UNIVERSIDAD PRIVADA ANTENOR ORREGO

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

"IMPLEMENTACIÓN DE UNA RED INFORMÁTICA HOSPITALARIA, USANDO METODOLOGÍA TOP-DOWN NETWORK DESIGN; PARA EL HOSPITAL CHANCAY Y SERVICIOS BASICOS DE SALUD"

Área de Investigación: Computación Centrada en Redes

TESIS PARA OPTAR EL TITULO PROFESIONAL DE INGENIERO DE COMPUTACIÓN Y SISTEMAS

AUTORES :

Br. Luján Vergara; Esmyder Arnaldo.

Br. Medina Osorio; César Alejandro.

ASESOR :

Ing. Agustín Eduardo Ullón Ramírez

TRUJILLO – PERÚ
2015

"IMPLEMENTACIÓN DE UNA RED INFORMÁTICA HOSPITALARIA, USANDO METODOLOGÍA TOP-DOWN NETWORK DESIGN; PARA EL HOSPITAL CHANCAY Y SERVICIOS BASICOS DE SALUD"

Presentada Por :

Br. Luján Vergara; Esmyder Arnaldo.

Br. Medina Osorio; César Alejandro.

Aprobado Por :

Ing. José Manuel Rodríguez Mantilla
Presidente
CIP: 139579

Ing. Jaime Eduardo Díaz Sánchez
Secretario
CIP: 73304

Ing. Karla Vanessa Meléndez Revilla
Vocal
CIP: 120097

Ing. Agustín Eduardo Ullón Ramírez
Asesor
CIP: 137602

PRESENTACIÓN

Señores Miembros del Jurado:

De conformidad dando cumplimiento a los requisitos estipulados en el Reglamento de Grados y Títulos de la Universidad Privada Antenor Orrego; el Reglamento Interno de la Escuela Profesional de Ingeniería de Computación y Sistemas, ponemos a su disposición nuestra Tesis Titulada: *"IMPLEMENTACIÓN DE UNA RED INFORMÁTICA HOSPITALARIA, USANDO METODOLOGÍA TOP-DOWN NETWORK DESIGN; PARA EL HOSPITAL CHANCAY Y SERVICIOS BASICOS DE SALUD"* para obtener el Título Profesional de Ingeniero de Computación y Sistemas.

El contenido del presente trabajo ha sido desarrollado tomando como marco de referencia los lineamientos establecidos por la Universidad para el desarrollo de la Tesis, en base a los conocimientos obtenidos durante nuestros años de formación profesional, así como la experiencia profesional obtenida en el campo laboral, consultas bibliográficas realizadas en libros, manuales y/o a través del internet, siendo conscientes que el conocimiento es una fuente inagotable de nuevos términos y conceptos que varían en el tiempo y el espacio. Este trabajo tiene por finalidad, de mejorar la trasmisión de datos entre las diversas unidades y áreas existentes en el Hospital Chancay y Servicios Básicos de Salud, las mismas que una vez ejecutada nuestra Tesis, se contaran con información fidedigna, segura, suficiente y confiable.

Aprovechamos la oportunidad para expresar adelantadamente nuestro agradecimiento a la atención que puedan prestarle a este trabajo señores miembros del jurado,

Los Autores.

DEDICATORIA

A mis Padres que los amo. Porque con su amor, su apoyo y sus ejemplos son ellos los que más han influenciado en mi vida, dándome los mejores consejos, guiándome y ayudándome satisfactoriamente a mi formación como persona y profesional.

A mi esposa con mucho amor, cariño y respeto por su comprensión, cariño y constante apoyo para lograr mis objetivos.

A mis hermanos a quienes quiero mucho, son parte importante de mi vida y están siempre brindándome su apoyo incondicional.

A mis hijas, que son mi adoración. Para motivarlas a estudiar con empeño y dedicación.

Br. ***LUJÁN VERGARA; Esmyder Arnaldo.***

DEDICATORIA

A la memoria de mi madre, para ti con todo cariño por tu dedicación y amor, tú que sacrificaste tu tiempo, tú que me motivaste día a día, para ser un hombre de bien, te dedico cada una de las páginas.

Dedico a mi padre por su entrega, su don de trabajo; por cada minuto de sacrificio por verme profesional, por esa mano fraterna que cuando sentía que el camino se terminaba, estabas siempre tú; mi querido viejo.

A mis hermanas, sobrinos y sobrina por el apoyo constante e incondicional, por ese calor de hogar que siempre sentí al estar rodeado de ustedes.

A mi hija Cielo Alejandra por ser la fuente incansable de amor, por ser la luz que ilumina mi camino y la dueña de mis sentimientos más puros.

A mis maestros por su paciencia y comprensión, a ustedes lo dedico por compartir sus conocimientos que fueron fragua y forja de mi formación profesional, a ustedes por ser guía de muchos jóvenes, forjadores de sus sueños.

Br. MEDINA OSORIO; César Alejandro

AGRADECIMIENTOS

A Dios Por la vida que me ha regalado, y darme fuerzas para superar obstáculos y dificultades a lo largo de mi vida.

A mis padres Roger y Chabuca ya que con sus incansables esfuerzos y buenos ejemplos demostrados hacia a mí, me enseñaron a superar los obstáculos que a lo largo de mi vida se me han presentado, para poder surgir por medio de la educación, el trabajo y las buenas costumbres.

A mis hermanos Yudit y Elder por el amor y apoyo que siempre he recibido, a ustedes por enseñarme a luchar por mis seres queridos, por enseñarme lo bueno que es tener hermanos y poder compartir cosas con ellos y aprender cosas de ellos.

A mi familia en especial mi tío Amaro, a la familia Rodríguez Castañeda y Obeso Rodríguez por el apoyo que siempre me brindaron día a día en el transcurso de cada año de mi carrera universitaria.

A mi esposa Betty, y mis hijas Angie y Grace, por ser la fuente de mi inspiración y motivación para superarme cada día más y así poder luchar para que la vida nos depare un futuro mejor.

De igual manera a mi Asesor Ing. Agustín Eduardo Ullón Ramírez, que compartió generosamente sus conocimientos para la exitosa consecución de este trabajo.

Br. ***LUJÁN VERGARA; Esmyder Arnaldo.***

AGRADECIMIENTOS

Agradezco a Dios por haberme dado la oportunidad de existir, por haberme acompañado y guiado a lo largo de estos años de vida.

Agradecer a mis padres quienes día a día guiaron mis pasos, por su entrega y dedicación incondicional, ellos que con amor, ternura, y su ejemplo hicieron de mí un hombre de bien.

A mis hermanas Cecilia, Jannelly, Luz, Magdalena, a mi hermano Santiago, por el apoyo incondicional y por su ejemplo de superación; a cada uno de ustedes, mil gracias.

A mi hija Cielo Alejandra por su comprensión y por las horas que no pude pasar a su lado.

Así mismo deseo agradecer a mi Asesor Ing. Agustín Eduardo Ullón Ramírez por las horas dedicadas a brindarme sus consejos, guiándonos este proyecto hasta su consolidación.

Finalmente a mis amigos Maximiliano De La Cerna, Edwin Tapia, Elder Lujan, Jhonny Clavijo, Esmyder Lujan, Daniel Oyola, Margarita Cano, Nathali Yovera, Susan Miranda, con quienes compartí gratos momentos de mi vida y supieron alentarme cada día.

Br. MEDINA OSORIO; César Alejandro

"IMPLEMENTACIÓN DE UNA RED INFORMÁTICA HOSPITALARIA, USANDO METODOLOGÍA TOP-DOWN NETWORK DESIGN; PARA EL HOSPITAL CHANCAY Y SERVICIOS BASICOS DE SALUD"

RESUMEN

La información hoy en día fluye de manera horizontal en todas y cada una de las organizaciones, cuya importancia es relevante en la toma de decisiones, en el sector salud es una condición indispensable para el desarrollo humano y un medio fundamental para alcanzar el bienestar individual y colectivo. Al ser de interés público la protección de la salud de la población, el Estado a través del Ministerio de Salud, Direcciones Regionales de Salud, Hospitales y Centros Hospitalarios, tiene la responsabilidad de regularla, vigilarla y promoverla, bajo esta perspectiva la información que fluye en estas instituciones es de vital importancia, donde la Red Informática Hospitalaria en el Hospital Chancay y Servicios Básicos de Salud, juega un rol trascendental ya que permite compartir la información y los recursos entre todos los usuarios de la misma, por ello se hace imperiosa la necesidad de contar con una Red Informática Hospitalaria que nos garantice una fluidez de información real, eficiente, suficiente y segura.

El presente proyecto de Tesis, consiste en la "IMPLEMENTACIÓN DE UNA RED INFORMÁTICA HOSPITALARIA, USANDO METODOLOGÍA TOP-DOWN NETWORK DESIGN; PARA EL HOSPITAL CHANCAY Y SERVICIOS BASICOS DE SALUD", que le permitirá contar con una red informática hospitalaria moderna, automatizada tecnológicamente, con la finalidad de agilizar la trasferencia de información (voz, datos, texto, imágenes) entre sus unidades y áreas de trabajo, en beneficio de los usuarios finales que son los pacientes.

Para el desarrollo de este Proyecto de Tesis, se tuvo en cuenta en primer lugar el estado actual en el que se encuentra la red de informática del Hospital Chancay y Servicios Básicos de Salud, realizando un análisis e identificando la realidad problemática por la que viene atravesando el Hospital de Chancay y Servicios Básicos de Salud, en cuanto a su de trasmisión de información entre sus diversas unidades y áreas.

Siguiendo el desarrollo de la Tesis, hacemos mención al fundamento teórico, guía que nos permite determinar los requerimientos para la Implementación de una Red Informática Hospitalaria, usando Metodología Top-Down Network Design, para contar con una ágil, adecuada, suficiente, eficiente, suficiente y segura trasmisión de información, logrando agilizar el intercambio de información entre las diversas unidades y áreas del Hospital Chancay y Servicios Básicos de Salud.

Culminamos este Proyecto Tesis definiendo los componentes tecnológicos para el Diseño e Implementación de una Red Informática Hospitalaria, usando Metodología Top-Down Network Design; para el Hospital Chancay y Servicios Básicos de Salud; cuya plataforma para la Administración de la Red Informática Hospitalaria será de Windows Server 2012.

"IMPLEMENTATION OF A COMPUTER NETWORK HOSPITAL USING TOP-DOWN METHODOLOGY NETWORK DESIGN; FOR HOSPITAL CHANCAY BASIC HEALTH SERVICES"

ABSTRACT

The information today flows horizontally in each and every one of the organizations whose importance is relevant in decision-making in the health sector is a prerequisite for human development status and an essential means of achieving individual wellbeing and collective. To be in the public interest to protect the health of the population, the State through the Ministry of Health, Regional Health, Hospitals and Medical Centers, has a responsibility to regulate, monitor it and promote it, from this perspective the information flowing in these institutions it is of vital importance, where the Computer Hospital Network in Chancay Hospital and basic health services, plays a vital role as sharing information and resources among all users of the same, therefore it is imperative the need for a Hospital Information Network that guarantees fluidity of real, efficient, adequate and secure.

This thesis project consists in the "IMPLEMENTATION OF A COMPUTER NETWORK HOSPITAL USING TOP-DOWN METHODOLOGY NETWORK DESIGN; CHANCAY FOR HOSPITAL AND HEALTH SERVICES BASIC ", allowing you to have a modern hospital computer network, automated technologically, in order to expedite the transfer of information (voice, data, text, images) between its units and work areas for the benefit of end users who are patients.

For the development of this thesis project it was taken into account first the state in which is the computer network of Chancay Hospital and basic health services, analyzing and identifying problems by actually coming through Hospital Chancay and basic health services, in terms of transmission of information between the various units and areas.

Following the development of the thesis, we mention the theoretical foundation, guide allowing us to determine the requirements for the implementation of a hospital computer

network, using methodology Top-Down Network Design, to have a quick, appropriate, adequate, efficient and safe transmission of information, making rapid exchange of information between the various units and areas of Chancay Hospital and basic health services.

We completed this thesis project defining technology components for the Design and Implementation of Computer Hospital Network, using methodology Top-Down Network Design; for Chancay Hospital and basic health services; whose platform for Computer Network Administration Hospital is Windows Server 2012.

INDICE DE CONTENIDOS

INDICE DE FIGURAS

INDICE DE TABLAS

CAPITULO I

INTRODUCCION

Al encontrarnos frente a los grandes cambios tecnológicos, donde la información fluye de manera unidireccional, hemos ido viendo a través del tiempo, como la infraestructura del Hospital Chancay y Servicios Básicos de Salud, viene dotándose de: aire acondicionado, suministro eléctrico, megafonía, etc… características que no implica mayor dificultad y nos permite tener edificaciones automatizadas, pero si a esta infraestructura le implementamos de una Red Informática Hospitalaria, capaz de transferir (datos, voz, texto e imágenes) empezamos a hablar de una infraestructura hospitalaria moderna y automatizada tecnológicamente. Así como en las grandes ciudades donde existen Centros Hospitalarios que explotan favorablemente la tecnología informática. El Hospital Chancay y Servicios Básicos de Salud, no se siente ajeno a estos cambios muy por el contrario desea hacer uso de la tecnología actual en busca de brindar mejores servicios a sus pacientes, ya que en la actualidad el Hospital cuenta con Red Informática que se modificó día a día de acuerdo a las necesidades que se presentaban; sin contar con un plan de desarrollo que vaya de acorde con las nuevas tecnologías existentes, se puede observar una red informática que no cuenta con una topología definida, no respeta normas de seguridad y cuya infraestructura en algunos casos data de más de 10 años, con cables a la intemperie y sin ninguna protección originando en muchos de los casos la caída constante de la red, situación actual la cual desea cambiar, al contar con un Red Informática Hospitalaria que vaya de acorde con el avance tecnológico y la necesidades hospitalarias, de esta manera facilitara y agilizará la trasferencia de información (voz, datos, texto, imágenes) entre sus unidades y áreas de trabajo, en beneficio de los usuarios finales que son los pacientes.

Esta tesis tiene por objetivo hacer el levantamiento de información del estado actual de la Red Informática Hospitalaria del Hospital Chancay y Servicios Básicos de Salud, a la vez determinar los requerimientos, definir los componentes tecnológicos, bajo la metodología Top-Down Network Design, con la finalidad de agilizar los procesos automatizados, contando con información rápida, eficiente, suficiente y segura; donde el Capítulo I tratamos el planteamiento del problema, objetivos, aportes y la base teórica; Capitulo II el desarrollo de la metodología aplicada terminando con las conclusiones y recomendaciones.

1.1. Planteamiento del Problema.

En la actualidad en el Hospital de Chancay y Servicios Básicos de Salud, se puede observar la presencia de colas tanto en Caja, Farmacia y Admisión, ya que el crecimiento de su población adscrita a la institución cada año supera el 15% del año anterior y el tiempo de espera de un paciente a ser atendido supera las 2 horas, originando disgusto, incomodidad y malestar a los mismos, a la fecha existe un sinnúmero de quejas constantes; ante ello de la institución se pude decir que cuenta con un parque informático que carece de una adecuada red informática hospitalaria, ya que la red existente, si bien es cierto cubre de alguna manera la necesidad actual, funciona en condiciones inadecuadas, con cableado de red que ha ido creciendo según las necesidades, sin contar con una planificación, sin respetar normas y especificaciones técnicas, en muchos casos la red data de más de 10 años de antigüedad, contando con cables que se encuentran a la intemperie deteriorados y sin ninguna protección, causante inequívoca de constantes caídas de red, en estas condiciones; no se podrá atender de manera inmediata al paciente por tener problemas al acceso de la información, la misma que requiere privacidad, responsabilidad y cuidado, ya que la información del paciente en los establecimientos hospitalarios es confidencial, bajo estas condiciones el Hospital no podrá cumplir con su Misión que es: "Brindar atención integral y especializada de salud a la población del Hospital Chancay y Servicios Básicos de Salud de la Región Lima, con equidad, calidad y transparencia; priorizando grupos vulnerables, en concertación con los sectores público, privado y otros actores sociales".

Ante esta situación se propone la implementación de una red informática hospitalaria, usando una metodología Top-Down Network Design, que garantice, el cambio de las condiciones inadecuadas en las que viene funcionando la trasmisión de datos, y optimizar el uso del parque informático, se prevé contar con una red informática hospitalaria, que cumpla las normas, especificaciones técnicas, soporte nuevas tecnologías de acorde con el avance tecnológico y las necesidades hospitalarias, con la finalidad de agilizar la trasferencia de información (voz, datos, texto, imágenes) entre sus unidades, servicios y áreas de trabajo, siendo ampliamente beneficiados los pacientes.

1.2. Formulación del Problema

¿Cómo mejorar la comunicación y la seguridad de la información, al hacer uso de una metodología y tecnología de la información, en el Hospital Chancay y Servicios Básicos de Salud?

1.3. Antecedentes del Problema.

El Hospital de Chancay, se inaugura el 17 de Setiembre de 1971, cuya infraestructura desde ese entonces ha ido creciendo con el transcurrir de los años, adaptándose a las necesidades, en aquellos años la información no era automatizada, cuyo trabajo administrativo del Hospital era la formulación, planificación, organización, ejecución y evaluación de las acciones integrales de salud en el ámbito de la jurisdicción del distrito de Chancay, conforme pasan los años, el avance tecnológico vertiginoso ha dado lugar a nuevos escenarios de trabajo, de procesos no automatizados a procesos automatizados donde el campo informático juega un rol de gran importancia, en este caso en el campo de la salud, es por ello que en el año 92, se adquiere las primeras computadoras personales, el parque informático de la institución fue creciendo paulatinamente hasta contar en el año 2002 con la primera red de datos, ahora se cuenta con una red de datos que ha crecido desordenadamente sin una planificación adecuada que brinda un servicio deficiente, no cuenta con plano de distribución, no se ha respetado normas técnicas, con cables sin ninguna protección, la caída de la red es constante por ello se realizó visitas a otros Centros de Salud y Hospitales como Arzobispo Loayza y el Hospital María Auxiliadora, en ambos casos se pudo observar una Red Informática Hospitalaria, que satisface plenamente las necesidades de estos Hospitales, frente a esta situación se elabora el presente perfil con la finalidad de determinar la necesidad de Implementar una Red Informática Hospitalaria, haciendo uso de una Metodología, que nos garantice el éxito del proyecto en pos de alcanzar los objetivos propuestos.

1.4. Esta investigación tiene las justificaciones siguientes:

- ✓ Se podrá compartir los recursos informáticos, como archivos, impresoras, aplicaciones, escáner, fotocopiadoras, etc. Sin depender del espacio geográfico en el que nos encontremos.

- ✓ Reducción de tiempo en la trasmisión de datos, de manera que la gestión de las tareas se vuelve mucho más ágiles y rápidas, con el ahorro de tiempo y esfuerzo que esto supone
- ✓ Ahorro significativo de espacio en hardware, software. No es necesario disponer, de múltiples impresoras en una oficina, bastaría con una central que esté conectada en red y todos podrán imprimir en la misma.
- ✓ Información ordenada, centralizada y de fácil acceso a ella por cualquier usuario.
- ✓ Reducción de tiempo en la atención a los pacientes, reducción de colas en los Servicios de Caja y Admisión.

1.5. Los aportes de esta investigación son:

- ✓ Documentar la necesidad imperiosa de contar con una Red Informática Hospitalaria que cumpla con las Normas Técnicas Existentes amparada en la Metodología Top-Down Network Design.
- ✓ Mejorar de manera significativa la transferencia de información (datos, voz, texto e imágenes), entre las distintas Unidades, Áreas y Departamentos del Hospital de Chancay.
- ✓ Enriquecer el conocimiento en cuanto a desarrollo de Redes Informáticas Hospitalarias, ya que el conocimiento es una fuente dinámica inagotable de nuevas definiciones y conceptos.

1.6. Hipótesis

La Implementación de una Red Informática Hospitalaria, Usando Metodología Top Down Network Design, mejorar la comunicación y la seguridad de la información dentro del Hospital Chancay y Servicios Básicos de Salud.

1.7. EL Objetivo General es:

Implementación de una Red Informática Hospitalaria, Usando Metodología Top-Down Network Design, para el Hospital Chancay y Servicios Básicos de Salud.

1.8. Los Objetivos Específicos son:

- ✓ Conocer la realidad problemática por la que viene atravesando el Hospital Chancay y Servicios Básicos de Salud, en cuanto a la trasmisión de información entre sus diversas unidades y áreas.

- ✓ Determinar los requerimientos de la Red Informática Hospitalaria, que permita una ágil, adecuada, eficiente y segura trasmisión de información.
- ✓ Definir los componentes tecnológicos para la Implementación de una Red Informática Hospitalaria para el Hospital Chancay y Servicios Básicos De Salud.
- ✓ Agilizar el intercambio de información entre los diversos departamentos, áreas, unidades y servicios del Hospital Chancay y Servicios Básicos de Salud.
- ✓ Realizar una investigación y obtener aportes de la metodología que se pretende emplear Top-Down Network Design.

CAPITULO II

MARCO TEÓRICO

2.1. Red Informática

Se conoce como Red Informática a la infraestructura que posibilita la transmisión de información a través del intercambio de datos y compartiendo recursos como impresoras, quemadores/lectores de DVD, archivos, unidades de disco, etc.

Las redes informáticas, tiene como objetivos (Joskowicz, 2008):

- ✓ Compartir recursos, equipos, información y programas que se encuentran localmente o dispersos geográficamente.
- ✓ Brindar confiabilidad a la información, disponiendo de alternativas de almacenamiento.
- ✓ Obtener una buena relación costo / beneficio.
- ✓ Transmitir información entre usuarios distantes de la manera ágil, suficiente, eficiente y segura.

2.2. Red Informática Hospitalaria

Una Red Informática Hospitalaria, viene a ser el conjunto de equipos electrónicos (computadores, impresoras, servidores, servo cunas, ecógrafo multipropósito, máquinas de anestesia con sistema de monitoreo, cámaras de frio, hornos, esterilizadores, contadores de bacterias etc.) que comparten recursos, permitiendo el intercambio de información y respetando normas exclusivas para Centros Hospitalarios.

2.3. Reseña Histórica de Redes

El primer indicio de redes de comunicación fue de tecnología telefónica y telegráfica. En 1940 se transmitieron datos desde la Universidad de Darmouth, en Nuevo Hampshire, a Nueva York. A finales de la década de 1960 y en los posteriores 70 fueron creadas las minicomputadoras. En 1976, Apple introduce el Apple I, uno de los primeros computadores personales. En 1981, IBM introduce su primera PC. A mitad de la década de 1980 las PC comienzan a usar los módems para compartir archivos con otras computadoras, en un rango de velocidades que comenzó en 1200 bps y llegó a los 56 kbps (comunicación punto a punto), cuando empezaron a ser

sustituidos por sistema de mayor velocidad, especialmente ADSL (Línea de abonado digital asimétrica) (http://es.wikipedia.org/wiki/Red_de_computadoras, 2013)

2.4. Clasificación de Redes

2.4.1. De Acuerdo a su Alcance

Las redes de datos se pueden clasificar según la distancia o extensión que abarcan; entre ellas contamos con:

2.4.1.1. Red de Área Personal (PAN)

Red de Área Personal (PAN) es una red de computadoras para la comunicación entre distintos dispositivos (tanto computadoras, puntos de acceso a internet, teléfonos celulares, PDA, dispositivos de audio, impresoras) cercanos al punto de acceso. Estas redes normalmente son de unos pocos metros y para uso personal.

2.4.1.2. Red de Área Local (LAN)

Red de Área Local (Local Área Network), es una red que se limita a un área especial relativamente pequeña tal como un cuarto, un solo edificio, una nave, o un avión. Las redes de área local a veces se llaman una sola red de localización. No utilizan medios o redes de interconexión públicos.

2.4.1.3. Red de Área Local Inalámbrica (WLAN)

Red de Área Local Inalámbrica, o WLAN (Wireless Local Area Network), es un sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes de área local cableadas o como extensión de estas.

2.4.1.4. Red de Área de Campus (CAN)

Red de Área de Campus, o CAN (Campus Area Network), es una red de computadoras de alta velocidad que conecta redes de área local a través de un área geográfica limitada, como un campus universitario, una base militar, hospital, etc. Tampoco utiliza medios públicos para la interconexión.

2.4.1.5. Red de Área Metropolitana (MAN)

Red de Área Metropolitana (MAN) (Metropolitan Área Network o MAN, en inglés) es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica más extensa que un campus, pero aun así limitado. Por ejemplo, una red que interconecte los edificios públicos de un municipio dentro de la localidad por medio de fibra óptica.

2.4.1.6. Redes de Área Amplia (WAN)

Red de Área Amplia WAN (Wide Área Network), son redes informáticas que se extienden sobre un área geográfica extensa utilizando medios como: satélites, cables interoceánicos, Internet, fibras ópticas públicas, etc.

2.4.1.7. Red de Área de Almacenamiento (SAN)

Red de Almacenamiento en inglés SAN (Storage Area Network), es una red concebida para conectar servidores, matrices (arrays) de discos y librerías de soporte, permitiendo el tránsito de datos sin afectar a las redes por las que acceden los usuarios.

2.4.1.8. Red de Área Local Virtual (VLAN)

Red de Área Virtual, o VLAN (Virtual LAN), es un grupo de computadoras con un conjunto común de recursos a compartir y de requerimientos, que se comunican como si estuvieran adjuntos a una división lógica de redes de computadoras en la cual todos los nodos pueden alcanzar a los otros por medio de broadcast (dominio de broadcast) en la capa de enlace de datos, a pesar de su diversa localización física. Este tipo surgió como respuesta a la necesidad de poder estructurar las conexiones de equipos de un edificio por medio de software, permitiendo dividir un conmutador en varios virtuales.

2.4.1.9. Red Inalámbrica de Área Personal (WPAN)

Una Red Inalámbrica de Área Personal (WPAN). Es una red de computadoras inalámbrica para la comunicación entre distintos

dispositivos (tanto computadoras, puntos de acceso a internet, teléfonos celulares, PDA, dispositivos de audio, impresoras) cercanos al punto de acceso. Estas redes normalmente son de unos pocos metros y para uso personal, así como fuera de ella. El medio de transporte puede ser cualquiera de los habituales en las redes inalámbricas pero las que reciben esta denominación son habituales en Bluetooth.

2.4.2. De Acuerdo a sus Medios

2.4.2.1. Medios Guiados

Cuando se usa en su estructura cable coaxial, cable de par trenzado, fibra óptica y otros tipos de cables.

- **El Cable Coaxial** se utiliza para transportar señales electromagnéticas de alta frecuencia que posee dos conductores concéntricos, uno central, llamado vivo y uno exterior denominado malla o blindaje, que sirve como referencia de tierra y retorno de las corrientes; los cuales están separados por un material dieléctrico que, en realidad, transporta la señal de información.

- **El Cable de Par Trenzado** es una forma de conexión en la que dos conductores eléctricos aislados son entrelazados para tener menores interferencias y aumentar la potencia y disminuir la diafonía de los cables adyacentes. Dependiendo de la red se pueden utilizar, uno, dos, cuatro o más pares.

- **La Fibra Óptica** es un 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.

2.4.2.2. Medios No Guiados

Cuando usa señales de radio, infrarrojos, microondas, láser y otras redes inalámbricas.

- **Red por Radio** es aquella que emplea la radiofrecuencia como medio de unión de las diversas estaciones de la red.

- **Red por Infrarrojos**, permiten la comunicación entre dos nodos, usando una serie de leds infrarrojos para ello. Se trata de emisores/receptores de ondas infrarrojas entre ambos dispositivos, cada dispositivo necesita al otro para realizar la comunicación por ello es escasa su utilización a gran escala. No disponen de gran alcance y necesitan de visibilidad entre los dispositivos.

- **Red por Microondas**, es un tipo de red inalámbrica que utiliza microondas como medio de transmisión. Los protocolos más frecuentes son: el IEEE 802.11b y transmite a 2,4 GHz, alcanzando velocidades de 11 Mbps (Megabits por segundo); el rango de 5,4 a 5,7 GHz para el protocolo IEEE 802.11ª; el IEEE 802.11n que permite velocidades de hasta 600 Mbps; etc.

2.4.3. De Acuerdo a la Relación Funcional

2.4.3.1. Peer to Peer

Red de pares, es una red de computadoras en la que todos o algunos aspectos de ésta funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí. Es decir, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red.

2.4.3.2. Cliente – Servidor

Es aquella red de comunicaciones en la que todos los clientes están conectados a un servidor, en el que se centralizan los diversos recursos y aplicaciones con que se cuenta; y que los pone a disposición de los clientes cada vez que estos son solicitados. Esto significa que todas las gestiones que se realizan se concentran en el servidor, de manera que en él se disponen los requerimientos provenientes de los clientes que tienen prioridad, los archivos que

son de uso público y los que son de uso restringido, los archivos que son de sólo lectura y los que, por el contrario, pueden ser modificados, etc.

2.4.4. Topología de Acuerdo a su Diseño Físico

La topología de red lo definimos por la forma en que está diseñada la red, sea en el plano físico o lógico. El concepto de red puede definirse como "conjunto de nodos interconectados". Un nodo es el punto en el que una curva se intercepta a sí misma.

2.4.4.1. Punto a Punto

La topología más simple es un enlace permanente entre dos puntos finales (también conocida como point-to-point, o abreviadamente, PtP). La topología punto a punto conmutado es el modelo básico de la telefonía convencional. El valor de una red permanente de punto a punto, la comunicación sin obstáculos entre los dos puntos finales.

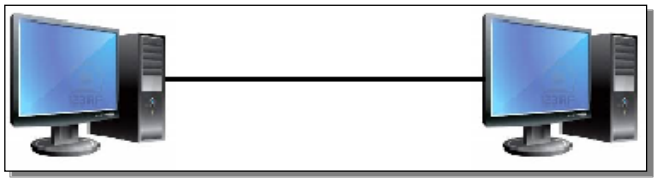


Figura Nº 01 TOPOLOGÍA DE RED PUNTO A PUNTO
Fuente: Elaborada por los Autores

2.4.4.2. En Bus

Una red en bus es aquella topología que se caracteriza por tener un único canal de comunicaciones (denominado bus, troncal o backbone) al cual se conectan los diferentes dispositivos. De esta forma todos los dispositivos comparten el mismo canal para comunicarse entre sí.

Figura Nº 02 TOPOLOGÍA DE RED EN BUS
Fuente: Elaborada por los Autores

2.4.4.3. En Estrella

Una red en estrella es una red en la cual las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de éste. Los dispositivos no están directamente conectados entre sí, además de que no se permite tanto tráfico de información. Dada su transmisión, una red en estrella activa tiene un nodo central activo que normalmente tiene los medios para prevenir problemas relacionados con el eco. Se utiliza sobre todo para redes locales. La mayoría de las redes de área local que tienen un enrutador (router), un conmutador (switch) o un concentrador (hub) siguen esta topología. El nodo central en éstas sería el enrutador, el conmutador o el concentrador, por el que pasan todos los paquetes de usuarios.

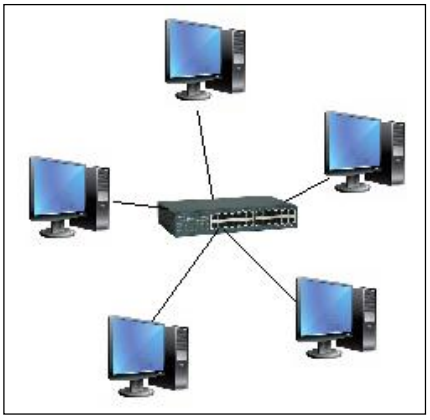


Figura Nº 03 TOPOLOGÍA DE RED EN ESTRELLA
Fuente: Elaborada por los Autores

2.4.4.4. En Anillo

Una red en anillo es una topología de red en la que cada estación tiene una única conexión de entrada y otra de salida. Cada estación tiene un receptor y un transmisor que hace la función de traductor, pasando la señal a la siguiente estación.

En este tipo de red la comunicación se da por el paso de un token o testigo, que se puede conceptualizar como un cartero que pasa recogiendo y entregando paquetes de información, de esta manera se evitan eventuales pérdidas de información debidas a colisiones.

En un anillo doble (Token Ring), dos anillos permiten que los datos se envíen en ambas direcciones (Token passing). Esta configuración crea redundancia (tolerancia a fallos). Evita las colisiones.

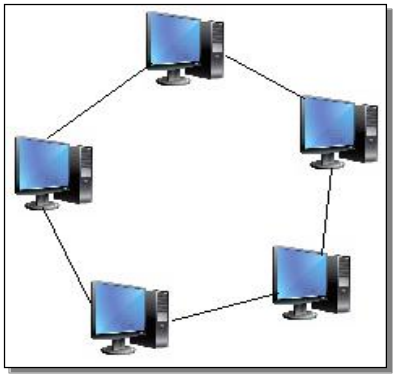


Figura Nº 04 TOPOLOGÍA DE RED EN ANILLO
Fuente: Elaborada por los Autores

2.4.4.5. En Malla

La topología de red mallada es una topología de red en la que cada nodo está conectado a todos los nodos. De esta manera es posible llevar los mensajes de un nodo a otro por distintos caminos. Si la red de malla está completamente conectada, no puede existir absolutamente ninguna interrupción en las comunicaciones. Cada servidor tiene sus propias conexiones con todos los demás servidores.

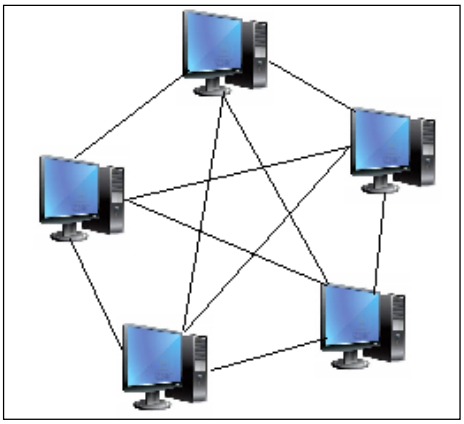


Figura Nº 05 TOPOLOGÍA DE RED EN MALLA
Fuente: Elaborada por los Autores

2.4.4.6. En Árbol

La red en árbol es una topología de red en la que los nodos están colocados en forma de árbol. Desde una visión topológica, es

parecida a una serie de redes en estrella interconectadas salvo en que no tiene un nodo central. En cambio, tiene un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos. Es una variación de la red en bus, la falla de un nodo no implica interrupción en las comunicaciones. Se comparte el mismo canal de comunicaciones.

