido de mecanismos de detección de fallas en cables de cobre y conectores de fibra óptica.
- u. Soporte de Multicast IGMPv1, v2 y v3 Snooping.
- v. Soportar al menos 1000 grupos IGMP en IPv4
- w. Soporte de IGMP snooping para IPv4 e IPv6 MLD v1 y v2
- x. Software actualizable. Incluir la última versión disponible.
- y. Soporte de enrutamiento dinámico y estático, como mínimo:
 - 1. RIP
 - 2. OSPF
- z. Soporte de tecnologías de Gateway para usuario como VRRP o similares.
- aa. Soporte de Multicast: PIM-SM y PIM-DM como mínimo.
- bb. Soporte de PBR o similares.
- cc. Puerto de Consola para gestión local con puerto RJ 45.
- dd. Puerto Ethernet 10/100 dedicado para administración fuera de banda.
- ee. Soporte de Telnet, HTTP y SSH para gestión remota
- ff. Registro de eventos vía Syslog
- gg. Soporte de SNMP v1, SNMP v2c, SNMP v3.
- hh. Debe permitir Administración vía Web.
- ii. Soporte del estándar IEEE 802.1AB (LLDP: Link Layer Discovery Protocol) para intercambio de información de dispositivos en redes multivendor.
- jj. Soportar múltiples niveles de privilegios de acceso (mínimo 4) por puerto de consola o Telnet para administración. Indicar la cantidad de niveles soportados.
- kk. Procesos de debug para análisis en caso de fallas.
- ll. El switch debe tener la capacidad de limitar la cantidad de direcciones MAC aprendidas en un puerto para evitar ataques MAC address flooding que llenen la tabla de direcciones MAC del switch.



- mm. Soporte de mecanismos para evitar ataques tipo DoS y MITM, basados en STP y DHCP, así como “VLAN Hopping”, “DHCP Rogue Server”.
- nn. Filtros aplicables por puerto.
- oo. Filtros basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP.
- pp. Soporte de autenticación 802.1x con asignación dinámica de VLAN y asignación dinámica de listas de control de acceso (ACL).
- qq. Control de acceso centralizado por RADIUS, ya sea para los administradores del switch como para los usuarios de la red que se autentican vía 802.1x.
- rr. Autenticación, Autorización y Accounting para administradores de red usando TACACS+.
- ss. Soporte de flexibilidad en la autenticación mediante 802.1x, que permita usar un perfil para invitados, autenticación por MAC y autenticación 1x de manera dinámica, asegurando que un dispositivo/usuario que se conecte tenga algún método disponible de autenticación.
- tt. Soporte de 802.1x, autenticación por MAC (MAB) y Web Authentication de manera dinámica para usuarios que se conectan detrás del teléfono.
- uu. Soporte de Calidad de Servicio QoS.
- vv. Manejo de prioridad a nivel de colas, ocho colas de salida por puerto basado en hardware, debe de incluir al menos una cola de prioridad.
- ww. IEEE 802.1p Clase de Servicio, CoS y DSCP
 - xx. Marcado y clasificación de paquetes basado en dirección IP origen y destino, MAC origen y destino y número de puertos TCP y UDP.
 - yy. Configuración automática de QoS
 - zz. Soporte de “port mirroring” por puerto y por VLAN.
- aaa. Soporte de múltiples sesiones de “port mirroring” así como "port mirroring" remoto.

Switch Tipo VI

Cantidad de Equipos

Trece (13) Unidades

Características Generales



- a. Debe contar con al menos 24 puertos de acceso 10/100/1000 en cobre RJ45 con autonegociación.
- b. Puertos uplink: Debe de contar con al menos 02 puertos SFP+ para el soporte de 10G. Estos puertos de uplink no deben bloquear puertos de acceso, maximizando así la cantidad de puertos totales por switch.
- c. Fuente de poder con alimentación de 100 a 240VAC, 9 a 4A, 50 o 60Hz
- d. Soporte de redundancia en fuentes internas de poder para maximizar la disponibilidad. Estas fuentes deben de ser reemplazables en caliente.
- e. Leds indicadores de operación por puerto.
- f. Capacidad mínima de conmutación local de transmisión de 80 Gbps.
- g. Capacidad mínima de reenvío de 65 Mpps.
- h. Capacidad para operar con al menos 32k direcciones MAC.
- i. Montable en rack de 19”
- j. El switch debe tener la capacidad de poder formar un stack de al dando como resultado del stack un plano de datos unificado, una sola configuración y una sola IP de gestión para todo el grupo de switches. Características mínimas esperadas del stack:
 1. Comunicación entre los switches dentro del stack debe ser de al menos 150Gbps.
 2. Capacidad de poder agregar o retirar miembros al stack sin impactar los servicios.
- k. El sistema operativo de la solución debe de ser modular.
- l. Soporte para 1000 VLAN como mínimo
- m. Soporte de Spanning Tree IEEE 802.1d, así como las mejoras tales como convergencia rápida (RST 802.1w) y múltiples instancias (MST 802.1s).
- n. Capacidad de operación de puertos en half y full dúplex
- o. Soporte de NTP
- p. Soporte de DHCP para IPv4 e IPv6.
- q. Soporte de protocolos de transferencia de archivos TFTP, FTP, SCP.
- r. Agregación de puertos, LACP, IEEE 802.3ad, de modo que se pueda usar cualquier puerto del mismo tipo y velocidad.



- s. Soporte embebido de mecanismos de detección de fallas en cables de cobre y conectores de fibra óptica.
- t. Soporte de Multicast IGMPv1, v2 y v3 Snooping.
- u. Soportar al menos 1000 grupos IGMP en IPv4
- v. Soporte de IGMP snooping para IPv4 e IPv6 MLD v1 y v2
- w. Software actualizable. Incluir la última versión disponible.
- x. Soporte de enrutamiento dinámico y estático, como mínimo:
 - 1. RIP
 - 2. OSPF
- y. Soporte de tecnologías de Gateway para usuario como VRRP o similares.
- z. Soporte de Multicast: PIM-SM y PIM-DM como mínimo.
- aa. Soporte de PBR o similares.
- bb. Puerto de Consola para gestión local con puerto RJ 45.
- cc. Puerto Ethernet 10/100 dedicado para administración fuera de banda.
- dd. Soporte de Telnet, HTTP y SSH para gestión remota
- ee. Registro de eventos vía Syslog
- ff. Soporte de SNMP v1, SNMP v2c, SNMP v3.
- gg. Debe permitir Administración vía Web.
- hh. Soporte del estándar IEEE 802.1AB (LLDP: Link Layer Discovery Protocol) para intercambio de información de dispositivos en redes multivendor.
- ii. Soportar múltiples niveles de privilegios de acceso (mínimo 4) por puerto de consola o Telnet para administración. Indicar la cantidad de niveles soportados.
- jj. Procesos de debug para análisis en caso de fallas.
- kk. El switch debe tener la capacidad de limitar la cantidad de direcciones MAC aprendidas en un puerto para evitar ataques MAC address flooding que llenen la tabla de direcciones MAC del switch.
- ll. Soporte de mecanismos para evitar ataques tipo DoS y MITM, basados en STP y DHCP, así como “VLAN Hopping”, “DHCP Rogue Server”.
- mm. Filtros aplicables por puerto.
- nn. Filtros basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP.

- oo. Soporte de autenticación 802.1x con asignación dinámica de VLAN y asignación dinámica de listas de control de acceso (ACL).
- pp. Control de acceso centralizado por RADIUS, ya sea para los administradores del switch como para los usuarios de la red que se autentican vía 802.1x.
- qq. Autenticación, Autorización y Accounting para administradores de red usando TACACS+.
- rr. Soporte de flexibilidad en la autenticación mediante 802.1x, que permita usar un perfil para invitados, autenticación por MAC y autenticación 1x de manera dinámica, asegurando que un dispositivo/usuario que se conecte tenga algún método disponible de autenticación.
- ss. Soporte de 802.1x, autenticación por MAC (MAB) y Web Authentication de manera dinámica para usuarios que se conectan detrás del teléfono.
- tt. Soporte de Calidad de Servicio QoS.
- uu. Manejo de prioridad a nivel de colas, ocho colas de salida por puerto basado en hardware, debe de incluir al menos una cola de prioridad.
- vv. IEEE 802.1p Clase de Servicio, CoS y DSCP
- ww. Marcado y clasificación de paquetes basado en dirección IP origen y destino, MAC origen y destino y número de puertos TCP y UDP.
- xx. Configuración automática de QoS
- yy. Soporte de “port mirroring” por puerto y por VLAN.
- zz. Soporte de múltiples sesiones de “port mirroring” así como "port mirroring" remoto.

Switch Tipo VII

Cantidad de Equipos

Veintiocho (28) Unidades

Características Generales

- a. Debe contar con al menos 48 puertos de acceso 10/100/1000 en cobre RJ45 con autonegociación.
- b. Puertos uplink: Debe de contar con al menos 02 puertos SFP+ para el soporte de 10G. Estos puertos de uplink no deben bloquear puertos de acceso, maximizando así la cantidad de puertos totales por switch.



- c. Fuente de poder con alimentación de 100 a 240VAC, 9 a 4A, 50 o 60Hz
- d. Soporte de redundancia en fuentes internas de poder para maximizar la disponibilidad. Estas fuentes deben de ser reemplazables en caliente.
- e. Leds indicadores de operación por puerto.
- f. Capacidad mínima de conmutación local de transmisión de 170 Gbps.
- g. Capacidad mínima de reenvío de 100 Mpps.
- h. Capacidad para operar con al menos 32k direcciones MAC.
- i. Montable en rack de 19”
- j. El switch debe tener la capacidad de poder formar un stack de al, dando como resultado del stack un plano de datos unificado, una sola configuración y una sola IP de gestión para todo el grupo de switches. Características mínimas esperadas del stack:
 - 1. Comunicación entre los switches dentro del stack debe ser de al menos 150Gbps.
 - 2. Capacidad de poder agregar o retirar miembros al stack sin impactar los servicios.
- k. El sistema operativo de la solución debe de ser modular.
 - l. Soporte para 1000 VLAN como mínimo
- m. Soporte de Spanning Tree IEEE 802.1d, así como las mejoras tales como convergencia rápida (RST 802.1w) y múltiples instancias (MST 802.1s).
- n. Capacidad de operación de puertos en half y full dúplex
- o. Soporte de NTP
- p. Soporte de DHCP para IPv4 e IPv6.
- q. Soporte de protocolos de transferencia de archivos TFTP, FTP, SCP.
- r. Agregación de puertos, LACP, IEEE 802.3ad, de modo que se pueda usar cualquier puerto del mismo tipo y velocidad.
- s. Soporte embebido de mecanismos de detección de fallas en cables de cobre y conectores de fibra óptica.
- t. Soporte de Multicast IGMPv1, v2 y v3 Snooping.
- u. Soportar al menos 1000 grupos IGMP en IPv4
- v. Soporte de IGMP snooping para IPv4 e IPv6 MLD v1 y v2
- w. Software actualizable. Incluir la última versión disponible.3



- x. Soporte de enrutamiento dinámico y estático, como mínimo:
 - 1. RIP
 - 2. OSPF
- y. Soporte de tecnologías de Gateway para usuario como VRRP o similares.
- z. Soporte de Multicast: PIM-SM y PIM-DM como mínimo.
- aa. Soporte de PBR o similares.
- bb. Puerto de Consola para gestión local con puerto RJ 45.
- cc. Puerto Ethernet 10/100 dedicado para administración fuera de banda.
- dd. Soporte de Telnet, HTTP y SSH para gestión remota
- ee. Registro de eventos vía Syslog
- ff. Soporte de SNMP v1, SNMP v2c, SNMP v3.
- gg. Debe permitir Administración vía Web.
- hh. Soporte del estándar IEEE 802.1AB (LLDP: Link Layer Discovery Protocol) para intercambio de información de dispositivos en redes multivendor.
- ii. Soportar múltiples niveles de privilegios de acceso (mínimo 4) por puerto de consola o Telnet para administración. Indicar la cantidad de niveles soportados.
- jj. Procesos de debug para análisis en caso de fallas.
- kk. El switch debe tener la capacidad de limitar la cantidad de direcciones MAC aprendidas en un puerto para evitar ataques MAC address flooding que llenen la tabla de direcciones MAC del switch.
- ll. Soporte de mecanismos para evitar ataques tipo DoS y MITM, basados en STP y DHCP, así como “VLAN Hopping”, “DHCP Rogue Server”.
- mm. Filtros aplicables por puerto.
 - nn. Filtros basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP.
 - oo. Soporte de autenticación 802.1x con asignación dinámica de VLAN y asignación dinámica de listas de control de acceso (ACL).
 - pp. Control de acceso centralizado por RADIUS, ya sea para los administradores del switch como para los usuarios de la red que se autentican vía 802.1x.
 - qq. Autenticación, Autorización y Accounting para administradores de red usando TACACS+.



- rr. Soporte de flexibilidad en la autenticación mediante 802.1x, que permita usar un perfil para invitados, autenticación por MAC y autenticación 1x de manera dinámica, asegurando que un dispositivo/usuario que se conecte tenga algún método disponible de autenticación.
- ss. Soporte de 802.1x, autenticación por MAC (MAB) y Web Authentication de manera dinámica para usuarios que se conectan detrás del teléfono.
- tt. Soporte de Calidad de Servicio QoS.
- uu. Manejo de prioridad a nivel de colas, ocho colas de salida por puerto basado en hardware, debe de incluir al menos una cola de prioridad.
- vv. IEEE 802.1p Clase de Servicio, CoS y DSCP
- ww. Marcado y clasificación de paquetes basado en dirección IP origen y destino, MAC origen y destino y número de puertos TCP y UDP.
- xx. Configuración automática de QoS
- yy. Soporte de “port mirroring” por puerto y por VLAN.
- zz. Soporte de múltiples sesiones de “port mirroring” así como "port mirroring" remoto.

Controlador de Redes Inalámbricas

Cantidad De Equipos

Una (1) Unidad

Características Generales

- a. Formato tipo appliance para la controlar todos los puntos de acceso a la red inalámbrica.
- b. El hardware ofertado deberá tener la capacidad de controlar hasta 1500 Access Points y una capacidad instalada inicial de controlar 350 AP's como mínimo. El crecimiento debe de ser licenciado sin necesidad de armar cluster de 2 o más controladores.
- c. Debe contar 2 puertos 10G SFP+ de tipo multimodo.
- d. Capacidad de fuente de poder redundante.



- e. Las interfases a colocar deben de poder establecer una agregación de enlace hacia el switch conectado. Esto permitirá tener un canal de mayores prestaciones hacia los usuarios.
- f. Debe manejar los estándares 802.11 a/b/g/n/ac.
- g. La solución de controlador debe de manejar túneles entre controlador y punto de acceso.
- h. Debe de operar conjuntamente con el resto de los equipos de la solución inalámbrica para soportar las aplicaciones de datos, voz y video.
- i. Debe ser capaz de controlar y administrar los puntos de acceso inalámbrico de forma centralizada incluyendo las funciones de actualización de configuraciones y software.
- j. Para un esquema de múltiples controladores en la red (distribuido), cada uno de ellos debe de poder trabajar de manera independiente sin la necesidad de que exista una coherencia obligatoria entre ellos para funcionar. Cada uno de los controladores deberá de mantener las funcionalidades de gestión y monitoreo.
- k. Deberá de contar con software que le permita adaptarse y administrar en tiempo real el entorno de RF. Entre estas funciones deberá de encontrarse:
 - a. Asignación dinámica de canales para optimizar la cobertura y desempeño.
 - b. Balanceo de carga de usuarios entre múltiples puntos de acceso inalámbricos.
 - c. Detección y corrección de huecos en la cobertura inalámbrica.
 - d. Control dinámico de potencia de acuerdo a las condiciones de la red.
 - e. En caso de falla de un punto de acceso inalámbrico, el controlador deberá de ser capaz de ajustar la potencia en los puntos de acceso adyacentes para cubrir el área que fue afectada.
 - f. Detección y capacidad de evitar interferencia 802.11 mediante la recalibración de la red.
- l. Deberá de proveer múltiples capas de seguridad, incluyendo:
 - a. Protección, detección y ubicación de intrusos a nivel inalámbrico mediante firmas predefinidas o la definición de nuevas. Al menos se deben de soportar las siguientes:
 - 1. Broadcast de authentication frame

2. Null probe response
 3. Management frame flood
 4. Wellenreiter
 5. EAPOL flood
 6. NetStumbler
- b. Detección y clasificación de puntos de acceso inalámbricos no legítimos (rogue) de manera automática, con opción a llevar acciones de contención como las siguiente:
1. Contención en el aire. Los puntos de acceso de la solución permiten contener al rogue incrementando su señal para que el cliente se asocie a la red adecuada.
- c. Debe de soportar mecanismos de protección de los mensajes de administración entre cliente-punto de acceso y punto de acceso-controlador. Por lo menos debe de asegurar la encriptación de los mensajes de administración desde los clientes.
- d. Seguridad en capa 2 mediante el manejo de filtrado por MAC, WEP, WEP dinámico, TKIP, WPA, 802.11i (WPA2), 802.1X (PEAP, EAP-TLS, EAP-TTLS) y L2TP.
- e. Capacidad de poder manejar autenticaciones basadas en web que pueda servir para la autenticación de usuarios invitados.
- f. Bloqueo de tráfico entre clientes asociados a un mismo SSID.
- g. Soporte de AAA mediante un servidor de RADIUS/TACACS+ para manejar las políticas de usuarios y derechos de gestión del equipo.
- h. Deberá de soportar autenticación de usuarios en base a un servidor de RADIUS, base de datos local, base de datos LDAP, directorio activo de Microsoft, entre otros.
- i. La solución debe de permitir que mediante el uso de un mismo SSID, se pueda diferenciar a los usuarios que se conectan y agregar políticas de acuerdo al rol tales como:
1. Listas de control de acceso.
 2. Calidad de servicio
 3. VLANs



- m. Deberá de ofrecer servicios de roaming entre puntos de acceso inalámbrico, sin importar que estos se encuentren en diferente subred y sin hacer cambios en la infraestructura de LAN, preservando las características del acceso en términos de QoS y Seguridad y logrando que el delay sea imperceptible por las aplicaciones de misión crítica como es el caso de la voz.
- n. Deberá soportar las siguientes funcionalidades de calidad de servicio:
 - a. Soporte de Wi-Fi Multimedia
 - b. Manejo de 802.1p
 - c. Soporte de DSCP
 - d. Soporte de 802.11e
 - e. Soporte de asignación de ancho de banda por perfil de usuario de acuerdo a su rol en la red y en el directorio activo
- o. Debe de soportar las siguientes funcionalidades en relación a los puntos de acceso inalámbrico que maneja:
 - a. Autenticación de puntos de acceso inalámbrico mediante el uso de certificados.
 - b. Soporte de hasta 16 SSIDs por punto de acceso inalámbrico cada uno de ellos con diversas políticas de seguridad y calidad de servicio.
 - c. Soporte de puntos de acceso que puedan trabajar de manera autónoma en una sede remota ante algún corte en el enlace WAN. Este cambio a autónomo de los APs no debe de cambiar la experiencia del usuario en lo siguiente:
 - 1. Capacidad de poder hacer switching del tráfico localmente.
 - 2. Capacidad de poder mantener la autenticación manteniendo los esquemas AAA (802.1x) usados para nuevos usuarios que se conecten durante el corte.
 - d. Soporte de puntos de acceso que puedan generar un túnel encriptado desde una ubicación externa a la red por Internet para la extensión de la red inalámbrica.
 - e. Operación de puntos de acceso inalámbricos en modo que permita dar acceso a usuarios además de realizar funciones de monitoreo de forma simultánea.



- f. Operación de puntos de acceso inalámbricos en modo de monitoreo que permita aumentar la densidad sin degradar el desempeño.
- g. Operación de puntos de acceso inalámbricos en modo de sniffer que permita capturar los paquetes en la red y enviarlos a un analizador de protocolos.
- h. Operación de puntos de acceso inalámbricos en modo de malla que permita obtener conectividad a los recursos de LAN vía inalámbrica a través de otro punto de acceso inalámbrico.
- p. Soporte de IGMP para la optimización del tráfico multicast.
- q. Debe tener la capacidad de funcionar como DHCP Proxy o DHCP Relay.
- r. Soporte de IPv4 e IPv6.
- s. Para la administración como mínimo debe de soportar el acceso vía HTTP, HTTPS, Telnet, SSH, SNMP v2c, 3.
- t. Debe manejar los estándares 802.11 d/e/h/r/u

Puntos de Acceso

Cantidad de Equipos

Trescientos Cincuenta (350) Unidades

Características Generales

- a. Los Access Point (AP) que forman parte de la solución inalámbrica, deben contar con la opción de conmutación de datos de forma distribuida, es decir sin pasar por el controlador inalámbrico, esto de requerirse en algún momento formar una red inalámbrica con parte o totalidad de los Access Point (AP).
- b. Capacidad habilitada para trabajar en las bandas de frecuencia de 2.4GHz y 5GHz en simultáneo.
- c. Capacidad habilitada para el soporte de los estándares IEEE 802.11a, IEEE 802.1b, IEEE 802.1g, IEEE 802.11n y IEEE 802.11ac.
- d. Capacidad habilitada del estándar IEEE 802.11e - Calidad de Servicio (QoS) a aplicaciones de datos, voz y video en redes inalámbricas como parte del sistema AP-Controlador.
- e. Soporte habilitado como mínimo del estándar IEEE 802.3af.



- f. Soporte habilitado como mínimo dos puertos 10/100/1000Base-T Ethernet para la conexión con la red cableada.
- g. Soporte habilitado de estándares IEEE 802.1q (Trunk)
- h. Soporte habilitado de IPv4 e IPv6.
- i. Soporte habilitado para la creación de múltiples Service Set Identifier (SSID).
- j. Capacidad habilitada para el soporte de un mínimo de 240 usuarios o dispositivos asociados por Access Point (AP).
- k. Soporte habilitado para creación de vlan y asignación de las mismas a SSID creados. Cada identificador de servicio deberá permitir definir una política de calidad de servicio como parte del sistema AP-Controlador.
- l. Soporte habilitado para asignar roles y/o perfiles autenticación específicos a SSID creados como parte del sistema AP-Controlador.
- m. Soporte habilitado para capacidad de roaming.
- n. Soporte habilitado de administración adaptativa de radio frecuencia. Lo comentado, en beneficio de optimizar el performance de la red inalámbrica.
- o. Soporte habilitado de análisis de espectro embebido para ambas bandas de frecuencias en simultáneo: 2.4GHz y 5GHz.
- p. Soporte habilitado para brindar servicio y monitoreo en simultáneo a los usuarios inalámbricos

Seguridad

- q. Soporte habilitado de estándar IEEE 802.1x para la autenticación de usuarios inalámbricos vía un servidor de autenticación externo Radius, LDAP u otro como parte del sistema AP-Controlador.
- r. Soporte habilitado que permita diferentes niveles o características de seguridad, como mínimo tales como: WEP, 802.1x, EAP-TLS, EAP-PEAP, WPA2, TKIP, AES para cada SSID.
- s. Soporte habilitado para la creación de listas y políticas de acceso.
- t. Soporte habilitado para la detección y clasificación de puntos de acceso inalámbricos no autorizados (Rogue AP).
- u. Soporte habilitado de estándares de seguridad vigentes.



- v. Soporte habilitado y embebido para la Detección y Protección contra Intrusos (IPS/IDS). Asimismo, Características habilitadas contra ataques relacionados con redes inalámbricas.

Plataforma de Gestión de Red

Cantidad De Equipos

Una (1) Unidad

Software de gestión de la red que permite poder mantener el ciclo de vida de configuración, mantenimiento, despliegue y diseño de la red inalámbrica y cableada.

- a. Software de gestión vía http/https.
- b. Debe de poder gestionar como mínimo 1000 dispositivos de red.
- c. La solución de administración de red debe cubrir aspectos de gestión de red como monitoreo, inventario, reportes, configuración y alarmas.
- d. La solución de gestión a nivel de tecnologías inalámbricas debe de lograr lo siguiente:
 - 1. Soporte de tecnologías 802.11 a/b/g/n/ac.
 - 2. La solución debe de contar con plantillas predefinidas para la configuración de controladores y puntos de acceso.
 - 3. Tracking de dispositivos en demanda, y capacidad de hacer tracking en tiempo real utilizando dispositivos especializados de localización.
 - 4. Monitoreo de seguridad y verificación de la salud de la red para poder determinar si la red tiene las políticas de seguridad óptimas a nivel de configuración.
 - 5. El sistema deberá contar con una herramienta de visualización gráfica que permita visualizar más fácilmente la información, así como también permita agregar los mapas de piso de la institución o mapas de exteriores para poder visualizar la cobertura RF, como eventos de seguridad o localización de dispositivos.
 - 6. El sistema deberá poder operar en modo de alta disponibilidad (redundante)
 - 7. El sistema deberá poder hacer aprovisionamiento masivo por medio de la importación de archivos tipo CSV



8. El sistema propuesto deberá tener la facilidad para actualizar las versiones de software de los AP controlados, desde la consola central.
 9. El sistema propuesto deberá contar con una herramienta embebida para realizar diagnóstico de fallas, reportes estadísticos y debugging logs.
 10. El sistema propuesto deberá contar con una herramienta de monitoreo de radiofrecuencia, rendimiento, estadísticas de radiofrecuencia, verificación de interferencia no Wi-fi y análisis de espectro en la red inalámbrica.
 11. Capacidad de asociar alarmas con APs específicos
 12. Capacidad de generación de reportes en formato de valores separados por coma (CSV) y PDF
 13. Capacidad de generación de reportes automáticos o basados en tiempo.
 14. Capacidad de envío de mensajes de correo electrónico ante el evento de generación de un reporte
 15. Capacidad de monitoreo de servicios de voz sobre Wireless (VoWLAN), así como herramientas de troubleshooting para este efecto
 16. Capacidad de detección de APs no autorizados en 802.11 a/b/g/n/ac con elementos especializados en la red.
 17. La solución debe de permitir poder hacer backups automáticos de la configuración del sistema.
- e. La solución a nivel de gestión de redes cableadas debe lograr lo siguiente:**
1. La solución de administración de red debe tener la capacidad de establecer límites de utilización de recursos tipo CPU, memoria, etc. de manera que cuando se pase este umbral envíe alertas vía correo electrónico.
 2. La solución de administración de red debe tener la capacidad de reconocer la versión de software de los switches y routers de su misma marca y verificar si está disponible una versión superior en la web del fabricante. Además de poder mostrar gráficos físicos del equipo a gestionar.
 3. La solución de administración de red debe proveer un inventario detallado de los equipos administrados, dicho inventario debe al menos

dar información de número de serie, imagen de sistema operativo y capacidad de memoria.

4. La solución de administración de red debe tener la capacidad de ser un servidor syslog.
5. La solución de administración de red debe poder cambiar la configuración tanto de un equipo solo como de un grupo de equipos a la vez.
6. Debe de poder contar con plantillas predefinidas de configuración para facilitar el despliegue de configuraciones y personalizar las mismas para adaptarlas a la red.
7. La solución debe de poder hacer backup de las configuraciones, pudiendo comparar diferentes versiones de configuraciones y remarcar los cambios que existieron.

f. Respecto al análisis de tráfico:

1. Soporte de Netflow, SFLOW o similares, protocolos de análisis de tiempo de respuesta de aplicaciones, análisis de tráfico de voz y video.
2. Debe de poder permitir interpretar en gráficos información de flujos de tráfico en la red, enviado por los equipos ofertados, para poder tener estadísticas de ancho de banda consumido por usuario, por aplicación, por sitio, etc.
3. La información del análisis de tráfico debe de ser normalizada, pudiendo tener la información completa estadística de un usuario, aplicación o sitio y poder hacer “drill down” de ser necesario.
4. Todos los dispositivos deben de estar cubiertos a nivel de licenciamiento para esta funcionalidad.

g. Sobre los reportes y dashboards:

1. Se debe de contar con dashboards que consoliden la información a nivel de estadísticas de la red cableada e inalámbrica.
2. Los dashboard deben de ser configurables y se puede personalizar la ventana de vista de dashboard.

3. Se debe de poder configurar reportes en demanda y bajo un calendario predefinido, incluyendo la posibilidad de hacer reportes históricos de la información.
4. Se deben de tener reportes ya predefinidos para poder ser personalizados en el tiempo. Como mínimo reportes del siguiente tipo: seguridad, estado de los clientes, estado de los dispositivos, estado del rendimiento de la red, etc.
5. La solución de administración de red debe permitir personalizar la página web por parte de los administradores. Esto quiere decir que si un administrador ve que la herramienta le muestra información que no le es relevante pueda retirar esa información y así mismo agregar información que si le es relevante.

h. Sobre la gestión de la herramienta y dispositivos:

1. El sistema deberá soportar la administración de privilegios basado en grupos
2. El sistema propuesto deberá soportar gestión jerárquica de acuerdo a los roles del administrador.
3. El sistema propuesto deberá soportar servicios de AAA vía RADIUS y TACACS
4. La solución de gestión debe de poder tener acceso a casos de soporte creados por el administrador ante la falla de algún equipo dentro de la red, además de poder consultas alertas con comunidades de soporte.

Soporte de descubrimiento vía SNMP, tablas de enrutamiento, tablas ARP, etc para automatizar este proceso.

Plataforma de Control De Acceso

Cantidad de Equipos

Una (1) Unidad

Características Generales



- a. El Control de Acceso a la red, debe de estar compuesto por una solución que permita controlar puntos importantes:
 1. Acceso a la red de los usuarios corporativos.
- b. La solución de control de acceso a la red debe de contemplar la siguiente cantidad de usuarios XXX para el acceso a la gestión de la infraestructura
- c. La solución de control de acceso debe de soportar XXX dispositivos de red.
- d. La solución debe de estar basada en appliance o en su defecto para un sistema virtualizado. El postor deberá indicar la mejor opción de acuerdo a los requerimientos actuales de la red.
- e. El sistema debe controlar el acceso de todos los usuarios de la red LAN, WLAN y WAN y VPN de la red.
- f. La solución debe basarse en un esquema AAA (autenticación, autorización y accounting).

Control del acceso de la red de los usuarios corporativos:

Sobre la autenticación:

- a. Para el control del acceso del usuario, la plataforma debe de soportar Radius e integrarse a los puntos de acceso a la red como switches, concentradores VPN y access-points.
- b. La solución deberá permitir que los usuarios puedan acceder a las vlans respectivas dependiendo del rol del mismo en el directorio activo, con el uso del protocolo 802.1X.
- c. Los clientes que soliciten acceso a la red podrán ser autorizados o denegados basados en:
 1. Atributos de red: MAC
 2. Atributos de usuario: usuario, clave, certificados, one-time passwords.
- d. El usuario debe validarse contra un dominio existente utilizando sus credenciales. En caso la red maneje esquemas de multidominio, la solución de control de acceso deberá asegurar que ello sea transparente para el usuario.



- e. En función del usuario y del estado general de cumplimiento de normas de seguridad y auditoría se deben asegurarse el cumplimiento de los siguientes casos:
1. Si el dispositivo a ingresar a la red posee un suplicante 802.1x y pertenece al dominio, permitir luego de la autenticación ingresar a la red.
 2. Si el dispositivo a ingresar a la red no pertenece al dominio, redireccionar su tráfico a un portal web para ingresar a un dominio restrictivo por un período de tiempo.
 3. Si el dispositivo no tiene un suplicante embebido como el caso de impresoras, UPS, teléfonos, etc debe de permitir ingresar a la red autenticándolo mediante su MAC.
- f. La solución debe de permitir la movilidad del usuario conectado a un teléfono, es decir que al desconectar a la máquina del teléfono exista la posibilidad de actualizar la MAC en el sistema y que el puerto vuelva al estado de no autorizado y permita que ese dispositivo se pueda conectar a otro puerto de la red de manera transparente y que esa MAC no sea personificada por otro dispositivo para acceder a la red.
- g. La solución debe soportar los siguientes métodos de autenticación como mínimo:
1. PAP
 2. CHAP
 3. MSCHAPv1
 4. EAP-MSCHAPv2
 5. EAP-MD5
 6. LEAP
 7. PEAP
 8. EAP-FAST
 9. EAP-TLS
 10. Machine Authentication



- h. La solución debe de poder integrarse como mínimo con los siguientes repositorios de identidad:
1. Windows Active Directory
 2. LDAP
 3. RSA SecurID
 4. Servidores Radius

Sobre la autorización:

- i. La solución debe dependiendo del perfil del usuario autenticado, poder asignarle políticas de manera granular de acuerdo a las siguientes condiciones combinadas o independientes:
1. Acceso a la red basado en tiempos: Determinación de intervalos de tiempo en donde está permitido el usuario en la red.
 2. Acceso de red basado en el tipo de acceso: Ante determinados medios de acceso como WLAN, VPN, LAN, etc si está autorizado darle acceso a la red.
 3. Atributos extraídos del directorio activo.
- j. De acuerdo a las condiciones descritas, poder aplicar algún tipo de política al usuario. Como mínimo las siguientes:
1. Asignación dinámica de vlans
 2. Asignación dinámica de listas de control de acceso.
 3. Redirección hacia una URL.

Integración de Servicios de Control de Acceso

- a. De encontrarse equipos que no debieran pasar el proceso de control de acceso (teléfonos IP, impresoras, UPS), que exista un filtrado de sus direcciones MAC de manera centralizada en la solución. Este filtrado puede darse de dos maneras:
1. Simple: Capacidad manual de agregar direcciones MAC a filtrar de manera centralizada en la solución sin necesidad de hacer el filtrado en la infraestructura de routers o switches.

2. Avanzada: La solución debe de poder identificar a profundidad el tipo de dispositivo que se conecta a la red, con la finalidad de poder hacer control de acceso del mismo. La identificación debe de poder llegar a clasificar dispositivos tipo Android, Apple, impresoras, etc.
- b. La solución debe de soportar la inclusión de un sistema de aprovisionamiento de cuentas de invitados propio de la solución y soportada y distribuida por el mismo fabricante. Este aprovisionamiento permitirá tener sponsors locales que generen las cuentas bajo parámetros globales de control de tiempo y establecimientos de contraseñas dinámicas.
 - c. Esta solución debe de permitir también hacer esquemas de reportes de la actividad del invitado. Se debe asegurar la solución para situaciones tipo hot-spot.
 - d. El sistema debe de poder integrarse con plataformas de Mobile Device Management (MDM) para soportar análisis de posturas de dispositivos móviles. De la misma manera la solución debe de proveer como mínimo un portal de registro de dispositivos móviles, en donde se pueda autenticar la identidad del dispositivo, y acceder a este portal para manejarlo, logrando como mínimo “dar de baja al equipo” y “dar de alta al equipo”.
 - e. La solución debe de contar con un esquema distribuido y centralizado.
 - f. La solución debe de ser del mismo fabricante que la infraestructura de red a nivel inalámbrica y cableada.

5.3. FASE 3: DISEÑO

5.3.1. Políticas de seguridad informática

Para añadirle un nivel de seguridad a la red, se diseñó unas políticas de seguridad que nos van a permitir restringir la usabilidad de la red y sus recursos de una manera jerárquica.

Esto con el fin de que todos los tipos de usuario no accedan de la misma manera al uso de los recursos de la red puesto que esto provocaría un caos en el fluido de información de nuestra red informática.

Entonces se definieron políticas de seguridad documentadas con respecto al uso que se le debe dar a la red informática local y sus recursos, tal como lo observamos en la propuesta líneas abajo.

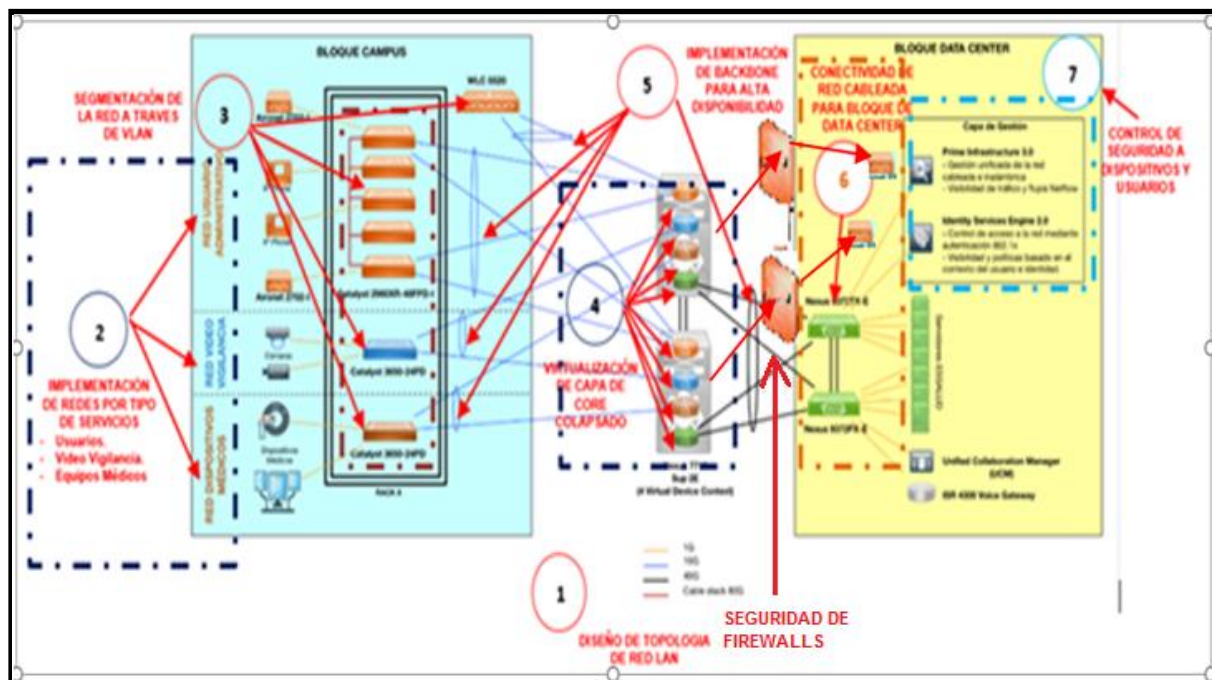


Figura 65. Diseño de Arquitectura Propuesta Seguridad a Través de Firewalls. Fuente: Elaboración Propia (2017).

Nota: Diseño de la Arquitectura Propuesta de Seguridad a Través de Firewall en el HNERM EsSALUD (2017).



PROPUESTA DE REQUERIMIENTO CARACTERÍSTICAS TÉCNICAS

Firewall de Nueva Generación – NGFW

Adquisición de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la información perimetral que incluye filtro de paquetes, control de aplicaciones, administración de ancho de banda (QoS), VPN IPsec y SSL, IPS, prevención contra amenazas de virus, Spyware/Anti-Bot y malware “Zero Day”, bien como controles de transmisión de datos y acceso a internet componiendo una plataforma de seguridad integrada y robusta.

Por plataforma de seguridad se entiende hardware y software integrados de tipo appliance.

Generales

- a. La solución debe consistir de un appliance de seguridad de red con funcionalidades de Next Generation Firewall (NGFW), y consola de administración y monitoreo.
- b. Por funcionalidades de NGFW se entiende: reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos.
- c. La plataforma debe soportar análisis de contenido de aplicaciones tanto en capa 3 como en capa 7.
- d. El software deberá ser ofrecido en su versión más estable y/o más avanzada.
- e. La marca de los equipos presentados en la solución debe contar con representantes y especialistas dentro del país para todos los modelos de equipos propuestos en la solución.
- f. Los equipos deben ser nuevos, sellados y sin uso.
- g. En ningún caso se podrá presentar soluciones con equipos que estén en etapa de obsolescencia o que hayan anunciado su “End-of-life”, o dejen de ser fabricadas, comercializadas y/o soportadas durante los 5 años siguientes a la instalación de los equipos a ser propuestos. Esto deberá ser respaldado con una carta del fabricante.
- h. La solución debe ser capaz de operar en modalidad layer 3(routing), modalidad in-line (bridge) y L2 (Port mirroring).



Detalle General del Equipamiento

- a. Los equipos deben ser nuevos, sellados y sin uso.
- b. Los firewalls ofertados deben realizar inspección profunda en todos los niveles de la capa OSI (Open System InterConnection) incluido tráfico cifrado.
- c. La inspección de tráfico deberá soportar protocolos y aplicaciones “bien conocidas” como Telnet, FTP, SMTP, http, DNS, ICMP, DHCP, ARP, RPC, SNMP (v3), Lotus Notes, Exchange etc. El proveedor debe especificar la lista de protocolos y aplicaciones dentro de esta categoría.
- d. Los firewalls deben soportar al menos 10 instancias de firewall lógicas (Virtualización). Se deben incluir las licencias necesarias para el correcto funcionamiento de esta funcionalidad.
- e. El equipo debe permitir la creación de políticas de tipo Firewall con capacidad de seleccionar campos como direcciones y redes, identificador de usuarios y aplicaciones.
- f. La solución debe ser capaz de crear políticas basadas en aplicaciones y determinar el comportamiento de estas.
- g. Las reglas de firewall deben analizar las conexiones que atraviesan en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs
- h. Las reglas del firewall deben tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando
- i. Las reglas de firewall deben poder tener limitantes y/o vigencia en base a tiempo.
- j. En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP.
- k. Los firewalls ofertados deben implementar Alta Disponibilidad en modo Activo-Activo y/o modo Activo-Pasivo
- l. Los firewalls deben permitir filtro de tráfico VoIP, implementando filtraje de protocolos SIP, H.323, MGCP y otros que el proveedor indique.
- m. Los firewalls deben filtrar tráfico IP del tipo IPv4 e IPv6. Estas reglas deben

ser configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario).

- n. Los firewalls deben filtrar protocolos P2P (e.g., Kazaa, Gnutella, BitTorrent e IRC), independiente de los puertos TCP utilizados para su comunicación.
- o. Los firewalls deben filtrar protocolos de comunicación instantánea como
- p. Yahoo, Messenger, Skype, Gtalk. El proveedor debe especificar cómo filtra y permite este tipo de protocolos.
- q. Los firewalls deben implementar protecciones contra ataques XSS y/o SQL Injection.
- r. Los firewalls deben detectar y filtrar ataques DoS

Protocolos de red y conectividad

- a. La solución soporta ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.
- b. La solución soporta políticas de ruteo (policy based routing).
- c. El soporte a políticas de ruteo permite que, ante la presencia de dos enlaces, se pueda decidir por que enlace egresa tráfico determinado.
- d. La solución debe soportar ECMP con peso. En este modo el tráfico será distribuido entre múltiples rutas, pero no en forma equitativa, sino en base a los pesos y preferencias definidas por el administrador.
- e. Debe permitir el controlar el acceso a archivos compartidos de Microsoft usando CIFS, y que el administrador decida que carpetas se pueden acceder y cuáles no.
- f. Debe contar con hardware basado en tecnología Hyper threading con el fin de duplicar de forma efectiva el número de núcleos de procesamiento disponibles.
- g. Los siguientes esquemas de autenticación deben ser soportados por los módulos de firewall y VPN: tokens (por ejemplo, SecureID), TACACS, RADIUS, certificados digitales y dispositivos biométricos.
- h. La solución debe permitir integración con analizadores de tráfico mediante el protocolo NetFlow.



- i. Los firewalls ofertados deben implementar protocolos de enrutamiento RIP, OSPF (v2 y v3) y BGP.
- j. Los firewalls deben trabajar con protocolos multicast y servidor multicast, implementando protocolos IGMP, PIM-SM, PIM-SSM y otros que el proveedor indique.
- k. Los firewalls deben soportar VLAN tagging y creación de zonas de seguridad en base a VLANs.
- l. Los firewalls deben soportar NAT/PAT dinámico y estático, siendo capaces de manejar aplicaciones basadas en H.323 y SIP.
- m. Los firewalls deben permitir manejo de ancho de banda de protocolos TCP y VoIP, permitiendo la definición de niveles mínimos y máximos.
- n. Los firewalls deben implementar QoS: ancho de banda garantizado, ancho de banda máximo, utilización de ancho de banda por prioridad, garantía de QoS y límites de QoS.
- o. La aplicación de QoS debe ser por protocolo y/o política de filtrado aplicada sobre el tráfico.
- p. Funcionalidad de DHCP:
 - 1. Servidor DHCP
 - 2. Reenvío (Relay) de solicitudes DHCP

Hardware e Interfaces

- a. El dispositivo debe ser un equipo de propósito específico. Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux.
- b. Debe ser capaz de albergar hasta 42 interfaces 10/100/1000Mbps RJ-45
- c. Debe tener capacidad para soportar interfaces de 10G SFP y 40Gb SFP
- d. El equipo NGFW debe ser provisto de un mínimo de 04 interfaces de fibra óptica a 10GB (SFP)
- e. El equipo NGFW debe ser provisto de un mínimo de 08 interfaces de fibra óptica a 1GB (SFP)



- f. El equipo NGFW debe ser provisto con al menos 2 interfaces de fibra óptica a 40GB (QSFP+)
- g. El equipo NGFW debe contar con 1 o 2 interfaces dedicadas para alta disponibilidad como mínimo.
- h. El equipo NGFW debe contar con 1 (una) interfaz de red 10/100/100 dedicada para la administración como mínimo
- i. El equipo NGFW debe contar con 1 (una) interfaz de tipo consola o similar como mínimo
- j. Soporte de 2TB como mínimo para almacenamiento de logs. Con posibilidad de disco redundante de al menos 1Tb
- k. Con la finalidad de incrementar el performance, los appliance (out of the box), para las plataformas multinúcleo, deben soportar la multi replicación del kernel del firewall y permitir que corran en otros núcleos.
- l. El equipo NGFW debe contar con redundancia de discos, fuentes de poder y ventiladores

Alta Disponibilidad

- m. La solución de seguridad debe permitir la configuración de clústers en modo de operación en alta disponibilidad (HA), tanto para IPv4 como para IPv6.
- n. La solución debe ser capaz de operar en modalidad Alta Disponibilidad Activo-Pasivo y Activo-Activo
- o. La solución de seguridad debe ser capaz de definir al menos dos interfaces para sincronización.
- p. La funcionalidad de failover de los firewalls debe mantener el estado de las sesiones en forma transparente en caso de falla.
- q. La sincronización entre el clúster de alta disponibilidad debe incluir al menos:
 - 1. Todas las sesiones.
 - 2. Certificados para desencriptar.
 - 3. Todos los cambios de configuración.
 - 4. Todas las tablas de enrutamiento



- r. La solución de seguridad debe ser capaz de operar sin utilizar Multicast para el modo alta disponibilidad.
- s. La solución permite definir interfaces de gestión independientes para cada miembro en un clúster.

Performance

- a. Throughput mínimo de 27 Gbps con la funcionalidad de control de aplicaciones habilitada e IPS.
- b. Throughput mínimo de 18 Gbps con las siguientes funcionalidades habilitadas simultáneamente para todas las firmas que la plataforma de seguridad posea debidamente activadas y actuando: control de aplicaciones, Filtrado de URL, IPS, Antivirus y AntiSpyware/Anti-Bot/Antibot.
- c. Soporte a como mínimo 12,000,000 sesiones simultáneas por appliance.
- d. Soporte a como mínimo 160,000 nuevas sesiones por segundo por appliance.

Geolocalización

- a. Soportar la creación de políticas por Geolocalización, permitiendo que el tráfico de determinado País/Países sean bloqueados.
- b. Debe posibilitar la visualización de los países de origen y destino en los logs de acceso.
- c. Debe posibilitar la creación de regiones geográficas desde la interfaz gráfica y crear políticas utilizando las mismas.

Control de Aplicaciones

- a. Reconocer por lo menos 2000 aplicaciones diferentes, incluyendo, mas no limitado: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, VoIP, áudio, vídeo, proxy, mensajería instantánea, compartición de archivos, e-mail.
- b. Reconocer por lo menos las siguientes aplicaciones: bittorrent, gnutella, skype, facebook, linked-in, Twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, Google drive, skydrive, db2, mysql, oracle,

- active directory, kerberos, ldap, radius, iTunes, Dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, Google-docs, etc;
- c. Debe inspeccionar el payload del paquete de datos con el objetivo de detectar a través de expresiones regulares firmas de aplicaciones conocidas por los fabricantes independiente del puerto y protocolo. El chequeo de firmas también debe determinar si una aplicación está utilizando su puerto default o no, incluyendo, mas no limitando a RDP en el puerto 80 en vez del 389.
 - d. Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis comportamental del tráfico observado, incluyendo, mas no limitado a Encrypted Bittorrent y aplicaciones VOIP que utilizan criptografía propietaria;
 - e. Identificar el uso de tácticas evasivas, o sea, debe tener la capacidad de visualizar y controlar las aplicaciones y los ataques que utilizan tácticas evasivas vía comunicaciones criptografiadas, tales como Skype y ataques mediante el puerto 443.
 - f. Para tráfico encriptado (SSL y SSH), debe desencriptar paquetes con el fin de posibilitar la lectura del payload para chequeo de firmas de aplicaciones conocidas por el fabricante;
 - g. Debe realizar decodificación de protocolos con el objetivo de detectar aplicaciones encapsuladas dentro del protocolo y validar si el tráfico corresponde con la especificación del protocolo, incluyendo, mas no limitado a Yahoo Instant Messenger usando HTTP. La decodificación de protocolo también debe identificar funcionalidades específicas dentro de una aplicación, incluyendo, mas no limitado a la compartición de archivos dentro de Webex. También debe detectar el archivo y otros contenidos que deben ser inspeccionados de acuerdo a las Reglas de seguridad implementadas;
 - h. Debe Actualizar la base de firmas de aplicaciones automáticamente.
 - i. Los dispositivos de seguridad de red deben poseer la capacidad de identificar al usuario de red con integración al Microsoft Active Directory, sin la necesidad de instalación de agente en el Domain Controlled, ni en las estaciones de los usuarios;
 - j. Debe alertar al usuario cuando una aplicación fuera bloqueada.

k. Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en características de las aplicaciones como:

1. Tecnología utilizada en las aplicaciones (Client-Server, Browser Based, Network Protocol, etc).
2. Nivel de riesgo de las aplicaciones.
3. Categoría y subcategoría de aplicaciones.
4. Aplicaciones que usen técnicas evasivas, utilizadas por malwares, como transferencia de archivos y/o uso excesivo de ancho de banda, etc.

Prevención de Amenazas

- a. Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS, Antivirus y Antispyware/Anti-Bot integrados en el propio appliance de Firewall.
- b. Debe incluir firmas de prevención de intrusos (IPS) y bloqueo de archivos maliciosos (Antivirus y Antispyware/Anti-Bot).
- c. Las funcionalidades de IPS, Antivirus y Antispyware/Anti-Bot deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante.
- d. El IPS integrado no debe configurarse en FailOpen por defecto.
- e. El IPS integrado debe poder escanear toda la sesión y no solo un porcentaje de la misma por defecto.
- f. Se deben poder añadir excepciones al IPS desde el LOG, para excluir por ejemplo direcciones IP de una firma de IPS.
- g. La solución debe incluir un mecanismo de búsqueda rápida y amigable en los Logs que permita mejorar la visibilidad de los eventos de seguridad de la red.
- h. La solución debe poder incluir Sandboxing y prevención de APTs, la misma que debe permitir la Prevención y el bloqueo de amenazas de día 0 en tiempo real.



- i. Debe sincronizar las firmas de IPS, Antivirus, Anti-Spyware/Anti-Bot cuando esté implementado en alta disponibilidad Activo/Activo e Activo/pasivo.
- j. Las firmas deben poder ser activadas o desactivadas, o incluso habilitadas apenas en modo de monitoreo.
- k. Excepciones por IP de origen o de destino deben ser posibles en las Reglas, de forma general y firma a firma.
- l. Debe soportar granularidad en las políticas de IPS Antivirus y Antispyware/Anti-Bot, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos esos ítems.
- m. Debe permitir el bloqueo de vulnerabilidades.
- n. Debe permitir el bloqueo de exploits conocidos.
- o. Debe incluir seguridad contra ataques de negación de servicios.
- p. Deberá poseer los siguientes mecanismos de inspección de IPS:
 - 1. Análisis de patrones de estado de conexiones;
 - 2. Análisis de decodificación de protocolo;
 - 3. Análisis para detección de anomalías de protocolo;
 - 4. Análisis heurístico;
 - 5. IP Desfragmentación;
 - 6. Reensamblado de paquetes de TCP;
 - 7. Bloqueo de paquetes malformados.
- q. Ser inmune y capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPflood, etc.
- r. Detectar y bloquear el origen de portscans.
- s. Identificar y prevenir ataques de phishing al limitar los sitios a los que los usuarios pueden enviar credenciales
- t. Bloquear ataques efectuados por worms conocidos, permitiendo al administrador adicionar nuevos patrones.
- u. Soportar los siguientes mecanismos de inspección contra amenazas de red: análisis de patrones de estado de conexiones, análisis de decodificación de protocolo, análisis para detección de anomalías de

- protocolo, análisis heurístico, IP Desfragmentación, reensamblado de paquetes de TCP y bloqueo de paquetes malformados.
- v. Posea firmas específicas para la mitigación de ataques DoS.
 - w. Posea firmas para bloqueo de ataques de buffer overflow.
 - x. Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.
 - y. Permitir el bloqueo de virus y Spyware/Bot en, por lo menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3.
 - z. Soportar bloqueo de archivos por tipo.
 - aa. Identificar y bloquear comunicaciones como botnets.
 - bb. Bloquear comunicaciones de command y control
 - cc. Debe soportar varias técnicas de prevención, incluyendo Drop y tcp-rst (Cliente, Servidor y ambos).
 - dd. Debe soportar referencia cruzada como CVE.
 - ee. Registrar en la consola de monitoreo las siguientes informaciones sobre amenazas identificadas.
 - ff. Debe soportar la captura de paquetes (PCAP), por firma de IPS y AntiSpyware/Anti-Bot.
 - gg. Debe permitir que en la captura de paquetes por firmas de IPS y AntiSpyware/Anti-Bot sea definido el número de paquetes a ser capturados. Esta captura debe permitir seleccionar, como mínimo, 50 paquetes.
 - hh. Debe poseer la función resolución de direcciones vía DNS, para que conexiones como destino a dominios maliciosos sean resueltas por el Firewall como direcciones (IPv4 e IPv6), previamente definidos.
 - ii. Permitir el bloqueo de virus, por al menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3.
 - jj. Los eventos deben identificar el país de donde partió la amenaza.
 - kk. Debe incluir seguridad contra virus en contenido HTML y javascript, software espía (Spyware/Anti-Bot) y worms.
 - ll. Seguridad contra descargas involuntarias usando HTTP de archivos ejecutables.



Maliciosos.

- a. Rastreo de virus en PDFs.
- b. Debe permitir la inspección en archivos comprimidos que utilizan o algoritmo deflate (zip, gzip, etc.).
- c. Debe ser posible la configuración de diferentes políticas de control de amenazas y ataques basados en políticas del firewall considerando Usuarios, Grupos de usuarios, origen, destino, zonas de seguridad, etc., o sea, cada política de firewall podrá tener una configuración diferente de IPS, siendo esas políticas por Usuarios, Grupos de usuario, origen, destino, zonas de seguridad.

Prevención de amenazas desconocidas

- a. Poseer la capacidad de análisis de amenazas no conocidas.
- b. Debido a los Malware hoy en día hay que ser muy dinámicos y un antivirus común no es capaz de detectar los mismos a la misma velocidad que sus variaciones son creadas, la solución ofertada debe poseer funcionalidades para análisis de Malwares no conocidos incluidas en la propia herramienta.
- c. El dispositivo de seguridad debe ser capaz de enviar archivos transferidos de forma automática para análisis en la nube donde el archivo será ejecutado y simulado en un ambiente controlado o sandboxing.
- d. Seleccionar a través de la política de Firewall que tipos de archivos sufrirán este análisis.
- e. Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows XP y Windows 7
- f. Debe soportar el monitoreo de archivos transferidos por internet (HTTP, FTP, HTTP, SMTP) como también archivos transferidos internamente en los servidores de archivos usando SMB.
- g. El sistema de análisis debe proveer informaciones sobre las acciones del Malware en la máquina infectada, informaciones sobre cuáles aplicaciones son utilizadas para causar/propagar la infección, detectar aplicaciones no confiables utilizadas por el Malware, generar firmas de Antivirus y Antispyware/Anti-Bot automáticamente, definir URLs no confiables



- utilizadas por el nuevo Malware y proveer informaciones sobre el usuario infectado (su dirección ip y su login de red).
- h. El sistema automático de análisis debe emitir relación para identificar cuáles soluciones de antivirus existentes en el mercado poseen firmas para bloquear el malware.
 - i. Debe permitir exportar el resultado de los análisis de malware de día Zero en PDF y CSV a partir de la propia interfaz de administración.
 - j. Debe permitir la descarga de los malware identificados a partir de la propia interfaz de administración.
 - k. Debe permitir visualizar los resultados de los análisis de malware de día zero en los diferentes sistemas operacionales soportados.
 - l. Debe permitir informar al fabricante cuando haya una sospecha de falso-positivo y falso-negativo en el análisis de malware de día Zero a partir de la propia interfaz de administración.
 - m. La solución debe ser capaz de observar procesos que busquen inyectar código malicioso y explotar vulnerabilidades por medio de heap spray
 - n. La solución debe detectar programas de auto-arranque, mutexes y actividades sospechosas en los servicios de Windows
 - o. La solución debe analizar todo el tráfico producido por el archivo a analizar, debe detectar la creación de backdoors, descargas posteriores de malware y conexiones a dominios de baja reputación
 - p. La solución de sandboxing debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de Hypervisor, inacción de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host
 - q. La solución debe enviar amenazas evasivas a un ambiente de hardware real, deshabilitando totalmente la habilidad de la amenaza de evadir sandboxing en máquinas virtuales
 - r. La solución de sandboxing debe ser capaz de detectar e interrumpir la comunicación de Command y control saliente a través de firmas específicas de DNS y Command & control.



Filtro URL

- a. La plataforma de seguridad debe poseer las siguientes funcionalidades de filtro de URL.
- b. Permite especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora).
- c. Debe ser posible crear políticas por usuario, grupo de usuario, ips, redes y zonas de seguridad.
- d. Deberá incluir la capacidad de creación de políticas basadas en la visibilidad y control de quién está utilizando cual URLs a través de la integración con servicios de directorio, autenticación vía LDAP, Active Directory, E-Directory y base de datos local.
- e. Debe permitir poder publicar los logs de URL con la información de los usuarios conforme a lo descrito en la integración con servicios de directorio.
- f. Debe soportar la capacidad de crear políticas basadas en control por URL y categoría URL.
- g. Debe bloquear el acceso a sitios de búsqueda (Google, Bing y Yahoo) en el caso de que la opción de Safe Search está deshabilitada. Debe en ese caso exhibir una página de bloqueo dando instrucciones al usuario de cómo habilitar dicha función.
- h. Debe soportar una caché local de URL en el appliance, evitando el delay de comunicación/validación de las URLs.
- i. Debe poseer al menos 60 categorías de URLs.
- j. Debe soportar la creación de categorías URL custom.
- k. Debe soportar la exclusión de URLs del bloqueo por categoría.
- l. Debe permitir la customización de la página de bloqueo.
- m. Debe permitir o bloquear y continuar (habilitando que el usuario accese a un sitio potencialmente bloqueado informándole del bloqueo y habilitando el botón de “continuar” para permitirle seguir a ese site).
- n. Debe soportar la inclusión de los logs del producto de las informaciones de las actividades de los usuarios.

Identificación de usuarios

- a. Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de quién está utilizando cuales aplicaciones a través de la integración como servicios de directorio, autenticación vía ldap, Active Directory, base de datos local.
- b. Debe poseer integración con Microsoft Active Directory para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios.
- c. Debe poseer integración con Radius para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios.
- d. Debe posea integración con Ldap para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en Usuarios y Grupos de usuarios.
- e. Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal).

QoS

- f. Como la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube, ustream, etc.) y tener un alto consumo de ancho de banda, se requiere que la solución, a la vez de poder permitir o negar ese tipo de aplicaciones, debe tener la capacidad de controlarlas por políticas de máximo de ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones, tanto de audio como de vídeo streaming.
- g. Soportar la creación de políticas de QoS por:
 1. Dirección de origen
 2. Dirección de destino
 3. Por usuario y grupo de LDAP/AD.
 4. Por puerto;



- h. El QoS debe permitir la definición de clases por:
 - 1. Ancho de Banda garantizado
 - 2. Ancho de Banda Máximo
 - 3. Cola de prioridad.
- i. Soportar priorización Real Time de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype.
- j. Disponer de estadísticas Real Time para clases de QoS.
- k. Deberá permitir el monitoreo del uso que las aplicaciones hacen por bytes, sesiones y por usuario.

VPN

- a. Soportar VPN Site-to-Site y Cliente-To-Site.
- b. Soportar IPSec VPN y licenciar (en el caso que se requiera una licencia) hasta el máximo de usuarios que permita el dispositivo.
- c. Soportar SSL VPN y licenciar (en el caso que se requiera una licencia) hasta el máximo de usuarios que permita el dispositivo.
- d. VPNs IPSec debe soportar:
 - 1. 3DES;
 - 2. Autenticación MD5 e SHA-1;
 - 3. Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
 - 4. Algoritmo Internet Key Exchange (IKE);
 - 5. AES 128, 192 e 256 (Advanced Encryption Standard)
 - 6. Autenticación vía certificado IKE PKI.
- e. Debe poseer interoperabilidad con los siguientes fabricantes:
 - 7. Cisco;
 - 8. Checkpoint;
 - 9. Juniper;
 - 10. Palo Alto Networks;
 - 11. Fortinet;
 - 12. Sonic Wall;

- f. Las VPN SSL deben permitir que el usuario realice la conexión por medio de cliente instalado en el sistema operacional del equipamiento o por medio de interfaz WEB;
- g. Las funcionalidades de VPN SSL deben ser atendidas con o sin el uso de agente:
 - 1. La asignación de dirección IP en los clientes remotos de VPN;
 - 2. La asignación de DNS en los clientes remotos de VPN;
 - 3. Debe haber la opción de ocultar el agente de VPN instalado en el cliente remoto, tornando el mismo invisible para el usuario;
- h. El portal de VPN debe enviar al cliente remoto la lista de gateways VPN activos para el establecimiento de la conexión, los cuales deben poder ser administrados centralizadamente
- i. Debe haber una opción en el cliente remoto de escoger manualmente el Gateway de VPN y de forma automática a través de la mejor respuesta entre los gateways disponibles con base al más rápido.
- j. Debe poseer la capacidad de identificar el origen de conexión de VPN si es interna o externa.

Administración Centralizada

- a. En caso de requerir un appliance dedicado para la gestión, se requiere de 2 equipos. Manteniendo de preferencia funcionalidad de gestor y otro reporteador, respectivamente.
- b. La administración de la solución debe posibilitar un conjunto de estadísticas de todo el tráfico que pasa por los equipos de la plataforma de seguridad.
- c. Debe controlar todos los dispositivos de la plataforma de seguridad en una única consola, con administración de roles, privilegios y funciones
- d. Debe permitir la creación de objetos y políticas compartidas
- e. Debe consolidar logs y reportes de todos los dispositivos administrados
- f. La solución debe contar con herramientas gráficas para visualizar fácilmente las sesiones en el equipo, que permitan adicionarse por el administrador en la página inicial de la solución (dashboard), incluyendo por lo menos por



- defecto Top de sesiones por origen, Top de sesiones por destino, y Top de sesiones por aplicación.
- g. La solución debe contar con una interface gráfica de usuario (GUI) la cual se podrá elegir al menos entre los idiomas inglés y español.
 - h. La solución debe poseer una Interface basada en línea de comando (CLI) para administración de la solución.
 - i. La solución de seguridad debe poseer comunicación cifrada y autenticada con usuario y contraseña, tanto como para la interface gráfica de usuario como la consola de administración de línea de comandos (SSH o telnet).
 - j. La solución de seguridad debe permitir al administrador del sistema autenticarse vía usuario/contraseña o vía certificados digitales.
 - k. La solución cuenta con la capacidad de asignar un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar. (RBAC)
 - l. La solución debe permitir a los administradores conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet, http o https.
 - m. La solución de seguridad cuenta con soporte de SNMP versión 3
 - n. La solución de seguridad permite integrar al menos 3 servidores syslog.
 - o. Monitoreo de comportamiento del appliance mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red.
 - p. La solución de seguridad debe permitir que el administrador de la plataforma pueda definir qué funcionalidades están disponibles o deshabilitadas para ser mostradas en la interfaz gráfica.
 - q. El software de administración debe proveer un medio de ver, filtrar y gestionar las trazas de tráfico registradas (logs).
 - r. Los registros (logs) del firewall deben contener información de la regla que está gatillando el mismo. Estos registros (logs) no deben ser modificables.
 - s. El sistema de gestión debe proveer estadísticas en tiempo real del estatus de la “salud” de los módulos del firewall en el dashboard de monitoreo, considerando parámetros como utilización de CPU y número total de sesiones concurrentes.



SOLUCIÓN DE PREVENCIÓN DE INTRUSOS – IPS (Embebida)

- a. Se requiere una solución de prevención de intrusiones de red (IDS/IPS), capaz de proteger a la organización contra amenazas tales como Exploits, Amenazas Avanzadas Persistentes, Malware avanzado, Botnets, Ataques de Denegación de Servicio Distribuido y Ataques de reconocimiento entre otros.
- b. Deberá estar compuesta por sensores desplegados en la red y un sistema de gestión centralizada.
- c. Los sensores deberán ser de funcionalidad dedicada, es decir, no deberán correr en hardware compartido tales como dispositivos multifuncionales (UTM) o Firewalls.
- d. Los sensores deberán estar basados en un sistema operativo pre-endurecido específico para seguridad. Por seguridad y facilidad de administración y operación, no se aceptarán soluciones sobre sistemas operativos genéricos tales como GNU/Linux, FreeBSD, SUN Solaris, HP-UX de HP, AIX de IBM o Microsoft Windows
- e. Poseer licenciamiento ilimitado de usuarios y host en su modalidad de IPS.
- f. Deberá Incluir todos los accesorios y cables necesarios para la total instalación y puesta en operación.
- g. Los sensores deberán implementarse en la red en forma transparente, en capa 2 del modelo OSI. No requerirá cambios de topología de red ni modificaciones al esquema de ruteo.
- h. La solución deberá tener la alternativa de desplegar tanto sensores físicos (hardware) como sensores en modalidad appliance virtual y ser gestionados desde el mismo sistema de gestión centralizada.

Especificaciones Generales

- a. Los sensores serán desplegados en 1 centro de datos protegiendo 4 segmentos de red.
- b. Cada puerto del sensor deberá poder implementarse en las siguientes modalidades:
 1. Puerto SPAN a través de Port Mirroring en un Switch
 2. Mediante un TAP

3. En línea, cerrando la red en caso de falla (fail-close)
4. En línea, abriendo la red en caso de falla (fail-open)
- c. Deberá contar con un puerto de gestión dedicado para la comunicación con la consola de Administración.
- d. Deberá contar con un puerto de respuesta dedicado en caso de implementarlo en modo SPAN (IDS).
- e. Deberá contar con la posibilidad de monitorear sin bloquear, aun estando en línea, e indicar en qué casos hubiera bloqueado (bloqueo simulado). Esta función deberá poder ser activada para el equipo entero o para interfaces individuales para aprender del tráfico y realizar actividades de tuning.
- f. Deberá permitir la definición de reglas de control de acceso (ACLs) para establecer el tráfico permitido o denegado con los siguientes componentes:
 - g. Dirección de host o red IPv4
 - h. Protocolo y/o puerto TCP/UDP
 - i. Los sensores no deberán contar con Interface de Gestión Local. Todo cambio deberá realizarse a través de la Consola de Gestión Centralizada. El sensor solo permitirá conexión SSH para troubleshooting y tareas de setup inicial.
 - j. Deberá ser capaz de inspeccionar tráfico SSL sin necesidad de hardware adicional. Informar cómo afecta la performance la activación de esta funcionalidad
 - k. El sensor deberá mantener una copia de la clave privada del servidor Web en memoria volátil de manera que no pueda ser comprometida siendo alojada en un medio de almacenamiento.
 - l. Deberá permitir definir puertos SSL no estándar, es decir, diferentes a TCP 443.
 - m. Permitirá capturar paquetes de sesión completa que permitan servir de evidencia ante el análisis de un incidente.
 - n. Deberá ser posible configurar las siguientes opciones de captura:
 1. Registrar el paquete entero cuando un ataque es descubierto
 2. Registrar solo los primeros n bytes del paquete
 3. Registrar solo el flujo entre origen y destino del ataque detectado
 4. Registrar todos los nuevos flujos originados en el atacante independientemente del destino y todos los flujos iniciados en la máquina víctima del ataque.
 5. Capturar paquetes por un período de tiempo configurable



Arquitectura

- a. Los sensores deberán estar disponibles en modalidad appliance (hardware) y en modalidad appliance virtual. Informar en este último caso, cuáles son las plataformas de virtualización soportadas.
- b. Se requiere proteger 4 segmentos de red de 1Gbps en Cobre, con opción de 1 segmento de red de 10Gbps en Fibra.
- c. Se requieren 2 appliances, estos appliances deben tener un throughput de 4 Gbps y de 10Gbps, respectivamente.
- d. Los segmentos conectados in-line requerirán mecanismos de bypass (fail-open) a fin de que un fallo en los equipos no impacte en el normal funcionamiento de la red. Los mismos pueden ser integrados en el mismo equipo o externos proporcionados por el mismo fabricante.
- e. El equipamiento deberá contar con discos de estado sólido (SSD).
- f. Deberá contar con fuentes redundantes
- g. Los sensores deberán ser implementados en Alta Disponibilidad en modalidad Activo-Activo y Activo-Pasivo con stateful failover
- h. Los sensores deberán contar con puertos seriales y para propósito de inicialización o troubleshooting.
- i. Toda comunicación entre los sensores y la consola de gestión deberá ser autenticada y encriptada. Indicar qué mecanismos se utilizan.

Performance de equipo 1:

- a. La solución deberá soportar un throughput de 4 Gbps medido sobre tráfico real
- b. El sensor deberá generar alertas en el caso que se observe alta latencia.
- c. Bajo condiciones de carga alta de tráfico en la red, el sensor deberá tener mecanismos dinámicos y automáticos para priorizar el análisis de cierto tráfico, salvando recursos para proteger segmentos importantes. Indicar cómo se logra este punto.
- d. Deberá albergar como mínimo 4 interfaces de cobre y 2 interfaces de 10Gbps

Performance de equipo 2:

- a. La solución deberá soportar un throughput de 10 Gbps medido sobre tráfico real

- b. Deberá soportar al menos 1,200,000 conexiones concurrentes
- c. El sensor deberá generar alertas en el caso que se observe alta latencia.
- d. Bajo condiciones de carga alta de tráfico en la red, el sensor deberá tener mecanismos dinámicos y automáticos para priorizar el análisis de cierto tráfico, salvando recursos para proteger segmentos importantes. Indicar cómo se logra este punto.
- e. Deberá albergar como mínimo 4 interfaces de cobre y 4 interfaces de 10Gbps

Efectividad

- a. La solución deberá contar con un motor de detección basado en firmas y un servicio de suscripción que permita descargar nuevas firmas frecuentemente
- b. Las firmas deberán tener un formato propietario y no estar expuesto al público en general de manera de que un atacante no tenga acceso a la lógica y tenga la capacidad de generar variantes de ataques que permita evadir dicha firma. No deberá utilizar SNORT o lenguajes similares como método primario de detección basado en firmas.
- c. Deberá incorporar una herramienta que permita importar firmas SNORT como método alternativo de detección.
- d. Deberá ser posible crear firmas personalizadas con el mismo lenguaje propietario del motor principal.
- e. Deberá proteger aplicaciones Web inspeccionando HTTP y HTTPS a través de análisis heurístico que identifique inyecciones de SQL (SQL injections). No deberá utilizar string-matching para esto, sino que deberá analizar la sentencia SQL, verificar que sea válida y legítima y, reconocer palabras claves maliciosas que alteren la estructura de una query (ej. UNIÓN).
- f. Deberá ser capaz de forzar a los clientes a utilizar TCP en lugar de UDP para los request de DNS con el objetivo de proteger los servidores DNS de ataques de DoS spoof.
- g. Deberá soportar la limitación de ancho de banda de un tipo de tráfico a través de políticas de rate limiting con el objetivo de limitar los efectos de un ataque de DoS (Denial of Service). Estas políticas podrán ser aplicadas por interface y por subinterface, por protocolo y puerto, por aplicación, por usuario de dominio,



- ubicación geográfica y direcciones IP.
- h. Deberá ser capaz de limitar el ancho de banda de las conexiones provenientes de hosts externos basado en la reputación y geo-localización de dichos hosts. Es decir, para hosts con reputación negativa, limitar el ancho de banda a un número de conexiones por segundo y generar alerta si el umbral se supera, evitando de esa manera ataques de DoS.
 - i. Deberá soportar el uso de SYN Cookies para asegurar que el three-way handshake se realice antes de dejar pasar la conexión al servidor de destino y de esa manera bloquear ataques de SYN flood.
 - j. Deberá contar con un mecanismo de aprendizaje de tráfico para desarrollar estadísticas tales como tasas de tráfico de largo plazo y de corto plazo y cantidad de direcciones IP. Con esta información, detectar desviaciones que busquen generar impacto mediante ataques de DoS.
 - k. Deberá ser capaz de parsear información contenida en el campo XFF (X-Forwarder-For) de manera de obtener la dirección IP real del cliente cuanto la conexión proviene de un servidor proxy. Deberá utilizar esa información en las vistas de alertas, dashboards, reportes, así como también en las políticas de firewall y de cuarentena para no bloquear una dirección IP de un proxy denegando el servicio a toda la red.
 - l. Deberá permitir definir la tasa de requests de URL por segundo por dirección IP a un website o a todos los websites para prevenir ataques de DoS.
 - m. El sensor tendrá la capacidad de detectar el browser web del cliente para mitigar ataques de DoS originados por bots.
 - n. Deberá coleccionar datos de capa de aplicación para los protocolos más importantes como HTTP, FTP y SMTP para análisis forense. Ej. En el caso de SMTP deberá capturar la dirección del emisor, la dirección del receptor, nombre de attachment. Informar cómo afecta la performance la activación de esta funcionalidad.
 - o. Deberá ser capaz de detectar ataques de reconocimiento tales como host sweeps, probes, escaneos de puertos, fuerza bruta de passwords e indexado de web servers.
 - p. Deberá detectar ataques de ARP spoofing.



Integración

- a. Deberá ser capaz de obtener detalles acerca de las estaciones de trabajo y servidores propios de la red desde algún sistema que posea esta información. Los datos deberán incluir Hostname, Nombre DNS, Nombre Netbios, Sistema Operativo, Service Packs instalados, Dirección IP, MAC Address, así como también el software de seguridad instalado en el endpoint. Indicar con qué sistema puede integrarse para obtener esta información.
- b. Será posible identificar los usuarios de dominio conectados en una dirección IP origen o destino en un evento, a través de la integración con Active Directory. Deberá soportar múltiples dominios y no requerir instalación de agentes en los Domain Controllers.
- c. Deberá ser capaz de realizar un análisis de impacto automático evaluando si un ataque logrará ser exitoso en un host vulnerable. Indicar que componentes adicionales se requieren para realizar dicha función.
- d. Deberá identificar las aplicaciones que corren dentro de los protocolos de manera de aplicar políticas específicas. Ej. Bloquear Facebook y permitir el resto del tráfico HTTP/HTTPS
- e. El fabricante actualizará periódicamente la lista de aplicaciones identificables y las categorizará de manera de aplicar políticas por tipo de aplicación
- f. Será capaz de controlar determinadas funcionalidades de la aplicación tales como bloquear la transferencia de archivos a través de Mensajería Instantánea sin bloquear la aplicación completamente.
- g. El sistema de gestión deberá proveer una API permitiendo que aplicaciones externas accedan a las funcionalidades de la solución. Indicar a través de que protocolo es posible acceder.
- h. La solución deberá ser capaz de coleccionar información acerca de un endpoint y descifrar su sistema operativo y tipo de dispositivo a través de DHCP DISCOVER, DHCP REQUESTS, el campo de HTTP User Agent, y de los paquetes SYN y SYN + ACK de TCP. Indicar si otros componentes externos a la solución pueden coleccionar y enviar a la solución dicha información
- i. Indicar si la solución puede obtener eventos de sensores de IPS basados en agentes (HIPS) instalados en estaciones de trabajo y servidores.



- j. La solución deberá integrarse con la solución de SIEM del Proveedor y entregar datos de eventos y de registro de paquetes capturados para análisis forense.
- k. Deberá soportar al menos el uso de SNMP, Syslog y queries de SQL para obtener los datos y reportarlos al SIEM.
- l. Debe tener la capacidad de integrarse a un sistema de reputación local para tener un intercambio de inteligencia de amenazas extendido
- m. Deberá permitir ejecutar respuestas en el sensor disparadas directamente desde el SIEM. Indicar si este mecanismo es nativo o requiere del desarrollo de scripts.
- n. El sensor será capaz de exportar Netflow para análisis de tráfico en Capa 7. haya un sistema de análisis de flujos el cual debe hacerse fuera de los equipos, pero del mismo fabricante sin costo adicional a través de una máquina virtual. Así mismo este análisis debe recopilar la información de procesos ejecutados en las estaciones finales mediante un agente para identificar anomalías (proceso vs tráfico de red)
- o. Deberá contar con firmas que, si bien no constituyan un ataque, reporten un comportamiento que va en contra de las políticas de seguridad. Ej. Detección de tráfico de Mensajería Instantánea, tráfico de gestión SSH, Telnet, RDP en segmentos que no deberían tenerlo, tráfico P2P, streaming de video o música

Gestión

- a. La consola de gestión deberá ser provista con todos sus componentes instalados en un appliance de propósito específico o en versión virtual. Para el cual el proveedor deberá incluir el hardware necesario.
- b. El proveedor de la solución será responsable de proveer todas las actualizaciones necesarias y del soporte de todos los componentes de la misma incluyendo Sistema Operativo, Base de Datos y la aplicación en sí.
- c. Deberá contar con una base de datos incluida en el producto. No requerirá la instalación o utilización de una base de datos externa.
- d. En caso de falla deberá incluir herramientas de respaldo que permitan recuperar la configuración ya establecida sin importar si el sistema de gestión centralizado se reubicara en un appliance de propósito específico, en un ambiente virtual o en una plataforma comercial certificada por el fabricante



- e. El acceso a la consola deberá ser vía Web a través de un navegador de uso general. No deberá requerir la instalación de ningún componente en la máquina de los administradores (cliente)
- f. Deberá soportar el acceso a través de dispositivos móviles
- g. Deberá contar con soporte de autenticación con los siguientes métodos:
 - 6. Base de usuarios local
 - 7. Radius
 - 8. LDAP (Active Directory)
 - 9. TACACS+ con control granular de comandos por CLI
- h. Deberá contar con múltiples perfiles de acceso que permita a los usuarios limitar sus acciones sobre la solución mediante privilegios entre ellos:
 - 10. Administrador
 - 11. Operador
 - 12. Generador de Reportes
 - 13. Analista o Experto
- i. Deberá contar con diferentes dominios de gestión, permitiendo que un administrador de un dominio no tenga visibilidad sobre los dominios restantes, tal como ocurre en sistemas multi-tenant.
- j. Deberá soportar el envío de alertas de eventos y de sistema a través de SNMP versión 1, 2c y 3.
- k. Deberá enviar alertas de eventos y de sistema a un Servidor de Syslog
- l. Deberá enviar alertas a través de email o pager
- m. Deberá contar con un algoritmo que calcule un factor de riesgo e indique cuales son los hosts que han tenido más actividad maliciosa. Deberá mostrar los datos tales como dirección IP, nombre DNS, Sistema Operativo, detalle de usuario y los indicadores de comportamiento.
- n. Deberá informar acerca de la importancia de una alerta utilizando información basada en el resultado del ataque, nivel de exposición a vulnerabilidades asociadas al ataque y sistema operativo, versión, nivel de parches de la host víctima. Esto permitirá priorizar los eventos y generar incidentes para su pronta mitigación.
- o. Deberá contar con un dashboard que permita tener un panorama general de la situación actual de eventos detectados.