La topología en árbol puede verse como una combinación de varias topologías en estrella. Tanto la de árbol como la de estrella son similares a la de bus cuando el nodo de interconexión trabaja en modo difusión, pues la información se propaga hacia todas las estaciones, solo que en esta topología las ramificaciones se extienden a partir de un punto raíz (estrella), a tantas ramificaciones como sean posibles, según las características del árbol.

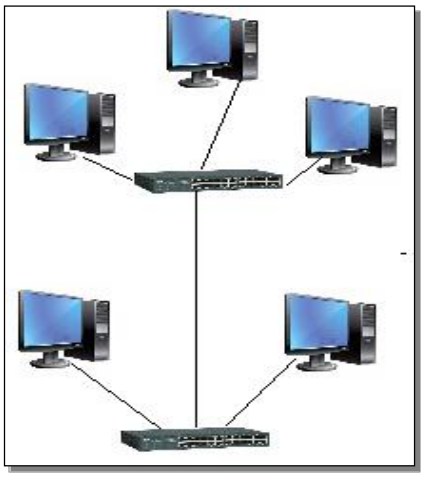


Figura Nº 06 TOPOLOGÍA DE RED EN ARBOL
Fuente: Elaborada por los Autores

2.4.4.7. Topología Hibrida

La topología híbrida es una de las más frecuentes y se deriva de la unión de varios tipos de topologías de red, de aquí el nombre de híbridas. Ejemplos de topologías híbridas serían: en árbol, estrella-estrella, bus-estrella, etc.

Su implementación se debe a la complejidad de la solución de red, o bien al aumento en el número de dispositivos, lo que hace necesario establecer una topología de este tipo. Las topologías híbridas tienen un costo muy elevado debido a su administración y mantenimiento,

ya que cuentan con segmentos de diferentes tipos, lo que obliga a invertir en equipo adicional para lograr la conectividad deseada.

2.5. Tecnologías de Red de Datos

La Tecnología en Redes y Comunicación de datos permite desarrollar destrezas para planear, diseñar e implantar redes de computadores para el intercambio de información entre ellos; así como administrar en forma técnica sus componentes o recursos a nivel de equipos, dispositivos de red, aplicaciones, entre otros. Esto, con el fin de garantizar la confiabilidad, disponibilidad, flexibilidad y calidad de la información.

2.5.1. Fast Ethernet

Fast Ethernet o Ethernet de alta velocidad es el nombre de una serie de estándares de IEEE de redes Ethernet de 100 Mbps (megabits por segundo). El nombre Ethernet viene del concepto físico de ether. En su momento el prefijo fast se le agregó para diferenciarla de la versión original Ethernet de 10 Mbps. Debido al incremento de la capacidad de almacenamiento y en el poder de procesamiento, los Pc's actuales tienen la posibilidad de manejar gráficos de gran calidad y aplicaciones multimedia complejas. Cuando estos ficheros son almacenados y compartidos en una red, las transferencias de un cliente a otro producen un gran uso de los recursos de la red.

Las redes tradicionales operaban entre 4 y 16 Mbps. Más del 40 % de todos los Pc's están conectados a Ethernet. Tradicionalmente Ethernet trabajaba a 10 Mbps. A estas velocidades, dado que las compañías producen grandes ficheros, pueden tener grandes demoras cuando envían los ficheros a través de la red. Estos retrasos producen la necesidad de mayor velocidad en las redes.

2.5.2. Gigabit Ethernet

Gigabit Ethernet, también conocida como GigaE, es una ampliación del estándar Ethernet (concretamente la versión 802.3ab y 802.3z del IEEE) que consigue una capacidad de transmisión de 1 gigabit por segundo,

correspondientes a unos 1000 megabits por segundo de rendimiento contra unos 100 de Fast Ethernet (También llamado 100BASE-TX).

Gigabit Ethernet fue la siguiente evolución, incrementando en este caso la velocidad hasta 1000 Mbit/s (1 Gbit/s).

2.5.3. 10 Gigabit Ethernet

10-gigabit Ethernet (XGbE o 10GbE) es el más reciente (año 2002) y más rápido de los estándares Ethernet. IEEE 802.3ae define una versión de Ethernet con una velocidad nominal de 10 Gbit/s, diez veces más rápido que gigabit Ethernet.

El estándar 10-gigabit Ethernet contiene siete tipos de medios para LAN, MAN y WAN. Ha sido especificado en el estándar suplementario IEEE 802.3ae, y será incluido en una futura revisión del estándar IEEE 802.3.

Hay diferentes estándares para el nivel físico (PHY). La letra "X" significa codificación 8B/10B y se usa para interfaces de cobre. La variedad óptica más común se denomina LAN PHY, usada para conectar routers y switches entre sí. Aunque se denomine como LAN se puede usar con 10GBase-LR y -ER hasta 80 km. LAN PHY usa una velocidad de línea de 10.3 Gbit/s y codificación 66B (1 transición cada 66 bits al menos). WAN PHY (marcada con una "W") encapsula las tramas Ethernet para la transmisión sobre un canal SDH/SONET STS-192c.

2.6. Componentes de una Red de Datos

Para poder formar una red de datos se requieren elementos: software, hardware y protocolos. Los componentes físicos se clasifican en dos grandes grupos: dispositivos de usuario final (hosts) y dispositivos de red. Los dispositivos de usuario final incluyen los computadores, impresoras, escáneres, y demás elementos que brindan servicios directamente al usuario y los segundos son todos aquellos que conectan entre sí a los dispositivos de usuario final, posibilitando su intercomunicación.

2.6.1. Software

- **Sistema Operativo de Red**

  Permite la interconexión de ordenadores para poder acceder a los servicios y recursos. Al igual que un equipo no puede trabajar sin un

sistema operativo, una red de equipos no puede funcionar sin un sistema operativo de red. En muchos casos el sistema operativo de red es parte del sistema operativo de los servidores y de los clientes, por ejemplo en Linux y Microsoft Windows.

- **Software de Aplicación**

  En última instancia, todos los elementos se utilizan para que el usuario de cada estación, pueda utilizar sus programas y archivos específicos. Este software puede ser tan amplio como se necesite ya que pueda incluir procesadores de texto, paquetes integrados, sistemas administrativos de contabilidad y áreas afines, sistemas especializados, correos electrónicos, etc. El software adecuado en el sistema operativo de red elegido y con los protocolos necesarios permite crear servidores para aquellos servicios que se necesiten.

2.6.2. Hardware

Está constituido por los elementos físicos que hacen posible la trasmisión de datos

2.6.2.1. Tarjeta de Red

Para lograr el enlace entre las computadoras y los medios de transmisión (cables de red o medios físicos para redes alámbricas e infrarrojos o radiofrecuencias para redes inalámbricas), es necesaria la intervención de una **Tarjeta de Red**, o NIC (Network Card Interface), con la cual se puedan enviar y recibir paquetes de datos desde y hacia otras computadoras, empleando un protocolo para su comunicación y convirtiendo a esos datos a un formato que pueda ser transmitido por el medio (bits, ceros y unos). Cabe señalar que a cada tarjeta de red le es asignado un identificador único por su fabricante, conocido como dirección MAC (Media Access Control), que consta de 48 bits (6 bytes). Dicho identificador permite direccionar el tráfico de datos de la red del emisor al receptor adecuado.

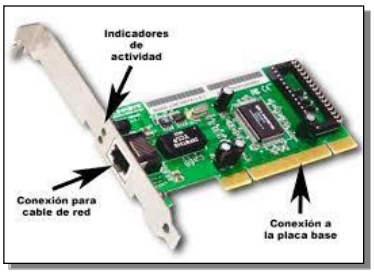


Figura Nº 07 TARJETA DE RED
Fuente: Recuperada de: http://definicion.de/wp-content/uploads/2009/04/tarjetadered.jpg

2.6.2.2. Servidores

Un servidor es un nodo que, formando parte de una red, provee servicios a otros nodos denominados clientes.

2.6.2.2.1. Tipos de Servidores

- ✓ **Servidor de Archivos**: almacena varios tipos de archivo y los distribuye a otros clientes en la red. Pueden ser servidos en distinto formato según el servicio que presten y el medio: FTP, SMB, etc… (http://es.wikipedia.org/wiki/Servidor, 2014).
- ✓ **Servidor de Impresión**: controla una o más impresoras y acepta trabajos de impresión de otros clientes de la red, poniendo en cola los trabajos de impresión (aunque también puede cambiar la prioridad de las diferentes impresiones), y realizando la mayoría o todas las otras funciones que en un sitio de trabajo se realizaría para lograr una tarea de impresión si la impresora fuera conectada directamente con el puerto de impresora del sitio de trabajo. (http://es.wikipedia.org/wiki/Servidor, 2014).
- ✓ **Servidor de Correo**: almacena, envía, recibe, en ruta y realiza otras operaciones relacionadas con el *e-mail* para los clientes de la red. (http://es.wikipedia.org/wiki/Servidor, 2014).
- ✓ **Servidor de Fax**: almacena, envía, recibe, en ruta y realiza otras funciones necesarias para la transmisión, la recepción y la distribución apropiadas de los fax,

con origen y/o destino una computadora o un dispositivo físico de telefax. (http://es.wikipedia.org/wiki/Servidor, 2014).

- ✓ **Servidor de Telefonía**: realiza funciones relacionadas con la telefonía, como es la de contestador automático, realizando las funciones de un sistema interactivo para la respuesta de la voz, almacenando los mensajes de voz, encaminando las llamadas y controlando también la red o Internet, etc. Pueden operan con telefonía IP o analógica. (http://es.wikipedia.org/wiki/Servidor, 2014).
- ✓ **Servidor Proxy**: realiza un cierto tipo de funciones en nombre de otros clientes en la red para aumentar el funcionamiento de ciertas operaciones (p. ej., prefetching y depositar documentos u otros datos que se soliciten muy frecuentemente). También «sirve» seguridad; esto es, tiene un firewall (cortafuegos). Permite administrar el acceso a Internet en una red de computadoras permitiendo o negando el acceso a diferentes sitios web, basándose en contenidos, origen/destino, usuario, horario, etc. (http://es.wikipedia.org/wiki/Servidor, 2014).
- ✓ **Servidor de Acceso Remoto** (RAS, del inglés *Remote Access Service*): controla las líneas de módems u otros canales de comunicación de la red para que las peticiones conecten una posición remota con la red, responden las llamadas telefónicas entrantes o reconocen la petición de la red y realizan los chequeos necesarios de seguridad y otros procedimientos necesarios para registrar a un usuario en la red. Gestionan las entradas para establecer las redes virtuales privadas, VPN. (http://es.wikipedia.org/wiki/Servidor, 2014).

- ✓ **Servidor Web**: almacena documentos HTML, imágenes, archivos de texto, escrituras, y demás material web compuesto por datos (conocidos normalmente como contenido), y distribuye este contenido a clientes que la piden en la red. (http://es.wikipedia.org/wiki/Servidor, 2014).
- ✓ **Servidor de Streaming**: servidores que distribuyen multimedia de forma continua, evitando al usuario esperar a la descarga completa del fichero. De esta forma se pueden distribuir contenidos tipo radio, vídeo, etc. en tiempo real y sin demoras. (http://es.wikipedia.org/wiki/Servidor, 2014).
- ✓ **Servidor de Autenticación**: es el encargado de verificar que un usuario pueda conectarse a la red en cualquier punto de acceso, ya sea inalámbrico o por cable, basándose en el estándar 802.1x y puede ser un servidor de tipo *RADIUS*. (http://es.wikipedia.org/wiki/Servidor, 2014).
- ✓ **Servidores para los Servicios de Red**: estos equipos gestionan aquellos servicios necesarios propios de la red y sin los cuales no se podrían interconectar, al menos de forma sencilla. Algunos de esos servicios son: servicio de directorio para la gestión de los usuarios y los recursos compartidos, Dynamic Host Configuration Protocol (DHCP) para la asignación de las direcciones IP en redes TCP/IP, Domain Name System (DNS) para poder nombrar los equipos sin tener que recurrir a su dirección IP numérica, etc. (http://es.wikipedia.org/wiki/Servidor, 2014).
- ✓ **Servidor de Aplicaciones**: ejecuta ciertas aplicaciones. Usualmente se trata de un dispositivo de software que proporciona servicios de aplicación a las computadoras cliente. Un servidor de aplicaciones

gestiona la mayor parte (o la totalidad) de las funciones de lógica de negocio y de acceso a los datos de la aplicación. Los principales beneficios de la aplicación de la tecnología de servidores de aplicación son la centralización y la disminución de la complejidad en el desarrollo de aplicaciones. (http://es.wikipedia.org/wiki/Servidor, 2014).

2.6.2.3. Estación de Trabajo

En informática una estación de trabajo (en inglés workstation) es un minicomputador de altas prestaciones destinado para trabajo técnico o científico. En una red de computadoras, es una computadora que facilita a los usuarios el acceso a los servidores y periféricos de la red. A diferencia de una computadora aislada, tiene una tarjeta de red y está físicamente conectada por medio de cables u otros medios no guiados con los servidores.

Figura Nº 08 ESTACIÓN DE TRABAJO
Fuente: Recuperada de:
http://www.risco.com.mx/prueba1/catalog/images/computadora.bmp

2.6.2.4. Switch

Un conmutador o switch es un dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red. Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los

puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las redes de área local.

Figura Nº 09 SWITCH
Fuente: Recuperada de:
http://www.risco.com.mx/prueba1/catalog/images/switch.bmp

2.6.2.5. Routers

Un router anglicismo también conocido enrutador o encaminador de paquetes y españolizado como rúter, es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un encaminador (mediante bridges), y que por tanto tienen prefijos de red distintos

Figura Nº 10 ROUTERS
Fuente: Recuperada de:
http://www.risco.com.mx/prueba1/catalog/images/routers.bmp

2.6.3. Protocolos

Existen diversos protocolos, estándares y modelos que determinan el funcionamiento general de las redes. Destacan el modelo OSI y el TCP/IP. Cada modelo estructura el funcionamiento de una red de manera distinta. El modelo OSI cuenta con siete capas muy definidas y con funciones diferenciadas y el TCP/IP con cuatro capas diferenciadas pero que combinan las funciones existentes en las siete capas del modelo OSI. Los protocolos están repartidos por las diferentes capas pero no están definidos como parte

del modelo en sí sino como entidades diferentes de normativas internacionales, de modo que el modelo OSI no puede ser considerado una arquitectura de red.

2.6.3.1. Modelo TCP/IP

Este modelo es el implantado actualmente a nivel mundial: fue utilizado primeramente en ARPANET y es utilizado actualmente a nivel global en Internet y redes locales. Su nombre deriva de la unión de los nombres de los dos principales protocolos que lo conforman: TCP en la capa de transporte e IP en la capa de red. (http://es.wikipedia.org/?title=Modelo_TCP/IP, 2014) .

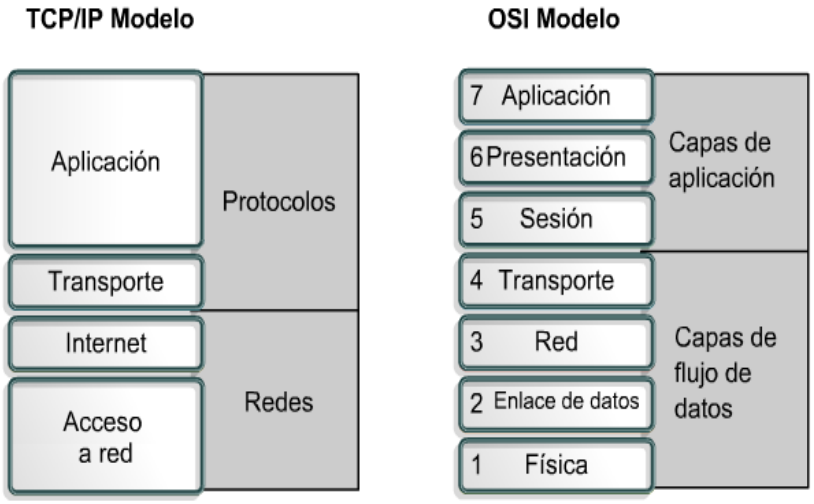


Figura Nº 11 MODELO TCP/IP - OSI
Fuente: Recuperada de: http://tecnologiayredes.tyrdomains.com/images/cisco/tcposi.png

2.7. Cableado Estructurado

Es la infraestructura de cable ordenada e instalada bajo Estándares y Normas Técnicas, destinada a transportar información, a lo largo y ancho de una edificación, que permite interconectar equipos activos, de diferentes o igual tecnología permitiendo la integración de los diferentes servicios como: voz, texto e imágenes que dependen del tendido de cables El sistema de cableado estructurado para edificios soporta una amplia gama de productos de telecomunicaciones sin necesidad de ser modificado.

2.7.1. Escalabilidad de una Red de Datos

Una Red de Datos capaz de adaptarse a un crecimiento posterior se denomina red escalable. Es muy importante planear con anterioridad la cantidad de tendidos y de derivaciones de cableado en el área de trabajo. Es una buena medida tender cables adicionales en el área de backbone para permitir posteriores ampliaciones se recomienda agregar un 20% de carga actual, así como tender un cable adicional hacia cada estación de trabajo. Permitiéndonos ofrecer protección contra pares que puedan fallar durante la instalación, y también permite la expansión. Por otro lado, es necesario colocar una cuerda de tracción cuando se instalan los cables para facilitar el agregado de cables adicionales en el futuro. Cada vez que se agregan nuevos cables, se debe también agregar otra cuerda de tracción.

En las áreas de trabajo se recomienda agregar un 40% de la carga actual ya que se podrá instalar en lo posterior, impresoras equipos, teléfonos IP ya que muchas oficinas pueden pasar de haber un único usuario a varios usuarios.

2.7.2. Normas de Cableado Estructurado

A la hora de garantizar una infraestructura, instalación o proyecto de un sistema de cableado, Unitel se basa en una serie de Normas sobre cableado estructurado, establecidas por una serie de organismo implicado en la elaboración de las mismas.

- ✓ **Organismos**
  - **TIA (Telecommunications Industry Association)**, fundada en 1985 después del rompimiento del monopolio de AT&T. Desarrolla normas de cableado industrial voluntario para muchos productos de las telecomunicaciones y tiene más de 70 normas pre establecidas.
  - **ANSI (American National Standards Institute),** es una organización sin ánimo de lucro que supervisa el desarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unidos. ANSI es miembro de la Organización Internacional para la Estandarización (ISO) y de la Comisión Electrotécnica Internacional (International Electrotechnical Commission, IEC).

- **EIA (Electronic Industries Alliance)**, es una organización formada por la asociación de las compañías electrónicas y de alta tecnología de los Estados Unidos, cuya misión es promover el desarrollo de mercado y la competitividad de la industria de alta tecnología de los Estados Unidos con esfuerzos locales e internacionales de la política.
- **ISO (International Standards Organization)**, es una organización no gubernamental creada en 1947 a nivel mundial, de cuerpos de normas nacionales, con más de 140 países. IEEE (Instituto de Ingenieros Eléctricos y de Electrónica), principalmente responsable por las especificaciones de redes de área local como 802.3 Ethernet, 802.5 Token Ring, ATM y las normas de Gigabit Ethernet.
- **NTP (Normas técnicas Peruanas).**

✓ **Normas**

- **ANSI/TIA/EIA-568-B**: Cableado de Telecomunicaciones en Edificios Comerciales sobre cómo instalar el Cableado: TIA/EIA 568-B1 Requerimientos generales; TIA/EIA 568-B2: Componentes de cableado mediante par trenzado balanceado; TIA/EIA 568-B3 Componentes de cableado, Fibra óptica.
- **ANSI/TIA/EIA-569-A**: Normas de Recorridos y Espacios de Telecomunicaciones en Edificios Comerciales sobre cómo enrutar el cableado.
- **ANSI/TIA/EIA-570-A**: Normas de Infraestructura Residencial de Telecomunicaciones.
- **ANSI/TIA/EIA-606-A**: Normas de Administración de Infraestructura de Telecomunicaciones en Edificios Comerciales.
- **ANSI/TIA/EIA-607**: Requerimientos para instalaciones de sistemas de puesta a tierra de Telecomunicaciones en Edificios Comerciales.
- **ANSI/TIA/EIA-758**: Norma Cliente-Propietario de cableado de Planta Externa de Telecomunicaciones.

✓ **Consideraciones a Tener en Cuenta**

- **Cableado Horizontal,** es decir, el cableado que va desde el Armario de Telecomunicaciones a la toma de usuario.

- No se permiten puentes, derivaciones y empalmes a lo largo de todo el trayecto del cableado.
- Se debe considerar su proximidad con el cableado eléctrico que genera altos niveles de interferencia electromagnética (motores, elevadores, transformadores, etc.) y cuyas limitaciones se encuentran en el estándar ANSI/EIA/TIA 569.
- La máxima longitud permitida independientemente del tipo de medio de Tx utilizado es 100m = 90 m + 3 m usuario + 7 m patchpannel.

- **Cableado Vertical**, es decir, la interconexión entre los armarios de telecomunicaciones, cuarto de equipos y entrada de servicios.
  - Se utiliza un cableado Multipar UTP y STP, y también, Fibra óptica Multimodo y Monomodo.
  - La Distancia Máximas sobre Voz, es de: UTP 800 metros; STP 700 metros; Fibra MM 62.5/125um 2000 metros.

En el caso de instalaciones hospitalarias rige la norma estándar ANSI/TIA 1179, ya que los requisitos de cableado en las instalaciones sanitarias pueden ser mucho más complejos que en un edificio comercial estándar o en un espacio de oficinas, los cuales son cubiertos por la serie de normas TIA-568.

La norma TIA-1179 se creó para tratar los requisitos únicos de las instalaciones sanitarias, usando esta norma podemos tener la confianza en que la infraestructura de cableado que se están diseñando está lista para tolerar las aplicaciones de hoy y también las de mañana. Si bien no describe todos los aspectos de la infraestructura de cableado, la Norma es útil como punto de partida para saber cómo se puede diseñar e implementar un sistema efectivo. Así como hay varias diferencias entre la serie de normas TIA-568 y la Norma TIA-1179, entre las que se incluyen:

- ✓ La recomendación de un mínimo de dos canales diferentes entre la sala de ingresos y las salas de equipos.
- ✓ Un factor de crecimiento estimado en un 100% para las salas de equipos y salas de telecomunicaciones.

- ✓ La recomendación de implementar canales cerrados en espacios de manejo de aire a fin de cumplir con los requisitos de control de infecciones (ICRs).
- ✓ Separación de los cables para diferentes redes y aplicaciones a fin de compatibilizar con los protocolos relativos a seguridad y protección personal. Esta separación puede ser física (separando los canales de cables) y visual (cables de diferentes colores para distintas redes).
- ✓ Densidad de la terminal del área de trabajo

Posiblemente el aspecto más importante de la norma TIA-1179 es la definición de áreas de trabajo. Los autores de la Norma comprenden la necesidad única de contar con diferentes áreas de trabajo en instalaciones sanitarias. Los requisitos de cableado para una sala de espera son muy diferentes a los de las habitaciones de los pacientes o la oficina de enfermería.

Para reflejar estos requisitos únicos, la Norma define 11 clasificaciones de áreas de trabajo, entre las que se incluyen:

- o Servicios al Paciente
- o Cirugía/Procedimientos/Sala de Operaciones
- o Emergencias
- o Cuidados Ambulatorios
- o Salud Femenina
- o Diagnóstico y Tratamiento
- o Cuidadores/Administración
- o Servicios/Soporte
- o Instalaciones
- o Operaciones
- o Cuidados Intensivos

Cada una de estas categorías contiene subgrupos específicos de áreas de trabajo, llevando el número total de áreas de trabajo definidas a 75. A cada área de trabajo se le da una densidad recomendada calificada como Baja, Media o Alta, lo que provee una pauta sobre cuántas terminales de información son apropiadas según el espacio.

- La baja densidad se define entre 2 y 6 terminales.

- La densidad media se define entre 6 y 14 terminales.
- La densidad alta se define para áreas de trabajo que deben contar con más de 14 terminales.

Si se siguen estas pautas se prevé bastante espacio para conexiones adicionales en el futuro y la capacidad para realizar conexiones temporales en las áreas de trabajo en donde sean importantes.

2.7.3. Materiales Básicos en Cableado Estructurado

Los denomino materiales a los diversos dispositivos utilizados en la implementación de una Red de Datos.

- ✓ **Cable UTP CAT 7**

  El cable contiene 4 pares de cable de cobre trenzado, al igual que estándares de cables de cobre anteriores. Aunque la categoría 7 está hecha con cable 23 AWG (American Wire Gauge), esto no es obligatorio; la especificación ANSI/TIA-568-B.2-1 aclara que el cable puede estar hecho entre 22 y 24 AWG, mientras que el cable cumpla todos los estándares de control indicados

  Si los componentes de los varios estándares de cables son mezclados entre sí, el rendimiento de la señal quedará limitado a la categoría que todas las partes cumplan. Como todos los cables definidos por TIA/EIA-568-B, el máximo de un cable Cat-7 horizontal es de 90 metros. Un canal completo (cable horizontal más cada final) se permite que llegue a los 100 metros en extensión.

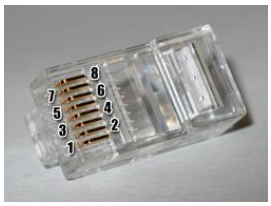
Nº	T568A COLOR	T568B COLOR	PATILLAS EN LA CARA DEL CONECTOR
1	Blanco/Verde	Blanco/Naranja	
2	Verde	Naranja	
3	Blanco/Naranja	Blanco/Verde	
4	Azul	Azul	
5	Blanco/Azul	Blanco/Azul	
6	Naranja	Verde	
7	Blanco/Marrón	Blanco/Marrón	
8	Marrón	Marrón	

Tabla Nº 01 NORMAS (ANSI/TIA T568A–ANSI/TIA T568B)
Fuente: Recuperada de: http://www.taringa.net/posts/hazlo-tu-mismo/14752745/Combinacion-de-colores-de-cables-de-red-RJ45.html

- ✓ **Fibra Óptica**

La fibra óptica es un 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.

El haz de luz queda completamente confinado y se propaga por el interior de la fibra con un ángulo de reflexión por encima del ángulo límite de reflexión total, en función de la ley de Snell. La fuente de luz puede ser láser.

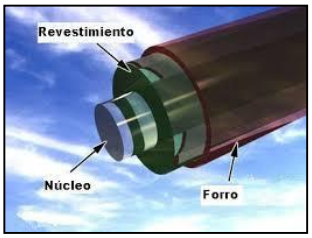


Figura Nº 12 FIBRA OPTICA
Fuente: Recuperada de: http://www.monografias.com/red-fibra-optica2.shtml

- ✓ **Racks**

  Un rack es un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones. Las medidas para la anchura están normalizadas para que sean compatibles con equipamiento de cualquier fabricante. También son llamados bastidores, cabinas, cabinets o armarios.

Figura Nº 13 VISTA DE UN RACK
Fuente: Recuperada de:
http://www.moibatec.com/paginas/servicios/productos/redes.html

- ✓ **Panel de Parcheo**

  Un panel de conexiones, también denominado bahía de rutas o patch panel, es el elemento encargado de recibir todos los cables del cableado estructurado. Sirve como un organizador de las conexiones de la red, para que los elementos relacionados de la Red LAN y los equipos de la conectividad puedan ser fácilmente incorporados al sistema y además los puertos de conexión de los equipos activos de la red (Switch, Router, etc.) no tengan algún daño por el constante trabajo de retirar e introducir en sus puertos.

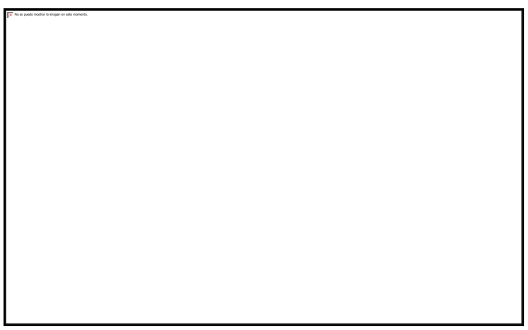


Figura Nº 14 PANEL DE PARCHEO
Fuente: Recuperada de:
http://www.taringa.net/posts/apuntes-y-monografias/panel-parcheo.html

- ✓ **Canaletas**

Son los ductos que se encargan de llevar y proteger los cables de red por una ruta pre establecida no se permitirá que por ella pasen cables de línea eléctrica ellos deberán estar a una distancia no menor de 25 cm., es necesario el uso de accesorios en caso de giros horizontales y verticales, evitando el deterioro del cable, los accesorios a tener en cuenta son:

- **Curva Plana**. Para giros verticales o rodear el marco de una puerta.
- **Rinconero**. Esquina interna de columna o esquina de dos paredes
- **Esquinero**. Esquina externa de una columna o final de pared a bordear.
- **T Plana**. Continuación lineal con derivación vertical
- **Unión Plana**. Une dos canaletas seguidas.
- **Tapa Final**. Cierra el extremo final de una rama de canaletas.

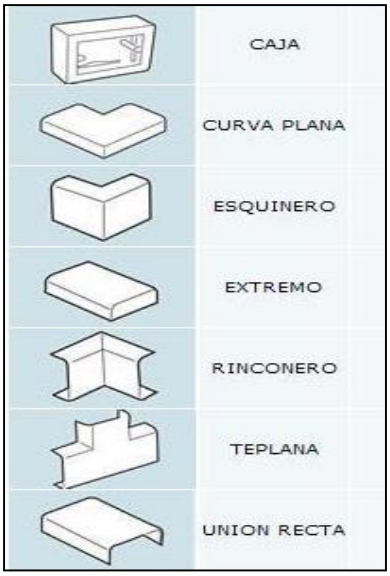


Figura Nº 15 ACCESORIOS PARA CANALETAS
Fuente: Recuperada de:
http://www.cegallo.com.mx/Canaletas-accesorioshtml

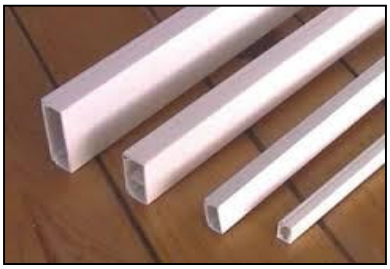


Figura Nº 16 CANALETAS
Fuente: Recuperada de:
http://www.cegallo.com.mx/Canaletas_y_Ductos.html

Tener en cuenta las medidas de las canaletas ya que son apropiadas para el uso en paredes. Su constitución amplia permite soportar cantidades superiores de cables algunas de ellas ofrecen un cierre hermético que protege del polvo y roedores.

Medidas de Canaletas Planas

15x10mm.	Cap.	1	cable
24x14mm.	Cap.	4	cables
39x18mm.	Cap.	8	cables
39x18mm.	C/div. Cap.	8	cables
60x22mm.	Cap.	20	cables
65x45mm.	Cap.	30	cables
100x50mm.	Cap.	50	cables

Tabla Nº 02 MEDIDAS DE CANALETAS PLANAS
Fuente: Elaborado por los Autores

Medidas de Canaletas de Piso

20G	Cap.	1	cable
50G	Cap.	3	cables
70G	Cap.	7	cables

Tabla Nº 03 MEDIDAS DE CANALETAS DE PISO
Fuente: Elaborado por los Autores

- ✓ **Rosetas**

Es el soporte donde se conectan los Path Cord, consta de una a 4 bahías de conexión.

Figura Nº 17 ROSETAS
Fuente: Recuperada de: http://www.cegallo.com.mx/Rosetas.html

- ✓ **Jacks**

Los Jack's son unos conectores que sirven de intermediario entre el Patch Cord que conecta una PC al cable que llega al Pacth Panel. Van dentro las cajas toma datos. Existen Jacks a presión y otros con herramienta de impacto.

Figura Nº 18 JACKS
Fuente: Recuperada de: http://www.cegallo.com.mx/jacks.html

- ✓ **Patch Cord**

Patch Cord o cable (UTP)' se usa en una red para conectar un dispositivo electrónico con otro. Se producen en muchos colores para facilitar su identificación. En cuanto a longitud, los cables de red pueden ser desde muy cortos (unos pocos centímetros) para los componentes apilados, o tener hasta 100 metros máximo. A medida que aumenta la longitud los cables son más gruesos y suelen tener apantallamiento para evitar la pérdida de señal y las interferencias (STP).

No existe un conector estándar ya que todo dependerá del uso que tenga el cable, pero generalmente se usa con un RJ45.

Aunque esta definición se usa con mayor frecuencia en el campo de las redes informáticas, pueden existir patch cords también para otros tipos de comunicación electrónica.

Los cables de red también son conocidos principalmente por los instaladores como chicote o latiguillo.

Figura Nº 19 PATCH CORD O LATIGUILLO
Fuente: Recuperada de:
http://www.semacables.com/sema/prodC6LAT.html

- ✓ **Conector RJ 45**

  RJ-45 (Registered Jack 45) es una interfaz física comúnmente usada para conectar redes de cableado estructurado, (categorías 4, 5, 5e, 6 y 6a). Es parte del Código Federal de Regulaciones de Estados Unidos. Posee ocho pines o conexiones eléctricas, que normalmente se usan como extremos de cables de par trenzado.

  Es utilizada comúnmente con estándares como TIA/EIA-568-B, que define la disposición de los pines o wiring pinout. Una aplicación común es su uso en cables de red Ethernet, donde suelen usarse 8 pines (4 pares).

Figura Nº 20 CONECTOR RJ45
Fuente: Recuperada de: http://www.pfarrell.com/technotes/rj45wiring.html

2.8. Wifi

Es una nueva tecnología que surgió por la necesidad de establecer un mecanismo de conexión inalámbrica que fuese compatible entre los distintos dispositivos, buscando esa compatibilidad fue que en 1999 las empresas 3Com, Airones, Intersil, Lucent Technologies, Nokia y Symbol Technologies se reunieron para crear la Wireless Ethernet Compatibility Alliance, o WECA, actualmente llamada Wi-Fi Alliance. (http://es.wikipedia.org/wiki/Wi-Fi, 2014). En abril de 2000 WECA certifica la interoperabilidad de equipos según la norma IEEE 802.11b, bajo la marca Wi-Fi. Esto quiere decir que el usuario tiene la garantía de que todos los equipos que tengan el sello Wi-Fi pueden trabajar juntos sin problemas, independientemente del fabricante de cada uno de ellos.

Al referirnos a **Wifi** decimos que es una de las tecnologías de comunicación inalámbrica mediante ondas utilizada hoy en día. WIFI, también llamada WLAN (Wireless Lan, Red Inalámbrica) o estándar IEEE 802.11.

2.8.1. Estándares de Certificación Wi-Fi

Los estándares aprobados son los siguientes:

- ✓ Los estándares IEEE 802.11b, IEEE 802.11g e IEEE 802.11n disfrutan de una aceptación internacional debido a que la banda de 2.4 GHz está disponible casi universalmente, con una velocidad de hasta 11 Mbit/s, 54 Mbit/s y 300 Mbit/s, respectivamente. (http://es.wikipedia.org/wiki/Wi-Fi, 2014).
- ✓ En la actualidad ya se maneja también el estándar IEEE 802.11a, conocido como WIFI 5, que opera en la banda de 5 GHz y que disfruta de una operatividad con canales relativamente limpios. La banda de 5 GHz ha sido recientemente habilitada y, además, no existen otras tecnologías (Bluetooth, microondas, ZigBee, WUSB) que la estén utilizando, por lo tanto existen muy pocas interferencias. Su alcance es algo menor que el de los estándares que trabajan a 2.4 GHz (aproximadamente un 10%), debido a que la frecuencia es mayor (a mayor frecuencia, menor alcance). (http://es.wikipedia.org/wiki/Wi-Fi, 2014).
- ✓ Existe un primer borrador del estándar IEEE 802.11n que trabaja a 2.4 GHz y a una velocidad de 108 Mbit/s. Sin embargo, el estándar802.11g es capaz de alcanzar ya transferencias a 108 Mbit/s, gracias a diversas técnicas de aceleramiento. Actualmente existen ciertos dispositivos que permiten utilizar esta tecnología, denominados *Pre-N*. (http://es.wikipedia.org/wiki/Wi-Fi, 2014).

2.8.2. Seguridad y Fiabilidad

Uno de los problemas a los cuales se enfrenta actualmente la tecnología Wi-Fi es la progresiva saturación del espectro radioeléctrico, debido a la masificación de usuarios, esto afecta especialmente en las conexiones de larga distancia (mayor de 100 metros). En realidad Wi-Fi está diseñado para conectar ordenadores a la red a distancias reducidas, cualquier uso de mayor alcance está expuesto a un excesivo riesgo de interferencias. (http://es.wikipedia.org/wiki/Wi-Fi, 2014).

Otro factor es la configuración por defecto de muchos dispositivos Wi-Fi es muy insegura (routers, por ejemplo) dado que a partir del identificador del

dispositivo se puede conocer la clave de éste; y por tanto acceder y controlar el dispositivo se puede conseguir en sólo unos segundos.

Si contamos con una red Wifi se debe tener en cuenta lo siguiente:

- ✓ Cambios frecuentes de la contraseña de acceso, utilizando diversos caracteres, minúsculas, mayúsculas y números.
- ✓ Se debe modificar el SSID que viene predeterminado.
- ✓ Realizar la desactivación del broadcasting SSID y DHCP.
- ✓ Configurar los dispositivos conectados con su IP (indicar específicamente qué dispositivos están autorizados para conectarse).
- ✓ Utilización de cifrado: WPA2.

Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son la utilización de protocolos de cifrado de datos para los estándares Wi-Fi como el WEP, el WPA, o el WPA2 que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos. La mayoría de las formas son las siguientes:

- ✓ WPA: presenta mejoras como generación dinámica de la clave de acceso. Las claves se insertan como dígitos alfanuméricos.
- ✓ IPSEC (túneles IP) en el caso de las VPN y el conjunto de estándares IEEE 802.1X, que permite la autenticación y autorización de usuarios.
- ✓ Filtrado de MAC, de manera que sólo se permite acceso a la red a aquellos dispositivos autorizados. Es lo más recomendable si solo se va a usar con los mismos equipos, y si son pocos.
- ✓ Ocultación del punto de acceso: se puede ocultar el punto de acceso (Router) de manera que sea invisible a otros usuarios.
- ✓ El protocolo de seguridad llamado WPA2 (estándar 802.11i), que es una mejora relativa a WPA. En principio es el protocolo de seguridad más seguro para Wi-Fi en este momento. Sin embargo requieren hardware y software compatibles.

Cabe señalar que, no existe ninguna alternativa totalmente fiable, ya que todas ellas son susceptibles de ser vulneradas en cualquier momento.

2.8.3. Dispositivos

Podemos enunciar dos tipos de dispositivos: dispositivos de distribución o red y dispositivos terminales.

2.8.3.1. Dispositivos de Distribución o Red

- ✓ **Los puntos de acceso** son dispositivos que generan un "set de servicio", que podría definirse como una "Red Wi-Fi" a la que se pueden conectar otros dispositivos. Los puntos de acceso permiten, en resumen, conectar dispositivos en forma inalámbrica a una red existente. Pueden agregarse más puntos de acceso a una red para generar redes de cobertura más amplia, o conectar antenas más grandes que amplifiquen la señal.

Figura Nº 21 ACCESS POINT
Fuente: Recuperada de:
http://www.peruanadeinformatica.com.pe/accesspoint.html

- ✓ **Los Repetidores Inalámbricos** son equipos que se utilizan para extender la cobertura de una red inalámbrica, éstos se conectan a una red existente que tiene señal más débil y crean una señal limpia a la que se pueden conectar los equipos dentro de su alcance. Algunos de ellos funcionan también como punto de acceso.

- ✓ **Los Router Inalámbricos** son dispositivos compuestos, especialmente diseñados para redes pequeñas (hogar o pequeña oficina). Estos dispositivos incluyen, un Router (encargado de interconectar redes, por ejemplo, nuestra red del hogar con internet), un punto de acceso (explicado más arriba) y generalmente un switch que permite conectar algunos equipos vía

cable (Ethernet y USB). Su tarea es tomar la conexión a internet, y brindar a través de ella acceso a todos los equipos que conectemos, sea por cable o en forma inalámbrica.

Figura Nº 22 ROUTER INALÁMBRICO
Fuente: Recuperada de: http://www.peruanadeinformatica.com.pe/router.html

2.8.3.2. Dispositivos Terminales

Los mismos que comprenden tres tipos: Tarjetas PCI, Tarjeta PCMCIA y Tarjetas USB. El Wifi puede ser desactivado por un dispositivo terminal.

- ✓ **Las Tarjetas PCI para Wi-Fi** se agregan (o vienen de fábrica) a los ordenadores de sobremesa. Hoy en día están perdiendo terreno debido a las tarjetas USB. Dentro de este grupo también pueden agregarse las tarjetas MiniPCI que vienen integradas en casi cualquier computador portátil disponible hoy en el mercado.

Figura Nº 23 TARJETA PCI WIFI
Fuente: Recuperada de:
http://www.peruanadeinformatica.com.pe/wifi.html

- ✓ **Las Tarjetas PCMCIA** son un modelo que se utilizó mucho en los primeros ordenadores portátiles, aunque están cayendo en desuso, debido a la integración de tarjeta inalámbricas internas en estos ordenadores. La mayor parte de estas tarjetas solo son

capaces de llegar hasta la tecnología B de Wi-Fi, no permitiendo por tanto disfrutar de una velocidad de transmisión demasiado elevada

Figura Nº 24 TARJETA PCMCIA
Fuente: Recuperada de:
http://www.peruanadeinformatica.com.pe/pcmcia.html

- ✓ **Las Tarjetas USB para Wi-Fi** son el tipo de tarjeta más común que existe en las tiendas y más sencillo de conectar a un pc, ya sea de sobremesa o portátil, haciendo uso de todas las ventajas que tiene la tecnología USB. Hoy en día puede encontrarse incluso tarjetas USB con el estándar 802.11N (Wireless-N) que es el último estándar liberado para redes inalámbricas.

Figura Nº 25 TARJETA USB WIFI
Fuente: Recuperada de:
http://www.peruanadeinformatica.com.pe/wifi-usb.html

Así mismo existen impresoras, cámaras Web y otros periféricos que funcionan con la tecnología Wi-Fi, permitiendo crear una red en lugares de difícil acceso.

2.9. Plataforma de Administración de la Red Informática Hospitalaria

2.9.1. Windows Server 2012

Es la última edición lanzada por Microsoft Corporation del Sistema Operativo Windows Server. Es la versión para servidores de Windows 8 y es el sucesor de Windows Server 2008 R2. El software está disponible para los

consumidores desde el 4 de septiembre de 2012. A diferencia de su predecesor, Windows Server 2012 no tiene soporte para computadoras con procesadores Intel Itanium y se venden cuatro ediciones.

Se han agregado o mejorado algunas características comparado con Windows Server 2008 R2, como una actualización de Hyper-V, un rol de administración de direcciones IP, una nueva versión del Administrador de Tareas de Windows, y se presenta un nuevo sistema de archivos: ReFS. (http://es.wikipedia.org/wiki/Windows_Server_2012,)

2.9.1.1. Escalabilidad

Windows Server 2012 admite las siguientes especificaciones máximas de hardware. Windows Server 2012 mejora respecto de su predecesor Windows Server 2008 R2 (http://es.wikipedia.org/wiki/Windows_Server_2012, 2013):

Especificación	Windows Server 2012	Windows Server 2008 R2
Procesadores Físicos	64	64
Procesadores Lógicos Cuando Hyper-V es Deshabilitado	640	256
Procesadores lógicos cuando Hyper-V es Habilitado	320	64
Memoria	4 TB	2 TB
Nodos de Conmutación por error de clúster (en cualquier clúster individual)	64	16

Tabla Nº 04 ESPECIFICACIÒN WIN SERVER 2012 – WIN SERVER 2008
Fuente: Recuperada de: ww.windowstecnico.com/archive/2012/10/03/ventajas-competitivas-de-windows-server-2012-frente-a-vmware-vsphere-5-1.aspx

2.9.1.2. Requisitos de Sistema

Según Microsoft, Windows Server 2012 sólo se ejecuta en procesadores x64, y ha indicado que Windows Server 2012 no soportará los procesadores de 32-bit (IA-32) o Itanium (IA-64).

Los mínimos requerimientos de sistema para correr Windows Server 2012 son:

- ✓ Arquitectura de processador: x64 (64 bit)
- ✓ Procesador: 1.4 GHz
- ✓ Memoria RAM: 512 MB
- ✓ Espacio libre en disco duro: 32 GB (más si hay 16 GiB o más de RAM)
- ✓ DVD-ROM
- ✓ Monitor SVGA con resolución 800×600 o superior
- ✓ Teclado
- ✓ Mouse o dispositivo apuntador compatible

Además, para añadir el rol de Hyper-V a Windows Server 2012, también se requiere que el procesador de 64 bit sea compatible con las instrucciones de virtualización AMD-V o Intel-VT y por lo menos 4 GB de RAM para correr hasta cuatro máquinas virtuales. Si se planea usar cinco o más máquinas virtuales, deberá contemplarse que será necesaria más memoria RAM.

Actualizaciones desde Windows Server 2008 y Windows Server 2008 R2 son compatibles, aunque las actualizaciones desde versiones anteriores no serán compatibles.

(http://es.wikipedia.org/wiki/Windows_Server_2012, 2013)

2.9.1.3. Ediciones

Windows Server 2012, a diferencia de Windows Server 2008 R2, solo tiene cuatro ediciones: Foundation, Essentials, Standard y Datacenter. (http://es.wikipedia.org/wiki/Windows_Server_2012, 2013).

ESPECIFICACIONES	FOUNDATION	ESSENTIALS	STANDARD	DATACENTER
Distribución	Sólo OEM	Retail, licenciamiento por volumen, OEM	Retail, licenciamiento por volumen, OEM	Licenciamiento por volumen, OEM
Modelo de licenciamiento	Por servidor	Por servidor	Por CPU+ CAL	Por CPU+ CAL
Precio	N/A	USD 501	USD 882	USD 4 809
Límite de chips de procesador	1	2	64	64
Límite de usuarios	**Parcial**: 15	**Parcial**: 25	✓ **Sin límite**	✓ **Sin límite**
Límite de servicios de archivos	**Parcial**: Una raíz DFS autónoma	**Parcial**: Una raíz DFS autónoma	✓ **Sin límite**	✓ **Sin límite**
Políticas de Red y límites de Servicios de Acceso	**Parcial**: 50 conexiones RRAS y 10 conexiones IAS	**Parcial**: 250 conexiones RRAS, 50 conexiones IAS, and 2 grupos de servidores IAS	✓ **Sin límite**	✓ **Sin límite**
Límites de Servicios de Escritorio Remoto	**Parcial**: 20 conexiones de Servicios de Escritorio Remoto	**Parcial**: 250 conexiones de Servicios de Escritorio Remoto	✓ **Sin límite**	✓ **Sin límite**
Permisos de Virtualización	N/A	**Parcial**: Una máquina virtual o un servidor físico, pero no los dos a la vez	**Parcial**: 2 máquinas virtuales	✓ **Sin límite**
Rol **DHCP**	✓ **Sí**	✓ **Sí**	✓ **Sí**	✓ **Sí**
Rol **DNS server**	✓ **Sí**	✓ **Sí**	✓ **Sí**	✓ **Sí**
Rol **Servidor de Fax**	✓ **Sí**	✓ **Sí**	✓ **Sí**	✓ **Sí**
Servicios UDDI	✓ **Sí**	✓ **Sí**	✓ **Sí**	✓ **Sí**
Servicios de Impresión y	✓ **Sí**	✓ **Sí**	✓ **Sí**	✓ **Sí**

Documentación				
Servicios Web (**Internet InformationServices**)	✓ **Sí**	✓ **Sí**	✓ **Sí**	✓ **Sí**
Windows DeploymentServices	✓ **Sí**	✓ **Sí**	✓ **Sí**	✓ **Sí**
Windows Server UpdateServices	✓ **Sí**	✓ **Sí**	✓ **Sí**	✓ **Sí**
Active Directory Lightweight Directory Services	✓ **Sí**	✓ **Sí**	✓ **Sí**	✓ **Sí**
Active Directory Rights Management Services	✓ **Sí**	✓ **Sí**	✓ **Sí**	✓ **Sí**
Rol **Aplicación de Servidor**	✓ **Sí**	✓ **Sí**	✓ **Sí**	✓ **Sí**
Server Manager	✓ **Sí**	✓ **Sí**	✓ **Sí**	✓ **Sí**
Windows Powershell	✓ **Sí**	✓ **Sí**	✓ **Sí**	✓ **Sí**
Active DirectoryDomainServices	✓ **Parcial**: Debe ser la raíz de bosque y dominio	✓ **Sí**	✓ **Sí**	✓ **Sí**
Active DirectoryCertificateServices	✓ **Parcial**: Solamente Autoridades de Certificación	✓ **Parcial**: Solamente Autoridades de Certificación	✓ **Sí**	✓ **Sí**
Active DirectoryFederationServices	✓ **Sí**	✗ **No**	✓ **Sí**	✓ **Sí**
Modo **Server Core**	✗ **No**	✗ **No**	✓ **Sí**	✓ **Sí**
Hyper-V	✗ **No**	✗ **No**	✓ **Sí**	✓ **Sí**

Tabla Nº 05 WINDOWS SERVER 2012

Fuente: Recuperada de: www.windowstecnico.com/archive/2014/10/03/ventajas-competitivas-de-windows-server-2012.aspx

2.9.1.3.1. Comparación con Otras Plataformas

SISTEMA OPERATIVO	WINDOWS SERVER 2012	UBUNTU SERVER	RHEL	FREEBSD	OPENBSD	OS X SERVER	AIX	HP-UX
Desarrollador	Microsoft Corporation	Canonical Ltd. y Fundación Ubuntu	Red Hat	Proyecto FreeBSD	Proyecto OpenBSD	Apple Inc.	IBM	Hewlett-Packard
Costo	$501 USD (Essentials) $882 USD (Standard) $4809 USD (Datacenter)	Gratuito Soporte técnico $750 USD y $1200 USD	?	Gratuito	Gratuito	$19.99 (paquete adicional a OS X) $499 USD	Incluido con el hardware	$400 USD
Licencia	Propietaria: Microsoft CLUF	Libre: GPL y otras	Libre: GPL y componentes propietarios	Libre: Licencia BSD, Licencia FreeBSD	Libre: Licencia BSD, Licencia ISC	Propietaria: Apple CLUF	Propietaria	Propietaria
Arquitecturas de procesador soportadas	x86-64	x86, x86-64, ARM	x86, x86-64, Power, ESA/390, z/Architecture	x86, x86-64, DEC Alpha, ARM, SPARC64, IA-64, PowerPC, MIPS	68000, Alpha, x86-64, i386, MIPS, PowerPC, SPARC 32/64, VAX, Zaurus y otras	x86-64	PA-RISC, IA-64	ROMP, IBM POWER, PowerPC, IBM PS/2, System/370, ESA/390
Sistemas de archivos soportados por defecto	ReFS, NTFS, FAT 12/16/32, ExFAT, ISO 9660, UDF	ext2, ext3, ext4, btrfs, FAT 12/16/32, ReiserFS, ISO 9660, UDF, NFS, HFS, HFS+, NTFS, HPFS, FFS, XFS, JFS, y otros	ext2, ext3, ext4, btrfs, FAT 12/16/32, ReiserFS, ISO 9660, UDF, NFS, HFS, HFS+, NTFS, HPFS, FFS, XFS, JFS, y otros	UFS 1/2, FAT 12/16/32, HPFS, FFS, ext2, ext3, ZFS, UDF, ISO 9660	FFS, ext2, FAT, ISO 9660, NFS, otros	HFS+, HFS, MFS, ISO 9660, FAT 12/16/32, UDF, ExFAT, FFS	JFS, JFS2, ISO 9660, UDF, NFS, SMBFS, GPFS	VxFS, HFS, ISO 9660, UDF, NFS, SMBFS
Memoria RAM mínima y máxima soportada	Min. 512 MiB Max. 4 TiB	Min. 128 MiB Max. ?	Min. 1 GiB Máx. 1 TiB (teórico)	Min. 24 MiB Max. ?	Min. 128 MiB Max. ?	Min. 2 GiB Max. ?	?	Min. 1,5 GiB Max. 4 TiB
Almacenamiento mínimo requerido	32 GB	1 GB	4 GB	150 MB	1 GB	10 GB	?	20 GB
Máximo de CPU físicas	64	?	64	?	?	?	?	?
Reloj de CPU mínimo	1.4 GHz	300 MHz	2 GHz	?	100 MHz	?	?	?

Tabla Nº 06 OTRAS PLATAFORMAS

Fuente: Recuperada de: www.windowstecnico.com/archive/2014/10/03/ventajas-competitivas-de-windows-server-2012.aspx

2.10. METODOLOGIA : Top-Down Network Design

Es una metodología propuesta por Cisco Press & Priscilla Oppenheimer (OPPENHEIMER, 2010), la misma que se centra en las necesidades de requerimientos y diseño arquitectónico de redes de comunicaciones que debe de completarse antes de la selección de determinados componentes específicos para construir una red física (OPPENHEIMER, 2010).

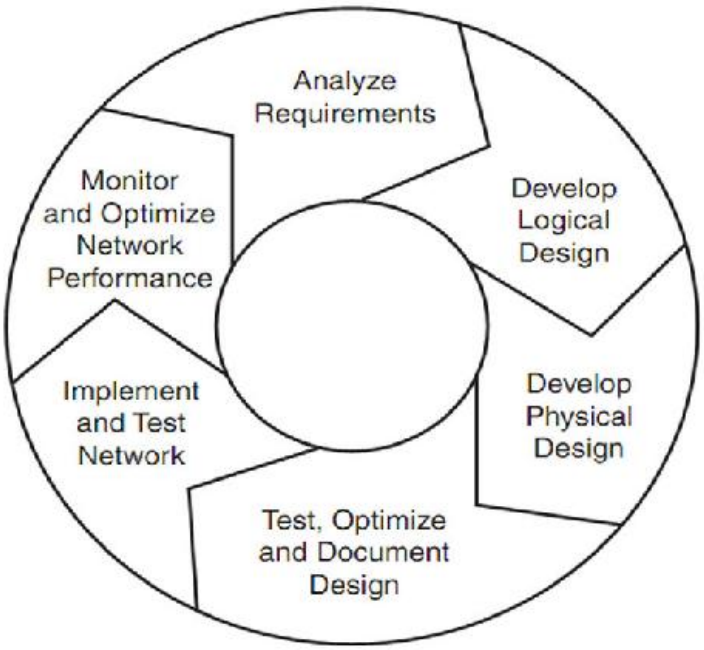


Figura Nº 26 FASES DE METODOLOGÌA TOP-DOWN-NETWORK DESIGN
Fuente: http://analisisydisenio.wikispaces.com/disenio_descendente.png

Esta metodología propone cuatro Fases, para el diseño de redes:

- ✓ Fase 1: Análisis de Negocios Objetivos y Limitaciones.
- ✓ Fase 2: Diseño Lógico.
- ✓ Fase 3: Diseño Físico.
- ✓ Fase 4: Pruebas, Optimización y Documentación de la Red.

2.10.1. I Fase de Identificación de Necesidades y Objetivos de los Clientes

Es la etapa inicial de todo proyecto, cuyo objetivo principal de este procedimiento es conocer las necesidades de negocio a las que tiene que dar solución. En función del conocimiento y la experiencia previa, se deberá invertir un menor o mayor esfuerzo en esta actividad que dependerá del

conocimiento que se tenga del cliente y su problemática, el esfuerzo en esta actividad se deberían centrar en obtener las nuevas necesidades de negocio y los objetivos a lograr. El comprender los objetivos comerciales es un aspecto, crítico del diseño de red, pero de ello depende para plantear una solución que sea aceptada por el cliente.

2.10.1.1. Análisis de los Objetivos y Restricciones del Negocio

Análisis de Objetivos

- Conocer Línea de Negocio y el Mercado del Cliente.

  Su objetivo principal es conocer la línea de negocio actual, especialmente sus procesos de negocio.

- Estructura Organizacional de la Empresa.

  Es la organización de cargos y responsabilidades que deben cumplir los miembros de una organización; es un sistema de roles que han de desarrollarlos miembros de una entidad para trabajar en equipo, de forma óptima y alcanzar las metas propuestas en el plan estratégico y plan de empresa. Los principios que guían el diseño de la estructura de la organización de una empresa son: Principio de autoridad y jerarquía que se fundamenta en la existencia de diferentes niveles de autoridad, ordenados en jerarquías según el grado de responsabilidad y control.

- Determinar la Autoridad Responsable para la Aceptación del Diseño de Red Propuesto.

  Se definirá quien estará a cargo de la aceptación el diseño de Red Propuesto, el mismo que debe ser un amplio conocedor, con experiencia ya que garantizara el desarrollo y la aceptación del diseño propuesto.

- Realizar un Cuestionario de Preguntas a los Clientes para Conocer sus Objetivos hacia su Negocio.

Análisis de Restricciones

El diseño depende muchas de las veces de los Costos (Presupuesto), Análisis del Retorno de la Inversión, de Políticas y Normas.

2.10.1.2. Análisis de los Objetivos Técnicos y sus Restricciones

- ✓ **Escalabilidad** El diseño de red debe ser capaz de adaptarse a los incrementos en el uso y alcance de la red; es decir; se refiere al crecimiento que un diseño de red debe soportar. Es importante tener en cuenta que hay muchas restricciones para la escalabilidad inherentes en tecnologías de redes.

- ✓ **Disponibilidad** Se refiere a la cantidad de tiempo que una red esta operativa para los usuarios, éste es a menudo un objetivo crítico para el diseño de red de los clientes. La tasa de disponibilidad obtenida entre el tiempo aceptable y el tiempo ideal (proporcionado por el cliente) que debe tener un diseño de red es expresada como porcentaje de tiempo por año, mes, semana, día u hora, comparada con el tiempo total en ese periodo.

  Tasa de Disponibilidad (TD) = Tiempo Aceptable*100
  Tiempo Ideal

  Dónde:

  Tiempo Aceptable = Tiempo Ideal - Tasa de Pérdida de Tiempo

- ✓ **Performance** Es considerado el nivel de servicio que ha sido estipulado con los clientes. Los criterios para que el cliente considere una buena performance de la red, incluye Rendimiento Exactitud, Eficiencia, Retraso y Variación del Retraso

- ✓ **Seguridad** El plan de seguridad es uno de los aspectos más importantes en el diseño de redes, especialmente cuando las

organizaciones agregan conexiones de Internet. Los problemas de seguridad no deben interrumpir el rumbo del negocio de la organización. El diseño de red necesita convicciones que ofrezca alguna protección contra los datos, servicios del negocio y otros recursos que se pueden perder o dañar.

- ✓ **Usabilidad.** La usabilidad se refiere a la facilidad de uso con que los usuarios pueden acceder a la red y sus servicios. La usabilidad enfoca en hacer los trabajos de usuario de la red más fácil. Es importante ganar una comprensión de cómo la usabilidad es importante para el diseño de la red del cliente, porque algunos componentes del diseño de red puede tener un efecto negativo en la usabilidad.

- ✓ **Adaptabilidad**

  Un diseño de red debería poder adaptarse y cambiarse a las nuevas tecnologías. Los cambios pueden entrar en la forma de nuevos protocolos, nuevas prácticas de negocio, nuevos objetivos fiscales, etc.

- ✓ **Accesibilidad**

  Es el grado en el que todas las personas pueden utilizar un objeto, visitar un lugar o acceder a un servicio de la red, independientemente del tipo de hardware, software, infraestructura de red, idioma, cultura, localización geográfica y capacidades de las mismas.

  En las redes, el bajo costo es a menudo un objetivo primario. Los clientes esperan poder implementar una infraestructura de red a bajo costo. Dependiendo de las aplicaciones que corren en los sistemas finales, el bajo costo es a menudo más importante que la disponibilidad y la performance en los diseños del campo de la red. Para redes empresariales, la

disponibilidad es normalmente más importante que el bajo costo.

2.10.1.3. Caracterización de la Red Existente

Es el documento que permite identificar, describir los diferentes componentes que conforman la red actual de computadoras.

2.10.1.4. Caracterización del Tráfico de la Red

Documentar las estadísticas de tráfico de la red, compuesta por el uso de protocolos, los principales emisores, los principales generadores de tráfico broadcast y las fuentes de error. Identificación y localización de los que acaparan ancho de banda. Análisis de las tendencias de rendimiento con informes de datos básicos

2.10.2. Fase II Diseño Lógico

En esta fase se diseñará la topología de red, el modelo de direccionamiento y nombramiento, y se seleccionará los protocolos de bridging, switching y routing para los dispositivos de interconexión. El diseño lógico también incluye la seguridad y la administración de la red.

2.10.2.1. Diseño de la Topología de Red.

Una topología es un mapa de red, que indica segmentos de red, puntos de interconexión, y comunidades de usuarios.

- Diseño de Red Jerárquica

  Un diseño de red jerárquico permite establecer redes que sean escalables y modulares. El modelo de tres niveles permite la agregación y filtración de tráfico en tres niveles sucesivos de routing o switching.

  - ⇒ Nivel central o núcleo
  - ⇒ Nivel de distribución
  - ⇒ Nivel de acceso.

- Diseño de Topologías de Red Redundantes

  El fallo de un equipo no afecta el resto de la Red (Red Malla)

- Diseño de la Red Modular

  El diseño modular de la red nos da como resultado una elevada escalabilidad de la misma.

- Diseño de la Topología de Red de un Campus.

  Una red de campus se extiende a otros edificios dentro de un campus o área industrial. Los diversos segmentos o LAN de cada edificio suelen conectarse mediante cables de la red de soporte.

2.10.2.2. Modelo de Direccionamiento y Nombramiento

Las asignaciones de direcciones y nombres sistemáticos ayudan a alcanzar los objetivos de escalabilidad, performance y gestión de la red.

- Un Modelo Estructurado para el direccionamiento significa que las direcciones son significativas, jerárquicas y planeadas.
- La asignación dinámica reduce la tarea de configuración de usuarios finales para acceder a la red.
- Las direcciones IP privadas son direcciones que un administrador de red asigna a la red interna.
- Los nombres deben ser cortos y significativos para simplificar la administración de la red.
- Considerar nombres de host, DNS, etc.

2.10.2.3. Selección de Protocolos de Switching y Routing

Las decisiones con respecto a los protocolos y tecnologías deben estar basadas en la información recolectada de los objetivos de negocios y técnicos de los clientes.

Principales Métodos de Switching

- Store and Forward

  Que almacenan cada grupo de datos en un buffer antes de retransmitirlo.

- Fragment - Free

Fue proyectado para eliminar el encaminamiento de runts por la red. El switch siempre lee los primeros 64 bytes de cada trama, asegurando que tenga por lo menos el tamaño mínimo.

- Cut - Through

  Los conmutadores cut-through fueron diseñados para reducir esta latencia. Esos switches minimizan el delay leyendo sólo los 6 primeros bytes de datos de la trama, que contiene la dirección de destino MAC, e inmediatamente la encaminan, permitiéndonos descartar paquetes defectuosos.

- Source-Route Switching (SRS)

  Está basado en Source Route Transparent Bridging SRS reenvía un frame que no tiene un campo de información de la ruta de la misma manera que lo hace el bridging trasparent. Todas las llamadas que son conmutadas a la ruta de origen tienen el mismo número de llamadas y el conmutador aprende las direcciones MAC de los dispositivos en estas llamadas.

  1) Los protocolos de routing se agrupan en dos principales clases: Protocolos Distance-Vector y Protocolos Link Protocolos de encaminamiento Ad hoc. Se encuentran en aquellas redes que tienen poca o ninguna infraestructura.
  2) IGPs (Interior Gateway Protocols). Intercambian información de encaminamiento dentro de un único sistema autónomo.
  3) EGPs (Exterior Gateway Protocol). Intercambian rutas entre diferentes sistemas autónomos. Encontramos:
     - ✓ EGP. Utilizado para conectar la red de backbones de la Antigua Internet.
     - ✓ BGP (Border Gateway Protocol). La actual versión, BGPv4 data de 1995.

2.10.2.4. Desarrollo de Estrategias de Seguridad de la Red.

El desarrollar estrategias de seguridad implica realizar una serie de acciones que permita la protección de la información trasmitida a

través de ella tratando de evitar que la información sea manipulada o malversada.

- **Identificar los Recursos y Riesgos de la Red**

  La identificación adecuada y documentada de los recursos y riesgos con los que cuenta una red nos permitirá tener un mayor control, es necesario muchas veces hacerse estas preguntas.

  - ¿Qué se necesita proteger?
  - ¿De quién debe de protegerlo?
  - ¿Cómo debe de protegerlo?

  Los activos de red pueden incluir hosts de la red (incluidos los sistemas operativos de los hosts, aplicaciones y datos), los dispositivos de interconexión (como routers y switches), y los datos que circulan por la red. Menos obvio, pero sigue siendo importante, los activos incluyen la propiedad intelectual, secretos comerciales, y la reputación de una empresa.

- **Analizar los Riesgos de Seguridad**

  La finalidad del análisis de riesgos es identificar porciones de red, asignar una calificación de riesgo a cada porción y aplicar los niveles de seguridad apropiados.

- **Analizar los Requerimientos de Seguridad.**

  Una vez identificados los riesgo, se puede adoptar controles y medidas de seguridad que permitan gestionarlos ya sea reduciendo las amenazas, las vulnerabilidades o bien disminuyendo el impacto frente a algún incidente de seguridad, estas medidas se traducen en requerimientos que deben ser analizados con la finalidad de garantizar la información que se trasmite por la red no sea manipulada ni malversada.

- **Desarrollar un Plan de Seguridad**

  Un Plan de seguridad es un documento debidamente elaborado y detallado de alto nivel donde se define los requerimientos y requisitos de seguridad de una red, basada en los objetivos de

los clientes, análisis de riesgos y recursos de la red. Haciendo referencia a la topología e incluye una lista de servicios definiendo quienes tienen acceso a estos servicios. Así como también se define la configuración e implementación del desarrollo del plan y políticas de seguridad es decir cómo se hace. Esta lista debe especificar que proporciona los servicios, quién tiene acceso a los servicios, cómo se proporciona el acceso, y quien administra los servicios

- **Definir Políticas de Seguridad**

  Una política de seguridad informa a los usuarios, administradores y personal técnico de sus obligaciones para la tecnología de proteger los activos de información. La política debe especificar los mecanismos por los que estas obligaciones pueden cumplirse. Como fue el caso con el plan de seguridad, la política de seguridad debe tener aceptación por parte de los empleados, gerentes, ejecutivos y personal técnico.

- **Mecanismos de Seguridad:**

  A continuación algunos mecanismos comunes para brindar la seguridad a una red de datos.

  ⇒ **Autenticación**

  Es el proceso de intento de verificar la identidad, de una persona que usa un ordenador, un sistema un acceso a la red, etc., es un modo de asegurar que los usuarios son quienes dicen que ellos son. Existen tres características de autenticación.

  - Sistemas basados en algo conocido. Ejemplo, un password (Unix) o passphrase (PGP).
  - Sistemas basados en algo poseído. Ejemplo, una tarjeta de identidad, una tarjeta inteligente (smartcard), dispositivo usb tipo epasstoken, smartcard o dongle criptográfico.