- p. La consola de gestión deberá proporcionar un sistema de gestión de incidentes que permita asignar a diferentes operadores y analistas actividades de análisis y remediación.
- q. Deberá soportar el rollback a versiones anteriores de políticas.
- r. Deberá reportar su propio estado de salud y la de todos sus componentes informando fallos, estado de actualización y otra información de sistema. Además, deberá monitorear el estado de salud de los dispositivos que administra.
- s. Cada acción que ejecuten los usuarios del sistema de gestión deberá quedar reportada en un registro de auditoría y deberá contener al menos la siguiente información: Usuario, acción realizada, resultado de la acción, día y hora.

Reporting

- a. Contará con reportes pre-definidos para su rápida utilización.
- b. Deberá permitir exportar reportes en formato PDF.
- c. Deberá permitir crear reportes customizados seleccionando el tipo de datos y la forma de visualizarlos mediante tablas, gráfico de tortas, gráficos de barras y los campos que quieren visualizarse.
- d. Contará con la capacidad de programar la ejecución automática de los reportes y el envío a través de correo electrónico
- e. Deberá permitir generar reportes de auditoría con todas las actividades ejecutadas sobre la consola y los sensores.

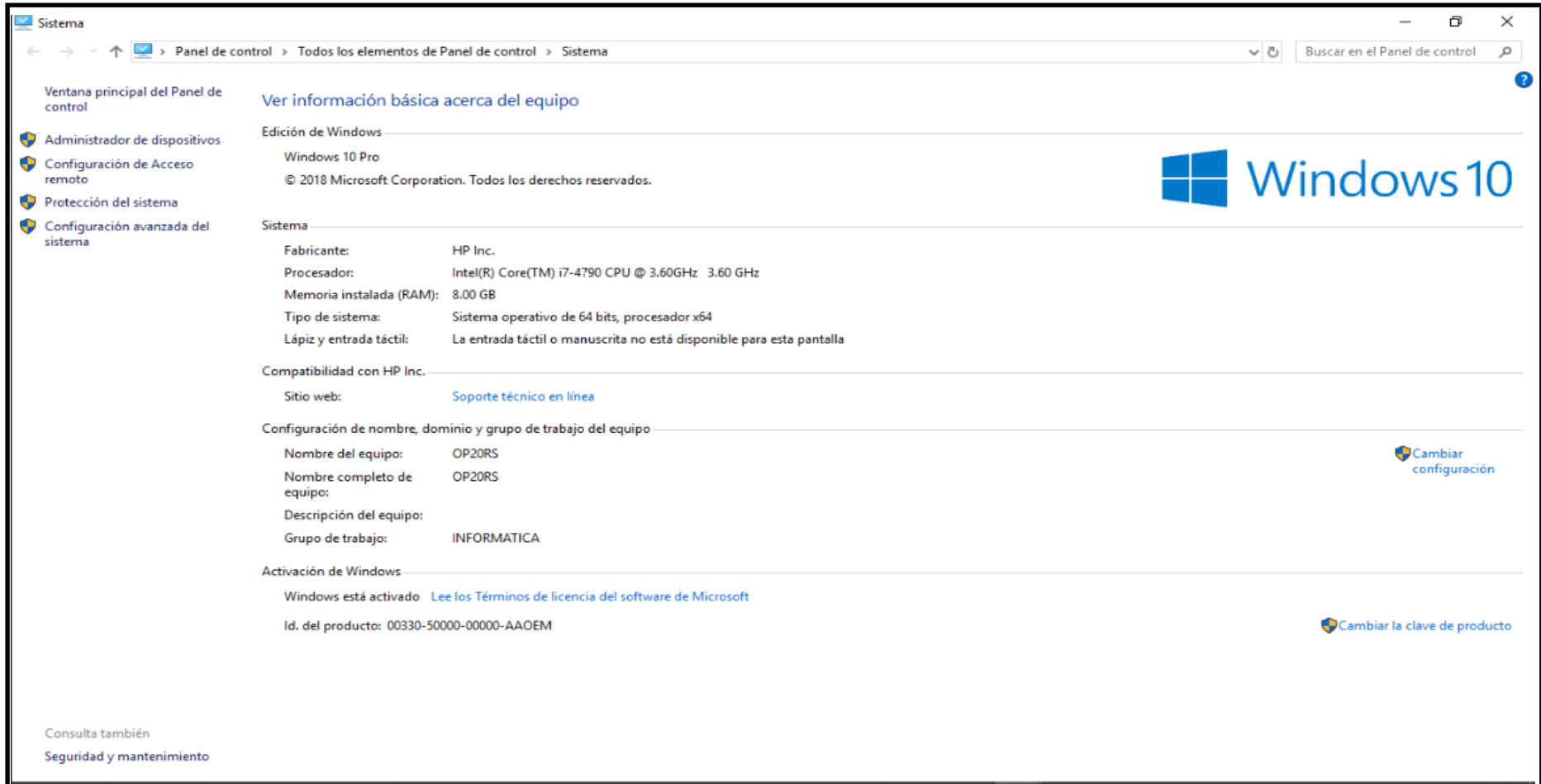


Figura 66. Seguridad Informática Actual en una PC. Usuario (OP20RS) de la OSI HNERM EsSALUD. Fuente: Oficina de Soporte Informático (2018).



1. ACCESO AL CORE CON SSH

```
SW-CORE-REBAGLIATI# show configuration snapshot aaa
! AAA :
aaa authentication console "local"
aaa authentication ftp "local"
aaa authentication http "local"
aaa authentication snmp "local"
aaa authentication ssh "local"
user password-size min 4
! PARTM :
! AVLAN :
! 802.lx :
```

2. ACCESO TELNET CIFRADO CON MD5

```
aaa authentication enable default enable
aaa authentication login default local
username administrador password 9158141cb68e337c020ble052dbfa73e level 15 enc
rypted
username comunicaciones password 4455964655a61e6a6cffd446ba40c4a9 level 15 en
crypted
username rrodriguezp password 5c6049609635bbeb6730b4eab526bfa9 level 15 encry
pted
ip ssh server
```

Captura de configuración global de un Switch Alcatel OmniStack LS 6224P ubicado en el gabinete b3.

3. Configuración estática de las ip por usuario

Detalles de la conexión de red

Propiedad	Valor
Sufijo DNS específico p...	
Descripción	Intel(R) Ethemet Connection (2) I219-LM
Dirección física	DC-4A-3E-6A-78-DD
Habilitado para DHCP	No
Dirección IPv4	10.1.51.8
Máscara de subred IPv4	255.255.255.0
Puerta de enlace predet...	10.1.51.1
Servidores DNS IPv4	172.20.0.175 172.20.0.27
Servidor WINS IPv4	
Habilitado para NetBios ...	Sí

Captura de pantalla de la dirección ip configurada en Windows 10 del área de Comunicaciones ubicado en el Gab J

Figura 67. Seguridad a Nivel de Capa 2 en la Red Local del HNERM EsSALUD. Fuente: Oficina de Soporte Informático HNERM EsSALUD (2018).



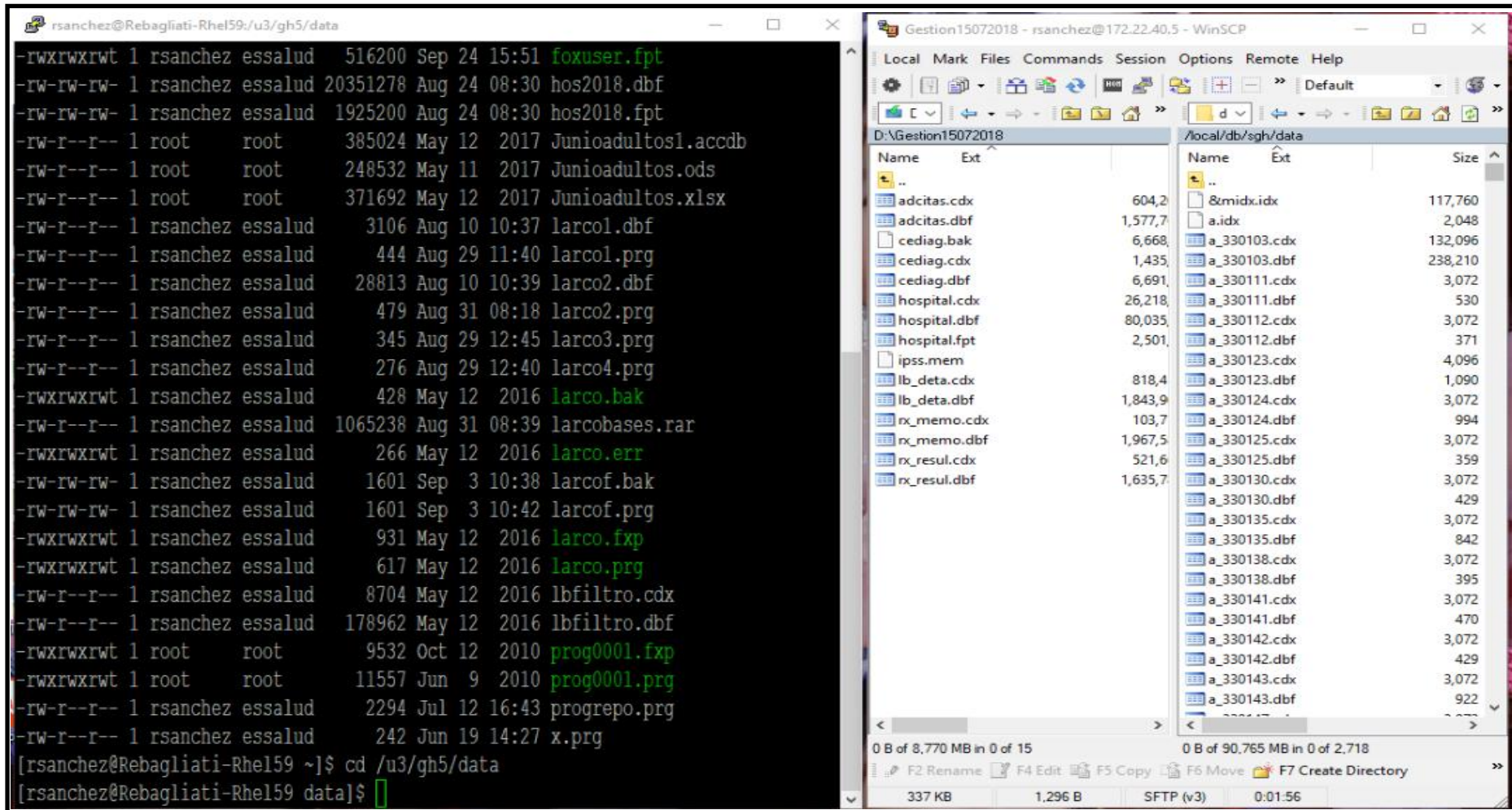


Figura 68. Acceso por PUTTY a través de S.O. Linux y Acceso por WinSCP de la PC. Usuario (OP20RS). Fuente: Oficina de Soporte Informático HNERM EsSALUD (2018).



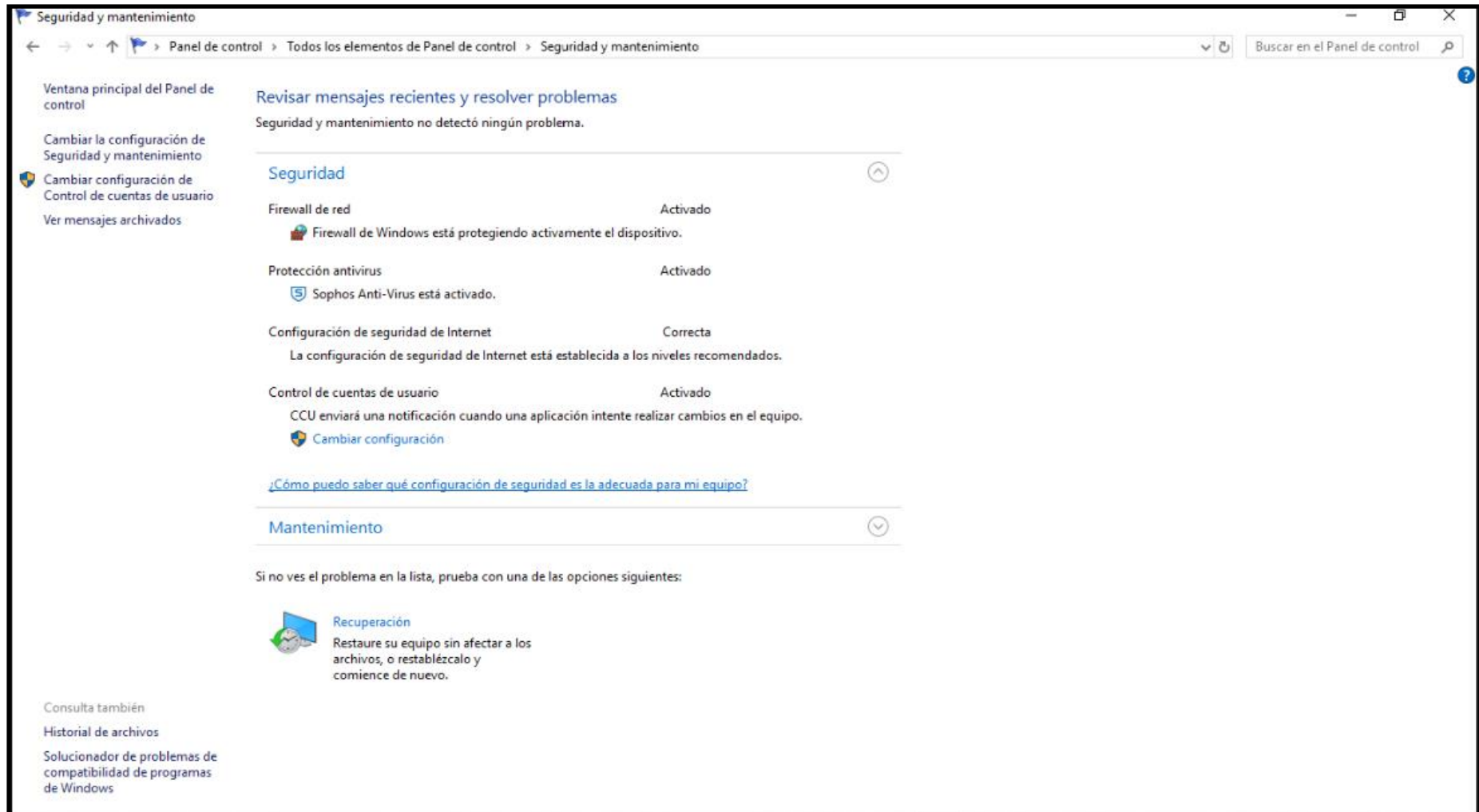


Figura 69. Seguridad a través de FIREWALL de la PC. Usuario (OP20RS). Fuente: Oficina de Soporte Informático HNERM EsSALUD (2018).



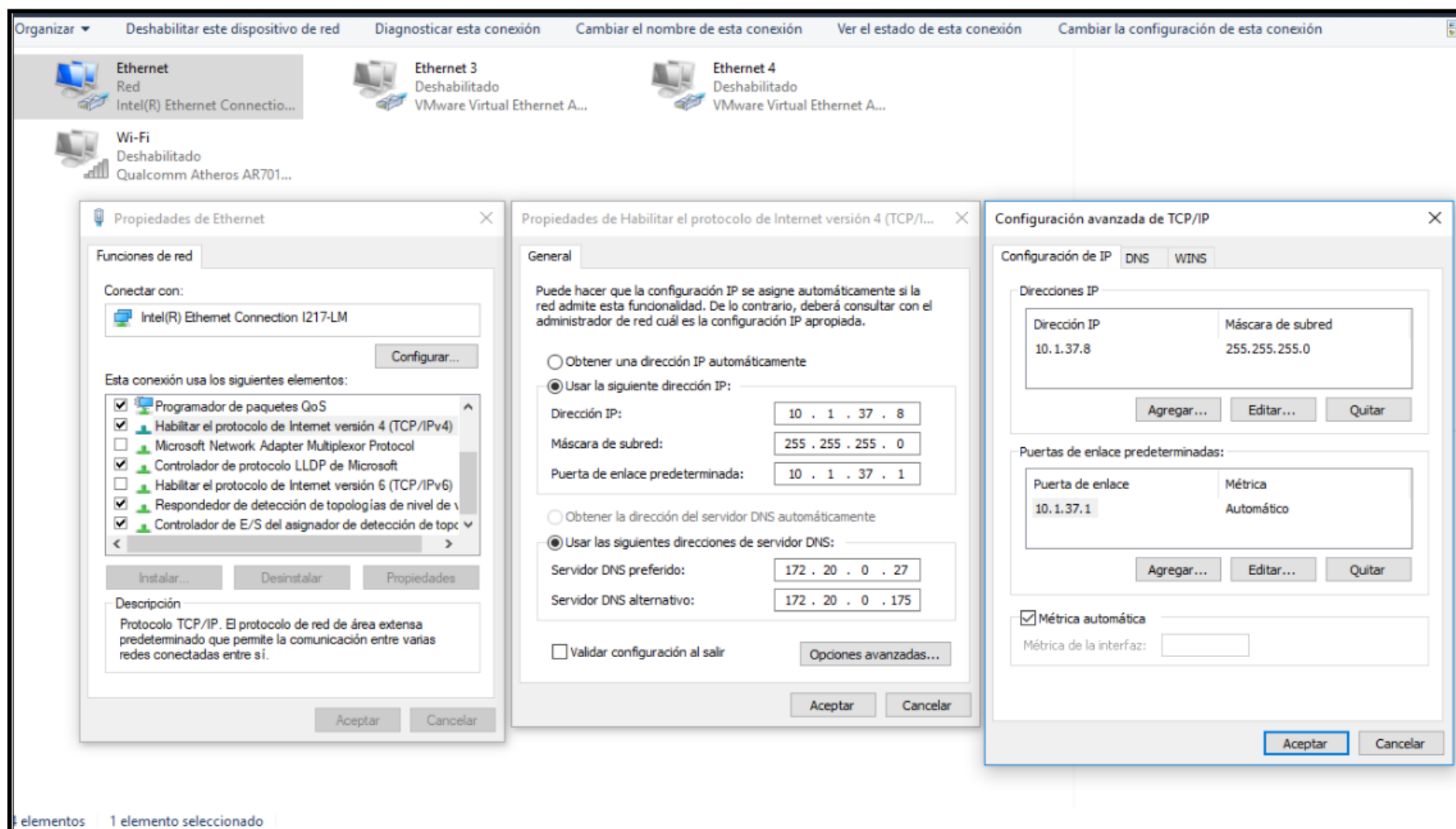


Figura 70. Las Propiedades de Protocolo TCP/IP de la PC. Usuario (OP20RS). Fuente: Oficina de Soporte Informático HNERM EsSALUD (2018).



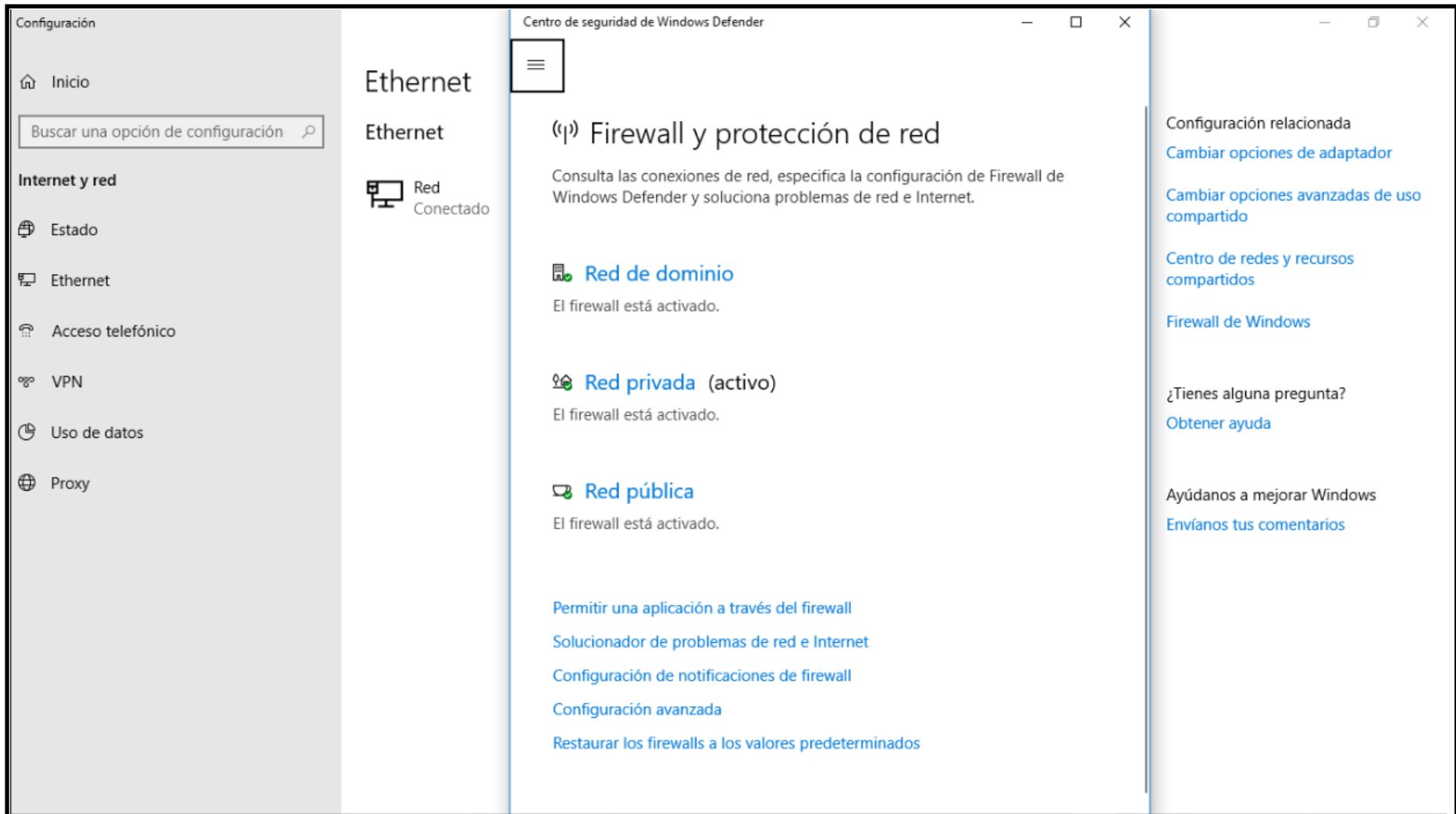


Figura 71. Seguridad por FIREWALL y protección de la RED de la PC. Usuario (OP20RS). Fuente: Oficina de Soporte Informático HNERM EsSALUD (2018).



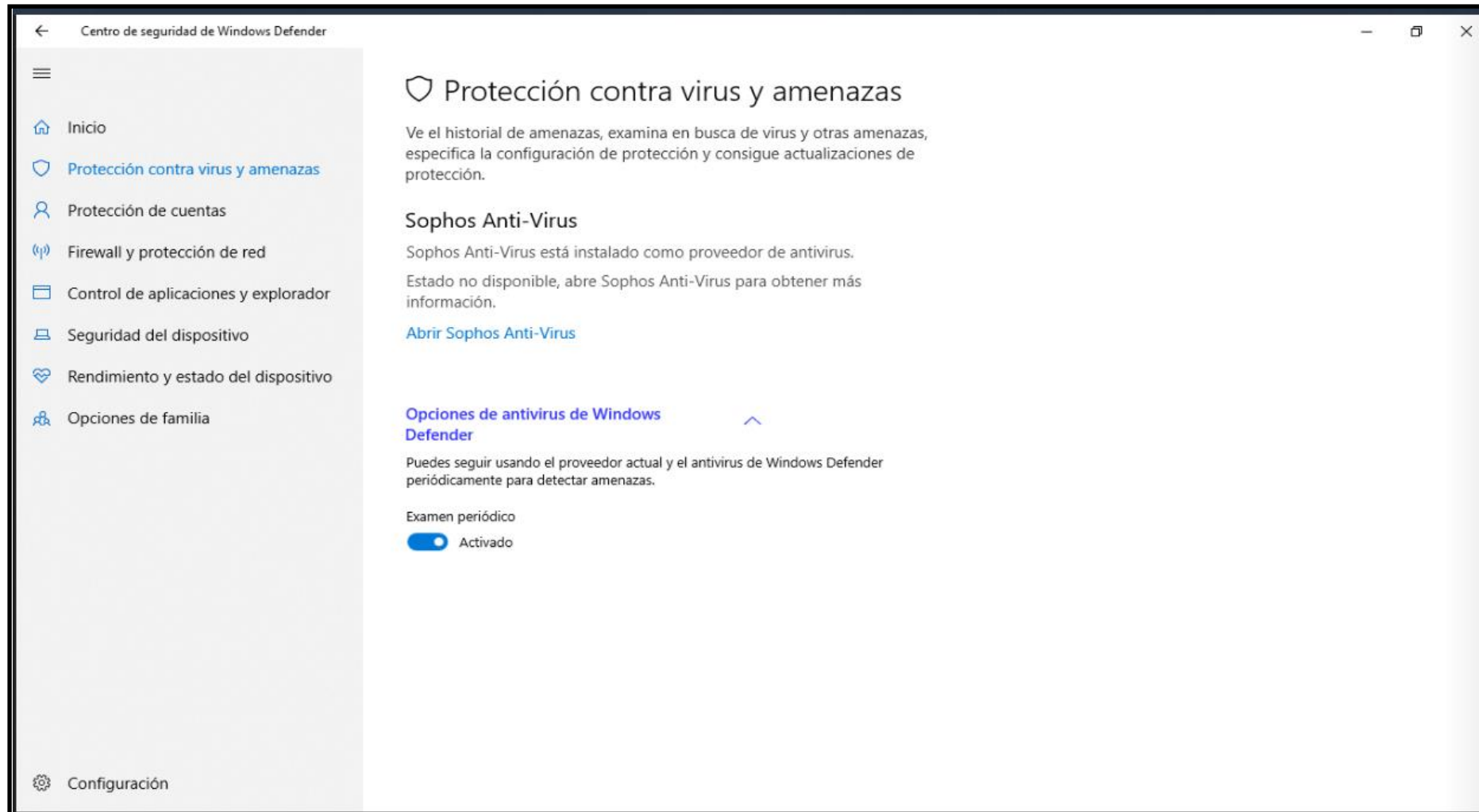


Figura 72. Seguridad de Protección contra Virus y Amenazas, Software Instalado Sophos Anti-Virus en la PC. Usuario (OP20RS). Fuente: Oficina de Soporte Informático HNERM EsSALUD (2018).



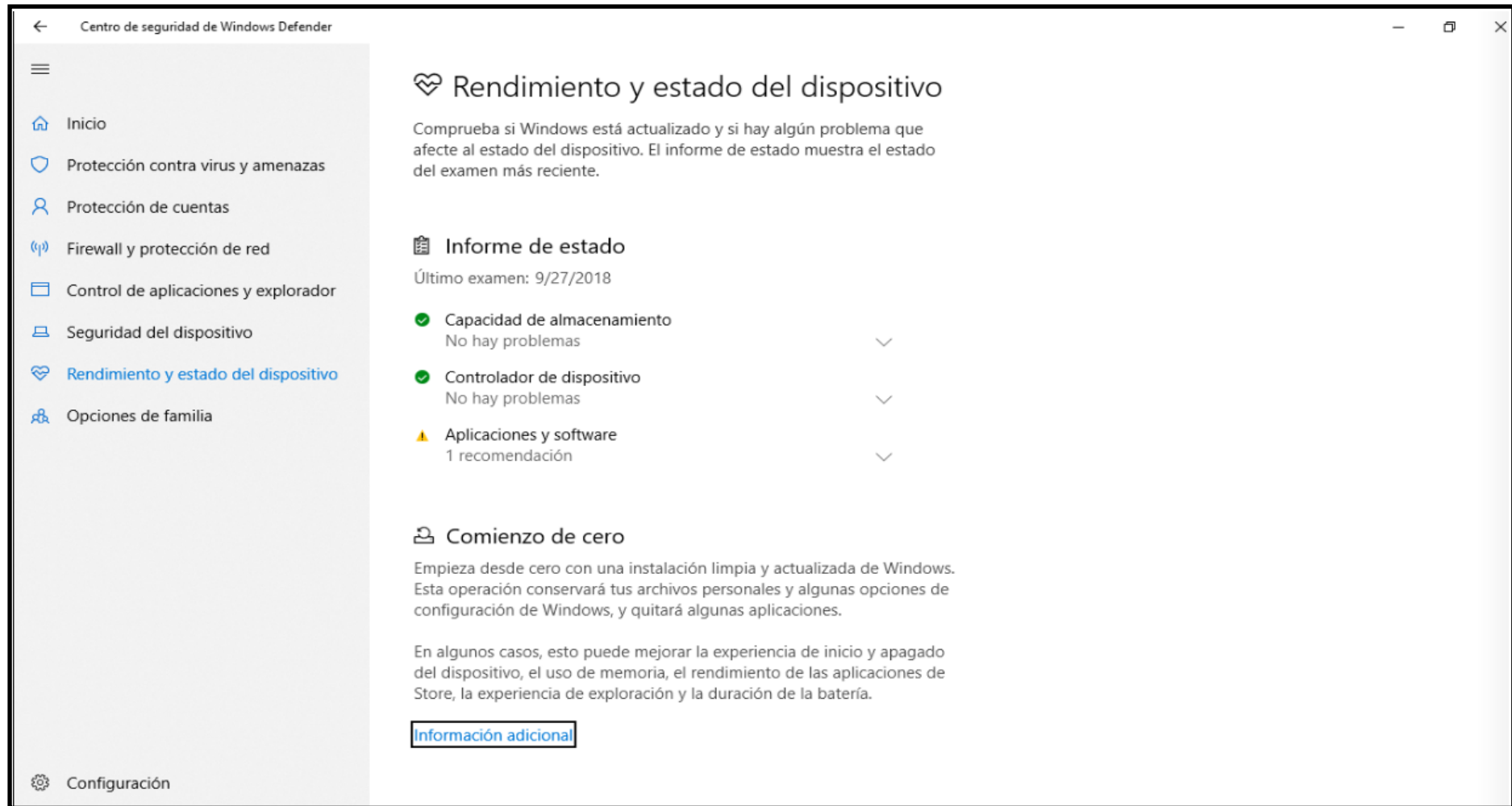


Figura 73. Rendimiento y estado de la PC. Usuario (OP20RS). Fuente: Oficina de Soporte Informático HNERM EsSALUD (2018).



5.3.2. Organigrama de la Oficina de Soporte Informático del HNERM EsSALUD.

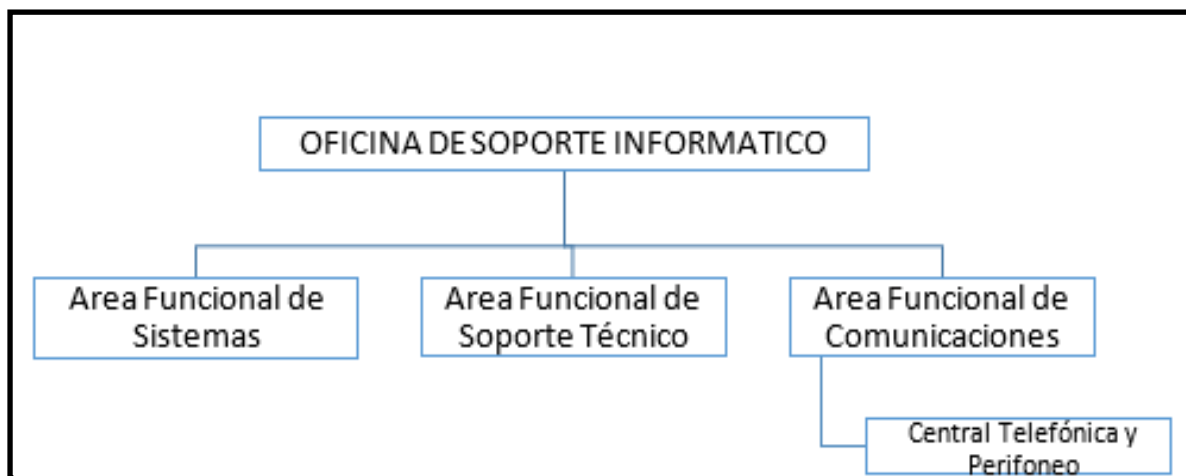


Figura 74. Organigrama Actual de la OSI HNERM EsSALUD. Fuente: Oficina de Soporte Informático (2017).

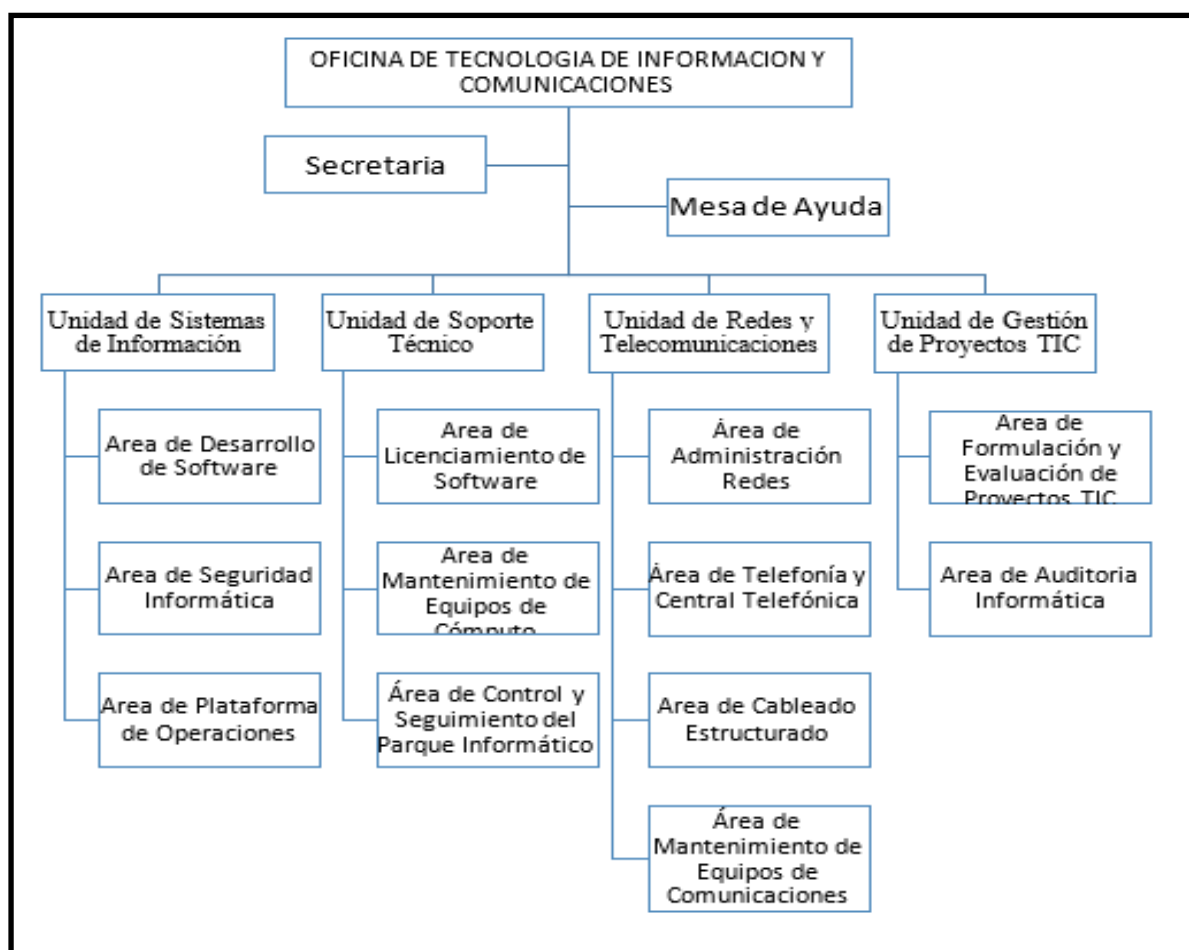


Figura 75. Organigrama Propuesto de la OSI HNERM EsSALUD. Fuente: Oficina de Soporte Informático (2018).



5.3.3. Análisis FODA de la Oficina de Soporte Informático del HNERM-ESSALUD.

Tabla 15

Análisis Interno de FODA HNERM EsSALUD

	FORTALEZAS	DEBILIDADES
SISTEMAS	<ul style="list-style-type: none"> • Contamos con personal Profesional Técnico (Analista Programador), Técnicos Administrativos y Personal Profesional (CAS) calificados, el cual cuenta con amplia experiencia en la administración del Sistemas de Gestión Hospitalaria, y otros, así como en el desarrollo e implementación de nuevos aplicativos acordes a la tecnología vigente. • Buen clima laboral. • Responsabilidad en el manejo de la información, equipamiento y materiales a su cargo. • Personal plenamente identificado con la institución. • Adecuado ambiente de trabajo, acorde a la infraestructura y tecnología moderna. • Acceso a información referente a recursos informáticos de última generación. 	<ul style="list-style-type: none"> • La estructura física no está correctamente distribuida y el espacio es muy reducido teniendo en cuenta la cantidad de personas que laboran en la oficina. • Carencia en muchos casos de un Hardware moderno en el cual se soporta nuestros sistemas de información (servidores y PC's). • Sistema de Videovigilancia obsoleto debido a su antigüedad en muchos casos los componentes (cámaras de videovigilancia) sufren fallas que no pueden ser reparadas. • El conocimiento, experiencia y funciones del personal no está acorde a las plazas que tienen asignadas. • El DATACENTER no está acorde a los estándares técnicos según la Norma TIA 942.

Fuente: Oficina de Soporte Informático (2017).



	FORTALEZAS	DEBILIDADES
COMUNICACIONES	<ul style="list-style-type: none"> • Contamos con Técnicos Administrativos, y Profesional (CAS) calificados y con experiencia en la administración de Redes y Telecomunicaciones. • Buen clima laboral. • Responsabilidad en el manejo de la información, equipamiento y materiales a su cargo. • Personal plenamente identificado con la institución. • Acceso a información referente a recursos informáticos de última generación. 	<ul style="list-style-type: none"> • La falta de herramientas (Hardware y Software) para la Administración de la red LAN que indique en forma estadística la utilización de sus medios de comunicación. • Limitación en la identificación del problema reportado en la red LAN de forma rápida. • Infraestructura inadecuada en las áreas de comunicaciones. • Carencia de Equipos y medios físicos de transmisión moderna en el cual transita nuestra información (Cableado Estructurado, Switches y otros). • Se cuenta con equipos obsoletos para nuestra Central Telefónica, generando dificultades en el servicio de voz. • Retraso para dar solución a la problemática de la Red LAN debido a la dependencia y necesidad de coordinar los permisos y configuraciones que se deben llevar a cabo en conjunto con el área de Comunicaciones de la Sede Central. • Falla continúa del Sistema de Circuito Cerrado de Televisión, debido a que sus componentes son obsoletos (Televisores) y que no pueden ser reparadas, asimismo se presenta casos de tarjetas y software de instalación se encuentran desactualizados.

Fuente: Oficina de Soporte Informático (2017).



Tabla 16
Análisis Externo de FODA HNERM EsSALUD

	OPORTUNIDADES	AMENAZAS
SISTEMAS	<ul style="list-style-type: none"> ● Cambio de Gestión. ● Nuevo Jefatura ● Nuevos Retos 	<ul style="list-style-type: none"> ● Nueva forma de Gestión ● Cambios de forma de trabajo ● Cambio de recurso humano.
SOPORTE TÉCNICO	<ul style="list-style-type: none"> ● Demanda Creciente ● Apoyo de las gerencias ● Política de reuniones en la gestión. ● Necesidad y requerimiento de información de la OTIC 	<ul style="list-style-type: none"> ● Limitado presupuesto para repuestos informáticos ● Escasos programas de capacitación. ● Hay presencia de riesgo del personal calificado por esquema remunerativo menor al mercado laboral Informático ● Desviación en los sectores político, ● Inestabilidad en el ciclo económico ● Fenómenos naturales.

Fuente: Oficina de Soporte Informático (2017).



	OPORTUNIDADES	AMENAZAS
COMUNICACIONES	<ul style="list-style-type: none"> • El avance Tecnológico proporciona un abanico de posibilidades que pueden ser aplicadas en los procesos de la Telefónica. • Posibilidad de lograr altos estándares de desarrollo de las telecomunicaciones. • Acceso a la Tecnología Informática que contribuya a la reducción de costos en las comunicaciones. • Acceso mediante Internet a la información técnica especializada para la adquisición de hardware y software. • Mejora continua de los procesos y procedimientos orientados a • brindar un mejor servicio a los usuarios internos y externos de la institución. • Posibilidad de contratar servicios de terceros para el desarrollo de actividades específicas que permita cumplir con las metas programadas. • Posibilidad de contratar servicios de comunicaciones. 	<ul style="list-style-type: none"> • Incremento de los requerimientos de renovación tecnológica de equipos de comunicaciones. • Situación económica del País, que se expresa en el escaso presupuesto para la adquisición de equipos de cómputo y Licencias de software. • Exigencia de los usuarios de una atención oportuna y segura, en la transmutación de sus solicitudes de servicio. • Constante amenazas de virus en la red. • Falta de confidencialidad con respecto a las claves de acceso, por parte del personal que labora con los sistemas de información • Rechazo por parte de los trabajadores a utilizar sistemas de información desconocidos. • Fallas constantes de los equipos, ya sea por su antigüedad u obsolescencia. • Elevados costos de hardware y software • Creciente demanda por servicios informáticos relacionados a consultas masivas. • Retraso en la entrega de insumos y repuestos necesarios para las actividades. • Interoperabilidad entre instituciones en proceso de Implementación.

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017).



5.3.4. Planes de contingencia

En cualquier proceso por razones obvias sabemos que en algún momento del tiempo de vida de ellas podría ocurrir cualquier evento inesperado que le podría causar problemas leves como graves que terminen alterando su funcionalidad y eficiencia, y para nuestro proyecto se han documentado una serie de pautas o recomendaciones a seguir en caso de que estas ocurran, esto con la finalidad de poder tener procedimientos establecidos que nos permitan tener una manera organizada de respuesta rápida en caso de que ocurran problemas en la red de área local, estas que las podrán ver líneas abajo:

I. Procesos de la Planificación

Evaluación

Análisis de los alcances que tendría en caso de ocurrir una incidencia, detallando las áreas afectadas.

Revisión

En esta etapa se toma en cuenta los planes que se llevarán a cabo previa evaluación.

No olvidemos que todo proceso se deberá documentar en cuanto haya sido atendido.

Ejecución

Acciones tomadas durante la ocurrencia de incidencias. Se estima tiempos de respuesta cortos para lograr la atención oportuna de las incidencias.

Estimación de riesgos en los diferentes aspectos a nivel software y hardware.

II. Análisis, Prevención y Mitigación de Riesgos

A continuación, destacamos los principales riesgos que debemos tener en cuenta ante cualquier incidente.

Tabla 17
Análisis Prevención y Mitigación de Riesgos

TIPO DE RIESGO	NIVEL DE RIESGO	PREVENCION Y MITIGACION	ENTREGABLE / PARAMETROS DE INFORMACION
Perdida de datos	Bajo	Realizar copias de respaldo de los aplicativos informáticos.	A través de un Informe que da a conocer la cantidad de copias de respaldo realizadas.
Difusión no autorizada de datos.	Bajo	Sancionar a nivel de reglamento según al área que corresponda.	Preventivo a través de memorándum .
Acceso no autorizado de datos	Medio	Realizar el cambio de claves de acceso como mínimo cada 30 días. Política de seguridad para acceso a personal competente. Inhabilitación de los accesos en coordinación de las áreas usuarias, en caso de cese, vacaciones, permisos o descansos médicos.	Se realiza previa solicitud por correo al jefe de informática. Ver anexo 1.
Malware	Medio	Antivirus institucional actualizado y actualizaciones de repositorio según corresponda, en coordinación con seguridad informática de GCTIC.	Informe del área encargada GCTIC de Sede central
Fraude	Bajo	Manejos de un super - usuario y usuarios para el ingreso a: Servidores de aplicaciones a nivel de usuario, operador y administrador.	Permiso asignado a personal autorizado.
Hurto de equipos	Medio	Cámaras de seguridad, Seguridad Privada, Alarmas, Copias de respaldo, Restricciones de acceso, Identificación plena de los equipos informáticos según inventario.	A través de un informe que da a conocer la ubicación de los equipos informáticos, así mismo cada equipo presenta código patrimonial para su identificación y traslado dentro del hospital, mediante formatos de traslado de equipos. Ver anexo 2.
Daños en el equipo	Medio	Mantenimiento preventivo y correctivo de los equipos.	Cuadro resumen de mantenimiento de equipos. Ver anexo 3.
Fuego	Medio	Sistema de alarma contra incendios (Extintores, aspersores automáticos, detectores de humo).	Informes del área encargada de defensa civil.
Humedad	Bajo	Mantener un sistema de temperatura adecuada de acuerdo a los estándares de la industria, con los elementos que implican: aire acondicionado, filtros de aire, alarma local.	Informes del área encargada de mantenimiento del HNERM.
Terremoto	Bajo	Cumplir con las normas antisísmicas. Cumplir con la norma ANSI/TIA-942, ANSI / TIA-1179: Infraestructura de telecomunicaciones para instalaciones sanitarias, Norma Técnica de Salud N°119-MINSA/DGIEM para Data Center, la cual considera equipamiento con redundancia en todos los sistemas instalados e infraestructura. Copias de respaldo.	Informe preventivo según la norma ANSI/TIA-942 para Data Center. Ver anexo 4.

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017).



III. Proyección de Indicadores

Se evaluarán según los entregables, siguiendo los siguientes lineamientos internacionales de preparación ante los desastres para una respuesta eficaz, citado por organismos internacionales.

Claridad

Ausencia de ambigüedad sobre lo que se está midiendo para neutralizar toda probabilidad de que se cuestione la interpretación de los resultados.

Eficacia en función de los costos

Los resultados justifican su inversión en tiempo y dinero. Los resultados deben basarse en procesos y actividades asequibles.

Fiabilidad

Los datos son de una calidad suficientemente fiable y constituyen una buena base para una adopción de decisiones segura.

Viabilidad

Los datos se pueden obtener de forma oportuna

Especificidad

El indicador debe medir únicamente la unidad o el proceso previsto.

IV. Niveles de Atención

Tabla 18
Cuadro de Niveles de Atención por tipo de Riesgo

TIPO DE RIESGO	NIVEL DE RIESGO	ENTREGABLE / PARAMETROS DE INFORMACION	INDICADORES
Perdida de datos	Bajo	Informe	Cantidad de copias por mes.
Difusión no autorizada de datos.	Bajo	Memorándum	Firma de recepción de conformidad por área.
Acceso no autorizado de datos	Medio	Solicitud	Porcentaje (%) solicitudes trimestralmente.
Malware	Medio	Informe	GCTIC de Sede central
Fraude	Bajo	Permisos	Porcentaje (%) de permisos.
Hurto de equipos	Medio	Informe	Cantidad de equipos con patrimonio.
Daños en el equipo	Medio	Cuadro resumen	Cantidad de equipos con mantenimiento preventivo.
Fuego	Medio	Informe	Defensa civil
Humedad	Bajo	Informe	Porcentaje (%) de humedad.
Terremoto	Bajo	Informe preventivo	Porcentaje de cumplimiento de la norma ANSI/TIA-942 anualmente.

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017).



V. Niveles de Atención

Debemos definir el nivel de atención tanto de los aplicativos informáticos como el hardware y el performance de la Red LAN, para saber cuál es la prioridad según su funcionamiento.

Tabla 19
Niveles de Atención de los Aplicativos Informáticos

NIVEL	NIVEL DE ATENCION	DESCRIPCION
1	Alta	Aplicativos informáticos y equipos que requieran alta disponibilidad de atención a los usuarios externos y manejen grandes volúmenes de información, equipos electrónicos y conmutadores (switches) de los cuales dependa directamente el funcionamiento de los aplicativos y el hardware que los contiene.
2	Normal	Aplicativos informáticos y equipos no relacionados con la atención a los usuarios y manejen bajo volumen de información. Ejemplo: Impresoras, Aplicativos que no requirieran conectividad y que cuenten con mayor plazo para la consulta y disponibilidad de información.

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017).



VI. Hardware Activo

Para la aplicación de la planificación necesitamos tener conocimiento de los equipos instalados en el HNERM–EsSALUD, a nivel prioritario tenemos los sistemas de comunicaciones conmutadores (switches), servidores, institucionales (equipos de cómputo).

Tabla 20

Servidores de la Oficina de Soporte Informático del HNERM EsSALUD

NOMBRE DEL SERVIDOR	NOMBRE ESPECIFICADO	SISTEMA OPERATIVO	
Servidor de Gestión Hospitalaria - Producción	WM - Rebagliati	Linux	Red Hat
Servidor de Gestión Hospitalaria – Histórico	WM - Rebagliati	Linux	Red Hat
Servidor de Gestión Hospitalaria - Producción Respaldo	WM - Rebagliati	Linux	Red Hat
Servidor de cámaras I	Ws-40409	Windows	Xp
Servidor de cámaras II	Ws-40410	Windows	Xp
Servidor de beckton dickinson citometria de flujo	Serverlab	Windows	Server 2008 r2 standard
Servidor de diagnostica peruana radians aga	Dpsac-pc	Windows	Seven
Servidor de roche datalab	Servidor	Windows	Server 2003 standard
Servidor de roche banco de órganos	Srvbanco	Windows	Server 2003 standard
Servidor de PAC's de imágenes	PAC's Rebagliati	Linux	Red hat 5.3
Servidor de PAC's de imágenes - Respaldo	PAC's Rebagliati	Linux	Red hat 5.3
Servidor de PAC's de imágenes – Producción nueva emergencia	PAC's Rebagliati	Linux	Red hat 5.3
Servidor de U MERC	UMERC	Windows	Centos 6.0
Servidor de gastroenterología	Gastro	Windows	Xp
Servidor repositorio de antivirus Sophos	SR-VII-Rebagliati	Linux	Red hat 5.3
Servidor repositorio de antivirus Sophos - Respaldo	SR-VII-Rebagliati	Linux	Red hat 5.3
Servidor de cevit	Rar-ogit	Linux	Red hat 5.3
Servidor de correo electrónico	Hreb	Linux	Suselinux
Servidor de correo electrónico - Respaldo	Hreb	Linux	Suselinux
Servidor de infinity roche	Srvinfinityreba	Windows	Server 2008 r2 standard
Servidor Enterprise representaciones medicas	Enterprise	Windows	Server 2008 r2 standard
Servidor de aplicaciones web 2	Localhost	Linux	Red hat 5.3
Servidor de mamografías	Serv-rebagliati	Linux	Red hat 5.3
Servidor de histórico de farmacia	Rar-farmacia	Linux	Red hat 5.3
Servidor de histórico de farmacia - Respaldo	Rar-farmacia	Linux	Red hat 5.3
Servidor de finanzas	Finanzas	Linux	Suselinux
Servidor Rebanet	Rebanet	Linux	
Servidor de control biométrico RRHH	Pc_servarchivos	Windows	Server 2000
Servidor de archivo RRHH	Pc_servremu	Windows	Xp
Servidor web linux RRHH	Servremu2	Linux	Ubuntu



Servidor web windows RRHH	Web	Windows	Ocho
Servidor de cubos de información - ogid	Cubos	Linux	
Servidor servicedesk	Servicedesk	Linux	Centos 6.0
Servidor pc_archivos - OGID	Archivos	Linux	
Servidor de transformación - OGID	Transformación	Linux	
Servidor de datos estadísticos - OGID	Estadística	Linux	
Servidor de aplicaciones - OGID	Aplicaciones	Linux	
Servidor de tamizaje neonatal	Srv-server	Windows	Server 2008 r2 standard
Servidor rochembiocare - lab core	Rochembiocare	Windows	Server 2008 r2 standard
Servidor UAL - delphy	Edelphynreba	Windows	Server 2012 r2 standard
Servidor interfaces - UAL	Interfasereba	Windows	Server 2008 r2 standard

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017).



Tabla 21
Dispositivos conmutadores en General del HNERM-EsSALUD

Equipos Intermedios Switches de la Red de Telecomunicaciones del Hospital Nacional Edgardo Rebagliati Martins												
N°	MARCA	TIPO	MODELO	VELOCIDAD	CONFIGURACION	VLAN	CAPA	SFP	GE	ETH	CANTIDAD	
1	ALCATEL-LUCENT	CORE PRINCIPAL	OmniSwitch 9800	10/100/1000	MODULAR	Administrables	SI	L2/L3	24	168	-	1
2	CISCO	CORE CAMARAS	Catalyst 3750	10/100/1000	FIJO	Administrables	SI	L2/L3	12	-	-	7
3	D - LINK	CORE BACKUP	DXS - 3326GSR	10/100/1000	FIJO	Administrables	SI	L2/L3	24	4	-	1
4	CISCO	-	Router BEFSR81	-	FIJO	-	-	-	-	-	8	1
5	D - LINK	-	DIR-400 ROUTER	-	FIJO	-	-	-	-	-	24	1
6	ALCATEL-LUCENT	BORDE DATOS	OmniStack LS 6224P	10/100	FIJO	Administrables	SI	L2	4	2	24	31
7	ALIED TELESIS	BORDE DATOS	AT 8000S/24POE	10/100	FIJO	Administrables	SI	L2	2	2	24	1
8	CISCO	BORDE CAMARAS	Catalyst 3560 Series POE	10/100	FIJO	Administrables	SI	L2	1	1	8	7
9	3COM	DISTRIBUCION	Super Stack 5500G -EL	10/100	FIJO	Administrables	SI	L2	2	2	24	6
10	3COM	DISTRIBUCION	Baseline Switch 2824	10/100	FIJO	Administrables	SI	L2	2	2	24	3
11	A VAYA	DISTRIBUCION	P334T	10/100	FIJO	Administrables	SI	L2	2	2	48	1
12	ALIED TELESIS	DISTRIBUCION	AT- GS950	10/100/1000	FIJO	Administrables	SI	L2	2	2	8	1
13	D - LINK	DISTRIBUCION	DGS - 3100	10/100/1000	FIJO	Administrables	SI	L2	4	24	-	1
14	D - LINK	DISTRIBUCION	DGS - 3024	10/100/1000	FIJO	Administrables	SI	L2	4	24	-	5
15	D - LINK	DISTRIBUCION	DGS - 3120	10/100/1000	FIJO	Administrables	SI	L2/L3	4	24	-	1
16	D - LINK	DISTRIBUCION	DGS - 1510	10/100/1000	FIJO	Administrables	SI	L2/L3	4	24	-	22
17	D - LINK	DISTRIBUCION	DGS - 1210	10/100/1000	FIJO	Administrables	SI	L2	4	24	-	3
18	D - LINK	DISTRIBUCION	DES - 1024A	10/100	FIJO	Stand-alone	NO	-	-	-	24	60
19	D - LINK	DISTRIBUCION	DES - 1024D	10/100	FIJO	Stand-alone	NO	-	-	-	24	79
20	D - LINK	DISTRIBUCION	DES - 1016D	10/100	FIJO	Stand-alone	NO	-	-	-	16	2
21	D - LINK	DISTRIBUCION	DES - 1060D	10/100	FIJO	Stand-alone	NO	-	-	-	16	1
22	TRENDnet	DISTRIBUCION	TEG - 516DG	10/100	FIJO	Stand-alone	NO	-	-	-	16	1

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017).



Tabla 22
Dispositivos conmutadores Administrables Switches D-LINK

SWITCHES D-LINK DGS-1510-28 SMARTPRO SWITCH																			
N°	MARCA	TIPO	MODELO	PART NUMBER	N° SERIE	VERSION	VELOCIDAD	IP	MASK	MAC	VOLTAJE			CONSOLA	N° PORT FIBRA	N° PORT COBRE	COD BARRAS	FECHA COMPRA	FECHA INSTAL
1	D-LINK	SMARTPRO SWITCH	DGS-1510-28	IGS15028A...A1G	RZHYIEA000004	1.10.005	10/100/1000	10.90.90.90	255.0.0.0	E8:CC:18:CB:62:A0:BF	100-240 VAC	50-60 HZ	0.75 A	SI	4	24	790069399466	8/06/2015	1/07/2015
2	D-LINK	SMARTPRO SWITCH	DGS-1510-28	IGS15028A...A1G	RZHYIEA000005	1.10.005	10/100/1000	10.90.90.90	255.0.0.1	E8:CC:18:CB:63:20:3F	100-240 VAC	50-60 HZ	0.75 A	SI	4	24	790069399466	8/06/2015	1/07/2015
3	D-LINK	SMARTPRO SWITCH	DGS-1510-28	IGS15028A...A1G	RZHYIEA000006	1.10.005	10/100/1000	10.90.90.90	255.0.0.2	E8:CC:18:CB:63:40:5F	100-240 VAC	50-60 HZ	0.75 A	SI	4	24	790069399466	8/06/2015	1/07/2015
4	D-LINK	SMARTPRO SWITCH	DGS-1510-28	IGS15028A...A1G	RZHYIEA000007	1.10.005	10/100/1000	10.90.90.90	255.0.0.3	E8:CC:18:CB:63:C0:DF	100-240 VAC	50-60 HZ	0.75 A	SI	4	24	790069399466	8/06/2015	1/07/2015
5	D-LINK	SMARTPRO SWITCH	DGS-1510-28	IGS15028A...A1G	RZHYIEA000008	1.10.005	10/100/1000	10.90.90.90	255.0.0.4	E8:CC:18:CB:63:A0:BF	100-240 VAC	50-60 HZ	0.75 A	SI	4	24	790069399466	8/06/2015	1/07/2015
6	D-LINK	SMARTPRO SWITCH	DGS-1510-28	IGS15028A...A1G	RZHYIEA000009	1.10.005	10/100/1000	10.90.90.90	255.0.0.5	E8:CC:18:CB:5F:E0:FF	100-240 VAC	50-60 HZ	0.75 A	SI	4	24	790069399466	8/06/2015	1/07/2015
7	D-LINK	SMARTPRO SWITCH	DGS-1510-28	IGS15028A...A1G	RZHYIEA000013	1.10.005	10/100/1000	10.90.90.90	255.0.0.6	E8:CC:18:CB:63:00:1F	100-240 VAC	50-60 HZ	0.75 A	SI	4	24	790069399466	8/06/2015	1/07/2015
8	D-LINK	SMARTPRO SWITCH	DGS-1510-28	IGS15028A...A1G	RZHYIEA000014	1.10.005	10/100/1000	10.90.90.90	255.0.0.7	E8:CC:18:CB:62:E0:FF	100-240 VAC	50-60 HZ	0.75 A	SI	4	24	790069399466	8/06/2015	1/07/2015
9	D-LINK	SMARTPRO SWITCH	DGS-1510-28	IGS15028A...A1G	RZHYIEA000015	1.10.005	10/100/1000	10.90.90.90	255.0.0.8	E8:CC:18:CB:63:80:9F	100-240 VAC	50-60 HZ	0.75 A	SI	4	24	790069399466	8/06/2015	1/07/2015
10	D-LINK	SMARTPRO SWITCH	DGS-1510-28	IGS15028A...A1G	RZHYIEA000016	1.10.005	10/100/1000	10.90.90.90	255.0.0.9	E8:CC:18:CB:63:60:7F	100-240 VAC	50-60 HZ	0.75 A	SI	4	24	790069399466	8/06/2015	1/07/2015
11	D-LINK	SMARTPRO SWITCH	DGS-1510-28	IGS15028A...A1G	RZHYIEA000017	1.10.005	10/100/1000	10.90.90.90	255.0.0.10	E8:CC:18:CB:64:20:3F	100-240 VAC	50-60 HZ	0.75 A	SI	4	24	790069399466	8/06/2015	1/07/2015
12	D-LINK	SMARTPRO SWITCH	DGS-1510-28	IGS15028A...A1G	RZHYIEA000018	1.10.005	10/100/1000	10.90.90.90	255.0.0.11	E8:CC:18:CB:63:E0:FF	100-240 VAC	50-60 HZ	0.75 A	SI	4	24	790069399466	8/06/2015	1/07/2015

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017).



a. Riesgos estructurales

1. Sismos, incendios y fugas de líquidos.
2. Falta de refrigeración.
3. Falta de suministro eléctrico.
4. Falla o errores en los aplicativos donde físicamente se encuentren instalados.
5. Pérdida de información.
6. Tardía respuesta de la empresa que realiza su mantenimiento.
7. Contratación o ejecución de soluciones inadecuadas o incompatibles con los recursos disponibles.

b. Soluciones en Contingencia

Garantizar el mantenimiento preventivo-correctivo 7x24.

En el momento de la emergencia, los usuarios deberán seguir una serie de pasos para la respuesta en el menor tiempo posible.

1. Se cuenta con la tercerización de servicios tales como: mantenimiento preventivo-correctivo de central telefónica, redes y comunicaciones; mantenimiento preventivo-correctivo de servidores; mantenimiento preventivo-correctivo de equipamiento informático.
2. Informar a la mesa de ayuda los problemas detectados en Hardware y Software. El reporte puede ser telefónicamente o personalmente.
3. El personal encargado recibe la solicitud del servicio (Hardware ó Software). Evalúa y atiende el servicio reportado.
4. El personal encargado verifica falla y/o requerimiento el área y elabora diagnóstico.
5. Al finalizar la atención el personal encargado documentará los procedimientos seguidos para la resolución del incidente.



VII. Software Activo

Para la aplicación del plan de contingencia necesitamos tener conocimiento de los aplicativos informáticos que maneja el HNERM– EsSALUD, tanto en el área asistencial como en el área administrativa.

Tabla 23

Cuadro de Aplicativos Informáticos Actuales de la OSI HNERM EsSALUD

NOMBRE DEL APLICATIVO	DESCRIPCION
SGH	Es el aplicativo más importante que Maneja el HNERM, su importancia radica en el uso que se realiza a nivel de todas las áreas del hospital.
PACS DE IMAGENES	Aplicativo que sirve para visualizar las imágenes radiológicas.
UMERC	Aplicativo que permite gestionar el proceso de diagnóstico y tratamiento de los pacientes de nefrología.
VISOR WEB DE LABORATORIO	Se Implementó la primera fase del aplicativo en el que se muestra los resultados de laboratorio en línea.
CITOLOGIA	Aplicativo que permite visualizar los resultados de PAP a nivel de Red.
SIGE	Esta aplicación alberga un panel de administración donde alberga los distintos sistemas a alojar, donde los accesos de usuarios son manejados por un Panel de Control donde se realizan los permisos respectivos alineados al perfil del usuario.
MODULO DE ADMINISTRACION RPM	Se desarrolló con la finalidad de obtener un mayor control sobre los equipos telefónicos RPM.
SERVICE DESK	Mesa de ayuda para registrar incidencias.
CODTELFCELM	Aplicativo que permite autogenerar aleatoriamente códigos de autorización de llamadas externas locales, nacionales y telefonía móvil.
SISTEMA DE VIDEOVIGILANCIA	Aplicativo para la seguridad a través de video en las diferentes áreas del HNERM.

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017).

Riesgos a nivel de software

- a. Falla o errores en los aplicativos donde se encuentren instalados.
- b. Pérdida de información
- c. Posible falla de equipos electrónicos
- d. Hardware con deficiencia anteriormente detectada.



Soluciones en contingencia

- a. Levantar los aplicativos desde los servidores virtualizados.
- b. Levantar los aplicativos con las copias de respaldo si fuera el caso
- c. Hacer de conocimiento al usuario los inconvenientes presentados para evitar el mal uso de los aplicativos mientras se encuentren restableciéndose.
- d. En el momento de la emergencia, los usuarios deberán seguir el protocolo para la respuesta en el menor tiempo posible.
- e. Reportar la falla en el aplicativo
- f. Esperar las indicaciones mientras se inician las acciones pertinentes para el restablecimiento del proceso.

VIII. Conclusiones

- a. En el presente Proyecto de Planificación de Sistemas de Información están descritos los procedimientos a seguir, de manera tal que se puedan cumplir estrictamente para la resolución de los incidentes en el menor tiempo posible.
- b. Lograr la continuidad de los diferentes servicios, los aplicativos informativos, el performance de la Red LAN y el hardware (parque informático) ante cualquier incidente.
- c. Informar a los usuarios los pasos a seguir en caso de ocurrir una incidencia en el uso de los aplicativos y/o hardware, de forma que sean reportados oportunamente.
- d. Concientizar a las áreas encargadas acerca de la seguridad de la información, tener en cuenta que el seguimiento del presente proyecto de Planificación de Sistemas de Información no solo implica a la Oficina de Soporte Informático, sino que debe comprometer a toda la institución, resaltando su importancia.



Anexo 1

Tabla 24

Cuadro del total de Usuarios en el HNERM EsSALUD

MODULO	CODIGO	Nº USUARIOS
ADMISION	AD	1019
CONSULTA EXTERNA	CE	702
FARMACIA	FA	346
HOSPITALIZACION	HO	999
EMERGENCIA	EM	830

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017).

Solicitud de Accesos

Todo acceso de usuarios se pide por correo electrónico dirigido al jefe de informática, el cual autoriza la creación, modificación y anulación de los mismos.

A continuación, se detalla un ejemplo de los usuarios creados y se adjunta los correos donde se solicita dichos permisos.

Tabla 25

Cuadro de Solicitantes vía correo en el HNERM EsSALUD

AREA SOLICITANTE	USUARIO	FECHA
Unidad de administración de personal – Rebagliati	Sandra Paola Mostacero Ventura	26/10/2016

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017).



Documentos de Sustento:

Altamirano Castillo Cesar Antonio

De: Cardenas Porras July
Enviado el: miércoles, 26 de octubre de 2016 12:10 p.m.
Para: Jose Eduardo Nonato Maravi
CC: Altamirano Castillo Cesar Antonio
Asunto: RE: Solicitud de accesos al SIAD

Saludos cordiales,

Estimado Sr. José, solicito lo siguiente:

- Creación de usuario:

DATOS DE CREACION DE USUARIOS Y ASIGNACION DE DEPENDENCIAS					
Nombres	Apellidos	DNI	Código Planilla	Código Dependencia	Dependencia
Sandra Paola	Mostacero Ventura	42178347	6116770	<0843>	Unidad De Admin. De Personal-Rebagliati
Paola Verónica	Laqui Flores	42370359	6113059	<0843>	Unidad De Admin. De Personal-Rebagliati

July Cárdenas Porras
 Oficina de Soporte Informático
 RPM #790081 – Anexo 3329

Antes de imprimir un e-mail piense bien si es necesario hacerlo. El medio ambiente es cosa de todos.

De: Sandra Mostacero Ventura [mailto:sandra.mostacero@essalud.gob.pe]
Enviado el: martes, 25 de octubre de 2016 03:43 p.m.
Para: Cardenas Porras July <externo.jcardenasp@essalud.gob.pe>
Asunto: RE: Solicitud de accesos al SIAD

Estimada July el código de planilla de la Sra. Paola Laqui Flores es el 6113059.

Atentamente,

De: Cardenas Porras July [mailto:externo.jcardenasp@essalud.gob.pe]
Enviado el: martes, 25 de octubre de 2016 12:38
Para: Sandra Mostacero Ventura
Asunto: RE: Solicitud de accesos al SIAD

Saludos cordiales,

Estimada Sandra, indicar cuál es el Código de Planilla del Paola Verónica.

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



Solicitud de requerimiento de cambio de dispositivos conmutadores.

Todas las observaciones y quejas se originan por las caídas frecuentes de la Red LAN que afectan la continuidad de 125 servicios de alta complejidad por la inoperatividad de los Aplicativos Institucionales, motivo por el cual no se pueden generar las recetas, citas, resultados, interconsultas, hojas sucintas e informes tanto en la hospitalización con más de 1500 camas, en las áreas de apoyo al diagnóstico como Laboratorio, Rx, Ecografía, Mamografía, Sonografía, Tomografía, Resonancia Magnética, PC/TCAN, en los 95 consultorios externos, las 05 Emergencias y las áreas administrativas del HNERM-EsSALUD; esto ocasiona el malestar de miles de pacientes que vienen a atenderse, siendo las prestaciones de salud la razón principal de nuestro negocio que brindamos a nuestros asegurados.

Estos requerimientos se solicitan y se gestionan a través de los correos electrónicos para acortar tiempo y disminuir la burocracia administrativa, esto va dirigido al jefe de la Oficina de Soporte informático el cual coordina directamente con el personal operativo del area de comunicaciones encargado de resolver de manera inmediata el funcionamiento de la Red LAN en HNERM-EsSALUD. A continuación, se detalla un ejemplo del requerimiento de adquisición de los dispositivos de conmutación y de las quejas sobre la problemática de la caídas de la Red LAN en el HNERM-EsSALUD.

Tabla 26
Cuadro de Usuarios Solicitantes en el HNERM EsSALUD

AREA SOLICITANTE	USUARIO	FECHA
Oficina de Admisión y Registro Médicos – Rebagliati	Dr. Grillo Cicirello Félix E.	02/10/2018
Oficina de Soporte Informático– Rebagliati	Ing. Cesar Altamirano Castillo	20/07/2017
Oficina de Administración– Rebagliati	Ing. José Aquino Caveró	28/03/2016

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017).



Documentos de Sustento:

De: Grillo Cicirello <>
Enviado el: sábado, 2 de junio de 2018 18:37
Para: 'Duniam Duniam Ángelo' <>
CC: edwin.estrada@essalud.gob.pe; 'Aldo Vasquez' <aldo.vasquez@essalud.gob.pe>; oscar.becerra@essalud.gob.pe; raul.cerna@essalud.gob.pe; yeni.seclen@essalud.gob.pe; jmatos@essalud.gob.pe; richard.anchante@essalud.gob.pe; juan.prieto@essalud.gob.pe;
Asunto: INFORME SOBRE SERVICIOS AFECTADOS SIN CONEXIÓN DE RED LAN - HNERM

Ingeniero

Ángelo D'Uniam D'Uniam

Jefe de la Oficina de Soporte Informático

Red Asistencial Rebagliati – EsSALUD

HNERM

Presente. -

ASUNTO : INFORME SOBRE SERVICIOS AFECTADOS SIN CONEXIÓN DE RED LAN – HNERM OCASIONA MALESTAR A LOS MILES DE ASEGURADOS.

Por medio de la presente me dirijo a Ud. para saludarlo muy cordialmente, y hacer de su conocimiento que no habido sistema de los aplicativos desde muy temprano afectando los diferentes servicios para la atención de los pacientes programados, esto se originó por las caídas de las conexiones de los Gabinetes de Red LAN, - Gab. J, Gab K, Gab Ñ, siendo afectados en su totalidad las siguientes áreas:

AREAS AFECTADAS**Gabinete J**

- Taller de Pinturas
- Taller de Carpintería
- Taller de Mecánica
- Taller de Persianas y Puertas
- Taller de Vidriería
- Unidad de Transportes – Ambulancias
- Área de Comunicaciones – Informática
- Área de Soporte Técnico – Informática
- Área de Mesa de Ayuda – Informática
- Caseta de seguridad y vigilancia – bajada rampa

Gabinete K

- Emergencia de Salud Mental
- Consultorios Externos de Salud Mental



- Hospitalización I de Salud Mental
- Hospitalización II de Salud Mental
- Programas de Salud Mental
- Farmacia de Salud Mental
- Hospital de Día Salud Mental
- Jefaturas Departamento Salud Mental
- Áreas Administrativas Salud Mental
- Caseta de Vigilancia Salud Mental

Gabinete Ñ

- Unidad de Terapia del dolor – antigua Emergencia Adultos
- unidad de atención rápida – antigua Emergencia Adultos
- Sala de Espera – Emergencia Adultos
- Ambiente de Toma de Muestras - entrada de Velatorio
- Ambiente de Relaciones Publicas - Emergencia Adultos
- caseta de Vigilancia Toma de Muestras – Antigua Emergencia

Es necesario la adquisición de nuevos equipos tecnológicos para la continuidad de los servicios y aplicativos institucionales.

Es cuanto informo a usted para los fines según correspondan.

Saludos cordiales



Dr. Grillo Cicirello Félix Eduardo
Oficina de Admisión y Registro Médicos
Hospital Nacional Edgardo Rebagliati Martins - EsSALUD
 Teléfono: 265-4901, - Anexo: 3284
Av. Rebagliati N°490, Jesús María - Lima



De: Altamirano Castillo Cesar Antonio [<mailto:antonio.altamirano@essalud.gob.pe>]

Enviado el: martes, 29 de noviembre de 2017 2:35 p. m.

Para: raul.sanchez@essalud.gob.pe

Asunto: RV: RE: Evaluación del Servidor de Producción del SGH - Hosp. REBAGLIATI
Coordinaciones sobre problemática del servidor de producción.

Saludos Cordiales

Atentamente.

Ing. Cesar Antonio Altamirano Castillo

Ingeniero de Sistemas e Informática-**CIP:134368**

Jefe de la Oficina de Soporte Informático

HNERM - RAR

Anexo: 2654901 - 3868

RPM: #041746

De: Altamirano Castillo Cesar Antonio

Enviado el: miércoles, 20 de julio de 2017 10:10 p.m.

Para: Diaz Velarde Luis Gary <gary.diaz@essalud.gob.pe>

CC: Valencia Huanca Yury Edwin <yury.valencia@essalud.gob.pe>; Aquino Cavero José <jose.aquino@essalud.gob.pe>; Arias Schreiber Barba Malu <malu.arias@essalud.gob.pe>; Pérez Pichis Luis <luis.perezp@essalud.gob.pe>

Asunto: Fwd: RE: Evaluación del Servidor de Producción del SGH - Hosp. REBAGLIATI

Ing. Luis Gary Diaz Velarde

Atención. _

De mi mayor consideración:

Estimado Ing. Diaz, previo un cordial saludo y agradecimiento por el apoyo que brinda y en razón a las incidencias presentadas en el servidor de producción que tiene instalado el Sistema de gestión hospitalaria, sobre el cual se registran todas las Atenciones asistenciales en el Hospital Rebagliati y La Nueva Emergencia, también considerando las recomendaciones del Ing. Wilfredo Guzmán es que solicito como tema muy URGENTE la instalación del Sistema de Gestión hospitalaria sobre el nuevo servidor Adquirido el mismo que ya se encuentra ubicado en el DATACENTER del hospital Rebagliati. Se sugiere se dé inicio a la instalación, configuración y migración de la data a partir de mañana, con el apoyo del Ing. Wilfredo Guzmán e Ing. Martin Toscano.

Cabe precisar que el servidor actual aun presenta problemas, el mismo que esta inestable en la gestión de sus recursos, lo que ocasiona lentitud sobre las transacciones, como consulta y grabación, tomando en ocasiones como 10 minutos solo para grabar una receta, solo por citar un ejemplo.

Me despido agradeciendo la atención a lo solicitado.

Atentamente

Ing. Cesar Altamirano Castillo
 Jefe de la Oficina de Soporte Informática.

----- Mensaje reenviado -----

De: Jorge Luis Matos Centeno <jmatos@essalud.gob.pe>
 Fecha: 20/7/2017 20:01
 Asunto: RE: Evaluación del Servidor de Producción del SGH - Hosp. REBAGLIATI
 Para: Altamirano Castillo Cesar Antonio <antonio.altamirano@essalud.gob.pe>
 Cc: Guzmán Pachерres Wilfredo <wguzman@essalud.gob.pe>, Richard Anchante Torres <richard.anchante@essalud.gob.pe>

Ing. Cesar Altamirano, es necesario indicar que la carga del Servidor de producción se mantuvo elevada entre 46% y 52%. En este momento con una cantidad mínima de usuarios de 110 se mantiene en 17.33%, además que ya no están en línea los usuarios de Consulta externa.

Como se muestra en la imagen adjunta.

```

root@Rhel53-Rebagliati:~
top - 19:52:07 up 2:03, 110 users, load average: 17.33, 29.49, 34.89
Tasks: 635 total, 1 running, 634 sleeping, 0 stopped, 0 zombie
Cpu(s): 1.7%us, 1.3%sy, 0.0%ni, 56.7%id, 40.1%wa, 0.0%hi, 0.2%si, 0.0%st
Mem: 12470976k total, 3543160k used, 8927816k free, 370336k buffers
Swap: 2096440k total, 0k used, 2096440k free, 2649900k cached

  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM    TIME+  COMMAND
 23553 mmurillo  15   0 19508 8140 2164 S   3.3   0.1   0:32.74  smbd
 28518 sesteban  15   0  2772 2080  892 S   1.7   0.0   0:00.17  foxr.pr
   6939 emer11   15   0  3068 2432  948 S   1.0   0.0   0:04.12  foxr.pr
 23556 root     16   0  2596 1468  828 S   1.0   0.0   0:26.00  top
   9048 fa01cext 16   0  2952 2316  948 S   0.7   0.0   0:03.93  foxr.pr
 10573 root     16   0  2584 1420  800 S   0.7   0.0   0:52.55  top
 22328 celim    16   0  4020 3388  952 S   0.7   0.0   0:03.06  foxr.pr
 28425 jefserv  15   0  2872 2204  916 S   0.7   0.0   0:00.92  foxr.pr
   3024 root     34  19     0     0     0 S   0.3   0.0   0:15.65  kipmi0
   8633 fa01slm  15   0 10136 1692 1128 S   0.3   0.0   0:00.98  sshd
   9016 root     15   0  1888  808  668 S   0.3   0.0   0:00.26  in.telnetd
 13180 emer01  16   0  3112 2468  936 S   0.3   0.0   0:05.22  foxr.pr
 14821 ho08a  15   0  2560 1888  912 S   0.3   0.0   0:02.00  foxr.pr
 18805 celim    15   0  3784 3164  964 S   0.3   0.0   0:03.21  foxr.pr
 22332 refer    15   0  2984 2328  928 S   0.3   0.0   0:02.66  foxr.pr
 28392 root     15   0  1888  804  668 S   0.3   0.0   0:00.04  in.telnetd
 29178 root     15   0  2596 1352  800 R   0.3   0.0   0:00.41  top
     1 root     15   0  2064  628  536 S   0.0   0.0   0:01.01  init
     2 root     RT  -5     0     0     0 S   0.0   0.0   0:00.00  migration/0
     3 root     34  19     0     0     0 S   0.0   0.0   0:00.00  ksoftirqd/0
    
```

Atentamente,
Jorge Luis Matos Centeno
 Oficina Tecnologías de Información y Comunicaciones
 Hospital Nacional Edgardo Rebagliati Martins



De: Guzmán Pacherras Wilfredo [<mailto:wguzman@essalud.gob.pe>]

Enviado el: miércoles, 20 de julio de 2017 19:26

Para: Diaz Velarde Luis Gary <gary.diaz@essalud.gob.pe>

CC: Altamirano Castillo Cesar Antonio <antonio.altamirano@essalud.gob.pe>; Mesa de Ayuda EsSALUD <mesadeayuda@essalud.gob.pe>; Jorge Matos <jmatos@essalud.gob.pe>

Asunto: Evaluación del Servidor de Producción del SGH - Hosp. REBAGLIATI

Buenas tardes **Gary**, te remito la evaluación realizada al Servidor de Producción del SGH del Hospital Rebagliati.

A las 11:00 am. que me apersono a evaluar el equipo, este se encontraba en el siguiente estado:

- **Servidor IBM System X3650 – Año 2007**
- **RAM 12 GB.**
- **3 Discos de 143 GB. c/u.**
- **Procesador Intel Xeon Quad Core de 2.66 GHZ.**

1. Con un promedio de consumo de recursos de 195% con 380 usuarios conectados.
2. Estaba activado el MYSQL y POSTGRES
3. Algunos procesos del CRON del usuario ROOT, estaban ejecutándose a intervalos muy pequeño de tiempo.

Para ubicar el origen de los problemas indicados anteriormente, se realizaron las siguientes acciones.

1. Se verifico que el arreglo de discos (RAID 5) del Servidor, este sin INTEGRO y sincronizado.
2. Se verifico que ningún de los discos tengas problemas FISICOS.
3. Se verifico que la tarjeta controladora de arreglo de discos NO presente problemas al iniciar el Servidor.
4. Se verifico que la BATERIA de la Controladora de Arreglo de Discos, NO este con problemas o descargada.
5. Se cambiaron los discos del Servidor de Producción, al Servidor Histórico del SGH, este equipo tiene solo 8 GB. de RAM, el de producción tiene 12 GB.

Las acciones realizadas lograron que el consumo de recursos del Servido disminuya un poco, pero mantenía la LENTITUD a la hora de GRABAR o IMPRIMIR una cita por el SGH.

Al momento de enviar este correo, el consumo de recursos del Servidor esta como se muestra en la siguiente pantalla, lo cual es ALTO, para la cantidad de usuarios que se tiene conectados en estos momentos, esto también NO ASEGURA que el servidor vuelva a presentar los mismos problemas de Hoy por la mañana.



```

root@Rhel53-Rebagliati:~# top - 18:46:34 up 58 min, 132 users,  load average: 13.28, 14.80, 13.9
Tasks: 711 total,  1 running, 710 sleeping,  0 stopped,  0 zombie
Cpu(s):  1.4%us,  0.9%sy,  0.0%ni, 49.7%id, 47.9%wa,  0.0%hi,  0.1%si,
Mem: 12470976k total, 3145252k used, 9325724k free, 283168k buffe
Swap: 2096440k total,  0k used, 2096440k free, 2336892k cache

  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM     TIME+  COMMAND
 10573 root        16   0  2584 1388  800  S   1.0   0.0   0:18.31 top
 18686 root        15   0  2596 1388  800  R   1.0   0.0   0:00.13 top
   9314 root        16   0  2592 1388  800  S   0.7   0.0   0:19.84 top
 10096 jefserv    16   0  2852 2164  892  S   0.7   0.0   0:00.26 foxxr.pr
14657 ho05c     16   0  3108 2576 1044  D   0.7   0.0   0:02.30 foxxr.pr
16596 rayosx    15   0  2552 1876  908  S   0.7   0.0   0:01.23 foxxr.pr
   222 root        15   0    0    0    0  S   0.3   0.0   0:00.35 pdflush
  2179 root        10  -5    0    0    0  D   0.3   0.0   0:02.50 kjournald
  7261 refer     15   0  3292 2652  940  S   0.3   0.0   0:03.73 foxxr.pr
  7747 fa0lumi    15   0  3572 2952  960  S   0.3   0.0   2:51.99 foxxr.pr
  8896 fa0lslm    15   0 10136 1596 1040  S   0.3   0.0   0:00.50 sshd
  8996 fa0lslm    16   0  2936 2296  944  D   0.3   0.0   0:02.82 foxxr.pr
10351 an06tec    16   0  2696 2012  904  S   0.3   0.0   0:01.09 foxxr.pr
10419 root        15   0  1888  808  668  S   0.3   0.0   0:00.11 in.telnetd
10637 celim06    15   0  2796 2136  924  S   0.3   0.0   0:01.75 foxxr.pr
11049 refer     16   0  3024 2344  896  D   0.3   0.0   0:04.08 foxxr.pr
11807 ucrq       16   0  2716 2044  912  S   0.3   0.0   0:01.97 foxxr.pr
16277 refer     15   0 10136 1596 1040  S   0.3   0.0   0:00.06 sshd
16301 refer     16   0  2928 2276  928  D   0.3   0.0   0:00.49 foxxr.pr
    1 root        15   0  2064  628  536  S   0.0   0.0   0:01.00 init
    2 root        RT  -5    0    0    0  S   0.0   0.0   0:00.00 migration/
    3 root        34  19    0    0    0  S   0.0   0.0   0:00.00 ksoftirqd/

```

La siguiente pantalla muestra, el porcentaje (%) de operaciones I/O que tiene el Servidor por atender, las cuales son ALTAS.

```

root@Rhel53-Rebagliati:~# iostat -x 1 1
2.24  0.00  1.50  45.14  0.00  51.12
Device:            tps    Blk_read/s    Blk_wrtn/s    Blk_read    Blk_wrtn
sda                177.00         72.00         2288.00         72         2288
sda7                0.00           0.00           0.00           0           0
sda6                79.00           0.00          185.00           0          185
sda5                0.00           0.00           0.00           0           0
sda4                0.00           0.00           0.00           0           0
sda3                0.00           0.00           0.00           0           0
sda2                0.00           0.00           0.00           0           0
sda1                0.00           0.00           0.00           0           0
avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           2.24    0.00    1.25   58.35    0.00   38.15

Device:            tps    Blk_read/s    Blk_wrtn/s    Blk_read    Blk_wrtn
sda                184.00         160.00        2392.00         160        2392
sda7                0.00           0.00           0.00           0           0
sda6                172.00           0.00          507.00           0          507
sda5                0.00           0.00           0.00           0           0
sda4                0.00           0.00           0.00           0           0
sda3                0.00           0.00           0.00           0           0
sda2                0.00           0.00           0.00           0           0
sda1                0.00           0.00           0.00           0           0
avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           3.02    0.00    0.75   48.74    0.00   47.49

Device:            tps    Blk_read/s    Blk_wrtn/s    Blk_read    Blk_wrtn
sda                174.00         552.00        2168.00         552        2168
sda7                0.00           0.00           0.00           0           0
sda6                600.00           0.00        1207.00           0        1207
sda5                0.00           0.00           0.00           0           0
sda4                0.00           0.00           0.00           0           0
sda3                0.00           0.00           0.00           0           0
sda2                0.00           0.00           0.00           0           0
sda1                0.00           0.00           0.00           0           0

```

Esta pantalla muestra que la partición sda6 (/local) del servidor, tiene la mayor carga de operaciones de Lectura y Escritura.



Esta otra pantalla, vuelve a mostrar el porcentaje de operaciones I/O (cpu – wait) que están pendientes de atender en el Servidor.

```

root@Rhel53-Rebagliati-
[root@Rhel53-Rebagliati ~]# vmstat 1
procs-----memory-----swap-----io-----system-----cpu-----
r b swpd free buff cache si so bi bo in cs us sy ld wa st
0 2 0 9271268 293488 2372512 0 0 148 248 462 1037 4 2 54 40 0
0 4 0 9271272 293500 2372500 0 0 184 1116 3238 6343 4 2 37 57 0
0 5 0 9264980 293532 2377664 0 0 72 3728 2966 12106 13 5 26 56 0
4 15 0 9264860 293552 2377644 0 0 64 3144 3324 5379 3 1 31 65 0
0 2 0 9264552 293592 2377888 0 0 100 916 3171 5895 4 2 48 47 0
0 13 0 9264180 293624 2377856 0 0 8 1208 2440 4887 2 1 41 55 0
1 1 0 9264244 293636 2378028 0 0 48 1156 2909 5171 2 1 52 45 0
3 5 0 9269328 293700 2373000 0 0 12 1080 2013 4205 2 1 54 43 0
1 13 0 9269208 293728 2373080 0 0 100 896 3103 5370 3 1 39 58 0
2 10 0 9269028 293752 2373056 0 0 192 888 1709 4572 2 1 38 60 0
3 4 0 9269032 293800 2373684 0 0 144 1124 2269 5792 4 1 34 60 0
0 5 0 9269156 293828 2373656 0 0 36 1256 2391 5229 3 1 35 61 0
0 1 0 9269112 293840 2373580 0 0 48 852 1626 4156 1 1 47 52 0
1 2 0 9268988 293864 2373556 0 0 28 1004 1705 4370 2 2 46 50 0
0 1 0 9269052 293876 2373696 0 0 40 880 1680 4609 2 1 51 46 0
0 1 0 9268808 293912 2373660 0 0 44 1072 1975 5157 2 1 46 52 0
3 4 0 9268824 293944 2373716 0 0 8 1144 3329 5855 2 2 51 45 0
0 5 0 9268764 293968 2373692 0 0 56 1064 1792 4819 2 2 45 51 0
0 3 0 9268764 293980 2373784 0 0 44 916 1781 5101 3 1 44 53 0
0 11 0 9268704 293996 2373768 0 0 44 852 1734 5143 2 1 34 62 0
3 4 0 9268400 294024 2373996 0 0 112 832 2241 5783 4 2 46 48 0
1 5 0 9268096 294036 2373984 0 0 188 1012 3104 6620 6 2 43 50 0
1 2 0 9268100 294060 2374480 0 0 128 728 1798 5637 4 1 47 48 0
2 4 0 9267544 294064 2374476 0 0 76 1244 2485 14233 7 8 29 56 0
1 2 0 9267360 294108 2374492 0 0 48 968 2748 5541 2 1 48 49 0
1 2 0 9267112 294140 2374460 0 0 24 1340 1747 5119 3 2 45 50 0
1 4 0 9266556 294148 2374684 0 0 60 1408 2042 5051 2 1 47 49 0
1 4 0 9266556 294184 2374648 0 0 32 1108 1935 4836 3 1 44 52 0
1 4 0 9266436 294188 2374744 0 0 112 1032 1737 4002 2 1 43 54 0
2 2 0 9266312 294204 2374728 0 0 4 836 1644 4164 1 1 41 56 0
0 4 0 9266312 294224 2374772 0 0 40 1032 1666 4467 2 1 46 51 0
1 1 0 9266068 294248 2375040 0 0 124 1176 2251 4402 1 1 26 71 0
    
```

Por lo antes indicado se recomienda lo siguiente:

1. Configurar un servidor físico con mejores características técnicas que el actual servidor de producción del SGH, para que reemplace el actual.
2. Otra alternativa, es configurar en el Servidor DELL R 730 que le fue asignado al Hospital Rebagliati, una máquina Virtual para el SGH, para que reemplace al actual servidor de producción.

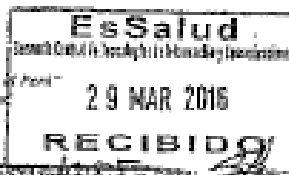
Atentamente.

Wilfredo Guzmán





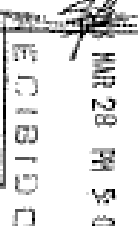
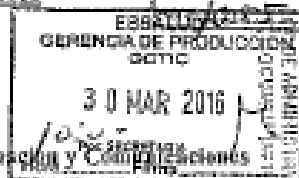
"Detalla de las Personas con Discapacidad en el Perú"
 Año de la conmemoración del Bicentenario



CARTA N° 571-0A-GRAR-ESSALUD-2016

Lima, **28 MAR 2016**

Señor:
ING. CARLOS SAITO SILVA
 Gerente Central de Tecnologías de la Información y Comunicaciones
 Presente. -



EsSalud Sede Central

ASUNTO : REITERO PEDIDO DE ADQUISICIÓN DE EQUIPOS SWITCH POR REPOSICIÓN Y/O OBSOLESCENCIA TECNOLÓGICA PARA EL HOSPITAL NACIONAL EDGARDO REBAGLIATI MARTÍNEZ.

REFERENCIA : a) CARTA N° 1103-0A-GRAR - 09/05/2014 NIT: 807-2014-181
 b) CARTA N° 2074-0A-GRAR - 09/09/2014 NIT: 807-2014-181
 c) CARTA N° 1543-OCTIC-ESSALUD-2014 - 23/01/2014
 d) RESOLUCIÓN DE GERENCIA GENERAL N° 1531-GG-ESSALUD-2013
 e) DIRECTIVA DE GERENCIA GENERAL N° 031-GG-ESSALUD-2013.

30 MAR 2016

De mi especial consideración:

Es grato dirigirme a usted, para saludarlo cordialmente, y a la vez informarle que el Hospital Nacional Edgardo Rebagliati Martínez, actualmente cuenta con una infraestructura tecnológica de equipos de comunicaciones (SWITCHES) obsoleta, los mismos que no cuentan con garantía vigente y/o contrato de servicio de soporte técnico, cabe mencionar que la reparación implica la compra de repuestos que en el mercado no se encuentran disponibles.



Con carta de la referencia a), se solicitó la adquisición de 26 equipos Switch por reposición, el mismo que se reiteró con carta de la referencia b), solicitando la adquisición de 29 equipos Switch adicional al pedido anterior, con carta de la referencia c), la gerencia Central de Tecnologías de Información y Comunicaciones responde al pedido de la referencia b), indicando que la Sub Gerencia de Comunicaciones de la Gerencia de Producción, se encuentra gestionando para el presente año (2014), la adquisición de conmutadores LAN para las sedes a nivel nacional dentro de los cuales estaba considerando la Red Asistencial Rebagliati, el mismo que a la fecha marzo 2016 el Hospital Rebagliati reitera el pedido por ser prioritario toda vez que los equipos presentan constantes fallas quedando inoperativos generando caídas de red, afectando a los servicios en su totalidad.



El sistema de red de área local proporciona seguridad, conectividad entre todos los servicios del hospital, calidad de aplicaciones en tiempo real, como son los servicios de Video, Imágenes, Voz y Data, además asegura que el acceso a la información y a los recursos en cualquier parte del hospital, reduciendo los costos de operaciones, teniendo en cuenta el nivel del hospital donde la necesidad del 7 x 24 es absoluta y la criticidad es máxima.

El presente cuadro da a conocer la diversidad de marcas existentes, donde el 100% de equipos ha cumplido el tiempo de vida útil, así mismo los modelos existentes se encuentran en obsolescencia tecnológica, considerando como "obsoletos" a todo equipo con más de cinco años de operación de acuerdo a lo estipulado en el documento de la referencia d) y e).

RED ASISTENCIAL REBAGLIATI
 Av. Edgardo Rebagliati N° 406 Breña Sur
 Teléfono: 14511001





EQUIPOS DE COMUNICACIONES PARA LA RED DE DATOS					
N°	DESCRIPCIÓN DE EQUIPO	MARCA	CANT.	FECHA DE INST.	VELOCIDAD (MBPS)
1	Switch administrable "CORE" OS 9800. Capa 3	Alcatel Lucent	1	2008	10/100/1000
2	Switch administrable. Capa 2	Alcatel Lucent, 3COM, D-Link, Allied Telesis, Avaya	76	2008	10/100
3	Switch no administrable.	D-Link, TP-Link	78	2008	10/100

EQUIPOS DE COMUNICACIONES PARA LA RED DE VIDEO					
N°	DESCRIPCIÓN DE EQUIPO	MARCA	CANT.	FECHA DE INST.	VELOCIDAD (MBPS)
1	Switch administrable. Capa 3	CISCO Catalyst 3750 12 Puertos	1	2007	10/100/1000
2	Switch administrable. Capa 2	CISCO Catalyst 3560 08 Puertos	8	2007	10/100

Fuente: Oficina de Soporte Informático - HNERM

Cabe mencionar que el crecimiento de la red LAN del Hospital, se debe a la evolución de dispositivos Médicos, Telefonía, Impresión y Cámaras de Video a tecnología IP, así mismo el crecimiento de los servicios que brinda el Hospital.

Con el objetivo de mitigar los riesgos, garantizar la continuidad operativa del servicio de red de comunicaciones ante una emergencia o desastre, se debe tener en cuenta el aspecto tecnológico y económico, para lo cual se requiere con urgencia la renovación, reposición o delegación para la compra de todos los equipos de comunicaciones que se adjuntan los mismos que proporcionarán mayor rendimiento, calidad de servicio y escalabilidad de la red, beneficiando a los pacientes en la mejora de atención ya que la alta disponibilidad de la red y el incremento de ancho de banda, asegura las comunicaciones del hospital en tiempo real el acceso a todos los aplicativos institucionales y permite responder con los procesos funcionales y necesidades de hospital,



Sin otro particular y agradeciendo su amable atención a la presente, quedo de usted.

Adjunto

- Anexo 1 – Estructura de Red de Data Center y Cuartos de Comunicaciones.
- Anexo 2 – Topología de Red LAN.
- Anexo 3 – Relación de Switch.

Atentamente,

ESSALUD
RED ASISTENCIAL REBAGLIATI - HNERM
[Signature]
Ing. Jose Aquino Cavero
Jefe de la Oficina de Administración

04-MARZO
JAC/CAAC/RARP
/ / 2016
807 2016 NIT. 8
C. Proyecto N° 8 -OSI-2016

LABORATORIO CENTRAL DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES
ESSALUD
Lima, 29 MAR. 2016
Proveído N° 499
Presupuesto: O.Prod
Para: AUDIOLAB SEUF
Y TRAMITE CORRESPONDIENTE - RARA
C.C.
[Signature]
Ing. CARLOS A. SANCHEZ
RED ASISTENCIAL REBAGLIATI
Av. Edgardo Rebagliati N° 490 Jesús María
Teléfono 265-4901

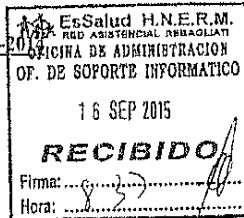
GER. JAC/CAAC/RARP
30 MAR. 2016
Ing. LUIS PEREZ NICHIS
CER NIT.





"Decenio de las Personas con Discapacidad en el Perú"
 "Año de la Promoción de la Industria Responsable y del Compromiso Climático"

Carta N° 03-OA-GRAR-EsSalud-2014



Lima, 16 MAY 2014

Señor
ING. CARLOS SAIÑO SILVA
 Jefe de la Oficina Central de Tecnologías de la Información y Comunicaciones - OCTIC
 Sede Central
Presente.-

Asunto : ADQUISICION DE 26 SWITCHES POR REPOSICION, PARA EL HOSPITAL EDGARDO REBAGLIATI MARTINS

De mi consideración:

Tengo el agrado de dirigirme a usted para saludarlo muy cordialmente y a la vez informarle que el Hospital Rebagliati, requiere urgentemente 26 SWITCHES, para realizar la reposición de los que actualmente se encuentran averiados, por lo que solicito a usted, la adquisición de las mismas, con el fin de garantizar el normal funcionamiento de la Red Informática.



Para lo cual se adjunta a la presente, la relación de los switches averiados.

Agradeciéndole por anticipado, se sirva usted atender nuestra solicitud, quedo de usted.

Atentamente

EsSalud
 RED ASISTENCIAL REBAGLIATI - HNERM

Ing. Jose Aquino Cavero
 Ing. Jose Aquino Cavero
 Jefe de la Oficina de Administración

OA-mayo
 JAC/TR/alv.
 08-05-2014

807	2014	NIT. 181
-----	------	----------

C. proyecto N°048-OSI-2014.

RED ASISTENCIAL REBAGLIATI
 Av. Edgardo Rebagliati N° 490 Jesús María
 Teléfono 265-4901



EsSalud

Seguridad Social para todos

"Decenio de las Personas con Discapacidad en el Perú"
"Año de la Promoción de la Industria Responsable y del Compromiso Climático"

CARTA N° 211-0A-GRAR-ESSALUD-2014

Lima,

Señor:

ING. CARLOS SAITO SILVA

Jefe de la Oficina de Tecnologías de la Información y Comunicaciones - OCTIC

Sede Central.

Presente.-

RECIBIDO
Fecha: 25/09/2014
Firma: [Signature]

1508010000
SECRETARIA
25 SET 2014

ASUNTO : REITERO PEDIDO DE ADQUISICIÓN DE EQUIPOS SWITCHES POR RÉPOSICIÓN PARA LA RED ASISTENCIAL REBAGLIATI.

REFERENCIA : a). Carta 1103-OA-GRAR - 08/05/2014
b). Resolución de Gerencia General N° 453-GG-ESSALUD-2007.

De mi Consideración:

Es grato dirigirme a usted, para saludarlo cordialmente, y a la vez informarle lo siguiente:

En la actualidad la Oficina de Soporte Informático de la Red Asistencial Rebagliati, cuenta con 29 Equipos SWITCHES INOPERATIVOS, debido que han cumplido el tiempo de vida útil.

Con documento a), de la referencia se solicitó a la Oficina Central de Tecnologías de la Información y Comunicaciones - OCTIC Sede Central, la adquisición de 26 switches por reposición, el mismo que a la fecha no se ha tenido respuesta.

Teniendo en cuenta el aspecto tecnológico y económico, se requiere con urgencia la reposición de 29 equipos switches que han dejado de ser útil para el fin que fueron adquiridos, los mismos que serán distribuidos en los Centros Asistenciales de la Red Asistencial Rebagliati, a fin de mantener el estándar de infraestructura de la red de comunicaciones, garantizando la continuidad de las operaciones. Adjunto Anexo 2 - Sustento Técnico de Reposición de Equipos Informáticos Existentes.

Sin otro particular y agradeciendo su amable atención a la presente, quedo de usted.



Atentamente,

ESSALUD
RED ASISTENCIAL REBAGLIATI - HINERAM

Ing. José Aquino Cavero

Jefe de la Oficina de Administración

0A-Ingesto

JAC/CAAC/RARP

28.08.14

807 2014 NIT.181

C. Proyecto N°065-DSE-2014

25 SET. 2014

2392
30 SET. 2014

RED ASISTENCIAL REBAGLIATI
Av. Edgardo Rebagliati N° 490 Jesús María
Teléfono 265-4901





RED ASISTENCIA REBAGUIATI
 OFICINA DE ADMINISTRACION
 OFICINA DE SOPORTE INFORMATICO
 RELACION DE EQUIPOS SWITCH DGS-3024

N	MARCA	MODELO	DESCRIPCIÓN	COD. PATRIMONIAL	SERIE	ESTADO	UBICACIÓN FÍSICA
1	D-Link	DGS-3024	Administrable, 24 Puertos	00602770	DRAH167000318	Baja Inoperativo	Almacén Patrimonio
2	D-Link	DGS-3024	Administrable, 24 Puertos	00602409	DRAH167000286	Baja Inoperativo	Almacén Patrimonio
3	D-Link	DGS-3024	Administrable, 24 Puertos	00602778	DRAH167000918	Baja Inoperativo	Almacén Patrimonio
4	D-Link	DGS-3024	Administrable, 24 Puertos	00602380	DRAH167000317	Baja Inoperativo	Almacén Patrimonio
5	D-Link	DGS-3024	Administrable, 24 Puertos	00602836	DRAH167000128	Baja Inoperativo	Almacén Patrimonio
6	D-Link	DGS-3024	Administrable, 24 Puertos	00602780	DRAH167000108	Baja Inoperativo	Almacén Patrimonio
7	D-Link	DGS-3024	Administrable, 24 Puertos	00602381	DRAH167000106	Baja Inoperativo	Almacén Patrimonio
8	D-Link	DGS-3024	Administrable, 24 Puertos	00602399	DRAH167000382	Baja Inoperativo	Almacén Patrimonio
9	D-Link	DGS-3024	Administrable, 24 Puertos	00602411	DRAH167000547	Baja Inoperativo	Almacén Patrimonio
10	D-Link	DGS-3024	Administrable, 24 Puertos	00602394	DRAH167000339	Baja Inoperativo	Almacén Patrimonio
11	D-Link	DGS-3024	Administrable, 24 Puertos	00602396	DRAH167000765	Baja Inoperativo	Almacén Patrimonio
12	D-Link	DGS-3024	Administrable, 24 Puertos	00602398	DRAH167000288	Baja Inoperativo	Almacén Patrimonio
13	D-Link	DGS-3024	Administrable, 24 Puertos	00602401	DRAH167000206	Baja Inoperativo	Almacén Patrimonio
14	D-Link	DGS-3024	Administrable, 24 Puertos	00602402	DRAH167000337	Baja Inoperativo	Almacén Patrimonio
15	D-Link	DGS-3024	Administrable, 24 Puertos	00602404	DRAH167000990	Baja Inoperativo	Almacén Patrimonio
16	D-Link	DGS-3024	Administrable, 24 Puertos	00607405	DRAH167000207	Baja Inoperativo	Almacén Patrimonio
17	D-Link	DGS-3024	Administrable, 24 Puertos	00602774	DRAH167000107	Baja Inoperativo	Almacén Patrimonio
18	D-Link	DGS-3024	Administrable, 24 Puertos	00602400	DRAH167000766	Baja Inoperativo	Oficina de Comunicaciones
19	D-Link	DGS-3024	Administrable, 24 Puertos	00602408	DRAH167000338	Baja Inoperativo	Oficina de Comunicaciones
20	D-Link	DGS-3024	Administrable, 24 Puertos	00602410	DRAH167000992	Baja Inoperativo	Oficina de Comunicaciones
21	D-Link	DGS-3024	Administrable, 24 Puertos	00602768	DRAH167000957	Baja Inoperativo	Oficina de Comunicaciones
22	D-Link	DGS-3024	Administrable, 24 Puertos	00602769	DRAH167000563	Baja Inoperativo	Oficina de Comunicaciones
23	D-Link	DGS-3024	Administrable, 24 Puertos	00602772	DRAH167000562	Baja Inoperativo	Oficina de Comunicaciones
24	D-Link	DGS-3024	Administrable, 24 Puertos	00602773	DRAH167000548	Baja Inoperativo	Oficina de Comunicaciones
25	D-Link	DGS-3024	Administrable, 24 Puertos	00602775	DRAH167000127	Baja Inoperativo	Oficina de Comunicaciones
26	D-Link	DGS-3024	Administrable, 24 Puertos	00602779	DRAH167000127	Baja Inoperativo	Oficina de Comunicaciones
27	D-Link	DGS-3024	Administrable, 24 Puertos	00602395	DRAH167000519	Baja Inoperativo	Oficina de Comunicaciones
28	D-Link	DGS-3024	Administrable, 24 Puertos	00602395	DRAH167000287	Baja Inoperativo	Oficina de Comunicaciones
29	D-Link	DGS-3024	Administrable, 24 Puertos	00602776	DRAH167000767	Baja Inoperativo	Oficina de Comunicaciones
					DRAH167000959	Baja Inoperativo	Oficina de Comunicaciones





CARTA N° 2074 -OCTIG-ESSALUD-2014

Lima, 23 OCT. 2014

Ingeniero
JOSE AQUINO CAVERO
Jefe de la Oficina de Administración
Red Asistencial Rebagliati
Presente.-

Asunto: Adquisición de equipos Switch LAN para la Red Asistencial Rebagliati

Ref.: Carta N° 2074 -GCI-ESSALUD-2014

Es grato dirigirme a usted para saludarlo cordialmente y en atención a la carta de la referencia, en la cual se solicita la adquisición por reposición de Switch LAN para las sedes de la Red Asistencial Rebagliati.

Al respecto, le informo que la Sub Gerencia de Comunicaciones de la Gerencia de Producción se encuentra gestionando, para el presente año, la adquisición de conmutadores LAN para las sedes a nivel nacional, dentro las cuales están consideradas las sedes de la Red Asistencial Rebagliati, con lo cual se atenderá su requerimiento.

Cabe mencionar que las coordinaciones se realizaron entre el Ing. Alejandro Andrade, Sub Gerente de Comunicaciones y el Sr. Vicente Icaza personal de la Oficina de Soporte Informático de la RAR.

Sin otro particular, quedo de usted.

Atentamente,



Ing. Carlos A. Saito Silva
Ing. CARLOS A. SAITO SILVA
Jefe de Oficina Central
ESSALUD

9607.03.0001.104
OS.I

Atención que corresponde

CSS/LPP/AAD
CC GP-SGC
NT 807-2014-181





"Año de la consolidación del Mar de Grau"
 "Año de la Conmemoración del Octogésimo Aniversario de la Creación de la Seguridad Social en el Perú"

INFORME TECNICO N° 321 -SGCOM-GPROD-GCTIC-ESSALUD-2016

ESSALUD
 SUB GERENCIA DE COMUNICACIONES
 GERENCIA DE PRODUCCION
 GCTIC
 20 JUL 2016
 Por: SECRETARIA
 Hora..... Firma.....

A: Ing. Alejandro Andrade Delgado
 Sub Gerente de Comunicaciones

De: Ing. Andrés Justiniano De La Cruz
 Profesionales de la Sub Gerencia de Comunicaciones

Asunto: Reitero pedido de Adquisición de Equipos Switch por reposición y/o obsolescencia tecnológica para el Hospital Nacional Edgardo Rebagliati Martins

Referencia: Carta N° 571-OA-GRAR-ESSALUD-2016

Fecha: 20 de julio del 2016

Es grato dirigirme a Ud. para saludarlo cordialmente y en atención al documento de la referencia remitido por la Oficina de Administración de la Red Asistencial Rebagliati.

A. Antecedentes

- Mediante la Carta N° 571-OA-GRAR-ESSALUD-2016, la Oficina de Administración de la Red Asistencial Rebagliati, solicita la adquisición de equipos switch para el Hospital Nacional Edgardo Rebagliati Martins, dado que se encuentran obsoletos y no cuentan con garantía vigente y/o contrato de servicio de soporte técnico.
- NT N° 0021-MINSA-DGSP V.01, Norma Técnica "Categorías de Establecimientos de Sector Salud"
- NTS N° 119-MINSA/DGIEM-V.01, Norma técnica de Salud "Infraestructura y equipamiento de los establecimientos de Salud del Tercer Nivel de Atención".

B. Análisis

En atención al requerimiento efectuado por la Oficina de Administración de la Red Asistencial Rebagliati debo de indicar lo siguiente:

- Según la NT N° 0021-MINSA-DGSP V.01, Norma Técnica "Categorías de Establecimientos de Sector Salud", establece el cuadro comparativos entre los centros asistenciales de ESSALUD y el MINSA

CUADRO COMPARATIVO NACIONAL

CATEGORIAS	MINSA	ESSALUD	PIP	FAP	NAVAL	PRIVADO
I - 1	Puesto de Salud		Puesto Sanitario	Posta Médica	* Enfermería * Servicios de Sanidad	Consultorio
I - 2	Puesto de Salud con Médico	Posta Médica	Posta Médica	Departamento Sanitario	* Departamento de Sanidad * Posta Naval	Consultorio Médicos
I - 3	Centro de Salud	Centro Médico	Policlínico	-	Centro Médico	* Policlínicos
I - 4	Centro de Salud con Instrumentos	Policlínico	Hospital Regional	Hospital Zona	Policlínico Naval	Centros Médicos
II - 1	Hospital I	Hospital I y II		Hospital Regional	Clinica Naval	Clinicas
II - 2	Hospital II	Hospital III y IV				Clinicas
III - 1	Hospital III	Hospital Nacional	Hospital Nacional	Hospital Central FAP	Hospital Naval	Clinicas
III - 2	Instituto de Diagnóstico y Referencia Epidemiológica	Instituto				Institutos

Este documento es CONFIDENCIAL queda prohibida su reproducción parcial o total sin previo consentimiento de EsSalud

Av. Domingo Cueto N° 120
 Jesús María





"Año de la consolidación del Mar de Grau"

"Año de la Conmemoración del Octogésimo Aniversario de la Creación de la Seguridad Social en el Perú"

2. Según la NT N° 0021-MINSA-DGSP V.01, al Hospital Nacional Edgardo Rebagliati Martins, le corresponde en equivalencia la Categoría de Establecimiento de Salud del Tercer Nivel de Atención, por lo cual para los estudios posteriores se tomarán en consideración la NTS N° 119- MINSA/DGIEM-V.01.
3. Según la NTS N° 119-MINSA/DGIEM-V.01, Norma técnica de Salud "Infraestructura y equipamiento de los establecimientos de Salud del Tercer Nivel de Atención", que establece:
 - a. Los criterios mínimos de diseño arquitectónico, diseño de instalaciones y dimensionamiento de la infraestructura física de los establecimientos de salud del tercer nivel de atención.
 - b. Criterios técnicos mínimos para el equipamiento de los establecimientos de salud del tercer nivel de atención.
4. Según la NTS N° 119-MINSA/DGIEM-V.01, el diseño de la infraestructura de red de un establecimiento de salud, contempla los siguientes aspectos:
 - a. Nivel Principal:
 - Permite interconectar con enlaces redundantes los niveles de distribución tanto en el centro de datos como el de Lan, así como los equipos de conexión a internet.
 - La velocidad de Transmisión mínima debe ser de 40 Gbps, en los diseños de gabinetes debe considerarse el crecimiento futuro de los equipos de este nivel.
 - El nivel principal, debe ser redundante en equipos y en abastecimiento eléctrico.
 - b. Nivel de Distribución Centro de Datos
 - Permite interconectar con enlaces redundantes los equipos de nivel principal, con los equipos de procesamiento y almacenamiento del centro de datos.
 - La velocidad de transmisión mínima debe ser de 40 Gbps, En los diseños de Gabinetes, debe considerarse el crecimiento futuro de los equipos de este nivel.
 - El Nivel de distribución debe ser redundante en equipos y abastecimiento eléctrico
 - c. Nivel de Distribución Lan
 - Permite interconectar con enlaces redundantes, los equipos del nivel principal con los equipos del nivel de borde.
 - La velocidad de transmisión mínima debe ser de 40Gbps, para la conexión con el nivel principal y de 10Gbps con el nivel de Borde. En los diseños de gabinetes debe considerarse el crecimiento futuro de equipos de este nivel.
 - d. Nivel de Borde
 - Permite Interconectar las salidas en las áreas de trabajo, con los equipos de nivel de distribución.
 - La velocidad de transmisión mínima, debe ser de 10Gbps para la conexión con el nivel de distribución y de 1 Gbps con las áreas de trabajo. Se deben considerar equipos de tecnología PoE y en los diseños de Gabinetes, debe considerarse el crecimiento futuro de este nivel.

[Handwritten signature]

Este documento es CONFIDENCIAL queda prohibida su reproducción parcial o total sin previo consentimiento de EsSalud

www.minsa.gob.pe

Av. Domingo Cueto N° 120
Jesús María
Lima 11 - Perú

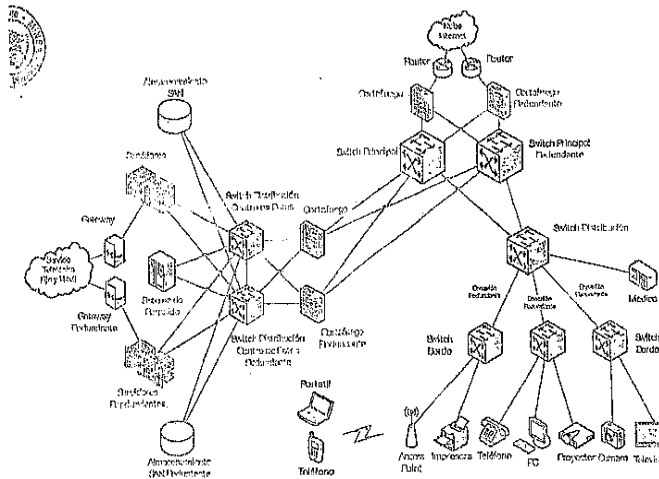




"Año de la consolidación del Mar de Grau"
 "Año de la Conmemoración del Octogésimo Aniversario de la Creación de la Seguridad Social en el Perú"

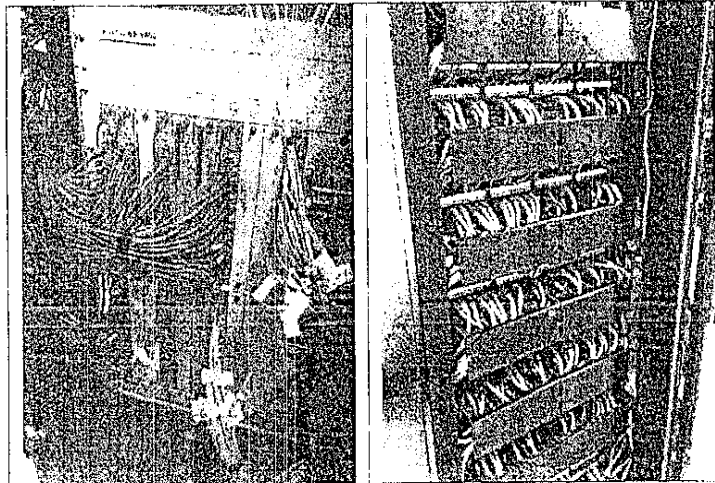
e. Diagrama Lógico Propuesto por la norma NTS 119-MINSA/DGIEM-V.01

ANEXO N° 4
 DIAGRAMA LÓGICO DE LA INFRAESTRUCTURA DE RED UNIDAD COMPLETA DE GESTIÓN DE INFORMACIÓN



5. Se procedió a efectuar las coordinaciones con el área usuaria, la Oficina de Soporte Informático del Hospital Nacional Edgardo Rebagliati Martins, a fin de recabar mayor información sobre el requerimiento efectuado mediante la carta de la referencia.
6. Se efectuó un recorrido por las instalaciones del Hospital Nacional Edgardo Rebagliati Martins, encontrándose lo siguiente:

A. Data Center



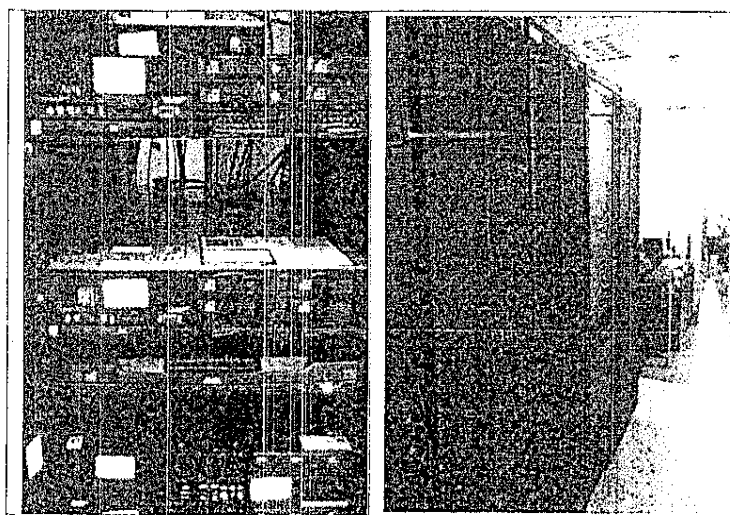
Este documento es CONFIDENCIAL queda prohibida su reproducción parcial o total sin previo consentimiento de EsSalud

Av. Domingo Cueto N° 120
 Jesús María
 Lima 11, Perú



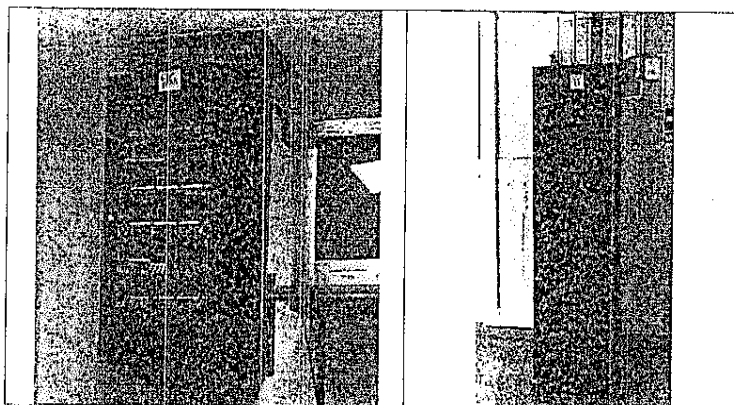


"Año de la consolidación del Mar de Grau"
"Año de la Conmemoración del Octogésimo Aniversario de la Creación de la Seguridad Social en el Perú"



El Centro de Datos del Hospital Nacional Edgardo Rebagliati Martins, cuenta con un Gabinete de Distribución Secundario, un Gabinetes de Distribución Principal y Gabinetes para Servidores.

B. Switches en Gabinetes Metálicos



Handwritten signature

Este documento es CONFIDENCIAL, queda prohibida su reproducción parcial o total sin previo consentimiento de EsSalud

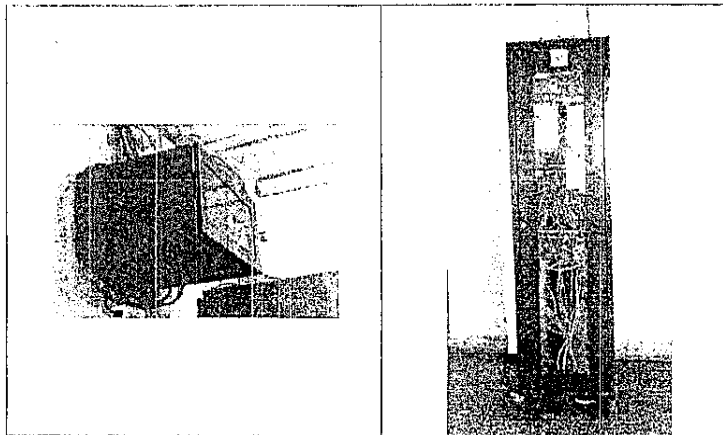
www.esa.gob.pe

Av. Domingo Cueto N° 120
Jesús María
Lima 11 - Perú



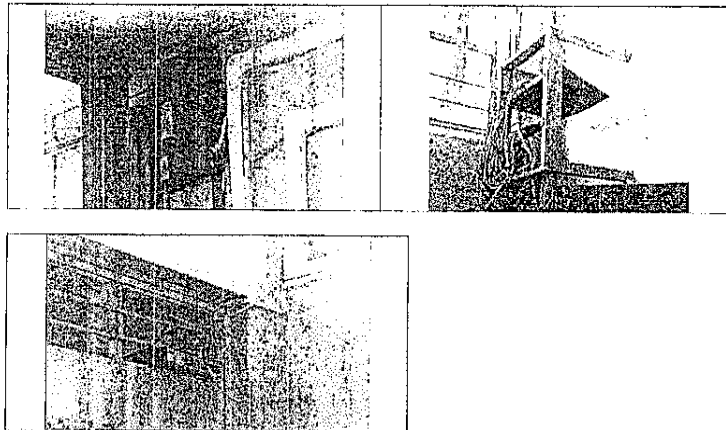


"Año de la consolidación del Mar de Grau"
"Año de la Conmemoración del Octogésimo Aniversario de la Creación de la Seguridad Social en el Perú"



La mayor parte de los equipos de networking se encuentran ubicados en los Gabinetes de Metálicos de Distribución Secundarios, los cuales como se puede observar difieren en tamaños, pero dada la magnitud del centro asistencial muchos de estos gabinetes se encuentran saturados, impidiendo la habilitación de nuevos puntos de red en dichos gabinetes.

C. Switches sin Gabinetes Metálicos



Para cubrir la demanda de nuevos puntos de red, se han habilitado de manera improvisada nodos de red, que en muchos casos no brinda las condiciones necesarias para el óptimo funcionamiento y protección de los equipos de networking.

Este documento es CONFIDENCIAL queda prohibida su reproducción parcial o total sin previo consentimiento de EsSalud

Av. Domingo Cueto N° 120
Jesús María

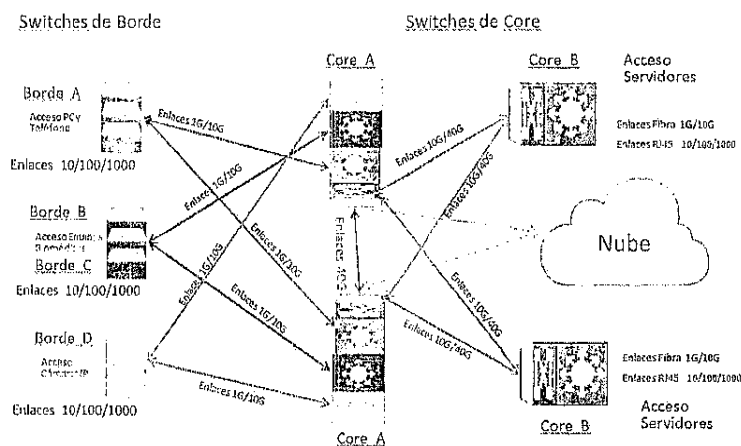




"Año de la consolidación del Mar de Grau"

"Año de la Conmemoración del Octogésimo Aniversario de la Creación de la Seguridad Social en el Perú"

7. Debido a la necesidad de mantener y mejorar las comunicaciones internas en el Hospital Nacional Edgardo Rebagliati Martins y el acceso a los diferentes servicios brindados por EsSalud; es necesario se efectuó la renovación de los equipos de networking, dado que dichos equipos son de tecnología obsoleta, no cuentan con garantía, ni contratos de servicio de mantenimiento ni disponibilidad de piezas de repuesto; por lo que en atención a la NTS N° 119-MINSA/DGIEM-V.01 y las coordinaciones efectuadas con la Jefatura de la Oficina de Soporte Informático del Hospital, y en atención a los principios de libertad de concurrencia, igualdad de trato, transparencia, competencia, vigencia tecnología de la Ley de Contrataciones del Estado Vigente se procedió a evaluar las diversas alternativas de las principales marcas de equipos de networking con presencia en el mercado peruano y a elaborar las especificaciones técnicas para la "Adquisición de equipos de networking para el Hospital Nacional Edgardo Rebagliati Martins". Considerando la siguiente topología:



Esta nueva topología comprende un alto grado de redundancia a nivel de servicios y accesos, según lo indicado en la NTS 119:

- o Dos Switches de Core Principales (Core_A) configurados en redundancia.
 - o Cada uno contara con 192 puertos SPF/SPF+
 - o Cada uno contara con 24 puertos QSPF+
- o Dos Switches de Acceso de Servidores (Core_B) configurados en redundancia, con la finalidad de disminuir la capacidad de procesamiento del Switch de Core.
 - o Cada uno contara con 96 puertos SPF/SPF+
 - o Cada uno contara con 96 puertos RJ45 10/100/1000
 - o Cada uno contara con 12 puertos QSPF+
- o Conjuntamente con el área usuaria se definieron Tres redes de acceso independientes físicamente pero interconectadas a nivel de Core:
 - o Voz y Datos (Borde A) (Equipos de networking de 48 Puertos 10/100/1000 PoE/PoE+ y 2 puertos SPF/SPF+)

Este documento es CONFIDENCIAL queda prohibida su reproducción parcial o total sin previo consentimiento de EsSalud

www.esalud.gob.pe

Av. Domingo Cueto N° 120
Jesús María
Lima 11 - Perú





"Año de la consolidación del Mar de Grau"
 "Año de la Conmemoración del Octogésimo Aniversario de la Creación de la Seguridad Social en el Perú"

- o Equipos Biomédicos (Borde C y D) (Equipos de networking de 24 y 48 Puertos 10/100/1000 y 2 puertos SPF/SPF+)
- o Cámaras IP (Borde B) (Equipos de networking de 24 Puertos 10/100/1000 PoE/PoE+ y 2 puertos SPF/SPF+)
- o Las cantidades han sido definidas por el área usuaria:

Tabla N° 01 Resumen de Switches							
Switches	Core_A	Core_B	Borde_A	Borde_D	Borde_C	Borde_B	Sub total
Distribuidos en GDS	2	2	70	36	13	27	150
No distribuidos, entregados a la Oficina de Soporte Informático (*)			5	5	5	5	20
Total	2	2	75	41	18	32	170

(*) Equipos de contingencia que en caso de no ser instalados durante el despliegue serán entregados a la Oficina de soporte Informático del Hospital Nacional Edgardo Rebagliati Martins, para ser implementados y puestos en producción según su necesidad.

Cabe indicar que la topología de red propuesta y coordinada con la Oficina de Soporte Informático del Hospital Nacional Edgardo Rebagliati Martins, para un óptimo funcionamiento y operatividad requiere de la ejecución de proyectos complementarios que garanticen el máximo aprovechamiento de la tecnología a ser implementada:

- o Renovación del Sistema de Cableado Estructurado Existente en el Hospital Nacional Edgardo Rebagliati Martins, mínimo F/UTP categoría 6A, el cual permitirá contar con velocidades de hasta 1Gbps desde el GDS hacia la PC del Usuario, el empleo de troncales de Fibra Óptica de 1G/10G para la interconexión entre los Gabinetes de Comunicaciones y el Centro de Datos.

Así mismo es necesario considerar para el dimensionamiento del sistema de cableado estructurado y equipos de networking, todos los sistemas a ser implementados en el corto, mediano y largo plazo.

- i. Sistema de Marcadores Biométricos de Asistencia
- ii. PCs
- iii. Equipos de Telefonía IP
- iv. Equipos Biomédicos
- v. Equipos de Imágenes Médicas
- vi. Sistema de Cámaras de Seguridad IP
- vii. Wireless Lan
- viii. Sistema de Llamada de Enfermera
- ix. Sistema de CCTV-video IP
- x. Entre otros.

- o Renovación y ampliación del centro de Datos del Hospital Nacional Edgardo Rebagliati Martins, lo cual nos permitirá contar con los medios de protección y energía eléctrica necesaria para un adecuado funcionamiento de los equipos, enlaces de cobre y fibra para el acceso a los diferentes equipos y servicios, garantizando así velocidades de transmisión de 10G/40G/100G.

Este documento es CONFIDENCIAL queda prohibida su reproducción parcial o total sin previo Consentimiento de EsSalud

Av. Domingo Cueto N° 120
 Jesús María





"Año de la consolidación del Mar de Grau"
 "Año de la Conmemoración del Octogésimo Aniversario de la Creación de la Seguridad Social en el Perú"

C. Conclusiones

1. De lo mencionado anteriormente y luego de las coordinaciones con la Oficina de Soporte Informático del Hospital Nacional Edgardo Rebagliati Martins, se procedió a la elaboración de las especificaciones técnicas para la "Adquisición de equipos de networking para el Hospital Nacional Edgardo Rebagliati Martins", las mismas que son remitidas para su conocimiento, evaluación y tramite correspondiente, salvo mejor parecer y opinión de su despacho.

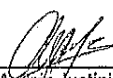
D. Recomendaciones

Para un adecuado funcionamiento de la solución y cuidado de los equipos de networking a adquirir SE RECOMIENDA:

1. Efectuar el **MEJORAMIENTO DEL CENTRO DE DATOS O DATA CENTER** del Hospital Nacional Edgardo Rebagliati Martins, a fin de garantizar un adecuado soporte en energía e infraestructura para los nuevos equipos de Core, y de esta manera aprovechar las bondades del diseño de networking propuesto, en cumplimiento de lo indicado en la NTS 119.
2. Efectuar la **RENOVACIÓN DEL SISTEMA DE CABLEADO ESTRUCTURADO** del Hospital Nacional Edgardo Rebagliati Martins", mínimo FUTP Categoría 6A, aumento de los enlaces de fibra óptica con soporte para velocidades de 1G/10G/40G, reubicación de los GDS, dimensionamiento de puntos de red permitiendo de esta manera aprovechar la nueva tecnología activa a ser implementada que nos permitirá administrar y gestionar mayores anchos de banda y velocidades de transmisión.
3. Para el dimensionamiento de los puntos de red, debe tomar en consideración todos los sistemas y equipos a ser implementados en el corto, mediano y largo plazo:
 - a. Sistema de Marcadores Biométricos de Asistencia
 - b. PCs y Equipos de Telefonía IP
 - c. Equipos Biomédicas
 - d. Equipos de Imágenes Medicas
 - e. Sistema de Cámaras de Seguridad IP
 - f. Sistema de Llamada de Enfermera
 - g. Sistema de CCTV-video IP
 - h. Entre otros.
4. El **Backbone de datos de Fibra Óptica** que forma parte de la **IMPLEMENTACIÓN DEL SISTEMA DE CABLEADO ESTRUCTURADO** que permite enlazar el Data Center con los GDS distribuidos por todo el Hospital Nacional Edgardo Rebagliati Martins, debe ser con enlaces redundantes con rutas alternativas y diferentes, empleando como mínimo enlaces con 12 hilos de fibra que garanticen velocidades de 1Gbps y 10Gbps, esta cantidad de hilos de fibra permitirá mantener la independencia física inicial de las Redes de PC/Voz, Equipos Biomédicos y Cámaras IP, en cada GDS así como permitir el crecimiento futuro de otros servicios exclusivos como CCTV-video IP, el cual requiere de un mayor ancho de banda.

Es todo cuanto debo informar, para los fines correspondientes.

Atte.


 Ing. Andrés Justiniano De la Cruz
 Profesional de la Sub Gerencia de Comunicaciones
 Gerencia de Producción – GCTIC
 EsSalud – Sede Central

NIT: 807-2014-181

Este documento es CONFIDENCIAL queda prohibida su reproducción parcial o total sin previo consentimiento de EsSalud

www.esalud.gob.pe

Av. Domingo Cuelto N° 120
 Jesús María
 Lima 11 - Perú

Fuente: Documentos de Sustento de la Oficina de Soporte Informático HNERM EsSALUD (2017).



Tabla 27

Bitácora de las Caidas de los servicios de la Red LAN del HNERM EsSALUD años del 2016 al 2018

Fecha/Hora/inicio	Motivo		Observación
02/02/2016 - 08:35:00 a.m.	Corte de fluido eléctrico intermitente originando que unas de las tablas dbf se malogren	02/02/2016 - 13:15 p.m.	El UPS esta inoperativo por lo que origino que el servidor y todos los switches cayeran y esto daño y se corrompieron las tablas principales de los diferentes sistemas del hospital NERM.
9/02/2016 11:00 a.m.	Intermitencia de sistema por consumo de memoria del servidor por los reportes y cierre de programación estadística	9/02/2016 12:00 m.n.	Cada vez que corren los diferentes aplicativos de Estadísticas que consultan diferentes tablas importantes pone lento la Red debido a que consume memoria del servidor y se sugiere cambiar por otro con mayores recursos.
15/02/2016 - 10:57:00 a.m.	Inestabilidad del aplicativo SGH	15/02/2016 - 11:15:00 a.m.	Software hecho en Foxprox Lan, no es compatible con versiones de Windows actuales se tiene que hacer instalaciones de interfases para que reconozcan dicha plataforma.
16/03/2016 - 8:30 a.m.	Inestabilidad de la Red LAN por problemas del Core Principal se quemó una tarjeta de 24 puertos.	16/03/2016 - 13:30 p.m.	correo ASUNTO: Continua la inoperatividad del SGH y los servicios.



17/03/2016 - 8:30 a.m.	Inestabilidad de Red por caidas de Switch de Borde del Gabinete I de consultorios externos	17/03/2016 – 13:45 p.m.	continua inestabilidad de la Red Lan y Sistema
18/03/2016 02:00 a.m.	Inestabilidad de la red	18/03/2016 02:00 a.m.	Intermitencias con DNS
16/05/2016 - 11:10 a.m.	Inestabilidad de red por loop en el area de farmacia.	16/05/2016 - 12:45 p.m.	Spanning Tree, Trafico de Broadcast
CELIM – 09:00 a.m.	SE ACTIVA	1/06/2016 10:00 a.m.	Restablecimiento de la Red LAN
19/07/2016 - 4:00 p.m.	Inestabilidad del Servidor falla pila de cache	22/07/2016 - 01:00 a.m.	(Se instaló Servidor Virtualizado)
05/12/2016 - 10:05 a.m.	Se Cayo uno de los DNS principales de Links de Consultas.	05/03/2017 - 11:30 a.m.	Problemas con acreditación HOST descansos médicos, citas SIGI, Referencias (se activa flag de acreditación)
06/03/2017 - 10:40 a.m.	Top elevado 36.40 (el corte de fluido eléctrico del día sábado 4 1:08 p.m. el fluido estaba intermitente UPS no soportaban el cambio de automático porque esta con fallas)	06/03/2017 - 14:40 p.m	Se colgó servidor por primera vez discos no realizaban lectura se desconoce el motivo.



17/04/2017 - 7:18 a.m.	Top elevado a 45.40, de los 2200 usuarios 01 se quedó pegado haciendo varios reportes pesados.	17/04/2017 – 10:00 a.m.	Se colgó servidor discos no realizaban lectura se desconoce el motivo, se reseteo Servidor.
30/06/2017 - 10:07 a.m.	Se Detectó Regleta Quemada	30/06/2017 - 11:15 a.m.	Se quemó 1 de las regletas en Data Center, se produjo corte del sistema.
08/09/2017 - 4:00 a.m.	Para evitar implicancias; se realizaron actualizaciones durante las semanas fechas 15, 16, 26 se generaron pantallazos de error para enviárselos a Jaime Agreda lo cual envió actualizaciones de programas en diferentes módulos.	30/09/2017 - 08:00 a.m.	Se aplicó super parche SGH
20/03/2018 - 8:00 a.m.	Trafico de broadcast (bucle físico)	20/03/2018 - 11:00 a.m.	Se encontró en Sala 1 de Tomografía un pachcort (entrada y salida) conectado en el mismo switch D-link de 8 puertos
23/03/2018 - 6:30 p.m.	Corte de fluido eléctrico interno en el hospital	23/03/2018 - 10:45 p.m.	El UPS está inoperativo por lo que origino que el servidor y todos los switches cayeran y esto dejó inoperativo los diferentes servicios de Emergencias importantes del hospital NERM.




06/04/2018 - 7:50 a.m.	Corte de fluido eléctrico (aparente corto circuito en uno de los gabinetes eléctricos)	06/04/2018 - 9:50 a.m.	Se quemó 2da regleta en Data Center, se produjo corte del sistema.
14/05/2018 - 10.00 a.m.	Se modifica en Fm_Alman (Farmacia 11 se Elimina) Esta Suspendido desde hace tiempo	14/05/2018 - 11.50 a.m.	Problemas con Citas a Futuro que o Se pueden Anular por tener Recetas en la Tabla Fm_R1100.Dbf
25/05/2018 - 08.00 a.m.	Gabinete "C" desconectado de la fuente de 220 v. Gabinete B del 13 desconectado de la fuente 220v además de detectarse 3 ips que estaban inundando la red provocando multicast	25/05/2018 - 15.22 p.m.	Problemas con la conexión a telnet puerto 23 bloqueado

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2018)



Anexo 2

Formatos de movilización de equipos informáticos



Seguridad Social para todos

MOVILIZACION DE EQUIPOS
Hospital Edgardo Rebagliati Martins – EsSalud

MOVILIZACION DE EQUIPOS

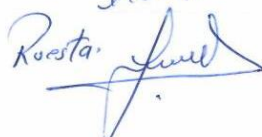
FECHA : 24 de Agosto del 2016
RESPONSABLE : ING. JULY CARDENAS PORRAS
AREA : OFICINA DE SOPORTE INFORMatico
LUGAR DE ORIGEN : OFICINA DE SOPORTE INFORMatico
LUGAR DE DESTINO : AUDITORIO 4 HNERM
MOTIVO : Traslado por reunión de videoconferencias

HARDWARE	LAPTOP
MARCA	DELL
MODELO	DELL PRECISION M4800
COD. PATRIMONIAL	-
SERIE	24367007342 / B6ZHJ72
CARACTERISTICAS ADICIONALES	CARGADOR CN-OWWW4XY48661 SAN-4VJG-A05

RED ASISTENCIAL REBAGLIATI
Hospital Nacional Edgardo Rebagliati Martins

Ing. Cesar A. Altamirano Castillo
Jefe E. Of. de Soporte Informático

Ing. Cesar Antonio Altamirano Castillo
Jefatura Oficina de soporte Informático
OSI-HNERM

Retorno - 24/08/16
Hº 24.
Ruesta. 

1

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2016)





MOVILIZACION DE EQUIPOS

Hospital Edgardo Rebagliati Martins – EsSalud

MOVILIZACION DE EQUIPOS

FECHA : 03 de Noviembre del 2016
RESPONSABLE : ING. CESAR ALTAMIRANO CASTILLO
AREA : OFICINA DE SOPORTE INFORMATICO
LUGAR DE ORIGEN : OFICINA DE SOPORTE INFORMATICO –
 NUEVA EMERGENCIA
LUGAR DE DESTINO : OFICINA DE SOPORTE INFORMATICO
MOTIVO : Desplazamiento

HARDWARE	CONTROLES DE AIRE ACONDICIONADO
MARCA	MCQUAY
MODELO	ZH/JT-03 Y YS1FF
CARACTERISTICAS ADICIONALES	CONTROL DE AIRE ACONDICIONADO UBICADOS EN EL DATA CENTER

RED ASISTENCIAL REBAGLIATI
 Hospital Nacional Edgardo Rebagliati Martins
 Ing. César A. Altamirano Castillo
 Jefe E. Of. de Soporte Informático

ING. CESAR ALTAMIRANO CASTILLO
 JEFE OSI-HNERM

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2016).



Anexo 3

Tabla 28

Mantenimiento preventivo equipos de cómputo Red Rebagliati 2016-2017

N°	UBICACIÓN	EQUIPOS DE COMPUTO	IMPRESORAS LASER	IMPRESORAS MATRICIALES	ESTIMACION X SEMANAS																		
					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	HOSPITAL NACIONAL EDGARDO REBAGLIATI MARTINS	1426	492	166	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■			
2	HOSPITAL III SUAREZ ANGAMOS	139	68	22																			
3	HOSPITAL II CAÑETE	68	21	18									■										
4	HOSPITAL I CARLOS ALCANTARA	100	39	26										■									
5	HOSPITAL I ULGARICO ROCCA	90	19	16											■								
6	CLINICA CENTRAL DE PREVENCION	47	17	7												■							
7	POLICLINICO RODRIGUEZ LAZO	74	31	24													■						
8	POLICLINICO PABLO BERMUDEZ	104	49	17														■					
9	POLICLINICO CHINCHA	53	15	10															■				
10	POLICLINICO PROCERES	59	21	17																■			
11	POLICLINICO SANTA CRUZ	25	24	3																■			
12	C. M. MALA	18	5	8																■			
13	CAP III SAN JUAN	47	34	2																■			
14	CAP III SAN ISIDRO	22	10	0																■			
15	CAP III SURQUILLO	25	10	0																■			
16	CAP III LURIN	20	4	0																■			

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2016-2017).



Tabla 29
Inventario Impresoras Láser de la Red Rebagliati de los años 2016 y 2017

N°	UBICACIÓN	Lexmark E342n	Lexmark E460n	Lexmark X644e	Lexmark MX511DE	Lexmark T644	HP 2015dn	HP 2055dn	HP 3005dn	HP 400 PRO	HP 3505 CP	HP 1215 CP	HP 2025 CP	HP 4350dn	TOTAL
1	HOSPITAL REBAGLIATI	15	2	24	5	4	224	105	75	19	1	2	2	14	492
2	HOSPITAL ULDARICO ROCA	0	0	1	0	0	13	0	3	2	0	0	0	0	19
3	POLICLINICO PROCERES	5	0	1	0	0	13	0	2	0	0	0	0	0	21
4	POLICLINICO BERMUDEZ	2	1	2	0	0	35	6	2	1	0	0	0	0	49
5	POLICLINICO MALA	1	0	1	1	0	2	0	0	0	0	0	0	0	5
6	CLINICA – LARCO	2	0	1	1	0	11	0	2	0	0	0	0	0	17
7	HOSPITAL SUAREZ-ANGAMOS	2	0	1	0	0	58	1	4	2	0	0	0	0	68
8	HOSPITAL RODRIGUEZ LAZO	1	1	1	0	0	20	2	4	2	0	0	0	0	31
9	POLICLINICO CHINCHA	2	0	1	0	0	10	0	2	0	0	0	0	0	15
10	HOSPITAL CAÑETE	0	0	1	0	0	17	1	1	1	0	0	0	0	21
11	HOSPITAL ALCANTARA	4	0	1	0	0	26	3	5	0	0	0	0	0	39
12	UBAP SANTA CRUZ	0	0	0	0	0	19	0	4	1	0	0	0	0	24
13	UBAP SURQUILLO	0	0	0	0	0	0	10	0	0	0	0	0	0	10
14	UBAP LURIN	0	0	0	0	0	1	1	0	2	0	0	0	0	4
15	UBAP SAN ISIDRO	0	0	0	0	0	0	10	0	0	0	0	0	0	10
16	UBAP SAN JUAN MIRAFLORES	0	0	0	0	0	8	26	0	0	0	0	0	0	34
	TOTAL	34	4	35	7	4	457	165	104	30	1	2	2	14	859

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2016-2017).



Tabla 30
Inventario Impresoras Matriciales Red Rebagliati de los años 2016 y 2017

N°	UBICACIÓN	Epson FX-890	Epson LX-300	Epson Fx-1170	Epson Fx-2190	Epson LX-350	Epson TMU-220A	TOTAL
1	HOSPITAL REBAGLIATI	106	10	5	17	15	13	166
2	HOSPITAL ULДАРICO ROCA	12	0	2	2	0	0	16
3	POLICLINICO PROCERES	15	0	0	2	0	0	17
4	POLICLINICO BERMUDEZ	10	0	5	2	0	0	17
5	POLICLINICO MALA	5	1	0	2	0	0	8
6	CLINICA – LARCO	3	0	0	2	0	2	7
7	HOSPITAL SUAREZ-ANGAMOS	19	0	0	3	0	0	22
8	HOSPITAL RODRIGUEZ LAZO	11	6	0	2	3	2	24
9	POLICLINICO CHINCHA	6	2	0	2	0	0	10
10	HOSPITAL CAÑETE	12	0	0	2	4	0	18
11	HOSPITAL ALCANTARA	21	1	0	2	0	2	26
12	UBAP SANTA CRUZ	0	2	1	0	0	0	3
13	UBAP SURQUILLO	0	0	0	0	0	0	0
14	UBAP LURIN	0	0	0	0	0	0	0
15	UBAP SAN ISIDRO	0	0	0	0	0	0	0
16	UBAP SAN JUAN MIRAFLORES	0	0	0	0	0	2	2
	TOTAL	220	22	13	38	22	21	336

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2016-2017).



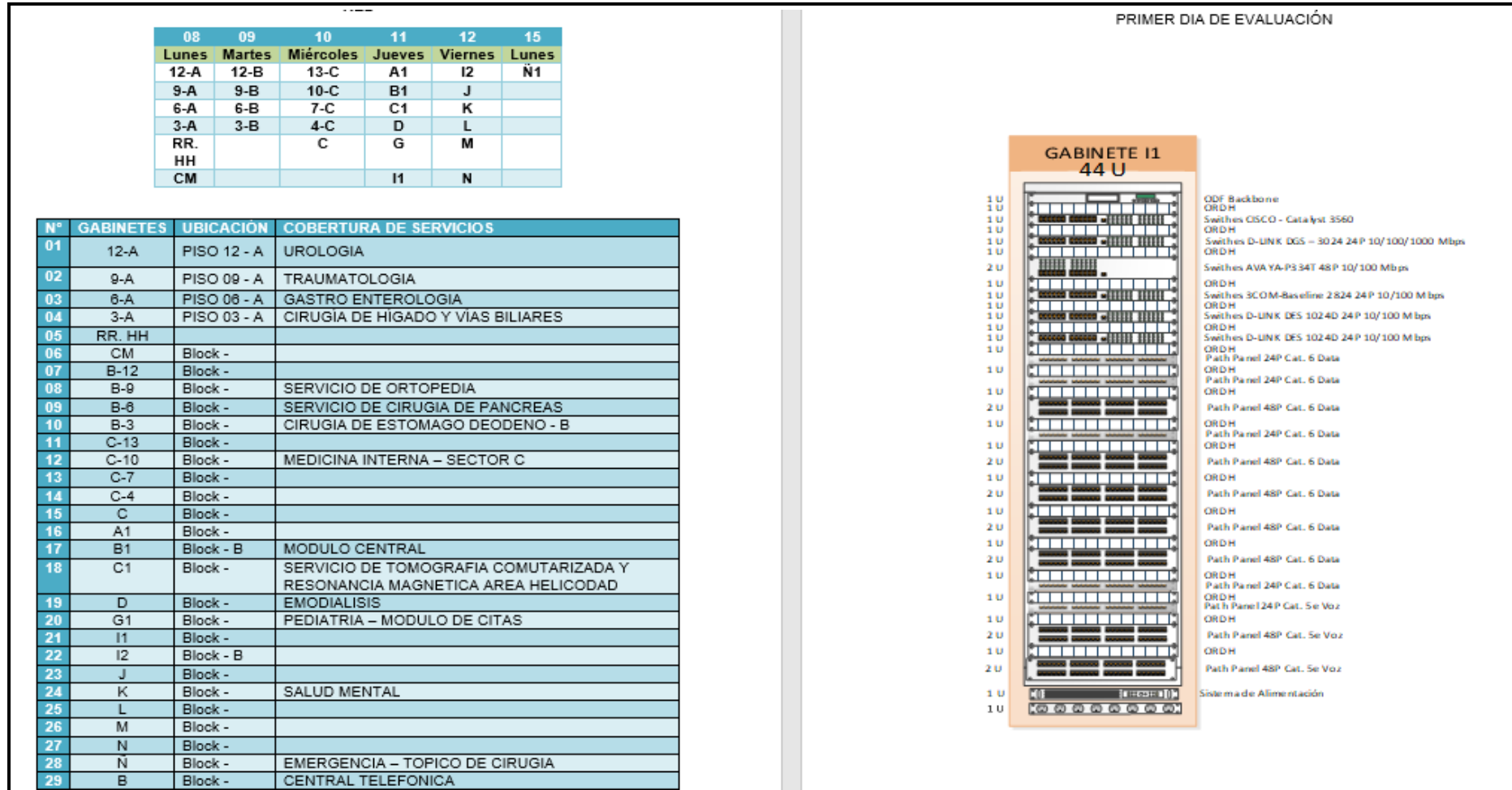


Figura 74. Diagnóstico de Gabinetes y Equipos Intermedios de la Red Rebagliati. Fuente: Oficina de Soporte Informático HNERM EsSALUD (2016-2017).



Anexo 4

Tabla 31

Resumen simplificado mantenimiento preventivo para data center ANSI /TIA-942

REQUERIMIENTOS GENERALES		
LOCALIZACIÓN	DISEÑO DE ARQUITECTURA	DISEÑO ELECTRICO
Evitar cercanía fuentes EMI. Evitar ventanas exteriores. Accesibilidad para grandes equipos.	<ul style="list-style-type: none"> • Dimensión física (proyección de crecimiento). • Considerar tableros eléctricos y UPS. • Altura de techo: mínimo 8.5 pies (2.59 m). • La iluminación no debe de ser provista del mismo panel de equipos. • La puerta debe ser por lo menos de 3 pies x 7 pies (0.90 m x 2.10 m). • La carga del piso debe ser: <ul style="list-style-type: none"> - Mínimo carga distribuida: 150 lbf/ft² (224 kg/m²) - Recomendado: 250 lbf/ft² (373 kg/m²) 	<p>Energía:</p> <ul style="list-style-type: none"> • Definir cantidades apropiadas de tomas eléctricas y tableros. • Puesta a tierra y cableado. • Cumplimiento de especificaciones de ANSI-J-STD-607-A.
ACCESO	CONDICIONES AMBIENTALES	OTRAS CONSIDERACIONES
Limitado a personal autorizado.	<ul style="list-style-type: none"> • Cuarto protegido de contaminantes • Operación continua 24/7/365 • Requerimiento de Temp/Humedad <ul style="list-style-type: none"> - 20 °c – 25 °c - 40% - 55% de humedad relativa • Medición de los equipos en operación • Mantener presión positiva • Adecuada ventilación de baterías • Vibración. Puede generar acoplamiento al cableado o equipos. 	<p>Protección de fuego:</p> <ul style="list-style-type: none"> • Detección temprana <p>Extinción</p> <p>Infiltración de agua:</p> <ul style="list-style-type: none"> • Reducir donde exista riesgo <p>Drenaje en el piso.</p> <p>No tubos o drenajes sobre piso.</p>

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017).



Anexo 5

Tabla 32

Equipos Intermedios Swithes de la Red de Telecomunicaciones del Hospital Nacional Edgardo Rebagliati Martins

N°	MARCA	TIPO	MODELO	VELOCIDAD	CONFIGURACION	VLAN		CAPA	SFP	GE	ETH	CANTIDAD
1	ALCATEL-LUCENT	CORE PRINCIPAL	OmniSwitch 9800	10/100/1000	MODULAR	Administrables	SI	L2/L3	24	168	-	1
2	CISCO	CORE CAMARAS	Catalyst 3750	10/100/1000	FIJO	Administrables	SI	L2/L3	12	-	-	7
3	D - LINK	CORE BACKUP	DXS - 3326GSR	10/100/1000	FIJO	Administrables	SI	L2/L3	24	4	-	1
4	CISCO	-	Router BEFSR81	-	FIJO	-	-	-	-	-	8	1
5	D - LINK	-	DIR-400 ROUTER	-	FIJO	-	-	-	-	-	24	1
6	ALCATEL-LUCENT	BORDE DATOS	OmniStack LS 6224P	10/100	FIJO	Administrables	SI	L2	4	2	24	31
7	ALIED TELESIS	BORDE DATOS	AT 8000S/24POE	10/100	FIJO	Administrables	SI	L2	2	2	24	1
8	CISCO	BORDE CAMARAS	Catalyst 3560 Series POE	10/100	FIJO	Administrables	SI	L2	1	1	8	7
9	3COM	DISTRIBUCION	Super Stack 5500G -EL	10/100	FIJO	Administrables	SI	L2	2	2	24	6
10	3COM	DISTRIBUCION	Baseline Switch 2824	10/100	FIJO	Administrables	SI	L2	2	2	24	3
11	A VAYA	DISTRIBUCION	P334T	10/100	FIJO	Administrables	SI	L2	2	2	48	1
12	ALIED TELESIS	DISTRIBUCION	AT- GS950	10/100/1000	FIJO	Administrables	SI	L2	2	2	8	1
13	D - LINK	DISTRIBUCION	DGS - 3100	10/100/1000	FIJO	Administrables	SI	L2	4	24	-	1
14	D - LINK	DISTRIBUCION	DGS - 3024	10/100/1000	FIJO	Administrables	SI	L2	4	24	-	5
15	D - LINK	DISTRIBUCION	DGS - 3120	10/100/1000	FIJO	Administrables	SI	L2/L3	4	24	-	1
16	D - LINK	DISTRIBUCION	DGS - 1510	10/100/1000	FIJO	Administrables	SI	L2/L3	4	24	-	22
17	D - LINK	DISTRIBUCION	DGS - 1210	10/100/1000	FIJO	Administrables	SI	L2	4	24	-	3
18	D - LINK	DISTRIBUCION	DES - 1024A	10/100	FIJO	Stand-alone	NO	-	-	-	24	60
19	D - LINK	DISTRIBUCION	DES - 1024D	10/100	FIJO	Stand-alone	NO	-	-	-	24	79
20	D - LINK	DISTRIBUCION	DES - 1016D	10/100	FIJO	Stand-alone	NO	-	-	-	16	2
21	D - LINK	DISTRIBUCION	DES - 1060D	10/100	FIJO	Stand-alone	NO	-	-	-	16	1
22	TRENDnet	DISTRIBUCION	TEG - 516DG	10/100	FIJO	Stand-alone	NO	-	-	-	16	1

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017).



5.3.5. Desarrollo de la Propuesta de Virtualización de los Dispositivos de Conmutación en el HNERM-EsSALUD.

La solución propuesta de la Virtualización estará conformada por un conjunto de componentes de infraestructura de red cableada e inalámbrica con una capa de gestión de red y control de acceso centralizado de última generación para cubrir las necesidades y demandas en conectividad de hoy en día dentro de la institución del HNERM-EsSALUD. En el siguiente diagrama (Gráfico N°53) se muestra el diseño de la Virtualización de dispositivos de conmutación propuesta en el HNERM-EsSALUD. Este diseño sigue un diseño modular que permite agrupar los dispositivos de conmutación de red según funcionalidades de tal manera que puedan cubrir las necesidades de la institución. Este diseño modular permitirá mejorar significativamente el desempeño de la Red LAN, a través de la convergencia de redes, calidad de servicio, seguridad, escalabilidad y alta disponibilidad, y sea fácil de gestionar y permita detectar fallas en menos tiempo.

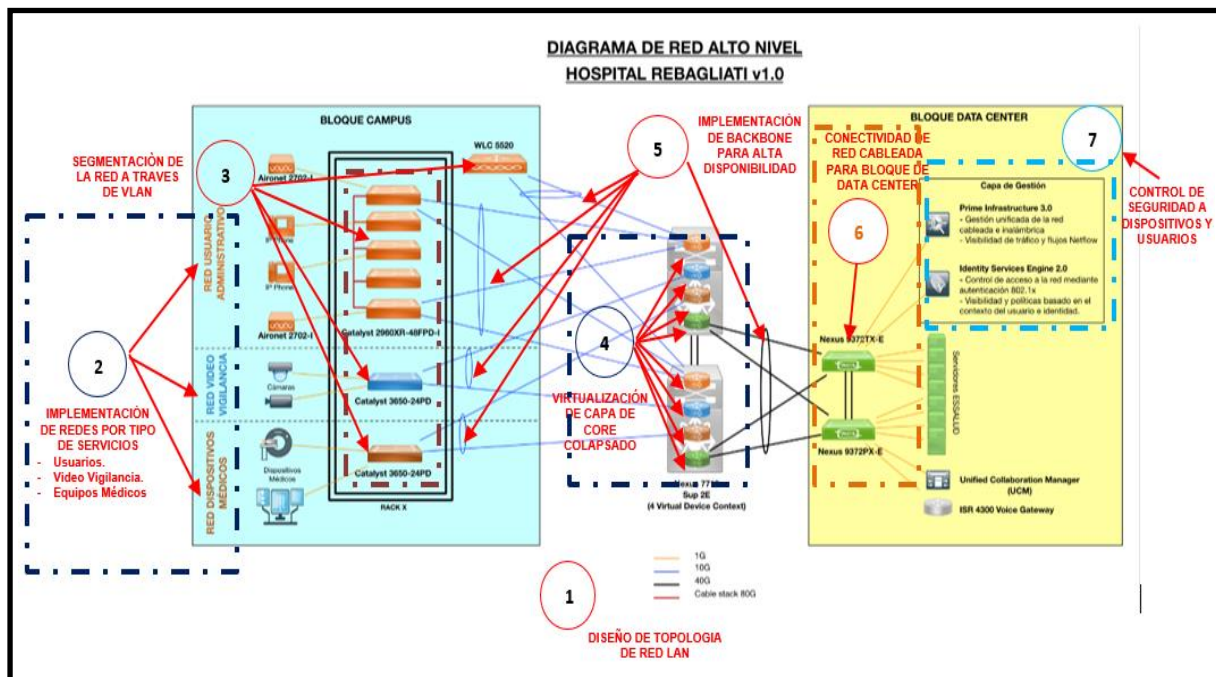


Figura 75. Diseño Diagrama de Red Alto Nivel HNERM EsSALUD. Fuente: Cisco (2013).

Nota: El Diseño de Alto Nivel que se está Proponiendo Brindará alta Disponibilidad, Implementación de Seguridad a Través de Firewall, Redundancia con los Servidores y Virtualización de los Switchs Core Nexus 7000 en el HNERM EsSALUD.



5.3.5.1. Conectividad de Red para el Bloque de Campus

El Bloque de Campus es el encargado de albergar la conectividad de los usuarios y terminales de usuario que accederán de manera directa o indirecta a los recursos del centro de datos para explotar la data y hacer análisis de la información.

Capa de acceso a la red

Esta capa lo conforman todos los dispositivos de conmutación de red que permiten dar acceso a usuarios mediante un medio cableado o inalámbrico a recursos internos (Internet, extranet o centro de datos). También se encuentran todos los terminales que interactúan con el usuario final, dispositivos IP que requieran conectividad, alimentación de energía por la red (video cámaras, impresoras, etc.) y componentes médicos.