- Sistemas basados en una característica física del usuario o un acto involuntario del mismo: Ejemplo, verificación de voz, de escritura, de huellas, de patrones oculares.

⇒ **Protección del Hardware**

El hardware es frecuentemente el elemento más caro de todo sistema informático y por tanto las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier organización. Problemas frecuentes a los que nos enfrentamos:

- Acceso Físico

  Si alguien que desee atacar un sistema tiene acceso físico al mismo todo el resto de medidas de seguridad implantadas se convierten en inútiles.

  De hecho, muchos ataques son entonces triviales, como por ejemplo los de denegación de servicio; si apagamos una máquina que proporciona un servicio es evidente que nadie podrá utilizarlo.

  Otros ataques se simplifican enormemente, por ejemplo si deseamos obtener datos podemos copiar los ficheros o robar directamente los discos que los contienen.

  Para evitar todo este tipo de problemas deberemos implantar mecanismos de prevención (control de acceso a los recursos) y de detección (si un mecanismo de prevención falla o no existe debemos al menos detectar los accesos no autorizados cuanto antes).

  Para la prevención hay soluciones para todos los gustos y de todos los precios: analizadores de retina, tarjetas inteligentes, videocámaras, vigilantes jurados, etc.

- Desastres Naturales

Además de los posibles problemas causados por ataques realizados por personas, es importante tener en cuenta que también los desastres naturales pueden tener muy graves consecuencias, sobre todo si no los contemplamos en nuestra política de seguridad y su implantación. Algunos desastres naturales a tener en cuenta:

- ✓ Terremotos y vibraciones
  - No situar equipos en sitios altos para evitar caídas,
  - No colocar elementos móviles sobre los equipos para evitar que caigan sobre ellos,
  - Separar los equipos de las ventanas para evitar que caigan por ellas o qué objetos lanzados desde el exterior los dañen,
  - Utilizar fijaciones para elementos críticos,
  - Colocar los equipos sobre plataformas de goma para que esta absorba las vibraciones,
- ✓ Tormentas Eléctricas
- ✓ Inundaciones y humedad
- ✓ Incendios y humos

- Alteraciones del Entorno

  En nuestro entorno de trabajo hay factores que pueden sufrir variaciones que afecten a nuestros sistemas que tendremos que conocer e intentar controlar. Deberemos contemplar problemas que pueden afectar el régimen de funcionamiento habitual de las máquinas como la alimentación eléctrica, el ruido eléctrico producido por los equipos o los cambios bruscos de temperatura.

  - ✓ Electricidad
  - ✓ Ruido Eléctrico
  - ✓ Temperaturas Extremas

⇒ **Protección de los Datos**

Además proteger el *hardware* nuestra política de seguridad debe incluir medidas de protección de los datos, ya que en realidad la mayoría de ataques tienen como objetivo la obtención de información, no la destrucción del medio físico que la contiene.

En los puntos siguientes mencionaremos los problemas de seguridad que afectan a la transmisión y almacenamiento de datos, proponiendo medidas para reducir el riesgo.

- Eavesdropping

  La *interceptación* o *eavesdropping*, también conocida por "passivewiretapping" es un proceso mediante el cual un agente capta información que va dirigida a él; esta captación puede realizarse por muchísimos medios: *sniffing* en redes ethernet o inalámbricas (un dispositivo se pone en modo promiscuo y analiza todo el tráfico que pasa por la red), capturando radiaciones electromagnéticas (muy caro, pero permite detectar teclas pulsadas, contenidos de pantallas, etc.).

- Copias de Seguridad

  Es evidente que es necesario establecer una política adecuada de copias de seguridad en cualquier organización; al igual que sucede con el resto de equipos y sistemas, los medios donde residen estas copias tendrán que estar protegidos físicamente.

  Lo primero que debemos pensar es dónde se almacenan los dispositivos donde se realizan las copias. Un error muy habitual es almacenarlos en lugares muy cercanos a la sala de operaciones, cuando no en la misma sala; esto, que en principio puede parecer correcto (y cómodo si necesitamos restaurar unos archivos) puede convertirse en un problema serio si se produce

cualquier tipo de desastre (como p. ej. un incendio). Hay que pensar que en general el hardware se puede volver a comprar, pero una pérdida de información puede ser ireemplazable.

- Soportes no Electrónicos

  Otro elemento importante en la protección de la información son los elementos no electrónicos que se emplean para transmitirla, fundamentalmente el papel. Es importante que en las organizaciones que se maneje información confidencial se controlen los sistemas que permiten exportarla tanto en formato electrónico como en no electrónico (impresoras, plotters, faxes, etc.).

2.10.2.5. Desarrollo de Estrategias de Gestión de la Red

La administración proactiva significa chequear la salud de la red durante una operación normal, para reconocer problemas potenciales, optimizando la performance y actualizaciones. (OPPENHEIMER, 2010).

Un buen diseño de gestión de la red puede ayudar a una organización a lograr la disponibilidad, el rendimiento y los objetivos de seguridad. Los procesos de gestión de redes eficaces pueden ayudar a una organización a medir qué tan bien se están cumpliendo los objetivos de diseño y ajustar los parámetros de la red si no se cumplen estos objetivos, también facilita alcanzar los objetivos de escalabilidad, ya que puede ayudar a una organización analizar el comportamiento actual de la red, permite realizar las actualizaciones adecuadamente y resolver cualquier problema con las actualizaciones.

Los componentes básicos de la estrategia de Gestión de Red son:

- Gestión de Performance

  De acuerdo con la norma ISO, la gestión del rendimiento permite la medición de la conducta y la eficacia de la red. La

gestión del rendimiento consiste en el examen aplicación y el protocolo de comportamiento de la red, análisis de la accesibilidad, la medición de tiempo de respuesta, y el registro de los cambios de ruta de la red. La gestión del rendimiento facilita la optimización de una red, cumpliendo los acuerdos de nivel de servicio (SLA), y la planificación para la expansión. Supervisión del rendimiento implica la recopilación de datos, el procesamiento de todos o algunos de los datos, visualización de los datos transformados, y el archivo de todos o algunos de los datos(OPPENHEIMER, 2010).

- Gestión de Falla

  Se refiere a la detección, aislamiento, diagnóstico y corrección de problemas. También incluye procedimientos para reportar problemas a los usuarios finales y los administradores, y el seguimiento de las tendencias relacionadas con problemas. En algunos casos, la gestión de fallos significa desarrollar soluciones hasta que un problema se puede solucionar. (OPPENHEIMER, 2010).

- Gestión de Configuración

  Gestión de configuración ayuda a un administrador de red de seguimiento de los dispositivos de red y mantener la información sobre la configuración de dispositivos. Con la gestión de la configuración, un administrador de red puede definir y guardar una configuración por defecto para los dispositivos similares, modifique la configuración por defecto para los dispositivos específicos, y cargar la configuración de los dispositivos. (OPPENHEIMER, 2010).

- Gestión de Seguridad

  Las políticas de Control y pruebas de seguridad y protección, el mantenimiento y la distribución de las contraseñas y otra información de autenticación y autorización, claves de

encriptación, gestión y auditoría adhesión a las políticas de seguridad.

- Gestión de Contabilidad o Auditoria

  Gestión contable facilita la facturación basada en el uso, por el que se pagan los departamentos o proyectos individuales para los servicios de red. Incluso en los casos en los que no hay intercambio de dinero, lo que representa el uso de la red puede ser útil para capturar los departamentos o individuos que realizan un inadecuado uso de la red "abuso". El abuso puede ser intencional (por ejemplo, un empleado descontento o ex empleados que causan problemas en la red) o no intencional. (People juegos en red en reproducción no tienen la intención de dañar la red, pero pueden causar un exceso de tráfico).

2.10.3. Fase III Diseño Físico

Esta fase implica en seleccionar las tecnologías y dispositivos específicos que darán satisfacción a los requerimientos técnicos de acuerdo al diseño lógico propuesto (LAN / WAN). (OPPENHEIMER, 2010).

2.10.3.1. Selección de Tecnologías y Dispositivos para la Red del Campus

- ✓ Diseño del Cableado Estructurado.

  Elaboración de Planos del cableado estructurando respetando normas de seguridad y estándares de fabricantes, este proceso implica el documentar el cableado de las redes de campus, incluyendo los siguientes puntos:

  1. Campus - y construir - cableado topologías.
     Planos de la infraestructura, y de telecomunicaciones.
  3. Tipos y longitudes de los cables entre edificios.
  4. La ubicación de los armarios de telecomunicaciones y salas de interconexión dentro de los edificios.
  5. Tipos y longitudes de cables para el cableado vertical entre plantas.

6. Tipos y longitudes de cables para el cableado horizontal en planta.
7. Tipos y longitudes de cables para el cableado del área de trabajo que va desde armarios de telecomunicaciones para estaciones de trabajo.

✓ Tecnologías LAN: ATM, Fast Ethernet, Giga Ethernet

- **ATM**

  Podríamos decir que es un paso evolutivo más allá de FrameRelay

  No se efectúa ni control de errores ni control de flujo en los enlaces internos entre los nodos de la red. Los paquetes tienen longitud fija y de tamaño pequeño y son llamados celdas o células (cells). Funcionalidad limitada en los encabezados (headers) de las celdas. Funciones primarias son la identificación de la celda y el tipo de circuito virtual, más unas pocas funciones de corrección de errores. No se hacen relaciones de tiempo respecto de las celdas en los nodos internos de la red. La multiplexación no es relativa a la posición de las celdas en un slot (casilla de tiempo) especifico, para ello cada celda tiene un identificador. De aquí la razón por la que se denomina transferencia asincrónica.

- **VoIP**

  VoIP conjuga dos mundos históricamente separados, la trasmisión de voz y de datos. Se trata de transportar la voz previamente digitalizada, entre dos puntos distantes, esto posibilita usar las redes de datos para efectuar las llamadas telefónicas, y desarrollar una única red convergente que se encargue de cursar todo tipo de comunicación, ya sea voz, datos, videos o imágenes. VoIP no es un servicio sino una tecnología que permite encapsular la voz en paquetes para poder transportarla sobre redes de datos sin necesidad de

disponer de un circuito conmutado convencional PSTN (Public Switched Telephone Network).

- **Switch**

  El switch opera en el nivel del cruzamiento o combinación de datos y tiene como finalidad principal garantizar la interconexión de un mínimo de dos segmentos de red, actúa de manera similar a la función de un puente (bridge). Este dispositivo de red se encarga de transmitir los datos de un segmento a otro de acuerdo a la dirección MAC que tengan como destino las tramas de esta estructura. Su tarea hace foco en la conexión de diferentes redes y sus correspondientes fusiones. El switch, por su utilidad, actúa como un filtro y optimiza el rendimiento de las redes de área local (conocidas como LAN por Local Area Network). Los switches tienen la capacidad de conservar las mencionadas direcciones MAC de los equipos a los que puede llegar desde cada uno de sus puertos.

- **Router**

  Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un enrutador (mediante bridges), y que por tanto tienen prefijos de red distintos.

- **Bridge**

  Es un dispositivo que sirve para conectar segmentos de red a través de medios físicos diferentes, como el cable coaxial y la fibra óptica. Se diferencia de un hub porque este último pasa cualquier trama con cualquier destino para todos los otros nodos conectados, en cambio, el primero sólo pasa las tramas pertenecientes a cada

segmento para mejorar el rendimiento de las redes al disminuir tráfico inútil.

- **Inalámbrico**

  Partamos de la definición de inalámbrico, este término se refiere al uso de la tecnología sin cables la cual permite la conexión de varios computadores entre sí. Es así como se ha ido convirtiendo en uno foco de estudio para los temas de transmisión de datos, adquiriendo mayor interés en lugares donde no es posible la instalación de redes alámbricas. El uso de esta tecnología inalámbrica permite dejar en el olvido de los cables sin la necesidad de dejar de establecer una conexión, desapareciendo las limitaciones de espacio y tiempo, dando la impresión de que puede ubicarse una oficina en cualquier lugar del mundo. Una aplicación de este caso podría ser la relación que se establece entre empleados ubicados en un lugar que no sea su centro de labores y una red adquiriendo la empresa mayor flexibilidad. Los dispositivos son conectados a otros dispositivos inalámbricos con el fin de brindar a los trabajadores dinámicos una estrategia de trabajo más efectiva y con menos complicaciones.

- **Radio Enlace**

  El radio enlace, establecen un concepto de comunicación del tipo dúplex, de donde se deben transmitir dos portadoras moduladas: una para la Transmisión y otra para la Recepción. Al par de frecuencia asignada para la transmisión y recepción de las señales, se lo denomina radio canal. Los enlaces se hacen básicamente entre puntos visibles, es decir, puntos altos de la topografía. Cualquiera que sea la magnitud del sistema de microondas, para un correcto funcionamiento es necesario que los recorridos entre enlaces tengan una altura libre

adecuada para la propagación en toda época del año, tomando en cuenta las variaciones de las condiciones atmosféricas de la región. Para poder calcular las alturas libres debe conocerse la topografía del terreno, así como la altura y ubicación de los obstáculos que puedan existir en el trayecto.

7.1.1.1. Selección de Tecnologías y Dispositivos para la Red Empresarial

Tecnología de Acceso Remoto

- ✓ Línea de Suscripción Digital (DSL)

  La DSL llama bastante la atención de implementadores y proveedores de servicios. Esto se debe a que proporciona velocidades de datos de banda ancha a ubicaciones dispersas con cambios relativamente pequeños a la infraestructura de telecomunicaciones existente.

  El término xDSL designa a diversas formas de DSL que compiten entre sí, incluida ADSL (DSL asimétrica).

- ✓ Red Privada Virtual (VPN)

  Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.

- ✓ Línea Dedicada

  Una línea dedicada es un contrato de servicios celebrado entre un proveedor y un cliente, por lo que el proveedor se compromete a entregar una línea de telecomunicaciones simétrica que conecta dos o más lugares a cambio de una renta mensual (de ahí el arrendamiento a largo plazo). A veces se

conoce como un "circuito privado" o "línea de datos". A diferencia de tradicionales líneas de la Red Telefónica Conmutada (PSTN), no tienen un número de telefónico porque cada lado de la línea está permanentemente conectado a la otra. Las líneas arrendadas pueden utilizarse para telefonía, para datos o para servicios de Internet.

- ✓ Acceso Satelital

  Una red satelital consiste de un transponder (dispositivo receptor-transmisor), una estación basada en tierra que controlar su funcionamiento y una red de usuario, de las estaciones terrestres, que proporciona las facilidades para transmisión y recepción del tráfico de comunicaciones, a través del sistema de satélite.

7.1.2. Fase IV Prueba, Optimización y Documentación

Cada sistema es diferente; la selección de métodos y herramientas de prueba correctos, requiere creatividad, ingeniosidad y un completo entendimiento del sistema a ser evaluado. (OPPENHEIMER, 2010).

Implementación de un Plan de Pruebas

7.1.2.1. Prueba del Diseño de la Red

- Usar Pruebas de los Fabricantes
- Construir un Prototipo de Pruebas

  El alcance de un prototipo de red puede depender de los objetivos tanto técnicos como no técnicos. Preste atención a los factores no técnicos, tales como los prejuicios de sus clientes, el estilo de negocio, y la historia de los proyectos de la red. Tal vez el cliente ya rechazó un diseño de la red debido a su falta de capacidad de gestión y las características de usabilidad y así podría estar predispuesto a buscar estos problemas en su sistema. Si este es el caso, uno de los objetivos de su prototipo debe ser el desarrollo de una demostración que muestra las prestaciones de manejabilidad y facilidad de uso.

Un prototipo puede ser implementado y probado en tres maneras:

- En una red de prueba en un laboratorio.
- Integrado en una red de producción pero a prueba durante las horas libres.
- Integrado en una red de producción y probado durante el horario normal.

➢ Herramientas de Prueba de Diseño de Redes

Cisco Works Internetwork Performance Monitor (IPM) es una solución de problemas de red y control de la aplicación de esa red medidores tiempo de respuesta y la disponibilidad. Ayuda a los administradores de red a descubrir los problemas de rendimiento de red de extremo a extremo, localizar cuellos de botella, el tiempo de respuesta de la medida, y diagnosticar problemas de latencia. CiscoWorks IPM es un componente de Cisco Works LAN Management Solution (LMS).

➢ La Prueba debe Incluir análisis de Performance y de Fallas:

✓ Prueba de Aplicación de Tiempo de Respuesta
✓ Prueba de Rendimiento
✓ Prueba de la Disponibilidad
✓ Prueba de Regresión

7.1.2.2. Optimización del Diseño de la Red

La optimización es un paso crítico del diseño para las organizaciones que utilizan gran ancho de banda. Para lograr los objetivos de negocio, estas organizaciones esperan que sus redes utilizcen el ancho de banda de manera eficiente, para controlar retardo. (OPPENHEIMER, 2010).

➢ Optimización del Uso del ancho de Banda con Tecnología IP Multicast
➢ Reduciendo el Delay de la Serialización.
➢ Optimización de la performance de la Red para QoS.

- Cisco Internetwork Operating System Features for Optimizing Network.

7.1.2.3. Documentación de la Red

- Respondiendo a la Propuesta de los Requerimientos del Cliente
  En este punto del proceso de diseño, usted debe tener un diseño integral que se basa en un análisis de los negocios de sus clientes y los objetivos técnicos, e incluye tanto componentes lógicos y físicos que han sido probados y optimizados, que van a satisfacer los requerimientos hechos por el cliente.
- Los Contenidos de los Documentos del Diseño de la Red
  Documenta la red existente, el diseño lógico y físico, y el presupuesto y los gastos relacionados con el proyecto.

CAPITULO III
DESARROLLO DEL TRABAJO DE TESIS

3.1. Metodología Top-Down Network Design

Actualmente, en el Hospital de Chancay y Servicios Básicos de Salud la infraestructura de red de datos no fue planificada mediante la utilización de una metodología formal, motivo por el cual el desempeño de la red existente, no se aproxima a las necesidades esperadas y mucho menos a un nivel óptimo. Esta situación es más que preocupante para la institución por ello se plantea desarrollar una red de datos, eficiente, segura y confiable, la misma que será fuente de constante estudio, desarrollo e investigación; contando con un dimensionamiento de la red basado en una metodología formal y la implementación de políticas de gestión de red. En el presente trabajo, se plantea la Implementación de una Red Informática Hospitalaria, Usando Metodología Top Down Network Design, dentro de la cual mediante estudios de capacidad, cobertura y operación del estándar se determinará su viabilidad. La metodología Top Down Network Design propuesta por Cisco Press & Priscilla Oppenheimer (OPPENHEIMER, 2010) la misma que se centra en las necesidades de requerimientos y diseño arquitectónico de redes de comunicaciones, plantea cuatro fases para el diseño de redes.

- ✓ Fase 1: Análisis de Negocios Objetivos y Limitaciones
- ✓ Fase 2: Diseño Lógico
- ✓ Fase 3: Diseño Físico
- ✓ Fase 4: Plan de Implementación.

3.1.1. Fase 1 Análisis de Negocio Objetivos y Limitaciones

El Hospital Chancay y Servicios Básicos de Salud, a través de su área administrativa consciente de los cambios y avances tecnológicos, en la actualidad presenta una red informática deficiente, causante de retraso en los procesos administrativos llevando consigo pérdidas de tiempo, desea contar en el más breve plazo con edificaciones modernas y automatizadas tecnológicamente, con personal altamente calificado para poder brindar de

manera adecuada servicios de salud a los pacientes; brindando información clara, suficiente, confidencial, oportuna y veraz

3.1.1.1. Identificación de Necesidades

El Hospital Chancay y Servicios Básicos de Salud, pretende optimizar el uso de recursos como hardware (impresoras, escáner, dispositivos de almacenamiento de datos, servocunas, centrifugadoras, hornos, etc.), centralizar su información manteniéndola actualizada para todos los usuarios permitiendo trabajar de forma grupal y simultanea evitando el uso de medios de almacenamiento (Cds, USB. etc.), insumos (papel, toner, tinta de impresora, etc); logrando un ahorro significativo de costos y tiempo. Cree conveniente Implementar una Red Informática Hospitalaria.

3.1.1.1.1. Institución

El Hospital Chancay, se inaugura el 17 de Setiembre de 1971, durante el segundo Gobierno Revolucionario del General Juan Velazco, siendo Ministro de Salud el Gral. FAP Fernando Miroquesada Bahamonde. Gracias al gobierno de Alemania se construyen dos centros de salud gemelos en infraestructura: el de Puente Piedra y el de Chancay edificado sobre un área de 6,273 m2. Mediante Resolución Directoral N° 063-DG-DSRS-III-LN-96, de fecha 18 de Marzo de 1996, se crea el Servicio Básico de Salud de Chancay, como órgano desconcentrado de la Dirección Subregional de Salud III Lima Norte, los mismos que tendrán a su cargo la formulación, planificación, organización, ejecución y evaluación de las acciones integrales de salud en el ámbito de la jurisdicción de los Distritos de Chancay y Aucallama de la provincia de Huaral, Departamento de Lima; a los Establecimientos de Salud que se detallan:

- Hospital de Apoyo Chancay

- Centro de Salud de Chancayllo
- Centro de Salud Aucallama
- Puesto de salud de Pampa Libre
- Puesto de Salud Cerro la Culebra
- Puesto de Salud Quepepampa
- Puesto de Salud Peralvillo
- Puesto de Salud Pasamayo
- Puesto de Salud Palpa

(En la actualidad los establecimientos de salud, pertenecen a la Red de Salud Huaral).

- **Misión**

  Brindar atención integral y especializada de salud a la población del Hospital Chancay y SBS de la Región Lima, con equidad, calidad y transparencia; priorizando grupos vulnerables, en concertación con los sectores público, privado y otros actores sociales.

- **Visión**

  Institución especializada y acreditada con recurso humano competente y comprometido en brindar servicios de salud de calidad, desarrollando una eficiente gestión por resultados, promoviendo estilos de vida saludable a la población de la Región.

3.1.1.1.2. Áreas, Unidades, Departamentos y Servicios de la Institución

- Dirección Ejecutiva
- Sub Dirección Ejecutiva
- Dirección Administrativa
- Oficina de Control Interno
- Oficina de Planeamiento
- Unidad de Epidemiología
- Departamento Consulta Externa

- Departamento Medicina
- Departamento Cirugía
- Departamento Pediatría
- Departamento Ginecología
- Departamento Enfermería
- Departamento Odontología
- Departamento Emergencia
- Departamento Anestesiología
- Departamento Patología Clínica
- Departamento Diagnostico
- Departamento Apoyo al Tratamiento
- Unidad Gestión de la Calidad
- Unidad Personal
- Unidad Economía
- Unidad Servicios Generales
- Unidad Estadística e Informática
- Unidad Apoyo a la Docencia
- Unidad Seguros
- Unidad Logística
- Unidad de Comunicaciones
- Servicio Cirugía
- Servicio Cirugía Especializada
- Servicio de Neonatología
- Servicio de Pediatría
- Servicio de Ginecología
- Servicio Obstétrico
- Servicio de Patología
- Servicio de Nutrición
- Servicio de Psicología
- Servicio Social
- Área de Salud Integral

ORGANIGRAMA ESTRUCTURAL DEL HOSPITAL DE CHANCAY Y SERVICIOS BÁSICOS DE SALUD

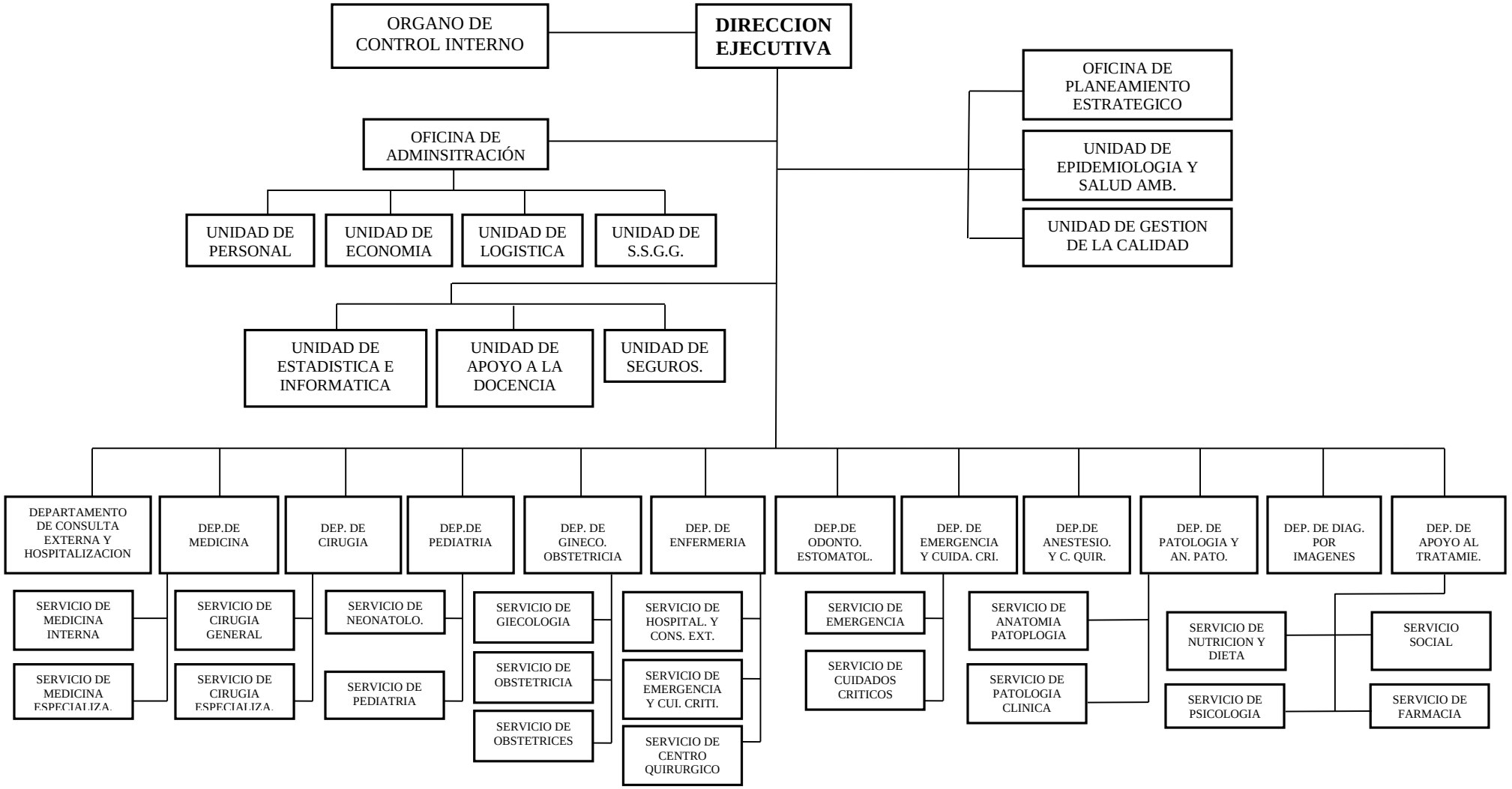


Figura Nº 27 ORGANIGRAMA ESTRUCTURAL DEL HOSPITAL CHANCAY Y S.B.S.

Fuente: Hospital Chancay y Servicios Básicos de Salud (2014), Recuperado de: Área de Comunicaciones.

3.1.1.1.3. Autoridad Responsable

- Director Ejecutivo: Dr. Víctor Virú Tang.
- Sub Director Ejecutivo: Dr. Lindón Trujillo Soto.
- Director Administrativo: Dr. Roger Benites Farfan.

3.1.1.1.4. Requerimiento de los Usuarios

Con la finalidad de recolectar información en cuanto a los requerimientos de los usuarios de la red, de las distintas Unidades, Departamentos y Servicios, se utilizó la herramienta de trabajo grupal, denominada lluvia de ideas o tormenta de ideas, mediante la cual los trabajadores aportaban con ideas respecto a las características que debe cumplir la Red de Datos a implementarse y las necesidades a cubrir, se obtuvo a partir de allí los siguientes resultados:

- Contar con infraestructura hospitalaria moderna y automatizada tecnológicamente.
- Contar con una red informática que garantice la trasmisión de datos, fidedigna, rápida, segura, oportuna suficiente y eficaz.
- Permitir un alto grado de comunicación entre áreas, unidades y departamentos.
- Hacer uso adecuado de tecnología automatizando los procesos administrativos hospitalarios.
- Ahorro costos en los servicios de trasmisión de información hospitalaria.
- Que se cuente con servicio de internet.
- Que sea de fácil acceso y uso.
- Contar con equipos que garanticen su funcionamiento adecuado en horas de trabajo.
- Reducción de tiempo en el proceso de la información.
- Aumentar las ventajas competitivas sobre los hospitales del mismo nivel.

- Que los cables de red no se encuentren a la vista y sin ninguna protección.
- Que el acceso de nuevos usuarios no ocasione mayores dificultades.

3.1.1.1.5. Cambios que se Generarían

Entre los principales cambios que generaría el contar con una Red Informática Hospitalaria tenemos:

- Compartir la información entre las diferentes áreas, de manera rápida, segura, suficiente y oportuna de manera económica.
- Compartir recursos como impresoras, escáner, fotocopiadoras, entre las diversas áreas hospitalarias. etc.
- Ahorro de tiempo en la trasmisión de datos, entre las diferentes áreas hospitalarias.
- Se administrara y se dará soporte a los equipos de las diferentes áreas hospitalarias, de manera centralizada.
- Colas de pacientes de menor número en Caja, Admisión y Farmacia.

3.1.1.1.6. Objetivos del Negocio

Entre los principales objetivos del Hospital de Chancay y Servicios Básicos de Salud tenemos:

- Brindar al paciente atención adecuada en la prevención y promoción de la salud, donde prácticamente el servicio es de consulta externa y urgencias médicas menores.
- Brindar al paciente atención adecuada a nivel hospitalario, contando con áreas de consulta externa, hospitalización, urgencias, terapia y quirófanos.
- Brindar al paciente atención adecuada, en procedimientos diagnósticos, especiales hechos por

especialistas como cardiólogos, neumólogos, nefrólogos, endocrinólogos, gastroenterólogos, neurólogos, etc.

- Agilizar la trasmisión de información de forma eficiente, suficiente y segura entre sus diversas áreas, unidades, departamentos y servicios.
- Contar con una infraestructura hospitalaria moderna y automatizada tecnológicamente.
- Compartir recursos como información, impresoras, escáner, fotocopiadoras, etc.
- Ahorro sustancial en costo de insumos (papel, tóner, tintas de impresión, usb, DVD, CD, etc.).
- Permitir la continuidad de los servicios ante un siniestro (desastre natural, incendio, robo o error humano, etc).
- Conseguir que el presente proyecto sea considerado en el Plan Operativo Institucional.

3.1.1.1.7. Alcance

El alcance del diseño de la Implementación de la Red Informática Hospitalaria se llevará a cabo en todas la Áreas, Departamentos, Unidades y Servicios del Hospital Chancay y Servicios Básicos De Salud.

3.1.1.1.8. Identificación de Aplicaciones

Las aplicaciones que se usan y deban de usarse en las áreas, unidades y servicios el Hospital de Chancay y Servicios Básicos de Salud son las siguientes:

APLICACIÓN	TIPO DE APLICACIÓN	RANGO CRITICO	COMETARIO
Windows Server 2012	Sistema Operativo de Servidor	Muy Importante	Es el Sistema Operativo que se instalara en nuestro Servidor
Windows 7	Sistema Operativo de Terminal	Muy Importante	Es el Sistema Operativo que se instalara en cada Estación de Trabajo
Windows 8	Sistema Operativo de Terminal	Muy Importante	Es el Sistema Operativo que se instalara en cada Estación de Trabajo
Microsoft Office 2010	Ofimática	Muy Importante	Es el software usado en la mayor parte de las Estaciones de Trabajo.
Microsoft Office 2007	Ofimática	Muy Importante	Es el software usado por algunas Estaciones de Trabajo.
Winrar	Ofimática	Importante	Usado para empacar y desempacar archivos.
Sophos	Antivirus	Muy Importante	Antivirus usado como consola y en todas las Estaciones de Trabajo.
Sighospi	Group Ware	Muy Importante	Es el software de gestión hospitalaria con que cuenta el Hospital
SIAF	Group Ware	Muy Importante	Es el sistema integrado de administración financiera.
Google Chrome	Internet	Importante	Software de navegación de internet de uso en el Hospital.

Tabla Nº 07 APLICACIONES A USARSE EN EL HOSPITAL CHANCAY Y S.B.S.
Fuente: Elaborada por los Autores

3.1.1.2.Análisis de Restricciones

En el análisis de restricciones a las que se enfrenta un proyecto; la mayor restricción es lograr el presupuesto donde la elaboración del mismo no es solo tomar en cuenta materiales y mano de obra sino también las circunstancias en las que se debe llevar a cabo el proyecto, en este caso tomaremos en cuenta la, restricción de

Personal y de Inversión en Infraestructura (Activo Fijo) y Costo de Servicios (Gasto)

- **Restricciones**
  - La institución no cuenta con personal especializado en la elaboración de proyectos.

- **Inversión en Infraestructura**

INVERSIÓN EN CABLEADO

Para realizar el cálculo de la inversión del Cableado las instalaciones del Hospital de Chancay y servicios Básicos de Salud, hemos creído conveniente segmentar (dividir) en Pabellones según las edificaciones con las que se cuenta:

- ✓ Pabellón A (Servicio Social, Consultorios de Cardiología y Archivo)
- ✓ Pabellón B (Servicio de Emergencia y Auditorio).
- ✓ Pabellón C (Servicio de Farmacia y Laboratorio).
- ✓ Pabellón D (Consultorios Externos, Hospitalización de Pediatría, Cirugía, Centro Quirúrgico).
- ✓ Pabellón E (Servicios Generales, Hospitalización de Materno, Medicina y Áreas Administrativas).
- ✓ Pabellón F (Nutrición, Dosis Unitaria, Almacén Medicamentos, Patrimonio y Biomédicos)

El cable a utilizarse será el Cable UTP NEWLINK NEW-9806342, CAT-7, conductor de cobre, cuyo diámetro de conductor 23AWG, 4 pares de hilos, color azul. El precio del metro de cable es actualmente de S/ 1.50 Nuevos Soles.