A nivel de red, esta capa proporciona la demarcación inteligente entre la infraestructura de red y los dispositivos de computación. Proporciona una capa de seguridad, calidad de servicio (QoS) y la política de límite de confianza y es un elemento clave para permitir múltiples servicios. Como base del diseño, se ha propuesto definir tres grupos de redes de acuerdo a los servicios que se brindará a los endpoints conectados:

a. Red de Usuarios Administrativos:

Dentro de esta red se permitirá la conexión hacia endpoints como computadoras, teléfonos, impresoras y puntos de acceso dirigido específicamente para la conexión a la red de los usuarios administrativos y empleados del HNERM-EsSALUD. Para esta red se implementarán los dispositivos de conmutación Switches con funcionalidades de entrega de energía por puertos PoE/PoE+ para la conexión hacia los teléfonos y puntos de acceso inalámbricos.



b. Red de Videovigilancia:

Esta red estará dedicada exclusivamente para la conexión con el sistema y las cámaras de video vigilancia para poder aplicar características de calidad de servicios específicos para el tipo de dato que será transportado por esta red.

Esta red estará compuesta por dispositivos de conmutación de alto rendimiento a nivel de acceso con funcionalidades de entrega de energía por puertos PoE/PoE+ para las cámaras de videovigilancia que lo requieran.

c. Red de Equipos Médicos:

Esta red estará dedicada exclusivamente para la conexión con los equipos médicos y la red del hospital. Ofreciendo una vía exclusiva para el tráfico de información de imágenes médicas, entre otros dentro de la red.

Se instalarán dispositivos de conmutación (Switches de alto rendimiento a nivel de acceso para garantizar un envío seguro y óptimo de la información a través de la Red).

Adicionalmente los dispositivos de conmutación Switches que estarán dentro del nivel de acceso del diseño tendrán una conexión hacia los dispositivos de conmutación Switches principales con enlaces de 10Gbps en redundancia utilizando protocolos de agregación de puertos para optimizar el ancho de banda en esta conexión. Por otro lado, se tendrá la opción de agrupar los dispositivos de conmutación Switches para tener una gestión centralizada y fuentes redundantes para garantizar la disponibilidad de los servicios y conexión a la red.



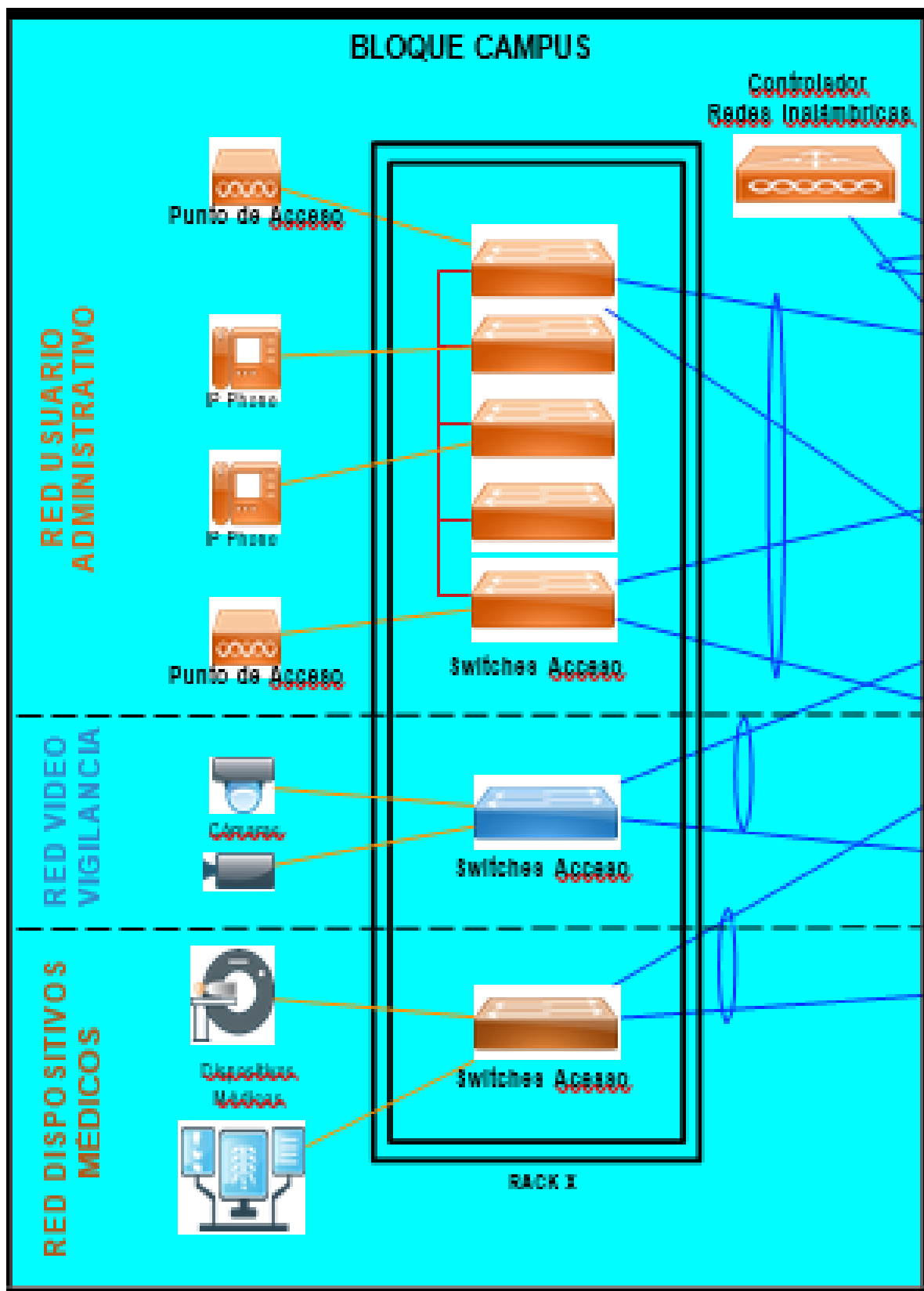


Figura 76. Bloque Campus. Fuente: Cisco (2013).



Capa de Core Colapsado

La capa de Core Colapsado permitirá agrupar funcionalidades de la capa de distribución y capa de Core dentro de un solo dispositivo de conmutación o dos si se maneja un diseño en alta disponibilidad. Esta capa se encargará de proporcionar acceso a los servicios y recursos de red de los usuarios y los dispositivos distribuidos en una única ubicación geográfica. Su diseño de arquitectura promueve el no-bloqueo, la convergencia rápida y ultra-alta, y una alta disponibilidad además de la aplicación funcionalidades de calidad de servicio, virtualización de la red y agregación de dispositivos de conmutación de capa 2.

Dentro de esta solución se tiene contemplado los dispositivos de conmutación Switches de Core de alto rendimiento y densidad de puertos para poder trabajar a velocidades de 10Gbps y 40 Gbps en el presente y 100Gbps en un futuro crecimiento de la red.

Además de poseer mecanismos de alta disponibilidad a nivel de hardware, supervisoras, fabrics, fuentes de energía y enlaces para la conexión hacia los demás componentes de la red.

Estos dispositivos de conmutación Switches serán capaces de poder virtualizar no solo funcionalidades de capa 2 (VLAN's) y capa 3 (VRF's) sino también crear contextos de dispositivos virtuales. Esto permitirá crear dispositivos de conmutación Switches lógicos únicos bajo el framework del dispositivo de conmutación switch físico original que serán configurados y gestionados como si fueran dispositivos de conmutación Switches físicos independientes.

Los procesos del sistema operativo y los recursos de hardware serán repartidos y agrupados para formar una entidad de dispositivo de conmutación switch virtual como se muestra en la (Gráfico N°48).



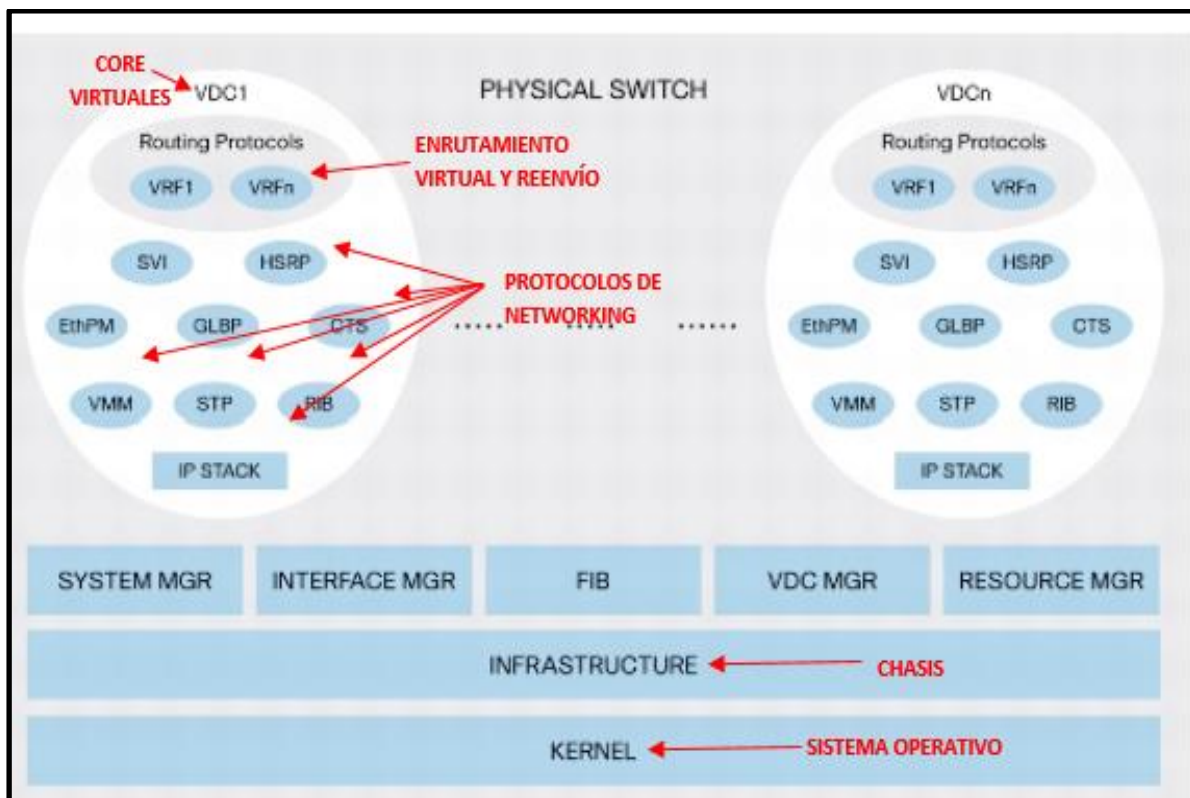


Figura 77. Diseño de Arquitectura del Conmutador Fuente: Cisco (2013).

Bajo este concepto de virtualización de dispositivos de conmutación, la solución ofrecerá dos Switches de Core con las características descritas y que además ofrezca la funcionalidad de poder crear cuatro Switches lógicos dedicados para la comunicación hacia las redes de usuarios administrativos, redes de video vigilancia, redes de equipos médicos, la red del centro de datos y un switch lógico adicional para la comunicación entre ellos.

Cada uno de estos Switches lógicos independientes estarán configurados de manera personalizada para poder atender las demandas y necesidades específicas de cada tipo de red definidas dentro de la institución de salud.

Adicionalmente, estos dispositivos de conmutación Switches ofrecerán una conexión entre sí de 40 Gbps para garantizar alta velocidades de transmisión entre los dos dispositivos.



La conexión hacia los Switches de acceso y la controladora de redes inalámbricas serán a velocidades de 10Gbps, mientras que la conexión hacia el centro de datos será a velocidades de 40Gbps.

Ambas conexiones estarán basadas en un esquema de alta disponibilidad con enlaces redundantes que permitan eliminar el bloqueo de puertos mediante el protocolo STP, uso del ancho de banda de todos los enlaces de subida disponibles y acelerar la convergencia en caso de la caída del enlace o dispositivo *Figura 56*.

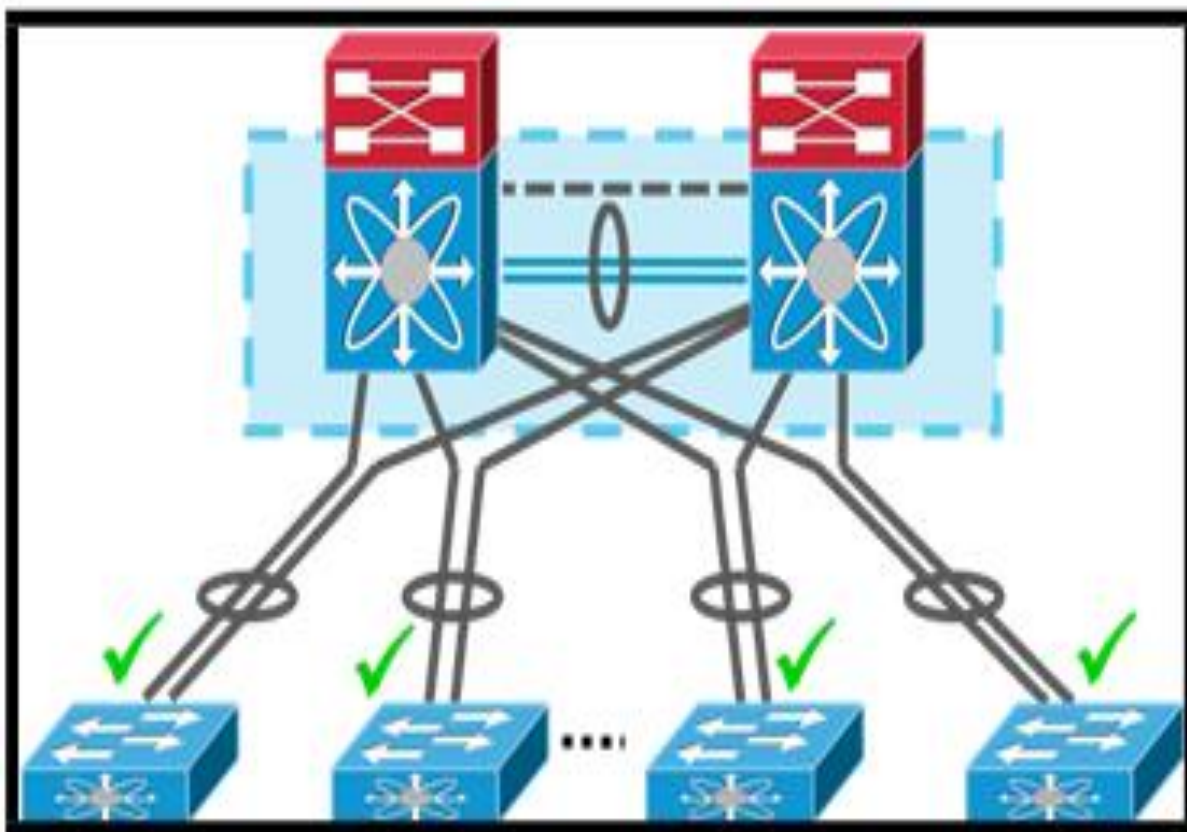


Figura 78. Enlaces Redundantes. Fuente: Cisco (2013).



5.3.5.2. Conectividad de Red inalámbrica para el Bloque de Campus

El acceso inalámbrico está disponible para los clínicos, médicos, contratistas y los pacientes/visitantes a través de arquitecturas inalámbricas altamente seguras y escalables.

Entre los componentes que conforman este renglón de la red se encuentran los puntos de acceso inalámbrico que serán utilizados para conectar los dispositivos inalámbricos autorizados.

Estos proveerán el servicio de radio frecuencia para cubrir las zonas designadas a proveer este acceso.

Además, se incluye el controlador de estos puntos de acceso inalámbrico, quien se encargará de distribuir la configuración apropiada a los puntos de acceso inalámbrico, monitoreo básico del espectro inalámbrico, y otras funciones de gestión.

Se considera que el Hospital, requiere implementar una red de datos inalámbrica, para dar acceso (a ciertos servicios de red), tanto a sus propios usuarios, como para visitantes; lo cual se ha de lograr con la instalación de puntos de acceso inalámbrico.

Por dicho motivo se ha considerado la Instalación de Access Points compatibles con los estándares 802.11a, 802.11b, 802.11g, 802.11n y 802.11ac. Dichos Access Point, también trabajarán con el estándar 802.3af. (GRÁFICO N°57).

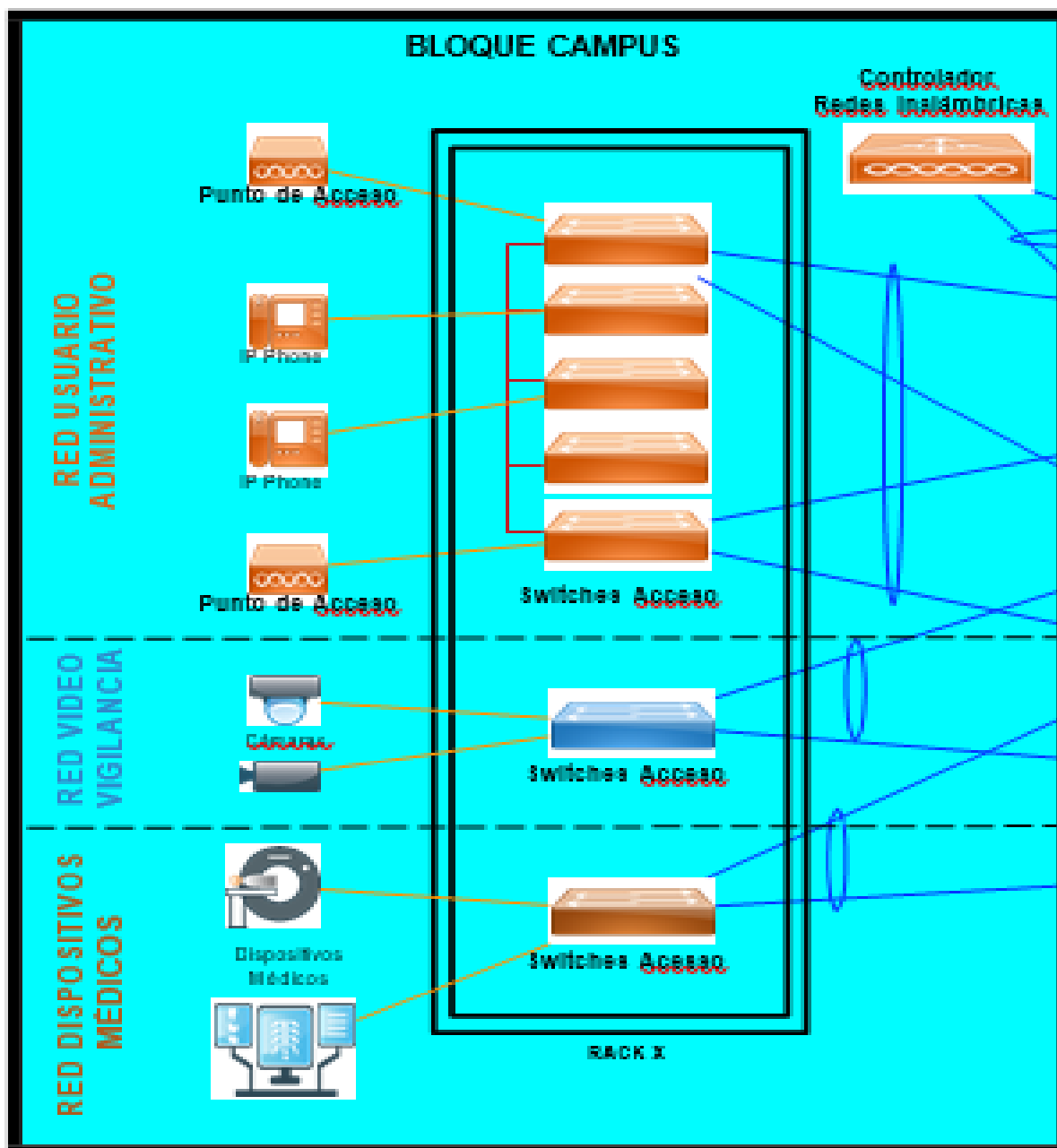


Figura 79. Conectividad de Red Inalámbrica Para el Bloque de Campus. Fuente: Cisco (2013).

Es necesario indicar que la red inalámbrica debe incluir un controlador inalámbrico que incluya las redes 802.11 a/b/g/n/ac, sumado a la capacidad de firewall en el aire, con capacidad de armar mapas de calor de los puntos de acceso, capacidad de monitoreo y gestión de la red inalámbrica, capacidad de reaccionar ante caídas de algún Access Point en forma automática; segmentación y control del tráfico en función de la identidad de usuarios, de forma que se pueda definir y controlar por ejemplo cuánto ancho de banda se le brinda a un médico versus a un visitante.



5.3.5.3. Conectividad de Red Cableada para el Bloque Data Center

En la actualidad, la arquitectura del centro de datos debe dar soporte a una fuerza laboral sumamente móvil, a la proliferación de dispositivos de conmutación y a modelos de negocio basados en datos.

Al mismo tiempo, debe poder incorporar sin inconvenientes aplicaciones y servicios en la nube.

Es por ello, que se necesitan implementar componentes de red especializados para un centro de datos que garantice un alto rendimiento que se vea reflejado en la comunicación eficiente y rápida entre los dispositivos de conmutación de acceso y las aplicaciones alojadas dentro de los servidores de la institución del HNERM-EsSALUD.

Dentro de este bloque, se contemplan dos dispositivos de conmutación Switches especializados para el centro de datos que podrán trabajar a velocidades de 1Gbps y 10Gbps para la conexión con los servidores actuales y a velocidades de 40Gbps en la conexión hacia los Switches de Core.

Además, se trabajará bajo un esquema de alta disponibilidad con enlaces redundantes hacia los dispositivos conmutadores Switches principales tal como se aprecia en la GRÁFICO N°58.

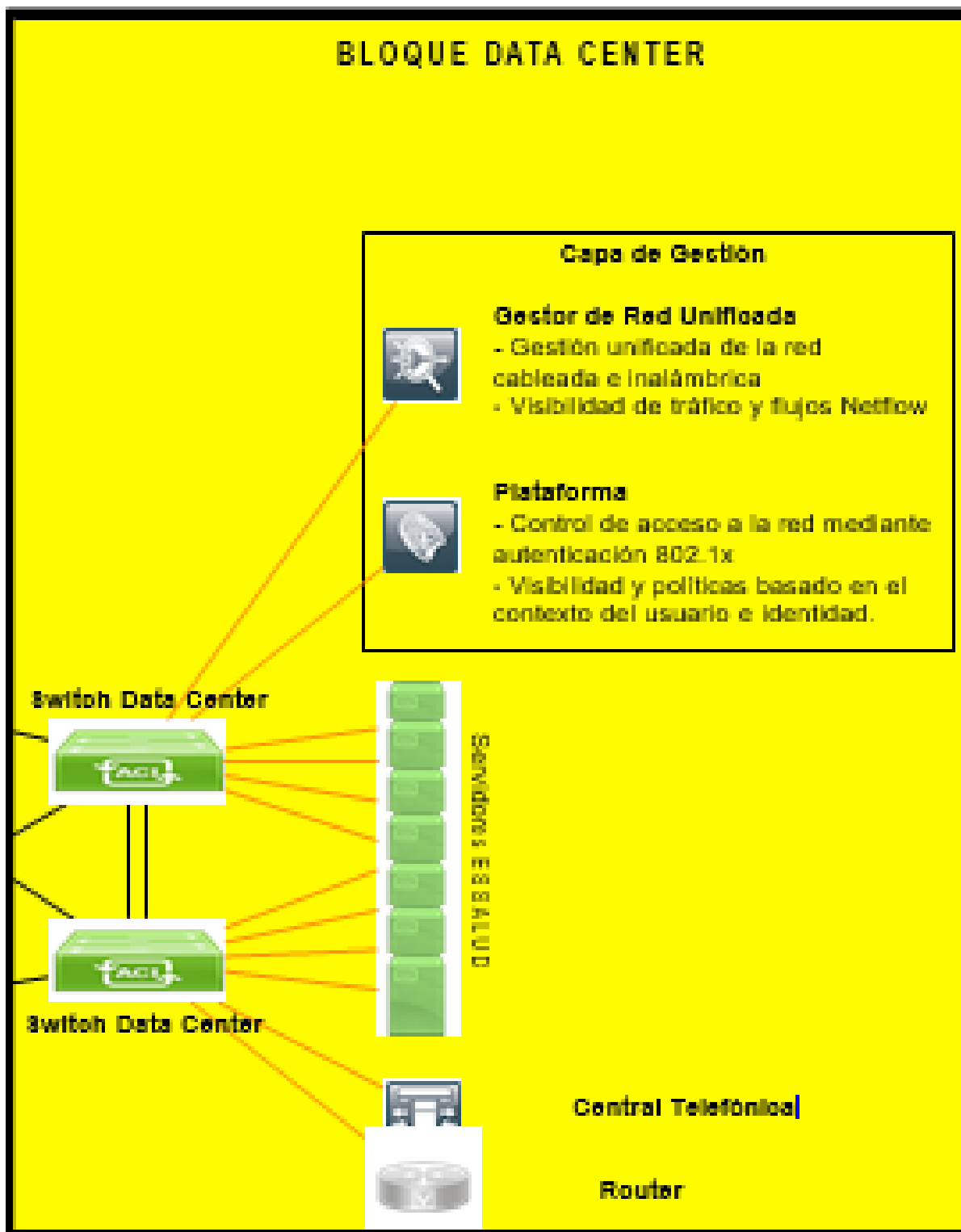


Figura 80. Bloque Data Center Fuente: Cisco (2013).



Acceso Seguro y Automático a dispositivos y usuarios

Dispositivos biomédicos, dispositivos informáticos y dispositivos móviles se identifican de forma dinámica y se aprovisionan de forma automática para el segmento de red apropiado. A los dispositivos no autorizados se les niega el acceso y son reportados a un sistema de gestión central.

El acceso para los dispositivos móviles (dispositivos iPad, iPhone, Android) está soportado para uso de los médicos, clínicos, visitantes y pacientes a través de un motor de política centralizada que hace cumplir las políticas de seguridad. A los usuarios se le brinda acceso a la información clínica y de recursos basado en sus funciones específicas. Este motor inteligente de control de acceso a la red puede ser una plataforma instalada dentro de un servidor dedicado o virtualizado en un servidor en operación con otras aplicaciones.

Plataforma de monitoreo y gestión de Red

La solución tendrá una plataforma que permita tener el control y visibilidad de la red de forma centralizado tanto para el acceso inalámbrico como para el cableado. Esta plataforma ofrecerá herramientas de configuración de red a través de plantillas predefinidas, despliegue de configuraciones en base a horarios específicos, monitoreo de los dispositivos de red y usuarios finales en el tiempo a través de gráficos estadísticos, visibilidad del tráfico de aplicaciones dentro de la red del hospital y la generación de diversos reportes para obtener información detallada del comportamiento de la red.

Con estas características la plataforma ofrecerá la simplificación de la gestión de la red. Esta plataforma inteligente puede ser una instalada dentro de un servidor dedicado o virtualizado en un servidor en operación con otras aplicaciones. Son conocidas muchas aplicaciones de Emuladores que sirven para virtualizar los dispositivos de Conmutación para administrar las redes LAN.

Para el presente proyecto decidimos desarrollar una propuesta de virtualización de los dispositivos de conmutación en este caso decidimos Emular el Switch Nexus 7000 de Cisco y usar el software Emulador GNS3.

Asimismo, cabe resaltar que los conmutadores Cisco ® Nexus 7000 introducen el soporte para la plataforma de software Cisco NX-OS, una nueva clase de sistema operativo diseñada para centros de datos.

Basado en la plataforma SAN-OS de Cisco MDS 9000, Cisco NX-OS introduce compatibilidad con contextos de dispositivos virtuales (VDCs), lo que permitirá virtualizar los conmutadores a nivel de dispositivo en el HNERM-EsSALUD. Todo el proceso y la metodología de desarrollo para la aplicación la podremos verlos líneas abajo:

Cada VDC configurado se presenta como un dispositivo único para los usuarios conectados dentro del marco de ese conmutador físico. El VDC se ejecuta como una entidad lógica independiente dentro del conmutador, manteniendo su propio conjunto único de procesos de software en ejecución, teniendo su propia configuración y siendo gestionado por un administrador independiente.

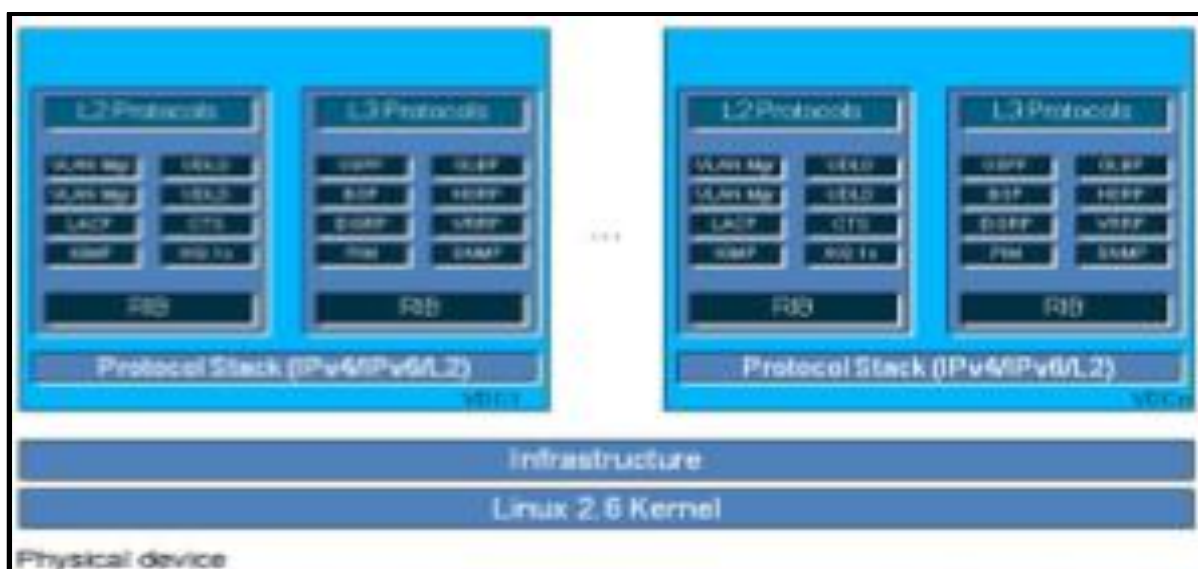


Figura 81. Arquitectura VDC Propuesto HNERM EsSALUD. Fuente: Cisco Nexus 7000 Series Virtual Device Context Configuration Guide (2014)



Cisco Nexus 7000 Series hereda una serie de tecnologías de virtualización presentes en el software Cisco IOS.

Desde una perspectiva de nivel 2, las LAN virtuales (VLAN) virtualizan los dominios de puente en el chasis de Nexus 7000. El soporte de virtualización para la capa 3 se admite mediante el concepto de instancias de reenvío de rutas virtuales (VRF). Un VRF se puede utilizar para virtualizar las tablas de encaminamiento y reenvío de Capa 3.

El aspecto de virtualización de la plataforma de software Cisco NX-OS se ha ampliado para dar soporte a la noción de contextos de dispositivos virtuales (VDCs). Un VDC se puede utilizar para virtualizar el propio dispositivo, presentando el switch físico como múltiples dispositivos lógicos. Dentro de ese VDC puede contener su propio conjunto único e independiente de VLANs y VRFs.

Cada VDC puede asignarle puertos físicos, permitiendo así que el plano de datos de hardware sea virtualizado también. Dentro de cada VDC, un dominio de gestión independiente puede gestionar el VDC propiamente dicho, permitiendo así que el propio plano de gestión también sea virtualizado. Asimismo, se pueden asignar por puerto. Las interfaces lógicas tales como SVI que están asociadas con la misma interfaz física no se pueden asignar a diferentes VDC en la implementación actual.

Por lo tanto, no es posible virtualizar una interfaz física y asociar las interfaces lógicas resultantes a diferentes VDC.

Sin embargo, es posible virtualizar una interfaz física y asociar las interfaces lógicas resultantes con diferentes VRF o VLAN. Por lo tanto, se puede asignar a las VDCs interfaces físicas, mientras que las VLAN y las VRF pueden asignar interfaces lógicas y físicas.

Un ejemplo de esto se puede ver en la Figura N°07. Los puertos 1 a 8 pertenecen a VDC 5 mientras que los puertos 41 a 48 pertenecen a VDC 10. Dentro de cada VDC, los puertos son además virtualizados pertenecientes a una VLAN o VRF.



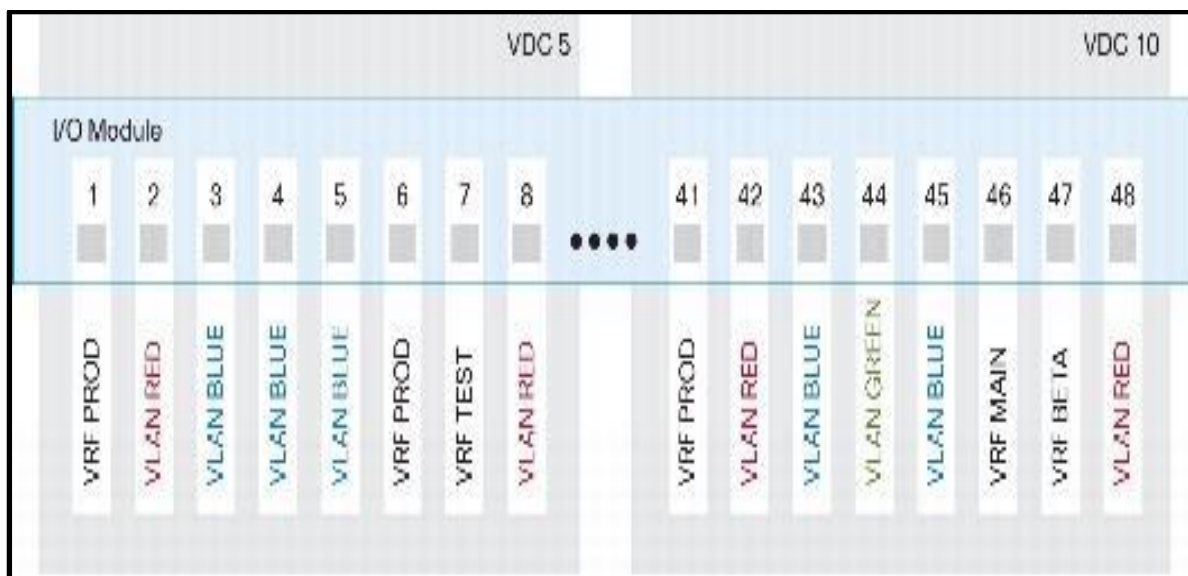


Figura 82. VDC. Fuente: Cisco (2014).

Después de asignar un puerto a un VDC por el administrador raíz a nivel VDC predeterminado, depende del VDC-admin administrar (configurar y utilizar) el puerto previamente asignado.

Ejecutar otros comandos relacionados, como un comando show interface, por ejemplo, permitirá al usuario ver sólo aquellas interfaces que han sido asignadas al VDC.

Cada VDC mantiene su propio archivo de configuración, reflejando la configuración real de los puertos bajo el control del VDC.

Además, la configuración local contendrá cualquier elemento de configuración específico de VDC, como una función de usuario VDC y el ámbito de mandato asignado a ese usuario.

Tener un archivo de configuración separado por VDC también proporciona un nivel de seguridad que protege este VDC de los cambios de configuración de operación que se pueden realizar en otro VDC.



Las VLAN son otro recurso importante que se ha extendido en Cisco NX-OS. Hasta 16.384 VLANs, definidas a través de VDCs múltiples, son compatibles en un Cisco Nexus 7000 Series Switch.

Cada VDC admite un máximo de 4096 VLAN según el estándar IEEE 802.1q.

La nueva compatibilidad con VLAN ampliada permitirá asignar una VLAN entrante a una VLAN por VDC. Nos referiremos a esta VLAN por VDC como un dominio de puente para mayor claridad.

De esta manera, un administrador de VDC puede crear VLANs numeradas en cualquier parte del rango de ID de VLAN 802.1q y el VDC asignará esa VLAN recién creada a uno de los dominios de puente 16.384 predeterminados disponibles en el conmutador.

Esto permitirá a los VDC del mismo conmutador físico reutilizar ID de VLAN en sus configuraciones, mientras que en el nivel de OS la VLAN es de hecho un dominio de puente único dentro del contexto del switch físico.

Por ejemplo, VDC A y VDC B podrían crear VLAN 100, que a su vez podrían ser asignadas a los dominios de puente 250 y 251, respectivamente.

Cada administrador utilizará los comandos show que hacen referencia a la VLAN 100 para supervisar y gestionar dicha VLAN.

Como puede verse en la Gráfico N° 61, un fallo en un proceso que se ejecuta en VDC 1 no afecta a ninguno de los procesos en ejecución en los otros VDC.

Otros procesos equivalentes seguirán funcionando desinhibidos por cualquier problema asociado con el proceso de ejecución defectuoso.

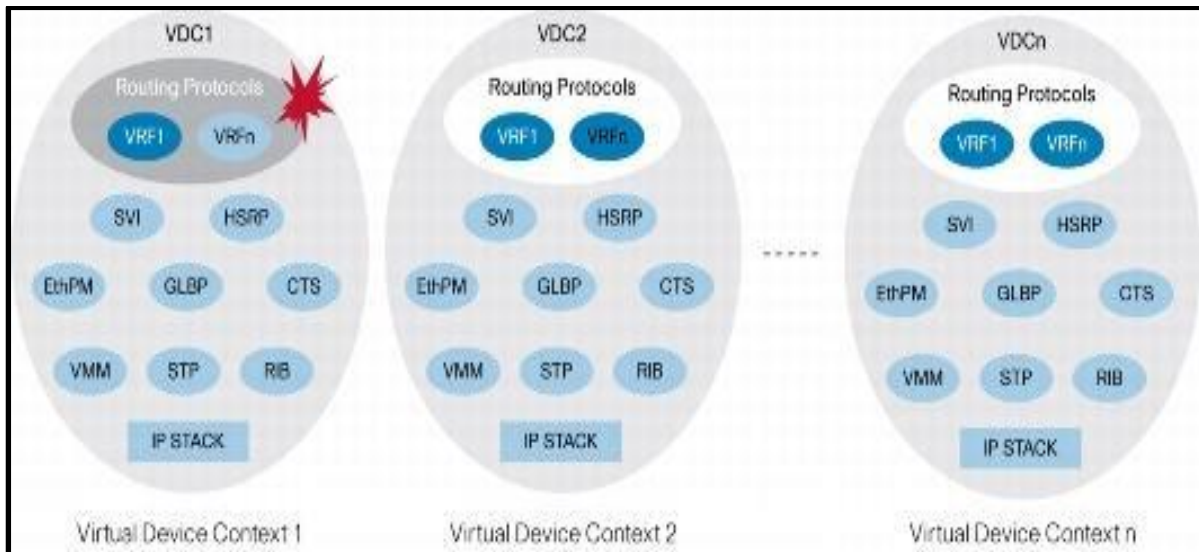


Figura 83. Aislamiento de Fallas VDC. Fuente: Cisco (2014).

El aislamiento de fallos se mejora con la capacidad de proporcionar comandos de depuración por VDC. El registro por VDC de mensajes a través de syslog es también otra característica importante de las capacidades de aislamiento de fallas VDC.

Cuando se combinan, estas dos características proporcionan una poderosa herramienta para los administradores en los problemas de localización, de esta manera los servicios continuarían y no generarían caídas ni tráficos de información de la Red LAN, gracias a este aislamiento de fallas.

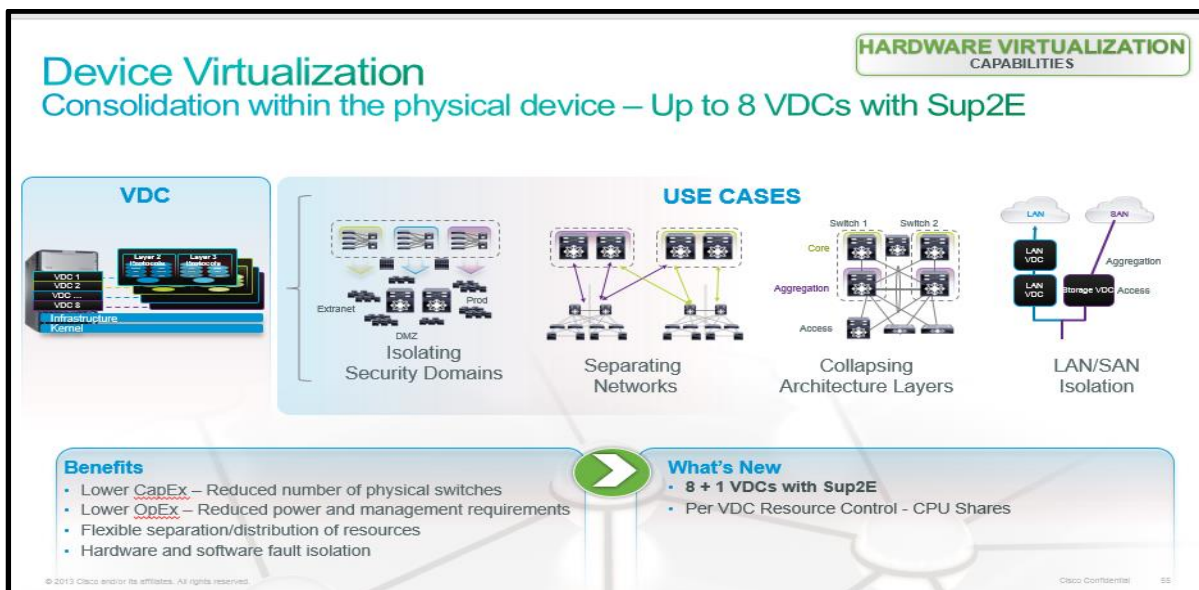


Figura 84. Device Virtualization VDC'S. Fuente: Cisco (2013).



Configuración inicial del VDC

La configuración para VDC comienza con la creación de un VDC. Pueden existir hasta cuatro VDC en el sistema al mismo tiempo.

Dado que siempre hay un VDC activo por defecto (VDC 1), esto significa que se pueden crear hasta tres VDC adicionales desde la CLI.

La creación de un VDC se realiza desde el modo de configuración utilizando el comando `vdc <nombre de vdc>`, como se muestra aquí: Creando los nombres de los VDC del HNERM-EsSALUD:

```

ESSALUD-N7K9-COREB# conf
ESSALUD-N7K9-COREB (config) # vdc Datos
ESSALUD-N7K9-COREB (config-vdc) # show vdc
Vdc_id vdc_name mac state
Reba_Sgh_Datos
1 active ESSALUD-N7K9-COREB 00: 18: ba: d8: 4c: 3d
2 active Datos 00: 18: ba: d8: 4c: 3e
ESSALUD-N7K9-COREB (config-vdc) # show vdc detail
Vdc id: 1
Vdc name: change
Status vdc: active
Vdc mac address: 00: 18: ba: d8: 4c: 3d
Vdc policy ha: RESET
Vdc id: 2
Vdc name: Datos
Status vdc: active
Vdc mac address: 00: 18: ba: d8: 4c: 3e
Policy vdc ha: BRINGDOWN

ESSALUD-N7K9-COREB # conf
ESSALUD-N7K9-COREB (config) # vdc Imagenes
ESSALUD-N7K9-COREB (config-vdc) # show vdc
    
```



Vdc_id vdc_name mac state

Reba_Sgh_Imagenes

1 active ESSALUD-N7K9-COREB 00: 13: ca: e8: 2c: 2d

2 active Imagenes 00: 17: aa: d7: 3c: 1e

ESSALUD-N7K9-COREB (config-vdc) # show vdc detail

Vdc id: 1

Vdc name: change

Status vdc: active

Vdc mac address: 00: 13: ca: e8: 2c: 2d

Vdc policy ha: RESET

Vdc id: 2

Vdc name: Imagenes

Status vdc: active

Vdc mac address: 00: 17: aa: d7: 3c: 1e

Policy vdc ha: BRINGDOWN

ESSALUD-N7K9-COREB # conf

ESSALUD-N7K9-COREB (config) # vdc Impresoras

ESSALUD-N7K9-COREB (config-vdc) # show vdc

Vdc_id vdc_name mac state

Reba_Sgh_Impresoras

1 active ESSALUD-N7K9-COREB 00: 13: ab: a7: 3b: 2b

2 active Impresoras 00: 12: ca: a8: 1c: 2a

ESSALUD-N7K9-COREB (config-vdc) # show vdc detail

Vdc id: 1

Vdc name: change

Status vdc: active

Vdc mac address: 00: 13: ab: a7: 3b: 2b

Vdc policy ha: RESET

Vdc id: 2

Vdc name: Impresoras

Status vdc: active



```

Vdc mac address: 00: 12: ca: a8: 1c: 2a
Policy vdc ha: BRINGDOWN

ESSALUD-N7K9-COREB # conf
ESSALUD-N7K9-COREB (config) # vdc Voz
ESSALUD-N7K9-COREB (config-vdc) # show vdc
Vdc_id vdc_name mac state
Reba_Sgh_Voz
1 active ESSALUD-N7K9-COREB 00: 11: cb: e7: 5c: 4d
2 active Voz 00: 12: ca: a8: 1c: 2a
ESSALUD-N7K9-COREB (config-vdc) # show vdc detail
Vdc id: 1
Vdc name: change
Status vdc: active
Vdc mac address: 00: 11: cb: e7: 5c: 4d
Vdc policy ha: RESET
Vdc id: 2
Vdc name: Impresoras
Status vdc: active
Vdc mac address: 00: 12: ca: a8: 1c: 2a
Policy vdc ha: BRINGDOWN
    
```

Quando se ha creado el VDC, el sistema lo coloca en el modo de configuración VDC, donde pueden asignarse otras opciones de configuración al VDC.

Un conjunto predeterminado de instrucciones de configuración se asigna al VDC cuando se crea como se puede ver en la siguiente salida:

```

ESSALUD-N7K9-COREB # show run | Start vcc
<Snip>
Datos id vdc 2
    
```



Default template

Hap bringdown

Resource limit vlan minimum 16 maximum 4094

Limit-resource span-ssn min 0 max 2

Resource limit vrf minimum 16 maximum 8192

Limit-port-channel resource minimum 0 maximum 256

Limit-resource glbp_group min 0 max 4096

<Snip>

ESSALUD-N7K9-COREB # show run | Start vcc

<Snip>

Imagenes id vdc 2

Default template

Hap bringdown

Resource limit vlan minimum 16 maximum 4094

Limit-resource span-ssn min 0 max 2

Resource limit vrf minimum 16 maximum 8192

Limit-port-channel resource minimum 0 maximum 256

Limit-resource glbp_group min 0 max 4096

<Snip>

ESSALUD-N7K9-COREB # show run | Start vcc

<Snip>

Impresoras id vdc 2

Default template

Hap bringdown

Resource limit vlan minimum 16 maximum 4094

Limit-resource span-ssn min 0 max 2

Resource limit vrf minimum 16 maximum 8192

Limit-port-channel resource minimum 0 maximum 256

Limit-resource glbp_group min 0 max 4096

<Snip>



```

ESSALUD-N7K9-COREB # show run | Start vcc
<Snip>
Voz id vdc 2
Default template
Hap bringdown
Resource limit vlan minimum 16 maximum 4094
Limit-resource span-ssn min 0 max 2
Resource limit vrf minimum 16 maximum 8192
Limit-port-channel resource minimum 0 maximum 256
Limit-resource glbp_group min 0 max 4096
<Snip>
    
```

Estas instrucciones de configuración proporcionan una definición sobre el consumo de recursos en el que el VDC puede trabajar.

Estos recursos incluyen VLAN, VRF, SPAN, PortChannels e ID de grupo GLBP. Sin embargo, las asignaciones de límite de recursos se pueden cambiar a través de la línea de comandos. Un ejemplo de cómo se cambia un límite de recursos se muestra aquí:

```

ESSALUD-N7K9-COREB (config) # vdc Datos
ESSALUD-N7K9-COREB (config-vdc) # limit-resource vlan minimum 32
maximum 4094
ESSALUD-N7K9-COREB (config-vdc) # show run | Start vcc
<Snip>
Vdc Datos ID 2
Preset template
Bringdown hap
Resource limit VLAN minimum 32 maximum 4094
Span of SSN sets minimum resource limit 0 Maximum value of 2
Resource limit VRF minimum 16 maximum 8192
Limit-resource of the minimum channel port 0 maximum 256
Resource limit glbp_group minimum 0 maximum 4096
    
```



<Snip>

ESSALUD-N7K9-COREB (config) # vdc Imagenes

ESSALUD-N7K9-COREB (config-vdc) # limit-resource vlan minimum 32
maximum 4094

ESSALUD-N7K9-COREB (config-vdc) # show run | Start vcc

<Snip>

Vdc Imagenes ID 2

Preset template

Bringdown hap

Resource limit VLAN minimum 32 maximum 4094

Span of SSN sets minimum resource limit 0 Maximum value of 2

Resource limit VRF minimum 16 maximum 8192

Limit-resource of the minimum channel port 0 maximum 256

Resource limit glbp_group minimum 0 maximum 4096

<Snip>

ESSALUD-N7K9-COREB (config) # vdc Impresoras

ESSALUD-N7K9-COREB (config-vdc) # limit-resource vlan minimum 32
maximum 4094

ESSALUD-N7K9-COREB (config-vdc) # show run | Start vcc

<Snip>

Vdc Impresoras ID 2

Preset template

Bringdown hap

Resource limit VLAN minimum 32 maximum 4094

Span of SSN sets minimum resource limit 0 Maximum value of 2

Resource limit VRF minimum 16 maximum 8192

Limit-resource of the minimum channel port 0 maximum 256

Resource limit glbp_group minimum 0 maximum 4096

<Snip>

ESSALUD-N7K9-COREB (config) # vdc Voz



```

ESSALUD-N7K9-COREB (config-vdc) # limit-resource vlan minimum 32
maximum 4094
ESSALUD-N7K9-COREB (config-vdc) # show run | Start vcc
<Snip>
Vdc Voz ID 2
Preset template
Bringdown hap
Resource limit VLAN minimum 32 maximum 4094
Span of SSN sets minimum resource limit 0 Maximum value of 2
Resource limit VRF minimum 16 maximum 8192
Limit-resource of the minimum channel port 0 maximum 256
Resource limit glbp_group minimum 0 maximum 4096
<Snip>
    
```

Este ejemplo muestra cómo se cambia el número mínimo de VLAN para la producción VDC de 16 a 32. El uso de plantillas de recursos proporciona un método alternativo para asignar recursos a una VCC. La configuración de una plantilla de recursos se realiza en el modo de configuración como se muestra en el siguiente ejemplo.

```

ESSALUD-N7K9-COREB (config)#VDC resource template n7000switch
ESSALUD-N7K9-COREB (config-VDC-template) # resource limit VLAN
minimum 32 maximum 256
ESSALUD-N7K9-COREB (config-VDC-template) # resource limit VRF
minimum 32 maximum 64
ESSALUD-N7K9-COREB (config-VDC-template) # exit
    
```

Una vez creada la plantilla de recursos que puede ser asignada a la VDC como se muestra en el siguiente ejemplo.

```

ESSALUD-N7K9-COREB (config) # VDC 2 Template n7000switch
ESSALUD-N7K9-COREB (config-VDC) # show VDC resource template
    
```



Template: n7000switch

essalud.gob.pe

Min Max Features

VRF 32 64

VLAN 32 256

:: template by default

Essalud.gob.pe

Min Max Features

Glbp_group 0 4096

Port channel 0 256

Datos-SSN 0 2

VLAN 16 4094

VRF 16 8192

ESSALUD-N7K9-COREB (config-VDC) #

Una vez creado el VDC, el administrador se coloca en el modo de configuración VDC.

La siguiente tarea es asignar los puertos físicos a este VDC. Puertos de las tarjetas de línea física no se pueden compartir entre diferentes CDA.

Por defecto, todos los puertos físicos pertenecen al VDC por defecto. Cuando se crea un VCC, los puertos pueden ser colocados bajo el control de este VDC usando la opción CLI siguiente:

ESSALUD-N7K9-COREB (config) # VDC member show

Vdc_id: 1 vdc_name: switch interfaces:

Ethernet3 / 1 Ethernet3 / 2 Ethernet3 / 3

Ethernet3 / 4 Ethernet3 / 5 Ethernet3 / 6

Ethernet3 / 7 Ethernet3 / 8 Ethernet3 / 9



Ethernet3 / 10 Ethernet3 / 11 Ethernet3 / 12
Ethernet3 / 13 Ethernet3 / 14 Ethernet3 / 15
Ethernet3 / 16 Ethernet3 / 17 Ethernet3 / 1
Ethernet3 / 19 Ethernet3 / 20 Ethernet3 / 21
Ethernet3 / 22 Ethernet3 / 23 Ethernet3 / 24
Ethernet3 / 25 Ethernet3 / 26 Ethernet3 / 27
Ethernet3 / 28 ethernet3 / 29 ethernet3 / 30
Ethernet3 / 31 Ethernet3 / 32 Ethernet3 / 33
Ethernet3 / 34 Ethernet3 / 35 Ethernet3 / 36
Ethernet3 / 37 Ethernet3 / 38 Ethernet3 / 39
Ethernet3 / 40 Ethernet3 / 41 Ethernet3 / 42
Ethernet3 / 43 Ethernet3 / 44 Ethernet3 / 45
Ethernet3 / 46 ethernet3 / 47 ethernet3 / 48

Vdc_id: 2 vdc_name: datos interfaces:

ESSALUD-N7K9-COREB (config) # VDC output

ESSALUD-N7K9-COREB (config-VDC) # assign Ethernet interface 3/48

ESSALUD-N7K9-COREB (config-VDC) # VDC member show

Vdc_id: 1 vdc_name: switch interfaces:

Ethernet3 / 1 Ethernet3 / 2 Ethernet3 / 3
Ethernet3 / 4 Ethernet3 / 5 Ethernet3 / 6
Ethernet3 / 7 Ethernet3 / 8 Ethernet3 / 9
Ethernet3 / 10 Ethernet3 / 11 Ethernet3 / 12
Ethernet3 / 13 Ethernet3 / 14 Ethernet3 / 15
Ethernet 3/16 Ethernet3 / 17 Ethernet3 / 18
Ethernet3 / 19 Ethernet3 / 20 Ethernet3 / 21
Ethernet3 / 22 Ethernet3 / 23 Ethernet3 / 24
Ethernet3 / 25 Ethernet3 / 26 Ethernet3 / 27
Ethernet3 / 28 ethernet3 / 29 ethernet3 / 30
Ethernet 3/31 Ethernet3 / 32 Ethernet3 / 33
Ethernet3 / 34 Ethernet3 / 35 Ethernet3 / 36
Ethernet3 / 37 Ethernet3 / 38 Ethernet3 / 39
Ethernet3 / 40 Ethernet3 / 41 Ethernet3 / 42



Ethernet3 / 43 Ethernet3 / 44 Ethernet3 / 45

Ethernet3 / 46 ethernet3 / 47

Vdc_id: 2 vdc_name: datos interfaces:

Ethernet3 / 48

El ejemplo anterior muestra cómo un puerto físico (Ethernet 3/48) se mueve bajo el control de la producción VDC.

Además, configuración de este y otros puertos que están asignados a esta VDC ahora debe ser completado dentro de la producción VDC.

En el Gráfico N°61 muestra la configuración de la separación tradicional de firewall con VLANs.

El Gráfico N°56 muestra la configuración de despliegue para los VDC con un cortafuego.

En el ejemplo VDC, se han creado dos VDC y, en total, tres VDC están en uso.

El VDC predeterminado, que existe en el sistema desde el arranque inicial, se utiliza para crear dos VDC adicionales.

Una vez creados los dos VDC adicionales, el VDC predeterminado actúa como VDC administrativo para todos los demás VDC.

Debido a los poderes administrativos generales asociados con el VDC administrativo, el VDC administrativo debe reservarse estrictamente para la administración de VDC en ambientes de alta seguridad.

Los dos VDC adicionales creados se utilizan para las áreas de seguridad "limpias" y "sucias" (es decir, dentro y fuera) de la infraestructura de firewall.

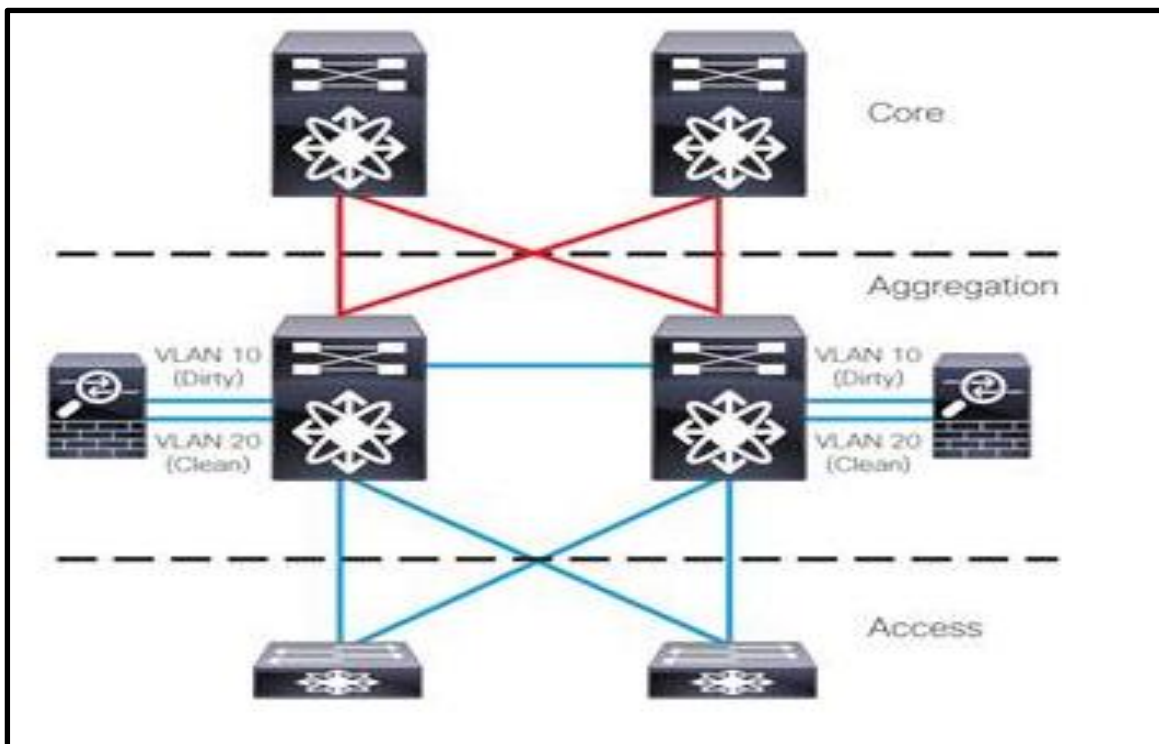


Figura 85. Traditional Firewall Separation with VDC'S. Fuente: Cisco (2014).

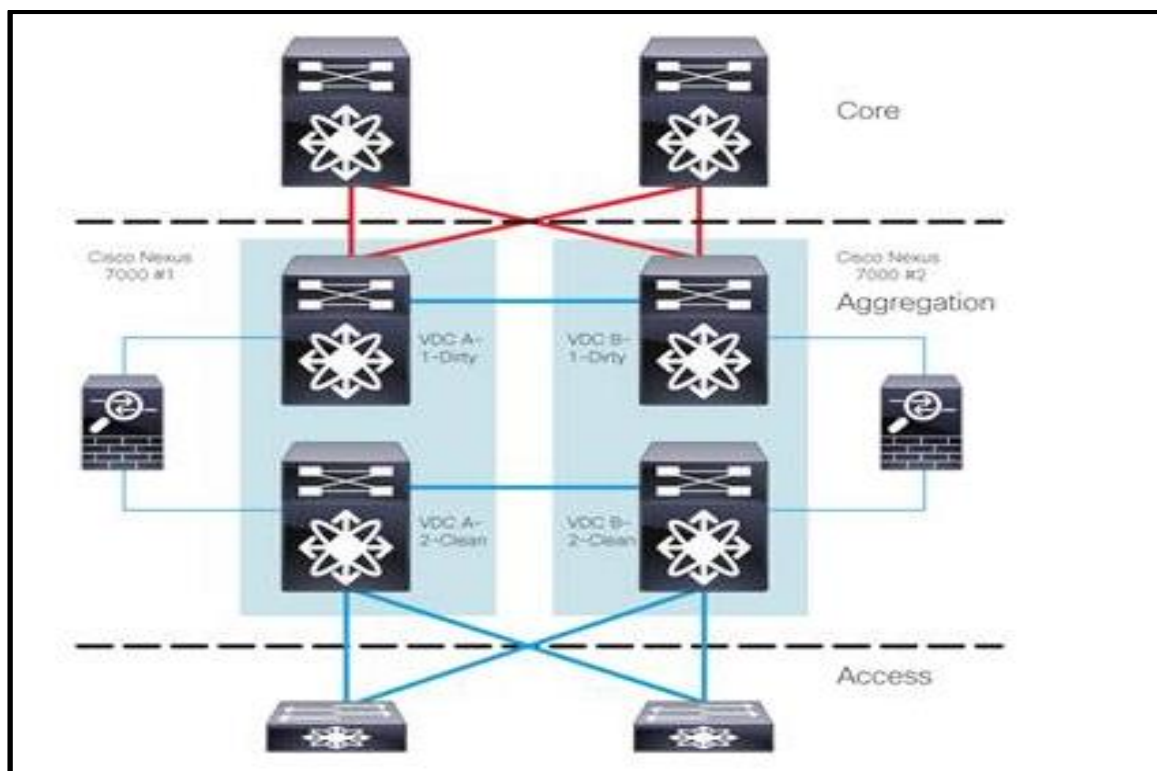


Figura 86. Enhanced Firewall Separation with VDC'S. Fuente: Cisco (2014).



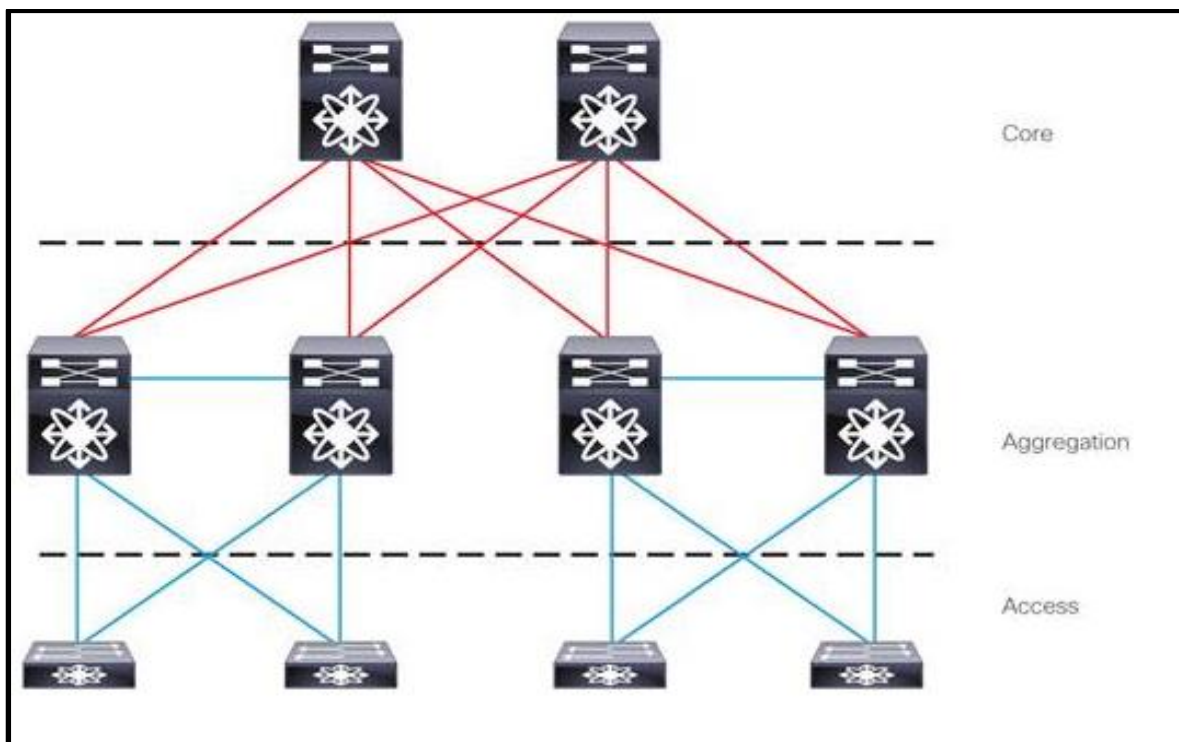


Figura 87. Typical Physical Topology. Fuente: Cisco (2014).

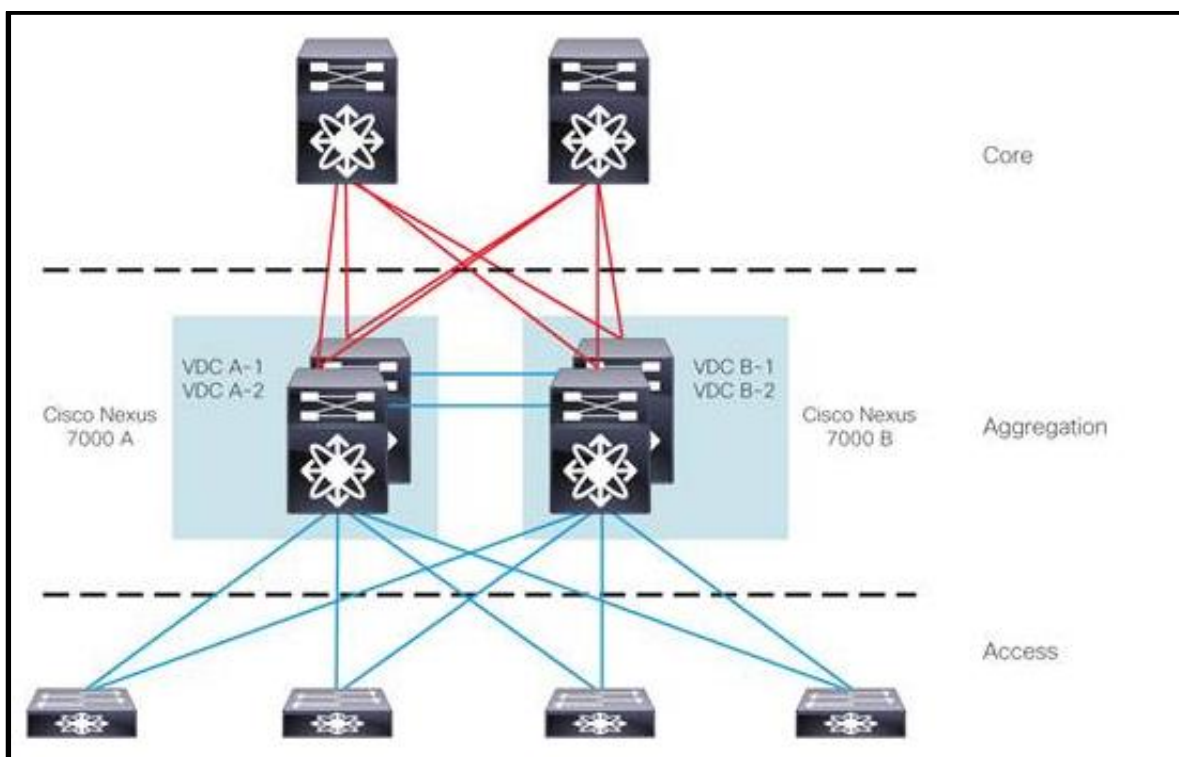


Figura 88. Horizontal Consolidation With VDC'S. Fuente: Cisco (2014).



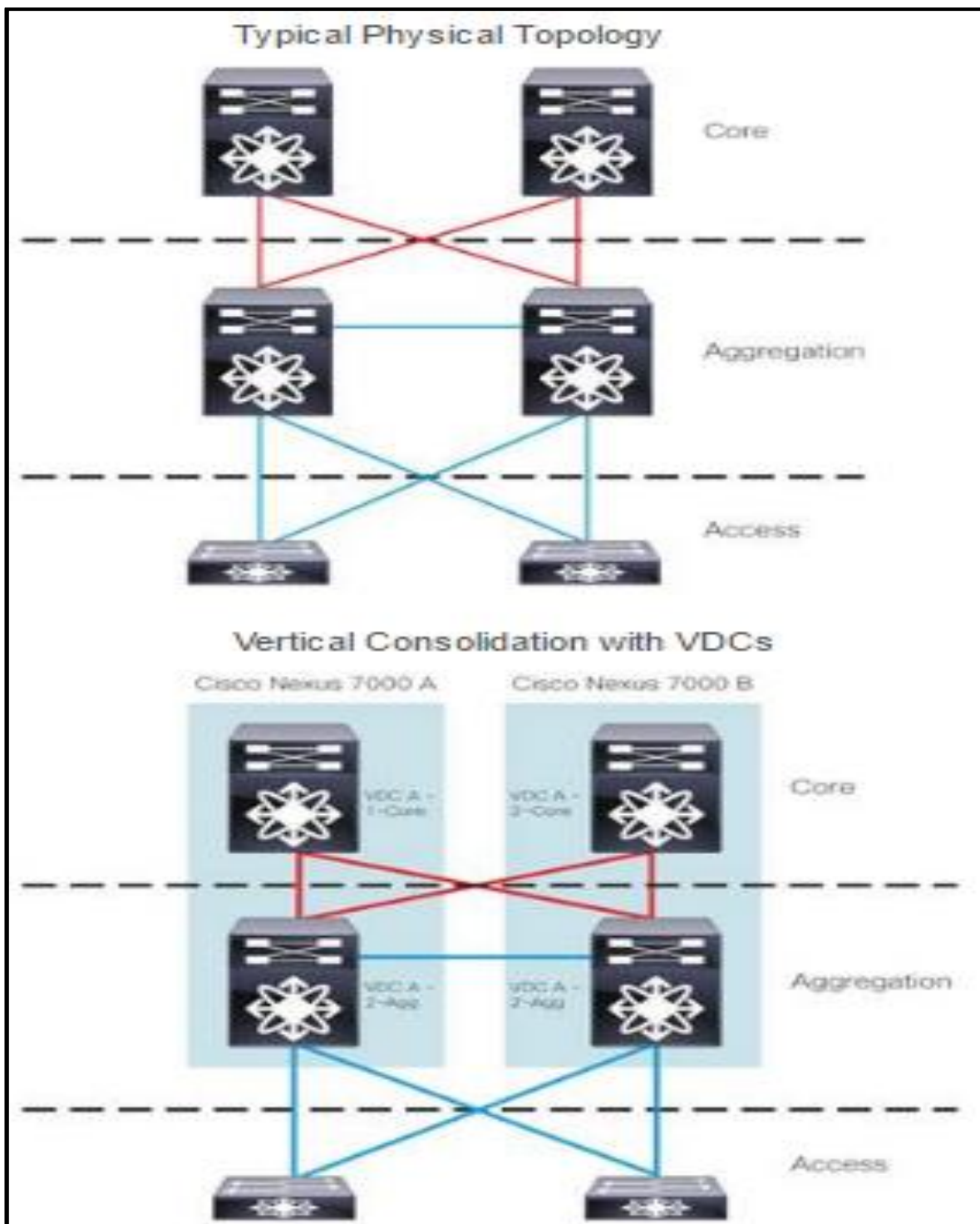


Figura 89. Both Typical and Vertical with VDC'S. Fuente: Cisco (2014).

Finalmente, después de ver los comandos de los VDC. Podemos configurarlo en el Software Emulador GNS3, podremos observar cómo se virtualizan los Nexus 7000 de Cisco propuestos para el HNERM-EsSALUD.



5.4. FASE 4: IMPLEMENTACIÓN (LifeCycle Services)

En esta fase se realizarán la implementación y puesta en práctica de los entregables.

5.4.1. Recepción e inspección

Recepción e Inspección se refiere a la verificación de la conformidad del trabajo de acuerdo al pedido definido en la fase de diseño validado.

Esta etapa se realiza de acuerdo con la **Fase de Diseño**, un compilado de documentos que estipula la forma en que debe inspeccionarse el trabajo.

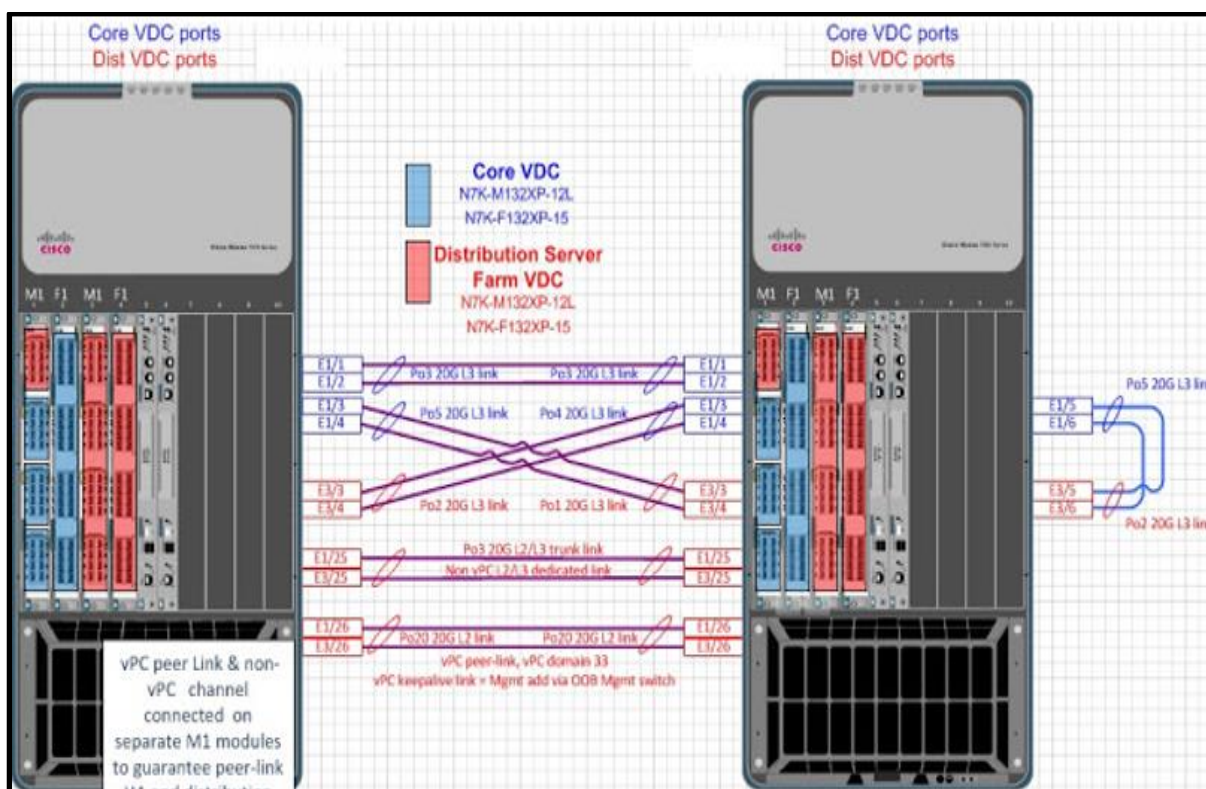


Figura 90. Arquitectura de los VDC'S de los Switches Nexus 7000. Fuente: Cisco (2016).



5.4.2. Prueba

La prueba consiste en la verificación de conformidad de los entregables con respecto a las especificaciones que se definieron.

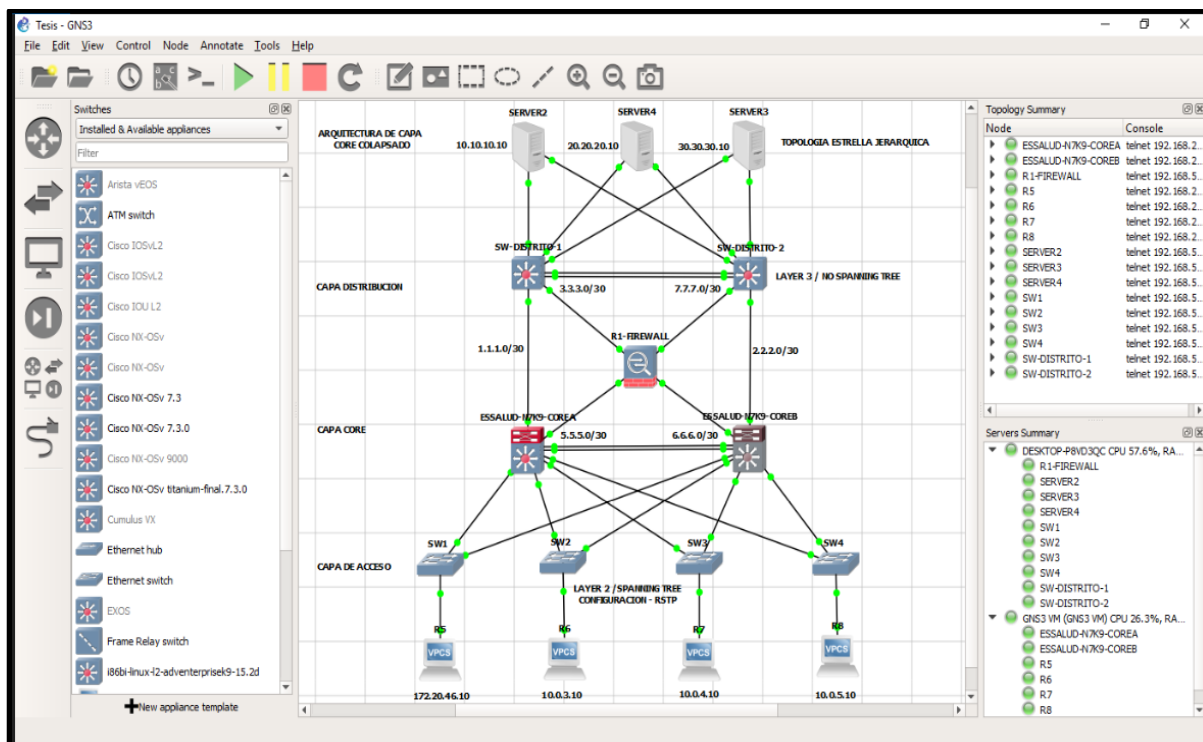


Figura 91: Virtualizando los Conmutadores Nexus 7000 en el Emulador GNS3. Fuente: Elaboración Propia (2018).

Una vez tenemos casi todo construido procedemos a empezar a verificar si lo que implementamos funciona, para posteriormente hacerle los ajustes necesarios.

Entonces pusimos en práctica nuestros entregables que son los documentos que permiten estandarizar actividades de la Red LAN del HNERM-EsSALUD.

Estos han sido desarrollados en la Etapa de Diseño y una herramienta usada para tal fin el Fluke Network con el fin de monitorear el tráfico de la Red LAN.