INVERSIÒN EN CABLE PRIMER PISO PABELLÓN "A"

CABLEADO PRIMER PISO PABELLÓN "A"		
PC	**CABLE (M)**	**COSTO**
A1 - PC01	9.50	14.25
A1 - PC02	17.50	26.25
A1 - PC03	9.00	13.50
A1 - PC04	10.80	16.20
A1 - PC05	12.40	18.60
A1 - PC06	12.00	18.00
A1 - PC07	14.80	22.20
A1 - PC08	20.50	30.75
A1 - PC09	11.80	17.70
A1 - PC10	17.30	25.95
A1 - PC11	22.60	33.90
A1 - PC12	25.00	37.50
TOTAL	**183.20**	**274.80**

Tabla Nº 08 INVERSIÓN EN CABLE PRIMER PISO PABELLÓN "A"
Fuente: Elaborada por los Autores

INVERSION EN OTROS MATERIALES PRIMER PISO PABELLÓN "A"

OTROS MATERIALES PRIMER PISO PABELLÓN "A"			
DESCRIPCIÓN	**CANTIDAD**	**PRECIO UNITARIO**	**SUB TOTAL**
Patch Cord	16	10.00	160.00
Jack RJ45	24	3.80	91.20
Cajas de Pared	11	2.00	22.00
Canaleta	100	5.00	500.00
Tapa Adosable	11	5.00	55.00
Cable Adicional	24	1.50	36.00
Otros			25.00
TOTAL			**889.20**

Tabla Nº 09 INVERSIÓN EN OTROS MATERIALES PRIMER PISO PABELLÓN "A"
Fuente: Elaborada por los Autores

INVERSIÒN EN CABLE SEGUNDO PISO PABELLÓN "A"

CABLEADO SEGUNDO PISO PABELLÓN "A"		
PC	**CABLE (M)**	**COSTO**
A2 - PC01	21.50	32.25
A2 - PC02	22.80	34.20
A2 - PC03	30.00	45.00
TOTAL	**74.30**	**111.45**

Tabla Nº 10 INVERSIÓN EN CABLE SEGUNDO PISO PABELLÓN "A"
Fuente: Elaborada por los Autores

INVERSIÒN EN OTROS MATERIALES SEGUNDO PISO PABELLÓN "A"

OTROS MATERIALES SEGUNDO PISO PABELLÓN "A"			
DESCRIPCIÓN	**CANTIDAD**	**PRECIO UNITARIO**	**SUB TOTAL**
Patch Cord	5	10.00	50.00
Jack RJ45	6	3.80	22.80
Cajas de Pared	3	2.00	6.00
Canaleta	40	5.00	200.00
Tapa Adosable	3	5.00	15.00
Cable Adicional	6	1.50	9.00
Otros			5.00
TOTAL			**307.80**

Tabla Nº 11 INVERSIÓN EN OTROS MATERIALES SEGUNDO PISO PABELLÓN "A"
Fuente: Elaborada por los Autores

INVERSIÒN EN CABLE PRIMER PISO PABELLÓN "B"

CABLEADO PRIMER PISO PABELLON "B"		
PC	**CABLE (M)**	**COSTO**
B1 - PC01	6.48	9.72
B1 - PC02	14.50	21.75
B1 - PC03	15.70	23.55
B1 - PC04	16.90	25.35
B1 - PC05	19.20	28.80
B1 - PC06	22.50	33.75
B1 - PC07	38.20	57.30
B1 - PC08	50.70	76.05
TOTAL	**184.18**	**276.27**

Tabla Nº 12 INVERSIÓN EN CABLE PRIMER PISO PABELLÓN "B"
Fuente: Elaborada por los Autores

INVERSIÒN EN OTROS MATERIALES PRIMER PISO PABELLÓN "B"

OTROS MATERIALES PRIMER PISO PABELLÓN "B"			
DESCRIPCIÓN	**CANTIDAD**	**PRECIO UNITARIO**	**SUB TOTAL**
Patch Cord	13	10.00	130.00
Jack RJ45	14	3.80	53.20
Cajas de Pared	7	2.00	14.00
Canaleta	97	5.00	485.00
Tapa Adosable	7	5.00	35.00
Cable Adicional	16	1.50	24.00
Otros			6.00
TOTAL			**747.20**

Tabla Nº 13 INVERSIÓN EN OTROS MATERIALES PRIMER PISO PABELLÓN "B"
Fuente: Elaborada por los Autores

INVERSIÒN EN CABLE SEGUNDO PISO PABELLÓN "B"

CABLEADO SEGUNDO PISO PABELLON "B"		
PC	**CABLE (M)**	**COSTO**
B2 - PC01	3.80	5.70
B2 - PC02	12.30	18.45
TOTAL	**16.10**	**24.15**

Tabla Nº 14 INVERSIÓN EN CABLE SEGUNDO PISO PABELLÓN "B"
Fuente: Elaborada por los Autores

INVERSIÒN EN OTROS MATERIALES SEGUNDO PISO PABELLÓN "B"

OTROS MATERIALES SEGUNDO PISO PABELLON "B"			
DESCRIPCIÓN	**CANTIDAD**	**PRECIO UNITARIO**	**SUB TOTAL**
Patch Cord	4	10.00	40.00
Jack RJ45	4	3.80	15.20
Cajas de Pared	2	2.00	4.00
Canaleta	8	5.00	40.00
Cable Adicional	4	1.50	6.00
Tapa Adosable	2	5.00	10.00
Otros			5.00
TOTAL			**120.20**

Tabla Nº 15 INVERSIÓN EN OTROS MATERIALES SEGUNDO PISO PABELLÓN "B"
Fuente: Elaborada por los Autores

INVERSIÒN EN CABLE PRIMER PISO PABELLÓN "C"

CABLEADO PRIMER PISO PABELLON "C"		
PC	**CABLE (M)**	**COSTO**
C1 - PC01	6.80	10.20
C1 - PC02	10.50	15.75
C1 - PC03	14.10	21.15
C1 - PC04	2.60	3.90
C1 - PC05	6.00	9.00
C1 - PC06	9.00	13.50
C1 - PC07	8.90	13.35
C1 - PC08	12.60	18.90
C1 - PC09	13.80	20.70
C1 – PC10	15.00	22.50
C1 – PC11	16.20	24.30
C1 – PC12	27.00	40.50
TOTAL	**142.50**	**213.75**

Tabla Nº 16 INVERSIÓN EN CABLE PRIMER PISO PABELLÓN "C"
Fuente: Elaborada por los Autores

INVERSIÒN EN OTROS MATERIALES PRIMER PISO PABELLÓN "C"

OTROS MATERIALES PRIMER PISO PABELLON "C"			
DESCRIPCIÓN	**CANTIDAD**	**PRECIO UNITARIO**	**SUB TOTAL**
Patch Cord	16	10.00	160.00
Jack RJ45	24	3.80	91.20
Cajas de Pared	11	2.00	22.00
Cable Adicional	24	1.50	36.00
Tapa Adosable	11	5.00	55.00
Canaleta	72	5.00	360.00
Otros			12.00
TOTAL			**736.20**

Tabla Nº 17 INVERSIÓN EN OTROS MATERIALES PRIMER PISO PABELLÓN "C"
Fuente: Elaborada por los Autores

INVERSIÒN EN CABLE SEGUNDO PISO PABELLÓN "C"

CABLEADO SEGUNDO PISO PABELLON "C"		
PC	**CABLE (M)**	**COSTO**
C2 - PC01	4.30	6.45
C2 - PC02	6.10	9.15
C2 - PC03	7.80	11.70
C2 - PC04	25.90	38.85
C2 - PC05	10.70	16.05
PRECIO	**54.80**	**82.20**

Tabla Nº 18 INVERSIÓN EN CABLE SEGUNDO PISO PABELLÓN "C"
Fuente: Elaborada por los Autores

INVERSIÒN EN OTROS MATERIALES SEGUNDO PISO PABELLÓN "C"

OTROS MATERIALES SEGUNDO PISO PABELLON "C"			
DESCRIPCIÓN	**CANTIDAD**	**PRECIO UNITARIO**	**SUB TOTAL**
Patch Cord	7	70.00	70.00
Jack RJ45	7	3.80	26.60
Cajas de Pared	5	2.00	10.00
Canaleta	28	5.00	140.00
Tapa Adosable	5	5.00	25.00
Cable Adicional	10	1.50	15.00
Otros			5.00
TOTAL			**291.60**

Tabla Nº 19 INVERSIÓN EN OTROS MATERIALES SEGUNDO PISO PABELLÓN "C"
Fuente: Elaborada por los Autores

INVERSIÒN EN CABLE PRIMER PISO PABELLON "D"

CABLEADO PRIMER PISO PABELLON "D"		
PC	**CABLE (M)**	**COSTO**
D1 - PC01	2.40	3.60
D1 - PC02	5.80	8.70
D1 - PC03	6.40	9.60
D1 - PC04	13.70	20.55
D1 - PC05	23.10	34.65
D1 - PC06	15.40	23.10
D1 - PC07	18.60	27.90
D1 - PC08	20.90	31.35
D1 - PC09	24.40	36.60
D1 – PC10	27.60	41.40
D1 – PC11	30.00	45.00
D1 – PC12	22.90	34.35
D1 - PC13	25.70	38.55
D1 – PC14	27.40	41.10
D1 – PC15	19.70	29.55
D1 – PC16	26.90	40.35
D1 – PC17	30.30	45.45
D1 – PC18	14.50	21.75
D1 – PC19	17.90	26.85
D1 – PC20	21.20	31.80
D1 – PC21	23.20	34.80
D1 – PC22	27.60	41.40
D1 – PC23	35.70	53.55
D1 – PC24	42.10	63.15
D1 – PC25	47.30	70.95
D1 – PC26	48.50	72.75
D1 – PC27	53.30	79.95
D1 – PC28	65.80	98.70
D1 – PC29	12.60	18.90
D1 – PC30	17.00	25.50
D1 – PC31	22.00	33.00
D1 – PC32	26.00	39.00
D1 – PC33	28.50	42.75
D1 – PC34	39.80	59.70
TOTAL	**884.20**	**1326.30**

Tabla Nº 20 INVERSIÓN EN CABLE PRIMER PISO PABELLÓN "D"
Fuente: Elaborada por los Autores

INVERSIÒN EN OTROS MATERIALES PRIMER PISO PABELLÓN "D"

OTROS MATERIALES PRIMER PISO PABELLON "D"			
DESCRIPCIÓN	**CANTIDAD**	**PRECIO UNITARIO**	**SUB TOTAL**
Patch Cord	56	10.00	560.00
Jack RJ45	78	3.80	296.40
Cajas de Pared	39	2.00	78.00
Canaleta	443	5.00	2215.00
Tapa Adosable	39	5.00	195.00
Cable Adicional	68	1.50	102.00
Otros			40.00
TOTAL			**3486.40**

Tabla Nº 21 INVERSIÓN EN OTROS MATERIALES PRIMER PISO PABELLÓN "D"
Fuente: Elaborada por los Autores

INVERSIÒN EN CABLE SEGUNDO PISO PABELLON "D"

CABLEADO SEGUNDO PISO PABELLON "D"		
PC	**CABLE (M)**	**COSTO**
D2 - PC01	23.00	34.50
D2 - PC02	24.60	36.90
D2 - PC03	26.60	39.90
D2 - PC04	2.60	3.90
D2 - PC05	5.70	8.55
D2 - PC06	8.70	13.05
D2 - PC07	13.10	19.65
D2 - PC08	15.40	23.10
D2 - PC09	4.40	6.60
D2 – PC10	6.90	10.35
D2 – PC11	8.80	13.20
D2 – PC12	11.40	17.10
D2 – PC13	13.40	20.10
D2 – PC14	4.30	6.45
D2 – PC15	13.80	20.70
D2 – PC16	19.60	29.40
D2 – PC17	21.60	32.40
D2 – PC18	9.90	14.85
D2 – PC19	15.40	23.10
D2 – PC20	18.70	28.05
D2 – PC21	20.80	31.20
D2 – PC22	15.00	22.50
D2 – PC23	18.80	28.20
D2 – PC24	35.60	53.40
D2 – PC25	38.00	57.00
D2 – PC26	10.50	15.75
TOTAL	**406.60**	**609.90**

Tabla Nº 22 INVERSIÓN EN CABLE SEGUNDO PISO PABELLÓN "D"
Fuente: Elaborada por los Autores

INVERSIÒN EN OTROS MATERIALES SEGUNDO PISO PABELLÓN "D"

OTROS MATERIALES SEGUNDO PISO PABELLON "D"			
DESCRIPCIÓN	**CANTIDAD**	**PRECIO UNITARIO**	**SUB TOTAL**
Patch Cord	36	10.00	360.00
Jack RJ45	52	3.80	197.60
Cajas de Pared	26	2.00	52.00
Canaleta	203	5.00	1015.00
Tapa Adosable	26	5.00	130.00
Cable Adicional	52	1.50	78.00
Otros			50.00
TOTAL			**1882.60**

Tabla Nº 23 INVERSIÓN EN OTROS MATERIALES SEGUNDO PISO PABELLÓN "D"
Fuente: Elaborada por los Autores

INVERSIÒN EN CABLE TERCER PISO PABELLON "D"

CABLEADO TERCER PISO PABELLON "D"		
PC	**CABLE (M)**	**COSTO**
D3 - PC01	14.40	21.60
D3 - PC02	21.80	32.70
D3 - PC03	11.80	17.70
D3 - PC04	18.00	27.00
D3 - PC05	15.70	23.55
D3 - PC06	32.40	48.60
D3 - PC07	36.60	54.90
TOTAL	**150.70**	**226.05**

Tabla Nº 24 INVERSIÓN EN CABLE TERCER PISO PABELLÓN "D"
Fuente: Elaborada por los Autores

INVERSIÒN EN OTROS MATERIALES TERCER PISO PABELLÓN "D"

OTROS MATERIALES TERCER PISO PABELLON "D"			
DESCRIPCIÓN	**CANTIDAD**	**PRECIO UNITARIO**	**SUB TOTAL**
Patch Cord	13	10.00	130.00
Jack RJ45	14	3.80	53.20
Cajas de Pared	7	2.00	14.00
Canaleta	76	5.00	380.00
Tapa Adosable	7	5.00	35.00
Cable Adicional	14	1.50	21.00
Otros			6.00
TOTAL			**639.20**

Tabla Nº 25 INVERSIÓN EN OTROS MATERIALES TERCER PISO PABELLÓN "D"
Fuente: Elaborada por los Autores

INVERSIÒN EN CABLE PRIMER PISO PABELLON "E"

CABLEADO PRIMER PISO PABELLON "E"		
PC	**CABLE (M)**	**COSTO**
E1 - PC01	34.00	51.00
E1 - PC02	26.30	39.45
E1 - PC03	16.80	25.20
E1 - PC04	27.90	41.85
E1 - PC05	26.20	39.30
E1 - PC06	24.30	36.45
E1 - PC07	11.80	17.70
E1 - PC08	13.40	20.10
E1 - PC09	14.46	21.69
E1 – PC10	20.60	30.90
E1 – PC11	23.40	35.10
E1 – PC12	26.80	40.20
TOTAL	**265.96**	**398.94**

Tabla Nº 26 INVERSIÓN EN CABLE PRIMER PISO PABELLÓN "E"
Fuente: Elaborada por los Autores

INVERSIÒN EN OTROS MATERIALES PRIMER PISO PABELLÓN "E"

OTROS MATERIALES PRIMER PISO PABELLON "E"			
DESCRIPCIÓN	**CANTIDAD**	**PRECIO UNITARIO**	**PRECIO**
Patch Cord	16	10.00	160.00
Jack RJ45	24	3.80	91.20
Cajas de Pared	11	2.00	22.00
Canaleta	133	5.00	665.00
Tapa Adosable	11	5.00	55.00
Cable Adicional	24	1.5	36.00
Otros			12.00
TOTAL			**1041.20**

Tabla Nº 27 INVERSIÓN EN OTROS MATERIALES PRIMER PISO PABELLÓN "E"
Fuente: Elaborada por los Autores

INVERSIÒN EN CABLE SEGUNDO PISO PABELLON "E"

CABLEADO SEGUNDO PISO PABELLON "E"		
PC	**CABLE (M)**	**COSTO**
E2 - PC01	20.40	30.60
E2 - PC02	18.40	27.60
E2 - PC03	3.90	5.85
E2 - PC04	2.80	4.20
E2 - PC05	1.60	2.40
E2 - PC06	1.80	2.70
E2 - PC07	2.80	4.20
E2 - PC08	3.80	5.70
E2 - PC09	5.00	7.50
E2 – PC10	2.60	3.90
E2 – PC11	3.60	5.40
E2 – PC12	4.60	6.90
E2 – PC13	5.60	8.40
E2 – PC14	6.60	9.90
E2 – PC15	8.20	12.30
E2 – PC16	10.90	16.35
E2 – PC17	12.10	18.15
E2 – PC18	13.10	19.65
E2 – PC19	4.50	6.75
E2 – PC20	6.80	10.20
E2 – PC21	11.60	17.40
E2 – PC22	16.20	24.30
E2 – PC23	19.30	28.95
E2 – PC24	5.50	8.25
E2 – PC25	6.40	9.60
E2 – PC26	7.30	10.95
TOTAL	**205.40**	**308.10**

Tabla Nº 28 INVERSIÓN EN CABLE SEGUNDO PISO PABELLÓN "E"
Fuente: Elaborada por los Autores

INVERSIÒN EN OTROS MATERIALES SEGUNDO PISO PABELLÓN "E"

OTROS MATERIALES SEGUNDO PISO PABELLON "E"			
DESCRIPCIÓN	**CANTIDAD**	**PRECIO UNITARIO**	**SUB TOTAL**
Patch Cord	36	10.00	360.00
Jack RJ45	52	3.80	197.60
Cajas de Pared	26	2.00	52.00
Canaleta	103	5.00	515.00
Tapa Adosable	26	5.00	13.00
Cable Adicional	52	1.50	78.00
Otros			5.00
TOTAL			**1220.60**

Tabla Nº 29 INVERSIÓN EN OTROS MATERIALES SEGUNDO PISO PABELLÓN "E"
Fuente: Elaborada por los Autores

INVERSIÒN EN CABLE TERCER PISO PABELLON "E"

CABLEADO TERCER PISO PABELLON "E"		
PC	**CABLE (M)**	**COSTO**
E3 - PC01	2.60	3.90
E3 - PC02	3.80	5.70
E3 - PC03	4.80	7.20
E3 - PC04	2.00	3.00
E3 - PC05	6.20	9.30
E3 - PC06	7.00	10.50
E3 - PC07	8.70	13.05
E3 - PC08	10.40	15.60
E3 - PC09	12.80	19.20
E3 – PC10	14.00	21.00
E3 – PC11	9.80	14.70
E3 – PC12	7.80	11.70
E3 – PC13	1.20	1.80
E3 – PC14	1.00	1.50
E3 – PC15	6.00	9.00
E3 – PC16	4.80	7.20
E3 – PC17	9.00	13.50
E3 – PC18	3.80	5.70
E3 – PC19	4.60	6.90
E3 – PC20	7.00	10.50
E3 – PC21	2.00	3.00
E3 – PC22	3.00	4.50
E3 - PC23	7.10	10.65
E3 – PC24	8.60	12.90
E3 – PC25	12.00	18.00
E3 – PC26	3.00	4.50
E3 – PC27	4.80	7.20
E3 – PC28	9.40	14.10
E3 – PC29	12.20	18.30
E3 – PC30	10.10	15.15
E3 – PC31	8.30	12.45
E3 – PC32	4.60	6.90
E3 – PC33	1.10	1.65
E3 – PC34	2.50	3.75
E3 - PC35	4.10	6.15
E3 – PC36	12.50	18.75
E3 – PC37	9.00	13.50
E3 – PC38	6.50	9.75
E3 – PC39	1.90	2.85
E3 – PC40	4.20	6.30
E3 – PC41	7.30	10.95
E3 – PC42	3.80	5.70
E3 - PC43	5.00	7.50
E3 – PC44	7.20	10.80
E3 – PC45	8.40	12.60
E3 – PC46	7.90	11.85
E3 – PC47	9.90	14.85
TOTAL	**303.70**	**455.55**

Tabla Nº 30 INVERSIÓN EN CABLE TERCER PISO PABELLÓN "E"
Fuente: Elaborada por los Autores

INVERSIÒN EN OTROS MATERIALES TERCER PISO PABELLÓN "E"

OTROS MATERIALES TERCER PISO PABELLON "E"			
DESCRIPCIÓN	**CANTIDAD**	**PRECIO UNITARIO**	**COSTO**
Patch Cord	61	10.00	610.00
Jack RJ45	122	3.80	463.60
Cajas de Pared	52	2.00	104.00
Canaleta	152	5.00	760.00
Tapa Adosable	52	5.00	260.00
Cable Adicional	94	1.50	141.00
Otros			6.00
TOTAL			**2344.60**

Tabla Nº 31 INVERSIÓN EN OTROS MATERIALES TERCER PISO PABELLÓN "E"
Fuente: Elaborada por los Autores

INVERSIÒN EN CABLE PRIMER PISO PABELLON "F"

CABLEADO PRIMER PISO PABELLON "F"		
PC	**CABLE (M)**	**PRECIO**
F1 - PC01	18.80	28.20
F1 - PC02	15.70	23.55
F1 - PC03	34.70	52.05
F1 - PC04	44.00	66.00
F1 - PC05	48.70	73.05
F1 - PC06	52.20	78.30
TOTAL	**214.10**	**321.15**

Tabla Nº 32 INVERSIÓN EN CABLE PRIMER PISO PABELLÓN "F"
Fuente: Elaborada por los Autores

INVERSIÒN EN OTROS MATERIALES PRIMER PISO PABELLÓN "F"

OTROS MATERIALES PRIMER PISO PABELLON "F"			
DESCRIPCIÓN	**CANTIDAD**	**PRECIO UNITARIO**	**COSTO**
Patch Cord	10	100.00	100.00
Jack RJ45	12	3.80	45.60
Cajas de Pared	10	2.00	20.00
Canaleta	108	5.00	540.00
Tapa Adosable	10	5.00	50.00
Cable Adicional	12	1.50	18.00
Otros			6.00
TOTAL			**759.60**

Tabla Nº 33 INVERSIÓN EN OTROS MATERIALES PRIMER PISO PABELLÓN "F"
Fuente: Elaborada por los Autores

INVENSION EN CABLE

INVENSION TOTAL EN CABLE		
DESCRIPCIÓN		**COSTO**
Inversión en Cable Pabellón "A" 1° Piso	274.80	286.25
Inversión en Cable Pabellón "A" 2° Piso	11.45	
Inversión en Cable Pabellón "B" 1° Piso	276.27	300.42
Inversión en Cable Pabellón "B" 2° Piso	24.15	
Inversión en Cable Pabellón "C" 1° Piso	213.75	295.95
Inversión en Cable Pabellón "C" 2° Piso	82.20	
Inversión en Cable Pabellón "D" 1° Piso	1326.30	2162.25
Inversión en Cable Pabellón "D" 2° Piso	609.90	
Inversión en Cable Pabellón "D" 3° Piso	226.05	
Inversión en Cable Pabellón "E" 1° Piso	398.94	1162.59
Inversión en Cable Pabellón "E" 2° Piso	308.10	
Inversión en Cable Pabellón "E" 3° Piso	455.55	
Inversión en Cable Pabellón "F" 1° Piso	321.15	321.15
TOTAL		**4528.61**

Tabla Nº 34 INVERSIÓN EN CABLE
Fuente: Elaborada por los Autores

INVENSION EN OTROS MATERIALES

INVERSIÓN EN OTROS MATERIALES		
DESCRIPCIÓN		**COSTO**
Inversión en Otros Materiales Pabellón "A" 1° Piso	889.20	1197.00
Inversión en Otros Materiales Pabellón "A" 2° Piso	307.80	
Inversión en Otros Materiales Pabellón "B" 1° Piso	747.20	867.40
Inversión en Otros Materiales Pabellón "B" 2° Piso	120.20	
Inversión en Otros Materiales Pabellón "C" 1° Piso	736.20	1027.80
Inversión en Otros Materiales Pabellón "C" 2° Piso	291.60	
Inversión en Otros Materiales Pabellón "D" 1° Piso	3486.40	6008.20
Inversión en Otros Materiales Pabellón "D" 2° Piso	1882.60	
Inversión en Otros Materiales Pabellón "D" 3° Piso	639.20	
Inversión en Otros Materiales Pabellón "E" 1° Piso	1041.20	4606.40
Inversión en Otros Materiales Pabellón "E" 2° Piso	1220.60	
Inversión en Otros Materiales Pabellón "E" 3° Piso	2344.60	
Inversión en Otros Materiales Pabellón "F" 1° Piso	759.60	759.60
TOTAL		**14466.40**

Tabla Nº 35 INVERSIÓN EN OTROS MATERIALES
Fuente: Elaborada por los Autores

INVERSIÓN EN EQUIPOS

EQUIPOS A ADQUIRIR			
DESCRIPCIÓN	**CANTIDAD**	**PRECIO UNITARIO**	**SUB TOTAL**
Servidor	01	17800.00	17800.00
UPS	12	1150.00	13800.00
Switch Core	01	8660.00	8660.00
Switch de Distribución	02	3060.00	6120.00
Switch de Borde	14	1650.00	23100.00
Gabinete para Servidores	01	4950.00	4950.00
Gabinetes para Switch	17	210.00	3570.00
Otros			3500.00
MONTO TOTAL			**81500.00**

Tabla Nº 36 INVERSIÓN EN EQUIPOS
Fuente: Elaborada por los Autores

INVERSIÓN EN MANO DE OBRA

MANO DE OBRA Y SERVICIOS			
DETALLE	**CANTIDAD**	**PRECIO UNITARIO**	**COSTO**
Jacks a Instalar	421	5.60	2357.00
Jacks Operativos	195	8.40	1638.00
Internet	3	190.00	570.00
TOTAL			**4565.00**

Tabla Nº 37 COSTO DE MANO DE OBRA
Fuente: Elaborada por los Autores

INVERSIÓN EN SOFTWARE

COSTO DE SOFTWARE			
DETALLE	**CANTIDAD**	**PRECIO UNITARIO**	**COSTO**
Windows Server 2012	1	2460.00	2460.00
TOTAL			**2460.00**

Tabla Nº 38 INVERSION EN SOFTWARE
Fuente: Elaborada por los Autores

RESUMEN TOTAL DE INVENSION

TOTAL DE INVERSIÓN REQUERIDA	
DESCRIPCIÓN	**COSTO**
Inversión en Cable	4528.61
Inversión en Otros Materiales	14466.40
Inversión en Equipos	81500.00
Inversión en Mano de Obra	4565.00
Inversión en Software	2460.00
MONTO TOTAL A INVERTIR	**107520.01**

Tabla Nº 39 RESUMEN TOTAL DE INVERSION
Fuente: Elaborada por los Autores

- **Análisis de Retorno**

  Para realizar el análisis de retorno de la inversión nos basamos, realmente, en que alguien en una posición muy alta sea capaz de conceptualizar y visualizar el valor de algo que no existe, donde se tiene que manejar cosas como el valor de proporcionar un mejor servicio a los clientes y el valor de hacer que las personas tomen mejores decisiones y más rápidas; en pocas palabras son elementos intangibles difíciles de cuantificar de manera monetaria; lo que podríamos lograr es elaborar un pequeño cuadro donde exprese los beneficios de como la elaboración más rápida de reportes, una mejor administración de la información, mejoran la toma de decisiones y usuarios más productivos.

COSTO	BENEFICIO
Presupuesto Inicial	Reducción de Burocracia
Costo de la Red	Reducción de Costos
Costo de Crecimiento	Mejorar los Servicios
Costo de Información	Menor Perdida de Datos
Costo de Servicio	Mayor Competitividad
Gasto de Consumo	Reducción de Tiempo
Gasto de Gestión	Mejor Administración
Seguridad	Menor fuga de conocimiento

Tabla Nº 40 ANALISIS DE RETORNO DE INVERSIÓN
Fuente: Elaborada por los Autores

Una vez visto los principales beneficios que nos ofrece contar con una Red de Datos podemos decir que calcular el Retorno de Inversión ROI (Return on Investment) es equivalente a medir la gestión del conocimiento del Hospital Chancay y Servicios Básicos de Salud, siendo el principal benéfico intangible y por lo tanto, no medible.

3.1.1.3. Objetivos de la Implementación de Red Informática Hospitalaria

3.1.1.3.1. Objetivos

Al iniciar este proyecto nuestro principal objetivo es el de plantear la:

Objetivo General

Implementación de una Red Informática Hospitalaria, usando, Metodología Top Down Network Design, Para el Hospital Chancay y servicios Básicos de Salud.

Objetivos Específicos

- Realizar el estudio de la metodología a emplearse en el desarrollo de este proyecto.
- Desarrollar el proyecto haciendo uso de la Metodología Top Down Network Design.
- Elaboración del esquema de cableado en toda la infraestructura del Hospital Chancay y Servicios Básicos de Salud.
- Identificar a las estaciones de trabajo para configurarlas en entorno de red.
- Compartir la información y los recursos de cada estación de trabajo.
- Permitir el acceso a las estaciones de trabajo de manera rápida y oportuna, mejorando los tiempos de respuesta.
- Administrar la Red de Datos con Windows Server 2012.
- Establecer políticas de seguridad con la finalidad de proteger la integridad física y lógica de la Red Informática Hospitalaria.

3.1.1.4.Objetivos Técnicos y sus Restricciones

3.1.1.4.1. Escalabilidad

Tomando en cuenta el crecimiento de la demanda (atenciones diarias), tomando como dato estadístico el mes de abril del 2014 eran en promedio de 560 atenciones diarias; el mes de abril del 2015 tenemos un

promedio de 637 atenciones diarias, un crecimiento de demanda del 13%, esta realidad conllevara a mayor uso de la red de datos proyectada, se cree conveniente tener en cuenta un 40% adicional de puntos operativos de acceso a la red (jacks operativos) y en un 40% de espacio en el tendido de canaletas; más aún sea considerado un 100% adicional de puntos muertos de acceso a la red (no cableado), que pueden entrar a operar en cuanto se considere necesario.

3.1.1.4.2. Disponibilidad

Al ser una red de datos de una institución hospitalaria, el tiempo operativo que se necesita tener la red es de 24 horas diarias y durante los 7 días de la semana, donde el paciente está dispuesto a esperar un máximo de 10 minutos, en base a estos datos calcularemos la Tasa de Disponibilidad de la Red:

Tiempo Ideal = 24 (horas/día) x 7 (dias/semana)
Tiempo Ideal = 168 (horas/semana) x 60 minutos
Tiempo Ideal = 10080

Tiempo Aceptable = Tiempo Ideal – Tasa de Perdida
Tiempo Aceptable = 10080 – 10
Tiempo Aceptable = 10070

Tasa de Disponibilidad (TD) = (TA/TI)*100
Tasa de Disponibilidad (TD) = (10070/10080)*100
Tasa de Disponibilidad (TD) = 99.90%

Tenemos una tasa alta de disponibilidad lo que nos indica que la red de datos funcionara adecuadamente.

3.1.1.4.3. Performance

La Implementación de la Red Informática Hospitalaria propone que la red tenga un buen desempeño o

rendimiento por lo escalable que podría ser nuestra red en el diseño propuesto, pero este rendimiento dependerá de algunos factores o parámetros definidos.

La monitorización permanente del performance nos permitirá evaluar el desempeño y la seguridad de la estructura de la red, en nuestro caso el monitoreo de performance será la medida de Latencia de la Red (que es el tiempo que tardan los paquetes de información en llegar de un punto A a un punto B).

La performance está ligada a medir el desempeño de la red y nuestra red al no estar aún instalada solo hago mención de cómo medir la performance de la red que se está implementando.

3.1.1.4.4. Seguridad

La seguridad de la red se basa en un conjunto de barreras que protegen la información del Hospital de Chancay y Servicios Básicos de Salud, utilizando diversas herramientas que si falla una, se mantendrán otras que protegerán la información y los datos de una gran variedad de ataques, la información que se maneja es confidencial por ello los datos serán manejados solo por personas autorizadas por el administrador de la red; el mismo que se encargara de dar los privilegios a los diferentes usuarios para poder acceder a la información de la red. La institución cuenta con servicio de Internet por ello es de vital importancia protegerse de los ataques, tanto externos como internos.

La medida principal es mantener a los servidores en oficina de acceso restringido con la finalidad de resguardad su integridad, en cuanto a software de seguridad se contará con software antivirus (Sophos Antivirus) el mismo que fue adquirido por la institución

por un periodo de tres años con la posibilidad de incrementar este contrato a cinco años o más.

Para la adquisición del antivirus se empleó la Guía de Evaluación de Software en la Administración Publica aprobado por Resolución Ministerial N° 139-2004-PCM

Los parámetros (métricas) están dados de acuerdo a los criterios de requerimiento del Hospital Chancay y Servicios Básicos de Salud y son lo siguientes.