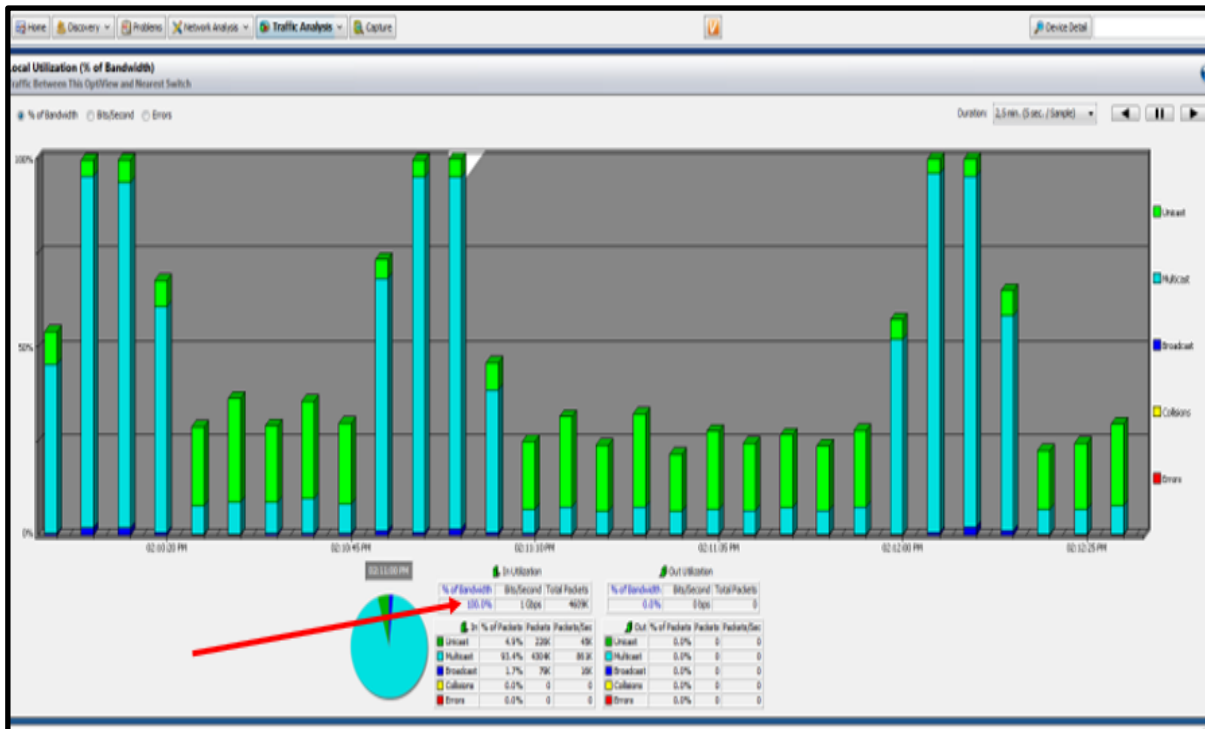


Figura 92. Generación de Inactividad Core Principal HNERM 16/08/2016 Unicast, Multicast, Broadcast, Ancho de Banda, Bps y Packets. Fuente: OptiView Fluke Networks Ref. Tabla 8 Caída 9, Resultado de Tráfico del Ancho de Banda al 100% Antes (2016).

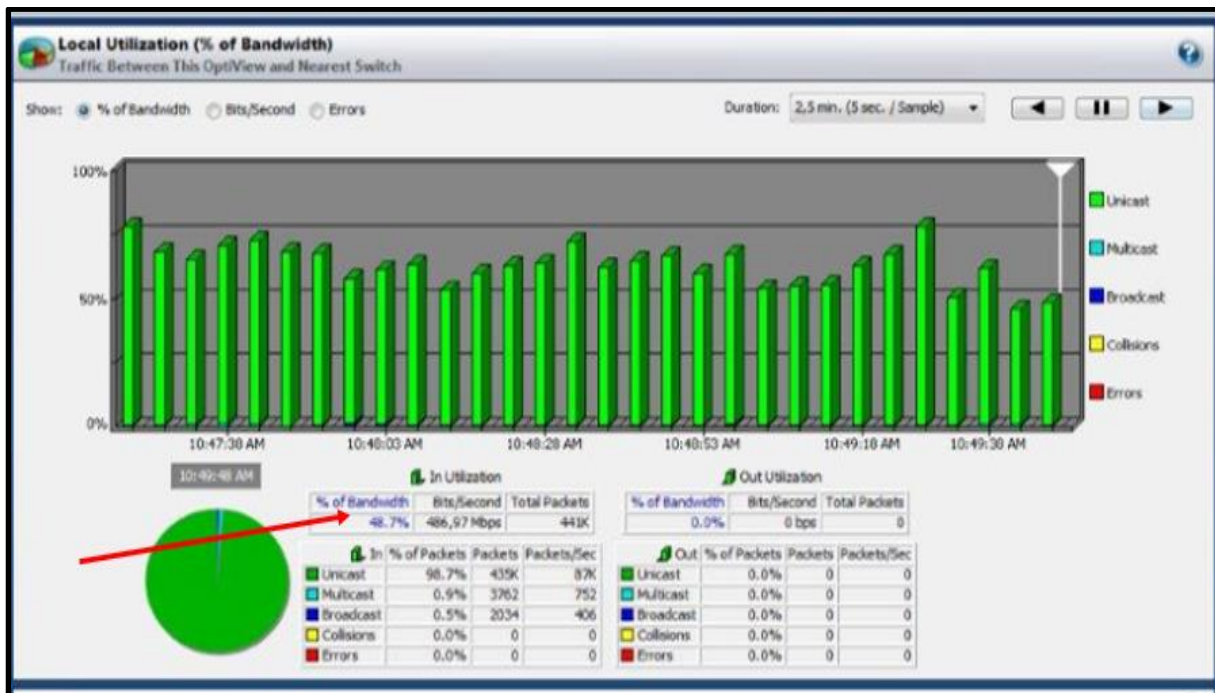


Figura 93. Generación de Inactividad Core Principal HNERM 01/12/2017 Unicast, Multicast, Broadcast, Ancho de Banda, Bps y Packets. Fuente: OptiView Fluke Networks Ref. Tabla 8, Resultado de Tráfico del Ancho de Banda al 48.7% Después (2017).



5.4.3. Documentos Elaborados

En el caso de los documentos que son Políticas de seguridad y Planes de contingencia en un principio por la inexperiencia hubo varios errores que nos comunicó el administrador de Red del HNERM-EsSALUD, posteriormente con las correcciones hechas y quizá con algunas faltantes se logró los documentos acordes y coherentes (**Etapa de Diseño**) que han sido y serán de mucha ayuda para la administración de Red LAN del HNERM-EsSALUD.

Son estos documentos tan importantes con los que no contaba la Red informática del HNERM-EsSALUD.

5.4.4. Aplicación

Y para el caso de la puesta en marcha y pruebas de la virtualización, como era de esperarse se ha tenido que lidiar con muchos errores, propios de una primera fase de pruebas, se tuvo que revisar las configuraciones y los requerimientos, la virtualización no ha sido sencilla desarrollarla ya que requirió de mucha investigación dado que hay poca experiencia en nuestro medio para trabajar con este tipo de Conmutadores Nexus 7000 de Cisco, sin embargo se pudo desarrollar usando los Virtual Devices Context.



Figura 94. Emulador GNS3. Fuente: <https://gns3.com/> (2018).

Al final se logró lo que queríamos Emular dicho conmutador el cual nos muestre la información precisa y puntual del performance de la Red LAN en todos los servicios del HNERM-EsSALUD.

Ejecutaremos las configuraciones requeridas para la virtualización de los dispositivos de conmutación Nexus 7000 propuestos al HNERM-EsSALUD, utilizando el Emulador GNS3.

Minimum Requirements	
OS	Windows 7 (64 bit) and later, Mavericks (10.9) and later, Any Linux Distro - Debian/Ubuntu are provided and supported
Processor	2 or more Logical cores - AMD-V / RVI Series or Intel VT-X / EPT - virtualization extensions present and enabled in the BIOS. More resources allows for larger simulation
Memory	4 GB RAM
Storage	1 GB available space (Windows Installation is < 200MB)
Additional Notes	More storage is needed for OS and Device Images.
Recommended Requirements	
OS	Windows 7 (64 bit) and later, Mavericks (10.9) and later, Any Linux Distro - Debian/Ubuntu are provided and supported
Processor	4 or more Logical cores - AMD-V / RVI Series or Intel VT-X / EPT - virtualization extensions present and enabled in the BIOS. More resources allows for larger simulation
Memory	8 GB RAM
Storage	SSD - 35 GB available space
Additional Notes	Additional RAM up to 16 gigs and i7 or equivalent for optimal usage. Virtualizing devices is processor and memory intensive. More is better but properly configured device trumps RAM and Processing power.

Figura 95. Requerimientos Mínimos para uso del Emulador GNS3. Fuente: <https://gns3.com/> (2018).



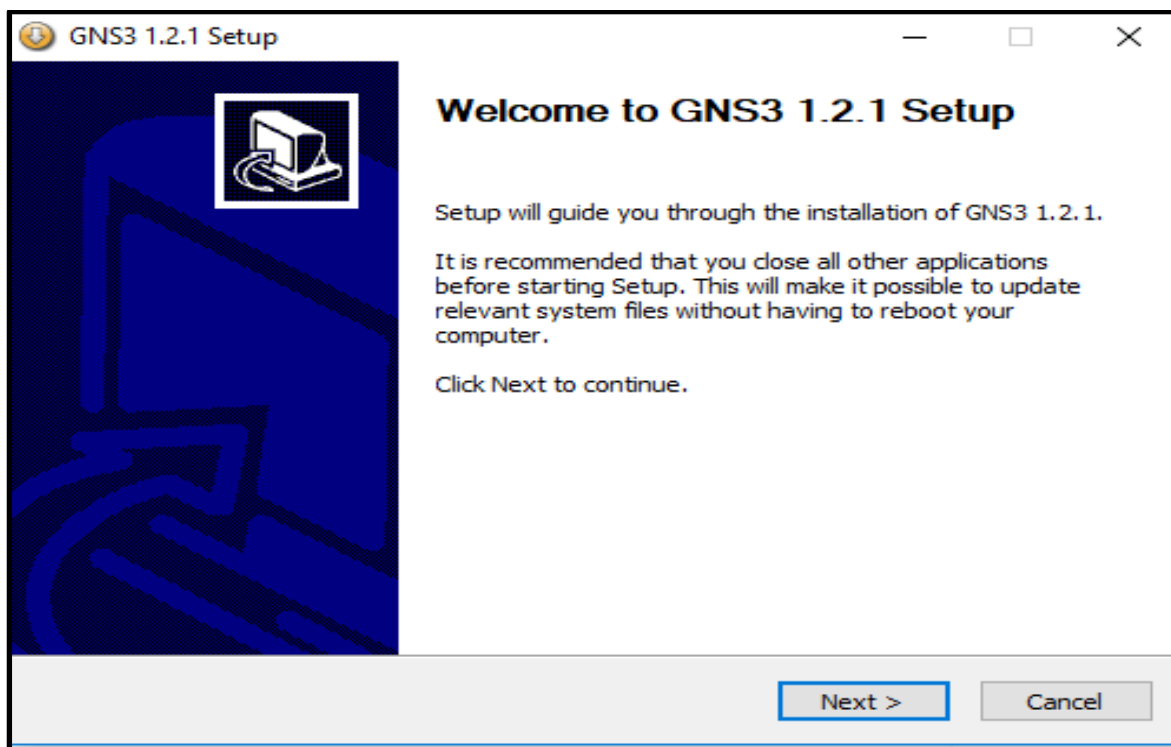


Figura 96. Instalación del Emulador GNS3. Fuente: <https://gns3.com/> (2018).

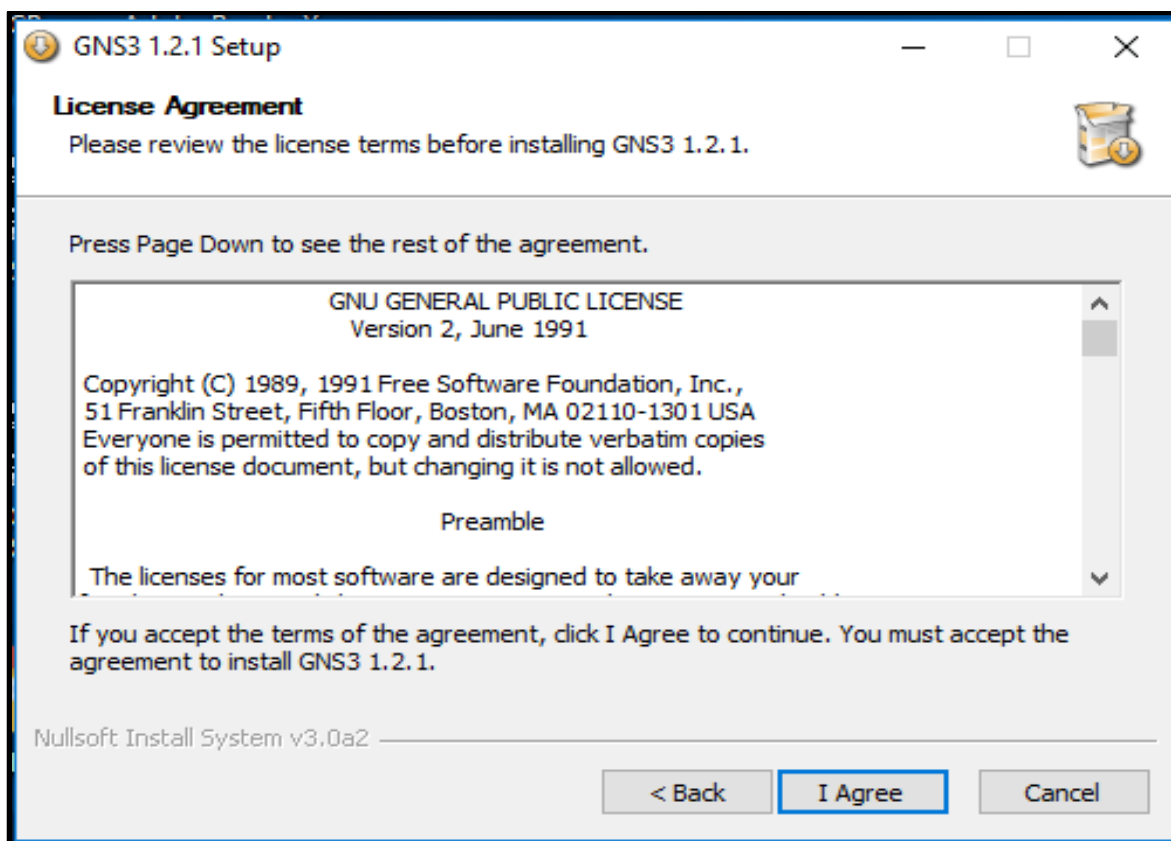


Figura 97. Instalación del Emulador GNS3. Fuente: <https://gns3.com/> (2018).



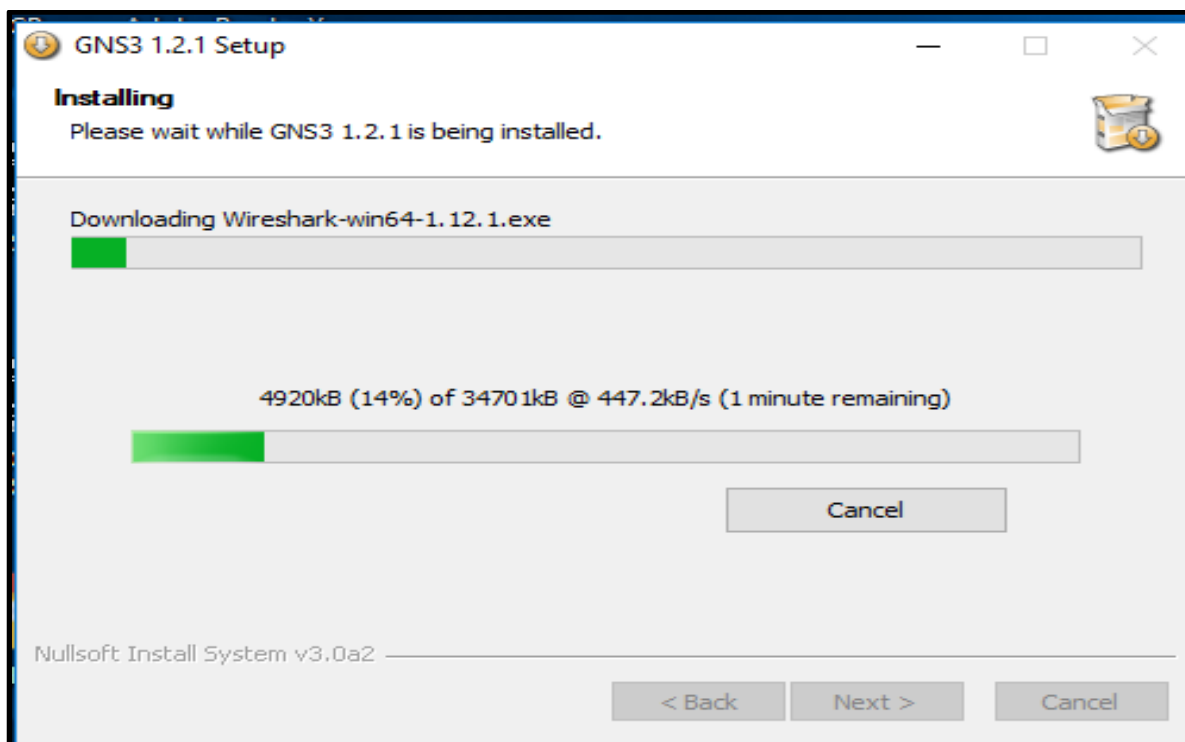


Figura 98. Instalación del Emulador GNS3. Fuente: <https://gns3.com/> (2018).

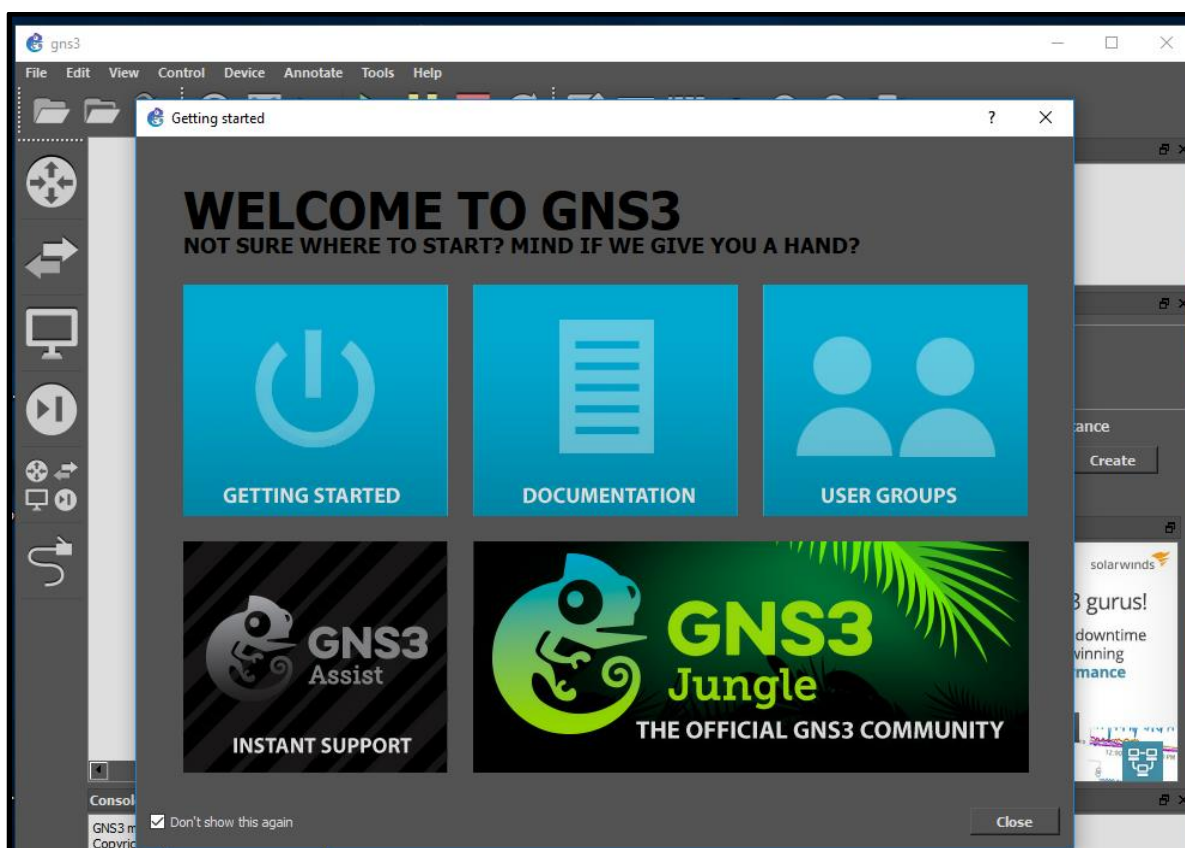


Figura 99. Ingresando al Entorno del Emulador GNS3. Fuente: <https://gns3.com/> (2018).



5.5. FASE 5: OPERACIÓN (LifeCycle)

En la fase de Operación de la red LAN en el HNERM-EsSALUD, nos ayuda a mejorar la disponibilidad de la red, a reducir los riesgos de seguridad y a disminuir el tiempo de caída de los diferentes sistemas que corren aplicaciones de misión crítica, así como también:

- a. Solución rápida de problemas a través de nuestros Planes de contingencia.
- b. Acceso autorizado a herramientas e información y recursos de la red, esto se estableció con las Políticas de Seguridad (Fase III Diseño).
- c. Reemplazo rápido de hardware según sea requerido, mediante un monitoreo con nuestra aplicación se puede determinar de manera más rápida de donde venían los problemas.
- d. Actualizaciones periódicas del software Emulador GNS3, lo que permite que la red se adapte más fácilmente a las necesidades cambiantes, y que está indicado en nuestros planes de contingencia.

Cronograma de Actividades

Tabla 33

Cuadro de Cronograma de las Fases, Actividades, Avance y Fechas

FASE	ACTIVIDADES	AVANCE	FECHA
I	Diagnóstico de la Red LAN (cuarto de equipos, cuartos de comunicaciones, áreas de trabajo y equipos intermedios).	100%	01/01/2016
II	Migración del CORE OmniSwitch 9700 al 9800.	100%	22/07/2016
III	Capacitación al personal del Área de Comunicaciones de esta Oficina en configuración de equipos intermedios, por parte de la Sede Central.	100%	01/08/2016
IV	Identificación de conexiones de puntos de Voz, Data, Video, Equipos Biomédicos, etc.	100%	10/11/2016
V	Limpieza y Mantenimiento de gabinetes y equipos intermedios.	85%	04/02/2017
VI	Redistribución de equipos intermedios.	50%	20/03/2017
VII	Migración de Direcciones IP, y segmentación de VLAN	90%	13/04/2017
VIII	Migración del CORE OmniSwitch 9800 al conmutador Core Nexus 7000	100%	30/06/2017

Fuente: Elaboración Propia Año (2017).



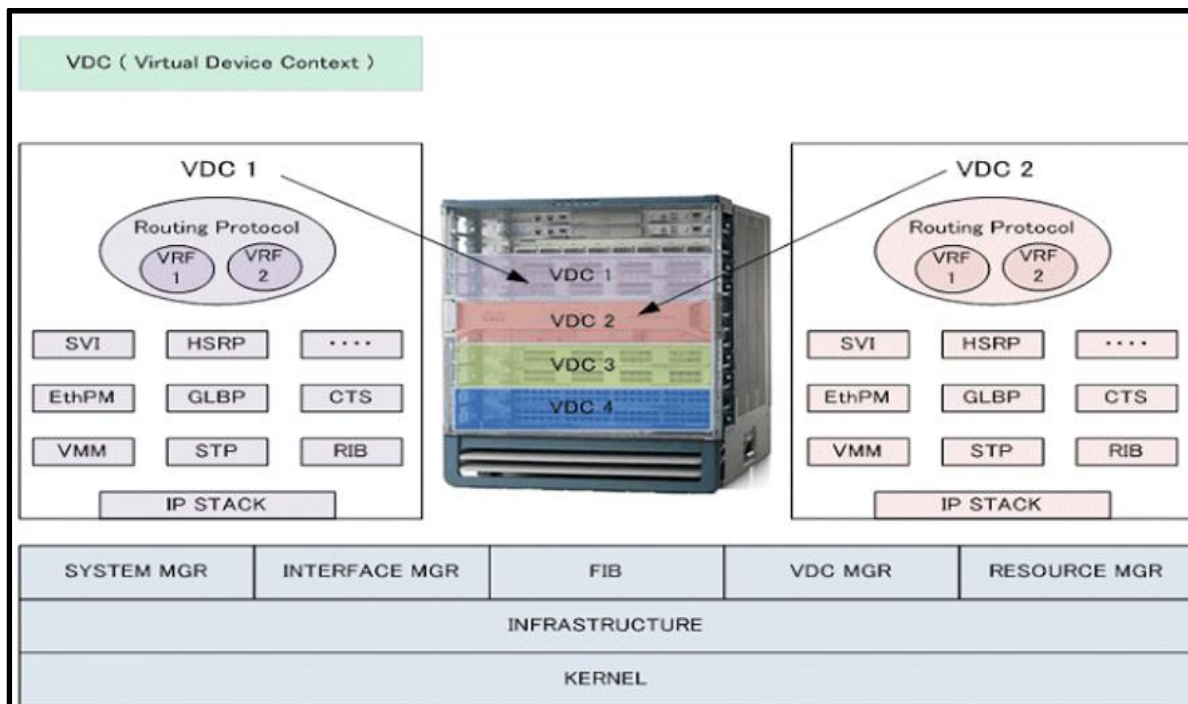


Figura 100. Chassis del Switch Nexus 7000. Fuente: Cisco (2016).

Se realizaron 2 tipos de operaciones o 2 etapas que se mencionan a continuación:

- a. Monitoreo Proactivo y administración de la red para maximizar su desempeño, capacidad, disponibilidad, confiabilidad y seguridad.



VLAN	SEGMENTO DE RED	SERVICIOS	PERFORMANCE	N° EQUIPOS CONECTADOS
1	172.22.40.0 /24	DATOS, VIDEO, IMPRESIÓN, IMÁGENES RX	96%	150
1	172.22.41.0 /24	DATOS, VIDEO, IMPRESIÓN, IMÁGENES RX	96%	150
1	172.22.42.0 /24	DATOS, VIDEO, IMPRESIÓN, IMÁGENES RX	96%	133
1	172.22.43.0 /24	DATOS, VIDEO, IMPRESIÓN, IMÁGENES RX	96%	162
1	172.22.44.0 /24	DATOS, VIDEO, IMPRESIÓN, IMÁGENES RX	96%	142
1	172.22.46.0 /24	DATOS, VIDEO, IMPRESIÓN, IMÁGENES RX	96%	150
1	172.22.47.0 /24	DATOS, VIDEO, IMPRESIÓN, IMÁGENES RX	96%	140
1	172.22.48.0 /24	ADMINISTRACIÓN	1%	15
1	172.22.49.0 /24	DATOS, VIDEO, IMPRESIÓN, IMÁGENES RX	96%	145
1	172.29.120.0 /24	VOZ IP	3%	40
				1227

Figura 101. Reporte del Performance de la Red LAN del HNERM EsSALUD anterior al 2016. Fuente: Elaboración propia (2017).

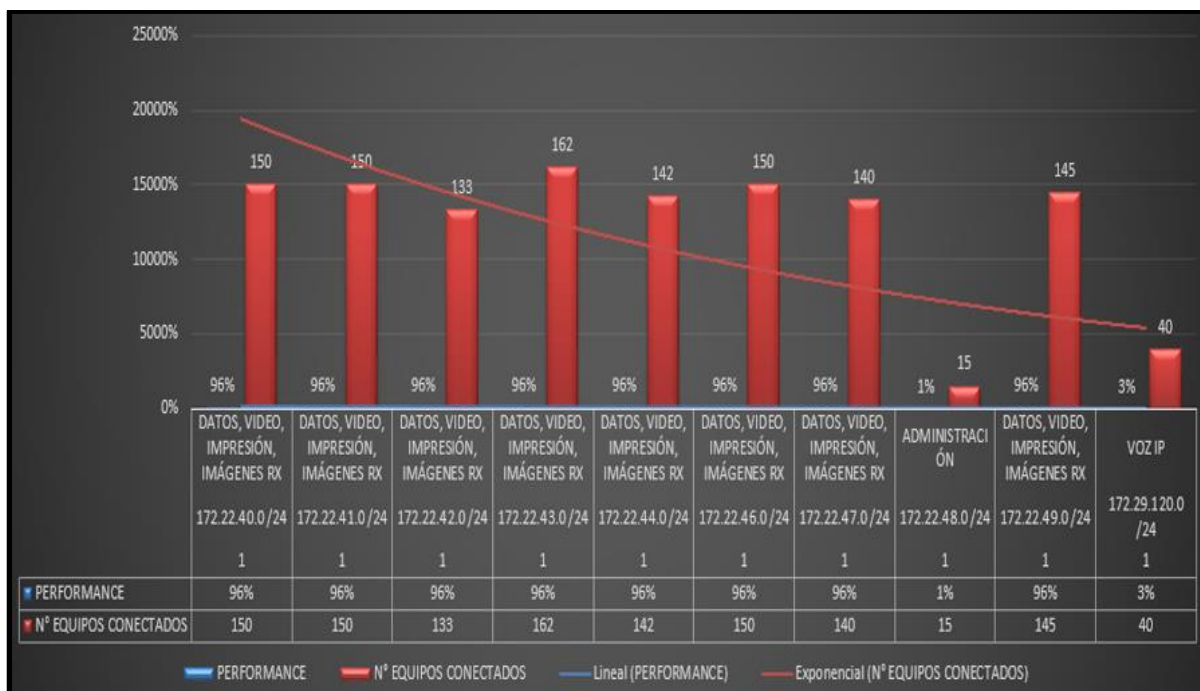


Figura 102. Gráfico del Performance de la Red LAN del HNERM EsSALUD anterior al 2016. Fuente: Elaboración propia (2017).



VLAN	SEGMENTO DE RED	SERVICIOS	PERFORMANCE	N° EQUIPOS CONECTADOS					
100	10.1.6.0 /23	Datos_Gab_A	46.3%	50	211	10.1.48.0 /25	Voz_Gab_B	55.5%	60
101	10.1.8.0 /24	Voz_Gab_A	27.8%	30	212	10.1.46.128 /27	Impresoras_Gab_B	27.8%	30
102	10.1.9.0 /26	Impresoras_Gab_A	18.5%	20	220	10.1.47.0 /24	Datos_Gab_D	11.1%	12
110	10.1.10.0 /23	Datos_Gab_C	55.5%	60	221	10.1.48.0 /25	Voz_Gab_D	37.0%	40
111	10.1.12.0 /24	Voz_Gab_C	27.8%	30	222	10.1.48.128 /27	Impresoras_Gab_D	8.3%	9
112	10.1.13.0 /26	Impresoras_Gab_C	18.5%	20	230	10.1.49.0 /24	Datos_Gab_G3	37.9%	41
120	10.1.14.0 /23	Datos_Gab_B3	44.4%	48	231	10.1.50.0 /25	Voz_Gab_G3	28.7%	31
121	10.1.16.0 /24	Voz_Gab_B3	22.2%	24	232	10.1.50.128 /27	Impresoras_Gab_G3	10.2%	11
122	10.1.17.0 /26	Impresoras_Gab_B3	11.1%	12	240	10.1.51.0 /24	Datos_Gab_J	55.5%	60
130	10.1.18.0 /23	Datos_Gab_A1	48.1%	52	241	10.1.52.0 /25	Voz_Gab_J	46.3%	50
131	10.1.20.0 /24	Voz_Gab_A1	9.3%	10	242	10.1.52.128 /27	Impresoras_Gab_J	55.5%	60
132	10.1.21.0 /26	Impresoras_Gab_A1	4.6%	5	250	10.1.53.0 /24	Datos_Gab_K	48.1%	52
140	10.1.22.0 /23	Datos_Gab_C1	37.0%	40	251	10.1.54.0 /25	Voz_Gab_K	46.3%	50
141	10.1.24.0 /24	Voz_Gab_C1	18.5%	20	252	10.1.54.128 /27	Impresoras_Gab_K	11.1%	12
142	10.1.25.0 /26	Impresoras_Gab_C1	9.3%	10	260	10.1.55.0 /24	Datos_Gab_L	41.6%	45
150	10.1.26.0 /23	Datos_Gab_I1	32.4%	35	261	10.1.56.0 /25	Voz_Gab_L	23.1%	25
151	10.1.28.0 /24	Voz_Gab_I1	16.7%	18	262	10.1.56.128 /27	Impresoras_Gab_L	13.9%	15
152	10.1.29.0 /26	Impresoras_Gab_I1	8.3%	9	270	10.1.57.0 /24	Datos_Gab_N	46.3%	50
160	10.1.30.0 /23	Datos_Gab_I2	27.8%	30	271	10.1.58.0 /25	Voz_Gab_N	32.4%	35
161	10.1.32.0 /24	Voz_Gab_I2	13.9%	15	272	10.1.58.128 /27	Impresoras_Gab_N	13.9%	15
162	10.1.33.0 /26	Impresoras_Gab_I2	6.5%	7	280	10.1.59.0 /24	Datos_Gab_N	27.8%	30
170	10.1.34.0 /24	Datos_Gab_G	46.3%	50	281	10.1.60.0 /25	Voz_Gab_N	18.5%	20
171	10.1.35.0 /24	Voz_Gab_G	13.9%	15	282	10.1.60.128 /27	Impresoras_Gab_N	9.3%	10
172	10.1.36.0 /26	Impresoras_Gab_G	7.4%	8	500	10.1.2.0 /24	Camaras_vigilancia	46.3%	50
180	10.1.37.0 /24	Datos_Gab_F	46.3%	50	510	10.1.3.0 /24	Imágenes_packs	23.1%	25
181	10.1.38.0 /24	Voz_Gab_F	18.5%	20	520	10.1.4.0 /24	Equipos_medicos	27.8%	30
182	10.1.39.0 /26	Impresoras_Gab_F	9.3%	10	530	10.1.5.0 /26	Marcadores_biometricos	5.6%	6
190	10.1.40.0 /24	Datos_Gab_M	55.5%	60	540	10.1.0.0 /25	SERVIDORES DATA CENTER	29.6%	32
191	10.1.41.0 /24	Voz_Gab_M	14.8%	16	999	10.1.1.0 /24	Admin_switches	9.3%	10
192	10.1.42.0 /26	Impresoras_Gab_M	7.4%	8					
200	10.1.43.0 /24	Datos_Gab_B1	29.6%	32					
201	10.1.44.0 /25	Voz_Gab_B1	9.3%	10					
202	10.1.44.128 /27	Impresoras_Gab_B1	5.6%	6					
210	10.1.45.0 /24	Datos_Gab_B	50.9%	55					

Figura 103. Reporte del Performance de la Red LAN del HNERM EsSALUD después al 2017.
Fuente: Elaboración propia (2017).

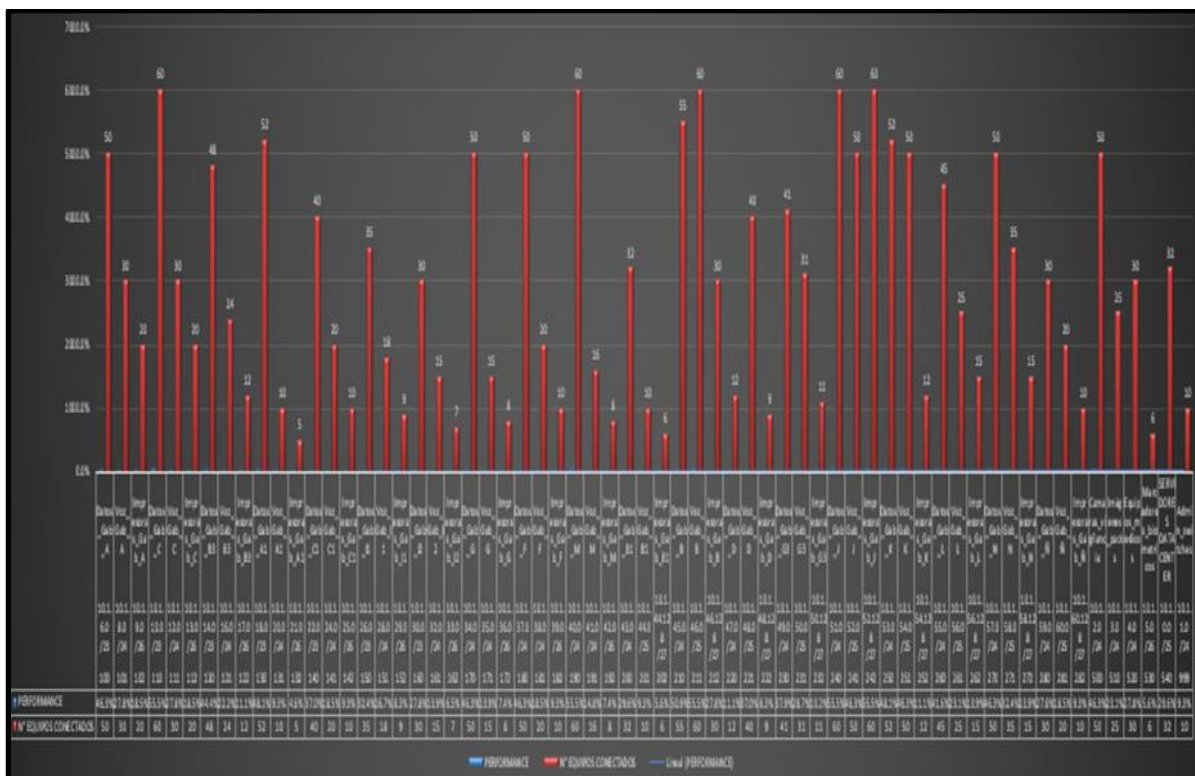


Figura 104. Gráfico del Performance de la Red LAN del HNERM EsSALUD anterior al 2016.
Fuente: Elaboración propia (2017).



b. Recursos Humanos:

Personal necesario: 2 personas encargados de la implementación, en este caso fueron los autores del proyecto quienes implementaron el sistema.

El área de Sistemas cuenta con 28 trabajadores distribuidos en sus diferentes unidades de trabajo, tal como se indica a continuación:

Tabla 34

Personal de la Oficina de Soporte Informático del HNERM EsSALUD

REGIMEN LABORAL	CARGO	CANTIDAD
728	JEFATURA	01
728	COORDINADOR	03
276	CENTRAL TELEFONICA, MESA DE AYUDA	04
728	SECRETARIA, OPERADORES DE RED	10
1057	OPERADORES DE LOS CAS	01
728	ADMINISTRADOR DE CORREOS E INTERNET	01
CAS	PROFESIONALES DE DESARROLLO	01
SERVICE	ADMINISTRADOR DE SIAD, RPM, TONER	07
TOTAL		28

Fuente: Oficina de Soporte Informático HNERM-EsSALUD (2018)



b.1. Roles Del Personal

Cargo:	PLANTILLA A33
	JEFE DE OFICINA (E4JEO)
Unidad Orgánica:	OFICINA DE SOPORTE INFORMATICO
Función Principal del Cargo:	
Planificar, organizar, dirigir, coordinar y controlar las actividades de la Oficina a fin de brindar el apoyo necesario para la adecuada prestación de los servicios de salud.	
Funciones Específicas del Cargo:	
<ol style="list-style-type: none"> 1. Programar, coordinar, controlar y evaluar la gestión de la Oficina a su cargo e impartir las disposiciones pertinentes. 2. Implementar las normas, procedimientos, metodologías y pautas técnicas emitidas por los órganos centrales y la Gestión de la Red que regulan el sistema de responsabilidad y evaluar su cumplimiento. 3. Formular y presentar los Planes de Gestión, de Capacitación y el Presupuesto de la Oficina a su cargo; evaluar los resultados, estableciendo indicadores de productividad y rentabilidad. 4. Gestionar y administrar los recursos humanos, materiales, presupuesto, servicios, asignados a la oficina, de acuerdo a las normas establecidas. 5. Elaborar reportes, informes técnicos e indicadores de gestión de la Oficina y proponer alternativas de mejora. 6. Elaborar y sustentar propuestas para la actualización, innovación o mejoras de los métodos, procedimientos y documentos normativos de apoyo a la gestión del sistema administrativo en el ámbito de su competencia. 7. Asesorar y absolver las consultas sobre temas de su competencia. 8. Establecer procedimientos de seguridad y control interno a fin de proteger los sistemas de información, base de datos y demás recursos en el ámbito de su competencia. Y evaluar su cumplimiento. 9. Implementar las recomendaciones contenidas en los informes del Órgano de Control Interno. 10. Registrar en la computadora personal asignada, con los niveles de acceso autorizados, los datos e información para la explotación de los aplicativos informáticos de su ámbito; guardando estricta confidencialidad de las claves y niveles de acceso autorizados. 11. Velar por la seguridad, mantenimiento y operatividad de los bienes asignados para el cumplimiento de sus labores. 12. Garantizar el cumplimiento de las funciones asignadas en el Reglamento de Organización y Funciones de la Red Asistencial Rebagliati para la Oficina de Soporte Informático. 13. Supervisar controlar y evaluar la utilización de los recursos informáticos. 14. Programar el horario y actividades de las dependencias a su cargo de acuerdo a la normativa institucional y supervisar su cumplimiento. 15. Implementar las iniciativas aprobadas por el Equipo de Gestión de la Red. 16. Garantizar la seguridad, respaldo e integridad de datos del HNERM y los Centros Asistenciales de la Red. 17. Remitir periódicamente las copias de seguridad para la custodia de datos a la Gerencia de Red. 18. Mantener informado al Jefe inmediato sobre las actividades que desarrolla. 19. Realizar otras funciones afines en el ámbito de competencia que le asigne el jefe inmediato. 	
Oficina de Gestión y Desarrollo / Oficina de Planificación Operativa - RAR	



Cargo:	PLANTILLA A33
	JEFE DE OFICINA (E4JEO)
Unidad Orgánica:	OFICINA DE SOPORTE INFORMÁTICO
Relaciones:	
Reporta a :	Jefe de la Oficina de Administración
Supervisa a:	Personal a su cargo
Coordina:	
Internamente:	Gerencias Médicas, Departamentos, Servicios, Centros Asistenciales de la RAR y con la Gerencia Central de Informática según indicaciones del Jefe de la Oficina de Administración.
Externamente:	No Aplica
Oficina de Gestión y Desarrollo / Oficina de Planificación Operativa - RAR	



Cargo:	PLANILLA C13
	PROFESIONAL TÉCNICO ASISTENCIAL (P4PTA)
Unidad Orgánica:	OFICINA DE SOPORTE INFORMÁTICO
Función Principal del Cargo:	
Ejecutar labores asistenciales complementarias bajo la supervisión del profesional de la salud.	
Funciones Específicas del Cargo:	
<ol style="list-style-type: none"> 1. Analizar y absolver las solicitudes y documentos técnicos que se procesan en la Oficina según instrucciones impartidas. 2. Realizar el seguimiento de expedientes que ingresan a la Oficina. 3. Apoyar en la programación, ejecución y control de las actividades de la Oficina referente al trabajo asignado. 4. Recopilar, verificar, ordenar y registrar información que se genera según indicaciones de la Jefatura de la Oficina. 5. Informar periódicamente sobre la elaboración, desarrollo, avances y evaluación del trabajo asignado. 6. Presentar información consolidada, gráficos, resultados y el seguimiento, garantizando la veracidad de la información y preservando las fuentes auditables. 7. Proponer mejoras de los procedimientos técnicos-administrativos del ámbito de competencia. 8. Mantener informado al Jefe de Oficina de Soporte Informático sobre las actividades que desarrolla. 9. Registrar en la computadora personal asignada, con los niveles de acceso autorizados, los datos e información para la explotación de los aplicativos informáticos de su ámbito; guardando estricta confidencialidad de las claves y niveles de acceso autorizados. 10. Velar por la seguridad, mantenimiento y operatividad de los bienes asignados para el cumplimiento de sus labores. 11. Cumplir con los principios y deberes establecidos en el Código de Ética del Personal del Seguro Social de Salud (EsSalud), así como, la Ley y Normas de Control Interno de las entidades del estado. 12. Realizar otras funciones afines en el ámbito de competencia que le asigne el Jefe de Oficina de Soporte Informático 	
Relaciones:	
Reporta a :	Jefe de Oficina de Soporte Informático
Supervisa a:	No aplica
Coordina:	
Internamente:	No aplica
Externamente:	No aplica
Oficina de Gestión y Desarrollo / Oficina de Planificación Operativa - RAR	



Cargo:	PLANTILLA B9
	ANALISTA PROGRAMADOR (T1APR)
Unidad Orgánica:	OFICINA DE SOPORTE INFORMÁTICO
Función Principal del Cargo:	
Diseñar, desarrollar y dar mantenimiento a los sistemas de información, de la Red Asistencial Rebagliati.	
Funciones Específicas del Cargo:	
<ol style="list-style-type: none"> 1. Implementar los sistemas de información, así como desarrollar actividades de capacitación del personal involucrado para la puesta en marcha de los mismos. 2. Confección y distribución de la documentación completa requerida. 3. Cumplir con las normas y estándares establecidos, así como con los niveles de seguridad, calidad y desempeño requeridos. 4. Confeccionar, actualizar y distribuir la documentación técnica de los aplicativos informáticos, especificaciones, diagramas y manuales. 5. Elaborar los mecanismos de control para asegurar la integridad y veracidad de la información. 6. Elaborar los pases a producción de los sistemas de información. 7. Proponer mejoras y actualizaciones a los estándares y metodología de desarrollo de sistemas. 8. Brindar asistencia técnica, capacitación y absolver las consultas de los temas relacionados al ámbito de competencia. 9. Mantener informado al Jefe de Oficina de Soporte Informático sobre las actividades que desarrolla. 10. Registrar en la computadora personal asignada, con los niveles de acceso autorizados, los datos e información para la utilización de los aplicativos informáticos de su ámbito; guardando estricta confidencialidad de las claves y niveles de acceso autorizados. 11. Velar por la seguridad, mantenimiento y operatividad de los bienes asignados para el cumplimiento de sus labores. 12. Cumplir con los principios y deberes establecidos en el Código de Ética del Personal del Seguro Social de Salud (EsSalud); así como, la Ley y Normas de Control Interno de las entidades del estado. 13. Realizar otras funciones afines en el ámbito de competencia que le asigne el Jefe de Oficina de Soporte Informático. 	
Oficina de Gestión y Desarrollo / Oficina de Planificación Operativa - RAR	



Cargo:	PLANTILLA B9
	ANALISTA PROGRAMADOR (T1APR)
Unidad Orgánica:	OFICINA DE SOPORTE INFORMATICO
Relaciones:	
Reporta a :	Jefe de Oficina de Soporte Informático
Supervisa a:	No aplica
Coordina:	
Internamente:	No aplica
Externamente:	No aplica
Oficina de Gestión y Desarrollo / Oficina de Planificación Operativa - RAR	



Cargo:	PLANTILLA B12
	ASISTENTE ADMINISTRATIVO (T2AAD)
Unidad Orgánica:	OFICINA DE SOPORTE INFORMATICO
Función Principal del Cargo:	
Ejecutar y coordinar actividades técnico administrativos relacionados con el procesamiento, clasificación y verificación de la información requerida por la Oficina de Soporte Informático.	
Funciones Específicas del Cargo:	
<ol style="list-style-type: none"> 1. Recopilar, analizar e interpretar la información clasificándola para la gestión del área en que se desempeña. 2. Ejecutar los procedimientos de apoyo a la gestión del área en que se desempeña. 3. Preparar reportes, cuadros, gráficos y resúmenes diversos que requiera la gestión y de acuerdo al ámbito de competencia. 4. Analizar y absolver las solicitudes y documentos técnicos que se procesan en el área en que se desempeña según instrucciones impartidas. 5. Apoyar en la programación, ejecución y control de la gestión de las actividades del área siguiendo instrucciones impartidas. 6. Hacer seguimiento e informar sobre los requerimientos de recursos del área en que se desempeña y apoyar en la administración de los mismos. 7. Mantener informado al Jefe de la Oficina de Soporte Informático sobre las actividades que desarrolla. 8. Registrar en la computadora personal asignada, con los niveles de acceso autorizados, los datos e información para la utilización de los aplicativos informáticos de su ámbito; guardando estricta confidencialidad de las claves y niveles de acceso autorizados. 9. Velar por la seguridad, mantenimiento y operatividad de los bienes asignados para el cumplimiento de sus labores 10. Cumplir con los principios y deberes establecidos en el Código de Ética del Personal del Seguro Social de Salud (EsSalud), así como, la Ley y Normas de Control Interno de las entidades del estado. 11. Realizar otras funciones afines en el ámbito de competencia que le asigne el Jefe de la Oficina de Soporte Informático. 	
Relaciones:	
Reporta a :	Jefe de la Oficina de Soporte Informático
Supervisa a:	No aplica.
Coordina:	
Internamente:	No aplica
Externamente:	No aplica
Oficina de Gestión y Desarrollo / Oficina de Planificación Operativa - RAR	



Cargo:	PLANTILLA B13
	TÉCNICO DE SERVICIO ADMINISTRATIVO Y APOYO (T2TAD)
Unidad Orgánica:	OFICINA DE SOPORTE INFORMÁTICO
Función Principal del Cargo:	
Brindar apoyo de actividades técnico administrativos en el desarrollo de las actividades que involucra el sistema administrativo de la Oficina de Soporte Informático.	
<ol style="list-style-type: none"> 1. Ejecutar los procedimientos técnicos del sistema administrativo del área al cual el cargo está adscrito. 2. Analizar y absolver las solicitudes y documentos técnicos que se procesan en el área en que se desempeña según instrucciones impartidas. 3. Realizar el seguimiento de expedientes que ingresan a la unidad orgánica. 4. Apoyar en la programación, ejecución y control de las actividades del área, siguiendo instrucciones impartidas. 5. Recopilar, verificar, ordenar y registrar información que se genera en el área en que se desempeña. 6. Preparar reportes, cuadros, gráficos y resúmenes diversos solicitados. 7. Absolver las consultas técnico-administrativas del ámbito de competencia y emitir el informe correspondiente. 8. Participar en reuniones y comisiones de trabajo según indicaciones. 9. Proponer mejoras de los procedimientos técnicos-administrativos del ámbito de competencia. 10. Apoyar en la elaboración de los reportes periódicos de Información Gerencial. 11. Mantener informado al jefe inmediato sobre las actividades que desarrolla. 12. Registrar en la computadora personal asignada, con los niveles de acceso autorizados, los datos e información para la explotación de los aplicativos informáticos de su ámbito; guardando estricta confidencialidad de las claves y niveles de acceso autorizados. 13. Velar por la seguridad, mantenimiento y operatividad de los bienes asignados para el cumplimiento de sus labores. 14. Realizar otras funciones afines en el ámbito de competencia que le asigne el jefe inmediato. 	
Relaciones:	
Reporta a :	Jefe de la Oficina de Soporte Informático.
Supervisa a:	No aplica.
Coordina:	
Internamente:	No aplica
Externamente:	No aplica
Oficina de Gestión y Desarrollo / Oficina de Planificación Operativa - RAR	



Cargo:	PLANTILLA B14
	TECNICO DE PROCESAMIENTO AUTOMATICO DE DATOS (T2TPD)
Unidad Orgánica:	OFICINA DE SOPORTE INFORMATICO
Función Principal del Cargo:	
Realizar las actividades operativas concernientes al procesamiento automático de datos, redes, conectividad y comunicaciones.	
Funciones Específicas del Cargo:	
<ol style="list-style-type: none"> 1. Procesar información técnica y emitir reportes e informes solicitados para gestión del área al cual el cargo está adscrito. 2. Brindar el soporte técnico en hardware y software en el ámbito de competencia, de acuerdo a normas y estándares establecidos. 3. Mantener operativo los equipos de informática, de comunicaciones, red de voz, datos e imagen. 4. Realizar los procedimientos necesarios de copias de respaldo de la base de datos del área al cual el cargo está adscrito. 5. Desarrollar actividades correspondientes al inventario informático e identificar, coordinar, consolidar y sustentar las necesidades informáticas y de comunicaciones requeridas para el área al cual el cargo está adscrito. 6. Aplicar procedimientos de seguridad a todos los sistemas de tecnología de información, equipos informáticos y de comunicación del área al cual el cargo está adscrito, según normativa Institucional vigente. 7. Mantener informado al jefe inmediato sobre las actividades que desarrolla. 8. Registrar en la computadora personal asignada, con los niveles de acceso autorizados, los datos e información para la explotación de los aplicativos informáticos de su ámbito; guardando estricta confidencialidad de las claves y niveles de acceso autorizados. 9. Velar por la seguridad, mantenimiento y operatividad de los bienes asignados para el cumplimiento de sus labores. 10. Realizar otras funciones afines al ámbito de competencia que le asigne el jefe inmediato. 	
Relaciones:	
Reporta a :	Jefe de Oficina de Soporte Informático
Supervisa a:	No aplica
Coordina:	
Internamente:	No aplica
Externamente:	No aplica
Oficina de Gestión y Desarrollo / Oficina de Planificación Operativa - RA	



Cargo:	PLANTILLA B19
	OPERADOR DE CONMUTADOR, TELÉFONO, RADIO Y EQUIPOS ELÉCTRICOS (T3OTE)
Unidad Orgánica:	OFICINA DE SOPORTE INFORMÁTICO
Función Principal del Cargo:	
Ejecutar procedimientos de electrónica, teleproceso, telecomunicaciones y circuitos eléctricos en el área al cual el cargo está adscrito.	
Funciones Específicas del Cargo:	
<ol style="list-style-type: none"> 1. Operar y verificar el funcionamiento de transmisores, equipos de radiocomunicación y central telefónica. 2. Realizar la reparación de los equipos y circuitos eléctricos, de telecomunicaciones o similar, en el ámbito de su competencia. 3. Revisar y determinar el estado de conservación de equipos electrónicos, material de trabajo y herramientas que le asigne bajo indicaciones. 4. Efectuar la vigilancia de equipos radiales y de comunicación mediante la lectura de instrumentos. 5. Operar equipos de procesamiento de datos o teleproceso. 6. Registrar y emitir informes de las actividades asignadas. 7. Mantener informado al Jefe de la Oficina de Soporte Informático sobre las actividades que desarrolla. 8. Registrar en la computadora personal asignada, con los niveles de acceso autorizados, los datos e información para la utilización explotación de los aplicativos informáticos de su ámbito; guardando estricta confidencialidad de las claves y niveles de acceso autorizados. 9. Velar por la seguridad, mantenimiento y operatividad de los bienes asignados para el cumplimiento de sus labores. 10. Cumplir con los principios y deberes establecidos en el Código de Ética del Personal del Seguro Social de Salud (EsSalud), así como, la Ley y Normas de Control Interno de las entidades del estado. 11. Realizar otras funciones afines en el ámbito de competencia que le asigne el Jefe de la Oficina de Soporte Informático 	
Relaciones:	
Reporta a :	Jefe de la Oficina de Soporte Informático
Supervisa a:	No aplica
Coordina:	
Internamente:	No aplica
Externamente:	No aplica
Oficina de Gestión y Desarrollo / Oficina de Planificación Operativa - RA	



Cargo:	PLANTILLA C21
	DIGITADOR ASISTENCIAL (T3DIA)
Unidad Orgánica:	OFICINA DE SOPORTE INFORMÁTICO
Función Principal del Cargo:	
Registrar y procesar datos del área asignada en los sistemas de información institucional autorizados.	
Funciones Específicas del Cargo:	
<ol style="list-style-type: none"> 1. Ingresar, registrar, codificar, hacer el seguimiento y control de calidad de los datos, en los sistemas de información institucional y aplicativos asignados. 2. Procesar información de las prestaciones de salud en el ámbito de competencia. 3. Verificar la vigencia del derecho a prestaciones asistenciales, otorgar cita/ticket de atención y brindar orientación al paciente en el ámbito de competencia. 4. Registrar datos personales, complementarios de los asegurados y mantener actualizada la información en la base de datos del Sistema de Información Institucional. 5. Consolidar información, emitir reportes y explotar los datos registrados, según indicación. 6. Custodiar y mantener la confidencialidad de datos, información y documentos que se procesa en el ámbito de responsabilidad. 7. Verificar el correcto funcionamiento del equipo a su cargo, detectar los errores que señala el sistema y reportar las anomalías observadas. 8. Mantener informado al Jefe de la Oficina de Soporte Informático sobre las actividades que desarrolla. 9. Registrar en la computadora personal asignada, con los niveles de acceso autorizados, los datos e información para la explotación de los aplicativos informáticos de su ámbito; guardando estricta confidencialidad de las claves y niveles de acceso autorizados. 10. Velar por la seguridad, mantenimiento y operatividad de los bienes asignados para el cumplimiento de sus labores. 11. Cumplir con los principios y deberes establecidos en el Código de Ética del Personal del Seguro Social de Salud (EsSalud), así como, la Ley y Normas de Control Interno de las entidades del estado. 12. Realizar otras funciones afines en el ámbito de competencia que le asigne el Jefe de la Oficina de Soporte Informático 	
Relaciones:	
Reporta a : Jefe de la Oficina de Soporte Informático	
Supervisa a: No aplica	
Coordina:	
Internamente: No aplica	
Externamente: No aplica	
Oficina de Gestión y Desarrollo / Oficina de Planificación Operativa - RA	



Cargo:	PLANTILLA B21
	DIGITADOR (T3DIG)
Unidad Orgánica:	OFICINA DE SOPORTE INFORMATICO
Función Principal del Cargo:	
Atender los requerimientos de citas de los asegurados, así mismo, verificar en el sistema: la acreditación, adscripción e historia clínica del asegurado.	
Funciones Específicas del Cargo:	
<ol style="list-style-type: none"> 1. Digitar adecuadamente la información que ingresa al sistema. 2. Emitir reportes según diseños previamente establecidos. 3. Mantener el orden, custodia y confidencialidad de los datos, información y documentos que procesa. 4. Mantener informado al Jefe de la Oficina de Soporte Informático sobre las actividades que desarrolla. 5. Registrar en la computadora personal asignada, con los niveles de acceso autorizados, los datos e información para la utilización de los aplicativos informáticos de su ámbito; guardando estricta confidencialidad de las claves y niveles de acceso autorizados. 6. Velar por la seguridad, mantenimiento y operatividad de los bienes asignados para el cumplimiento de sus labores. 7. Cumplir con los principios y deberes establecidos en el Código de Ética del Personal del Seguro Social de Salud (EsSalud); así como, la Ley y Normas de Control Interno de las entidades del estado. 8. Realizar otras funciones afines en el ámbito de competencia que le asigne Jefe de la Oficina de Soporte Informático. 	
Relaciones:	
Reporta a :	Jefe de la Oficina de Soporte Informático
Supervisa a:	No aplica
Coordina:	
Internamente:	No aplica
Externamente:	No aplica
Oficina de Gestión y Desarrollo / Oficina de Planificación Operativa - RA	



Cargo:	PLANTILLA C18
	TECNICO DE ENFERMERIA (T4TEN)
Unidad Orgánica:	OFICINA DE SOPORTE INFORMatico
Función Principal del Cargo:	
Participar en la entrega de reporte, haciendo un resumen de las áreas asignadas por la enfermera.	
Funciones Específicas del Cargo:	
<ol style="list-style-type: none"> 1. Asistir al paciente en la atención de la salud por indicación del profesional asistencial, en el ámbito de competencia. 2. Asistir al profesional de la salud en la atención del paciente en procedimientos de diagnóstico, terapéuticos y en los exámenes médicos. 3. Proporcionar cuidados al paciente relacionados con el confort, aseo personal y cambios posturales, según indicación del profesional asistencial. 4. Acudir y atender de inmediato el llamado del paciente en el ámbito de competencia y dar aviso al profesional asistencial. 5. Realizar procedimientos asistenciales simples en el marco de la normativa vigente y por indicación del profesional. 6. Asistir al profesional asistencial en curaciones, inyectables, tratamientos de rutina o especiales. 7. Participar en la aplicación de técnicas y métodos de menor complejidad para la atención del paciente, bajo supervisión del profesional asistencial. 8. Operar equipos biomédicos en el ámbito de competencia y bajo supervisión del profesional asistencial. 9. Participar en actividades de promoción de la salud y prevención de la enfermedad por indicación del profesional de la salud. 10. Mantener ordenada, preparada el área de trabajo, muebles, material e instrumental médico quirúrgico de la unidad a la que se encuentra asignado, según procedimientos vigentes. 11. Recoger, preparar, almacenar, ordenar y distribuir materiales, insumos, reactivos, instrumental médico quirúrgico, fármacos, formatería por indicación del profesional de la salud. 12. Trasladar muestras biológicas, biopsias, líquidos, secreciones y otros, de acuerdo a procedimiento vigente. 13. Participar en la preparación y trasladar el cadáver, según normas vigentes. 14. Preparar, movilizar y trasladar al paciente por indicación del profesional asistencial. 15. Realizar y registrar el inventario de las pertenencias del paciente a su ingreso y egreso del servicio en los formatos respectivos, firmar y hacer firmar por el paciente o familiar responsable debidamente identificado y entregar a enfermera de turno. 16. Realizar el control y registro de la ropa hospitalaria, materiales, insumos y equipamiento, según programación. 17. Tramitar citas para solicitudes de exámenes de diagnósticos, procedimientos terapéuticos, prescripción farmacológica, interconsultas. 18. Seleccionar, ordenar y devolver las historias clínicas, placas radiográficas y documentación complementaria a los archivos respectivos. 19. Cumplir con las normas de bioseguridad. 	
Oficina de Gestión y Desarrollo / Oficina de Planificación Operativa - RA	



Cargo:	PLANTILLA C18
	TECNICO DE ENFERMERIA (T4TEN)
Unidad Orgánica:	OFICINA DE SOPORTE INFORMATICO
<p>20. Eliminar residuos biológicos hospitalarios, bajo supervisión del profesional asistencial.</p> <p>21. Registrar las tareas o trabajos asignados e informar al profesional responsable.</p> <p>22. Velar por la seguridad, mantenimiento y operatividad de los bienes asignados para el cumplimiento de sus labores.</p> <p>23. Realizar otras funciones afines en el ámbito de competencia que le asigne el jefe inmediato.</p>	
Relaciones:	
Reporta a :	Jefe de la Oficina de Soporte Informático
Supervisa a:	No aplica
Coordina:	
Internamente:	No aplica
Externamente:	No aplica
<p>Oficina de Gestión y Desarrollo / Oficina de Planificación Operativa - RA</p>	



Cargo:	PLANTILLA B29
	TECNICO DE MANTENIMIENTO (T4TMA)
Unidad Orgánica:	OFICINA DE SOPORTE INFORMATICO
Función Principal del Cargo: Conservar y realizar el mantenimiento de instalaciones y equipos Informáticos.	
Funciones Específicas del Cargo:	
<ol style="list-style-type: none"> 1. Realizar el mantenimiento de los equipos médicos, electrónicos, mecánicos o similares. 2. Controlar el adecuado funcionamiento de los equipos y unidades especializadas, instalaciones eléctricas, líneas de agua, líquidos y/o gases, entre otros. 3. Verificar que los equipos, instalaciones y otras maquinas se encuentren en buenas condiciones y reportar las anomalías observadas. 4. Apoyar en la recepción, registro, almacenamiento y distribución de materiales. 5. Transportar, ordenar muebles, equipos y enseres según indicación. 6. Reportar al superior inmediato los trabajos realizados, pendientes y en proceso. 7. Velar por la seguridad, mantenimiento y operatividad de los bienes asignados para el cumplimiento de sus labores. 8. Cumplir con los principios y deberes establecidos en el Código de Ética del Personal del Seguro Social de Salud (EsSalud); así como, la Ley y Normas de Control Interno de las entidades del estado. 9. Realizar otras funciones afines en el ámbito de competencia que le asigne el jefe inmediato. 	
Relaciones:	
Reporta a : Jefe de la Oficina de Soporte Informático. Supervisa a: No aplica.	
Coordina:	
Internamente: No aplica Externamente: No aplica	
Oficina de Gestión y Desarrollo / Oficina de Planificación Operativa - RA	



Cargo:	PLANTILLA C19
	AUXILIAR DE SERVICIO ASISTENCIAL (A1ASA)
Unidad Orgánica:	OFICINA DE SOPORTE INFORMÁTICO
Función Principal del Cargo: Preparar el ambiente del consultorio así como el material a ser usado como gasas, vendas, estampillas, guantes, ropería y Recoger las tarjetas y órdenes de los pacientes citados.	
Funciones Específicas del Cargo:	
<ol style="list-style-type: none"> 1. Proporcionar cuidados al paciente relacionados con el confort y cambios posturales, según indicación del profesional asistencial. 2. Asistir al paciente en el cambio de ropa, aseo personal y alimentación, de acuerdo a necesidad y procedimientos establecidos. 3. Acudir y atender de inmediato el llamado del paciente en el ámbito de su competencia y dar aviso al profesional asistencial. 4. Asistir al paciente en la colocación y retiro de chata, urinario, escupidera, riñonera u otros recipientes higiénicos. 5. Mantener limpios, desinfectados y ordenados los recipientes higiénicos. 6. Limpiar, desinfectar, preparar las camas y equipar el ambiente donde se presta atención asistencial, según procedimientos vigentes. 7. Participar en el transporte, distribución de dietas, ordenamiento y limpieza del menaje y utensilios, bajo supervisión del profesional asistencial. 8. Lavar, secar, preparar y esterilizar el instrumental y material médico quirúrgico de acuerdo a procedimientos establecidos. 9. Recoger y distribuir materiales, insumos, reactivos, fármacos, formatería, de las áreas asignadas; ordenarlos y almacenarlos, según indicación del profesional asistencial. 10. Prestar apoyo en el registro e inventario de medicamentos y participar en la entrega de los mismos, por indicación del profesional asistencial. 11. Trasladar, almacenar y distribuir víveres frescos, secos y cárnicos según indicación del profesional asistencial. 12. Trasladar muestras biológicas, biopsias, líquidos, secreciones y otros, de acuerdo a procedimiento vigente. 13. Transportar y movilizar al paciente según indicaciones del profesional responsable. 14. Controlar y registrar la ropa hospitalaria, materiales, insumos y equipamiento, según su responsabilidad, de acuerdo al listado del servicio respectivo. 15. Realizar y registrar el inventario de las pertenencias del paciente a su ingreso y egreso del servicio en los formatos respectivos, firmar y hacer firmar por el paciente o familiar responsable debidamente identificado y entregar a enfermera de turno. 16. Seleccionar, ordenar y devolver las historias clínicas, placas radiográficas y documentación complementaria a los archivos respectivos. 17. Cumplir con las normas de bioseguridad. 18. Eliminar residuos biológicos hospitalarios, bajo supervisión del profesional asistencial. 19. Registrar las tareas y/o trabajos asignados e informar al profesional responsable. 20. Velar por la seguridad, mantenimiento y operatividad de los bienes asignados para el cumplimiento de sus labores. 	
Oficina de Gestión y Desarrollo / Oficina de Planificación Operativa - RA	



Cargo:	PLANTILLA C19
	AUXILIAR DE SERVICIO ASISTENCIAL (A1ASA)
Unidad Orgánica:	OFICINA DE SOPORTE INFORMÁTICO
Relaciones:	
Reporta a :	Jefe de la Oficina de Soporte Informático.
Supervisa a:	No aplica
Coordina:	
Internamente:	No aplica
Externamente:	No aplica
Oficina de Gestión y Desarrollo / Oficina de Planificación Operativa - RA	

Fuente: Oficina de Gestión y Desarrollo / Oficina de Planificación Operativa RAR (2014).



5.6. FASE 6: OPTIMIZACIÓN (LifeCycle)

En la fase de optimización se comprueban que los requerimientos se han cumplido para seguir mejorando la funcionalidad y operatividad de la red.

Requerimientos Cumplidos:

- a. Los modelos son capaces de adaptarse a un crecimiento posterior.
- b. El hardware existente se reutilizo en la implementación de la red LAN del HNERM-ESSALUD.
- c. La presencia de malware en la Red LAN del HNERM-EsSALUD está controlado.
- d. La implementación no generó costos de licencias de software; tanto del lado del servidor como del cliente.
- e. Que el hardware existente responda de manera satisfactoria en el desarrollo de las actividades del personal.
- f. Se establecieron políticas de seguridad para el correcto uso de la Red Informática y sus recursos.
- g. La red brinda disponibilidad y escalabilidad para el correcto funcionamiento de las estaciones de trabajo (ordenadores).
- h. Se elaboró un documento en el que indicamos los pasos o las pautas que debemos seguir para cuando suceda algún evento inesperado este documento es el Plan de contingencia, que no dirá cómo actuar ante un problema (**Fase II Planificación**).

Durante la Fase de Implementación del proyecto ya se empezaban a notar ciertos errores que requerían de una corrección para ir de a pocos mejorando y optimizando el sistema.



Ya se había mencionado antes, en el caso de los documentos se estuvieron corrigiendo desde la Fase de Implementación, en esta Fase de Optimización se hace algo parecido, a diferencia que aquí en esta Fase todo se ejecuta en conjunto y lo que nos queda es ir optimizando algunas falencias que pueda tener la virtualización de los equipos de conmutación.

En este caso el proyecto ha culminado y lo único que queda es dejarlo funcionando los VDC del Switch Nexus 7000 de Cisco.

Lugares y ubicaciones de los equipos y de los usuarios, materiales y personal participantes, los que se encuentran ubicados en las áreas del HNERM-EsSALUD.

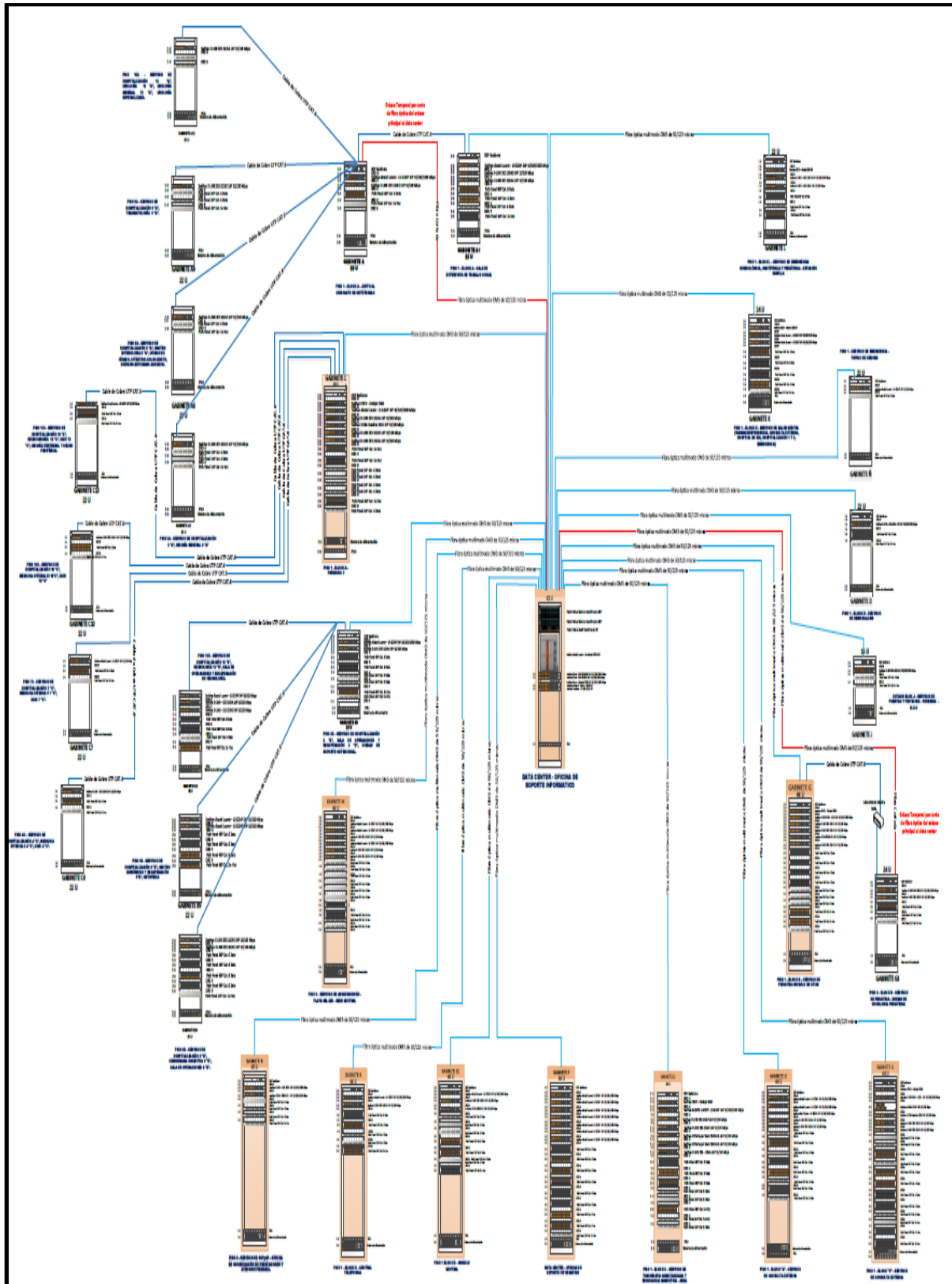


Figura 105. Mapa Ubicación Actual del Data Center y Gabinetes del HNERM EsSALUD año 2016.
Fuente: Oficina de Soporte Informático HNERM EsSALUD (2016).



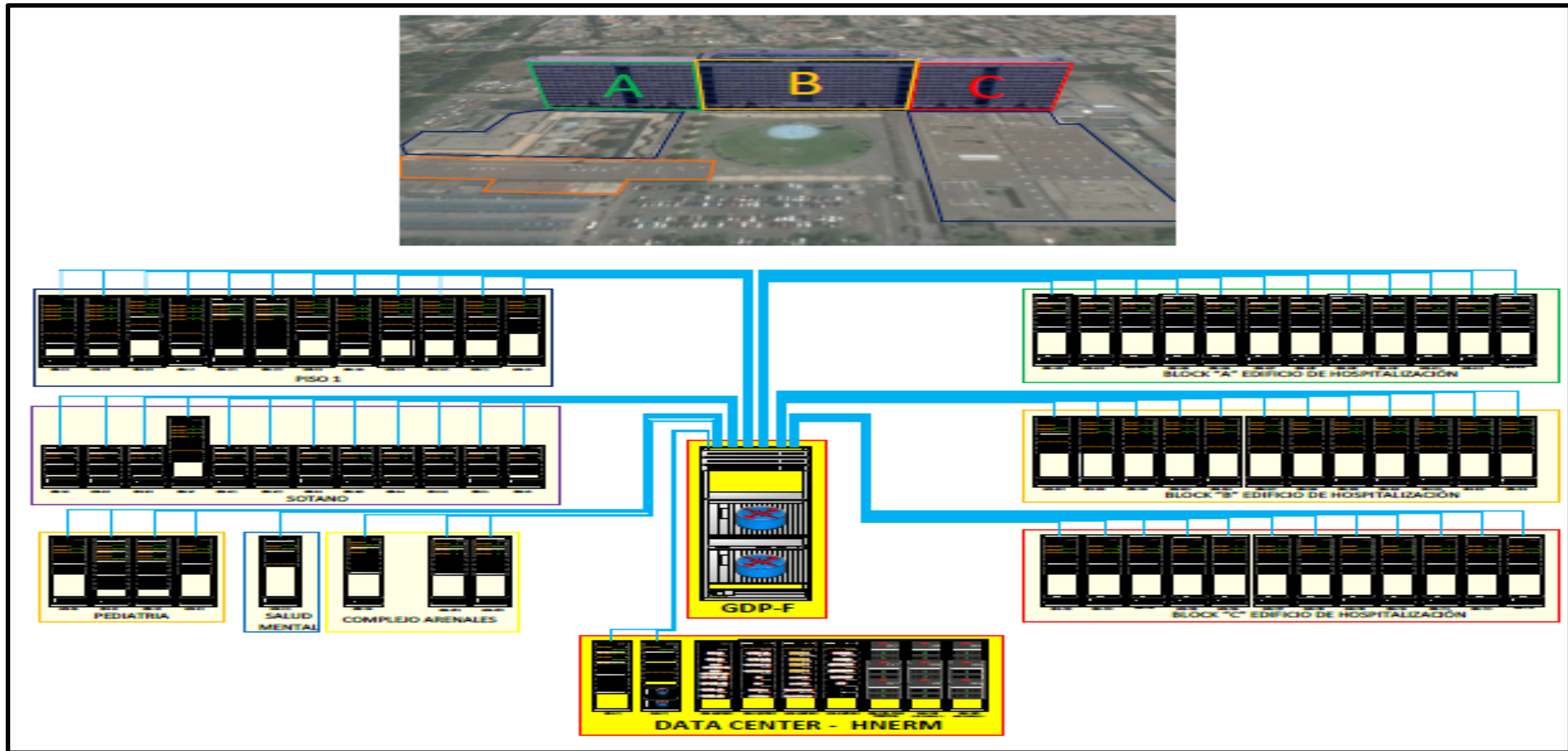


Figura 106. Mapa Ubicación Propuesto del Data Center y Gabinetes del HNERM EsSALUD año 2017. Fuente: Elaboración Propia (2017).

Nota: El Diseño de Red Jerárquico que ee está Proponiendo Brindará Alta Disponibilidad, Implementación de Seguridad a Través de Firewall, Redundancia con los Servidores y Virtualización de los Switches Core Nexus 7000.



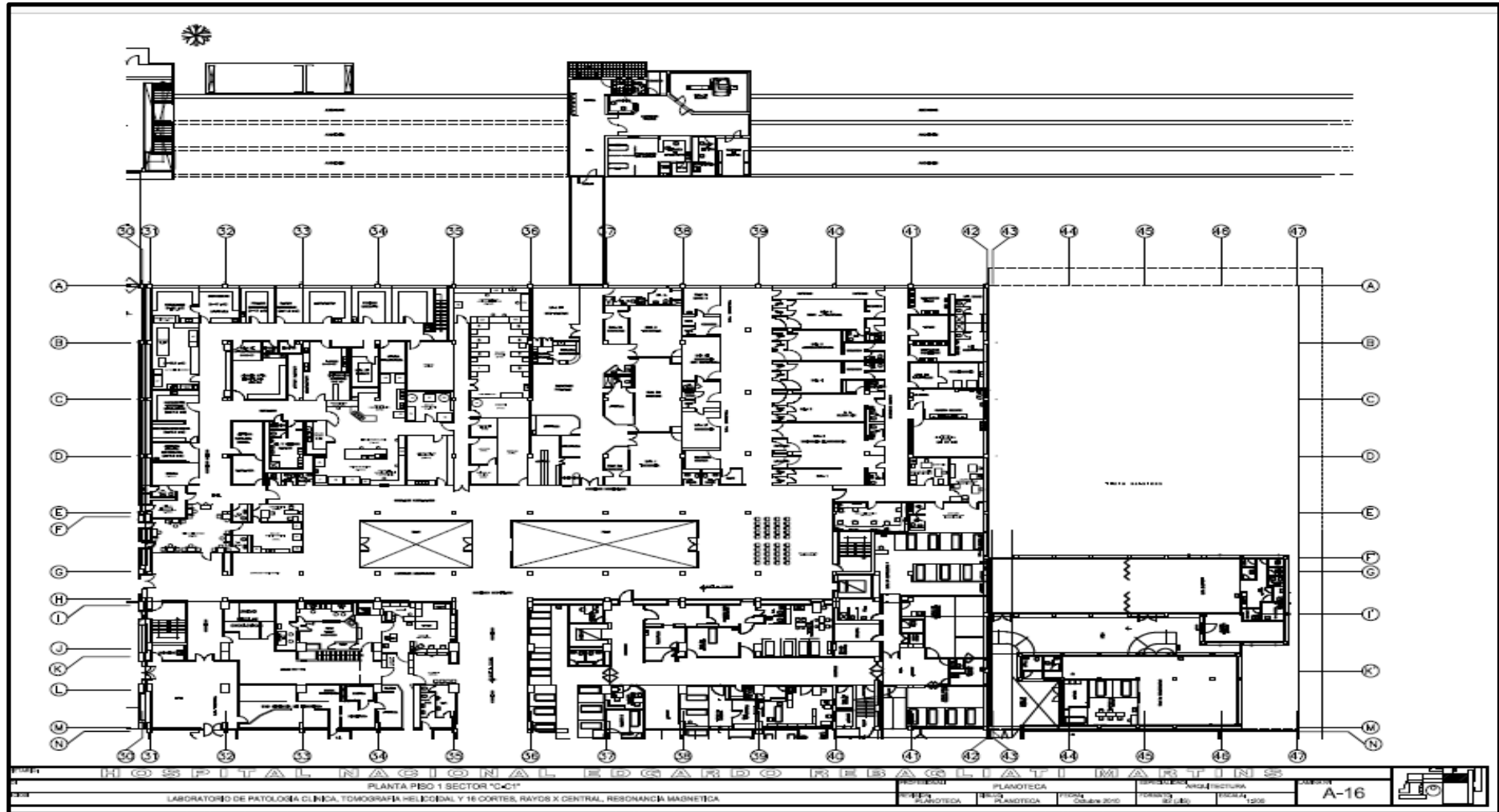


Figura 107. Plano de Ubicación Actual de la 1era. Planta del HNERM EsSALUD. Fuente: Servicios Generales Planoteca HNERM EsSALUD (2017).