ÍTEM	ATRIBUTO	ATRIBUTO TÉCNICAS
		ANTIVIRUS CORPORATIVO La entidad solicita una solución de software de un solo fabricante, una sola consola y un único agente que cubra con los requerimientos técnicos mínimos solicitados:
ATRIBUTOS INTERNOS		
1	Sistemas Operativos de Estaciones de Trabajo (en versiones de 32/64 bits)	• Microsoft Windows 2000 Professional. • Microsoft Windows XP Professional. • Microsoft Windows Vista. • Microsoft Windows 7. • Microsoft Windows 8.
2	Sistemas Operativos de Servidores de Red (en versiones de 32/64 bits)	• Microsoft Windows 2000 Server • Microsoft Windows 2003 Sever • Microsoft Windows 2008 Server • Microsoft Windows 2012 Server • Red Hat Enterprise 4/5 • SUSE Enterprise Linux 9/10
3	Protección y defensa frente a malware en portátiles, computadoras de escritorio y servidores	• La solución de seguridad para estaciones y servidores es de tipo integrada; es decir incluye un único agente que brinda protección frente a virus, spyware, adware, rootkits, comportamientos sospechosos, filtrado de seguridad URL, detección Web de ataques de scripts maliciosos y aplicaciones potencialmente peligrosas en todos los protocolos de la red. • La solución cuenta con una cuarentena de usuario final

		que permita controlar y/o autorizar el uso de ciertas aplicaciones no deseadas. • La solución tiene versiones para Linux el cual cuenta con un módulo de escaneo de archivos de alto rendimiento, estabilidad y eficacia el cual debe permitir el escaneado en acceso, en demanda y programado de unidades locales, extraíbles y compartidas (como NFS y Samba), y otros sistemas de archivos. La versión para Linux debe poder ser configurada y administrada desde la consola central. • La solución puede actualizarse (durante 12 meses) desde una consola centralizada y desde la web del fabricante simultáneamente con el fin de asegurar una completa protección aun cuando la consola central no se encuentre activa. • La solución de seguridad instalada en todas las plataformas requeridas debe notificar los eventos de virus, spyware, adware, aplicaciones no deseadas, intrusiones, cambios en la configuración del cliente de seguridad a la consola central. • El sistema de filtrado URL y el de detección Web de Ataques de Script maliciosos debe denegar el acceso al sitio y deber mostrar una página HTML de bloqueo en el navegador de internet (IE, Mozilla, Chrome, Opera, etc.) donde se indique el usuario y la razón por la que no ha podido acceder a dicha página. • La solución deberá incluir un sistema para el Control de acceso web a sitios inapropiados. Este sistema deberá estar integrado al agente antimalware y deben permitir notificar o bloquear el acceso a sitio web en base a categorías. • La solución para el Control de acceso a web a sitios inapropiados deberá incluir al menos 10 categorías de sitios web entre las que se encuentren principalmente Actividad Criminal, Armas, Contenido Ofensivo,

		Contenido para adultos, Juegos de Azar, Robo de Datos y Fraude, Programas Espía, Proxys anónimos, Violencia y Hackers. • La solución permite la creación de CD, DVD o USB Booteables de emergencia mediante imágenes .ISO u otro formato de grabación de medios para la recuperación y limpieza de equipos infectados. La creación de dichas imágenes no deberá depender de productos de terceros ni requerir licenciamiento de productos adicionales al del propio fabricante.
4	Firewall	• La solución incluye un firewall personal del mismo fabricante. • El firewall personal es administrado centralizadamente desde la consola de gestión. • El firewall permitirá bloquear, autorizar aplicaciones y puertos específicos tanto local como centralizadamente. • El firewall deberá permitir trabajar en modo oculto. • El firewall deberá permitir ser configurado en modo control o auditor con la finalidad de recoger información de aplicaciones, puertos y protocolos usados en el equipo de la red y que permite crear políticas de seguridad en forma rápida y simple. • El firewall deberá reconfigurarse automáticamente con otro tipo de política de protección de acuerdo a la ubicación donde se encuentre. Esta política deberá realizarse mediante la detección de la MAC Address del Gateway de Red o del DNS.
5	El sistema de prevención de intrusos de Host – HIPS y detección de desbordamiento de buffers (BOPS – Buffer Overflow Protection System)	• La solución incluye una tecnología de detección de intrusos de host (HIPS) incorporado en el agente antimalware que brinde protección en acceso. • La solución deberá incluir una tecnología para la detección de intentos de desbordamiento de buffers (SOPS – Buffer Overflow Protection System) incorporado en el agente antimalware. • La solución deberá contar con una tecnología de

		prevención y detección de intrusos que detecta malware antes de su ejecución (pre-execution) y en ejecución (on-execution). • El sistema HIPS está integrado en el agente antimalware y permite configurar en modo bloqueo de procesos o en modo solo alerta. • El sistema HIPS no requiere ejecutar o instalar agentes o programas adicionales al motor antimalware ni ejecutarse en forma programada para la prevención y/o detección de intrusos de hosts.
6	Control de dispositivos	• Para la protección contra el malware en dispositivos externos, la solución incluye un sistema de control de dispositivos que detecta el uso de dispositivos USB, grabadores de CD/DVD, floppy disk, lectores de CD/DVD, HDD externos y dispositivos wireless. • El sistema de control de dispositivos cuenta con opciones para permitir, bloquear, alertar y configurar en modo solo lectura los dispositivos indicados. • El sistema de control de dispositivos permite la autorización de dispositivos específicos (basados en modelos específicos o marcas) la utilización de dispositivos cifrados e incluso contra el uso de interfaces de red como los módems convencionales y los módems 3G. • El sistema de control de dispositivos estarán integrados en el agente antimalware, es decir no requiere la instalación de programas adicionales en los equipos. • El sistema de control de dispositivos cuenta con opciones para evitar el modo "puente-de-red" para dispositivos de red wireless y módems, incluyendo los 3G, que permita evitar que los usuarios incumplan las políticas corporativas de acceso a internet.
7	Protección contra ataques de día cero	• La solución deberá contar con tecnologías de detección proactiva de amenazas conocidas y basadas en la nube (in the cloud) del mismo fabricante.

		• La solución ofertada deberá ofrecer una rápida y eficaz detección de archivos sospechosos mediante la comprobación instantánea de archivos sospechosos en la nube. • El sistema de protección de filtrado URL realizando comprobaciones de direcciones web sospechosos (hackeadas, que albergan malware, etc.) en forma automática hacia la nube (base de datos del fabricante) para una rápida y efectiva protección contra este tipo de amenazas.
8	Seguridad	• La solución debe ser capaz de evitar que sus procesos, servicios, archivos o archivos de registro puedan ser detenidos, deshabilitados, eliminados o modificados para de esta manera garantizar su funcionamiento ante cualquier tipo de ataque de virus. • La solución deberá contar con medidas de seguridad para que el usuario de la estación de trabajo, sea este el administrador de la red o la PC no deje sin efecto políticas de seguridad corporativas. • La desinstalación del módulo o cliente y sus componentes debe estar protegido con una clave de seguridad asignada por el administrador de la solución. Esta clave puede ser configurada para un grupo específico o todos los equipos en la red. • La seguridad de la solución deberá integrarse al directorio activo de la red y con el sistema de grupos de Microsoft para una mejor y efectiva protección. • El usuario no podrá realizar una configuración particular a menos que el administrador de la red le otorgue privilegios ya sea localmente o mediante la integración con el Directorio Activo de Microsoft. • La solución deberá contar con un sistema de administración de parches de múltiples fabricantes como Microsoft, Adobe, Mozilla, Apple y Citrix que permita conocer la lista de parches que no se han aplicado en los

		equipos administrados. • La solución de administración de parches deberá mostrar además la lista de vulnerabilidades que son aprovechadas por atacantes o malwares específicos. • Cualquier intento de vulneración de las características de seguridad deberá ser reportado a la consola de gestión centralizada.
9	Control de aplicaciones	• La solución debe contar con un sistema que permita controlar el uso de determinados tipos de aplicaciones en los equipos de la red. • El sistema de control de aplicaciones debe permitir controlar y bloquear el uso de aplicaciones que causan un impacto negativo en el trabajo de los usuarios, en el uso del ancho de banda en la red y el incumplimiento de políticas corporativas las cuales se encuentran agrupadas o categorizadas por tipo de programas; al menos como Programas P2P, Mensajería Instantánea, Proxys, Herramientas de hacking, Control Remoto de Equipos y Máquinas Virtuales. • La solución debe permitir limpiar y desinstalar remotamente las principales aplicaciones P2P controlada (Peer-to-peer) desde la consola de administración. • La entidad puede solicitar al fabricante y/o postor la inclusión de nuevos programas y/o aplicaciones que considere que deben bloquearse y que se requiera incluir en dicho sistema.
10	Control de acceso a la red	• La solución debe contar con la capacidad de integración con las políticas de seguridad de Cisco NAC. • La solución incorpora un agente de control de acceso a la Red del mismo fabricante. Este agente también conocido como "Agente NAC" puede mantener todos los equipos sean estos administrados, no administrados o invitados (equipos que se conectan a la red esporádicamente) en buen estado y con la protección

		antivirus actualizado, así mismo, deberá asegurar que se corrijan las vulnerabilidades encontradas. • El agente de control de acceso a la red permitirá establecer políticas para verificar al menos: ✓ Si el antivirus está activo y actualizado: ✓ Si el equipo cliente tiene activado el sistema de actualización de parches del sistema operativo. ✓ Si el cliente firewall está activo. ✓ Si el equipo tiene activado algún sistema de encriptación de información. • La solución NAC permite integrarse con el sistema DHCP de Microsoft para establecer políticas de control de acceso a la red.
11	Control de fuga de información (DLP)	• La solución incluye un sistema para el control de fuga de datos conocido como DLP. • El sistema de control de fuga de datos permite controlar, restringir y auditar la información que es copiada o enviada fuera de la red corporativa mediante el uso de dispositivos externos como USB, Internet, Correo Electrónico y Mensajería Instantánea. • El sistema de control de fuga de datos debe ser del mismo fabricante y deberá poder controlar la información saliente por tipo de contenido y tipo de archivo. • El sistema de control de fuga de datos incluirá listas de control pre-configuradas para la elaboración rápida de políticas corporativas. • La administración de este sistema se realiza desde la consola de administración central de la solución de seguridad antimalware.
12	Encriptación de discos duro	• La solución incluye un sistema de encriptación de archivos y carpetas en el explorador de Windows, así como la encriptación de archivos adjuntos.
ATRIBUTOS EXTERNOS		
13	Instalación y despliegue	• La instalación del software a las computadoras de los

	del software	usuarios se puede realizar mediante: o Instalación automática, mediante la sincronización con el Directorio Activo de Microsoft. o Instalación remota desde la consola de administración o Instalación manual mediante CD. • El instalador debe incorporar un Sistema de Eliminación de Software de Seguridad de Terceros (agentes antimalware y firewall) que permita desinstalar automáticamente otro productos de seguridad sin requerir realizar manualmente dicho proceso con el fin de optimizar el proceso de despliegue de la solución. • La solución permite crear a pedido de la institución instaladores que permitan el despliegue del producto mediante CD o vía Web. Estos instaladores pueden ser personalizados y permitan por ejemplo contener información relativa a la propiedad de la institución. • El Sistema de Eliminación de Software de Seguridad de Terceros debe ser del mismo fabricante. • El Sistema de Eliminación de Software de Seguridad de Terceros está incorporado en el sistema de instalación del agente antimalware es decir puede activarse o desactivarse al momento del despliegue de la solución. • El instalador permite la instalación del agente de Control de Acceso a la Red durante el despliegue de la solución.
14	Actualización de firma y nueva versiones de producto	• Las actualizaciones se realizaran automáticamente (programadas) y manualmente del fichero de firmas de virus y del motor de escaneado del malware en los servidores y estaciones de trabajo desde internet. • La actualización de firmas automáticas deberá realizarse cada 30 minutos o menos. • El tamaño de las actualizaciones de firmas de virus es pequeño de tal modo que no tenga un impacto negativo en el tráfico de la red (máximo 100 Kb por

		actualización). • La actualización de nuevas versiones del producto se pueden realizar automáticamente y no requiere la desinstalación y/o reinstalación de algún componente previo, estas actualizaciones son incrementales. • La solución permite programar la comprobación de nuevas versiones de la solución al menos 12 horas y programar la instalación automática de ellas en horas de menos tráfico de red. Para este fin, la solución debe contar con opciones para la programación del horario por día y hora especificada.
15	Consola de administración	• La solución deberá contar con una consola de administración centralizada desde donde pueda administrar y controlar todos los componentes de la solución ofertada en forma centralizada y distribuida. • La herramienta deberá tener incluido la capacidad de gestión de las políticas de control de acceso a la red sin requerir instalar productos adicionales. • La consola debe permitir la administración simultáneamente de equipos y servidores Windows, Linux y Mac. • La herramienta deberá ser escalable y debe permitir la administración de complejas redes, permitiendo la administración centralizada y distribuida de más de 500 equipos desde una sola consola • La consola debe sincronizarse con el Directorio Activo para la instalación automática de la solución de seguridad en los equipos. • La administración deberá estar basada en políticas y deberá contener al menos políticas para Actualización, Opciones Antimalware, HIPS, Control de Aplicaciones, Control de Dispositivos, Control de Fuga de Datos, NAC y Firewall. • Cualquier cambio en las políticas deberán desplegarse automáticamente a los equipos sean estos Windows,

		Linux o Mac. • Debe contar con filtros de control que permitan detectar de forma rápida los equipos no protegidos o los que no cumplen con las políticas de seguridad. • El administrador deberá poder crear políticas desde la consola para evitar el uso de aplicaciones no deseadas así como eliminar, autorizar y limpiar las mismas en los clientes. • La consola deberá poder utilizar al menos 3 tipos diferentes de mecanismos para detectar equipos en la red (TCP/IP, Active Directory y otros) • Se deberá poder crear políticas de actualización para equipos con conexión lenta pudiendo limitarse el ancho de banda utilizado durante las actualizaciones. • La consola deberá ser capaz de determinar equipos que cumplan con las políticas centrales y/o fueron modificadas localmente. Eventualmente deberá poder "forzar" a los equipos a cumplir con las políticas centrales con tan solo un Click. • La consola deberá contar con un sistema de reportes y mecanismos de notificación de eventos vía correo electrónico. • La consola deberá almacenar un histórico de eventos de cada equipo administrado pudiéndose conocer también el nombre del equipo, descripción, SO, Service Pack, IP, Grupo, última actualización, eventos de error, etc. desde la consola. • La consola deberá administrar el sistema de prevención contra intrusiones de host (HIPS) y el sistema de protección contra desbordamiento de buffers (BOPS) como políticas de seguridad. • La consola deberá permitir delegar la administración basada en roles y ubicaciones geográficas, permitiendo de esta forma delegar la administración por áreas geográficas manteniendo de esta forma el control de la

		seguridad corporativa. • El sistema para la delegación de roles deberá contener un administrador de permisos, pudiendo crear distintos perfiles con permisos particulares para cada administrador. • La consola deberá permitir crear excepciones para el control de dispositivos (control total, solo lectura y bloqueo), filtrado URL (por nombre, IP's o rango de IP's) para un grupo particular de equipos o toda la red. • Debe incluir la capacidad para la desinfección y limpieza remota de adware/aplicaciones potencialmente peligrosas, así como también de virus, troyanos, gusanos, rootkits y spyware. • La consola deberá permitir acceder a un sistema de visualización y búsqueda de eventos para las políticas de control de aplicaciones, dispositivos, fuga de datos y firewall. • La consola deberá tener integrada un visor de parches con la finalidad de que el administrador de la solución pueda verificar la lista de parches que faltan aplicar en los equipos administrados así como conocer la cantidad de equipos a los cuales falta aplicar un determinado parche. • La consola deberá tener integrado un visor para el control web el cual deberá permitir visualizar los sitios web a los cuales los usuarios han intentado ingresar en contra las políticas de seguridad de la empresa. • Desde el sistema de visualización y búsqueda de eventos se deberá poder generar excepciones a las políticas de seguridad y control previamente establecidas.
16	Administración de licencias	• La solución debe permitir el manejo flexible de las licencias, de manera que puedan ser reasignadas en caso se cambie de equipo. • La licencia del software propuesto deberá permitir el uso de la solución antivirus en una PC de casa de los

		trabajadores de la institución hasta un máximo del número de licencias adquiridas.
ATRIBUTOS DE USO		
17	Alertas y Reportes	• La solución deberá ser capaz de notificar los eventos de virus a través de diferentes medios (correo electrónico, alerta de registros, etc.) • La solución deberá generar reportes gráficos, imprimibles y exportables de la cobertura de versiones, actualizaciones e infecciones. • La solución deberá contener un sistema de reportes que permitir ver el estado de la protección de la red en línea. Este sistema debe mostrar en tiempo real lo que está ocurriendo en la red. • La solución deberá permitir acceder a reportes basados en el usuario que permita conocer rápidamente el cumplimiento de políticas por cada usuario. • La solución deberá incorporar un sistema de reportes que permita programar la creación y envió de reportes en formato PDF y HTML vía correo en una determinada hora y fecha de día. • La solución deberá incorporar un mecanismo de conexión con la base de datos para la creación de reportes personalizados y directos a la base de datos.
18	Soporte técnico	• La solución debe contar con soporte técnico 24/7 escalable hacia la casa matriz incluido en la licencia y en español. • El postor deberá contar con al menos 02 especialistas certificados por el fabricante en las áreas de antivirus y control de acceso a la red. • El postor capacitara a un mínimo de 05 horas en las herramientas administrativas del software dictado y certificado por el postor, para 5 personas como mínimo. • El postor deberá brindar el servicio de instalación, configuración y pruebas del aplicativo antivirus en el 50% de equipos de la institución.

		• El postor tendrá 05 días calendario para realizar la implementación del software señalado líneas arriba contabilizados desde el día siguiente de colocada la orden de compra.

Tabla Nº 41 PARAMETROS DE SEGURIDAD
Fuente: Recuperado de: MINSA (2013), Unidad de Estadística e Informática

3.1.1.4.5. Usabilidad

La facilidad de uso así como la familiarización de los usuarios con la red no tendrá mayor impacto ya que el software que se encuentra en uso, será el mismo que seguirán usando una vez instalada la red, si existiera renovación de software que modifique el entorno de trabajo el usuario deberá recibir capacitación, por ello el efecto de contar con una nueva red informática será positivo para la institución.

3.1.1.4.6. Adaptabilidad

La adaptabilidad al crecimiento que va de la mano de los avances tecnológicos está plenamente garantizado desde el momento que hacemos uso de la metodología Top Down Network Design, la que nos permite sentar bases de estudio constante e investigación permanente; garantía de irrefutable crecimiento institucional. La Red informática Hospitalaria se adaptara a los nuevos cambios tecnológicos y a nuevas soluciones integrales, sin sufrir mayores cambios en su entorno de trabajo. Cuya restricción se encontraría en los dispositivos de interconexión que debido al avance tecnológico sufran drásticos cambios en los estándares protocolares.

3.1.1.4.7. Accesibilidad

El acceso al uso de la red estará únicamente normado y regulado de acuerdo a las políticas de seguridad y los niveles de acceso de los usuarios. La accesibilidad a la

red será administrada única y exclusivamente por el Administrador de la Red.

3.1.1.5.Caracterización de la Red Existente

La red informática existente en el Hospital de Chancay y Servicios Básicos de Salud, consta de dos Servidores HP ProLiant Server ML350 G6 Quad Core Intel Xeon 5606 G6 los mismos que tienen una antigüedad de 6 años, la cantidad de switchs, es de 8, que fueron adquiriendo de acuerdo a las necesidades presentadas, cuenta con tres modem para el servicio de internet (Área Administrativa, SIS, Cuerpo Médico), el cableado de su red de datos, es una red que se ha ido adaptando a través del tiempo y de acuerdo a las necesidades sin contar con un plan de crecimiento proyectado ni sujeta a ninguna norma, en muchos de los casos esta red tiene una antigüedad que supera los 10 años, donde se puede percibir cables a la intemperie y sin ninguna protección o aislamiento, cuando se presentan fallas de caídas de red, en la mayoría de casos son difíciles de detectar el lugar donde se origina la falla; se observa en los terminales RJ45 desgastados y no se ha respetado las normas técnicas, por consiguiente no existe una buena conductividad; se cuenta con un total de 169 estaciones de trabajo de las cuales 37 son laptop y 132 computadores sobremesa, de estos equipos solo 67 se encuentran interconectadas.

Se observa que los equipos no se encuentran protegidos ya que la red eléctrica es compartida con las iluminarias y tomas de corriente, donde se alimenta equipos biomédicos de alta frecuencia en general, a pesar que algunos computadores cuentan con estabilizadores

UNIDAD / DEPARTAMENTO	N° PC	TIPO		MEMORIA	MODELO
		LAP.	PC.		
Órgano de Control Institucional	1		x	2 GB	CORE I3
	1		x	3 GB	CORE I3
	1	x		1 GB	CORE 2 DUO
	1		x	1 GB	CORE 2 DUO
	1		x	1 GB	CORE 2 DUO
Dirección Ejecutiva	1	x		1 GB	CORE 2 DUO
	1		x	2 GB	CORE I5
	1	x		2 GB	CORE I3
	1	x		2 GB	CORE I3
	1	x		2 GB	CORE 2 DUO
	1	x		2 GB	CORE I3
	1		x	1 GB	CORE 2 DUO
	1		x	512 MB	CELERON
	1		x	1 GB	CELERON
Planeamiento Estratégico	1		x	512 MB	CORE 2 DUO
	1		x	2 GB	CORE I5
	1		x	2 GB	CORE 2 DUO
	1		x	512 MB	CELERON
	1		x	1 GB	CORE2 DUO
	1	x	x	4 GB	CORE2 DUO
Epidemiología y Salud Ambiental	1	x		2 GB	DUAL CORE
	1	x		2 GB	CORE I3
	1		x	1 GB	DUALCORE
	1		x	4 GB	CORE I3
	1		x	512 MB	CORE 2 DUO
	1		x	512 MB	CORE 2 DUO
Gestión de la Calidad	1	x		2 GB	DUAL CORE
	1	x		2 GB	DUAL CORE
	1		x	2 GB	CORE 2 DUO
	1		x	512 MB	CELERON
	1		x	1 GB	CORE2 DUO
	1		x	2 GB	DUAL CORE
	1		x	2 GB	CORE 2 DUO
	1		x	2 GB	CORE I3
	1		x	1 GB	DUALCORE
Unidad de Personal	1	x		2 GB	CORE 2 DUO
	1		x	512 MB	CELERON
	1		x	2 GB	CORE 2DUO
	1		x	2 GB	CORE I3
	1		x	1 GB	CORE 2DUO
	1		x	2 GB	CORE 2DUO
	1		x	1 GB	CORE 2DUO
	1		x	512 MB	CELERON
	1		x	512 MB	CELERON
Unidad de Economía	1	x		2 GB	DUAL CORE
	1		x	2 GB	PENTIUM®
	1		x	1 GB	CORE 2DUO
	1		x	2 GB	CORE 2DUO

	1		x	512 MB	PENTIUM4
	1		x	512 MB	CELERON ®
	1		x	1 GB	CORE 2DUO
	1		x	2 GB	CORE 2DUO
	1		x	512 MB	CELERON
	1		x	1 GB	CORE2 DUO
	1		x	2 GB	DUAL CORE
	1		x	2 GB	DUAL CORE
	1		x	2 GB	DUAL CORE
	1		x	2 GB	DUAL CORE
	1		x	1 GB	CORE2 DUO
	1		x	512 MB	PENTIUM4
Unidad de Logística	1		x	2 GB	CORE I3
	1	x		2 GB	DUAL CORE
	1	x		2 GB	CELERON®
	1		x	2 GB	CORE I3
	1		x	4 GB	CORE I5
	1		x	2 GB	CORE 2DUO
	1		x	2 GB	CORE 2DUO
	1		x	2 GB	CORE 2DUO
	1		x	4 GB	CORE I3
	1		x	4 GB	CORE I3
	1		x	4 GB	CORE 2DUO
	1		x	2 GB	DUAL CORE
	1		x	1 GB	PENTIUM ®
	1		x	2 GB	DUAL CORE
	1		x	512 MB	PENTIUM ®
Servicios Generales	1		x	2 GB	CORE I3
	1		x	2 GB	CORE I3
	1		x	1 GB	CORE 2 DUO
	1		x	1 GB	CORE 2 DUO
Estadística e Informática	1		x	4 GB	CORE 3
	1		x	1 GB	CORE 2 DUO
	1		x	4 GB	CORE I3
	1		x	2 GB	CORE 2 DUO
	1		x	1 GB	CORE 2 DUO
	1		x	4 GB	CORE I3
	1		x	4 GB	CORE I3
	1		x	4 GB	CORE I3
	1		x	2 GB	CORE 2DUO
	1		x	2 GB	DUAL CORE
	1		x	1 GB	DUAL CORE
	1		x	2 GB	CORE 2 DUO
	1		x	4 GB	CORE I5
	1		x	4 GB	CORE I5
	1	x		2 GB	CORE 2 DUO
	1	x		2 GB	CORE 2 DUO
	1		x	1 GB	CORE 2 DUO
	1		x	1 GB	CORE 2 DUO
Apoyo a la Docencia e Investigación	1	x		2 GB	CORE I3
	1	x		2 GB	CORE I3
	1		x	2 GB	CORE 2 DUO

Unidad de Seguros	1	x		2 GB	CORE I3
	1		x	4 GB	CORE I3
	1	x		2 GB	CORE I3
	1		x	4 GB	CORE I3
	1		x	4 GB	CORE I3
	1		x	4 GB	CORE I3
	1		x	2 GB	CORE 2 DUO
	1		x	2 GB	CORE 2 DUO
	1		x	1 GB	PENTIUM
	1		x	1 GB	PENTIUM
	1		x	512 MB	PENTIUM
	1	x		2 GB	CORE I3
Consulta Externa y Hospitalización	1		x	2 GB	CORE 2 DUO
	1	x		2 GB	CORE I3
	1	x		2 GB	CORE I3
	1		x	2 GB	CORE 2 DUO
Departamento de Medicina	1	x		2 GB	CORE I3
Departamento de Cirugía	1	x		2 GB	CORE I3
Departamento de Pediatría	1	x		2 GB	CORE 2 DUO
	1		x	2 GB	CORE I3
Dep. de Gineco Obstetricia	1	x		2 GB	CORE I3
	1		x	4 GB	CORE I5
	1		x	4 GB	CORE I5
	1	x		2 GB	CORE 2 DUO
	1		x	2 GB	CORE I3
	1		x	1 GB	CORE 2 DUO
	1		x	1 GB	CORE 2 DUO
	1		x	512 MB	PENTIUM
Departamento de Enfermería	1		x	4 GB	CORE I3
	1		x	512 MB	CELERON ®
Dep. de Odonto Estomatología	1		x	512 MB	PENTIUM
	1	x		1 GB	CORE 2 DUO
	1		x	2 GB	CORE I3
Emergencia y Cuidados Críticos	1	x		2 GB	CORE I3
	1	x		2 GB	DUAL CORE
	1	x		2 GB	DUAL CORE
	1		x	2 GB	CORE I3
Anestesiología y Centro Quirúrgico	1		x	1 GB	CORE 2 DUO
	1		x	2 GB	CORE I3
	1		x	2 GB	CORE I3
Patología Clínica y Anatomía Pat.	1		x	1 GB	DUAL CORE
	1		x	2 GB	CORE 2 DUO
	1		x	4 GB	CORE I5
	1		x	2 GB	CORE I3
	1		x	2 GB	CORE 2 DUO
Dep. Diagnóstico por Imágenes	1		x	4 GB	CORE I5
	1		x	2 GB	CORE I3
Dp. Apoyo al Tratamiento	1		x	2 GB	CORE I3
	1		x	2 GB	CORE 2 DUO
	1	x		2 GB	CORE 2 DUO
	1		x	2 GB	DUAL CORE
	1	x		2 GB	CORE 2 DUO

	1		x	512 MB	PENTIUM
	1		x	1 GB	PENTIUM
	1	x		2 GB	CORE 2 DUO
	1		x	1 GB	DUAL CORE
	1		x	512 MB	PENTIUM
	1		x	1 GB	CORE 2 DUO
	1		x	2 GB	CORE 2 DUO
	1		x	2 GB	DUAL CORE
	1		x	2 GB	CORE I3
	1	x		2 GB	CORE 2 DUO
	1	x		2 GB	CORE 2 DUO
Cuerpo Médico	1		x	4 GB	CORE I3
	1		x	4 GB	CORE I5
Admisión	1		x	4 GB	CORE I3
	1		x	4 GB	CORE I3
	1		x	4 GB	CORE I3
	1		x	4 GB	CORE I3
TOTAL	**169**	**37**	**132**		

Tabla Nº 42 PARQUE INFORMATICO
Fuente: Recuperado de: H.CH. y S.B.S. (2014), Servicio de Computo

3.1.1.6. Caracterización del Tráfico de la Red

Medir el tráfico de la red existente no es el caso de estudio, ya que se plantea un Diseño de una nueva Red Informática, ya que la que existe data de muchos años y no se ajusta a ninguna norma técnica y dado que los equipos de monitorización y captura de tráfico son muy complejos y caros.

3.1.2. Fase II Fase de Diseño Lógico

En esta fase se diseñará la topología de la Red de Datos del Hospital Chancay y Servicios Básicos de Salud, donde detallaremos el modelo de direccionamiento y nombramiento, los protocolos a usarse en los dispositivos de interconexión, la seguridad y la administración de la misma.

3.1.2.1. Diseño de la Topología de Red.

La Topología planteada para dar solución al problema de transferencia de datos del Hospital de Chancay y Servicios Básicos de Salud es una Red jerárquica de tres capas, cuya segmentación se realizó de acuerdo a las necesidades. Donde cada capa realiza funciones específicas asignadas y no se refiere a una separación

física, sino lógica; así que podemos tener distintos dispositivos en una sola capa o un dispositivo haciendo las funciones en más de una de las capas.

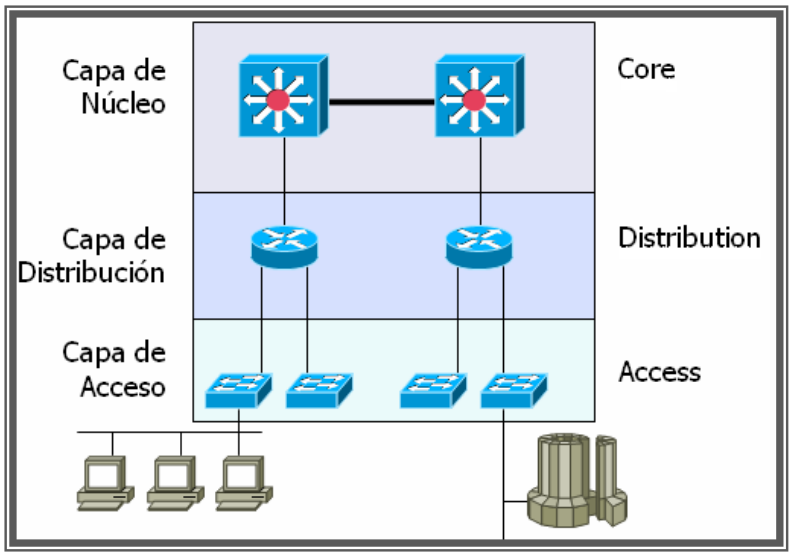


FIGURA N° 28 DISEÑO LOGICO DE RED JERARQUICA
Fuente: Recuperado de: https://ipref.wordpress.com/2008/11/28/modelo-jerarquico-de-red/

3.1.2.1.1. Beneficios:

Escalabilidad

Las redes jerárquicas pueden expandirse con facilidad

Redundancia

La redundancia a nivel del núcleo y de la distribución asegura la disponibilidad de la ruta

Rendimiento

El agregado del enlace entre los niveles y núcleo de alto rendimiento y switches de nivel de distribución permite casi la misma velocidad de data en el cable de toda la red

Seguridad

La seguridad del puerto en el nivel de acceso y las políticas en el nivel de distribución hacen que la red sea más segura

Facilidad de administración

La consistencia entre los switches hace que la administración sea más simple

Facilidad de mantenimiento

La modularidad del diseño jerárquico permite que la red escale sin volverse demasiado complicada.

3.1.2.1.2. Diseño de Red Jerárquica

⇒ **Diseño de Nivel Central o Núcleo**

Se caracteriza de llevar grandes cantidades de tráfico de manera confiable, la latencia y la velocidad son factores de gran importancia para esta capa. En nuestro caso será el de proveer internet a la Red de D, cuyo servicio es proporcionado y configurado por la empresa que brinda el servicio.

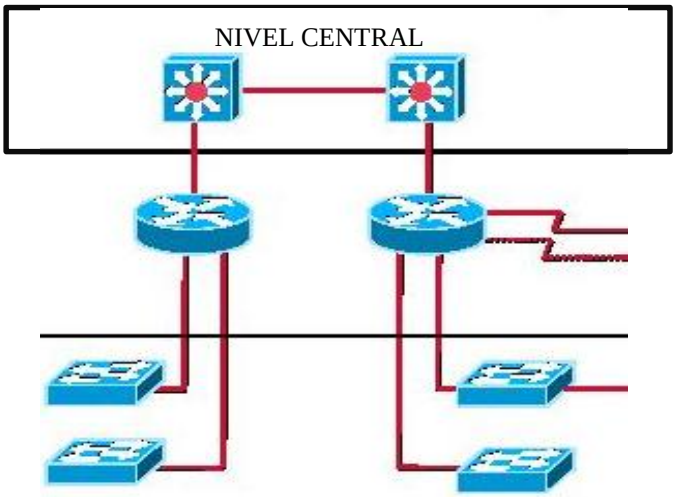


FIGURA N° 29 DISEÑO NIVEL CENTRAL O NUCLEO
Fuente: Recuperado de:
https://yomevaya.wordpress.com/tag/redes/

⇒ **Diseño Nivel de Distribución**

En esta capa se provee el ruteo, la segmentación de la Red de Datos, se implementan políticas de seguridad; sirve de puente o nexo entre la Nivel Central o Núcleo y el Nivel de Acceso. Constituido por el Switch Principal y los Servidores de nuestra Red de Datos.

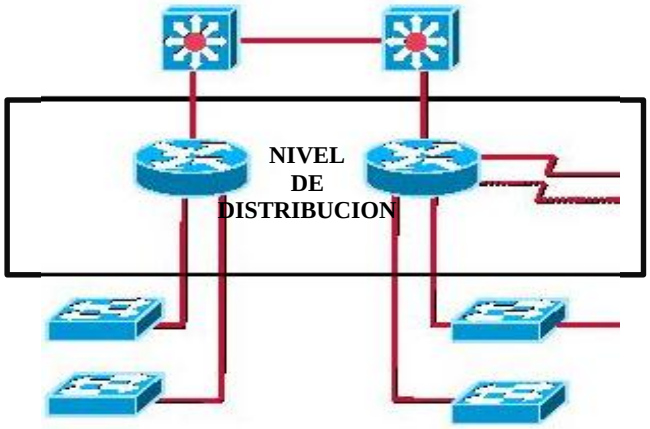


FIGURA N° 30 DISEÑO NIVEL DE DISTRIBUCION
Fuente: Recuperado de:
https://yomevaya.wordpress.com/tag/redes/

⇒ **Diseño Nivel de Acceso.**

En este Nivel de diseño de Red es proporcionar acceso a todas y cada una de las estaciones o terminales de trabajo de la Red Informática, teniendo un control de acceso y políticas; cuyo proceso para diseñar el Nivel de Acceso es el siguiente:

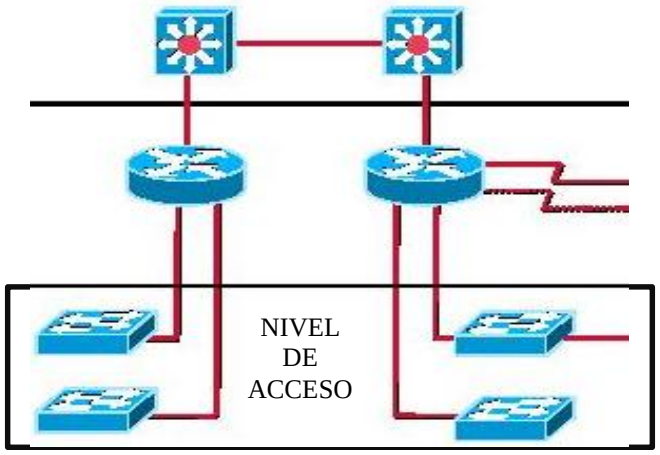


FIGURA N° 31 DISEÑO NIVEL DE ACCESO
Fuente: Recuperado de:
https://yomevaya.wordpress.com/tag/redes/

⇒ **Desarrollo de la Segmentación de la Red de Datos**

Existen motivos suficientes para dividir una red en segmentos, uno de ellos es aislar el tráfico entre fragmentos y obtener un ancho de banda mayor por usuario y fácil administración de los mismos, Según los procesos que se maneja en los diferentes departamentos, unidades y servicios del Hospital Chancay y Servicios Básicos de Salud, se requiere la siguiente segmentación teniendo en cuenta la norma ANSI/TIA-1179:

1. Servicios al Paciente
2. Cirugía/Procedimientos/Sala de Operaciones
3. Emergencias
4. Cuidados Ambulatorios
5. Salud Femenina
6. Diagnóstico y Tratamiento
7. Cuidadores/Administración
8. Servicios/Unidades
9. Instalaciones/Departamentos de Apoyo
10. Operaciones/Soporte
11. Cuidados Intensivos

DEPARTAMENTO, UNIDAD O SERVICIO	SEGMENTO	N° Pcs
Servidores	10	2
Centro de Computo	10	4
Sub Dirección Administrativa	7	2
Unidad de Logística	8	9
Asesoría Jurídica	7	2
Unidad Economía	8	10
Unidad Estadística e Informática	8	7
Unidad de Planeamiento Estra.	8	4
Unidad Personal	8	6
Atención Integral e Salud	4	9
Oficina de Control Interno	7	5
Departamento Medicina	9	2
Oficina de Seguros SIS	8	7
Oficina Etapa Vida Niño	4	1
Oficina Etapa Vida Adolescente	4	2
Oficina Materno	5	3

Control de Emergencias Materno	5	2
Hospitalización Materno	5	1
Almacén General	7	3
Unidad Servicios Generales	8	3
Servicio de Nutrición	8	2
Almacén Medicamentos	7	1
Patrimonio	7	1
Mantenimiento Biomédico	9	1
Salud Materna Neonatal	5	1
Oficina de Emergencias y Desastr.	9	1
Rehabilitación	6	1
Ecografía Materno	5	1
Consultorio Medicina	6	1
Consultorio de Cirugía	6	1
Consultorio de Odontología	6	1
Consultorio de Dermatología	6	1
Tópico	2	1
Cirugías Menores	1	1
Consultorio Traumatología	1	1
Consultorio Oftalmología	1	1
Servicio de Psiquiatría	1	1
Consultorio de Endocrinología	1	1
Unidad de Procedimientos	1	1
Ecografías	2	1
Archivo Rayos X	7	1
Rayos X	2	1
Consultorio de Medicina General	1	1
Consultorio de Nutrición	1	1
Colposcopia	2	1
Control de Vacunación	2	1
Obstetricia	5	1
Ginecología	5	1
Planificación Familiar	5	1
Maternidad	5	1
Caja 1	1	1
Caja 2	1	1
Oficina de Seguros	4	5
Consultorio de Pediatría 1	1	1
Consultorio de Pediatría 2	1	1
Servicio de Psicología	1	1
Comunicaciones	7	2
Departamento de Epidemiología	4	6
Dirección	7	2
Sub Dirección	7	2
Secretaria	7	2
Hospitalización Pediátrica	6	2
Oficina Jefatura Pediatría	9	1
Sala de Reunión de Pediatría	8	1
Departamento de Enfermería	9	3
Unidad Apoyo a la Docencia	9	5
Jefatura de Cirugía	9	1
Consultorio Anestesiológico	1	1
Hospitalización Cirugía	6	2
Centro Quirúrgico	2	1
Sala de Recuperaciones	2	1
Tópico de Cirugía	2	1
Vigilancia	10	1

Farmacia	1	4
Farmacotecnia	1	1
Jefatura Farmacia	7	3
Toma de Muestras	1	3
Anatomía Patológica	2	1
Hematología y Uroanálisis	2	1
Sala de Reuniones de Laboratorio	9	1
Jefatura Patología Clínica	9	2
Auditorio General	10	1
Sala de Residencia Medica	7	1
Tópico Emergencia	3	1
Admisión Emergencia	3	2
Caja Emergencia	3	1
Consultorio de Pediatría Emerge.	3	1
Tópico de Tratamientos	2	1
Unidad de Cuidados Intensivos	11	1
Central de Esterilización	2	1
Sala de Archivos	7	3
Oficina Servicio Social	1	6
Sala de Procedimientos Gástricos	2	1
Sala de Procedimientos de Bronco	2	1
Consultorio de Neumología	1	1
Consultorios de Cardiología	1	3
Admisión	1	4

Tabla Nº 43 SEGMENTACION DE LA RED
Fuente: Elaborada por los Autores

Segmentos teniendo en cuenta la norma ANSI/TIA-1179:

SEGMENTO	N° Pcs
1	34
2	14
3	5
4	7
5	9
6	9
7	30
8	40
9	16
10	8
11	1

Tabla Nº 44 SEGMENTACION DE LA RED
Fuente: Elaborada por los Autores

⇒ **Direccionamiento y Nombramiento de la Red**

Siendo conocedor que la red maneja dos importantes recursos que son: Dirección IP y su correspondiente estructura de nombre dentro de la red. Para proveer

una efectiva comunicación entre hosts o estaciones en una red, cada estación debe mantener una única identidad. En una red IP esto es alcanzado por la Dirección IP.

Las asignaciones de direcciones y nombres sistemáticos ayudan a alcanzar los objetivos de escalabilidad, performance y gestión de la red por lo tanto las asignación de Ip se lo hará a través del servicio DHCP (Dynamic Host Configuration Protocol) cuya tarea del Servicio DHCP es llevar direcciones permanentes IP's a cada estación de trabajo El Servicio DHCP será configurado en el Domain Controller.

SERVIDOR DE DOMINIO (DOMAIN CONTROLLER)	
Nombre	IP
domainsvr .hospitalchancay.gob.pe	192.168.1.2

Tabla Nº 45 SERVIDOR DE DOMINIO
Fuente: Elaborada por los Autores

SERVIDOR DE DNS	
Nombre	IP
domainsvr .hospitalchancay.gob.pe	192.168.1.2

Tabla Nº 46 SERVIDOR DE DNS
Fuente: Elaborada por los Autores

SERVIDOR DE ASIGNACION DE IP DINAMICO (DHCP)			
Función	Nombre	Rango de IP's Privadas	
Primario	domainsvr .hospitalchancay.gob.pe	192.168.1.2	192.168.1.x

Tabla Nº 47 SERVIDOR DE ASIGNACIÓN DE IPS
Fuente: Elaborada por los Autores

SERVIDOR PROXY/FIREWALL	
Nombre	IP Publica
pfsvr.hospitalchancay.gob.pe	Telefónica
	IP Privada
	192.168.1.2

Tabla Nº 48 SERVIDOR PROXY/FIREWALL
Fuente: Elaborada por los Autores

NOMBRE	RANGO DE IP´S PRIVADAS
Segmento de Red 1	192.168.1.11 - 192.168. 1.50
Segmento de Red 2	192.168.1.52 - 192.168.1.70
Segmento de Red 3	192.168.1.72 – 192.168.1.80
Segmento de Red 4	192.168.1.82 – 192.168.1.95
Segmento de Red 5	192.168.1.97 – 192.168.1.115
Segmento de Red 6	192.168.1.117 – 192.168.1.130
Segmento de Red 7	192.168.1.132 – 192.168.1.180
Segmento de Red 8	192.168.1.182 – 192.168.1.225
Segmento de Red 9	192.168.1.127 – 192.168.1.240
Segmento de Red 10	192.168.1.242 – 192.168.1.251
Segmento de Red 11	192.168.1.252 – 192.168.1.254

Tabla Nº 49 ASIGNACIÓN DE IP PARA SEGMENTOS DE RED
Fuente: Elaborada por los Autores

3.1.2.2. Selección de Protocolos de Switching y Routing

La decisión que se cree conveniente con respecto a los protocolos y tecnologías se basa en la información recolectada de los objetivos del negocio y técnico de los clientes.

3.1.2.2.1. Selección de Métodos de Switching

Una buena selección de método de switching nos permitirá contar con:

- Comunicaciones libres de coaliciones.
- Ancho de bandas dedicado en cada puerto.
- Múltiples conversaciones simultáneas.
- Redes más confiables y de mayor rendimiento.
- Simple administración y facilidad de mantenimiento.

- Reutilización de la infraestructura de cableado.

El método será el Source-Route Switching (SRS), que se basa en Source Route Transparent Bridging.

3.1.2.2.2. Selección de Protocolos de Routing

Se usará RIP (Routing Information Protocol) (Protocolo de Información de Enrutamiento). Es un protocolo de puerta de enlace interna. Su algoritmo de encaminamiento está basado en el vector de distancia, ya que calcula la métrica o ruta más corta posible hasta el destino a partir del número de "saltos" o equipos intermedios que los paquetes IP deben atravesar. El límite máximo de saltos en RIP es de 15, de forma que al llegar a 16 se considera una ruta como inalcanzable o no deseable. A diferencia de otros protocolos RIP es un protocolo libre es decir que puede ser usado por diferentes router.

3.1.2.3. Desarrollo de Estrategias de Seguridad de la Red.

El desarrollar estrategias de seguridad implica realizar una serie de acciones como análisis de riesgos, que permita la protección de la información trasmitida no sea manipulada o malversada (amenazas) y protegerlo íntegramente de ellas.

3.1.2.3.1. Identificar los Recursos y Riesgos de la Red

Análisis de Riesgos

La identificación adecuada y documentada de los recursos y riesgos con los que cuenta una red de datos nos permitirá tener un mayor control, es necesario muchas veces hacerse estas preguntas.

- **¿Qué se necesita proteger?**

  Prioritariamente necesitamos proteger la información con la que contamos ya que la perdida de ella nos puede acarrear graves consecuencias como pérdidas financieras, perdidas de información confidencial de los pacientes, por ello es necesario contar con herramientas y acciones de

protección que se adapten a la realidad de nuestra institución. Si bien es cierto no podemos proteger la información en un 100% se debe poner énfasis en proteger la información confidencial de los pacientes, información financiera y los servidores.

- **¿De quién debe de protegerlo?**

  Debido al avance tecnológico vertiginoso el aumento de conexiones se ha incrementado sustancialmente sobre todo el internet, donde en la actualidad podemos encontrar una gran cantidad de intrusos (Hackers, Troyanos, etc.) dispuestos a robarse la información estos hechos criminales no solo se limitan a empresas sino también cualquier persona que tenga información personal en una computadora que cuente con internet. Por ello es necesario tomar las medidas necesarias para proteger la información de estos intrusos, además de las personas que laboran en la misma institución (sabotaje).

- **¿Cómo debe de protegerlo?**

  La principal medida para proteger nuestra información es contar con personal calificado y de confianza en el Área de Computo, donde se encuentra centralizada la información (Servidores), con la finalidad de proteger la información de ataques internos como sabotaje, la siguiente medida a tener en cuenta es contar con un cortafuegos (fireweall); y un antivirus (shopos) para evitar la pérdida de información por ataques externos (virus, hackers, troyanos, etc.).

3.1.2.3.2. Analizar los Riesgos de Seguridad

Los riesgos a los que se encuentra expuesta la información de la Red Informática Hospitalaria del Hospital de Chancay y Servicios Básicos de Salud son distinguidos en dos grandes grupos que son:

a. Amenazas

Son los eventos que pueden causar alteraciones a la información de nuestra organización ocasionando pérdidas materiales, económicas, de información, y de prestigio. Las amenazas es prácticamente imposible controlarlas y menos aún eliminarlas.

Las fuentes de amenaza a las cuales estamos expuestos por su origen son cinco: humanas, de hardware, de software, de red, desastres naturales.

- **Amenazas Humanas**

  El personal que labora en nuestra institución es la amenaza más latente que existen en la Red, en ello se invierten muchos recursos para controlarlos y contrarrestar sus efectos; ya dentro del grupo del personal de la institución se pude identificar atacantes pasivos (usuarios curiosos que navegan en la red que a su vez desean contar con mayores privilegios, no destruyen ni modifican información; personal de limpieza que de manera accidental corta el fluido eléctrico o el cable de red, personal de computo que realiza malas operaciones); y los atacantes activos (personal que hacen daño de manera deliberada borrando o modificando archivos, robo de algún dispositivo del entorno de la Red; otra amenaza es el sabotaje quien malogra deliberadamente algún dispositivo del entorno de Red).

  Existe presencia de practicantes con horarios rotativos en las áreas restringidas.

- **Amenazas de Software**

  Amenaza lógica que puede ser el software incorrecto o bajado de internet, que de manera involuntaria ocasiona daños, una vez instalados por el personal encargado de la administración de la red dejando puertos abiertos que

pueden ser explotados por hackers o virus afectando el buen desempeño de la Red.

No se realiza copias de seguridad de la información periódicamente.

- **Amenazas de Hardware**

  Se da esta amenaza por fallas físicas que presente cualquiera de los elementos de hardware que conforman la Red. Estas fallas físicas pueden ser por defectos de fabricación o mal diseño del hardware, pero también pueden ser el resultado de un mal uso, falta de mantenimiento o culminación de su tiempo de vida útil; puede presentarse de manera continua en los meses de invierno, debido al desgaste por el tiempo de uso y el clima de la zona no es favorable por ser demasiado húmedo; los dispositivos presentan corrosión al poco tiempo de haber sido instalados.

  No existe un inventario del parque informático del hospital.

  No existe un registro de fallas de los equipos informáticos.

- **Amenazas de Red**

  Esta amenaza se presenta por la no disponibilidad de la red, y la extracción lógica de información a través de ésta.

  Los cables de red se encuentran expuestos y a simple vista.

- **Amenazas de Desastres Naturales**

  Entre los tipos de desastres naturales que amenazan a nuestra red de Datos, tenemos la amenaza de incendio, terremotos; la existencia de cables eléctricos en los techos del mismo se encuentran a la intemperie y sin protección, la infraestructura del hospital cuenta con ventanas que se

pueden rompen ante un movimiento sísmico, existe infraestructura del Hospital que ha sido construida con material prefabricado, para tratar de menguar su accionar, es necesario tomar un punto geográfico adecuado para llevar a cabo la instalación de los dispositivos de la Red Informática, Centro de Servicios de Información, Centro de Cómputo, Sala de Equipos, etc.

b. Vulnerabilidades

Una vulnerabilidad es un elemento, que puede ser aprovechado por un atacante para violar la seguridad, así mismo pueden causar daños por sí mismos sin tratarse de un ataque intencionado. A las vulnerabilidades se les consideran elementos internos, existen varios tipos de vulnerabilidades a las que nos encontramos expuestos:

- **Vulnerabilidad Física**

  Está relacionada con el acceso físico a las instalaciones donde se tienen los equipos que contienen la información o forman parte de la Red Las vulnerabilidades de este tipo se pueden presentar mayormente por la mala práctica de las políticas de acceso de personal, el uso de los medios físicos de almacenamiento de información que permitan extraer datos de manera no haya autorizada.

  Todos los equipos no cuentan con los muebles adecuados para ser ubicados adecuadamente, en cualquier momento pueden caer.

  Algunos equipos se encuentran en consultorios expuestos a ser sustraídos por personas ajenas a la institución.

- **Vulnerabilidad de Hardware**

  Las vulnerabilidades de hardware representan la probabilidad de que las piezas físicas fallen (ya sea por mal uso, descuido, corrosión, mal diseño etc.) dejando a la Red desprotegida o inoperable.

Excesiva presencia de humedad en el medio ambiente, produce corrosión en los equipos.

- **Vulnerabilidad de Software**

  Cada programa (ya sea de paquetería o de sistema operativo) puede ser usado como medio para atacar, se debe mayormente a errores de programación, o porque en el diseño no fueron considerados ciertos aspectos (por ejemplo controles de acceso, drivers de las pcs).

  No se encuentra restringido el acceso a la instalación de nuevas aplicaciones que pueden causar errores en la red.

- **Vulnerabilidad de Factor Humano**

  Las vulnerabilidades de origen humano más comunes son la falta de capacitación y concientización, lo que dará lugar a la negligencia en el seguimiento de las políticas de seguridad.

  No existe un manual de procedimientos que el personal deba seguir ante una situación adversa.

  Personal no cuenta con capacitación en el manejo de la administración de redes.

- **Vulnerabilidad de Red**

  Las redes pueden llegar a ser sistemas muy vulnerables, al tratarse de una serie de equipos conectados entre sí compartiendo recursos, es posible atacar a toda la red penetrando primero en uno de los equipos y posteriormente expandirse al resto.

  No existen restricciones para poder ingresar a internet o tener acceso a un ordenador de la red.

- **Vulnerabilidad Natural**

  Recordemos que las amenazas naturales son todo tipo de desastres causados por fuerzas naturales que causan daño.

  No estar prevenido para un amago de incendio.

  No conocer el uso adecuado de un extinguidor.

Finalmente es importante hacer una reflexionen el sentido de que las vulnerabilidades se pueden reducir, eliminar o controlar lo que ayuda entonces a contrarrestar la posibilidad de que una amenaza se materialice y llegue a convertirse en un ataque.

AMENAZAS A LAS CUALES ESTAMOS EXPUESTOS

AMENAZA	EJEMPLO
Suplantación de Identidad	• Acceso ilegal a la información de otro usuario.
Modificación de Datos	• Modificar datos de manera no autorizada.
Repudio	• Realizar una operación ilegal en un sistema sin que exista la posibilidad de realizar un seguimiento de la misma.
Divulgación de Información	• Un usuario lee archivos donde no se a proporcionado el acceso.
Denegación de Servicio	• Deshabilitar temporalmente el servidor de datos.
Elevación de Privilegios	• El agresor burla con éxito la seguridad y obtiene privilegio de administrador de manera informal.

Tabla Nº 50 AMENAZAS EN LA RED
Fuente: Elaborada por los Autores

3.1.2.3.3. Analizar los Requerimientos de Seguridad.

Una vez identificados los riesgo y/o amenazas, se puede adoptar controles y medidas de seguridad que permitan gestionarlos ya sea reduciendo las amenazas, las vulnerabilidades o bien disminuyendo el impacto frente a algún incidente de seguridad.

AMENAZA O VULNERABILIDAD	COMO EVITAR QUE SE CONVIERTA EN ATAQUE
Suplantación de Identidad	• Elegir una contraseña segura (mínimo de 6 dígitos, combinación de caracteres y números). • Evitar usar nombres y fechas de nacimiento. • Evitar revelar su contraseña.
Incendio	• Contar con detectores de humo, extintores en buenas condiciones. • Revisar periódicamente las fechas de vencimiento de los extintores. • Evitar tener instalaciones eléctricas a la intemperie.
Repudio	• Evitar que personal haga uso de estaciones de trabajo fuera de sus horas de trabajo.
Personal poco identificado con la Institución	• Brindar charlas y capacitaciones de personal, concientizándolo permanentemente.
Corte de Cables de Red	• Evitar que los cables de Red estén expuestos y cercanos a cables energizados.
Corte de Fluido Eléctrico	• La institución cuenta con un grupo electrógeno cuyo tiempo de respuesta es de 15 segundos. • Los servidores y switch así como las estaciones de trabajo de Áreas críticas (Admisión, Caja, Farmacia) deberán estar instalados a un UPS.

Tabla Nº 51 COMO EVITAR AMENAZAS EN LA RED
Fuente: Elaborada por los Autores

3.1.2.3.4. Desarrollo del Plan y Políticas de Seguridad

Un Plan de Seguridad de nuestra Red contesta a la pregunta de ¿Cómo nos podemos proteger? Para dar respuesta a esta pregunta, es que nosotros podemos hacer uso de una serie de mecanismos de protección, así como también implantar normas y políticas de seguridad que nos permita tener confidencialidad, integridad y disponibilidad de la red; nuestros recursos de la Red serán un blanco perfecto y nuestro objetivo es protegerlos.

Seguridad Física

- El hardware es el más caro de los recursos, es importante no colocar equipos en lugares altos e inseguros para evitar caídas.
- No colocar objetos móviles sobre los equipos, corren el riesgo de hacer sobre ellos y deterióralos.
- Utilizar fijaciones para elementos críticos (gabinetes para switch).
- Evitar colocar equipos cerca a las ventanas, para evitar que caigan objetos lanzados del exterior.

Seguridad Perimetral

- Instalar detectores de movimiento.
- Instalar cercos eléctricos si la infraestructura así lo requiere.
- Instalar circuito cerrado de cámaras.
- El acceso a los servidores estará bajo llave y se ubicaran en un lugar adecuado de acceso restringido.

Seguridad de Equipos

- Mantener un inventario actualizado de todos los equipos que forman parte de nuestra red.
- Instalar extintores en lugares visibles y de fácil acceso en caso de una emergencia.
- Instalar detectores de humo en lugares críticos.
- Los usuarios que tengan cualquier tipo de inconveniente con los equipos informar de inmediato al responsable de la Administración de la Red.

- Los usuarios no podrán ingerir alimentos y líquidos cerca a los equipos de la Red.

Suministro Eléctrico

- La responsabilidad del buen funcionamiento de la sub estación eléctrica estará a cargo del Área de Servicios Generales.
- El balanceo de cargas eléctricas debe ser el adecuado para evitar fallas eléctricas en los equipos.
- Contar con pozos a tierra.
- Ante corte de fluido eléctrico se debe contar con un grupo electrógenos de respuesta rápida.

Mantenimiento de Equipos

- El mantenimiento de los equipos se realizara por personal autorizado.
- Documentar todo tipo de falla y mantenimientos preventivos.
- Se debe cumplir con el plan de mantenimiento de equipos según cronogramas establecidos.
- Contar con un manual de procedimientos ante fallas comunes y típicas que se presenten.

3.1.2.3.5. Definir Políticas de Seguridad

Las Políticas de Seguridad viene a ser la elaboración detallada de normas a ser cumplidas por los usuario, en este caso el Hospital Chancay y Servicios Básicos de Salud, contara con una Red de Datos, por lo cual los empleados autorizados podrán hacer uso de misma, ya que el uso de la red es un privilegio y no un derecho, los usuarios deberán tener en cuenta lo siguiente:

- El usuario que haga uso de esta red tendrá que previamente identificarse.
- Se brindara al usuario el permiso necesario para poder manejar la información que necesite dentro de la red.

- Se tomara las medidas necesarias para proteger la información que circula por la red garantizando la disponibilidad e integridad del servicio.
- Las responsabilidades de la administración de la Red recaerán en el área de cómputo, en cuya Área existirá una persona responsable denominada Administrador de Red.
- Todo incremento de Estación de Trabajo que desea tener acceso a la red debe de tener conocimiento el Administrador de la Red.
- El Administrador de la Red debe de Monitorear constantemente el desempeño de las Estaciones de Trabajo.
- Toda Estación de Trabajo debe ser instalada y configurada por el personal del área de Cómputo.
- Ningún usuario estará facultado de instalar equipos ajenos a la institución, a la red de datos de la misma.
- Las Estaciones de Trabajo contaran con identificación de código patrimonial y de Red, a la vista, asignada por el Área de Patrimonio y Administrador de la Red.
- El Usuario no podrá acceder a recursos de la red sino se encuentra autorizado.
- El Usuario no podrá instalar deliberadamente aplicaciones sin autorización del Administrador de la Red.
- Se prohíbe la trasmisión de cualquier material discriminatorio u hostil, degradante o intimidatorio.
- Se prohíbe distribuir mensajes que revelen cuestiones personales o privadas relativas a cualquier persona
- No se debe usar la identidad de otro usuario sin previa autorización del mismo.

3.1.2.3.6. Mecanismos de Seguridad:

Entre los mecanismos de seguridad que podemos tomar en cuenta para acceder a la Red de Datos del Hospital de Chancay tenemos:

- Identificador de Red: es el nombre de la Red, la cual lo va a identificar y todos los usuarios deberán tener configurado el nombre de la Red para poder acceder a la misma de manera correcta.
- Identificador de Usuario: Es el nombre de la Estación de Trabajo que debe ser único tan igual que su dirección IP para evitar conflictos.
- El usuario deberá contar con nombre de usuario y una contraseña para poder acceder a los servicios de la Red.

3.1.2.3.7. Otros Criterios a Tomar en Cuenta

- **Protección del Hardware**

  El hardware es frecuentemente el elemento más caro de todo sistema informático y por tanto las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier organización.

  Para la detección de accesos se pretende emplear medios técnicos, como cámaras de vigilancia de circuito cerrado, y otro criterio a tomar en cuenta es que el personal que labora se conoce entre sí, y cada uno cuenta con sus responsabilidades, de modo que les resulte sencillo detectar a personas desconocidas o a personas conocidas que se encuentran en sitios no adecuados o realizando una labor no autorizada.

- **Desastres Naturales**

  Los desastres naturales más comunes a los que nos encontramos expuestos son:

- ✓ **Terremotos y Sismos**

  El Distrito de Chancay, Provincia de Huaral Departamento de Lima, se encuentra ubicado en una zona de constante actividad sísmica por lo que se cree conveniente tomar en cuenta para prevenir problemas causados por terremotos o sismos.

  - No situar equipos en sitios altos para evitar caídas.
  - No colocar elementos móviles sobre los equipos para evitar que caigan sobre ellos.
  - Separar los equipos de las ventanas para evitar que caigan por ellas o qué objetos lanzados desde el exterior los dañen.
  - Utilizar fijaciones para elementos críticos.
  - Colocar los equipos sobre plataformas de goma para que esta absorba las vibraciones.

- ✓ **Inundaciones y humedad**

  Las inundaciones son poco frecuentes, lo que si suele suceder el desbordamiento de los tanques elevados de agua, para tal caso ya se cuenta con llaves automáticas, en cuanto a los niveles de humedad se presentan con mayor frecuencia, el clima es húmedo con un grado de humedad de un 80%, que produce condensación en los circuitos integrados dando origen a cortocircuitos, para prevenir se hará uso de tizas o de cloruro de calcio como extractores de humedad aunque se recomienda que más adelante se haga uso de extractores de humedad electrónicos.

- ✓ **Incendios y humos**

  Por último mencionaremos el fuego y los humos, que por lo general provendrán del incendio de equipos por sobrecarga eléctrica. Contra ellos emplearemos sistemas de extinción (extintores de polvo químico seco o bióxido de carbono), que aunque pueden dañar los equipos, actualmente son más o menos inocuos. Además del fuego, también el humo es perjudicial para los equipos (incluso el del tabaco), al ser un abrasivo que ataca a todos los componentes, por ello quedara terminantemente prohibido fumar en el Centro de Computo.

- ✓ **Electricidad**

  Quizás los problemas derivados del entorno de trabajo más frecuentes son los relacionados con el sistema eléctrico que alimenta nuestros equipos; cortocircuitos, picos de tensión, cortes de flujo. Para corregir los problemas con las subidas de tensión se contara con pozos a tierra que en la actualidad son 7.

  Para los cortes de fluido eléctrico, al menos los Servidores, Switch y las Estaciones de Trabajo catalogadas como elementales contaran con Sistema de Alimentación Ininterrumpida (SAI), que además de proteger ante cortes, mantienen el flujo de corriente constante, evitando las subidas y bajadas de tensión. Además de contar con un Grupo Electrógeno de 140 HP de reacción rápida de encendido y apagado automático.

  Por último indicar que además de los problemas del sistema eléctrico también debemos

preocuparnos de la corriente estática, se empleará espráis antiestáticos se debe tener cuidado de no tocar componentes metálicos, evitar que el ambiente esté excesivamente seco, etc.

- ✓ **Protección de los Datos**

  Además proteger el *hardware* nuestra política de seguridad debe incluir medidas de protección de los datos, ya que en realidad la mayoría de ataques tienen como objetivo la obtención de información, no la destrucción del medio físico que la contiene.

  Para ello se contara con firewall y antivirus, así como también se realizara copias de seguridad de la información de manera periódica, la información en algunos casos se guardara tanto en forma digital como también impresa guarda con absoluto celo.

3.1.3. Fase III Diseño Físico

3.1.3.1. Selección de Tecnologías y Dispositivos para la Red.

3.1.3.1.1. Cable UTP Categoría – 7

Características Técnicas

- ✓ Conductor: hilo de cobre desnudo, 23 AWG
- ✓ Aislamiento: SFS PO, 1.43 mm
- ✓ Cantidad de hilos: 8
- ✓ Cantidad de pares: 4
- ✓ Color de los pares trenzados:

  Blanco/azul - azul

  Blanco/naranja - naranja

  Blanco/verde - verde

  Blanco/marrón - marrón
- ✓ Cada par está envuelto en una lámina de aluminio-poliéster (lámina de aluminio por fuera) que cubre el 100% del revestimiento del par trenzado

- ✓ 4 pares trenzados 23 AWG dispuestos alrededor del alambre de drenaje
- ✓ Pantalla exterior: revestimiento trenzado de cobre estañado, que cubre el 55% del revestimiento del cable
- ✓ Material del forro: LSZH (refractario, de baja emisión de humo, no contiene halógenos).
- ✓ Diámetro exterior del cable: 8.4 mm.
- ✓ Peso del cable: 61 kg/km.
- ✓ Temperatura de almacenaje: -30ºC - +70ºC.
- ✓ Temperatura de instalación: -5ºC - +50ºC.
- ✓ El cable está en conformidad con el estándar de protección contra incendios: UL VW-1, IEC 60332-1.
- ✓ Radio mínimo de curvatura: 10xØ durante la instalación, 8xØ en régimen operativo
- ✓ Esfuerzo durante el tendido del cable: 130 N máximo durante la instalación

Aplicación

Cable que servirá para realizar la instalación del cableado estructurado de la Red Informática en toda la infraestructura de la institución.

Especificaciones

- ✓ ISO/IEC 754-2
- ✓ ISO/IEC DIS 11801
- ✓ EIA/TIA BULLETIN TSB-36
- ✓ ISO/IEC 1034-1, 1034-2
- ✓ ANSI/EIA/TIA CARLINGA STANDARD 568-A/B
- ✓ CENELEC EN 50288
- ✓ CENELEC EN 50173
- ✓ CENELEC EN 50167, 50168, 50169

3.1.3.1.2. Patch Cord UTP Categoría 7

Características Técnicas

- ✓ Conductor: 7 hilos de cobre Ø0.2±0.01 mm, 24 AWG.

- ✓ Aislamiento: polietileno denso, grosor mínimo 0.18 mm.
- ✓ Diámetro del hilo 1.03±0.02 mm.
- ✓ 4 Pares trenzados con forro de PVC (0.4 mm) color de pares: (azul - blanco/azul, naranja - blanco/naranja, verde - blanco/verde, marrón –blanco/marrón).
- ✓ Diámetro exterior del cable 5.3±0.2 mm
- ✓ Temperatura de funcionamiento: +75ºC, resistente al fuego.

Aplicación

Utilizado para realizar el parcheo en el rack entre panel y switch, conexiones entre las estaciones de trabajo y switch (toma de red).

Especificaciones

Cumple con los estándares UL444/UL1581, TIA/EIA 568B.2-1

3.1.3.1.3. Gabinete de Piso 37U

Características Técnicas

- ✓ Cumple con las especificaciones ANSI/EIA RS-310-D, DIN41491: PART1, IEC297-2, DIN41494: PART7 y GB/T3047.92.
- ✓ Marco de estructura sólida construido con material de alta calidad, especial para colocar equipos pesados
- ✓ Puertas principal y posterior con rejilla de alta densidad para ventilar y disipar el calor.
- ✓ Base de apoyo y ruedas facilitan el transporte e instalación de la unidad.
- ✓ Sistema de administración de cables integrado en la parte superior interna del gabinete.
- ✓ Concebido para albergar equipos de montaje en bastidor conforme al estándar EIA de 19 pulgadas.
- ✓ Profundidad ajustable en tramos de 25 mm para acomodarse a los requerimientos de su instalación.

- ✓ Superficie con acabado especial para evitar la corrosión y el daño causado por otros factores externos.
- ✓ Hoja de acero de alta calidad laminado en frío. Grosor: 2.0 mm en los bordes de los ángulos, el resto presenta un espesor de 1.2 a 1.5 mm.
- ✓ Máxima carga estacionaria de 1.300 kg / 2.860 lb.