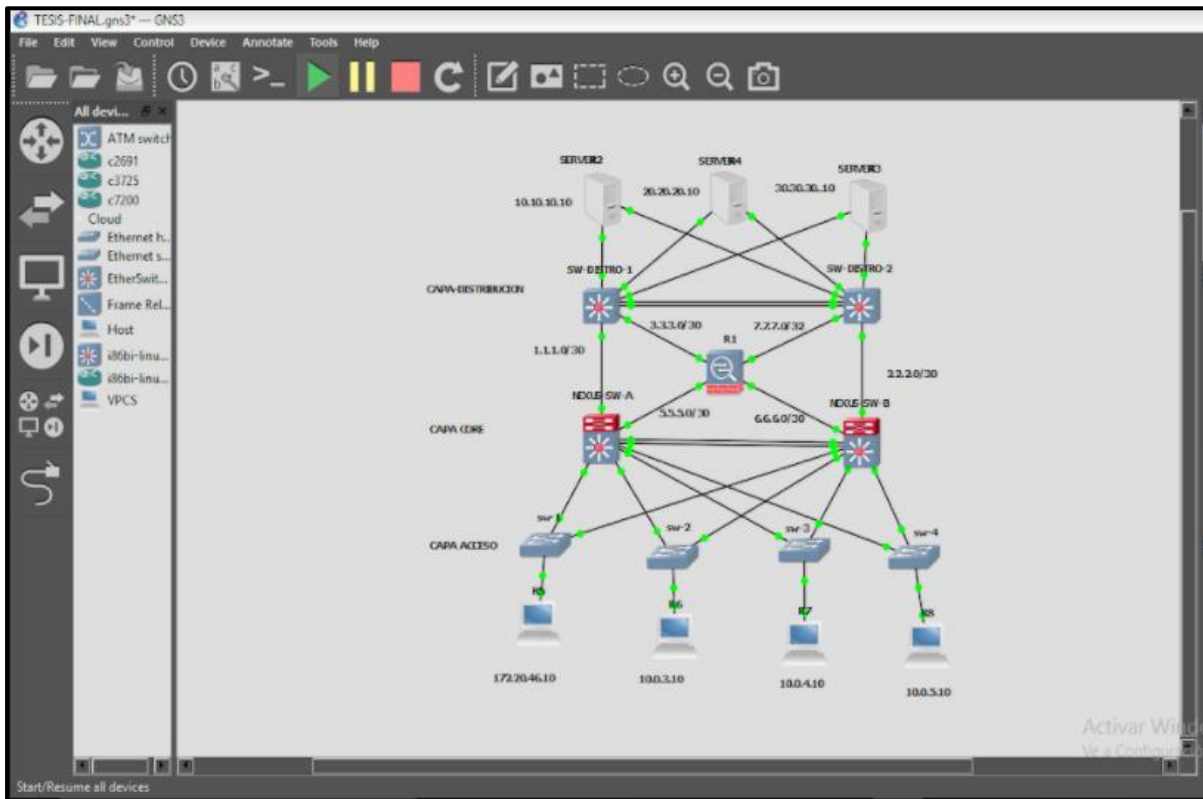


Figura 108. Topología Estrella Jerárquica Propuesta para los Dispositivos de Conmutación del HNERM EsSALUD. Fuente: Elaboración Propia (2017).

```

ESSALUD-N7K9-COREB# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Documents: http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html
Copyright (c) 2002-2016, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

NX-OSv is a demo version of the Nexus Operating System

Software
  loader:          version N/A
  kickstart:       version 7.3(0)D1(1)
  system:          version 7.3(0)D1(1)
  kickstart image file is: bootflash:///titanium-d1-kickstart.7.3.0.D1.1.bin
  kickstart compile time: 1/11/2016 16:00:00 [02/11/2016 10:30:12]
  system image file is:  bootflash:///titanium-d1.7.3.0.D1.1.bin
  system compile time:  1/11/2016 16:00:00 [02/11/2016 13:08:11]

Hardware
  cisco NX-OSv Chassis ("NX-OSv supervisor Module")
  QEMU virtual CPU version 2.5 with 3064740 kB of memory.
  Processor Board ID TM74AA5F00B

  Device name: ESSALUD-N7K9-COREB
  bootflash: 3184776 kB

kernel uptime is 0 day(s), 0 hour(s), 37 minute(s), 5 second(s)

plugin
  Core Plugin, Ethernet Plugin

Active Package(s)
ESSALUD-N7K9-COREB#
    
```

Figura 109. Comandos de la Virtualización de los VDC'S. Fuente: Elaboración Propia (2017).



```

ESSALUD-N7K9-CoreA# show license usage
Feature                Ins Lic      Status Expiry Date Comments
                       Count
-----
MPLS_PKG               No  -    Unused
STORAGE-ENT           No  -    Unused
VDC_LICENSES          No  0    Unused      Grace 119D 23H
ENTERPRISE_PKG        No  -    Unused
FCOE-N7K-F132XP       No  0    Unused
FCOE-N7K-F248XP       No  0    Unused
ENHANCED_LAYER2_PKG   No  -    Unused
SCALABLE_SERVICES_PKG No  -    Unused
TRANSPORT_SERVICES_PKG No  -    Unused
LAN_ADVANCED_SERVICES_PKG No  -    Unused
LAN_ENTERPRISE_SERVICES_PKG Yes -    In use Never
    
```

Figura 110. Comandos de la Virtualización de los VDC'S. Fuente: Elaboración Propia (2017).

```

hostname ESSALUD-N7K9-COREB
vdc ESSALUD-N7K9-COREB id 1
  limit-resource module-type m1 m1x1 m2x1 f2e
  allocate interface Ethernet2/1-48
  allocate interface Ethernet3/1-48
  allocate interface Ethernet4/1-48
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 96 maximum 96
  limit-resource u6route-mem minimum 24 maximum 24
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

feature eigrp
feature interface-vlan
feature dhcp

username admin password 5 $5$0tc7T0NC$K.u1n5ZnsyXLrTGnBdtLgZJXEa8EeNx.BrDz98xyk2
  role network-admin
no password strength-check
ip domain-lookup
vlan dot1q tag native
system default switchport
system jumbomtu 0
no logging event trunk-status enable
copp profile strict
snmp-server user admin auth md5 0x328945d53e05e8e7207f8c20b142f0b7 priv 0x328945
d53e05e8e7207f8c20b142f0b7 localizedkey engineID 128:0:0:9:3:0:0:0:0:0
rmon event 1 log description FATAL(1) owner PMON@FATAL
rmon event 2 log description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log description ERROR(3) owner PMON@ERROR
rmon event 4 log description WARNING(4) owner PMON@WARNING
rmon event 5 log description INFORMATION(5) owner PMON@INFO
snmp-server enable traps link

vlan 1

service dhcp
ip dhcp relay
ipv6 dhcp relay
vrf context management
    
```

Figura 111. Comandos de la Virtualización de los VDC'S. Fuente: Elaboración Propia (2017).




```

ESSALUD-N7K9-COREA# show running-config

!Command: show running-config
!Time: Mon Mar 12 21:34:28 2018

version 7.3(0)d1(1)
power redundancy-mode redundant
license grace-period

hostname ESSALUD-N7K9-COREA
vdc ESSALUD-N7K9-COREA id 1
  limit-resource module-type m1 m1x1 m2x1 f2e
  allocate interface Ethernet2/1-48
  allocate interface Ethernet3/1-48
  allocate interface Ethernet4/1-48
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 96 maximum 96
  limit-resource u6route-mem minimum 24 maximum 24
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

username admin password 5 $$50tc7T0NC$K.u!nSznsyXLRtGNBdtLgZJXEa8Eenx.BrDz98xyK2
C role network-admin
no password strength-check
ip domain-lookup
vlan dot1q tag native
system default switchport
system jumbomtu 0
no logging event trunk-status enable
copp profile strict
snmp-server user admin auth md5 0x328945d53e05e8e7207f8c20b142f0b7 priv 0x328945
d53e05e8e7207f8c20b142f0b7 localizedkey engineID 128:0:0:9:3:0:0:0:0:0:0
rmon event 1 log description FATAL(1) owner PMON@FATAL
rmon event 2 log description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log description ERROR(3) owner PMON@ERROR
rmon event 4 log description WARNING(4) owner PMON@WARNING
rmon event 5 log description INFORMATION(5) owner PMON@INFO
snmp-server enable traps link

vlan 1

```

Figura 112. Comandos de la Virtualización de los VDC'S. Fuente: Elaboración Propia (2017).

```

ESSALUD-N7K9-COREA# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Documents: http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html
Copyright (c) 2002-2016, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

NX-OSV is a demo version of the Nexus Operating System

Software
  loader:      version N/A
  kickstart:  version 7.3(0)d1(1)
  system:     version 7.3(0)d1(1)
  kickstart image file is: bootflash:///titanium-d1-kickstart.7.3.0.D1.1.bin
  kickstart compile time: 1/11/2016 16:00:00 [02/11/2016 10:30:12]
  system image file is: bootflash:///titanium-d1.7.3.0.D1.1.bin
  system compile time: 1/11/2016 16:00:00 [02/11/2016 13:08:11]

Hardware
  cisco NX-OSV Chassis ("NX-OSV Supervisor Module")
  QEMU Virtual CPU version 2.5 with 3064740 kB of memory.
  Processor Board ID TM74DC5200B

  Device name: ESSALUD-N7K9-COREA
  bootflash: 3184776 kB

Kernel uptime is 0 day(s), 0 hour(s), 35 minute(s), 10 second(s)

plugin
  Core Plugin, Ethernet Plugin

Active Package(s)
ESSALUD-N7K9-COREA# █

```

Figura 113. Comandos de la Virtualización de los VDC'S. Fuente: Elaboración Propia (2017).



```

ESSALUD-N7K9-CoreA# show vdc detail

Switchwide mode is m1 f1 m1x1 f2 m2x1 f2e f3

vdc id: 1
vdc name: ESSALUD-N7K9-CoreA
vdc state: active
vdc mac address: e4:c7:22:0b:87:c1
vdc ha policy: RELOAD
vdc dual-sup ha policy: SWITCHOVER
vdc boot Order: 1
CPU Share: 5
CPU Share Percentage: 25%
vdc create time: Thu Dec 15 21:40:10 2016
vdc reload count: 0
vdc uptime: 451 day(s), 19 hour(s), 20 minute(s), 17 second(s)
vdc restart count: 0
vdc type: Ethernet
vdc supported linecards: m1 m1x1 m2x1 f2e

vdc id: 2
vdc name: DATOS
vdc state: active
vdc mac address: e4:c7:22:0b:87:c2
vdc ha policy: RESTART
vdc dual-sup ha policy: SWITCHOVER
vdc boot Order: 1
CPU Share: 5
CPU Share Percentage: 25%
vdc create time: Mon Mar 12 16:58:20 2018
vdc reload count: 0
vdc uptime: 0 day(s), 0 hour(s), 3 minute(s), 0 second(s)
vdc restart count: 0
vdc type: Ethernet
vdc supported linecards: m1 m1x1 m2x1 f2e
    
```

Figura 114. Comandos de la Virtualización de los VDC'S. Fuente: Elaboración Propia (2017).

```

vdc id: 3
vdc name: VOZ
vdc state: active
vdc mac address: e4:c7:22:0b:87:c3
vdc ha policy: RESTART
vdc dual-sup ha policy: SWITCHOVER
vdc boot Order: 1
CPU Share: 5
CPU Share Percentage: 25%
vdc create time: Mon Mar 12 16:58:48 2018
vdc reload count: 0
vdc uptime: 0 day(s), 0 hour(s), 2 minute(s), 17 second(s)
vdc restart count: 0
vdc type: Ethernet
vdc supported linecards: m1 m1x1 m2x1 f2e

vdc id: 4
vdc name: impresoras
vdc state: active
vdc mac address: e4:c7:22:0b:87:c4
vdc ha policy: RESTART
vdc dual-sup ha policy: SWITCHOVER
vdc boot Order: 1
CPU Share: 5
CPU Share Percentage: 25%
vdc create time: Mon Mar 12 16:59:09 2018
vdc reload count: 0
vdc uptime: 0 day(s), 0 hour(s), 1 minute(s), 57 second(s)
vdc restart count: 0
vdc type: Ethernet
vdc supported linecards: m1 m1x1 m2x1 f2e

ESSALUD-N7K9-CoreA# █
    
```

Figura 115. Comandos de la Virtualización de los VDC'S. Fuente: Elaboración Propia (2017).



```
vdc ESSALUD-N7K9-CoreA id 1
  limit-resource module-type m1 m1x1 m2x1 f2e
  cpu-share 5
  allocate interface Ethernet3/1-48
  allocate interface Ethernet4/1-48
  allocate interface Ethernet5/1-48
  allocate interface Ethernet6/1-48
  allocate interface Ethernet7/1-48
  allocate interface Ethernet8/1-48
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource monitor-session-erspan-dst minimum 0 maximum 23
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 96 maximum 96
  limit-resource u6route-mem minimum 24 maximum 24
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8
  limit-resource monitor-session-inband-src minimum 0 maximum 1
  limit-resource anycast_bundleid minimum 0 maximum 16
  limit-resource monitor-session-mx-exception-src minimum 0 maximum 1
  limit-resource monitor-session-extended minimum 0 maximum 12
vdc DATOS id 2
  limit-resource module-type m1 m1x1 m2x1 f2e
  cpu-share 5
  boot-order 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource monitor-session-erspan-dst minimum 0 maximum 23
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 8 maximum 8
  limit-resource u6route-mem minimum 4 maximum 4
  limit-resource m4route-mem minimum 8 maximum 8
  limit-resource m6route-mem minimum 5 maximum 5
  limit-resource monitor-session-inband-src minimum 0 maximum 1
  limit-resource anycast_bundleid minimum 0 maximum 16
  limit-resource monitor-session-mx-exception-src minimum 0 maximum 1
  limit-resource monitor-session-extended minimum 0 maximum 12
vdc VOZ id 3
  limit-resource module-type m1 m1x1 m2x1 f2e
  cpu-share 5
  boot-order 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource monitor-session-erspan-dst minimum 0 maximum 23
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 8 maximum 8
  limit-resource u6route-mem minimum 4 maximum 4
  limit-resource m4route-mem minimum 8 maximum 8
  limit-resource m6route-mem minimum 5 maximum 5
  limit-resource monitor-session-inband-src minimum 0 maximum 1
  limit-resource anycast_bundleid minimum 0 maximum 16
  limit-resource monitor-session-mx-exception-src minimum 0 maximum 1
  limit-resource monitor-session-extended minimum 0 maximum 12
vdc impresoras id 4
  limit-resource module-type m1 m1x1 m2x1 f2e
  cpu-share 5
  boot-order 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource monitor-session-erspan-dst minimum 0 maximum 23
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 8 maximum 8
  limit-resource u6route-mem minimum 4 maximum 4
  limit-resource m4route-mem minimum 8 maximum 8
  limit-resource m6route-mem minimum 5 maximum 5
  limit-resource monitor-session-inband-src minimum 0 maximum 1
  limit-resource anycast_bundleid minimum 0 maximum 16
  limit-resource monitor-session-mx-exception-src minimum 0 maximum 1
  limit-resource monitor-session-extended minimum 0 maximum 12
```

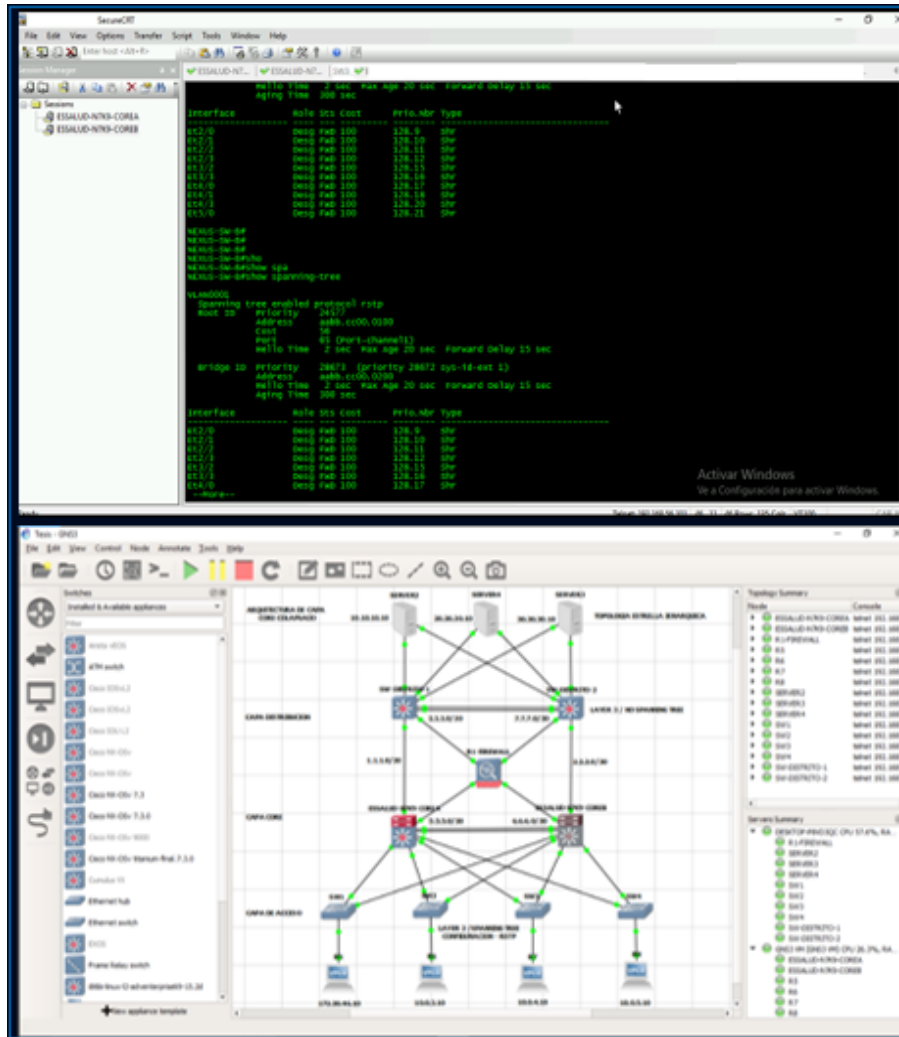
Figura 116. Comandos de la Virtualización de los VDC'S. Fuente: Elaboración Propia (2017).

```
vdc VOZ id 3
  limit-resource module-type m1 m1x1 m2x1 f2e
  cpu-share 5
  boot-order 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource monitor-session-erspan-dst minimum 0 maximum 23
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 8 maximum 8
  limit-resource u6route-mem minimum 4 maximum 4
  limit-resource m4route-mem minimum 8 maximum 8
  limit-resource m6route-mem minimum 5 maximum 5
  limit-resource monitor-session-inband-src minimum 0 maximum 1
  limit-resource anycast_bundleid minimum 0 maximum 16
  limit-resource monitor-session-mx-exception-src minimum 0 maximum 1
  limit-resource monitor-session-extended minimum 0 maximum 12
vdc impresoras id 4
  limit-resource module-type m1 m1x1 m2x1 f2e
  cpu-share 5
  boot-order 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource monitor-session-erspan-dst minimum 0 maximum 23
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 8 maximum 8
  limit-resource u6route-mem minimum 4 maximum 4
  limit-resource m4route-mem minimum 8 maximum 8
  limit-resource m6route-mem minimum 5 maximum 5
  limit-resource monitor-session-inband-src minimum 0 maximum 1
  limit-resource anycast_bundleid minimum 0 maximum 16
  limit-resource monitor-session-mx-exception-src minimum 0 maximum 1
  limit-resource monitor-session-extended minimum 0 maximum 12
```

ESSALUD-N7K9-CoreA#

Figura 117. Comandos de la Virtualización de los VDC'S. Fuente: Elaboración Propia (2017).





- Se logró crear la Máquina Virtual del GNS3 VM para plataforma Windows.
- Se logró crear el IOSv ó IOU Titanium para levantar los dispositivos de los Switches Nexus 7000 de cisco para L2 y L3 en el Mware.
- El periodo de gracia de la licencia que te dan es de 120 días solo para crear un Solo VDC como Demo.
- Se logró crear la Virtualización de 3 VDC's como lo pueden apreciar en el trabajo presentado, cabe recalcar que la licencia por cada VDC tiene un costo.
- Se logró comprobar la conectividad total de Extremo a Extremo desde los Servidores de la capa de Core y Distribución hacia los dispositivos finales que se encuentran en la capa de Acceso en la Arquitectura de Red de Capa de Core Colapsado.
- Se logra visualizar en el Emulador GNS3 los Cisco NX-OSv Titanium-Final.7.3.0 y los Cisco Nx-Osv 7.3.0 Switches Nexus 7000 donde se ha diseñado la Topología Estrella Jerárquica.
- Se visualiza los comandos de las configuraciones realizadas con los protocolos EIGRP (Enhanced Internal Gateway Routing Protocol) y RSTP (Rapid Spanning Tree) que a través de ellos se logrará mayor capacidad de VLAN'S, convergencia y performance de la Red LAN, soporte de enlaces troncales que corran a 10/40/100 GB. en un mismo chasis que equivalen a tener 8 sistemas operativos independientes.

Figura 118. Demostración de la Virtualización de los Conmutadores Nexus 7000 de Cisco. Fuente: Elaboración Propia (2017).



```

Vlan type: rtr => Router Vlan, reserved for rtr-port IP Interface
          stree
          mble  src
vlan type admin oper lxl flst auth ip ipx tag lrn name
-----
  1  std  on   on   on   on   off  on  NA  off  on  VLAN 1
  2  std  on   on   on   on   off  on  NA  off  on  Server-Voz
  9  std  on   off  on   on   off  on  NA  off  on  Wan-Backup-Tdp
 10  std  on   on   off  off  off  on  NA  off  on  Enlace-Sede-Central
100  std  on   on   on   on   off  on  NA  off  on  Datos_Gab_A
101  std  on   off  on   on   off  off  NA  off  on  Voz_Gab_A
102  std  on   off  on   on   off  off  NA  off  on  Impresoras_Gab_A
110  std  on   on   on   on   off  on  NA  off  on  Datos_Gab_C
111  std  on   off  on   on   off  off  NA  off  on  Voz_Gab_C
112  std  on   on   on   on   off  on  NA  off  on  Impresoras_Gab_C
120  std  on   on   on   on   off  on  NA  off  on  Datos_Gab_B3
121  std  on   off  on   on   off  off  NA  off  on  Voz_Gab_B3
122  std  on   on   on   on   off  on  NA  off  on  Impresoras_Gab_B3
130  std  on   on   on   on   off  on  NA  off  on  Datos_Gab_A1
131  std  on   off  on   on   off  off  NA  off  on  Voz_Gab_A1
132  std  on   on   on   on   off  on  NA  off  on  Impresoras_Gab_A1
140  std  on   on   on   on   off  on  NA  off  on  Datos_Gab_C1
141  std  on   on   on   on   off  off  NA  off  on  Voz_Gab_C1
142  std  on   off  on   on   off  off  NA  off  on  Impresoras_Gab_C1
150  std  on   on   on   on   off  on  NA  off  on  Datos_Gab_I1
151  std  on   on   on   on   off  on  NA  off  on  Voz_Gab_I1
152  std  on   off  on   on   off  on  NA  off  on  Impresoras_Gab_I1
160  std  on   on   on   on   off  on  NA  off  on  Datos_Gab_I2
161  std  on   off  on   on   off  off  NA  off  on  Voz_Gab_I2
162  std  on   on   on   on   off  on  NA  off  on  Impresoras_Gab_I2
170  std  on   on   on   on   off  on  NA  off  on  Datos_Gab_G
171  std  on   off  on   on   off  off  NA  off  on  Voz_Gab_G
172  std  on   off  on   on   off  on  NA  off  on  Impresoras_Gab_G
173  std  on   off  on   on   off  off  NA  off  on  Wireless_Gab_G
180  std  on   on   on   on   off  on  NA  off  on  Datos_Gab_F
182  std  on   on   on   on   off  on  NA  off  on  Impresoras_Gab_F
190  std  on   on   on   on   off  on  NA  off  on  Datos_Gab_M
191  std  on   off  on   on   off  off  NA  off  on  Voz_Gab_M
192  std  on   on   on   on   off  on  NA  off  on  Impresoras_Gab_M
200  std  on   on   on   on   off  on  NA  off  on  Datos_Gab_B1
221  std  on   off  on   on   off  off  NA  off  on  Voz_Gab_D
230  std  on   on   on   on   off  on  NA  off  on  Datos_Gab_G3
240  std  on   on   on   on   off  on  NA  off  on  Datos_Gab_J
241  std  on   on   on   on   off  on  NA  off  on  Voz_Gab_J
242  std  on   on   on   on   off  on  NA  off  on  Impresoras_Gab_J
250  std  on   on   on   on   off  on  NA  off  on  Datos_Gab_K
251  std  on   on   on   on   off  on  NA  off  on  Voz_Gab_K
252  std  on   on   on   on   off  on  NA  off  on  Impresoras_Gab_K
260  std  on   on   on   on   off  on  NA  off  on  Datos_Gab_L
262  std  on   on   on   on   off  on  NA  off  on  Impresora_Gab_L
270  std  on   on   on   on   off  on  NA  off  on  Datos_Gab_N
272  std  on   on   on   on   off  on  NA  off  on  Impresoras_Gab_N
280  std  on   off  on   on   off  off  NA  off  on  Datos_Gab_N1
282  std  on   off  on   on   off  off  NA  off  on  Impresoras_Gab_N1
450  std  on   on   on   on   off  on  NA  off  on  Voz-0
451  std  on   on   on   on   off  on  NA  off  on  Voz-1
452  std  on   on   on   on   off  on  NA  off  on  Voz-2
500  std  on   on   on   on   off  on  NA  off  on  Camaras_vigilancia
510  std  on   on   on   on   off  on  NA  off  on  Imagenes_Packs
530  std  on   on   on   on   off  on  NA  off  on  Marcadores_biotricos
540  std  on   on   on   on   off  on  NA  off  on  Server
999  std  on   on   on   on   off  on  NA  off  on  Admin_Switches
    
```

Figura 119. Reporte en S.O. Linux de las VLAN'S Vel VDC1 del Core Nexus 7000 HNERM EsSALUD. Fuente: OSI HNERM EsSALUD (2017).



Tabla 35

Consolidado del Ancho de Banda y Trafico del Performance de la Red LAN del HNERM EsSALUD Años 2016 y 2017

Fecha-Inicio	Hora-Inicio	Fecha-Fin	Hora-Fin	Tiempo (Días)	Tiempo (Hrs)	Usuarios Afectados	T.UNICAST	T.MULTICAST	T.BROADCAST	Ancho de Banda	Cargas BPS	Cargas Packets	Motivo
02/02/2016	15:45:00	02/02/2016	4:32:00 PM	0	0:47:00	1210.00	31.6%	9.8%	58.6%	2.2%	22,552Mbps	2M	Loop GDS-C1
21/04/2016	10:25:00	21/04/2016	10:48:00 AM	0	0:23:00	618.00	18.3%	9.3%	72.4%	6.3%	63,663Mbps	6M	Loop GDS-C2
22/04/2016	16:00:00	22/04/2016	4:33:00 PM	0	0:33:00	900.00	42.4%	52.0%	5.6%	51.4%	554,663Mbps	52M	Loop GDS-C1
22/04/2016	13:21:00	25/04/2016	1:25:00 PM	3	0:04:00	869.00	40.2%	50.0%	5.0%	50.2%	550,552Mbps	52M	Loop GDS-C2
16/05/2016	11:25:00	16/05/2016	12:30:00 PM	0	1:05:00	1200.00	50.6%	36.4%	13.0%	41.1%	441,668 Mbps	442K	Anomalia Trafico Multicast a consecuencia de
19/05/2016	8:25:00	19/05/2016	9:43:00 AM	0	1:18:00	950.00	3.5%	92.9%	3.6%	93.1%	993,630 Mbps	4346K	Anomalia Trafico Multicast a consecuencia de
14/07/2016	9:15:00	14/07/2016	1:02:00 PM	0	3:47:00	1250.00	42.4%	52.0%	5.6%	51.4%	554,663Mbps	52M	Anomalia Trafico Multicast a consecuencia de
04/08/2016	13:15:00	04/08/2016	2:00:00 PM	0	0:45:00	1100.00	3.3%	95.8%	0.9%	99.7%	998,740 Mbps	4586K	Anomalia Trafico Multicast a consecuencia de
16/08/2016	13:10:00	16/08/2016	2:15:00 PM	0	1:05:00	1600.00	4.9%	93.4%	1.7%	100%	1 Gbps	4609K	Anomalia Trafico Multicast a consecuencia de
17/08/2016	14:23:00	17/08/2016	2:25:00 PM	0	0:02:00	1600.00	4.1%	94.6%	1.3%	98.9%	988,687 Mbps	4557K	Anomalia Trafico Multicast a consecuencia de
22/08/2016	13:50:00	22/08/2016	2:15:00 PM	0	0:25:00	1300.00	86.6%	12.8%	0.6%	77.3%	772,557 Mbps	3394K	Anomalia Trafico Multicast a consecuencia de
29/08/2016	12:10:00	29/08/2016	1:15:00 PM	0	1:05:00	1450.00	14.1%	12.2%	73.7%	66.8%	668,084 Mbps	1846K	Trafico Broadcast en VLAN 1
01/09/2016	9:02:00	01/09/2016	9:45:00 AM	0	0:43:00	1300.00	8.9%	29.5%	3.9%	27.0%	270,334Mbps	1786K	Anomalia Trafico Multicast a consecuencia de
01/09/2016	13:52:00	01/09/2016	2:08:00 PM	0	0:16:00	1200.00	40.0%	29.5%	1.0%	76.1%	761,054Mbps	3078K	Anomalia Trafico Multicast a consecuencia de
07/09/2016	12:45:00	07/09/2016	12:48:00 PM	0	0:03:00	1300.00	42.4%	52.0%	5.6%	51.4%	554,663Mbps	52M	Loop GDS-N
28/09/2016	12:05:00	28/09/2016	12:32:00 PM	0	0:27:00	1800.00	14.1%	12.1%	73.7%	66.8%	668,084 Mbps	1846K	Trafico Broadcast en VLAN 1
28/06/2017	10:00:00	28/06/2017	11:00:00 AM	0	1:00:00	1801.00	60.0%	32.0%	8.0%	70.2%	702,020 Mbps	1886K	Trafico Broadcast en VLAN 1
30/06/2017	7:55:00	30/06/2017	8:25:00 AM	0	0:30:00	1802.00	-	-	-	-	-	-	Corte de Fluído Eléctrico

Fuente: Elaboración Propia (2017).

Nota: En el presente cuadro se muestra la medición del consolidado de la bitácora de caídas del conmutador (CORE Principal), donde se detalla el tiempo de inactividad en número de días, horas, ancho de banda consumido, principales cargas en Mbps y pkts. y usuarios afectados.

- El año 2016 presentó 16 caídas de red con un tiempo de inactividad de 12 horas con 48 minutos, el mismo que afectó a un promedio 1,227 usuarios.
- Para el año 2017 mes de junio se han presentado 2 caídas de red, las mismas que ocasionaron un tiempo de inactividad de 01 hora con 30 minutos afectando a un total de 1,801 usuarios.



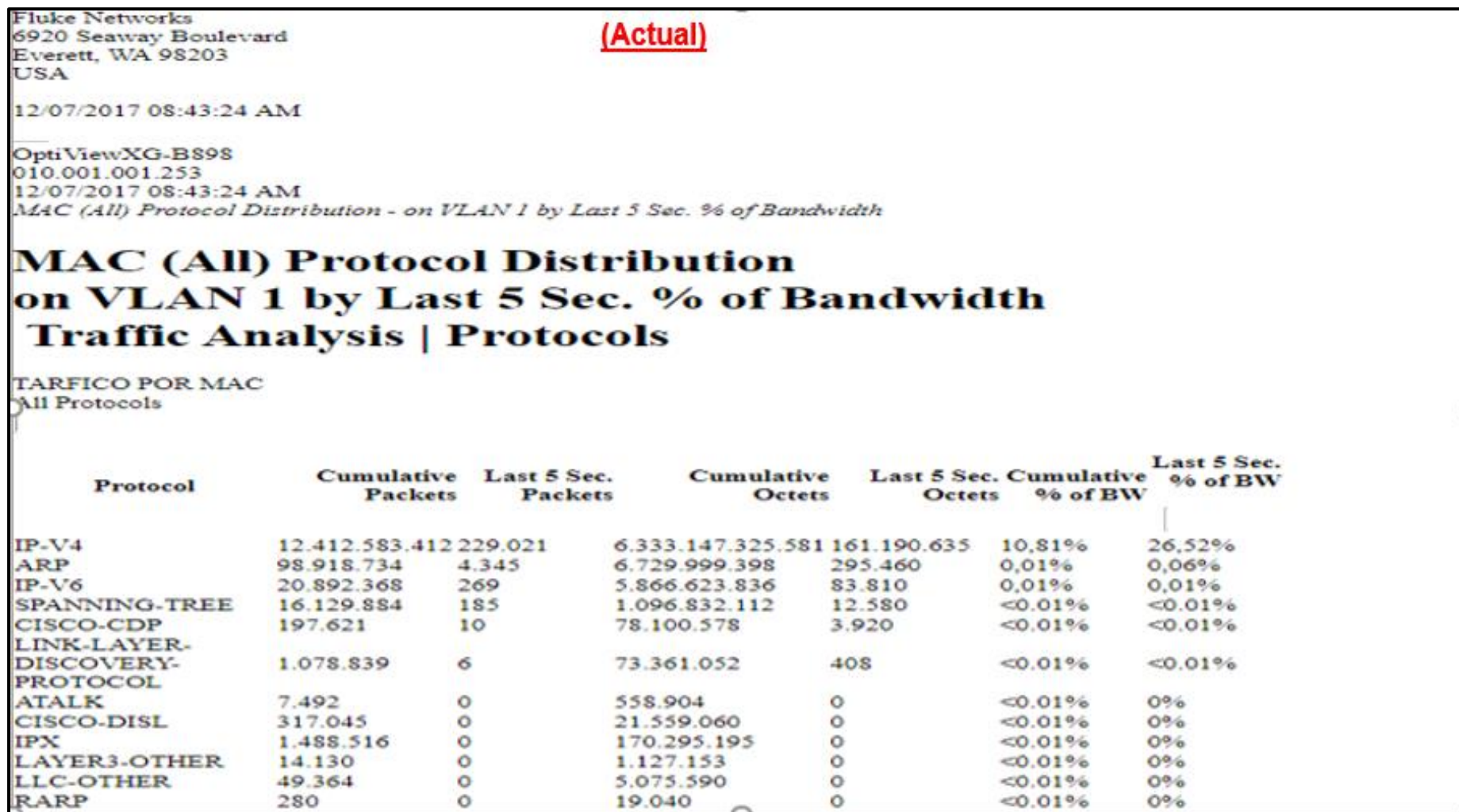


Figura 120. Reporte de Trafico por MAC de todos los Protocolos. Fuente: OSI HNERM EsSALUD (2017).



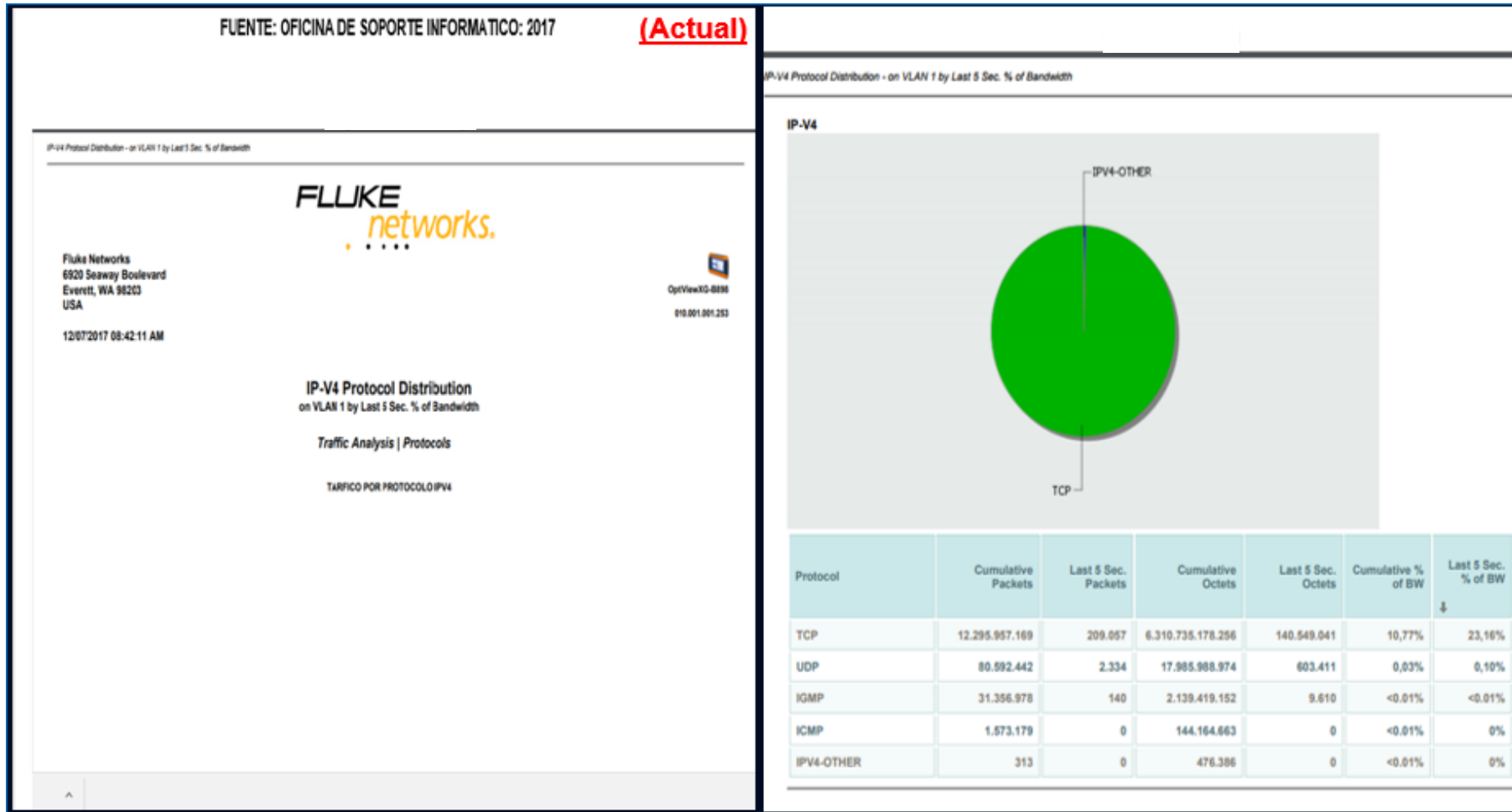


Figura 121. Cuadro Estadístico del Reporte de Trafico por MAC de todos los Protocolos. Fuente: OSI HNERM EsSALUD (2017).



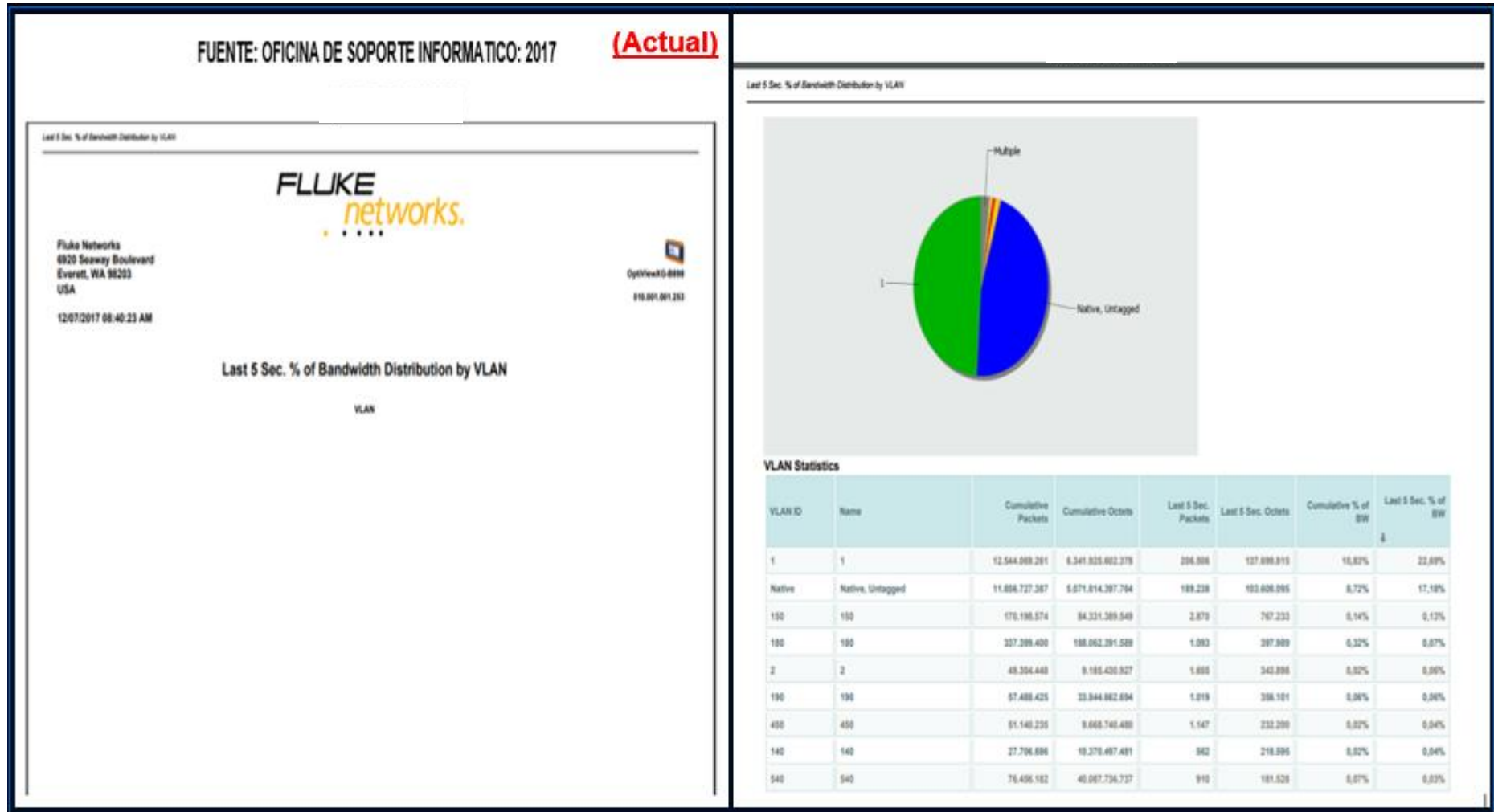


Figura 122. Cuadro Estadístico del Reporte de Trafico por VLAN'S. Fuente: OSI HNERM EsSALUD (2017).



(Sistemas Actuales)



Figura 123. Funcionamiento de los Sistemas y Aplicativos en los Diferentes Servicios del HNERM EsSALUD. Fuente: OSI HNERM EsSALUD (2017).



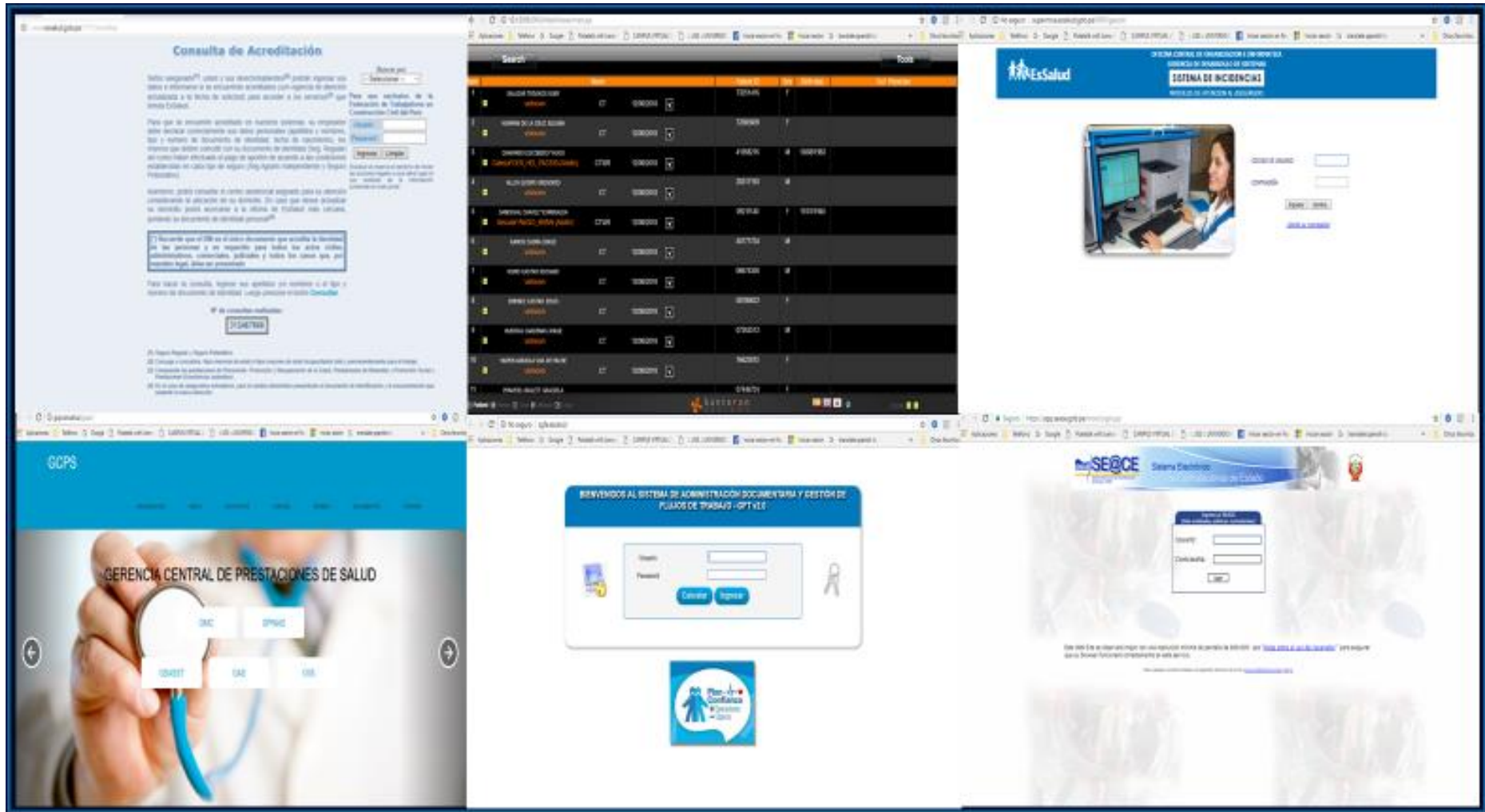


Figura 124. Funcionamiento de los Sistemas y Aplicativos en los Diferentes Servicios del HNERM EsSALUD. Fuente: OSI HNERM EsSALUD (2017).



NX-OS 6.2 Freetown – Software Highlights Scale Improvement Targets (Sup2E)

Feature	Today	NX-OS 6.2
VPC multicast routes	15,000	25,000
VRF / MPLS Layer 3 VPN	1,000	4,000
BGP peers	1,000	2,000
OTV (sites, VLAN, MAC)	6 / 256 / 32,000	10 / 2,000 / 32,000
FabricPath (switchID / VLAN)	256/ 4000	512 / 4,000
Static routes	1,000	8,000
FEX (# of modules and # of server ports)	48 and 2048	64 and 3072

Notes:

- ❖ Scale improvements are targeted for Supervisor 2E. Supervisor 1/2 will largely remain at current scale with exceptions where higher scale can be achieved.
- ❖ Check Nexus 7000 Verified Scalability Guide after NX-OS 6.2 FCS for more details

Figura 125. Razones porque usar Tecnología Cisco Switch Nexus 7000. Fuente: Cisco (2016).



Figura 126. Razones porque usar Tecnología Cisco Switch Nexus 7000. Fuente: Cisco (2016).



Playbook de Soluciones para la Industria: Banca y Finanzas

Resumen | Cliente | Solución | Metodología | Experiencia

Tamaño del Mercado de la Industria de Banca y Finanzas

Presentamos los ingresos referenciales y esperados por Cisco en los diversos sectores, podemos observar que los Servicios Financieros son el segundo sector en inversión de TI en Latinoamérica (LATAM); siendo UCS la tecnología que mayores ingresos percibió en dicho sector.

TAM de Cisco por Sector (en Millones) en la región LATAM.
Fuente: Cisco Global Market

SECTOR	2011	2012	2013	2014	2015
Proveedor de Servicios	\$ 2.465	\$ 2.666	\$ 2.782	\$ 2.972	\$ 3.178
Servicios Financieros	\$ 898	\$ 976	\$ 1.052	\$ 1.125	\$ 1.198
Manufactura	\$ 505	\$ 552	\$ 604	\$ 660	\$ 721
Gobierno	\$ 421	\$ 449	\$ 482	\$ 516	\$ 546
Energía	\$ 291	\$ 317	\$ 342	\$ 369	\$ 392
Servicios Profesionales	\$ 277	\$ 302	\$ 321	\$ 342	\$ 361
Servicios Técnicos	\$ 197	\$ 215	\$ 235	\$ 253	\$ 267
Educación	\$ 200	\$ 210	\$ 219	\$ 229	\$ 239
Comercio	\$ 175	\$ 180	\$ 188	\$ 193	\$ 197
Servicios a Personas	\$ 168	\$ 177	\$ 187	\$ 195	\$ 203
Transporte	\$ 95	\$ 103	\$ 109	\$ 115	\$ 121
Salud	\$ 60	\$ 66	\$ 71	\$ 77	\$ 82
Entretenimiento	\$ 58	\$ 61	\$ 62	\$ 61	\$ 62
Hoteles & Ocio	\$ 30	\$ 34	\$ 39	\$ 43	\$ 47
TOTAL	\$ 5.839	\$ 6.309	\$ 6.693	\$ 7.151	\$ 7.615

TAM de Cisco por Tecnología (en Millones) en la región LATAM del Sector Financiero.
Fuente: Cisco Global Market

TECNOLOGÍA	2011	2012	2013	2014	2015
Otras Tecnologías Cisco	\$ 677	\$ 743	\$ 812	\$ 878	\$ 940
Unified Computing Systems (UCS)	\$ 220	\$ 234	\$ 240	\$ 247	\$ 258
TOTAL	\$ 898	\$ 976	\$ 1.052	\$ 1.125	\$ 1.198

©2013 Cisco Systems, Inc. Todos los derechos reservados. Documento Confidencial. Solo para uso interno y para partners.

Figura 127. Razones porque usar Tecnología Cisco Switch Nexus 7000. Fuente: Cisco (2016).

Esta Arquitectura funciona de manera Homogénea en todo el portafolio Cisco?

Red Cableada

Table 1 Supported Network Access Devices

Device	Minimum OS Version ¹	MAB	802.1X	Web Auth	Session CoA	VLAN	DACL	SGA
Access Switches								
Catalyst 2940	IOS v12.1(22)EA1	Yes	Yes	No	No	Yes	No	No
Catalyst 2950	IOS v12.1(22)EA1	No	Yes	No	No	Yes	No	No
Catalyst 2955	IOS v12.1(22)EA1	No	Yes	No	No	Yes	No	No
Catalyst 2960, Catalyst 2960S, ISR EtherSwitch ES2	IOS v12.2(52)SE LAN Base	Yes	Yes	Wireless LAN Controller (WLC) 2100, 4400, and 5500 Series		7.0.116.0	No	Yes
Catalyst 2960, Catalyst 2960S	IOS v12.2(52)SE LAN Lite ²	Yes	Yes	WISM Blade for 6500		7.0.116.0	No	Yes
Catalyst 2970	IOS v12.2(25)SE	Yes	Yes	WLC for ISR (ISR2 ISM, SRE700, and SRE900)		7.0.116.0	No	Yes
Catalyst 2975	IOS v12.2(52)SE	Yes	Yes	WLC for 3750		7.0.116.0	No	Yes
Catalyst 3550	IOS v12.2(44)SE	Yes	Yes	Wireless LAN Controller (WLC) do not support downloadable ACLs (dACLs), but support named ACLs. WLCs prior to release 7.0.116.0 do not support CoA and require deployment of an ISE Inline Posture Node to support posture services. Use of Inline Posture Node requires WLC version 7.0.98 or later. Autonomous AP deployments (no WLC) also require deployment of an Inline Posture Node for posture support. Profiling services are currently supported for 802.1X-authenticated WLANs only on the WLC with CoA support. HREAP is not supported. WLCs do not currently support MAC Authentication Bypass (MAB).				
Catalyst 3560	IOS v12.2(52)SE	Yes	Yes	An issue has been observed during wireless login scenarios where the WLC is running firmware version 7.0.116.0. Unless you require new features available only in version 7.0.116.0, Cisco recommends returning your WLC firmware version to 7.0.98.218. For more information, see the Release Notes for the Cisco Identity Services Engine, Release 1.0.4.				

Red Inalámbrica

Wireless (An ISE Inline Posture node is required if the WLC does not support CoA as discussed in Footnote #4. WLCs with the code specified in this table do support CoA without an ISE Inline Posture node) #3

¹ For 802.1X authentications, you need IOS version 12.2(55)SE3.
² Does not support posture and profiling services.
³ SGA only
⁴ An issue has been observed during wireless login scenarios where the WLC is running firmware version 7.0.116.0. Unless you require new features available only in version 7.0.116.0, Cisco recommends returning your WLC firmware version to 7.0.98.218. For more information, see the Release Notes for the Cisco Identity Services Engine, Release 1.0.4.

http://www.cisco.com/en/US/docs/security/ise/1.0.4/compatibility/ise104_sdt.html

Alcatel-Lucent Enterprise

Copyright © 2013 Alcatel-Lucent. All rights reserved.

Figura 128. Razones porque usar Tecnología Cisco Switch Nexus 7000. Fuente: Cisco (2016).



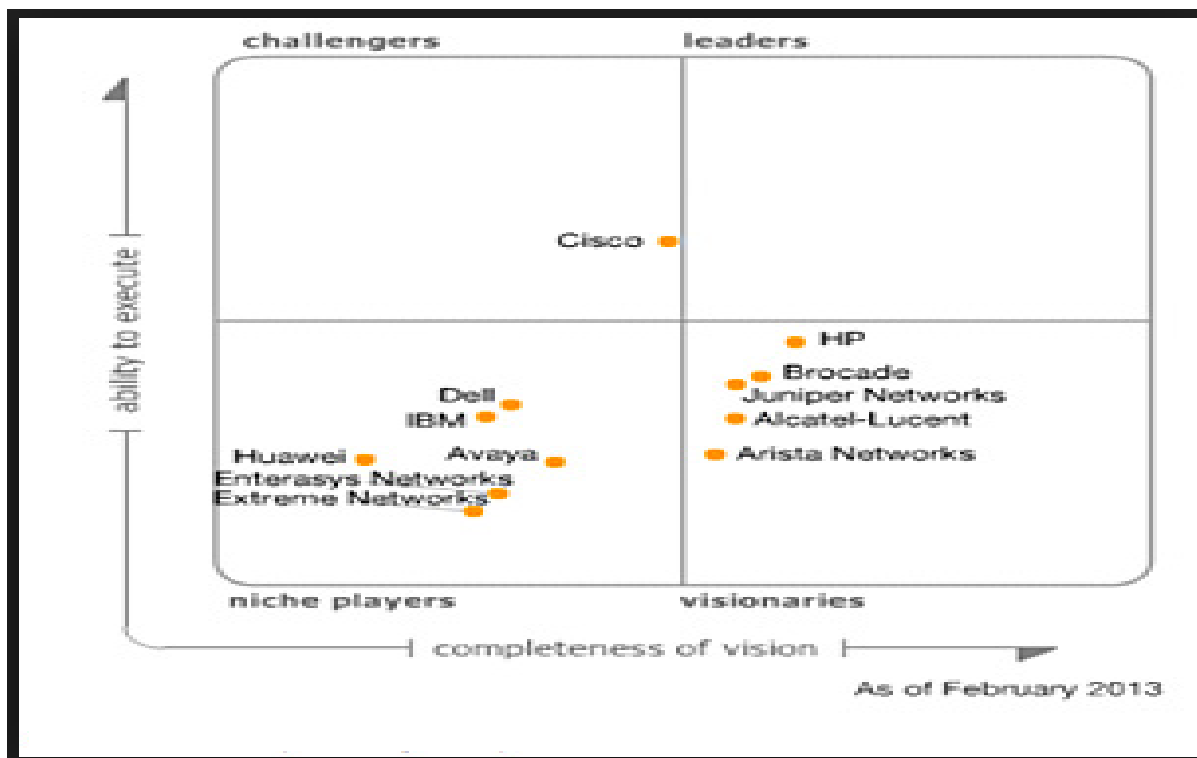


Figura 129. Cisco Líder en Tecnología. Fuente: Gartner (2013).

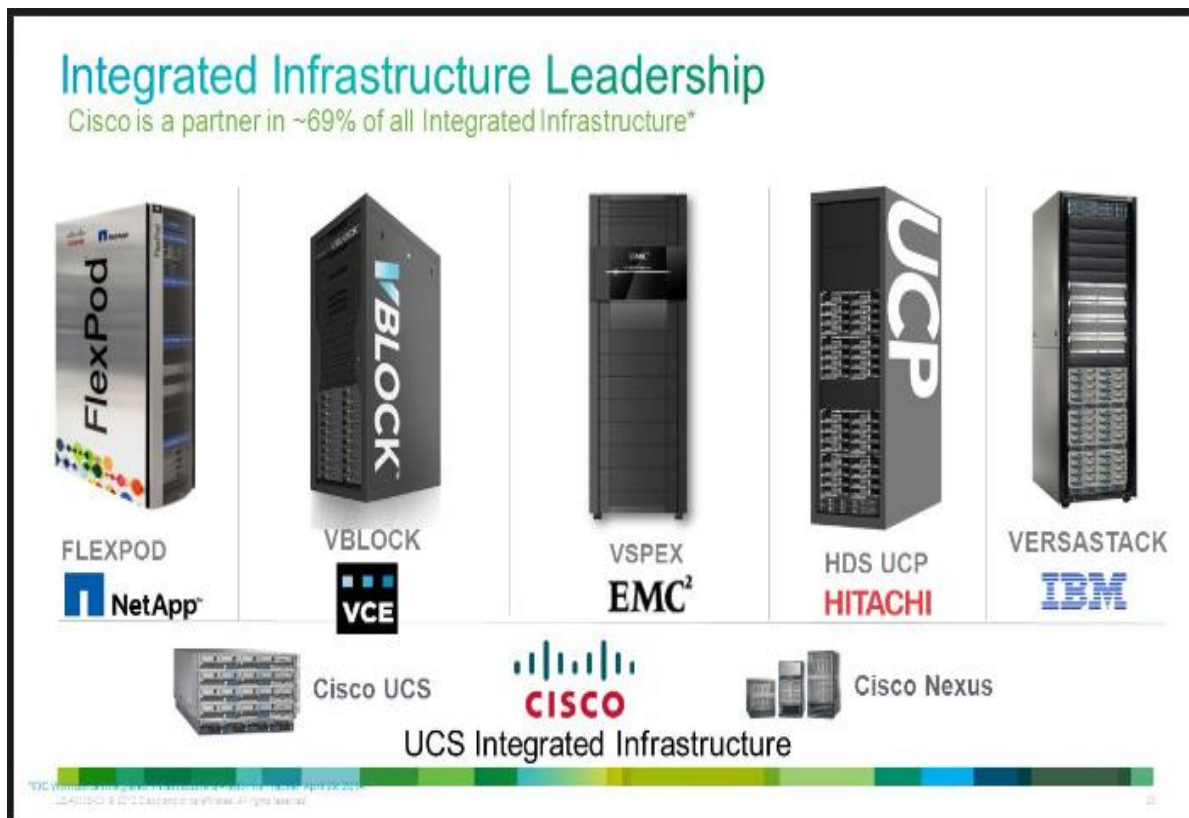


Figura 130. Cisco Líder en Integrar Infraestructura. Fuente: Cisco (2016).



CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

3.1. Conclusiones

En base a los objetivos propuestos en la presente investigación se describen las siguientes conclusiones generales:

- a. Se desarrolló la propuesta de diseño de arquitectura de Red de Alto Nivel haciendo uso de Virtualización de Dispositivos de Conmutación de la Red LAN en el HNERM-EsSALUD.
- b. Se desarrolló el plan de segmentación la Red LAN a través de la implementación de Redes de Área Local Virtual (Virtual Local Area Network) por tipo de servicio (Voz, Datos, Video, Impresión, Imágenes Pac's, WIFI).
- c. Se desarrolló la propuesta de los niveles de Seguridad de la red LAN a través de reglas, regulaciones y políticas por puerto, Vlans y protocolos a fin de mitigar las vulnerabilidades a posibles ataques en la Red.

3.2. Recomendaciones

Detallamos las siguientes recomendaciones generales:

- a. Se puede aplicar este desarrollo de propuesta de virtualización de los dispositivos de conmutación porque permitirá mejorar el performance de los servicios de la Red LAN del HNERM-EsSALUD, diseñando una arquitectura de Red de Alto Nivel, segmentación de la Red LAN por VLAN y niveles de seguridad de la Red LAN a través de reglas, regulaciones y políticas por puerto, Vlans y protocolos a fin de mitigar las vulnerabilidades a posibles ataques en la Red, asimismo se justifica metodológicamente, cómo se aborda la investigación la misma que servirán como referencia para otras Organizaciones e instituciones como: las EPS, APP y Clínicas Privadas Contratadas que tienen convenios Prestacionales con el HNERM-EsSALUD.
- b. Se recomienda al Ministerio de Salud MINSa aplicar la Metodología Lifecycle Services Cisco ya que el enfoque de Lifecycle Services de Cisco define el conjunto mínimo de actividades necesarias, por tecnología y por nivel de complejidad de la red, para ayudar a los clientes a instalar y operar exitosamente tecnologías de Cisco, y optimizar su desempeño a través del ciclo de vida de la red como también la adquisición de los Switches Cisco Nexus 7000 que son la última extensión de los conmutadores modulares de la serie Cisco Nexus 7000, esto será a Nivel Local y Regional.
- c. Se recomienda a las Clínicas Privadas de Nivel II que la presente propuesta es una buena alternativa de solución que les permitirá mejorar significativamente el desempeño de los servicios de la Red LAN y sus sistemas institucionales, mejorando la atención de sus servicios, logrando satisfacer a sus Usuarios asistenciales, administrativos y a su población asegurada, optimizando sus costos y recursos humanos, donde la criticidad de los servicios es absoluta, por último contribuye a la humanización de los servicios de salud, a la consolidación de una organización sólida, con una buena gestión que logrará fidelizar al paciente que se convertirá en un cliente frecuente.



Referencias

- Andrés, S. (2003). *Redes de Computadoras (4ª edición) publicada por Pearson Education*. Usa Inc., publicada como: Prentice-Hall Inc., copyright © 2003.
- Anixer, (2006). *Estándar Reference Guide*. Usa.
- Barrio, et. al. (2011). *Redes Integradas de Servicios de Salud: el Desafío de los Hospitales.*, Santiago, Chile: Ops/Oms, 2011.
- Bravo, Y. (2013). *Cableado Estructurado definiciones básicas I y II (Sce- fundamentos 1-2013.pdf - Sce-fundamentos 2-2013.pdf).*, Perú.
- Bautista, J. (2017). *Glosario Redes de Computadoras ~ Red Cisco, CCNA Certification*: Usa:<https://es.scribd.com/document/352428127/Glosario-Redes-de-Computadoras-Red-Cisco-CCNA-Certification>.
- Cisco. (2016). *Cisco y VMware Innovar virtualización.*, Usa: [http : // www.cisco.com/c/en/us/solutions/data-center-virtualization/server_virtualization-vmware/index.html](http://www.cisco.com/c/en/us/solutions/data-center-virtualization/server_virtualization-vmware/index.html).
- Cisco. (2014). *Resumen de diseño de la red Lan cableada del campus.*, Usa: editado ©2013 Cisco Systems, Inc. todos los derechos reservados.
- Cisco. (2006). *Metodología LifeCycle Services de Cisco*, Usa: http://www.cisco.com/c/dam/global/es_mx/assets/serviciospartners/otros_archivos/pdf/brochurelcsp_esp2006.pdf.
- Díaz Alvear, P. A. (2010). *Diseño e implementación de una red privada virtual para la Empresa Eléctrica Quito S.A., matriz las casas, para la transmisión de datos de voz sobre IP.*, Quito/EPN/2010.
- Espinoza E., Lobatón L. (2014). *Implementación de virtualización en el centro de cómputo de la oficina de tecnología de información del Ministerio de Transportes y Comunicaciones.*,<http://www.repositorioacademico.usmp.edu.pe/handle/usmp/1027>.


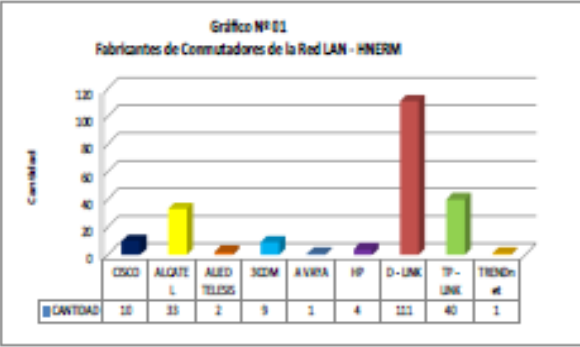


- Gili, G. (2001). *La An-estética de la Arquitectura de Neil Leach* by Peter Krieger.*, Barcelona-México: Editado ©2016 Universidad Nacional Autónoma de México, Revista Anales del Instituto de Investigaciones Estéticas Issn1870-3062.
- Jaurapoma, G. (2015). *Propuesta de Virtualización de Escritorios dirigido a Instituciones Educativas.*, Lima, Perú., Universidad Nacional Mayor de San Marcos Facultad de Ingeniería Industrial E.A.P. de Ingeniería Industrial., <http://cybertesis.unmsm.edu.pe/handle/cybertesis/4612>
- Lévy, P. (1995). *¿Qué es lo virtual? En P. Lévy, (pág. 10).*, Buenos Aires: Editorial Paidós, Saicf.
- Moerbeck, M. (2015). *Información sobre administración de la virtualización de última generación.*, Latín América. <http://www.vmware.com/go/Expand-Paper>.
- Molina R, Julio E. (2012). *Propuesta de segmentación con redes virtuales y priorización del ancho de banda con QoS para la mejora del rendimiento y seguridad de la red LAN en la Empresa Editora El Comercio Planta Norte".* Chiclayo, Perú., Tesis de pregrado, Universidad Católica Santo Toribio de Mogrovejo.
- Puga M., Diego A. (2015). *Rediseño y optimización de la red de voz y datos del Centro de Convenciones Eugenio Espejo. Facultad de Ingenierías y Ciencias Agropecuarias.* UDLA. Quito. 101 p.
- Ramírez, M. (2015). *Segmentación de La Red Y Priorización Del Ancho De Banda Para Mejorar El Rendimiento Y Seguridad La Universidad Nacional De San Martín – Tarapoto.* Perú. <https://studylib.es/doc/8307550/mirko-ram%C3%ADrez-rodr%C3%ADguez---repositorio-de-tesis-unsm-t>.
- Rivero G., Yeraldy C. (2006). *Análisis de tráfico de la red del servicio de la administración aduanera del estado ZuliaTélématique, vol. 5, núm. 2, 2006, p. 1*Universidad Privada Dr. Rafael Beloso Chacín Zulia, Venezuela

ANEXOS

ANEXO 1: CONMUTADORES

Fotos del 1 al 22

14. CONMUTADORES ES. (SISTEMAS DE CONECTIVIDAD).																																						
CANT.	COMENTARIOS	OBJETIVO VISUAL																																				
4	Vista Frontal / Posterior / Vista Oblicua (45° sexagesimales), Panorámica, y que se visualice la marca, modelo y puertos usados).	Ubicación del Conmutadores , Grado de ocupabilidad de puertos, marca, modelo,																																				
FOTO 1 – VISTA FRONTAL																																						
																																						
COMENTARIOS																																						
<p>PROPIO (X)</p> <p>MARCA: Alcatel, Cisco, D-Link, TP-Link, 3com, Allied Telesis, HP, Avaya, TRENDnet</p> <p>MODELO: OS 9800, OS 6224P, DGS1210, DGS1510, DES 1024A, DES 1024D.</p> <p>TECNOLOGIA: UP LINK, POE, L2 - L3, STAND-ALONE</p> <p>DESCRIPCION: El hospital Rebagliati actualmente cuenta con una infraestructura de comunicaciones totalmente obsoleta la misma que tiene aproximadamente 12 años:</p>		<p>Comentario: El equipamientos de comunicaciones el 100 % ha cumplido su vida útil, (12 años), de los cuales 44% son administrables y el 55% son Stan alone (hub), con una trasmisión de 100 mbps, así mismo existen diversidad de marcas (09 marcas) lo que dificulta la administración de los mismos.</p> <p>El 70 % de equipos de comunicaciones presenta errores lógicos a nivel de interfaces de red tales como desbordamiento de base de datos, apagado de puertos, falla de fuente de poder, lo que genera intermitencia en la red y caída de los sistemas afectando la atención al asegurado.</p> <p>Para cubrir la demanda de nuevos puntos de red, se han habilitado de manera provisional e improvisada nodos de red en áreas de trabajo, los mismos que no brindan las condiciones técnicas para el óptimo funcionamiento toda vez que son de uso doméstico los mismos que causan degradación del performance de la red LAN exponiendo a los equipos de networking.</p> <p>Actualmente la infraestructura de comunicaciones no cuenta con redundancia lo que no garantiza la continuidad operativa del servicio en caso de emergencias o desastres, teniendo en cuenta que el hospital Rebagliati tiene el máximo nivel de atención siendo el referente del Seguro Social.</p> <p>La centralización de compras de equipos activos (Parque informático) por parte de GCTIC sede central no permite atender los nuevos requerimientos de los proyectos contemplados con los avances de la telemedicina (renovación tecnológica de equipos biomédicos de alta tecnología).</p> <p>La renovación de equipos de comunicaciones debe ser planificado cumpliendo estrictamente lo establecido por el fabricante (vida útil) toda vez que el hospital trabaja 24x7x365 siendo la necesidad absoluta y la criticidad es máxima.</p>																																				
<table border="1"> <thead> <tr> <th>MARCA</th> <th>CISCO</th> <th>ALCATEL</th> <th>ALIED TELESIS</th> <th>3COM</th> <th>A AVAYA</th> <th>HP</th> <th>D-LINK</th> <th>TP-LINK</th> <th>TRENDnet</th> </tr> </thead> <tbody> <tr> <td>CANTIDAD</td> <td>10</td> <td>33</td> <td>2</td> <td>9</td> <td>1</td> <td>4</td> <td>111</td> <td>40</td> <td>1</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>CAPA</th> <th>CAPA 3</th> <th>CAPA 2</th> <th>STAND-ALONE</th> </tr> </thead> <tbody> <tr> <td>CANTIDAD</td> <td>2</td> <td>93</td> <td>115</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>SW-3POE</th> <th>SW-POE</th> <th>SW-40 UP-LINK</th> <th>SW-24 UP-LINK</th> </tr> </thead> <tbody> <tr> <td>25</td> <td>10</td> <td>4</td> <td>92</td> </tr> </tbody> </table>		MARCA	CISCO	ALCATEL	ALIED TELESIS	3COM	A AVAYA	HP	D-LINK	TP-LINK	TRENDnet	CANTIDAD	10	33	2	9	1	4	111	40	1	CAPA	CAPA 3	CAPA 2	STAND-ALONE	CANTIDAD	2	93	115	SW-3POE	SW-POE	SW-40 UP-LINK	SW-24 UP-LINK	25	10	4	92	
MARCA	CISCO	ALCATEL	ALIED TELESIS	3COM	A AVAYA	HP	D-LINK	TP-LINK	TRENDnet																													
CANTIDAD	10	33	2	9	1	4	111	40	1																													
CAPA	CAPA 3	CAPA 2	STAND-ALONE																																			
CANTIDAD	2	93	115																																			
SW-3POE	SW-POE	SW-40 UP-LINK	SW-24 UP-LINK																																			
25	10	4	92																																			
<p style="text-align: center;">Gráfico Nº 01 Fabricantes de Conmutadores de la Red LAN - HNERM</p>  <table border="1"> <thead> <tr> <th>MARCA</th> <th>CISCO</th> <th>ALCATEL</th> <th>ALIED TELESIS</th> <th>3COM</th> <th>A AVAYA</th> <th>HP</th> <th>D-LINK</th> <th>TP-LINK</th> <th>TRENDnet</th> </tr> </thead> <tbody> <tr> <td>CANTIDAD</td> <td>10</td> <td>33</td> <td>2</td> <td>9</td> <td>1</td> <td>4</td> <td>111</td> <td>40</td> <td>1</td> </tr> </tbody> </table>		MARCA	CISCO	ALCATEL	ALIED TELESIS	3COM	A AVAYA	HP	D-LINK	TP-LINK	TRENDnet	CANTIDAD	10	33	2	9	1	4	111	40	1																	
MARCA	CISCO	ALCATEL	ALIED TELESIS	3COM	A AVAYA	HP	D-LINK	TP-LINK	TRENDnet																													
CANTIDAD	10	33	2	9	1	4	111	40	1																													

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 2 – VISTA FRONTAL.



COMENTARIOS

PROPIO (X)

MARCA:

Alcatel, Cisco, D-Link, TP-Link, 3com, AlliedTelesis, HP, Avaya, TRENDnet

MODELO:

OS 9800, OS 6224P, DGS1210, DGS1510, DES 1024A, DES 1024D,

TECNOLOGIA:

UP LINK, POE, L2 - L3, STAND-ALONE

DESCRIPCION:

Detalle de la Infraestructura de Comunicaciones.



- En el Gráfico Nº 1 – Fabricantes de conmutadores de la Red LAN – HNERM, El 53 % de los conmutadores predomina el fabricante D-LINK, con el 19 % TP-Link, con 16% Alcatel, con el 5% Cisco y el 7% otras marcas, lo que se puede determinar que el 72% de equipos de marcas D-Link y TP-Link son de uso doméstico, lo que degradan totalmente el performance de la red.

- En el Gráfico Nº 2 – Tipos de Conmutadores Red LAN – HNERM, El 44 % de los conmutadores son Capa 2, es decir administrables los mismos que permiten trabajar con el protocolo 802.1q, también permite controlar el dominio de colisión por puerto independiente a diferencia de los tipo stand-alone que contamos con 55% los cuales trabajan con un solo dominio de colisión, lo cual no es recomendable usar hub en una red tan grande debido que generan constantemente colisiones degradando el performance de la red, así mismo se cuenta con 1% de Conmutadores de CORE, los mismos que trabajan en capa 3.

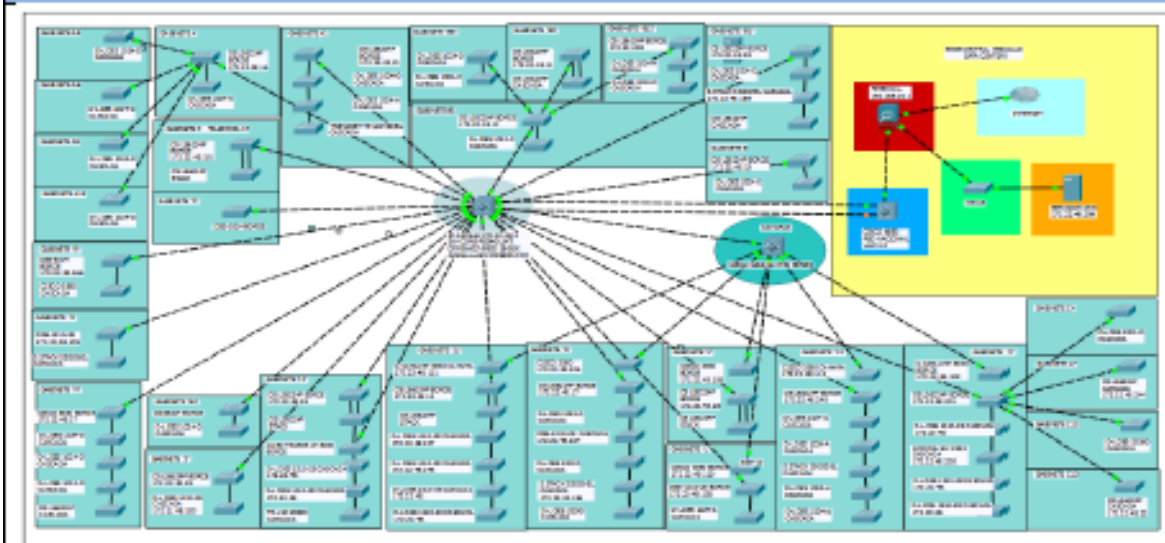
- En el Gráfico Nº 3 – Características de Conmutadores – En GDS, Podemos apreciar que el 29% de Conmutadores marca Alcatel de 24 Puertos cuentan con POE, los mismo que se encuentran configurados como Conmutadores de Borde para la red de datos, El 10 % de los conmutadores marca Cisco de 8 puertos cuentan con POE, de uso exclusivo para las Cámaras de Video, el 66% de conmutadores con UP-Link es decir no cuentan con la tecnología (POE) Power Over Ethernet.

- En el Gráfico Nº 4 –Conmutadores en Áreas de Trabajo – Cascada, predomina los hub de 8 puertos con un 47 %, el 31% hub de 24 puertos, el 11% hub de 4 puertos, 7% hub de 5 puertos y el 4% hub de 16 puertos.

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 3 – CUADRO RESUMEN



Topología de red lógica de la Red LAN del Hospital Nacional Edgardo Rebagliati Martins

SUBNETS	EN 10/100			EN 10/100			EN 10/100			EN 10/100			EN 10/100			N - NEW GARDIAN	N - CALL CENTER	TOTAL - NEW	LAYER 2	LAYER 3	START - ALDOR				
	P - PAREDES	F - FERIA	N - NEW	P - PAREDES	F - FERIA	N - NEW	P - PAREDES	F - FERIA	N - NEW	P - PAREDES	F - FERIA	N - NEW	P - PAREDES	F - FERIA	N - NEW										
A	X			1	24	0	24																		
A01	X			1	24	0	24																		
A03		X																							
A06		X																							
A09		X																							
A12		X																							
B	X			1	24	0	24																		
B1	X			1	24	0	24	1	8	0	8														
B1-5	X			1	18	6	24	1	8	2	8														
B3		X		1	24	0	24																		
B6		X																							
B9		X		2	48	0	48																		
B12		X		1	22	2	24																		
C	X			1	24	0	24	1	8	0	8														
C1	X			1	24	0	24	1	8	0	8	2	96	0	96										
C4		X																							
C7		X		1	20	4	24																		
C10		X																							
C13		X																							
D		X																							
F	X			3	72	0	72																		
F1	X																								
G	X			1	24	0	24	1	8	0	8														
G3		X		1	24	0	24																		
H	X			1	24	0	24	1	8	2	8	2	96	10	96										
H-5		X						1	7	1	8														
I2	X			2	48	0	48																		
J	X	X		1	11	13	24																		
K		X		2	40	8	48	1	4	4	8														
L		X						1	2	8	8														
M	X			2	48	0	48																		
N	X			1	24	0	24																		
N		X						1	2	8	8														
N1		X		3	36	33	72																		
TOTAL	34	13	21	0			29				10			4			62			104	104	208	38	2	116

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 4 – VISTA FRONTAL.



COMENTARIOS

PROPIO (X)	- Equipos que estaban configurados como Conmutadores de borde en distintos segmentos de red, los mismo no contaban con fuente redundante.
MARCA: Alcatel	
MODELO: OS 6224P	
TECNOLOGIA: POE, L2	
DESCRIPCION: Conmutadores de Borde Alcatel Lucent dados de baja por problemas con la fuente de poder, placa y caída de interfaces trocales y puertos de distribución.	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 5 – VISTA FRONTAL.



COMENTARIOS

PROPIO (X)	- Equipos que estaban configurados como Conmutadores de distribución en distintos segmentos de red, los mismos que se adquirieron por caja chica toda vez que los Conmutadores de capa 2 de uso empresarial eleva enormemente los costos.
MARCA: D-LINK	
MODELO: DES-1024D	
TECNOLOGIA: STAND-ALONE	
DESCRIPCION: Conmutadores STAND-ALONE dados de baja por problemas con la fuente de poder, placa y caída de interfaces de distribución.	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 6 – VISTA FRONTAL.



COMENTARIOS

PROPIO (X)	<ul style="list-style-type: none"> - Equipos que estaban configurados como conmutadores de distribución en distintos segmentos de red, los mismos que se adquirieron por caja chica toda vez que los Conmutadores de capa 2 de uso empresarial eleva enormemente los costos. - En la segunda foto se muestra conmutadores de capa 3 dados de baja por problemas de fuente de poder y placa.
MARCA: 3-COM D-LINK	
MODELO: Superstack 5500G-E1 DXS - 3328GSR	
TECNOLOGIA: CAPA 2	
DESCRIPCION: Conmutadores de CAPA 2 y CAPA 3 dados de baja por problemas con la fuente de poder, placa y caída de interfaces trocales y puertos de distribución.	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)





COMENTARIOS

<p>PROPIO (X)</p> <p>MARCA: CISCO D-LINK</p> <p>MODELO: Catalyst 3560 DES-1024D</p> <p>TECNOLOGIA: CAPA 2</p> <p>DESCRIPCION: Conmutadores de CAPA 2 POE y Conmutadores Stand-alone destinados para cámaras de seguridad dados de baja por problemas con la fuente de poder, placa y caída de interfaces trocales y puertos de distribución.</p>	<p>- Equipos que estaban configurados como Conmutadores de distribución en distintos segmentos de red, los mismos que se adquirieron por caja chica toda vez que los Conmutadores de capa 2 de uso empresarial eleva enormemente los costos.</p>
--	--

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 8 – VISTA FRONTAL.

OFICINA DE SEGUROS



OFICINA CONTRATOS RR.HH COMPLEJO ARENALES

LABORATORIO



LABORATORIO – AREA DE APOYO ADMINISTRATIVO






F:\FOTOS CEL\IMG_20170331_102202.jpg

<p>PROPIO (X)</p> <p>3 COM</p> <p>D-LINK</p> <p>MODELO:</p> <p>Superstack 5500G-E1</p> <p>DGS 3128, DES 1024</p> <p>TECNOLOGIA:</p> <p>CAPA 2</p> <p>DESCRIPCION:</p> <p>Conmutadores de CAPA 2 y Stand-alone ubicados en rack de pared en áreas de trabajo debido al crecimiento no planificado de las oficinas.</p>	<ul style="list-style-type: none"> - La ubicación de oficinas es muy dinámico, donde lo planificado se ve alterado por decisiones de los servicios.
---	--

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 9 – VISTA FRONTAL.								
DEPARTAMENTO DE ANATOMIA PATOLOGICA	OFICINA DE ATENCION AL ASEGURADO							
								
TOMA DE MUESTRAS DE LABORATORIO								
								
COMENTARIOS								
<table border="1"> <tr> <td>PROPIO (X)</td> </tr> <tr> <td>3 COM</td> </tr> <tr> <td>D-LINK</td> </tr> <tr> <td>MODELO: Superstack 5500G-E1</td> </tr> <tr> <td>DGS 3128, DES 1024</td> </tr> <tr> <td>TECNOLOGIA: CAPA 2</td> </tr> <tr> <td>DESCRIPCION: Conmutadores de CAPA 2 y Stand-alone ubicados en rack de pared en áreas de trabajo debido al crecimiento no planificado de las oficinas.</td> </tr> </table>	PROPIO (X)	3 COM	D-LINK	MODELO: Superstack 5500G-E1	DGS 3128, DES 1024	TECNOLOGIA: CAPA 2	DESCRIPCION: Conmutadores de CAPA 2 y Stand-alone ubicados en rack de pared en áreas de trabajo debido al crecimiento no planificado de las oficinas.	<ul style="list-style-type: none"> - La ubicación de oficinas es muy dinámico, donde lo planificado se ve alterado por decisiones de los servicios.
PROPIO (X)								
3 COM								
D-LINK								
MODELO: Superstack 5500G-E1								
DGS 3128, DES 1024								
TECNOLOGIA: CAPA 2								
DESCRIPCION: Conmutadores de CAPA 2 y Stand-alone ubicados en rack de pared en áreas de trabajo debido al crecimiento no planificado de las oficinas.								

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 10 – VISTA FRONTAL.

OFICINA DE CONTRATOS - RRHH



OFICINA DE RECURSOS HUMANOS



AREA DE SOPORTE TECNICO



OFICINA DE FACTURACION Y COBRANZAS



COMENTARIOS

PROPIO (X)

3 COM
D-LINK
TP-LINK

MODELO:
Superstack 5500G-E1
DGS 3128, DES 1024

TECNOLOGIA:
CAPA 2

DESCRIPCION:

Conmutadores de CAPA 2 y Stand-alone ubicados en áreas de trabajo debido al crecimiento no planificado de las oficinas.

- La ubicación de oficinas es muy dinámica, donde lo planificado se ve alterado por decisiones de los servicios.

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 11 – VISTA FRONTAL.

FARMACIA PRINCIPAL	BIBLIOTECA - HNERM
	
OFICINA DE INTELIGENCIA SANITARIA	OFICINA DE EQUIPOS BIOMEDICOS Y ELECTR.
	
COMENTARIOS	
<p>PROPIO (X)</p> <p>3 COM D-LINK TP-LINK</p> <p>MODELO: Superstack 5500G-E1 DGS 3128, DES 1024</p> <p>TECNOLOGIA: CAPA 2</p> <p>DESCRIPCION: Conmutadores de CAPA 2 y Stand-alone ubicados en áreas de trabajo debido al crecimiento no planificado de las oficinas.</p>	<p>- La ubicación de oficinas es muy dinámico, donde lo planificado se ve alterado por decisiones de los servicios.</p>

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)





FOTO 12 – VISTA FRONTAL.

BIOQUIMICA	AREA DE SELECCIÓN DE PERSONAL
	
AREA DE SELECCIÓN DE PERSONAL	DEPTO. ANATOMIA PATOLOGICA
	
COMENTARIOS	
<p>PROPIO (X)</p> <p>3 COM</p> <p>D-LINK</p> <p>TP-LINK</p> <p>MODELO:</p> <p>Superstack 5500G-E1</p> <p>DGS 3128, DES 1024</p> <p>TECNOLOGIA:</p> <p>CAPA 2</p> <p>DESCRIPCION:</p> <p>Conmutadores de CAPA 2 y Stand-alone ubicados en áreas de trabajo debido al crecimiento no planificado de las oficinas.</p>	<ul style="list-style-type: none"> - La ubicación de oficinas es muy dinámico, donde lo planificado se ve alterado por decisiones de los servicios.

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 13 – VISTA FRONTAL.	
LABORATORIO CENTRAL - SOTANO	AREA DE HORMONAS – LABORATORIO CENTRAL
	
COMENTARIOS	
<p>PROPIO (X)</p> <p>3 COM</p> <p>D-LINK</p> <p>TP-LINK</p> <p>MODELO:</p> <p>Superstack 5500G-E1</p> <p>DGS 3128, DES 1024</p> <p>TECNOLOGIA:</p> <p>CAPA 2</p> <p>DESCRIPCION:</p> <p>Conmutadores de CAPA 2 y Stand-alone ubicados en áreas de trabajo debido al crecimiento no planificado de las oficinas.</p>	<ul style="list-style-type: none"> - La ubicación de oficinas es muy dinámico, donde lo planificado se ve alterado por decisiones de los servicios.

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)

FOTO 14 – VISTA FRONTAL.

INGENIERIA SANITARIA



UNIDAD DE EQUIPOS BIOMEDICOS Y ELECTRO.



COMENTARIOS

PROPIO (X)	- La ubicación de oficinas es muy dinámico, donde lo planificado se ve alterado por decisiones de los servicios.
MARCA: D-LINK	
MODELO: DES 1008, 1005	
TECNOLOGIA: STAND-ALONE	
DESCRIPCION: Commutadores de tipo Stand-alone ubicados en áreas de trabajo debido al crecimiento no planificado de las oficinas.	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 15 - VISTA FRONTAL.



COMENTARIOS

PROPIO (X)

MARCA:

D-LINK

MODELO:

DES 1008, 1005

TECNOLOGIA:

STAND-ALONE

DESCRIPCION:

Conmutadores de tipo Stand-alone ubicados en áreas de trabajo debido al crecimiento no planificado de las oficinas.

- La ubicación de oficinas es muy dinámico, donde lo planificado se ve alterado por decisiones de los servicios.

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 16 – VISTA FRONTAL.



COMENTARIOS

PROPIO (X)

MARCA:
D-LINK

MODELO:
DES 1008, 1005

TECNOLOGIA:
STAND-ALONE

DESCRIPCION:

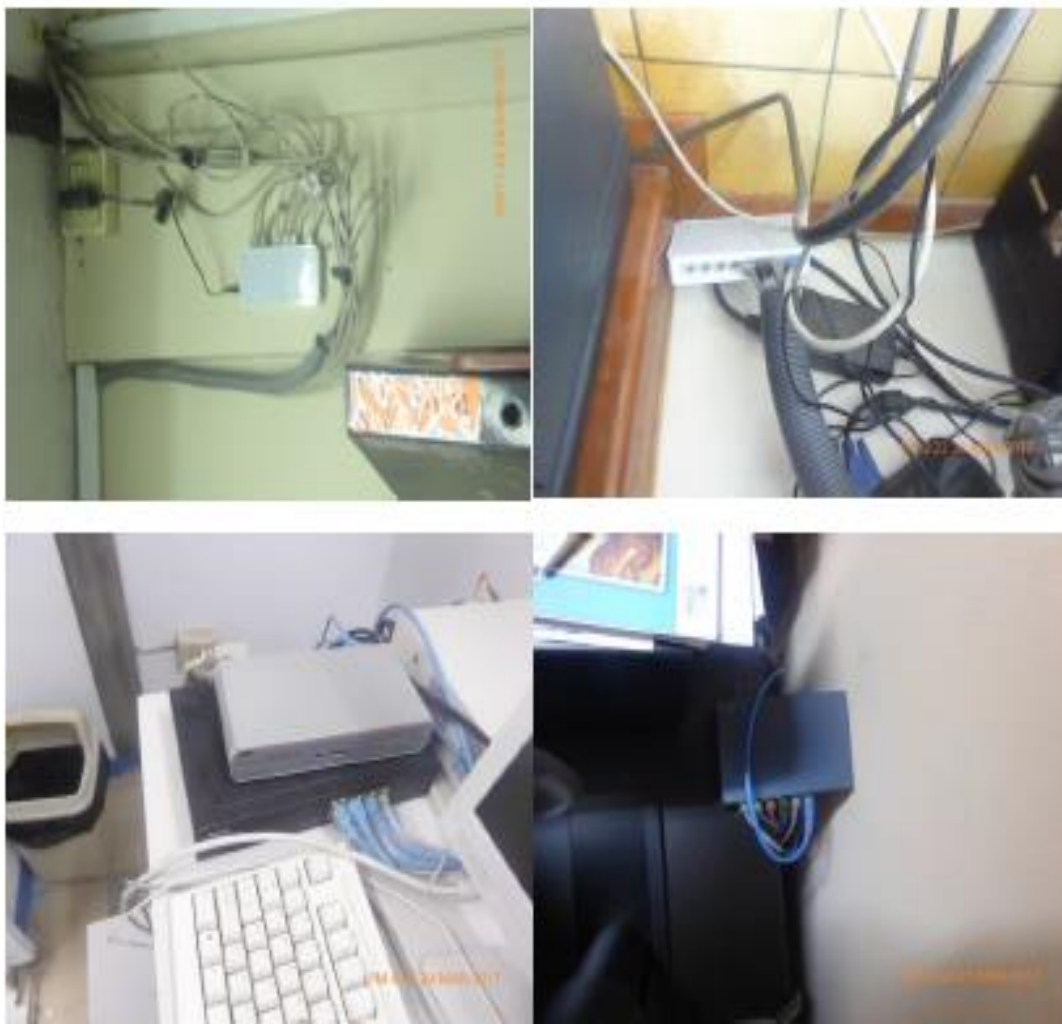
Conmutadores de tipo Stand-alone ubicados en áreas de trabajo debido al crecimiento no planificado de las oficinas.

- La ubicación de oficinas es muy dinámico, donde lo planificado se ve alterado por decisiones de los servicios.

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 17 - VISTA FRONTAL.



COMENTARIOS

PROPIO (X)	<ul style="list-style-type: none"> - La ubicación de oficinas es muy dinámica, donde lo planificado se ve alterado por decisiones de los servicios.
MARCA: D-LINK	
MODELO: DES 1008, 1005	
TECNOLOGIA: STAND-ALONE	
DESCRIPCION: Conmutadores de tipo Stand-alone ubicados en áreas de trabajo debido al crecimiento no planificado de las oficinas.	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 18 – VISTA FRONTAL.



COMENTARIOS

PROPIO (X)	- La ubicación de oficinas es muy dinámico, donde lo planificado se ve alterado por decisiones de los servicios.
MARCA: D-LINK TP-LINK HP	
MODELO: DES 1008, 1005	
TECNOLOGIA: STAND-ALONE	
DESCRIPCION: Conmutadores de tipo Stand-alone ubicados en áreas de trabajo debido al crecimiento no planificado de las oficinas.	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 19 – VISTA FRONTAL.



COMENTARIOS

PROPIO (X)	<ul style="list-style-type: none"> - La ubicación de oficinas es muy dinámico, donde lo planificado se ve alterado por decisiones de los servicios.
MARCA: D-LINK TP-LINK HP	
MODELO: DES 1008, 1005	
TECNOLOGIA: STAND-ALONE	
DESCRIPCION: Conmutadores de tipo Stand-alone ubicados en áreas de trabajo debido al crecimiento no planificado de las oficinas.	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 20 – VISTA FRONTAL.



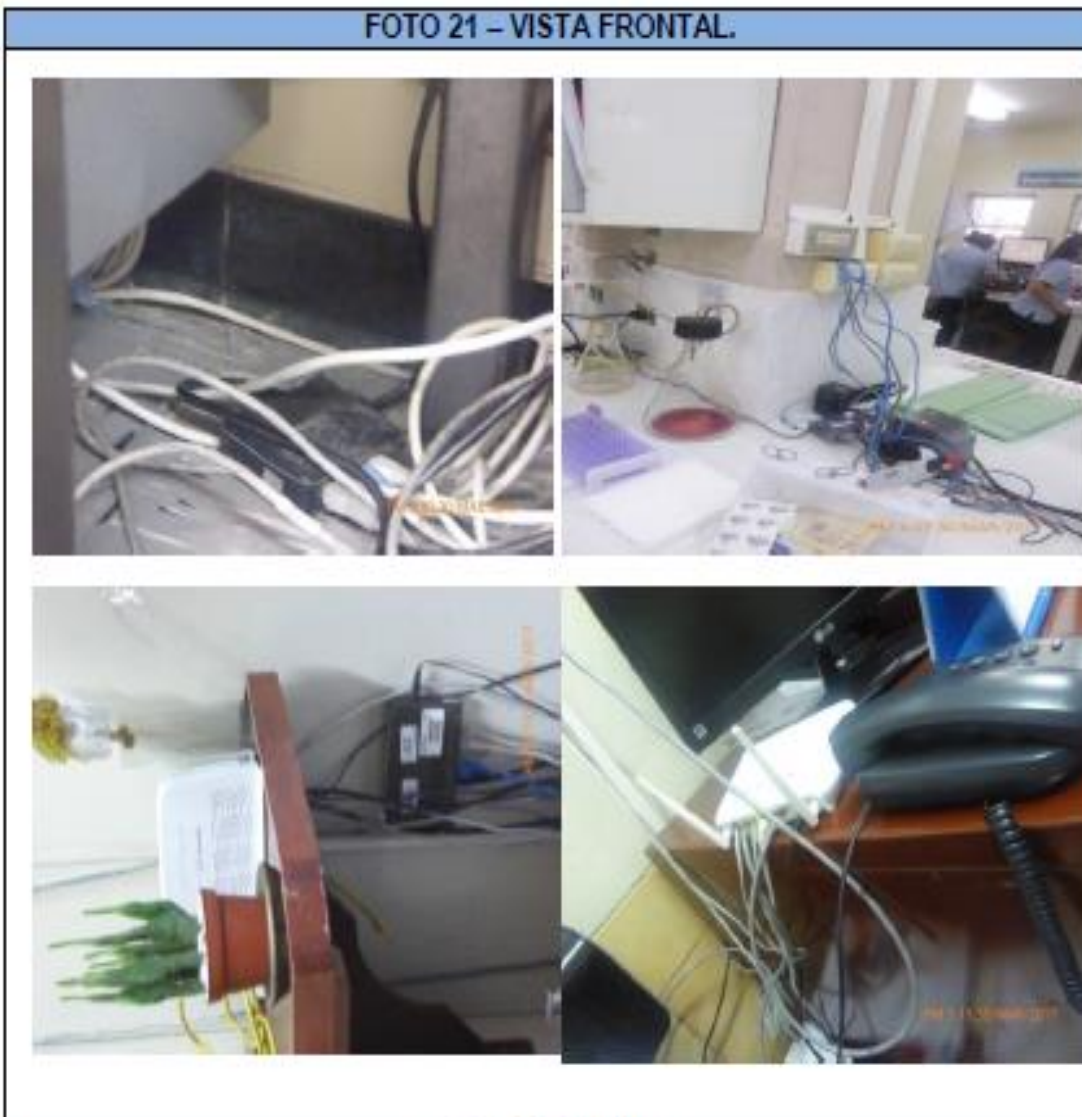
COMENTARIOS

PROPIO (X)	<ul style="list-style-type: none"> - La ubicación de oficinas es muy dinámico, donde lo planificado se ve alterado por decisiones de los servicios.
MARCA: D-LINK TP-LINK HP	
MODELO: DES 1008, 1005	
TECNOLOGÍA: STAND-ALONE	
DESCRIPCIÓN: Conmutadores de tipo Stand-alone ubicados en áreas de trabajo debido al crecimiento no planificado de las oficinas.	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 21 - VISTA FRONTAL.



COMENTARIOS

<p>PROPIO (X)</p> <p>MARCA: D-LINK TP-LINK HP</p> <p>MODELO: DES 1008, 1005</p> <p>TECNOLOGIA: STAND-ALONE</p> <p>DESCRIPCION: Conmutadores de tipo Stand-alone ubicados en áreas de trabajo debido al crecimiento no planificado de las oficinas.</p>	<ul style="list-style-type: none"> - La ubicación de oficinas es muy dinámico, donde lo planificado se ve alterado por decisiones de los servicios.
--	--

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 22 – VISTA FRONTAL.



COMENTARIOS

PROPIO (X)

MARCA:

TP-LINK

MODELO:

DES 1008, 1005

TECNOLOGIA:

STAND-ALONE

DESCRIPCION:

Conmutador de tipo Stand-alone ubicado en áreas de trabajo debido al crecimiento no planificado de las oficinas.

- La ubicación de oficinas es muy dinámico, donde lo planificado se ve alterado por decisiones de los servicios.

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)

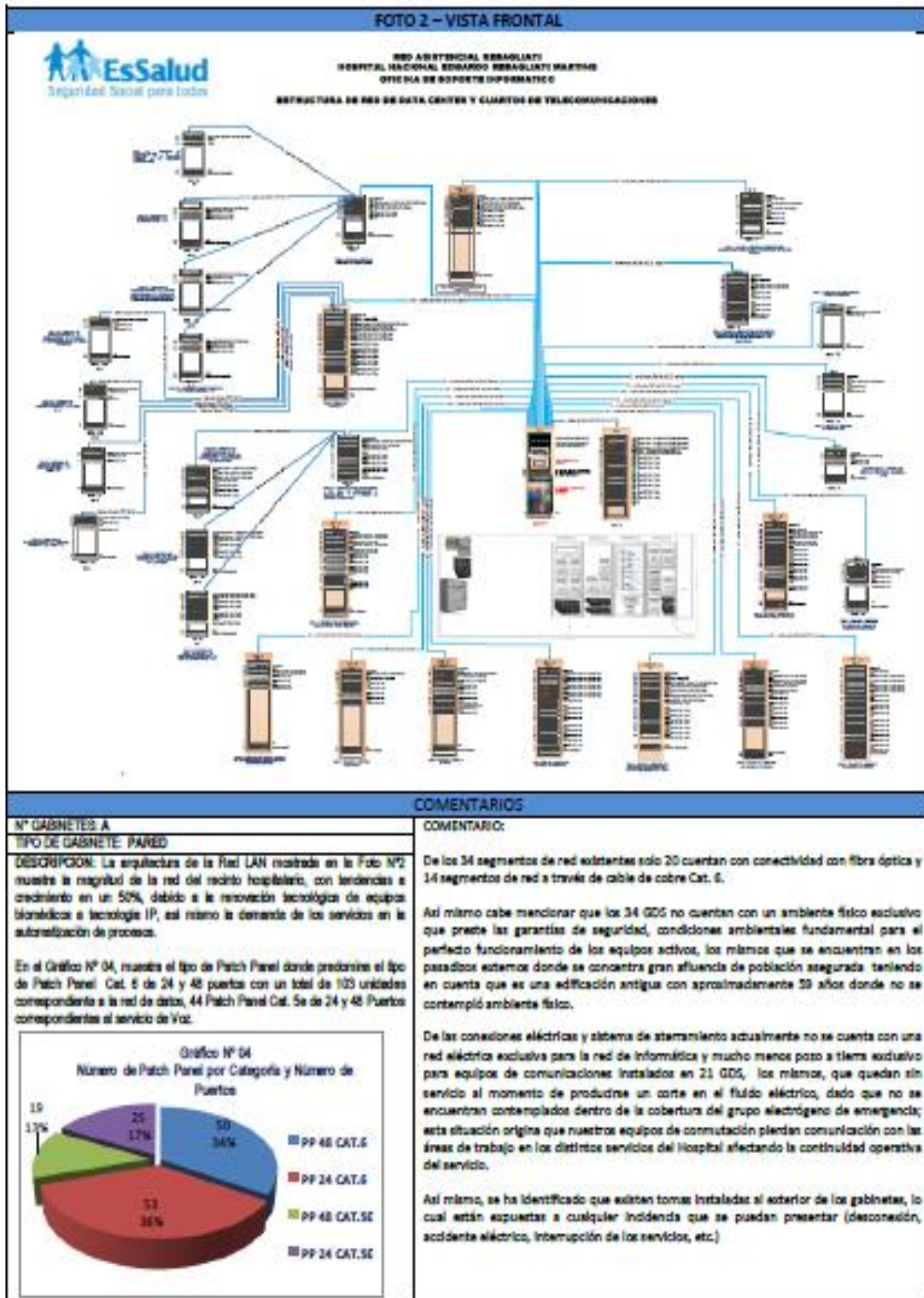


ANEXO 2: GABINETES
Fotos del 1 al 36

09. DISTRIBUCION PRINCIPAL (GABINETES/RACK). EQUIPAMIENTO PRINCIPAL DE TODOS LOS SUBSISTEMAS.																																																																																																																																														
CANT.	COMENTARIOS	OBJETIVO VISUAL																																																																																																																																												
4	Vista Frontal / Vista Oblicua (45° sexagesimales) / Vista Posterior / Vista inferior; por CADA Gabinete/Rack de Distribución Troncal o Backbone.	Tamaño, Tipo del Gabinete / Rack, cantidad de equipos existentes, grado de ocupabilidad, estado actual. Cant. Patch Panel, Ordenadores, PDU, Barra Sist. Puesta Tierra.																																																																																																																																												
FOTO 1 – VISTA FRONTAL.																																																																																																																																														
<p>Gráfico N° 01</p> <p>Total de Puntos de Red Gabinete de Distribución Secundaria (GDS)</p> <table border="1"> <thead> <tr> <th>Segmento</th> <th>Series1</th> <th>Series2</th> <th>Series3</th> </tr> </thead> <tbody> <tr><td>A</td><td>72</td><td>108</td><td>72</td></tr> <tr><td>AD</td><td>48</td><td>72</td><td>48</td></tr> <tr><td>AD0</td><td>36</td><td>36</td><td>36</td></tr> <tr><td>AD6</td><td>36</td><td>36</td><td>36</td></tr> <tr><td>AD8</td><td>36</td><td>36</td><td>36</td></tr> <tr><td>AD9</td><td>48</td><td>48</td><td>48</td></tr> <tr><td>D</td><td>192</td><td>240</td><td>48</td></tr> <tr><td>D1</td><td>240</td><td>48</td><td>48</td></tr> <tr><td>D1-S</td><td>36</td><td>36</td><td>36</td></tr> <tr><td>D3</td><td>144</td><td>144</td><td>144</td></tr> <tr><td>D6</td><td>144</td><td>144</td><td>144</td></tr> <tr><td>D9</td><td>144</td><td>144</td><td>144</td></tr> <tr><td>D12</td><td>144</td><td>144</td><td>144</td></tr> <tr><td>E</td><td>264</td><td>264</td><td>264</td></tr> <tr><td>E1</td><td>264</td><td>264</td><td>264</td></tr> <tr><td>E4</td><td>72</td><td>72</td><td>72</td></tr> <tr><td>E7</td><td>72</td><td>72</td><td>72</td></tr> <tr><td>E9</td><td>72</td><td>72</td><td>72</td></tr> <tr><td>E10</td><td>72</td><td>72</td><td>72</td></tr> <tr><td>E11</td><td>72</td><td>72</td><td>72</td></tr> <tr><td>F</td><td>406</td><td>406</td><td>406</td></tr> <tr><td>F1</td><td>304</td><td>96</td><td>406</td></tr> <tr><td>G</td><td>354</td><td>354</td><td>354</td></tr> <tr><td>G0</td><td>354</td><td>354</td><td>354</td></tr> <tr><td>H</td><td>456</td><td>456</td><td>456</td></tr> <tr><td>H-S</td><td>24</td><td>24</td><td>24</td></tr> <tr><td>I0</td><td>48</td><td>48</td><td>48</td></tr> <tr><td>J</td><td>72</td><td>72</td><td>72</td></tr> <tr><td>K</td><td>36</td><td>36</td><td>36</td></tr> <tr><td>L</td><td>144</td><td>144</td><td>144</td></tr> <tr><td>M</td><td>288</td><td>288</td><td>288</td></tr> <tr><td>N</td><td>24</td><td>24</td><td>24</td></tr> <tr><td>N</td><td>24</td><td>24</td><td>24</td></tr> <tr><td>RS</td><td>72</td><td>72</td><td>72</td></tr> </tbody> </table>			Segmento	Series1	Series2	Series3	A	72	108	72	AD	48	72	48	AD0	36	36	36	AD6	36	36	36	AD8	36	36	36	AD9	48	48	48	D	192	240	48	D1	240	48	48	D1-S	36	36	36	D3	144	144	144	D6	144	144	144	D9	144	144	144	D12	144	144	144	E	264	264	264	E1	264	264	264	E4	72	72	72	E7	72	72	72	E9	72	72	72	E10	72	72	72	E11	72	72	72	F	406	406	406	F1	304	96	406	G	354	354	354	G0	354	354	354	H	456	456	456	H-S	24	24	24	I0	48	48	48	J	72	72	72	K	36	36	36	L	144	144	144	M	288	288	288	N	24	24	24	N	24	24	24	RS	72	72	72
Segmento	Series1	Series2	Series3																																																																																																																																											
A	72	108	72																																																																																																																																											
AD	48	72	48																																																																																																																																											
AD0	36	36	36																																																																																																																																											
AD6	36	36	36																																																																																																																																											
AD8	36	36	36																																																																																																																																											
AD9	48	48	48																																																																																																																																											
D	192	240	48																																																																																																																																											
D1	240	48	48																																																																																																																																											
D1-S	36	36	36																																																																																																																																											
D3	144	144	144																																																																																																																																											
D6	144	144	144																																																																																																																																											
D9	144	144	144																																																																																																																																											
D12	144	144	144																																																																																																																																											
E	264	264	264																																																																																																																																											
E1	264	264	264																																																																																																																																											
E4	72	72	72																																																																																																																																											
E7	72	72	72																																																																																																																																											
E9	72	72	72																																																																																																																																											
E10	72	72	72																																																																																																																																											
E11	72	72	72																																																																																																																																											
F	406	406	406																																																																																																																																											
F1	304	96	406																																																																																																																																											
G	354	354	354																																																																																																																																											
G0	354	354	354																																																																																																																																											
H	456	456	456																																																																																																																																											
H-S	24	24	24																																																																																																																																											
I0	48	48	48																																																																																																																																											
J	72	72	72																																																																																																																																											
K	36	36	36																																																																																																																																											
L	144	144	144																																																																																																																																											
M	288	288	288																																																																																																																																											
N	24	24	24																																																																																																																																											
N	24	24	24																																																																																																																																											
RS	72	72	72																																																																																																																																											
COMENTARIOS																																																																																																																																														
<p>N° GABINETES: 34 Gabinetes de Comunicaciones</p> <p>TIPO DE GABINETE: Piso y Pared</p> <p>DESCRIPCION: El Hospital cuenta con 34 segmentos de red denominados Gabinetes de Distribución Secundaria - GDS, de los cuales se detallan a continuación.</p>																																																																																																																																														
<p>Gráfico N° 02 Tipos de Gabinetes Utilizados</p> <p>Gráfico N° 03 Puntos de Red de Tipo por Tipo de Servicio Voz y Datos</p>																																																																																																																																														
<ul style="list-style-type: none"> - El Gráfico N° 01, Total de puntos de red por Gabinete de Distribución Secundaria, se puede apreciar que existen 5,184 Puntos de Red, Donde El GDS "H" representa el 9% con 456 puntos de red, el GDS "F" representa el 8% con 406 puntos de red, el GDS "G" 7% con 354 puntos de red, el 6% representan cada GDS "C1, I2 y M" con 288 puntos de red cada uno, así mismo el GDS "C" con un 5% con un total de 264 puntos de red. - El Gráfico N° 02, Tipos de Gabinetes Utilizados, cabe precisar que el hospital cuenta con 34 GDS en todo el recinto Hospitalario donde el 62 % son Tipo Rack de Pared y el 38 % son Gabinetes de Piso, así mismo cabe precisar que los gabinetes de comunicaciones no son los adecuados para el Sistema de Cableado Estructurado, toda vez que son para servidores. - El Gráfico N° 03, Puntos de Red de Tipo por Tipo de Servicio Voz y Datos representa los porcentajes del total de puntos que son 5,184, se cuenta con 3,660 puntos de datos que representa el 71% el mismo que se utiliza para dispositivos como PC, Impresoras, Cámaras de Video y Equipos médicos; el 29 % restante que equivale a 1,524 puntos de red corresponde al servicio de Voz (Analógico, Digital e IP) - Cabe mencionar que los GDS antes mencionados están saturados toda vez que cubren hasta tres pisos de gran área, lo que ha impedido la habilitación de nuevos puntos de red desde los gabinetes de comunicaciones lo que genera incumplimiento de las normas de la industria de telecomunicaciones, optando por realizar instalaciones inadecuadas en forma de cascada. 																																																																																																																																														

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)





Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 3 – PUNTOS DE RED POR GABINETE DE DISTRIBUCIÓN SECUNDARIA





GABINETE			CAT. A SEP	CAT. B SEP	CAT. C SEP	CAT. D SEP	N - PUNTOS DE RED	T - PUNTOS DE RED	T - PUNTOS DE RED
N	P	P	N - PUNTOS DE RED	N - PUNTOS DE RED	N - PUNTOS DE RED	N - PUNTOS DE RED			
A		X	1			1	72	48	24
A01	X		2	1	1		188	120	48
A03		X		2		1	72	48	24
A08		X		1		1	48	24	24
A09		X		2		1	72	48	24
A12		X		1		1	48	24	24
B	X		2	2	1		192	144	48
B1	X		2	4	1		240	192	48
B1-S	X			2			48	36	12
B3		X	2	2	1	1	216	144	72
B6		X	3	1	1		216	188	48
B8		X	3		1		192	144	48
B12		X	2	1	1		188	120	48
C	X		2	4	1	1	264	192	72
C1	X		3	3	1	1	288	216	72
C4		X	1			1	72	48	24
C7		X	1			1	72	48	24
C10		X	1			1	72	48	24
C13		X	1			1	72	48	24
D		X	1			1	72	48	24
F	X		8		2	1	408	288	120
F1	X						0	0	0
G	X		4	3	2	1	384	284	120
G3		X	1	1		1	96	72	24
H	X		3	4	2	1	456	336	120
H-S		X		1			24	24	0
I2	X		3	3	1	1	288	216	72
J		X		1		1	48	24	24
K		X	3			1	188	144	24
L		X	1	1	1		120	72	48
M	X			8	2	2	288	144	144
N	X			3		1	96	72	24
N		X		1		1	48	24	24
MS		X		3		1	96	72	24
							6.184	5.000	1.624

COMENTARIO

- Detalle de puntos de red por tipo de servicio de los Gabinetes de Distribución Secundaria.

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 4 - VISTA FRONTAL							
GABINETE A							
Vista Frontal del Gabinete	Parte Posterior del Gabinete	Vista de la parte Interna del Gabinete	Estado de la Unidad de Ventilación				
							
<p>COMENTARIOS</p> <table border="1"> <tr> <td>N° GABINETES: A</td> <td rowspan="3"> <p>COMENTARIO:</p> <p>Rack</p> <p>Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en un pesadizo donde la afluencia de público es bastante considerable el mismo que representa un inminente peligro ante un desprendimiento de la estructura toda vez que las bisagras de material "Antimonio" están deterioradas.</p> <p>Así mismo podemos evidenciar que existe saturación de cableado, no contando con sistema de eléctrico de contingencia, atornillamiento de la estructura, y limitante de proyección o crecimiento de puntos de red contemplados en el mencionado segmento de red.</p> <p>La longitud de los Patch Cord utilizados en su mayoría son de tres metros, lo cual genera una mayor densidad de cableado saturando los ordenadores.</p> <p>Recomendaciones</p> <ul style="list-style-type: none"> - Renovación de Gabinete de Comunicaciones, contemplando la instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones. </td> </tr> <tr> <td>TIPO DE GABINETE: PARED</td> </tr> <tr> <td> <p>DESCRIPCIÓN: El Gabinete de Distribución Secundario "A", se encuentra ubicado junto al Sindicato de Obstétricas, el mismo que se enlaza a través de Fibra Óptica desde el Gabinete de Distribución Principal F1, ubicado en el data center de la Oficina de Soporte Informático.</p> <p>Este Rack cuenta con 22 UR, Aloja una bandeja de fibra óptica de 3 Puertos, 3 Pares F.O Multimodo de 50/125 m, OMC marca SIEMON, 01 Patch Panel de 48P Cat. 6, 01 Patch Panel de 24P Cat. 5e, cuenta con 02 conmutadores de 24 puertos requerido y 02 conmutadores ubicados en áreas de trabajo, cuenta con 72 Puntos de red de los cuales 48 puntos son para el servicio de Datos y 24 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Departamento de Medicina Física y Rehabilitación, Unidad de Administración de Personal de Recursos Humanos, Oficina de Control Post Hospitalario Especializado (PADOMI). Así mismo interconecta con los conmutadores principales de los Gabinetes de Distribución Secundario de "A3, A6, A9, A12" ubicados en el Block "A" de Hospitalización desde el Piso 2 al 13 el cual es el encargado de distribuir los servicios de Voz, Datos y Video, cuenta con cableado UTP categoría 6 LSZH.</p> <p>Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.</p> </td> </tr> </table>				N° GABINETES: A	<p>COMENTARIO:</p> <p>Rack</p> <p>Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en un pesadizo donde la afluencia de público es bastante considerable el mismo que representa un inminente peligro ante un desprendimiento de la estructura toda vez que las bisagras de material "Antimonio" están deterioradas.</p> <p>Así mismo podemos evidenciar que existe saturación de cableado, no contando con sistema de eléctrico de contingencia, atornillamiento de la estructura, y limitante de proyección o crecimiento de puntos de red contemplados en el mencionado segmento de red.</p> <p>La longitud de los Patch Cord utilizados en su mayoría son de tres metros, lo cual genera una mayor densidad de cableado saturando los ordenadores.</p> <p>Recomendaciones</p> <ul style="list-style-type: none"> - Renovación de Gabinete de Comunicaciones, contemplando la instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones. 	TIPO DE GABINETE: PARED	<p>DESCRIPCIÓN: El Gabinete de Distribución Secundario "A", se encuentra ubicado junto al Sindicato de Obstétricas, el mismo que se enlaza a través de Fibra Óptica desde el Gabinete de Distribución Principal F1, ubicado en el data center de la Oficina de Soporte Informático.</p> <p>Este Rack cuenta con 22 UR, Aloja una bandeja de fibra óptica de 3 Puertos, 3 Pares F.O Multimodo de 50/125 m, OMC marca SIEMON, 01 Patch Panel de 48P Cat. 6, 01 Patch Panel de 24P Cat. 5e, cuenta con 02 conmutadores de 24 puertos requerido y 02 conmutadores ubicados en áreas de trabajo, cuenta con 72 Puntos de red de los cuales 48 puntos son para el servicio de Datos y 24 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Departamento de Medicina Física y Rehabilitación, Unidad de Administración de Personal de Recursos Humanos, Oficina de Control Post Hospitalario Especializado (PADOMI). Así mismo interconecta con los conmutadores principales de los Gabinetes de Distribución Secundario de "A3, A6, A9, A12" ubicados en el Block "A" de Hospitalización desde el Piso 2 al 13 el cual es el encargado de distribuir los servicios de Voz, Datos y Video, cuenta con cableado UTP categoría 6 LSZH.</p> <p>Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.</p>
N° GABINETES: A	<p>COMENTARIO:</p> <p>Rack</p> <p>Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en un pesadizo donde la afluencia de público es bastante considerable el mismo que representa un inminente peligro ante un desprendimiento de la estructura toda vez que las bisagras de material "Antimonio" están deterioradas.</p> <p>Así mismo podemos evidenciar que existe saturación de cableado, no contando con sistema de eléctrico de contingencia, atornillamiento de la estructura, y limitante de proyección o crecimiento de puntos de red contemplados en el mencionado segmento de red.</p> <p>La longitud de los Patch Cord utilizados en su mayoría son de tres metros, lo cual genera una mayor densidad de cableado saturando los ordenadores.</p> <p>Recomendaciones</p> <ul style="list-style-type: none"> - Renovación de Gabinete de Comunicaciones, contemplando la instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones. 						
TIPO DE GABINETE: PARED							
<p>DESCRIPCIÓN: El Gabinete de Distribución Secundario "A", se encuentra ubicado junto al Sindicato de Obstétricas, el mismo que se enlaza a través de Fibra Óptica desde el Gabinete de Distribución Principal F1, ubicado en el data center de la Oficina de Soporte Informático.</p> <p>Este Rack cuenta con 22 UR, Aloja una bandeja de fibra óptica de 3 Puertos, 3 Pares F.O Multimodo de 50/125 m, OMC marca SIEMON, 01 Patch Panel de 48P Cat. 6, 01 Patch Panel de 24P Cat. 5e, cuenta con 02 conmutadores de 24 puertos requerido y 02 conmutadores ubicados en áreas de trabajo, cuenta con 72 Puntos de red de los cuales 48 puntos son para el servicio de Datos y 24 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Departamento de Medicina Física y Rehabilitación, Unidad de Administración de Personal de Recursos Humanos, Oficina de Control Post Hospitalario Especializado (PADOMI). Así mismo interconecta con los conmutadores principales de los Gabinetes de Distribución Secundario de "A3, A6, A9, A12" ubicados en el Block "A" de Hospitalización desde el Piso 2 al 13 el cual es el encargado de distribuir los servicios de Voz, Datos y Video, cuenta con cableado UTP categoría 6 LSZH.</p> <p>Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.</p>							

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 5 – VISTA FRONTAL			
GABINETE A1			
Parte Posterior del Gabinete	Vista de la parte Interna del Gabinete	Vista del Cableado	
COMENTARIOS			
N° GABINETES: A1	COMENTARIO:		
TIPO DE GABINETE: PISO	Rack		
DESCRIPCION: El Gabinete de Distribución Secundario A1, se encuentra ubicado en el interior de la Sala de Entrevista de Trabajo Social, el mismo que se enlaza a través de Fibra Óptica desde el Gabinete de Distribución Principal F1, ubicado en el data center de la Oficina de Soporte Informático.	Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en un pasadizo donde la afluencia de público es bastante considerable el mismo que representa un inminente peligro ante un desprendimiento de la estructura toda vez que las bisagras de material "Antimonio" están deterioradas.		
Este Gabinete cuenta con 44 UR, Aloja una bandeja de fibra óptica de 3 Puertos, 3 Pares F.O Multimodo de 50/125 m, OM3 marca SIEMON, 02 Patch Panel de 48P Cat. 6, 01 Patch Panel de 24P Cat. 6, 01 Patch Panel de 48P Cat. 5e, cuenta con 04 conmutadores de 24 puertos requerido y 04 conmutadores ubicados en áreas de trabajo, cuenta con 168 Puntos de red de los cuales 120 puntos son para el servicio de Datos y 48 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Comité Farmacológico, Evaluación de Personal, Departamento de Enfermeras, Servicio Social, TBC, Biblioteca, Oficina de Capacitación, Auditorio N° 2, 3, 4, 5 y 6" el cual es el encargado de distribuir los servicios de Voz, Datos y Video, cuenta con cableado UTP categoría 6 LSZH.	Así mismo podemos evidenciar que existe saturación de cableado, no contando con sistema de eléctrico de contingencia, aterramiento de la estructura, y limitante de proyección a crecimiento de puntos de red contemplados en el mencionado segmento de red.		
Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.	La longitud de los Patch Cord utilizados en su mayoría son de tres metros, lo cual genera una mayor densidad de cableado saturando los ordenadores.		
	Recomendaciones		
	<ul style="list-style-type: none"> Renovación de Gabinete de Comunicaciones, contemplando la Instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones. 		

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 6 – VISTA FRONTAL			
GABINETE A3			
Vista Frontal del Gabinete	Parte Posterior del Gabinete	Vista de la parte interna del Gabinete	Estado de la Unidad de Ventilación
COMENTARIOS			
N° GABINETES: A3	COMENTARIO:		
TIPO DE GABINETE: PARED	Rack		
DESCRIPCIÓN: El Gabinete de Distribución Secundario A3, se encuentra ubicado en el Piso 3 Sección A - Servicio de Cirugía de Hígado y Vías Biliares, el mismo que se enlaza a través de Cableado Cat. 6, desde el Gabinete de Distribución Secundario "A".	Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en la sala de espera del servicio de Cirugía de Hígado y Vías Biliares, cabe mencionar que las bisagras de material "Antimonio" están deterioradas lo que dificulta realizar el mantenimiento preventivo y correctivo ante el inminente peligro de desprendimiento de estructura.		
Este Rack cuenta con 22 UR, cuenta con dos enlaces broncales de cable de cobre UTP Cat. 6 el mismo que se conecta directamente al switch de borde configurado como cascada desde el GDS "A", aloja 02 Patch Panel de 24P Cat. 6, 01 Patch Panel de 24P Cat. 5e, cuenta con 01 conmutador de 24 puertos requerido, cuenta con 72 Puntos de red de los cuales 48 puntos son para el servicio de Datos y 24 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Hospitalización 2A Servicio de Neonatología, Hospitalización 3A Servicio de Cirugía General 3, Hospitalización Dermatología, Reumatología, Endocrinología 4" el cual es el encargado de distribuir los servicios de Voz, Data, cuenta con cableado UTP categoría 6 LSZH.	Así mismo podemos evidenciar que no cuenta con sistema de eléctrico de contingencia, atenuamiento de la estructura, y limitante de proyección o crecimiento de puntos de red contemplados en el mencionado segmento de red.		
Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de atenuamiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.	Recomendaciones		
	<ul style="list-style-type: none"> Renovación de Gabinete de Comunicaciones, contemplando la instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones. 		





Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 7 – VISTA FRONTAL			
GABINETE A6			
Vista Frontal del Gabinete	Parte Posterior del Gabinete	Vista de la parte Interna del Gabinete	Estado de la Unidad de Ventilación
COMENTARIOS			
N° GABINETES: A6	COMENTARIO:		
TIPO DE GABINETE: PARED	Rack		
<p>DESCRIPCIÓN: El Gabinete de Distribución Secundario A6, se encuentra ubicado en el Piso 6 Sección A, Servicio de Gastroenterología, el mismo que se enlaza a través de Cableado Cat. 6, desde el Gabinete de Distribución Secundario "A".</p> <p>Este Rack cuenta con 22 UR, cuenta con dos enlaces troncales de cable de cobre UTP Cat. 6 el mismo que se conecta directamente al switch de borde configurado como cascada desde el GDS "A", aloja 01 Patch Panel de 24P Cat. 6, 01 Patch Panel de 24P Cat. 5e, cuenta con 01 conmutador de 24 puertos requerido, cuenta con 48 Puntos de red de los cuales 24 puntos son para el servicio de Datos y 24 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Hospitalización 5A Servicio de Obstetricia, Neonatología, Medicina Fetal, Unidad de Vigilancia Fetal, Hospitalización 6A Servicio de Gastro Enterología, Unidad de Hígado, Intestino-Colon-Recto, Esofago-Estomago-Duodeno, Hospitalización 7A Servicio de Ginecología, Onco Ginecología" el cual es el encargado de distribuir los servicios de Voz, Data, cuenta con cableado UTP categoría 6 LSZH.</p> <p>Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.</p>	<p>Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en la sala de espera del Servicio de Gastroenterología, cabe mencionar que las bisagras de material "Antimonio" están deterioradas lo que dificulta realizar el mantenimiento preventivo y correctivo ante el inminente peligro de desprendimiento de estructura.</p> <p>Así mismo podemos evidenciar que no cuenta con el sistema de eléctrico de contingencia, aterramiento de la estructura, y limitante de proyección a crecimiento de puntos de red contemplados en el mencionado segmento de red.</p> <p>Recomendaciones</p> <ul style="list-style-type: none"> Renovación de Gabinete de Comunicaciones, contemplando la Instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones. 		

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 8 – VISTA FRONTAL			
GABINETE A9			
Vista Frontal del Gabinete	Parte Posterior del Gabinete	Vista de la parte interna del Gabinete	Estado de la Unidad de Ventilación
 <p>Cableado UTP ubicado en la parte externa</p>	 <p>Chapa de puerta cerrada estropeada</p> <p>Sistema eléctrico convencional, sin protección</p>	 <p>Interior de Gabinete presenta polvo</p>	 <p>Falta de mantenimiento a la Unidad de Ventilación, tiempo excesivo</p>
COMENTARIOS			
N° GABINETES: A9	COMENTARIO:		
TIPO DE GABINETE: PARED	Rack		
<p>DESCRIPCION: El Gabinete de Distribución Secundario A9, se encuentra ubicado en el Piso 9 Sección A – Servicio de Traumatología, el mismo que se enlaza a través de Cableado Cat. 6, desde el Gabinete de Distribución Secundario A.</p> <p>Este Rack cuenta con 22 UR, cuenta con dos enlaces broncales de cable de cobre UTP Cat. 6 el mismo que se conecta directamente al switch de borde configurado como cascada desde el GDS "A", aloja 02 Patch Panel de 24P Cat. 6, 01 Patch Panel de 24P Cat. 5e, cuenta con 01 conmutador de 24 puertos requerido, cuenta con 72 Puntos de red de los cuales 48 puntos son para el servicio de Datos y 24 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Hospitalización Piso 8A Servicio de Trasplante de Medula ÓSEA (UTMO), Oncología Médica, Hospitalización Piso 9A Servicio de Traumatología, Hospitalización Piso 10A Servicio de Nefrología, Unidad de Trasplante Renal, Nefrología Clínica y Especialidad" el cual es el encargado de distribuir los servicios de Voz, Datos, cuenta con cableado UTP categoría 6 LSZH.</p> <p>Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.</p>	<p>Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en la sala de espera del Servicio de Traumatología, cabe mencionar que las bisagras de material "Antimonio" están deterioradas lo que dificulta realizar el mantenimiento preventivo y correctivo ante el inminente peligro de desprendimiento de estructura.</p> <p>Así mismo podemos evidenciar que no cuenta con el sistema de eléctrico de contingencia, aterramiento de la estructura, y limitante de proyección o crecimiento de puntos de red contemplados en el mencionado segmento de red.</p> <p>Recomendaciones</p> <ul style="list-style-type: none"> Renovación de Gabinete de Comunicaciones, contemplando la Instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones. 		

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 9 – VISTA FRONTAL			
GABINETE A12			
Vista Frontal del Gabinete	Parte Posterior del Gabinete	Vista de la parte Interna del Gabinete	Estado de la Unidad de Ventilación
COMENTARIOS:			
N° GABINETES: A12	COMENTARIO:		
TIPO DE GABINETE: PARED	Rack		
DESCRIPCIÓN: El Gabinete de Distribución Secundario A12, se encuentra ubicado en el Piso 12 Sección A – Servicio de Urología, el mismo que se enlaza a través de Cableado Cat. 6, desde el Gabinete de Distribución Secundario A.	Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en la sala de espera del Servicio de Urología, cabe mencionar que las bisagras de material "Antimonio" están deterioradas lo que dificulta realizar el mantenimiento preventivo y correctivo ante el inminente peligro de desprendimiento de estructura.		
Este Rack cuenta con 18 UR, cuenta con dos enlaces troncales de cable de cobre UTP Cat. 6 el mismo que se conecta directamente al switch de borde configurado como cascada desde el GDS "A", elije 01 Patch Panel de 24P Cat. 6, 01 Patch Panel de 24P Cat. 5e, cuenta con 01 conmutador de 24 puertos requeado, cuenta con 48 Puntos de red de los cuales 24 puntos son para el servicio de Datos y 24 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Hospitalización 11A Servicio de Neurología, UCIN 11, Cirugía de Tórax y Cardiovascular, Cirugía de Corazón, Hospitalización 12A Servicio de Urología General y Especializada, Hospitalización 13A Servicio de Neurología General, Enfermedades Neurovasculares y Epilepsia" el cual es el encargado de distribuir los servicios de Voz, Datos, cuenta con cableado UTP categoría 6 LSZH.	Así mismo podemos evidenciar que no cuenta con el sistema de eléctrico de contingencia, aterramiento de la estructura, y limitante de proyección a crecimiento de puntos de red contemplados en el mencionado segmento de red.		
Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.	Recomendaciones		
	- Renovación de Gabinete de Comunicaciones, contemplando la instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones.		

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 10 – VISTA FRONTAL			
GABINETE B			
Vista Frontal del Gabinete	Parte Posterior del Gabinete	Vista de la parte Interna del Gabinete	Estado de la Unidad de Ventilación
			
COMENTARIOS			
Nº GABINETES: B	COMENTARIO:		
TIPO DE GABINETE: PISO	Rack		
DESCRIPCION: El Gabinete de Distribución Secundario B, se encuentra ubicado en el Block B – Central Telefónica, el mismo que se enlaza a través de Fibra Óptica desde el Gabinete de Distribución Principal F1, ubicado en el data center de la Oficina de Soporte Informático.	Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en un pasadizo del Block B – Central Telefónica donde la afluencia de público es bastante considerable.		
Este Gabinete cuenta con 44 UR, Aloja una bandeja de fibra óptica de 3 Puertos, 3 Pares F.O Multimodo de 50/125 m, OM3 marca SIEMON, 02 Patch Panel de 48P Cat. 6, 02 Patch Panel de 24P Cat. 6, 01 Patch Panel de 48P Cat. 5e, cuenta con 03 conmutadores de 24 puertos requerido y 03 conmutadores ubicados en áreas de trabajo, cuenta con 192 Puntos de red de los cuales 144 puntos son para el servicio de Datos y 48 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Central Telefónica, Procura, URVI, Recursos Propios, Servicio de Nutrición, Perifoneo" el cual es el encargado de distribuir los servicios de Voz, Data y Video, cuenta con cableado UTP categoría 6 LSZH.	Así mismo podemos evidenciar que existe saturación de cableado en la parte vertical, sistema de enfriamiento en mal estado.		
Debe mencionarse que no cuenta con sistema de enfriamiento, sistema de almacenamiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.	La longitud de los Patch Cord utilizados en su mayoría son de tres metros, lo cual genera una mayor densidad de cableado saturando los ordenadores.		
	Recomendaciones		
	- Renovación de Gabinete de Comunicaciones, contemplando la instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones.		

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 11 – VISTA FRONTAL			
GABINETE B1			
Vista Frontal del Gabinete	Parte Posterior del Gabinete	Vista de la parte Interna del Gabinete	Estado de la Unidad de Ventilación
COMENTARIOS			
N° GABINETES: B1	COMENTARIO:		
TIPO DE GABINETE: PISO	Rack		
DESCRIPCION: El Gabinete de Distribución Secundario B1, se encuentra ubicado en el Block B1 – Módulo Central, el mismo que se enlaza a través de Fibra Óptica desde el Gabinete de Distribución Principal F1, ubicado en el data center de la Oficina de Soporte Informático.	Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en un pasadizo del Block B1 – Módulo Central donde la afluencia de público es bastante considerable.		
Este Gabinete cuenta con 44 UR, Aloja una bandeja de fibra óptica de 3 Puertos, 3 Pares F.O Multimodo de 50/125 m, OM3 marca SIEMON, 02 Patch Panel de 48P Cat. 6, 04 Patch Panel de 24P Cat. 6, 01 Patch Panel de 48P Cat. 5e, cuenta con 04 conmutadores de 24 puertos rackeado y 03 conmutadores ubicados en áreas de trabajo, cuenta con 240 Puntos de red de los cuales 192 puntos son para el servicio de Datos y 48 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Módulo Central de Citas, Consulta Externa Ginecológica, Oncología Médica, Litotricia, Tomografía, Ecografía, Rayos X, Módulo de Registros Médicos, Módulo de Oncología Médica, Acelerador Lineal, Planificación Familiar, Servicio de Nutrición ubicado en el Sótano" el cual es el encargado de distribuir los servicios de Voz, Datos y Video, cuenta con cableado UTP categoría 6 LSZH.	Así mismo podemos evidenciar que existe saturación de cableado en la parte vertical, Peinado del cableado es inadecuado, sistema de enfriamiento en mal estado, falta de mantenimiento a los equipos de conmutación.		
Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.	La longitud de los Patch Cord utilizados en su mayoría son de tres metros, lo cual genera una mayor densidad de cableado saturando los ordenadores.		
	Recomendaciones		
	- Renovación de Gabinete de Comunicaciones, contemplando la instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones.		





Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 12 – VISTA FRONTAL			
GABINETE B3			
Vista Frontal del Gabinete	Parte Posterior del Gabinete	Vista de la parte Interna del Gabinete	Estado de la Unidad de Ventilación
COMENTARIOS			
<p>N° GABINETES: 03</p> <p>TIPO DE GABINETE: PARED</p> <p>DESCRIPCION: El Gabinete de Distribución Secundario B3, se encuentra ubicado en el Piso 3 Sección B – Servicio de Cirugía y Estomago Duodeno, el mismo que se enlaza a través de Fibra Óptica, desde el Gabinete de Distribución Principal F1.</p> <p>Este Rack cuenta con 22 UR, Aloja una bandeja de fibra óptica de 3 Puertos, 3 Pares F.O Multimodo de 50/125 m, OMB marca SIEMON, 02 Patch Panel de 48P Cat. 6, 02 Patch Panel de 24P Cat. 6, 01 Patch Panel de 48P Cat. 5e, 01 Patch Panel de 24P Cat. 5e, cuenta con 02 conmutadores de 24 puertos rackeado, cuenta con 216 Puntos de red de los cuales 144 puntos son para el servicio de Datos y 72 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Hospitalización 2B Departamento de Anestesiología y Centro Quirúrgico, UCRQ - Almacén Interno, Hospitalización 3B Sala de Operaciones y Recuperación, Unidad de Soporte Nutricional, Hospitalización 4B Sala de Operaciones de Emergencia, Gabinetes de Comunicaciones 6B, 9B, 12B" ubicados en el Block "B" de Hospitalización desde el Piso 2 al 13 el cual es el encargado de distribuir los servicios de Voz, Datos y Video, cuenta con cableado UTP categoría 6 LSZH.</p> <p>Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.</p>		<p>COMENTARIO:</p> <p>Rack</p> <p>Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en la sala de espera de visitantes de hospitalización del Servicio Cirugía y Estomago Duodeno, cabe mencionar que las bisagras de material "Antimonio" están deterioradas lo que dificulta realizar el mantenimiento preventivo y correctivo ante el inminente peligro de desprendimiento de estructura.</p> <p>Así mismo podemos evidenciar que existe saturación de cableado, no contando con sistema de eléctrico de contingencia, aterramiento de la estructura, y limitante de proyección a crecimiento de puntos de red contemplados en el mencionado segmento de red.</p> <p>La longitud de los Patch Cord utilizados en su mayoría son de tres metros, lo cual genera una mayor densidad de cableado saturando los ordenadores.</p> <p>Recomendaciones</p> <ul style="list-style-type: none"> - Renovación de Gabinete de Comunicaciones, contemplando la Instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones. 	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 13 – VISTA FRONTAL			
GABINETE B6			
Vista Frontal del Gabinete	Vista de la parte Interna del Gabinete	Parte Posterior del Gabinete	Path Cord Desordenados
			
COMENTARIOS			
<p>N° GABINETES: 06</p> <p>TIPO DE GABINETE: PARED</p> <p>DESCRIPCION: El Gabinete de Distribución Secundario B6, se encuentra ubicado en el Piso 6 Sección B – Servicio de Cirugía y Estómago Duodeno, el mismo que se enlaza a través de Cableado Cat. 6, desde el Gabinete de Distribución Secundario B3.</p> <p>Este Rack cuenta con 22 UR, cuenta con dos enlaces troncales de cable de cobre UTP Cat. 6 el mismo que se conecta directamente al switch de borde configurado como cascada desde el GDS "B3", alojó 03 Patch Panel de 48P Cat. 6, 01 Patch Panel de 24P Cat. 6, 01 Patch Panel de 48P Cat. 5e, cuenta con 03 conmutador de 24 puertos requerido, cuenta con 216 Puntos de red de los cuales 168 puntos son para el servicio de Datos y 48 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Hospitalización 5 B Servicio de Obstetricia y Neonatología, Sala de Dilatación, Sala de Partos, Hospitalización 6 B Servicio de Hemorragia Digestiva, Sala de Operaciones, Hospitalización 7 B Unidad de Cuidados Intermedios (UCIN)" el cual es el encargado de distribuir los servicios de Voz, Datos, cuenta con cableado UTP categoría 6 LSZH.</p> <p>Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.</p>		<p>COMENTARIO:</p> <p>Rack</p> <p>Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en la sala de espera del Servicio de Cirugía y Estómago Duodeno, cabe mencionar que los biosegres de material "Antimonio" están deteriorados lo que dificulta realizar el mantenimiento preventivo y correctivo ante el inminente peligro de desprendimiento de estructura.</p> <p>Así mismo podemos evidenciar que no cuenta con sistema de eléctrico de contingencia, aterramiento de la estructura, y limitante de proyección a crecimiento de puntos de red contemplados en el mencionado segmento de red.</p> <p>Recomendaciones</p> <ul style="list-style-type: none"> - Renovación de Gabinete de Comunicaciones, contemplando la instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones. 	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)







FOTO 14 – VISTA FRONTAL

GABINETE B9			
Vista Frontal del Gabinete	Parte Posterior del Gabinete	Vista de la parte Interna del Gabinete	Estado de la Unidad de Ventilación
			
COMENTARIOS			
<p>N° GABINETES: 09</p> <p>TIPO DE GABINETE: PARED</p>		<p>COMENTARIO:</p> <p>Rack</p> <p>Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en la sala de espera del Servicio de Ortopedia, cabe mencionar que las bisagras de material "Artimonio" están deterioradas lo que dificulta realizar el mantenimiento preventivo y correctivo ante el inminente peligro de desprendimiento de estructura.</p> <p>Así mismo podemos evidenciar que no cuenta con sistema de eléctrico de contingencia, aterramiento de la estructura, y limitante de proyección a crecimiento de puntos de red contemplados en el mencionado segmento de red.</p> <p>Recomendaciones</p> <ul style="list-style-type: none"> Renovación de Gabinete de Comunicaciones, contemplando la Instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones. 	
<p>DESCRIPCIÓN: El Gabinete de Distribución Secundario B9, se encuentra ubicado en el Piso 9 Sección B – Servicio de Ortopedia, el mismo que se enlaza a través de Cableado Cat. 6, desde el Gabinete de Distribución Secundario B3.</p> <p>Este Rack cuenta con 22 UR, cuenta con dos enlaces broncales de cable de cobre UTP Cat. 6 el mismo que se conecta directamente al switch de borde configurado como cascada desde el GDS "B3", alaja 03 Patch Panel de 48P Cat. 6, 01 Patch Panel de 48P Cat. 5e, cuenta con 02 conmutador de 24 puertos requestado, cuenta con 192 Puntos de red de los cuales 144 puntos son para el servicio de Datos y 48 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Hospitalización 8 B Servicio de Hematología, Radioterapia, Hospitalización 9 B Centro Quirúrgico y Recuperación, Ortopedia, Hospitalización 10 B Servicio de Nefrología, Oftalmología, Sala de Operaciones de Oftalmología" el cual es el encargado de distribuir los servicios de Voz, Data, cuenta con cableado UTP categoría 6 LSZH.</p> <p>Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.</p>			

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 15 – VISTA FRONTAL			
GABINETE B12			
Vista Frontal del Gabinete	Parte Posterior del Gabinete	Vista de la parte interna del Gabinete	Estado de la Unidad de Ventilación
			
COMENTARIOS			
N° GABINETES: B12		COMENTARIO:	
TIPO DE GABINETE: PARED		Rack	
<p>DESCRIPCION: El Gabinete de Distribución Secundario B12, se encuentra ubicado en el Piso 12 Sección B – Servicio de Neumología, el mismo que se enlaza a través de Cableado Cat. 6, desde el Gabinete de Distribución Secundario B3.</p> <p>Este Rack cuenta con 22 UR, cuenta con dos enlaces broncales de cable de cobre UTP Cat. 6 el mismo que se conecta directamente al switch de borde configurado como cascada desde el GDS "B3", aljofa 02 Patch Panel de 48P Cat. 6, 01 Patch Panel de 24P Cat. 6, 01 Patch Panel de 48P Cat. 5e, cuenta con 03 conmutador de 24 puertos requerido, cuenta con 168 Puntos de red de los cuales 120 puntos son para el servicio de Datos y 48 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Hospitalización 11 B Servicio de Cardiología, UCI y UCIN de Cardiología, Hospitalización 12 B Servicio de Neumología, Sala de Operaciones y Recuperación de Neumología, Hospitalización 13 B Servicio de Neurocirugía, Cirugía Cerebral y NEUROINT y UCI Neurocirugía" el cual es el encargado de distribuir los servicios de Voz, Datos, cuenta con cableado UTP categoría 6 LSZH.</p> <p>Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.</p>		<p>Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en la sala de espera del Servicio de Neumología, cabe mencionar que las bisagras de material "Antimonio" están deterioradas lo que dificulta realizar el mantenimiento preventivo y correctivo ante el inminente peligro de desprendimiento de estructura.</p> <p>Así mismo podemos evidenciar que no cuenta con sistema de eléctrico de contingencia, aterramiento de la estructura, y limitante de proyección a crecimiento de puntos de red contemplados en el mencionado segmento de red.</p> <p>Recomendaciones</p> <ul style="list-style-type: none"> Renovación de Gabinete de Comunicaciones, contemplando la Instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones. 	




Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 16 – VISTA FRONTAL			
GABINETE C			
Vista Frontal del Gabinete	Parte Posterior del Gabinete	Vista de la parte interna del Gabinete	Estado de la Unidad de Ventilación
COMENTARIOS			
<p>N° GABINETES: C</p> <p>TIPO DE GABINETE: PISO</p> <p>DESCRIPCION: El Gabinete de Distribución Secundario C, se encuentra ubicado en el Sector C – Frente a Farmacia 2, el mismo que se enlaza a través de fibra óptica desde el Gabinete de Distribución Principal F1, ubicado en el data center de la Oficina de Soporte Informático.</p> <p>Este Gabinete cuenta con 44 UR, Aloja una bandeja de fibra óptica de 3 Puertos, 3 Pares F.O Multimodo de 50/125 m, OM3 marca SIEMON, 02 Patch Panel de 48P Cat. 6, 04 Patch Panel de 24P Cat. 6, 01 Patch Panel de 48P Cat. 5e, 01 Patch Panel de 24P Cat. 5e, cuenta con 06 conmutadores de 24 puertos ragueado y 08 conmutadores ubicados en áreas de trabajo, cuenta con 264 Puntos de red de los cuales 192 puntos son para el servicio de Datos y 72 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Farmacia Citotóxicos, Sala de Lectura - Resonancia Magnética, Sala de Comando - Resonancia Magnética, Sagen, Cobalto, Farmacia Dosis Unitaria, Hospitalización 2C Servicio de Unidad de Cuidados Intensivos UCI, Calderas Auditorio de Médicos, Lavandería, Enfermeras de Emergencia Adultos, Administración, SCUT de Es Salud, Servicios Generales, Gabinetes de Comunicaciones 4C, 7C, 10C, 13C", ubicados en el Block "C" de Hospitalización desde el Piso 2 al 13 el cual es el encargado de distribuir los servicios de Voz, Datos y Video, cuenta con cableado UTP categoría 6 LSZH.</p> <p>Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de almacenamiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.</p>		<p>COMENTARIO:</p> <p>Rack</p> <p>Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en un pasadizo del Block C – Frente a Farmacia 2, donde la afluencia de público es bastante considerable.</p> <p>Así mismo podemos evidenciar que existe saturación de cableado en la parte vertical, Peinado del cableado es inadecuado, sistema de enfriamiento en mal estado, falta de mantenimiento a los equipos de conmutación.</p> <p>La longitud de los Patch Cord utilizados en su mayoría son de tres metros, lo cual genera una mayor densidad de cableado saturando los ordenadores.</p> <p>Recomendaciones</p> <ul style="list-style-type: none"> Renovación de Gabinete de Comunicaciones, contemplando la Instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones. 	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 17 – VISTA FRONTAL			
GABINETE C1			
Vista Frontal del Gabinete	Parte Posterior del Gabinete	Vista de la parte Interna del Gabinete	Estado de la Unidad de Ventilación
			
COMENTARIOS			
N° GABINETES: C1		COMENTARIO:	
TIPO DE GABINETE: PISO		Rack	
<p>DESCRIPCION: El Gabinete de Distribución Secundario C1, se encuentra ubicado en el Sector C1 – Pasadizo Externo de Departamento de Patología Clínica y Servicio de Tomografía, el mismo que se enlaza a través de fibra óptica desde el Gabinete de Distribución Principal F1, ubicado en el data center de la Oficina de Soporte Informático.</p> <p>Este Gabinete cuenta con 44 UR, Aloja una bandeja de fibra óptica de 3 Puertos, 3 Pares F.O Multimodo de 50/125 m, OM3 marcas SIEMON, 03 Patch Panel de 48P Cat. 6, 03 Patch Panel de 24P Cat. 6, 01 Patch Panel de 48P Cat. 5e, 01 Patch Panel de 24P Cat. 5e, cuenta con 07 conmutadores de 24 puertos rackeado y 23 conmutadores ubicados en áreas de trabajo, cuenta con 288 Puntos de red de los cuales 216 puntos son para el servicio de Datos y 72 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Oficina de Apoyo al departamento, Bioquímica, Citometría de Flujo, Medicina Tras funcional - Banco de Sangre, Cuarto de Revelado, Admisión Emergencia Adulto, Hemostasia, Autoanálisis - Hematología, Servicio Hematología - Lectura de Laminas, Microbiología - Ingreso de Solicitudes, Bacteriología - Microbiología, Parasitología, Farmacia, RX Central, Servicio de Tomografía, Departamento de Radio Diagnostico, Salas de RX, Resonancia Magnética, Almacén Hospitalario", el cual es el encargado de distribuir los servicios de Voz, Datos y Video, cuenta con cableado UTP categoría 6 LSZH.</p> <p>Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.</p>		<p>Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en un pasadizo del Sector C1 – Pasadizo Externo de Departamento de Patología Clínica y Servicio de Tomografía, donde la afluencia de público es bastante considerable.</p> <p>Así mismo podemos evidenciar que existe saturación de cableado en la parte vertical, Peinado del cableado es inadecuado, sistema de enfriamiento en mal estado, falta de mantenimiento a los equipos de conmutación.</p> <p>La longitud de los Patch Cord utilizados en su mayoría son de tres metros, lo cual genera una mayor densidad de cableado saturando los ordenadores.</p> <p>Recomendaciones</p> <ul style="list-style-type: none"> - Renovación de Gabinete de Comunicaciones, contemplando la Instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones. 	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 18 – VISTA FRONTAL			
GABINETE C4			
Vista Frontal del Gabinete	Parte Posterior del Gabinete	Vista de la parte Interna del Gabinete	Estado de la Unidad de Ventilación
			
COMENTARIOS			
<p>N° GABINETES: C4</p> <p>TIPO DE GABINETE: PARED</p> <p>DESCRIPCION: El Gabinete de Distribución Secundario B12, se encuentra ubicado en el Piso 12 Sección B – Servicio de Neumología, el mismo que se enlaza a través de Cableado Cat. 6, desde el Gabinete de Distribución Secundario B3.</p> <p>Este Rack cuenta con 22 UR, cuenta con dos enlaces broncales de cable de cobre UTP Cat. 6 el mismo que se conecta directamente al switch de borde configurado como cascada desde el GDS "C", aloja 01 Patch Panel de 48P Cat. 6, 01 Patch Panel de 24P Cat. 5e, cuenta con 01 conmutador de 24 puertos requerido, cuenta con 72 Puntos de red de los cuales 48 puntos son para el servicio de Datos y 24 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Hospitalización 3C Servicio de Medicina Interna 3, Cirugía General, UCIN3, Hospitalización 4C Servicio de Medicina Interna II, UCIN 4, Hospitalización 5C Servicio de Obstetricia y Neonatología" el cual es el encargado de distribuir los servicios de Voz, Data, cuenta con cableado UTP categoría 6 LSZH.</p> <p>Debe mencionarse que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.</p>		<p>COMENTARIO:</p> <p>Rack</p> <p>Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en la sala de espera del Servicio de Neumología, cabe mencionar que las bisagras de material "Antimonio" están deterioradas lo que dificulta realizar el mantenimiento preventivo y correctivo ante el inminente peligro de desprendimiento de estructura.</p> <p>Así mismo podemos evidenciar que no cuenta con sistema de eléctrico de contingencia, aterramiento de la estructura, y limitante de proyección a crecimiento de puntos de red contemplados en el mencionado segmento de red.</p> <p>Recomendaciones</p> <ul style="list-style-type: none"> Renovación de Gabinete de Comunicaciones, contemplando la instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones. 	





Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 19 – VISTA FRONTAL			
GABINETE C7			
Vista Frontal del Gabinete	Parte Posterior del Gabinete	Vista de la parte interna del Gabinete	Estado de la Unidad de Ventilación
			
COMENTARIOS			
<p>N° GABINETES: C7</p> <p>TIPO DE GABINETE: PARED</p> <p>DESCRIPCION: El Gabinete de Distribución Secundario C7, se encuentra ubicado en el Piso 7 Sector C - Servicio de Medicina Interna, el mismo que se enlaza a través de Cableado Cat. 6, desde el Gabinete de Distribución Secundario C.</p> <p>Este Rack cuenta con 22 UR, cuenta con dos enlaces troncales de cable de cobre UTP Cat. 6 el mismo que se conecta directamente al switch de borde configurado como cascada desde el GDS "C", aloja 01 Patch Panel de 48P Cat. 6, 01 Patch Panel de 24P Cat. 5e, cuenta con 01 conmutador de 24 puertos requerido, cuenta con 72 Puntos de red de los cuales 48 puntos son para el servicio de Datos y 24 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Hospitalización 6C Servicio de Medicina Interna IV, UCIN 6, Hospitalización 7C Servicio de Medicina Interna V, UCIN 7, Hospitalización 8C Servicio de Medicina Interna, Cirugía Plástica Reconstructiva" el cual es el encargado de distribuir los servicios de Voz, Datos, cuenta con cableado UTP categoría 6 LSZH.</p> <p>Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.</p>		<p>COMENTARIO:</p> <p>Rack</p> <p>Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en la sala de espera del Servicio de Medicina Interna, cabe mencionar que las bisagras de material "Antimonio" están deterioradas lo que dificulta realizar el mantenimiento preventivo y correctivo ante el inminente peligro de desprendimiento de estructura.</p> <p>Así mismo podemos evidenciar que no cuenta con sistema de eléctrico de contingencia, aterramiento de la estructura, y limitante de proyección o crecimiento de puntos de red contemplados en el mencionado segmento de red.</p> <p>Recomendaciones</p> <ul style="list-style-type: none"> Renovación de Gabinete de Comunicaciones, contemplando la Instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones. 	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 20 – VISTA FRONTAL			
GABINETE C10			
Vista Frontal del Gabinete	Parte Posterior del Gabinete	Vista de la parte interna del Gabinete	Estado de la Unidad de Ventilación
			
COMENTARIOS			
N° GABINETES: C10		COMENTARIO:	
TIPO DE GABINETE: PARED		Rack	
DESCRIPCION: El Gabinete de Distribución Secundario C10, se encuentra ubicado en el Piso 10 Sector C - Servicio de Medicina Interna III, el mismo que se enlaza a través de Cableado Cat. 6, desde el Gabinete de Distribución Secundario C.		Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en la sala de espera del Servicio de Medicina Interna, cabe mencionar que las bisagras de material "Antimonio" están deterioradas lo que dificulta realizar el mantenimiento preventivo y correctivo ante el inminente peligro de desprendimiento de estructura.	
Este Rack cuenta con 18 UR, cuenta con dos enlaces troncales de cable de cobre UTP Cat. 6 el mismo que se conecta directamente al switch de borde configurado como cascada desde el GDS "C", alija 01 Patch Panel de 48P Cat. 6, 01 Patch Panel de 24P Cat. 5e, cuenta con 01 conmutador de 24 puertos roqueado, cuenta con 72 Puntos de red de los cuales 48 puntos son para el servicio de Datos y 24 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Hospitalización 9C – Servicio de Medicina Interna Cirugía Plástica Reconstructiva, Hospitalización 9C – Servicio de Traumatología, URCA, Hospitalización 10C – Servicio de Medicina Interna III, UCIN 10, Hospitalización 11C – Servicio de Medicina Interna VI, UCIN 11" el cual es el encargado de distribuir los servicios de Voz, Data, cuenta con cableado UTP categoría 6 LSZH.		Así mismo podemos evidenciar que no cuenta con sistema de eléctrico de contingencia, aterramiento de la estructura, y limitante de proyección o crecimiento de puntos de red contemplados en el mencionado segmento de red.	
Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.		Recomendaciones	
		- Renovación de Gabinete de Comunicaciones, contemplando la instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones.	



Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 21 – VISTA FRONTAL			
GABINETE C13			
Vista Frontal del Gabinete	Parte Posterior del Gabinete	Vista de la parte Interna del Gabinete	Estado de la Unidad de Ventilación
			
COMENTARIOS			
<p>N° GABINETES: C13</p> <p>TIPO DE GABINETE: PARED</p> <p>DESCRIPCION: El Gabinete de Distribución Secundario C13, se encuentra ubicado en el Piso 13 Sector C - Servicio de Medicina Interna III, el mismo que se enlaza a través de Cableado Cat. 6, desde el Gabinete de Distribución Secundario C.</p> <p>Este Rack cuenta con 18 UR, cuenta con dos enlaces troncales de cable de cobre UTP Cat. 6 el mismo que se conecta directamente al switch de borde configurado como cascada desde el GDS "C", alojó 01 Patch Panel de 48P Cat. 6, 01 Patch Panel de 24P Cat. 5e, cuenta con 01 conmutador de 24 puertos roqueado, cuenta con 72 Puntos de red de los cuales 48 puntos son para el servicio de Datos y 24 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Hospitalización 12C – Servicio de Medicina Interna de Infectología, UCIN 12, Hospitalización 12C – Servicio de Neurocirugía Vertebral y Neuro Periférica, Piso 14 Central de Monitoreo" el cual es el encargado de distribuir los servicios de Voz, Delta, cuenta con cableado UTP categoría 6 LSZH.</p> <p>Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.</p>		<p>COMENTARIO:</p> <p>Rack</p> <p>Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en la sala de espera del Servicio de Medicina Interna III, cabe mencionar que las bisagras de material "Antimonio" están deterioradas lo que dificulta realizar el mantenimiento preventivo y correctivo ante el inminente peligro de desprendimiento de estructura.</p> <p>Así mismo podemos evidenciar que no cuenta con sistema de eléctrico de contingencia, aterramiento de la estructura, y limitante de proyección a crecimiento de puntos de red contemplados en el mencionado segmento de red.</p> <p>Recomendaciones</p> <ul style="list-style-type: none"> Renovación de Gabinete de Comunicaciones, contemplando la instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones. 	





Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 22 – VISTA FRONTAL			
GABINETE D			
Vista Frontal del Gabinete	Parte Posterior del Gabinete	Vista de la parte Interna del Gabinete	Estado de la Unidad de Ventilación
			
COMENTARIOS			
N° GABINETES: D	COMENTARIO:		
TIPO DE GABINETE: PARED	Rack		
<p>DESCRIPCIÓN: El Gabinete D, se encuentra ubicado en el Primer Piso – Junto al Servicio de Hemodiálisis, el mismo que se enlaza a través de fibra óptica desde el Gabinete de Distribución Principal F1, ubicado en el data center de la Oficina de Soporte Informático.</p> <p>Este Rack cuenta con 22 UR, Aloja una bandeja de fibra óptica de 3 Puertos, 3 Pares F.O Multimodo de 50/125 m, OM3 marca SIEMON, 01 Patch Panel de 48P Cat. 6, 01 Patch Panel de 24P Cat. 5e, cuenta con 01 conmutador de 24 puertos, cuenta con 72 Puntos de red de los cuales 48 puntos son para el servicio de Datos y 24 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Servicio de Hemodiálisis" es el encargado de distribuir los servicios de Voz, Datos y Video, cuenta con cableado UTP categoría 6 LSZH.</p> <p>Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.</p>	<p>Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en un pasadizo donde la afluencia de público es bastante considerable el mismo que representa un inminente peligro ante un desprendimiento de la estructura toda vez que las bisagras de material "Antimonio" están deterioradas.</p> <p>Así mismo podemos evidenciar que no existe sistema de eléctrico de contingencia, aterramiento de la estructura.</p> <p>La longitud de los Patch Cord utilizados en su mayoría son de tres metros, lo cual genera una mayor densidad de cableado saturando los ordenadores.</p> <p>Recomendaciones</p> <ul style="list-style-type: none"> - Renovación de Gabinete de Comunicaciones, contemplando la Instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones. 		

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 23 – VISTA FRONTAL			
GABINETE G			
Vista Frontal del Gabinete	Parte Posterior del Gabinete	Vista de la parte Interna del Gabinete	Estado de la Unidad de Ventilación
			
COMENTARIOS			
N° GABINETES: G	COMENTARIO:		
TIPO DE GABINETE: PISO	Rack		
DESCRIPCION: El Gabinete G, se encuentra ubicado en el Primer Piso - Block G – Servicio de Pediatría - Módulo de Citas, el mismo que se enlaza a través de fibra óptica desde el Gabinete de Distribución Principal F1, ubicado en el data center de la Oficina de Soporte Informático.	Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en el Block G – Servicio de Pediatría - Módulo de Citas, el mismo que el ambiente está sellado, no contando con sistema de enfriamiento.		
Este Gabinete cuenta con 44 UR, Aloja una bandeja de fibra óptica de 3 Puertos, 3 Pares F.O Multimodo de 50/125 m, OM3 marca SIEMON, 04 Patch Panel de 48P Cat. 6, 03 Patch Panel de 24P Cat. 6, 02 Patch Panel de 48P Cat. 5e, 01 Patch Panel de 24P Cat. 5e, cuenta con 08 conmutadores de 24 puertos requeado y 13 conmutadores ubicados en áreas de trabajo, cuenta con 384 Puntos de red de los cuales 264 puntos son para el servicio de Datos y 120 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Oficina de Control Interno, Marcador Block G, Banco de Organos - Laboratorio de Histocompatibilidad, Banco de Organos, Rayos X Pediátrica, Laboratorio Madre Niño, Bienestar Social, Módulo de Citas Pediátrica, Consultorios Externos Pediátricos, Almacén de Historias Clínicas Pediátrica, OGID, Hospitalización, Pediátrica, Sala de Operaciones, Clínica de Pediátrica", el cual es el encargado de distribuir los servicios de Voz, Data y Video, cuenta con cableado UTP categoría 6 LSZH.	Así mismo podemos evidenciar que existe saturación de cableado en la parte vertical y Horizontal toda vez que el mencionado Gabinete Cobertura EL Sótano, Primer Piso y Segundo Piso , Peinado del cableado es inadecuado, sistema de enfriamiento en mal estado, falta de mantenimiento a los equipos de conmutación.		
Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.	La longitud de los Patch Cord utilizados en su mayoría son de tres metros, lo cual genera una mayor densidad de cableado saturando los ordenadores.		
	Recomendaciones		
	- Renovación de Gabinete de Comunicaciones, contemplando la Instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones.		


Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 24 – VISTA FRONTAL			
GABINETE G3			
Vista Frontal del Gabinete	Parte Posterior del Gabinete	Vista de la parte interna del Gabinete	Estado de la Unidad de Ventilación
			
COMENTARIOS			
N° GABINETES: G3	COMENTARIO:		
TIPO DE GABINETE: PARED	Rack		
<p>DESCRIPCIÓN: El Gabinete de Distribución Secundario G3, se encuentra ubicado en el Primer Piso - Block G - Servicio de Pediatría - Unidad de Oncología Pediátrica, el mismo que se enlaza a través de fibra óptica desde el Gabinete de Distribución Principal F1, ubicado en el data center de la Oficina de Soporte Informático.</p> <p>Este Rack cuenta con 22 UR, Aloja una bandeja de fibra óptica de 3 Puertos, 3 Pares F.O Multimodo de 50/125 m, OMS marca SIEMON, 01 Patch Panel de 48P Cat. 6, 01 Patch Panel de 24P Cat. 6, 01 Patch Panel de 24P Cat. 5e, cuenta con 02 conmutadores de 24 puertos y 2 conmutadores ubicados en áreas de trabajo como cascadas, cuenta con 96 Puntos de red de los cuales 72 puntos son para el servicio de Datos y 24 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Servicio de Clínica Pediátrica, Oncología Pediátrica y Sala de Operaciones Pediátrica" es el encargado de distribuir los servicios de Voz, Datos y Video, cuenta con cableado UTP categoría 6 LSZH.</p> <p>Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.</p>	<p>Como se puede evidenciar en las imágenes la chepa de seguridad del GDS está en mal estado, así mismo está ubicado en el Block G - Servicio de Pediatría, en un cuarto de Deposito del Servicio existe un inminente peligro ante un desprendimiento de la estructura toda vez que las bisagras de material "Antimonio" están deterioradas.</p> <p>Así mismo podemos evidenciar que no existe sistema de eléctrico de contingencia, aterramiento de la estructura.</p> <p>La longitud de los Patch Cord utilizados en su mayoría son de tres metros, lo cual genera una mayor densidad de cableado saturando los ordenadores.</p> <p>Recomendaciones</p> <ul style="list-style-type: none"> - Renovación de Gabinete de Comunicaciones, contemplando la Instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones. 		

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 24 – VISTA FRONTAL			
GABINETE I1			
Vista Frontal del Gabinete	Parte Posterior del Gabinete	Vista de la parte Interna del Gabinete	Estado de la Unidad de Ventilación
			
COMENTARIOS			
N° GABINETES: 11	COMENTARIO:		
TIPO DE GABINETE: PISO	Rack		
DESCRIPCION: El Gabinete de Distribución Secundario I1, se encuentra ubicado en el Primer Piso - Block D – Servicio de Consulta Externa, el mismo que se enlaza a través de fibra óptica desde el Gabinete de Distribución Principal F1, ubicado en el data center de la Oficina de Soporte Informático.	Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en el pasadizo del Primer Piso - Block D – Servicio de Consulta Externa Adultos, el mismo que está expuesto a cualquier amenaza, no contando con sistema de enfriamiento.		
Este Gabinete cuenta con 44 UR, Aloja una bandeja de fibra óptica de 3 Puertos, 3 Pares F.O Multimodo de 50/125 m, OM3 marca SIEMON, 05 Patch Panel de 48P Cat. 6, 04 Patch Panel de 24P Cat. 6, 02 Patch Panel de 48P Cat. 5e, 01 Patch Panel de 24P Cat. 5e, cuenta con 07 conmutadores de 24 puertos requeado y 10 conmutadores ubicados en áreas de trabajo configurados como cascadas, cuenta con 456 Puntos de red de los cuales 336 puntos son para el servicio de Datos y 120 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Módulos de Consulta Externa 09 – 22, Auditorio N°1, Laboratorio de Hormonas, Cuerpo Médico, Control de Personal Médico, Anatomía Patológica, Archivo de Placas Radiográficas, Farmacia 2, Inteligencia Sanitaria, Oficina de Atención al Asegurado, Sala de Informes - Oficina de Atención al Asegurado, Fotografía médica - Servicio de Patología Quirúrgica Bueno, Unidad de Equipos Biomédicos y Electro médicos – UBE, Hormonas, Unidad de Seguridad Integral y Defensa Civil, Archivo de Historias Clínicas", el cual es el encargado de distribuir los servicios de Voz, Datos y Video, cuenta con cableado UTP categoría 6 LSZH.	Así mismo podemos evidenciar que existe saturación de cableado en la parte vertical y Horizontal toda vez que el mencionado Gabinete Cobertura EL Solano, Primer Piso, Peinado del cableado es inadecuado, sistema de enfriamiento en mal estado, falta de mantenimiento a los equipos de conmutación.		
Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de almacenamiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.	La longitud de los Patch Cord utilizados en su mayoría son de tres metros, lo cual genera una mayor densidad de cableado saturando los ordenadores.		
	Recomendaciones		
	- Renovación de Gabinete de Comunicaciones, contemplando la instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones.		





Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 25 – VISTA FRONTAL			
GABINETE 12			
Vista Frontal del Gabinete	Parte Posterior del Gabinete	Vista de la parte interna del Gabinete	Inadecuada Instalación de Equipos
			
COMENTARIOS			
N° GABINETES: 12	COMENTARIO:		
TIPO DE GABINETE: PISO	Rack		
DESCRIPCION: El Gabinete de Distribución Secundario 12, se encuentra ubicado en el Primer Piso - Block C – Servicio de Consulta Externa, el mismo que se enlaza a través de fibra óptica desde el Gabinete de Distribución Principal F1, ubicado en el data center de la Oficina de Soporte Informático.	Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en el pesadizo del Primer Piso - Block C – Servicio de Consulta Externa Adultos, el mismo que está expuesto a cualquier amenaza, no contando con sistema de enfriamiento.		
Este Gabinete cuenta con 44 UR, Aloja una bandeja de fibra óptica de 3 Puertos, 3 Pares F.O Multimodo de 50/125 m, OM3 marca SIEMON, 03 Patch Panel de 48P Cat. 6, 03 Patch Panel de 24P Cat. 6, 01 Patch Panel de 48P Cat. 5e, 01 Patch Panel de 24P Cat. 5e, cuenta con 06 conmutadores de 24 puertos requeado y 8 conmutadores ubicados en áreas de trabajo configurados como cascadas, cuenta con 288 Puntos de red de los cuales 216 puntos son para el servicio de Datos y 72 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Área de Recepción de Almacén de Material no Hospitalaria, Unidad de Mantenimiento e Infraestructura, Consultorios Externos de Adultos del 01 al 43, Módulos de Citas de 01-08, Archivo Central, Archivo de Tesorería, Almacén de Drogas, Unidad de Control Patrimonial", el cual es el encargado de distribuir los servicios de Voz, Datos y Video, cuenta con cableado UTP categoría 6 LSZH.	Así mismo podemos evidenciar que existe saturación de cableado en la parte vertical y Horizontal toda vez que el mencionado Gabinete Cobertura EL Sótano, Primer Piso, Peinado del cableado es inadecuado, sistema de enfriamiento en mal estado, falta de mantenimiento a los equipos de conmutación.		
Debe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.	La longitud de los Patch Cord utilizados en su mayoría son de tres metros, lo cual genera una mayor densidad de cableado saturando los ordenadores.		
	Recomendaciones		
	- Renovación de Gabinete de Comunicaciones, contemplando la instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones.		

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)







FOTO 26 – VISTA FRONTAL			
GABINETE J			
Vista Frontal del Gabinete	Parte Posterior del Gabinete	Vista de la parte Interna del Gabinete	Inadecuada Instalación de Equipos
			
COMENTARIOS			
N° GABINETES: J	COMENTARIO:		
TIPO DE GABINETE: PARED	Rack		
DESCRIPCIÓN: El Gabinete de Distribución Secundario J, se encuentra ubicado en el sótano – Puertas y Ventanas Vidriera – B.U.C, el mismo que se enlaza a través de fibra óptica desde el Gabinete de Distribución Principal F1, ubicado en el data center de la Oficina de Soporte Informático.	Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en el sótano – Puertas y Ventanas Vidriera – B.U.C.		
Este Rack cuenta con 18 UR, Aloja una bandeja de fibra óptica de 3 Puertos, 3 Pares F.O Multimodo de 50/125 m, OM3 marca SIEMON, 01 Patch Panel de 24P Cat. 6, 01 Patch Panel de 24P Cat. 5e, cuenta con 01 conmutador de 24 puertos y 2 conmutadores ubicados en áreas de trabajo como cascadas, cuenta con 48 Puntos de red de los cuales 24 puntos son para el servicio de Datos y 24 del servicio de 'Voz', brinda servicio a las áreas de trabajo de 'Área de Soporte, Área de Comunicaciones, Área de Transportes, Talleres de Pintura, Persianas, Puertas y Ventanas, Jefatura de Caseta de Vigilancia, Cord Servicios Generales, Relaciones Públicas, Sala de Espera de Emergencia Adultos' es el encargado de distribuir los servicios de Voz, Datos y Video, cuenta con cableado UTP categoría 6 LSZH.	Así mismo podemos evidenciar que no existe sistema de eléctrico de contingencia, aterramiento de la estructura.		
Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.	La longitud de los Patch Cord utilizados en su mayoría son de tres metros, lo cual genera una mayor densidad de cableado saturando los ordenadores.		
	Recomendaciones		
	<ul style="list-style-type: none"> - Renovación de Gabinete de Comunicaciones, contemplando la Instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones. 		

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)







FOTO 27 – VISTA FRONTAL

GABINETE K			
Vista Frontal del Gabinete	Parte Posterior del Gabinete	Vista de la parte Interna del Gabinete	Inadecuada Instalación de Equipos
			
COMENTARIOS			
N° GABINETES: K	COMENTARIO:		
TIPO DE GABINETE: PARED	<p>Rack</p> <p>Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en el Block K en las Instalaciones del Servicio Salud Mental – Hospital de Día, en el hall de espera existe un inminente peligro ante un desprendimiento de la estructura toda vez que las bisagras de material "Antimonio" están deterioradas.</p> <p>Así mismo podemos evidenciar que no existe sistema de eléctrico de contingencia, aterramiento de la estructura.</p> <p>La longitud de los Patch Cord utilizados en su mayoría son de tres metros, lo cual genera una mayor densidad de cableado saturando los ordenadores.</p> <p>Recomendaciones</p> <ul style="list-style-type: none"> Renovación de Gabinete de Comunicaciones, contemplando la Instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones. 		
<p>DESCRIPCIÓN: El Gabinete de Distribución Secundario K, se encuentra ubicado en el Block K en las Instalaciones del Servicio Salud Mental – Hospital de Día, el mismo que se enlaza a través de fibra óptica desde el Gabinete de Distribución Principal F1, ubicado en el data center de la Oficina de Soporte Informático</p> <p>Este Rack cuenta con 22 UR, Aloja una bandeja de fibra óptica de 3 Puertos, 3 Pares F.O Multimodo de 50/125 m, OM3 marca SIEMON, 03 Patch Panel de 48P Cat. 6, 01 Patch Panel de 24P Cat. 5e, cuenta con 03 conmutadores de 24 puertos y 1 conmutador ubicado en áreas de trabajo como cascadas, cuenta con 96 Puntos de red de los cuales 72 puntos son para el servicio de Datos y 24 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Servicio de Salud Mental, Emergencia de Salud Mental, Hospitalización Hombres, Mujeres, Consulta Externa, Hospital de Día, Unidad de Fármaco Dependencia" es el encargado de distribuir los servicios de Voz, Datos y Video, cuenta con cableado UTP categoría 6 LSZH.</p> <p>Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.</p>			

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 28 – VISTA FRONTAL			
GABINETE L			
Vista Frontal del Gabinete	Parte Posterior del Gabinete	Vista de la parte Interna del Gabinete	Saturación de cables
			
COMENTARIOS			
<p>N° GABINETES: L</p> <p>TIPO DE GABINETE: PARED</p>		<p>COMENTARIO:</p> <p>Rack</p> <p>Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en el Block D en las Instalaciones del Servicio Emergencia Pediátrica - Estación de Camilla, en la estación camilla se ha instalado un típico de laboratorio el mismo que existe un inminente peligro ante un desprendimiento de la estructura toda vez que las bisagras de material "Antimonio" están deterioradas, el cual puede causar daños personales y materiales.</p> <p>Así mismo podemos evidenciar que no existe sistema de eléctrico de contingencia, aterramiento de la estructura.</p> <p>La longitud de los Patch Cord utilizados en su mayoría son de tres metros, lo cual genera una mayor densidad de cableado saturando los ordenadores.</p> <p>Recomendaciones</p> <ul style="list-style-type: none"> - Renovación de Gabinete de Comunicaciones, contemplando la instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones. 	
<p>descripcion: El Gabinete de Distribución Secundario L, se encuentra ubicado en el Block D en las Instalaciones del Servicio Emergencia Pediátrica - Estación de Camilla, el mismo que se enlaza a través de fibra óptica desde el Gabinete de Distribución Principal F1, ubicado en el data center de la Oficina de Soporte Informático.</p> <p>Este Rack cuenta con 22 UR, Aloja una bandeja de fibra óptica de 3 Puertos, 3 Pares F.O Multimodo de 50/125 m, OMB marca SIEMON, 01 Patch Panel de 48P Cat. 6, 01 Patch Panel de 24P Cat. 6, 01 Patch Panel de 48P Cat. 5e, cuenta con 03 conmutadores de 24 puertos y 03 conmutadores ubicado en áreas de trabajo como cascadas, cuenta con 120 Puntos de red de los cuales 72 puntos son para el servicio de Datos y 48 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Emergencia Ginecológica, Emergencia Pediátrica, Rehabilitación" es el encargado de distribuir los servicios de Voz, Data y Video, cuenta con cableado UTP categoría 6 LSZH.</p> <p>Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.</p>			





Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 29 – VISTA FRONTAL			
GABINETE M			
Vista Frontal del Gabinete	Vista Frontal del desorden existente	Parte Posterior del Gabinete	Saturación de cables
			
COMENTARIOS			
N° GABINETES: M		COMENTARIO:	
TIPO DE GABINETE: PISO		Gabinete	
<p>DESCRIPCIÓN: El Gabinete de Distribución Secundario M, se encuentra ubicado en las Instalaciones del Área de Adquisiciones – Playa Miller Edificio de la Sede Central de EsSalud, el mismo que se enlaza a través de fibra óptica desde el Gabinete de Distribución Principal F1, ubicado en el data center de la Oficina de Soporte Informático</p> <p>Este Gabinete cuenta con 44 UR, Aloja una bandeja de fibra óptica de 3 Puntos, 3 Pares F.O Multimodo de 50/125 m, OM3 marca SIEMON, 06 Patch Panel de 24P Cat. 6, 02 Patch Panel de 48P Cat. 5e, 02 Patch Panel de 24P Cat. 5e, cuenta con 06 conmutadores de 24 puertos requerido y 7 conmutadores ubicados en áreas de trabajo configurados como cascadas, cuenta con 288 Puntos de red de los cuales 144 puntos son para el servicio de Datos y 144 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Oficina de Logística, Unidad de Programación, Unidad de Adquisiciones, Oficina de Planificación Operativa, Unidad de Selección de Personal y Área de Facturación, Oficina N°136 CEBIT, Oficina de Contabilidad", el cual es el encargado de distribuir los servicios de Voz, Datos y Video, cuenta con cableado UTP categoría 6 LSZH.</p> <p>Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.</p>		<p>Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en el Área de Adquisiciones – Playa Miller Edificio de la Sede Central de EsSalud, el mismo que está expuesto a cualquier amenaza, no contando con sistema de enfriamiento.</p> <p>Así mismo podemos evidenciar que existe saturación de cableado en la parte vertical y Horizontal toda vez que el mencionado Gabinete Cobertura EL 3 Pisos, Peinado del cableado es inadecuado, sistema de enfriamiento en mal estado, falta de mantenimiento a los equipos de conmutación, no cuenta con las puertas laterales y frontales.</p> <p>La longitud de los Patch Cord utilizados en su mayoría son de tres metros, lo cual genera una mayor densidad de cableado saturando los ordenadores.</p> <p>Recomendaciones</p> <ul style="list-style-type: none"> - Renovación de Gabinete de Comunicaciones, contemplando la instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones. 	





Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 30 – VISTA FRONTAL			
GABINETE N			
Vista frontal del Gabinete	Vista frontal del desorden existente	Parte Posterior del Gabinete	Equipos activos
			
COMENTARIOS			
N° GABINETES: N	COMENTARIO:		
TIPO DE GABINETE: PISO	Gabinete		
DESCRIPCION: El Gabinete de Distribución Secundario N, se encuentra ubicado en las Instalaciones de la Red Desconcentrada Rebagliati, Playa Miller Edificio de la Sede Central de EsSalud, el mismo que se enlaza a través de fibra óptica desde el Gabinete de Distribución Principal F1, ubicado en el data center de la Oficina de Soporte Informático.	Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en el Instalaciones de la Red Desconcentrada Rebagliati, Playa Miller Edificio de la Sede Central de EsSalud, el mismo que está expuesto a cualquier amenaza, no contando con sistema de enfriamiento.		
Este Gabinete cuenta con 44 UR, Aloja una bandeja de fibra óptica de 3 Puertos, 3 Pares F.O Multimodo de 50/125 m, OM3 marca SIEMON, 03 Patch Panel de 24P Cat. 6, 01 Patch Panel de 24P Cat. 5e, cuenta con 02 conmutadores de 24 puertos rackeado y 6 conmutadores ubicados en áreas de trabajo configurados como cascadas, cuenta con 96 Puntos de red de los cuales 72 puntos son para el servicio de Datos y 24 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Gerencia de Red Desconcentrada Rebagliati, Oficina de Recursos humanos, unidad de administración de personal, Unidad de Legajos, Control de Tiempo, Unidad de Tramite", el cual es el encargado de distribuir los servicios de Voz, Data y Video, cuenta con cableado UTP categoría 6 LSZH.	Así mismo podemos evidenciar que no cuenta con sistema de enfriamiento, falta de mantenimiento a los equipos de conmutación.		
Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.	La longitud de los Patch Cord utilizados en su mayoría son de tres metros, lo cual genera una mayor densidad de cableado saturando los ordenadores.		
	Recomendaciones		
	- Renovación de Gabinete de Comunicaciones, contemplando la Instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones.		

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 31 – VISTA FRONTAL			
GABINETE N			
Vista Frontal del Gabinete	Vista Frontal del desorden existente	Parte Posterior del Gabinete	Equipos activos
			
COMENTARIOS			
N° GABINETES: N	COMENTARIO:		
TIPO DE GABINETE: PARED	Rack		
DESCRIPCION: El Gabinete de Distribución Secundario N, se encuentra ubicado en las Instalaciones del Servicio de Emergencia - Tópico de Cirugía, el mismo que se enlaza a través de fibra óptica desde el Gabinete de Distribución Principal F1, ubicado en el data center de la Oficina de Soporte Informático.	Como se puede evidenciar en las imágenes la chapa de seguridad del GDS está en mal estado, así mismo está ubicado en el Block N en las Instalaciones del Servicio de Emergencia - Tópico de Cirugía.		
Este Rack cuenta con 18 UR, Aloja una bandeja de fibra óptica de 3 Puertos, 3 Pares F.O Multimodo de 50/125 m, OM3 marca SIEMON, 01 Patch Panel de 24P Cat. 6, 01 Patch Panel de 24P Cat. 5e, cuenta con 02 conmutadores de 24 puertos, cuenta con 48 Puntos de red de los cuales 24 puntos son para el servicio de Datos y 24 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Servicio de Emergencia, Tópico de Cirugía" es el encargado de distribuir los servicios de Voz, Data y Video, cuenta con cableado UTP categoría 6 LSZH.	Así mismo podemos evidenciar que no existe sistema de eléctrico de contingencia, aterramiento de la estructura, Chapa de seguridad en mal estado.		
Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.	La longitud de los Patch Cord utilizados en su mayoría son de tres metros, lo cual genera una mayor densidad de cableado saturando los ordenadores.		
	El mantenimiento preventivo y correctivo del gabinete y equipos activos es complicado realizarlo toda vez que es un tópico de emergencia donde siempre existen personas en el ambiente se recomienda sacarlo a otro ambiente no crítico.		
	Recomendaciones		
	<ul style="list-style-type: none"> Renovación de Gabinete de Comunicaciones, contemplando la Instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones. 		

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 32 – VISTA FRONTAL			
GABINETE RS			
Vista Frontal del Gabinete	Vista Frontal del Resorden existente	Parte Posterior del Gabinete	Equipos activos
			
COMENTARIOS			
N° GABINETES:RS		COMENTARIO: Rack Como se puede evidenciar en las imágenes es una estructura de rack nuevo el mismo que no cuenta problemas, así mismo está ubicado en Instalaciones del Medicina Nuclear. Así mismo podemos evidenciar que no existe sistema de eléctrico de contingencia, Chapa de seguridad en mal estado.	
TIPO DE GABINETE: PARED			
DESCRIPCIÓN: El Gabinete de Distribución Secundario RS, se encuentra ubicado en las Instalaciones del Medicina Nuclear, el mismo que se enlaza a través de fibra óptica desde el Gabinete de Distribución Principal F1, ubicado en el data center de la Oficina de Soporte Informático. Este Rack cuenta con 18 UR, Aloja una bandeja de fibra óptica de 3 Puertos, 3 Pares F.O Multimodo de 50/125 m, OM3 marca Furukawa, 03 Patch Panel de 24P Cat. 6, 01 Patch Panel de 24P Cat. 5e, cuenta con 03 conmutadores de 24 puertos, cuenta con 96 Puntos de red de los cuales 72 puntos son para el servicio de Datos y 24 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Medicina Nuclear" es el encargado de distribuir los servicios de Voz, Data y Video, cuenta con cableado UTP categoría 6 LSZH. Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.			





Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 33 – VISTA FRONTAL			
GABINETE B1-S			
Vista Frontal del gabinete	Vista Frontal del desarrollo existente	Plano posterior del gabinete	Equipos activos
			
COMENTARIOS			
N° GABINETES: B1-S		COMENTARIO: Gabinete Como se puede evidenciar es un Gabinete de Comunicaciones Nuevo instalado por la empresa ROCA, en coordinación con la Oficina de Soporte Informático.	
TIPO DE GABINETE: PISO			
DESCRIPCIÓN: El Gabinete de Distribución Secundario B1-S, se encuentra ubicado en el Sótano en el cuarto de Comunicaciones del Acelerador Lineal, el mismo que se enlaza a través de Cableado Cat. 6, desde el Gabinete de Distribución Secundario B1. Este Rack cuenta con 44 UR, cuenta con un enlace troncal de cable de cobre UTP Cat. 6 el mismo que se conecta directamente al switch de borde configurado como cascada desde el GDS "B1", aloja 02 Patch Panel de 24P Cat. 6, cuenta con 03 conmutadores de 24 puertos requerido, cuenta con 48 Puntos de red de los cuales 36 puntos son para el servicio de Datos y 12 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Servicio de Resonancia Magnética" el cual es el encargado de distribuir los servicios de Voz, Datos, y Video cuenta con cableado UTP categoría 6 LSZH. Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.			

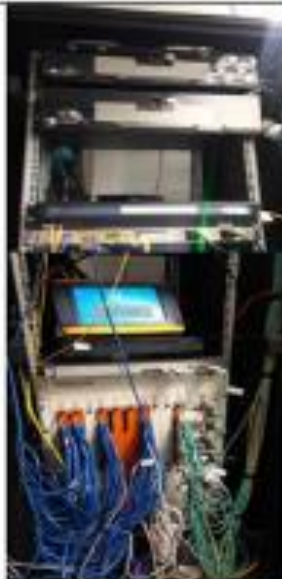



Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 34 – VISTA FRONTAL			
GABINETE F			
Vista Frontal del Gabinete	Vista Frontal del desorden existente	Parte Posterior del Gabinete	Equipos activos
			
COMENTARIOS			
<p>N° GABINETES: F</p> <p>TIPO DE GABINETE: PISO</p> <p>DESCRIPCION: El Gabinete de Distribución Secundario F se encuentra ubicado en las Instalaciones de la Oficina de Soporte Informático, ubicado en el Centro de Datos.</p> <p>Este Gabinete cuenta con 44 UR, Alojamiento 06 Patch Panel de 48P Cat. 6, 02 Patch Panel de 48P Cat. 5e, 01 Patch Panel de 24P Cat. 5e, cuenta con 04 conmutadores de 24 puertos requerido, cuenta con 408 Puntos de red de los cuales 288 puntos son para el servicio de Datos y 120 del servicio de "Voz", brinda servicio a las áreas de trabajo de "Gerencia General, Gerencia Quirúrgica, Gerencia Clínica, Gerencia Ayuda Diagnóstico y Tratamiento, Gerencia Médica, Oficina de Administración, Oficina de Asuntos Jurídicos, Unidad de Trámite Documentario, Oficina de Gestión y Desarrollo, Oficina de Estadística, Oficina de Tesorería y Presupuesto, Oficina de Admisión y Registros Médicos, Oficina de Soporte Informático, Sala de Servidores – (Data Center), Oficina de Aseguramiento, Oficina de Finanzas, Unidad de Referencias y Contra-Referencias, Oficina de Archivo e Historia Clínica, Oficina de Voluntariado, Oficina de Atención al Asegurado, Oficina de Imagen Institucional y Comunicaciones, Unidad de Quimioterapia Ambulatoria", el cual es el encargado de distribuir los servicios de Voz, Datos y Video, cuenta con cableado UTP categoría 6 LSZH.</p> <p>Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.</p>		<p>COMENTARIO:</p> <p>Gabinete</p> <p>Como se puede evidenciar en las imágenes existe un desorden en el cableado debido a la sobresaturación de puntos de red existentes, así mismo el gabinete de comunicaciones no es el adecuado teniendo en cuenta que no cuenta con ordenadores verticales.</p> <p>Se debe considerar la instalación de un nuevo gabinete para descongestionar el existente y así tener disponibilidad para instalaciones futuras.</p> <p>Recomendaciones</p> <ul style="list-style-type: none"> - Renovación de Gabinete de Comunicaciones, contemplando la instalación de Sistema Eléctrico de la red de datos, Sistema de puesta a tierra, UPS cumpliendo los estándares de la industria de telecomunicaciones. 	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)


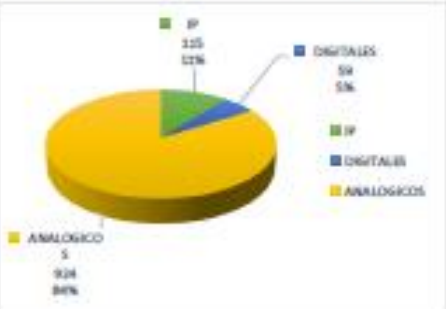


FOTO 35 – VISTA FRONTAL			
GABINETE F1			
Vista Frontal del Gabinete	Vista Frontal del desorden existente	Parte Posterior del Gabinete	Equipos activos
			
COMENTARIOS			
N° GABINETES: F1		COMENTARIO:	
TIPO DE GABINETE: PISO		Gabinete	
<p>DESCRIPCION: El Gabinete de Distribución Secundario F se encuentra ubicado en las Instalaciones de la Oficina de Soporte Informático, ubicado en el data center de la Oficina de Soporte Informático.</p> <p>Este Gabinete cuenta con 44 UR, Aloja 02 bandeja de fibra óptica de 24 Puertos, 3 Pares F.O Multimodo de 50/125 m, OM3 marca SIEMON, 01 Bandeja de Fibra Óptica del enlace del Multiplexor "Fibra Oscura" con sede Central, cuenta con 02 conmutadores de capa 3 uno marca Alcatel Lucent 9800 CORE Principal que cuenta con 8 Tarjetas de 24 puertos 7 Gigabits y Tarjeta de Fibra Óptica, cuenta con 04 fuentes redundantes, 02 tarjetas controladores, 01 switch de Core Cisco de 12 puertos el mismo que está dedicado para la plataforma de cámaras, así mismo existen 12 conmutadores configurados como cascada toda vez que no se cuenta con disponibilidad de puertos, las áreas de trabajo que cobertura son las del Gabinete F", el cual es el encargado de distribuir los servicios de Voz, Data y Video, cuenta con cableado UTP categoría 6 LSZH.</p> <p>Cabe mencionar que no cuenta con sistema de enfriamiento, sistema de aterramiento, sistema eléctrico de contingencia, UPS, Lo que no garantiza la continuidad operativa del servicio.</p>		<p>Como se puede evidenciar en las imágenes Gabinete de Comunicaciones aloja el Core Principal, bandeja Principal de Fibra Óptica, Core de Cámaras, cabe mencionar que no se cuenta con un CORE de respaldo en caso que caiga el actual, los servidores esta conectados directamente lo que genera una vulnerabilidad, por tema de seguridad los servidores deben estar en obo switch de CORE exclusivo contemplando redundancia,</p> <p>Los Puntos de que están conectados a los servidores están conectados directamente al switch de CORE, no cumpliendo con las normas establecidas.</p>	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



ANEXO 3: TELEFONIA
Fotos del 1 al 12

15. TELEFONO.																													
CANT.	COMENTARIOS	OBJETIVO VISUAL																											
12	2 en el mejor estado y 6 para las mas deficientes. Indicar el Piso, Área o Zona. 4 en central telefónica (Vista Frontal / Posterior / Vista Oblicua, Panorámica, y que se visualice la marca, modelo y puertos usados).	Estado/Tipo de Teléfono.																											
FOTO 1 – MEJOR ESTADO "A".																													
																													
COMENTARIOS																													
PROPIO MARCA: ALCATEL MODELO: OmniPCX Enterprise Communication 4400 TECNOLOGIA: CENTRAL HIBRIDA (Telefonía Analógica, Digital e IP) DESCRIPCION: - Consta de 03 gabinetes HW Crystal M2 de dos ACT cada uno, pueden albergar hasta 28 interfaces. Como elemento redundante se cuenta con un Servidor IBM System X.		Comentario: - La Central Telefónica del Hospital Rebagliati fue instalada el año 2005, la misma que es una extensión de la central telefónica ubicada en Sede Central, la misma que está configurada en modo redundante en ambas sedes. - Actualmente el Hospital Rebagliati cuenta con 1008 anexos de los cuales están distribuidos de la siguiente manera 115 teléfonos ip, 59 Teléfonos Digitales y 824 Teléfonos analógicos. - Cabe mencionar que actualmente existe una demanda de 500 anexos, los mismos que son solicitados en reiteradas ocasiones por los servicios asistenciales y a su vez a sede central. - Frente a esta demanda de los servicios se han instalado hasta el 2016, 100 conexiones tipo puente en telefonía analógica.																											
<table border="1"> <thead> <tr> <th colspan="3">HW CRYSTAL NRO. 4 y 7</th> </tr> <tr> <th>Interfaces</th> <th>Descripción</th> <th>Cantidad</th> </tr> </thead> <tbody> <tr> <td>e232</td> <td>2 Interfaz analógica de 32 pto.</td> <td>34</td> </tr> <tr> <td>NDD2, LSX5</td> <td>Troncales</td> <td>5</td> </tr> <tr> <td>INIT-IP2</td> <td>Enlace entre HW y voz IP</td> <td>2</td> </tr> <tr> <td>eUA32</td> <td>2 Interfaz digital 32 pto.</td> <td>8</td> </tr> <tr> <td>GPA2</td> <td>2 Generador de tonos</td> <td>2</td> </tr> <tr> <td>N9BAE-2</td> <td>2 Interfaz E1/RDSI</td> <td>2</td> </tr> <tr> <td>PCM2</td> <td>Linka PCM</td> <td>1</td> </tr> </tbody> </table>		HW CRYSTAL NRO. 4 y 7			Interfaces	Descripción	Cantidad	e232	2 Interfaz analógica de 32 pto.	34	NDD2, LSX5	Troncales	5	INIT-IP2	Enlace entre HW y voz IP	2	eUA32	2 Interfaz digital 32 pto.	8	GPA2	2 Generador de tonos	2	N9BAE-2	2 Interfaz E1/RDSI	2	PCM2	Linka PCM	1	
HW CRYSTAL NRO. 4 y 7																													
Interfaces	Descripción	Cantidad																											
e232	2 Interfaz analógica de 32 pto.	34																											
NDD2, LSX5	Troncales	5																											
INIT-IP2	Enlace entre HW y voz IP	2																											
eUA32	2 Interfaz digital 32 pto.	8																											
GPA2	2 Generador de tonos	2																											
N9BAE-2	2 Interfaz E1/RDSI	2																											
PCM2	Linka PCM	1																											
<table border="1"> <thead> <tr> <th colspan="3">HW-CRYSTAL NRO. 8</th> </tr> <tr> <th>Interfaces</th> <th>Descripción</th> <th>Cantidad</th> </tr> </thead> <tbody> <tr> <td>NDD2, LSX5</td> <td>Troncales</td> <td>3</td> </tr> <tr> <td>GPA2</td> <td>Generador de tonos</td> <td>1</td> </tr> <tr> <td>INIT-IP2</td> <td>Enlace entre HW y voz IP</td> <td>1</td> </tr> </tbody> </table>		HW-CRYSTAL NRO. 8			Interfaces	Descripción	Cantidad	NDD2, LSX5	Troncales	3	GPA2	Generador de tonos	1	INIT-IP2	Enlace entre HW y voz IP	1													
HW-CRYSTAL NRO. 8																													
Interfaces	Descripción	Cantidad																											
NDD2, LSX5	Troncales	3																											
GPA2	Generador de tonos	1																											
INIT-IP2	Enlace entre HW y voz IP	1																											
																													

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 2 – MEJOR ESTADO “B”.



COMENTARIOS

<p>PROPIO</p> <p>MARCA: ALCATEL</p> <p>MODELO: OmniPCX Enterprise Communication 4400</p> <p>TECNOLOGIA: CENTRAL HIBRIDA (Telefonía Analógica, Digital e IP)</p> <p>DESCRIPCION: Equipos Periféricos</p> <table border="1"> <thead> <tr> <th>Descripción</th> <th>Marcas/Modelos</th> <th>Cod. Pat.</th> </tr> </thead> <tbody> <tr> <td>Switch</td> <td>Alcatel OmniStack 6124</td> <td>0062015404</td> </tr> <tr> <td>Servidor</td> <td>IBM System X 3250 M2</td> <td>00882394</td> </tr> <tr> <td>UPS</td> <td>PCM POWERCOM UL3-1800 (KVA (arrivado))</td> <td>0062015104</td> </tr> <tr> <td>Battery Pack</td> <td>RAATTIGPAQ</td> <td>0062015204</td> </tr> <tr> <td>Btu. De Baterías</td> <td>DCSB 36 Silver Plus 2 4</td> <td>Si</td> </tr> <tr> <td>Refrigerador/ventilador</td> <td>Energy Prod FRC4EV75A</td> <td>Si</td> </tr> <tr> <td>Consolas celular</td> <td>82 Tipos Multimedios E1</td> <td>00887221,00887249</td> </tr> <tr> <td colspan="3" style="text-align: center;">Consolas de operadores</td> </tr> <tr> <td>04 Keyboard</td> <td>Alcatel 8049-4950 (1 arrivado)</td> <td>00882411,00882408 00882409,00882418</td> </tr> <tr> <td>03 CPU</td> <td>Dell Vostro 220e</td> <td>00882400,00882402</td> </tr> <tr> <td>03 Monitor</td> <td>Dell</td> <td>00882390,00882396 00882397</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>ANALÓGICOS</th> <th>MODELO</th> </tr> </thead> <tbody> <tr> <td>Alcatel</td> <td>3618 Mary, Temporis Pro 12</td> </tr> <tr> <td>Panasonic</td> <td>KX-TS508LX</td> </tr> <tr> <td>Samsung</td> <td>P2108</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>DIGITALES</th> <th>MODELO</th> </tr> </thead> <tbody> <tr> <td>Alcatel</td> <td>Raflex 4028</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>IP</th> <th>MODELO</th> </tr> </thead> <tbody> <tr> <td>Alcatel</td> <td>IP700ak 4018, IP700ak 4028</td> </tr> </tbody> </table>	Descripción	Marcas/Modelos	Cod. Pat.	Switch	Alcatel OmniStack 6124	0062015404	Servidor	IBM System X 3250 M2	00882394	UPS	PCM POWERCOM UL3-1800 (KVA (arrivado))	0062015104	Battery Pack	RAATTIGPAQ	0062015204	Btu. De Baterías	DCSB 36 Silver Plus 2 4	Si	Refrigerador/ventilador	Energy Prod FRC4EV75A	Si	Consolas celular	82 Tipos Multimedios E1	00887221,00887249	Consolas de operadores			04 Keyboard	Alcatel 8049-4950 (1 arrivado)	00882411,00882408 00882409,00882418	03 CPU	Dell Vostro 220e	00882400,00882402	03 Monitor	Dell	00882390,00882396 00882397	ANALÓGICOS	MODELO	Alcatel	3618 Mary, Temporis Pro 12	Panasonic	KX-TS508LX	Samsung	P2108	DIGITALES	MODELO	Alcatel	Raflex 4028	IP	MODELO	Alcatel	IP700ak 4018, IP700ak 4028	<p>Comentario:</p> <ul style="list-style-type: none"> - Las consolas instaladas en el año 2005 a la fecha, están presentando problemas contando con una totalmente inoperativa, 01 con funcionamiento irregular y 02 en condiciones totalmente operativas. - Falta de mantenimiento preventivo y correctivo de equipos de comunicaciones como son switch y servidor. - En lo concerniente a las tarjetas de digitales y analógicas presentan deformaciones en la carcasa debido fallas en el sistema de enfriamiento. - El sistema de enfriamiento que cuenta es tipo confort el mismo que no es el adecuado para este tipo de ambientes, concluyendo que debe ser un sistema de precisión redundante.
Descripción	Marcas/Modelos	Cod. Pat.																																																			
Switch	Alcatel OmniStack 6124	0062015404																																																			
Servidor	IBM System X 3250 M2	00882394																																																			
UPS	PCM POWERCOM UL3-1800 (KVA (arrivado))	0062015104																																																			
Battery Pack	RAATTIGPAQ	0062015204																																																			
Btu. De Baterías	DCSB 36 Silver Plus 2 4	Si																																																			
Refrigerador/ventilador	Energy Prod FRC4EV75A	Si																																																			
Consolas celular	82 Tipos Multimedios E1	00887221,00887249																																																			
Consolas de operadores																																																					
04 Keyboard	Alcatel 8049-4950 (1 arrivado)	00882411,00882408 00882409,00882418																																																			
03 CPU	Dell Vostro 220e	00882400,00882402																																																			
03 Monitor	Dell	00882390,00882396 00882397																																																			
ANALÓGICOS	MODELO																																																				
Alcatel	3618 Mary, Temporis Pro 12																																																				
Panasonic	KX-TS508LX																																																				
Samsung	P2108																																																				
DIGITALES	MODELO																																																				
Alcatel	Raflex 4028																																																				
IP	MODELO																																																				
Alcatel	IP700ak 4018, IP700ak 4028																																																				

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 3 – CONDICIONES DEFICIENTES “A”.



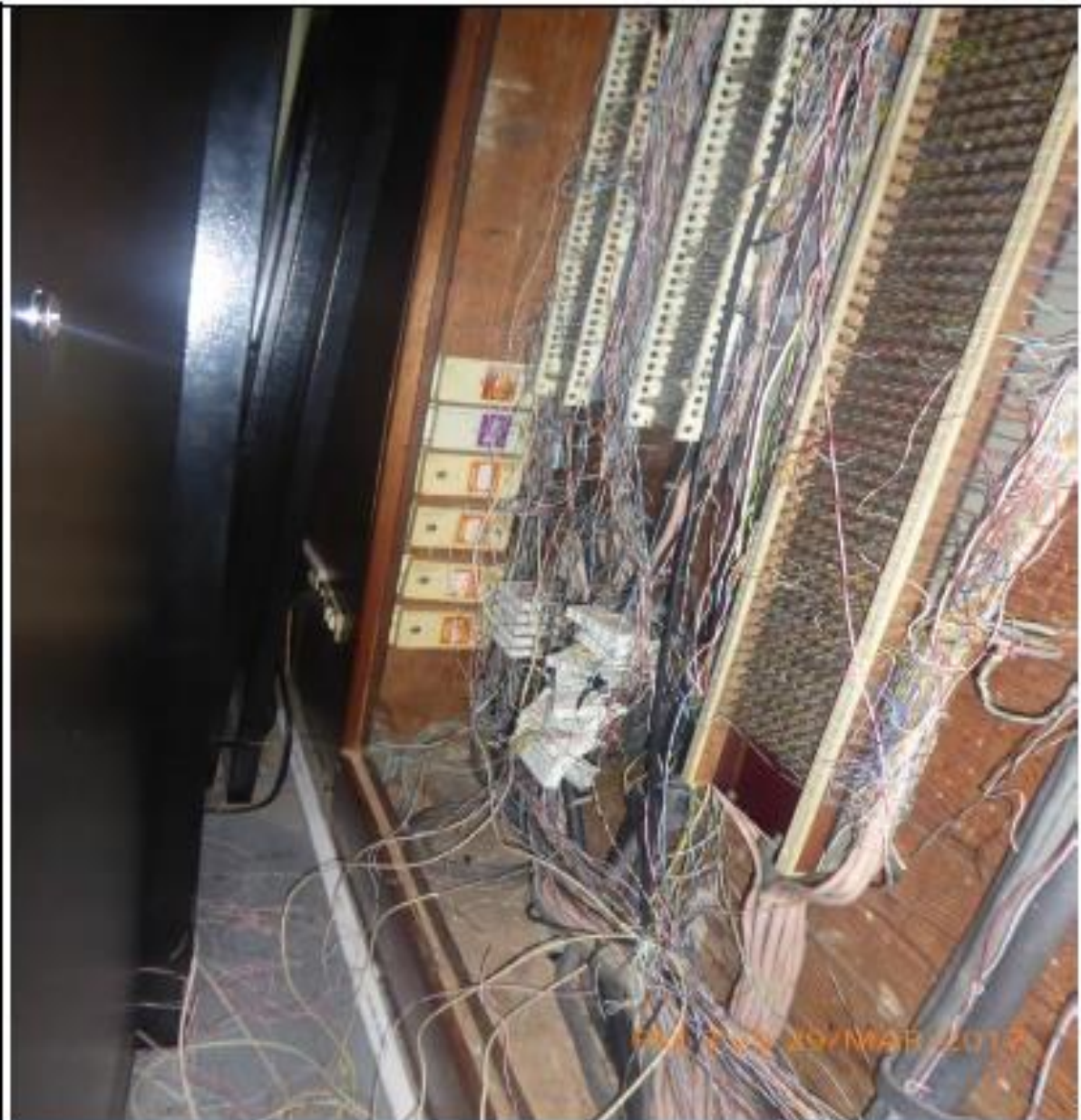
COMENTARIOS

PROPIO	Comentario:
MARCA: ALCATEL	
MODELO: OmniPCX Enterprise Communication 4400	
TECNOLOGIA: CENTRAL HIBRIDA (Telefonía Analoga, Digital e IP)	
PROPIO	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 4 - CONDICIONES DEFICIENTES "B".



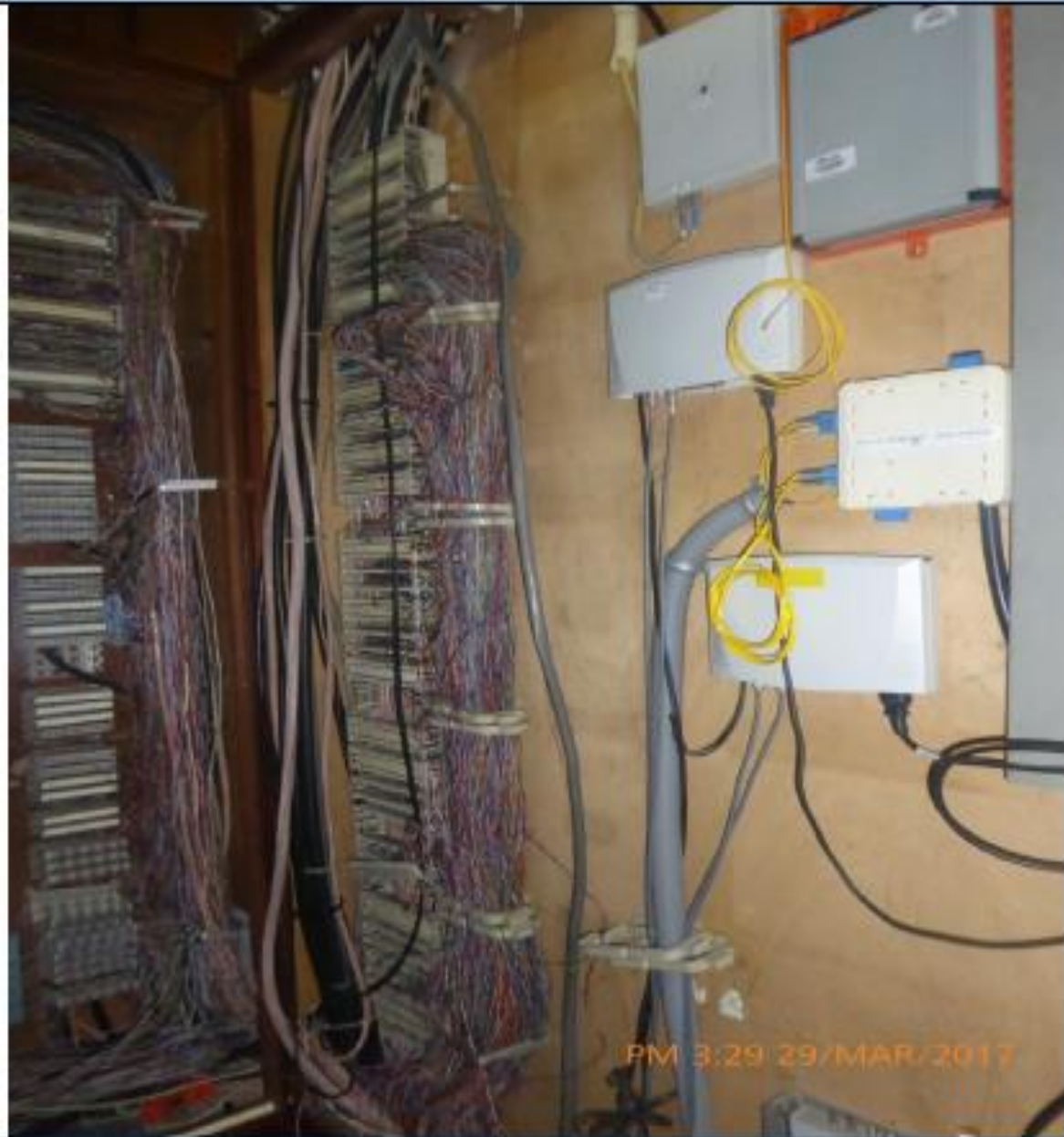
COMENTARIOS

PROPIO	Comentario: Borneras de entrada de Líneas Troncales de la telefonía analógica digital.
MARCA: ALCATEL	
MODELO: OmniPCX Enterprise Communication 4400	
TECNOLOGIA: CENTRAL HIBRIDA (Telefonía Analógica, Digital e IP)	
DESCRIPCION:	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 5 - CONDICIONES DEFICIENTES "C".



COMENTARIOS

PROPIO	Comentario: Vista del Distribuidor Principal (MDF) de la antigua Central Telefónica Meridian – Nortel Telecom.
MARCA: ALCATEL	
MODELO: OmniPCX Enterprise Communication 4400	
TECNOLOGIA: CENTRAL HIBRIDA (Telefonía Analógica, Digital e IP)	
DESCRIPCION:	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 6 - CONDICIONES DEFICIENTES "D".



COMENTARIOS

PROPIO	<p>Comentario: Vista del rectificador de 48 VDC / 75 AMP de la Central Telefónica.</p> <p>Actualmente el UPS esta inoperativo lo cual trabaja de manera directa no garantizando la continuidad operativa del servicio.</p>
MARCA: ALCATEL	
MODELO: OmniPCX Enterprise Communication 4400	
TECNOLOGIA: CENTRAL HIBRIDA (Telefonía Analógica, Digital e IP)	
DESCRIPCION:	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 7 - CONDICIONES DEFICIENTES "E".



COMENTARIOS

PROPIO	Comentario: Vista de conversores para la comunicación con la telefonía móvil.
MARCA: ALCATEL	
MODELO: OmniPCX Enterprise Communication 4400	
TECNOLOGIA: CENTRAL HIBRIDA (Telefonía Analógica, Digital e IP)	
DESCRIPCION:	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 8. DATA CENTER ENLACE CON CENTRAL TELEFONICA

CANT.	COMENTARIOS	OBJETIVO VISUAL
3	1 Foto Vista Exterior. 2 fotos Vista Interior (ángulos o vistas opuestas) por CADA ambiente identificado, tales como: Cuarto de Acometida, Sala de Telecomunicaciones Centro de Datos y espacios complementarios.	Identificación de espacios especiales
FOTO 1 – VISTA EXTERIOR.		
		
COMENTARIOS		
NOMBRE DEL AMBIENTE: Data Center - HNERM ANCHO (m): 3 Metros LARGO (m): 2 Metros CANTIDAD DE PUNTOS DE DATOS: VOZ: 24 OTROS: CUENTA CON SISTEMA PUESTA A TIERRA: (SI) (NO) CUENTA CON UPS: (SI) (NO) CANTIDAD DE GABINETES EXISTENTES: 6 TIPOS DE GABINETES: Piso de Servidores DESCRIPCION: Se cuenta con un área de 10 m2 de los cuales se alojan 06 gabinetes de comunicaciones, 01 switch de CORE, 32 servidores de aplicaciones, 01 aire de precisión un aire de confort, 02 UPS de 10 KVA cada uno, repartido para todos los equipos existentes.		Comentario: El data center del HNERM, actualmente no cumple con los estándares establecidos por la norma ANSI/TIA 942. El área física asignada es 10 m², de los cuales se alojan 6 gabinetes de comunicaciones de los cuales 2 están asignados a equipos de comunicaciones (Switch CORE modular 06 9800, OptiView XG, Bandejas de Fibra Óptica, Telefonía IP), los cuatro gabinetes restantes alojan 32 Servidores donde están instalados los distintos aplicativos Institucionales y gran parte aplicativos de las casas comerciales sesión en uso), 01 aire acondicionado de precisión y uno de confort, 02 UPS de 10 kva. El cableado Horizontal establecido para los Servidores no está certificado. No cuenta con grupo electrógeno exclusivo para el data center, sistema contra incendios inoperativo, espacios físicos para el aire frío y caliente, sistema de aire acondicionado de precisión de contingencia. No cuenta con un Plan de Contingencia que garantice la continuidad operativa. Sistema de Seguridad Inoperativo.

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 9 – VISTA FRONTAL.



COMENTARIOS

PROPIO	Comentario:
MARCA: ALCATEL	
MODELO: OmniPCX Enterprise Communication 4400	
TECNOLOGIA: CENTRAL HIBRIDA (Telefonía Analógica, Digital e IP)	
DESCRIPCION:	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 10 -CENTRAL TELEFONICA



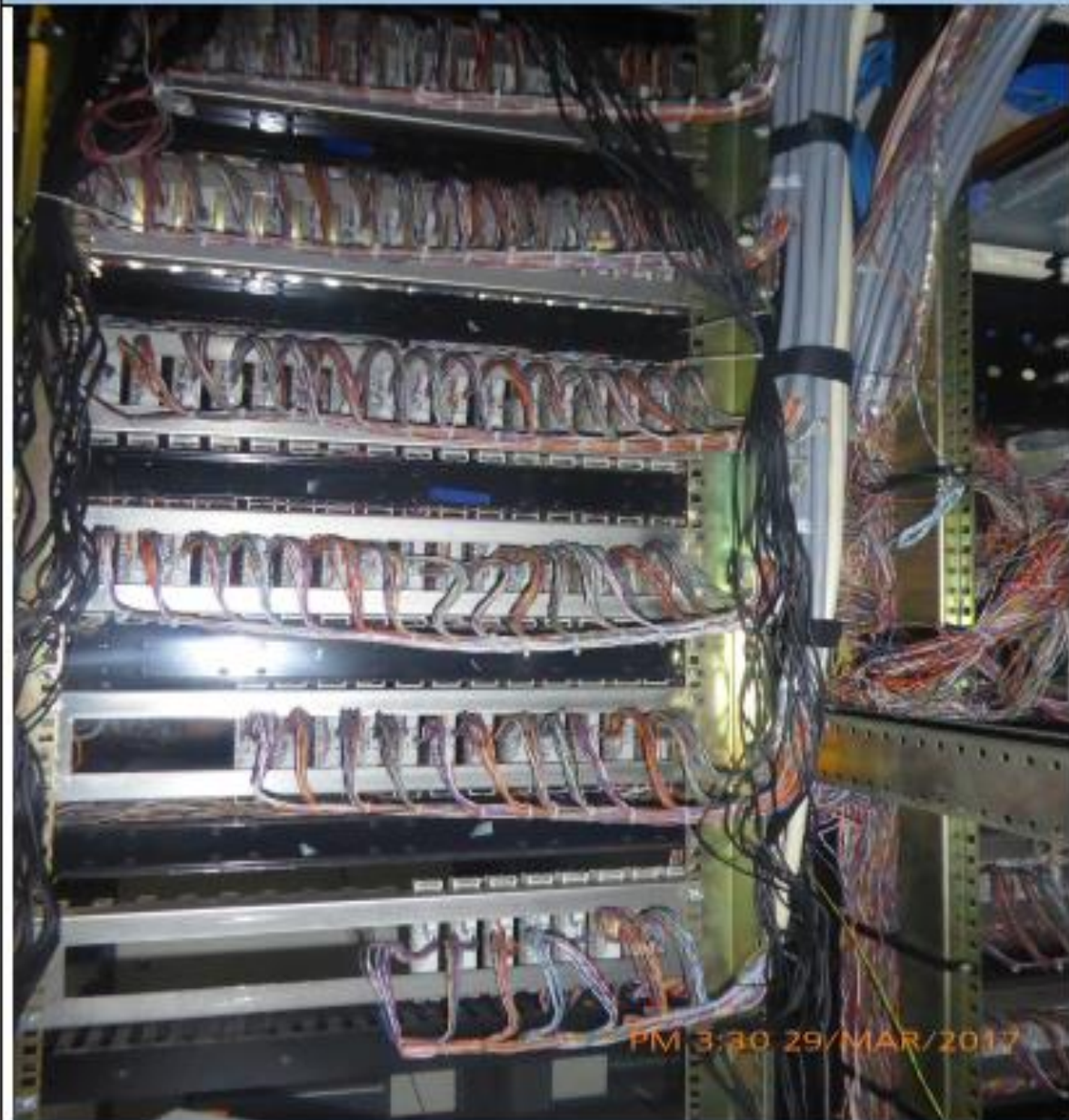
COMENTARIOS

PROPIO	Comentario:
MARCA: ALCATEL	
MODELO: OmniPCX Enterprise Communication 4400	
TECNOLOGIA: CENTRAL HIBRIDA (Telefonia Análoga, Digital e IP)	
DESCRIPCION:	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 11 – VISTA OBLICUA.



COMENTARIOS

PROPIO	Comentario:
MARCA: ALCATEL	
MODELO: OmniPCX Enterprise Communication 4400	
TECNOLOGIA: CENTRAL HIBRIDA (Telefonía Analógica, Digital e IP)	
DESCRIPCION:	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 12 – PANORAMICA.




COMENTARIOS

PROPIO	Comentario:
MARCA: ALCATEL	
MODELO: OmniPCX Enterprise Communication 4400	
TECNOLOGIA: CENTRAL HBRIDA (Telefonia Análoga, Digital e IP)	
DESCRIPCION:	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



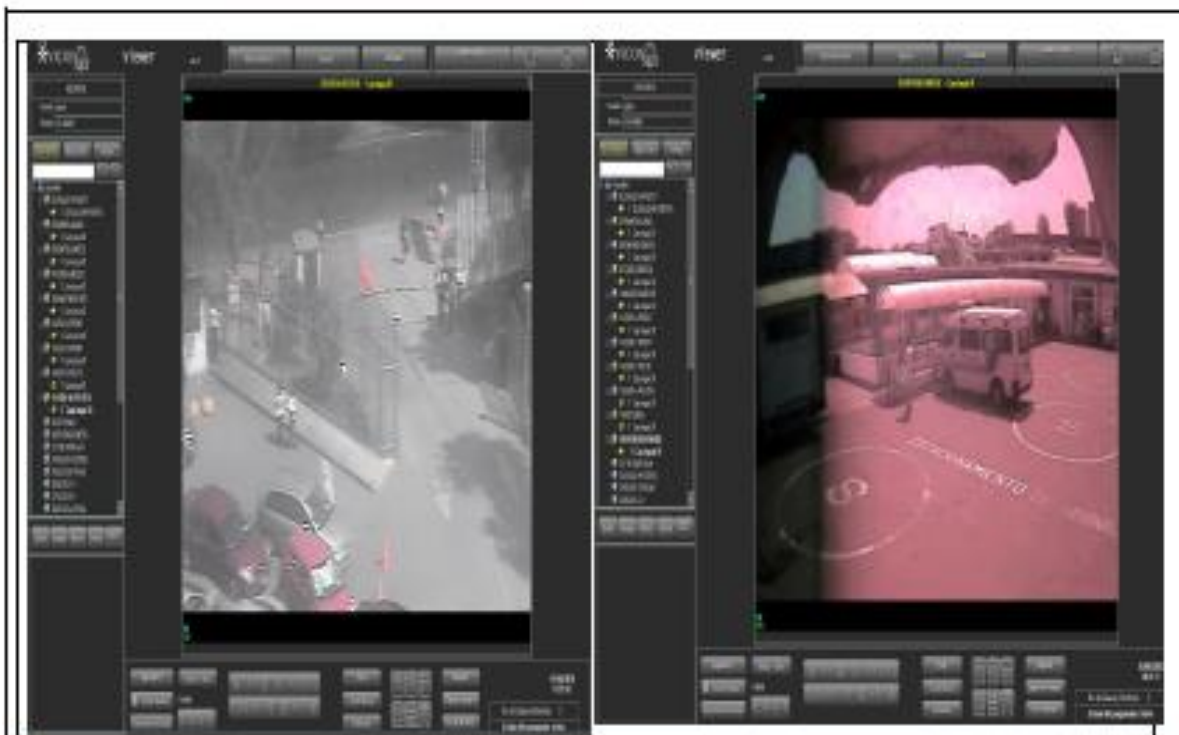
ANEXO 4: CAMARA VIDEO VIGILANCIA
Fotos del 1 al 9

16. CAMARAS DE VIDEO VIGILANCIA		
CANT.	COMENTARIOS	OBJETIVO VISUAL
10	2 en el mejor estado y 4 para las más deficientes. Indicar el Piso, Área o Zona. 4 en NVR, Servidor, o DVR (Vista Frontal / Posterior / Vista Oblicua, Panorámica, y que se visualice la marca, modelo y puertos usados).	Estado/Tipo de Cámara.
FOTO 1 – MEJOR ESTADO “A”.		
		
COMENTARIOS		
PROPIO(X)	<p>Comentario: Esta imagen representa el Centro de Control del Sistema de Seguridad del Centro de Emergencia del Hospital Rebagliati.</p> <p>Este es un sistema moderno instalado el año 2016, cuenta con 104 cámaras de seguridad, 1 servidor NVR y dos Storage.</p> <p>El sistema funciona adecuadamente, está operativo, plataforma con tecnología IP, marca Pelco.</p>	
MARCA: PELCO		
MODELO:		
TECNOLOGIA: IP		
DESCRIPCION:		

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 2 – MEJOR ESTADO "B".



COMENTARIOS

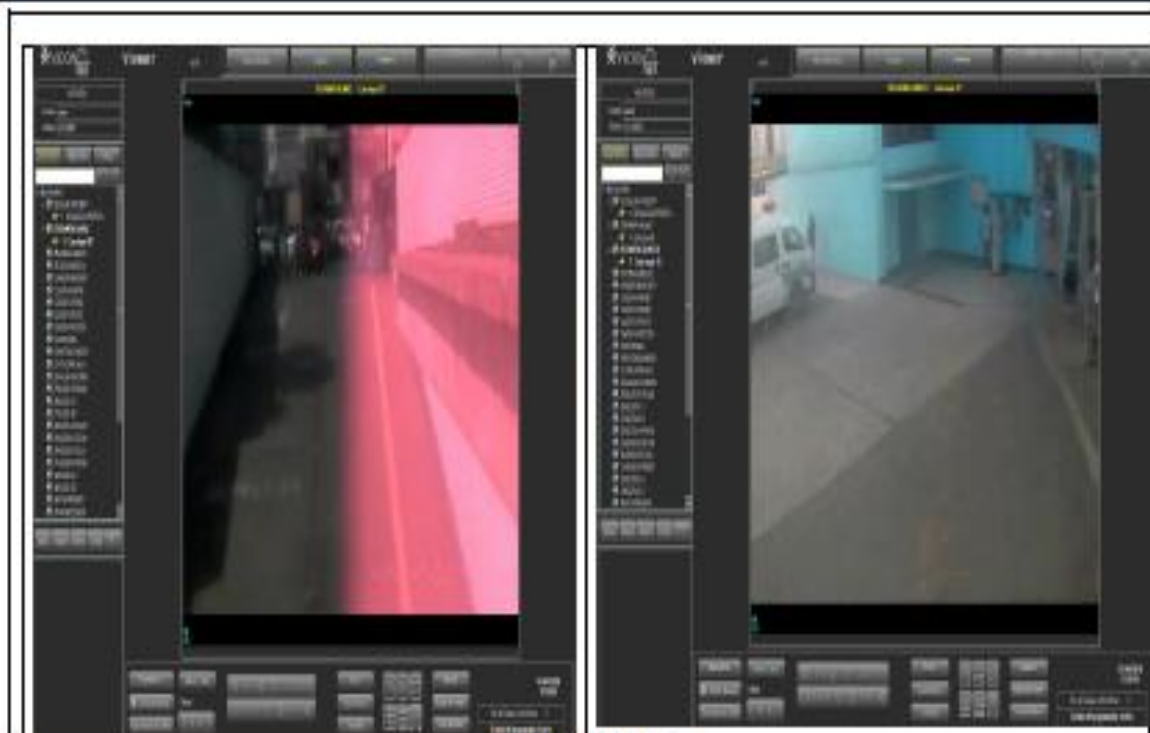
PROPIO (X)	<p>Comentario:</p> <p>Las cámaras de video se han realizado el mantenimiento y limpieza respectiva a todos los componentes el mismo que continua presentando problemas.</p> <p>Así mismo cabe mencionar que en el visor que integra las cámaras no se puede integrar cámaras de otro fabricante.</p> <p>Se debe tener en consideración que el recinto hospitalario atiende las 24 x 7 x 365, donde el arribo de personas diario son aproximadamente 16,000 donde los activos fijo e insumos de farmacia, almacenes son de alto costo para la institución.</p> <p>El video sistema de video cámaras es una herramienta que cumple una función DISUASIVA, pues su instalación normalmente es hecha pública, lo que inhibe a potenciales infractores de actuar bajo su mirada. Al registrar lo que ven, permiten, eventualmente, identificar al infractor y a su víctima, y dar cuenta de los hechos, lo que puede constituir un elemento probatorio ante la justicia penal, así mismo se debe contemplar el componente REACTIVO como son los sistemas RFID, el mismo que elevaría el nivel de seguridad y aseguraría el recinto hospitalario en tiempo real, permitiendo responder con los procesos funcionales y las necesidades de hospital como son incidencias diarias, inventario en tiempos cortos.</p>
MARCA-VICON	
MODELO:	
TECNOLOGIA: ANALOGICA, DIGITAL,	
DESCRIPCION	

Las cámaras de video que se visualizan en el visor muestran una calidad deficiente, el mismo que no se puede determinar a las personas que sean participe de algún delito como hurto, sabotaje, agresión, etc.

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 3 – CONDICIONES DEFICIENTES "A".



COMENTARIOS

PROPIO [X]

MARCA: VICON

MODELO:

TECNOLOGIA: ANALOGICA, DIGITAL

DESCRIPCION:

El Hospital Nacional Edgardo Rebagliati Martins, actualmente cuenta con un Sistema de monitoreo por videocámaras marca vicon, el mismo que es una plataforma osada es decir no permite integrar equipos multimarca, el sistema cuenta con más de 10 años de antigüedad, el cual a la fecha no cuenta con garantía vigente y/o contrato de servicio de soporte técnico, cabe mencionar que la reparación implica la compra de repuestos que en el mercado no se encuentran disponibles.

El estado actual de los componentes del sistema de video cámaras, es obsoleto donde el 100% de equipos ha cumplido el tiempo de vida útil, así mismo los modelos existentes se encuentra en obsolescencia tecnológica.

A continuación se detalla la plataforma tecnológica:

Comentario:

EQUIPOS DE COMUNICACIONES PARA LA RED DE DATOS					
N°	DESCRIPCION DE EQUIPO	MARCA	CANT.	FECHA DE INST.	ESTADO
1	CABLEA TIPO CAT6M	3CON	17	2006	DEFICIENTE
2	CABLEA TIPO CAT6M	3CON	24	2006	DEFICIENTE
3	CABLEA TIPO P12	3CON	5	2006	DEFICIENTE
SISTEMA CCTV – IMPLEMENTADO POR LA EMPRESA COMESA C					
N°	DESCRIPCION DE EQUIPO	MARCA	CANT.	FECHA DE INST.	ESTADO
	CAMERA TIPO P12A	3CON	10	2011	ESTABLE
EQUIPOS DE COMUNICACIONES PARA LA RED DE VIDEO					
N°	DESCRIPCION DE EQUIPO	MARCA	CANT.	FECHA DE INST.	ESTADO
1	SWITCH ADMINISTRABLE, CAPA 3 DE 12 PUERTOS SFP 16-1681008	CISCO CATALYST	1	2007	DEFICIENTE INOPERATIVO
2	SWITCH ADMINISTRABLE, CAPA 2 DE 8 PUERTOS ETHERNET 10/100/1000	CISCO CATALYST	1	2007	DEFICIENTE
SISTEMA DE ALMACENAMIENTO – NETWORK VIDEO RECORDER (NVR)					
N°	CARACTERISTICAS TECNICAS	CANT.	FECHA DE INST.	ESTADO	
1	NVR - SERVIDOR DISCO DURO 80 GB MEMORIA RAM 04 GB PROCESADOR SISTEMA OPERATIVO IP	1	2006	DEFICIENTE	
2	NVR - SERVIDOR DISCO DURO 80 GB MEMORIA RAM 04 GB PROCESADOR SISTEMA OPERATIVO IP	1	2006	DEFICIENTE	

Fuente: Oficina de Soporte Informático HNERM EsSALUD – (2017)

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 04 – CENTRAL Y CAMARAS UBIADAS EN AREAS DE SALUD



Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 5 - CONDICIONES DEFICIENTES "C".



COMENTARIOS

PROPIO (X)	Comentario:
MARCA/VICÓN	
MODELO:	
TECNOLOGIA: ANALÓGICA, DIGITAL	
DESCRIPCIÓN - Vista frontal de pesadizo del servicio de consulta externa.	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 6 - CONDICIONES DEFICIENTES "D".

	
COMENTARIOS	
PROPIO (X) MARCA: VICON MODELO: TECNOLOGIA: ANALOGICA, DIGITAL DESCRIPCION: <ul style="list-style-type: none"> - Vista frontal de puntos de ingresos y salidas del recinto hospitalario. - Vista del ambiente de farmacia de alto costo. 	Comentario:

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)

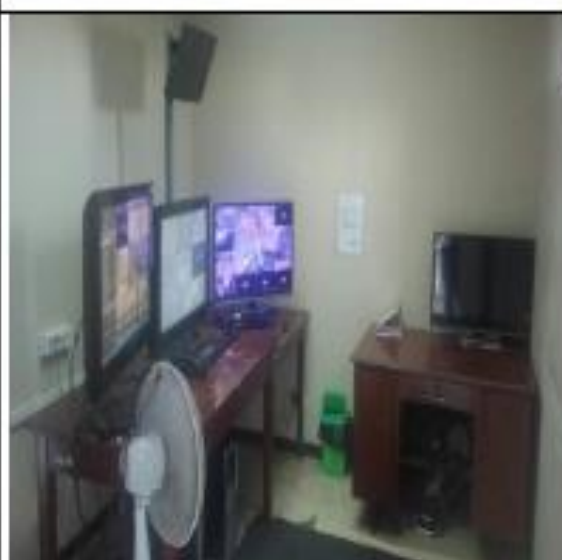


FOTO 7 - NVR



SISTEMA DE ALMACENAMIENTO - NETWORK VIDEO RECORDER (NVR)				
Nº	CARACTERÍSTICAS TÉCNICAS	CANT.	FECHA DE INST.	ESTADO
1	NVR - SERVIDOR DISCO DURO 80 GB MEMORIA RAM 04 GB PROCESADOR SISTEMA OPERATIVO #	1	2006	DEFOBETE
2	NVR - SERVIDOR DISCO DURO 80 GB MEMORIA RAM 04 GB PROCESADOR SISTEMA OPERATIVO #	1	2006	DEFOBETE

Fuente: Oficina de Soporte Informático - HNERM



COMENTARIOS

PROPIO (X)	<p>Comentario: El Sistema del almacenamiento cuenta con dos servidores NVR marca Vicon, con discos duros de 80GB y sistema operativo Windows XP. Este sistema fue puesto en operación en el año 2006; tiene el inconveniente de ser cerrado, pues no permite añadir equipos compatibles, solo los equipos propietarios del fabricante. La factibilidad en horas del sistema, llegó a término: requiere ser reemplazado por uno moderno, adecuado a las necesidades del hospital.</p>
MARCA: VICON	
MODELO:	
TECNOLOGIA: ANALOGICA, DIGITAL	
DESCRIPCION:	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 8 – AMBIENTE DE LA CENTRAL DE MONITOREO HNERM



COMENTARIOS

PROPIO <input type="checkbox"/> Alquilado <input checked="" type="checkbox"/>	<p>Comentario:</p> <ul style="list-style-type: none"> - Cabe mencionar que los dos sistemas DVR, instalados son de propiedad de la empresa de seguridad ESVICSAC, el mismo que están en alquiler de servicio.
MARCA:	
MODELO:	
TECNOLOGIA: Analoga	
DESCRIPCION:	

- El Hospital Rebagjati actualmente cuenta con tres sistemas provisión ISR, instalados en distintos ambientes del Hospital.
- Ambiente de Central de Monitoreo ubicado en el piso 14 el mismo que cuenta con un DVR de 12 canales con 10 cámaras instaladas.
- Ambiente de Monitoreo de Farmacia un DVR de 16 canales ubicado en el sótano.
- Ambiente de Cobalto Terapia instalación de 8 cámaras análogas instaladas en un DVR de 8 canales en el mismo servicio.

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)




FOTO 09 – CENTRAL Y CAMARAS UBICADAS EN AREAS DE SALUD



Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



ANEXO 5: BACKBONE – CANALIZACIÓN DE ACOMETIDA – HNERM
Fotos del 1 al 8

05. CANALIZACION DE ACOMETIDA DEL PROVEEDOR TELECOM		
CANT.	COMENTARIOS	OBJETIVO VISUAL
6	1 Punto de llegada (Router), 1 Roseta de Conexión interna, 2 Recorrido interno, 2 recorrido externo a poste o buzón; por CADA Proveedor	Estado situacional para toma de decisiones de las posibles mejoras.
FOTO 1 – PUNTO DE LLEGADA		
		
COMENTARIOS		
PVC: (x)		
CONDUIT:		
CANALETA:		
CORRUGADO:		
NINGUNO:		
DESCRIPCION:	COMENTARIO: Existen 2 bandejas de Fibra Óptica donde se interconectan 19 Fibras Ópticas de 6 Hilos 3 Pares con un total de 57 pares que son los enlaces trocales con cada GDS.	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 2 – ROSETA DE CONEXIÓN INTERNA



COMENTARIOS

PVC: X 2.5"	<p>Comentario:</p> <p>Tubería PVC deterioradas la misma que está expuesta la fibra.</p> <p>Como se puede apreciar el cableado de datos está pasando por la misma tubería del cableado troncal.</p> <p>Exposición de Fibra Óptica.</p>
CONDUIT:	
CANALETA:	
CORRUGADO:	
NINGUNO:	
DESCRIPCION:	
<p>Existen 2 Líneas Troncales que separan los edificios las mismas que están cubiertas con tubería PVC.</p>	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 3 – RECORRIDO INTERNO “A”



COMENTARIOS

PVC: (X) 2.5"	<p>COMENTARIO:</p> <p>Como se puede evidenciar en la foto, existe un empalme fusión que se realizó a dos segmentos de red, GDS A y GDS G3, el mismo que fue ocasionado por un acto de vandalismo realizado 2014.</p> <p>En ese sentido se debe adoptar medidas correctivas haciendo uso de CONDUIT y de ser el caso hacer uso de Fibra con coberturas de Planta externa.</p>
CONDUIT:	
CANALETA:	
CORRUGADO:	
NINGUNO:	
DESCRIPCION:	
<p>Tendido de Fibra Óptica Interno a los GDS, Galería Baja, edificio Block A, B, C, G, C1, D y L</p>	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 4 – RECORRIDO INTERNO "B"



COMENTARIOS

PVC: (X) 2.5"	<p>COMENTARIO:</p> <p>Como se puede apreciar el cableado de datos está pasando por la misma tubería del cableado troncal.</p> <p>Exposición de Fibra Óptica.</p>
CONDUIT:	
CANAleta:	
CORRUGADO:	
NINGUNO:	
DESCRIPCION:	
<p>Tendido de Fibra Óptica Interno a los GDS, Galeria Baja, edificio Block A, B, C, G, C1, D y L</p>	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 5 – RECORRIDO INTERNO “C”



COMENTARIOS

PVC: (X) 2.5"	<p>COMENTARIO:</p> <p>Como se puede apreciar el cableado de datos está pasando por la misma tubería del cableado troncal.</p> <p>Exposición de Fibra Óptica.</p>
CONDUIT:	
CANALETA:	
CORRUGADO:	
NINGUNO:	
DESCRIPCION:	
<p>Tendido de Fibra Óptica Interno a los GDS, Galería Baja, edificio Block A, B, C, G, C1, D y L</p>	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2017)



FOTO 6 – RECORRIDO INTERNO “D”



COMENTARIOS

PVC: (X) 2.5"	<p>COMENTARIO:</p> <p>Como se puede apreciar el cableado de datos está pasando por la misma tubería del cableado troncal.</p> <p>Exposición de Fibra Óptica.</p>
CONDUIT:	
CANALETA:	
CORRUGADO:	
NINGUNO:	
DESCRIPCION:	
<p>Tendido de Fibra Óptica Interno a los GDS, parte posterior del edificio Block A, B, G, C1, D y L</p>	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2018)



FOTO 7 – RECORRIDO INTERNO “E”



COMENTARIOS

PVC: (X) 2.5"	<p>COMENTARIO: Como se puede apreciar La tubería de PVC de 2.5" se encuentra en malas condiciones, cajas de paso destapadas, expuesta a cualquier tipo peligro, Húmeda, Corte de Fibra, etc.</p>
CONDUIT:	
CANALETA:	
CORRUGADO:	
NINGUNO:	
DESCRIPCION: Tendido de Fibra Óptica Interno a los GDS, parte posterior del edificio Block A, B, G, C1, D y L	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2018)



FOTO 8 – RECORRIDO EXTERNO A POSTE O BUZON “A”



COMENTARIOS

PVC: (X) 2.5"	<p>COMENTARIO: Como se puede apreciar el cableado de datos está pasando por la misma tubería del cableado troncal.</p>
CONDUIT:	
CANALETA:	
CORRUGADO:	
NINGUNO:	
DESCRIPCION: Tendido de Fibra Óptica Interno a los GDS, parte posterior del edificio Block I, J, K, M, N	

Fuente: Oficina de Soporte Informático HNERM EsSALUD (2018)