Aplicación

Este resistente gabinete diseñado para albergar equipos informáticos trae puertas con llave para asegurar y controlar el acceso a los componentes de la red. Puertas con rejillas de alta densidad garantizan la óptima ventilación en el interior del gabinete. La puerta posterior doble permite acomodar el gabinete en cuartos para servidores con diferente disposición, ya que minimiza el espacio que se necesita para tener acceso por detrás de la unidad.

3.1.3.1.4. Gabinete de Pared 6RU

Características

- ✓ Diseñado según la norma EIA – 310D.
- ✓ Fabricado con acero LAF de 1.2mm.
- ✓ Cuenta con 2 rieles, tropicalizado, con perforaciones circulares, normalizados en 19".
- ✓ Diseñado bajo procesos desengrasante, fosfatizado y anti oxidante.
- ✓ Ofrece una resistencia cinco veces mayor al óxido y ralladuras.
- ✓ Entrada y salida de cables a través del marco desmontable.
- ✓ Puerta con centro de acrílico polarizado de 3mm.

Aplicación

El gabinete de pared SATRA de 6RU, está diseñado para brindar seguridad a sus equipos de red, distribuidores y demás equipos de telecomunicaciones, los cuales no pueden ser instalados en espacios limitados de piso. Diseñado según las normas internacionales con materiales de la mejor calidad lo cual brinda mayor resistencia y duración de la estructura. El marco de anclaje del gabinete de pared cuenta con 6 orificios para la distribución adecuada de cable, el cual se puede separar de la estructura para la administración de los equipos y cableado por la parte posterior.

Especificaciones

Acabado con pintura en polvo electrostático de 70 a 80 micras, color negro texturizado, espesor de la estructura1.2mm., ventilación Kit de 2 ventiladores, entrada de cable (orificio 7.8 cm diámetro, seguridad 2 chapas (1 puerta y 1 marco), 1 llave.

3.1.3.1.5. Canaletas, T, Codo, Uniones y Terminaciones Plásticas

Características

- ✓ La dimensión de las canaletas será variable de acuerdo a las líneas de cable a pasar x su interior.

15x10mm.	Cap.	1	cable
24x14mm.	Cap.	4	cables
39x18mm.	Cap.	8	cables
39x18mm.	C/div. Cap.	8	cables
60x22mm.	Cap.	20	cables
65x45mm.	Cap.	30	cables
100x50mm.	Cap.	50	cables

Tabla Nº 52 CAPACIDAD DE CABLES POR CANALETA
Fuente: Elaborada por los Autores

- ✓ El material deberá ser de PVC de baja emisión de gases.
- ✓ Material resistente a los golpes, con flexibilidad adecuada de fácil manipulación y adecuarse a cualquier tipo de pared.
- ✓ El material de la canaleta debe permitir ser pintada fácilmente.

Aplicación

Servirá para proteger al cable UTP durante su recorrido en la Red

Especificaciones

Debe cumplir con las normas TIA/EIA

3.1.3.1.6. Cajas Adosables

Características

- ✓ El material deberá ser de PVC de baja emisión de gases.
- ✓ Material resistente a los golpes.
- ✓ Caja de fácil adhesión a las paredes o empotrados.

Aplicación

Accesorio indispensable para el correcto ordenamiento de su canaleteado. Fácil de instalar en superficies planas mediante tornillos de fijación

Especificaciones

Debe cumplir con las normas TIA/EIA

3.1.3.1.7. Jack RJ45

Características

- ✓ Interfaz usada para empalmar el cable horizontal y los patch cords.
- ✓ Jack modulares para 4 pares trenzados.
- ✓ Código de colores según la normativa para ambas terminaciones T568A/T568B.

- ✓ La conexión de los conectores es por desplazamiento de aislante, IDC estilo 110,
- ✓ Diseñados para cumplir y exceder los requerimientos del estándar ANSI/TIA-568-C.2.
- ✓ Instalables tanto en los Face-Plate (Placa de Pared) como también en los Patch Panel.
- ✓ Ideal para aplicaciones de datos, voz o video con la mínima atenuación.
- ✓ Todos nuestros Jacks están certificados por la UL (Underwriter Laboratory).

Aplicación

Se usara el conector RJ45 para todo nuestro sistema de cableado estructurado.

Especificaciones

Debe cumplir con las normas TIA/EIA

3.1.3.1.8. Placa de Pared (Face Plate)

Características

- ✓ Contar con dos puertos para conectores UTP.
- ✓ Face Plate con dos puerto tipo icono que cuenten con ángulo de 45 grados para conexiones de redes, telefonía y video jack modulares para 4 pares trenzados.
- ✓ Debe soportar hasta 4 estándares de conectores para instalaciones individualizadas.
- ✓ Su presentación viene en diversos colores más usados el marfil y el blanco.

Aplicación

Se usara para la instalación de puntos en las áreas de trabajo y donde sea necesario contar con puntos de toma de red.

Especificaciones

Debe cumplir con las normas TIA/EIA

3.1.3.1.9. SWITCH D-LINK DGS-3120 (Borde)

Características

- ✓ Es administrable.
- ✓ Cuenta con 44 puertos 10/100/1000Base-T; 4 puertos 10/100/1000Base-T/SFP.
- ✓ Cuenta con 4 puestos SFP.
- ✓ Alimentación eléctrica de 100 a 240 VAC.
- ✓ Seguridad NetBIOS/NetBEUI Filtering.

Aplicación

Sirve para conectar los puntos de acceso de las estaciones de trabajo, garantizando el acceso a la red.

Especificaciones

Debe cumplir con las normas TIA/EIA

3.1.3.1.10. SWITCH D-LINK DGS-3420 (Distribución)

Características

- ✓ Es administrable.
- ✓ Cuenta con 48 puertos RJ45 10/100/1000PoE.
- ✓ Alimentación eléctrica de 100 a 240 VAC.

Aplicación

Sirve para segmentar grupos de trabajo, las políticas de conectividad están configuradas en esta capa, garantizando el orden en la red de fácil administración.

Especificaciones

Debe cumplir con las normas TIA/EIA

3.1.3.1.11. SWITCH HP 5500-24G EI (Core)

Características

- ✓ Administrable, Intelligent Management Center (central de Administración Inteligente), Interfaz de línea de comandos, Navegador Web, Administrador de SNMP, MIB Ethernet IEEE 802.3
- ✓ 24 Puertos RJ-45 10/100/1000 Mbps.
- ✓ 4 Puertos SFP.

- ✓ 2 Slot de Expansión.
- ✓ 1 Puertos RJ-45 para consola serial.
- ✓ Alimentación eléctrica de 100 a 240 VAC.

Aplicación

Sirve para proveer de alta velocidad al backbone y al puerto WAN manejar los paquetes tan rápido como sea posible, es el cerebro de la red en cuanto a la conectividad de alto nivel de disponibilidad y debe adaptarse a los cambios que sufra la red de manera inmediata.

Especificaciones

Debe cumplir con las normas TIA/EIA

3.1.3.2. Cableado Estructurado de la Red Informática.

3.1.3.2.1. Topología del Cableado Estructurado

La Topología a emplearse en el Cableado Estructurado de la Red Informática Hospitalaria para el Hospital Chancay y Servicios Básicos de Salud es la Topología Estrella y Protocolo de comunicación TCP/IP.

3.1.3.2.2. Tipo de Cable a usar en la Red Informática

El cable que se usara para el tendido de la Red Informática para el Hospital Chancay y Servicios Básicos de Salud será el cable UTP de 8 Hilos categoría 7, que me garantizara la trasmisión de 10-Gigabit Ethernet (XGbE o 10GbE), que actualmente es el más rápido de los estándares Ethernet, pudiendo trasmitir una velocidad nominal de 10 Gbit/s.

3.1.3.2.3. Elementos del Cableado Estructurado

- ✓ **Cableado Horizontal**

  Constituido por el cable que va desde el Área de Trabajo hasta el Gabinete de los Dispositivos, la Topología del Cableado será Estrella, un punto para cada toma de las Estaciones de Trabajo, deberán

terminar en una Caja Adosable protegida por su Face Plate, la distancia máxima que recorre el cable a nivel de piso no deberá de exceder a 90 metros lineales, distancia medida desde el Área de Trabajo hasta el Cuarto de Equipos; Los Patch Cord no deberán de exceder de los 3 metros lineales. La cantidad de de Cable y material a utilizar, realizó la medición desde el Gabinete de los Dispositivos hacia todas las Estaciones de Trabajo.

- ✓ **Cableado Vertical**

  El backbone será constituido por Cable UTP Categoría 6 color azul marca Newlink, este se extiende, desde la Unidad de Informática hacia los Gabinetes de cada piso.

  Para la protección se usara canaleta a lo largo de su recorrido.

- ✓ **Cuarto de Equipos**

  Es el lugar donde existe la concentración de los equipos y las conexiones activas que conforman la red Switch, Servidores (Archivos, Aplicaciones, ect.) y un Router que se utilizará para la conexión de la red a internet.

- ✓ **Área de Trabajo**

  Formada por los Patch Cord, de Categoría 7, que unirá el Face Plate con la Estación de Trabajo.

- ✓ **Gabinetes de Dispositivos**

  Constituido por los Gabinetes que alojan a los Dispositivos de Interconexión (Switches, Servidores, Router) y a donde llegan las terminaciones de los Cables que vienen de los puntos de las Estaciones de Trabajo.

El Cableado Estructura proyectado para el Hospital Chancay y Servicios Básicos de Salud, se muestra en el diseño del plano adjunto.

3.1.3.3. Dispositivos de Interconexión a Usar.

Se usara dos dispositivos de interconexión el Swicth y el Router (Modem) para seleccionar estos dispositivos fueron los siguientes:

Swicth

DISPOSITIVO	CARACTERÍSTICAS
Switch	✓ Soporta Tecnología LAN. ✓ Cantidad de Puertos. ✓ Operaciones a nivel de Capa de Enlace ✓ Auto sensibilidad de Velocidad ✓ Costo Bajo. ✓ Disponibilidad de soporte técnico. ✓ Dispositivo certificado.

Tabla Nº 53 CARACTERISTICAS DE SWICTH
Fuente: Elaborada por los Autores

Router (Modem)

Dispositivo que cuenta con cuenta con tecnología ADSL, es proporcionado y configurado por una empresa externa al Hospital por tal motivo no existe características de selección por parte nuestra.

3.1.3.4. Seguridad.

El Hospital Chancay y Servicios Básicos de Salud al ser una Institución Pública y contando con una infraestructura definida se considera conveniente que el Cuarto de Servidores se encuentre situado al costado del Área Administrativa y de Soporte Técnico, en el Tercer Piso del Edificio E, ya que no existe otro lugar que reúna las condiciones necesarias para la implementación, por lo que se ha solicitado colocar una puerta de acceso al Tercer Piso del Pabellón E además de contar con la Puerta de Acceso a la Oficina

Administrativa de Informática y del Área de Soporte Técnico, también se recomienda tomar en cuenta lo siguiente:

- ✓ Asegurar el ingreso al Cuarto de Equipos mediante una puerta prohibiendo el acceso a personal no autorizado.
- ✓ Contar con equipo de aire acondicionado con la finalidad de mantener la temperatura adecuada para el funcionamiento de los equipos.
- ✓ Evitar el humo, el polvo dentro del Cuarto de Equipos.
- ✓ Lugar alejado de los ruidos eléctricos y del agua.
- ✓ Prohibir el consumo de bebidas y comida en el Cuarto de Equipos.
- ✓ Contar con servicio eléctrico ininterrumpido en el cuarto de Equipos.
- ✓ Contar con extintores 100% operativos tipo C.

3.1.3.5. Plano propuesto para el diseño físico de la red

En el siguiente plano se mostrara la distribución física del cableado estructurado y de los equipo de comunicación, servidores, equipos para la protección física, instalación del pozo tierra.

Tenemos 6 edificios:

- ✓ Pabellón A (Servicio Social, Consultorios de Cardiología y Archivo)
- ✓ Pabellón B (Servicio de Emergencia y Auditorio).
- ✓ Pabellón C (Servicio de Farmacia y Laboratorio).
- ✓ Pabellón D (Consultorios Externos, Hospitalización de Pediatría, Cirugía, Centro Quirúrgico).
- ✓ Pabellón E (Servicios Generales, Hospitalización de Materno, Medicina y Áreas Administrativas).
- ✓ Pabellón F (Nutrición, Dosis Unitaria, Almacén Medicamentos, Patrimonio y Biomédicos)

En el cuarto de servidores tenemos la instalación de los servidores junto con su rack y los pach panel, los equipos de comunicación, switch, routers, su diseño han considerado la ANSI/TIA/EIA 569, que nos propone requerimientos a función de espacios y dimensiones. También se ha considerado la instalación de un pozo tierra para descarga electrostática de los

equipos de comunicación, basándose en la norma ANSI/TIA/EIA 607, que nos sugiere la instalación de estos para evitar perjuicios en los equipos por la acumulación de carga electrostática.

En los planos observaremos a continuación:

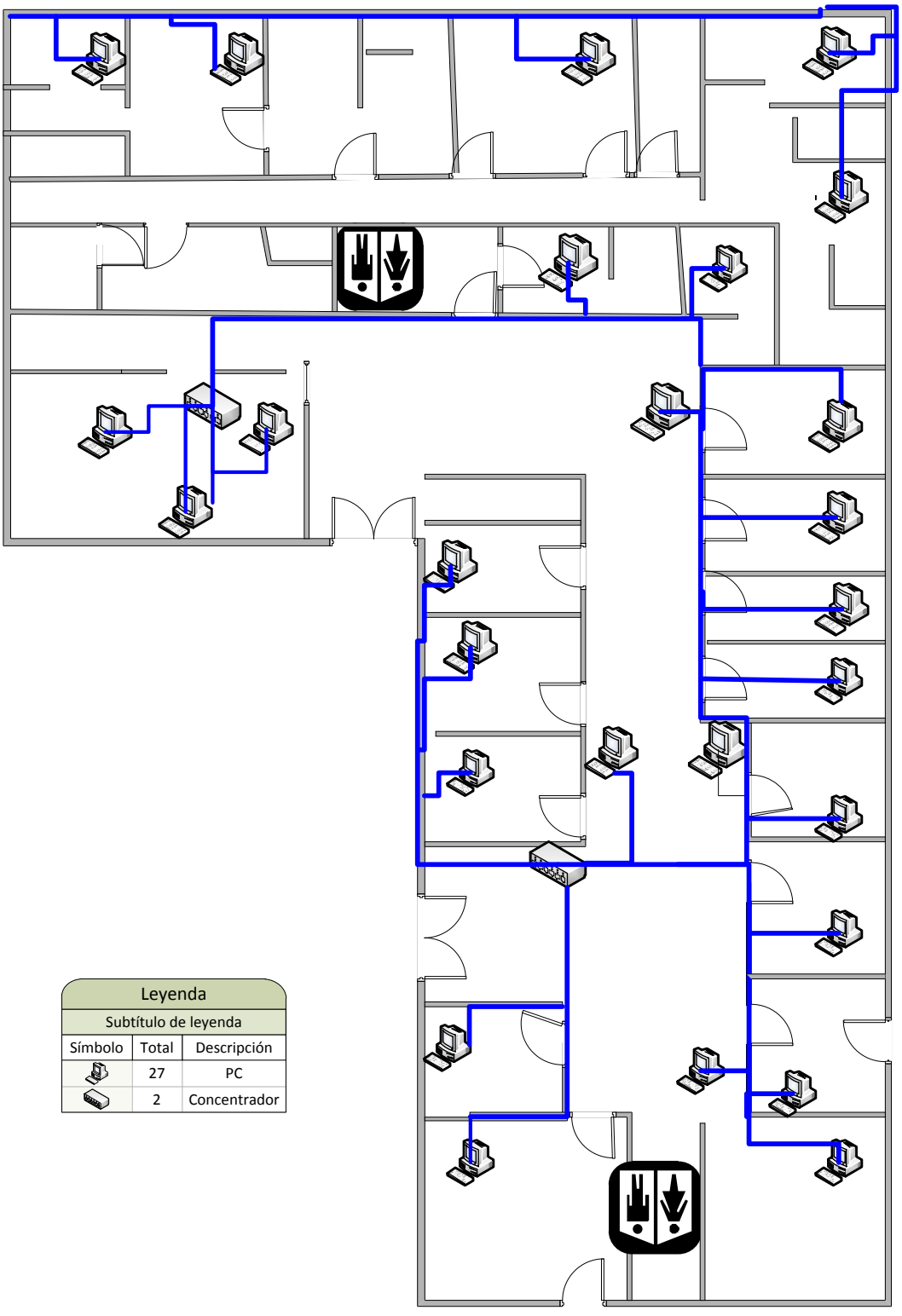


Figura 29: Edificio B: Historial y Consultorio Externo

Edificio C: Servicios médicos

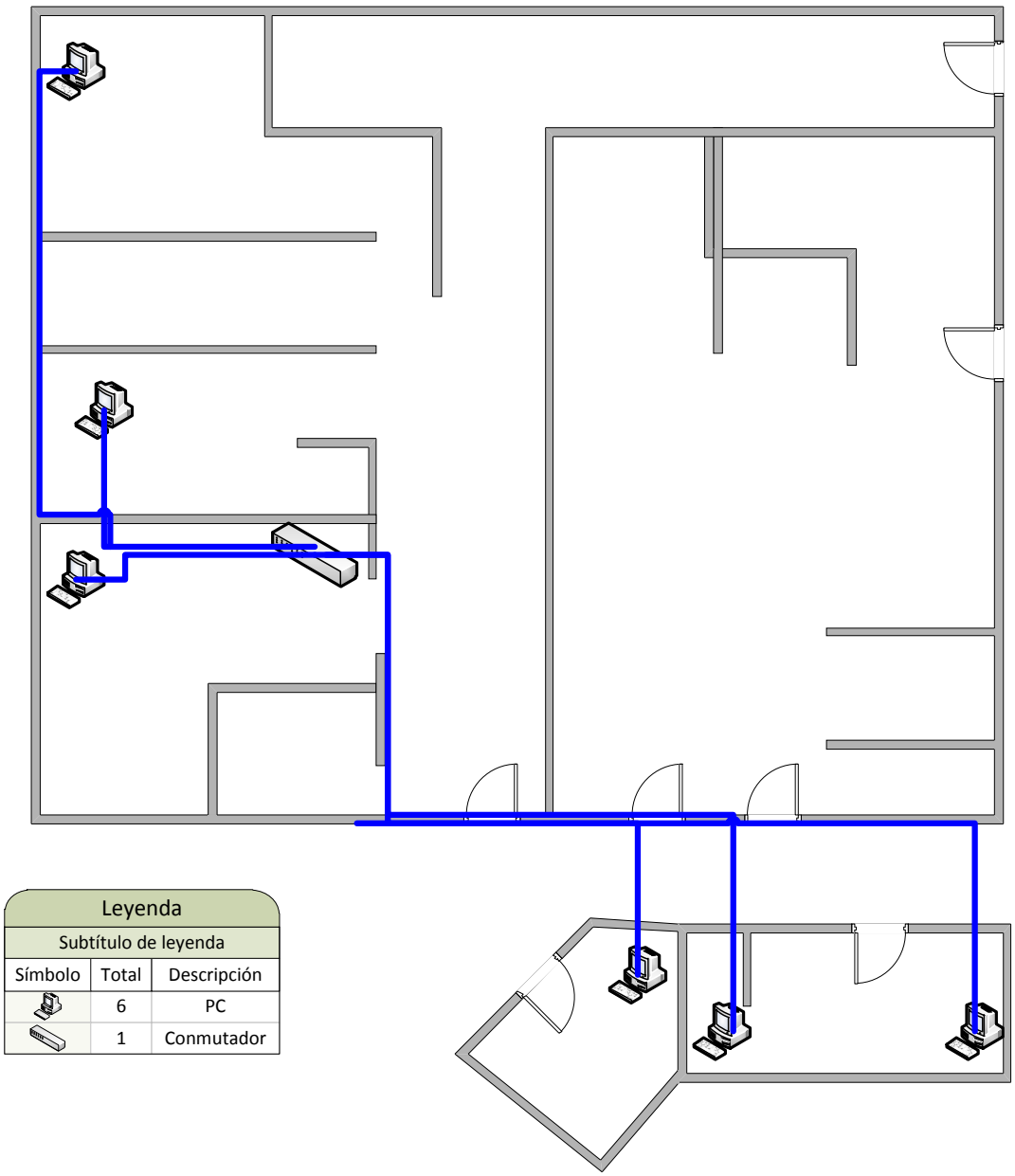


Figura 30:Edificio C: Servicios Médicos

Edificio D: Rehabilitación física, Almacén y Servicios Médicos (Tópico)

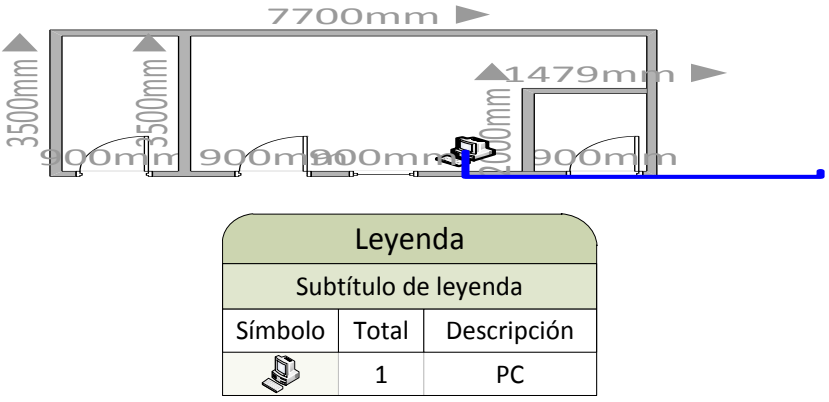


Ilustración 1:Edificio D: Servicios Médicos (tópicos)

Fuente: Elaboración Propia

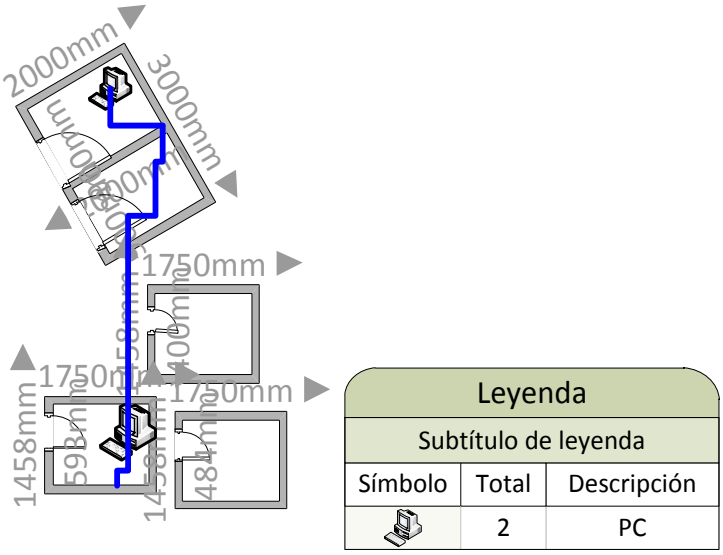


Figura 31:Edificio D: Rehabilitación física y Almacén

Edificio E -1: Área de sistema, Caja, laboratorio clínico y nutrición

3.1.4. PLAN DE IMPLEMENTACIÓN DE LA RED INFORMÁTICA.

3.1.4.1. Directivas para instalación y configuración de DNS

- Nombre DNS: domainsvr.hospitalchancay.gob.pe
- Zonas de búsqueda: directa e inversa.
- Direcciones IP del Servidor. 192.168.1.2
- Tipo de Servidor: Solo Primario.
- Integrado al DA: si
- Estructura de unidad organizativa: según el organigrama del hospital

3.1.4.2. Directivas para instalación y configuración del DA

- Tipo de Controlador de dominio: para un nuevo dominio.
- Tipo de dominio a crear: Dominio en un nuevo Bosque.
- Nombre DNS para el nuevo dominio: hospitalchancay.gob.pe
- Nombre NetBios: hospitalchancay
- Tipo de permisos predeterminados para usuarios y objetos de grupo: compatible con Windows 2012.
- Establecemos contraseña de Administrador de modo remoto.
- Finaliza la instalación de Active Directory.

3.1.4.3. Directivas para la políticas de seguridad en el dominio

Como políticas de seguridad dentro del dominio se establece las directivas de contraseña, Directiva de Bloqueo de cuentas. En Directivas Locales tenemos políticas para Directivas de Auditoria, Directivas de Asignación de Derechos de Usuario, opciones de Seguridad.

- **Directivas de Cuentas:**

Directiva	Configuración
Almacenar contraseña usando cifrado de todos los usuarios del domino	Deshabilitada
Forzar el historial de contraseñas	6 Contraseñas recordadas
Las contraseñas deben cumplir el requisito de complejidad	Habilitada
Longitud mínima de contraseña	8 Caracteres
Vigencia máxima de contraseña	42 Días
Vigencia mínima de contraseña	2 Días

Tabla Nº 54 DIRECTIVAS DE CUENTAS
Fuente: Elaborada por los Autores

- **Directivas de Bloqueo de Cuentas**:

Directiva	Configuración
Duración del bloqueo de cuentas	30 Minutos
Restablecer la cuenta de bloqueos después de	30 Minutos
Umbral de bloqueos de cuenta	3 Intentos incorrectos

Tabla Nº 55 DIRECTIVAS DE BLOQUEO DE CUENTAS
Fuente: Elaborada por los Autores

Directivas Locales.

- **Directivas de Auditoria:**

Directiva	Configuración
Auditar el acceso a objetos	Erróneo
Auditar el acceso de servicios de directorio	Erróneo
Auditar el cambio de directivas	Correcto, erróneo
Auditar el uso de privilegios	Erróneo
Auditar la administración de cuentas	Correcto, Erróneo
Auditar sucesos de inicio de sesión	Erróneo
Auditar de inicio de cuenta de sesión	Erróneo
Auditar sucesos del sistema	Erróneo

Tabla Nº 56 DIRECTIVAS DE AUDITORIA
Fuente: Elaborada por los Autores

- **Directivas de Asignación de Derecho de Usuario:**

Directiva	Configuración
Agregar las estaciones de trabajo	Administradores
Backup de archivos y directorios	Administradores
Denegar el acceso desde la red a este equipo	Administradores
Denegar el inicio de sesión localmente	Administradores
Incremento de cuotas	Administradores
Inicio de sesión local	Administradores
Carga y descarga driver de dispositivos	Administradores
Restaurar archivos y directorios	Administradores
Apagar el sistema	Administradores

Tabla Nº 57 DIRECTIVAS DE ASIGNACION DE DERECHOS DE USUARIO
Fuente: Elaborada por los Autores

- **Opciones de Seguridad.**

Directiva	Configuración
Cerrar automáticamente la sesión de los usuarios cuando termine el tiempo de sesión local	Habilitada.
Deshabilitar el requisito de presionar CTRL+ALT+SUPR para iniciar sesión.	Deshabilitar.
Impedir mantenimiento de la contraseña de la cuenta de equipo	Deshabilitar.
Impedir que los instalen controladoras de impresoras	Habilitado.
No mostrar el último nombre de usuario en la pantalla de inicio de sesión.	Habilitado.
Numero de inicio de sesión en la cache (en casos en que el controlador de dominio este no disponible).	0 Inicio de sesión.
Pedir al usuario Cambiara contraseña antes de que caduque.	10 días.
Permite apagar el sistema antes que inicie la sesión.	Deshabilitada.
Restringir el acceso al CD-ROM solo al usuario con sesión iniciada localmente	Habilitada.
Restringir el acceso a la Unidad de diskette solo al usuario con sesión iniciada localmente	Habilitada.
Tiempo de inactividad requerido antes desconectar la sesión.	15 Minutos
Título de mensajes para los usuarios que intenten conectarse	Todo Intento de Validación quedara registrado, por favor abstenerse de hacerlo.

Tabla Nº 58 DIRECTIVAS DE SEGURIDAD
Fuente: Elaborada por los Autores

3.1.4.4. Directivas para instalación y configuración DHCP

- Asignación de nombre al ámbito:
  Nombre del ámbito: hospitalchancay
  Descripción: ámbito hospitalchancay
- Definir intervalos de dirección IP de DHCP para cada ámbito: se usan red para las diferentes aéreas.
  A partir de 192.168.1.11
- Agregar intervalos de exclusión IP: 192.168.1.1 – 192.168.1.10
- Establecer la Duración de la concesión: 12 días.
- Determinar la puerta de enlace: 192.168.1.1
- Especificamos la IP del servidor DNS: 192.168.1.2
- En la consola Activa el ámbito.
- Finalización del asistente.

3.1.4.5. Directivas instalación y configuración de servicios de correo

Para la instalación y configuración utilizaremos los servicios POP3

En servidor:

- **Nombre del servidor:** SRV3_Correo/web**.**
- **Tipo de servidor:** integrado a Active Directory.
- **Dominio de trabajo con POP3:** server02.hospitalchancay.gob.pe
- **Tipo de Buzón:** asociado para el usuario del buzón.

En Outlook:

- **Nombre de Usuario:** Administrador
- **Dirección de Correo Electrónico:** nombre-administrador@ server02.hospitalchancay.gob.pe
- **Servidor de correo entrante:** servidor-ad
- **Servidor de correo:** servidor-ad

Servidor Web:

Para la configuración de este servidor se instaló el servicio de internet Information Services, el cual nos permitirá que actuara como el servidor web de la intranet del hospital.

- Se creó un sitio web:
  Descripción: página web
- Dirección IP y configuración de puerto:
  Dirección IP: 192.168.1.4
  Puerto TCP: 80
  Encabezado de host: www.hospitalchancay.gob.pe
- Directorio particular para el sitio web:
  C:\Inetpub\wwwrot\PaginaWeb
- Permisos de Acceso:
  Leer
  Ejecutar sentencia de comando
  El objetivo de tener un servidor web y salida al internet es para alojar sus páginas y tener mayor ventaja competitiva con el resto de empresas.

3.1.4.6. Directivas para instalación y configuración del proxy/firewall

Para la configuración de nuestro servidor Proxy/Firewall, se ha hecho uso de Microsoft Internet Security and Acceleration Server 2006(ISA SERVER 2006).

A continuación mostramos las directivas para poder instalar y configurar el firewall:

- Configurar 2 tarjetas de red en el servidor (entrada/salida) en el servidor proxy
- Establecer el rango de IP'S de la red interna 192.168.1.1 hasta 192.168.1.254
- Establecer las siguiente reglas de acceso a la red:
- Creando una regla de acceso de permiso para todos los usuario en todo momento.

Ficha	Propiedad	Configuración
General	Descripción	Permite el acceso no restringido a internet a todos los usuarios
General	Habilitar	Seleccionado
Protocolos	Se aplica	Protocolo seleccionados: HTTP HTTPS
De	Se aplica al tráfico de estos orígenes	Red internet.
Ficha	Propiedad	Configuración
De	Excepciones	ninguno
A	Se aplica al tráfico a estos destino	Red externa (internet)
A	Excepciones	Ninguna
Usuarios	Se aplica a las peticiones de los siguientes conjuntos de usuarios	Todos los usuarios
Usuarios	Excepciones	Ninguna
Programación	Programaciones	Ninguna
Tipos de contenido	Se aplica a: todos los tipos de contenido. Tipos de contenido seleccionado	Todos los tipos de contenidos

Tabla Nº 59 REGLA DE ACCESO DE PERMISO A LOS USUARIOS
Fuente: Elaborada por los Autores

- Creando una regla de acceso de denegación para el personal de la red interna.

Ficha	Propiedad	Configuración
General	Nombre	Regla de denegación de acceso a internet desde la red interna
General	Descripción	Permite el acceso a internet desde la red interna, excepto a sitios específicos.
General	Habilitar	Seleccionado
Acción	Permitir/denegar	Denegar
Protocolos	Esta regla se aplica a	Protocolo seleccionados: HTTP HTTPS FTP
De	Se aplica al tráfico de estos orígenes	Red internet.
Ficha	Propiedad	Configuración
De	Excepciones	ninguno
A	Se aplica al tráfico enviado a estos destino	Red externa (internet)
A	Excepciones	El conjunto de direcciones URL de los sitios permitidos durante la jornada laboral
Usuarios	Excepciones	El conjunto de direcciones URL de los sitios permitidos durante la jornada laboral
Programación	Programación	Jornada Laboral
Tipos de contenido	Se aplica a: todos los tipos de contenido.	Todos los tipos de contenidos

Tabla Nº 60 REGLA DE ACCESO DE DENEGACIÓN PARA EL PERSONAL
Fuente: Elaborada por los Autores

3.1.4.7. Directivas para instalación y configuración del servicio de archivos

Para configuración de este servidor se configuro para que proporcione el servicio de compartir documentos, archivos y datos en toda la red. Aplicando las políticas de quotas de disco se controlara el uso eficiente a un espacio máximo de 2 GB para cada usuario, 50 GB para el sistema operativo y 50 Gb para las

aplicaciones. Los permisos asignados a los usuarios de la red, organizados en grupos para las carpetas compartidas.

Consideramos la instalación y conexión de los equipos que forman parte de la Red.

3.1.4.8. Instalación Windows Server 2012

Usaremos una máquina virtual para fines netamente ilustrativos ya que el presente proyecto aún no recibe el presupuesto solicitado, al Gobierno Regional de Lima Provincias para su implementación.

Pasos a Seguir

- ✓ Conecte el equipo a la red con un cable de red.
- ✓ Encienda el equipo y, a continuación, inserte el DVD de Windows Server 2012.
- ✓ Cuando aparezca el mensaje Presione cualquier tecla para iniciar desde el CD o el DVD, presione una tecla.
- ✓ Seleccione el Idioma de la instalación, el Formato de hora y moneda y el Teclado o método de entrada y, a continuación, haga clic en Siguiente.

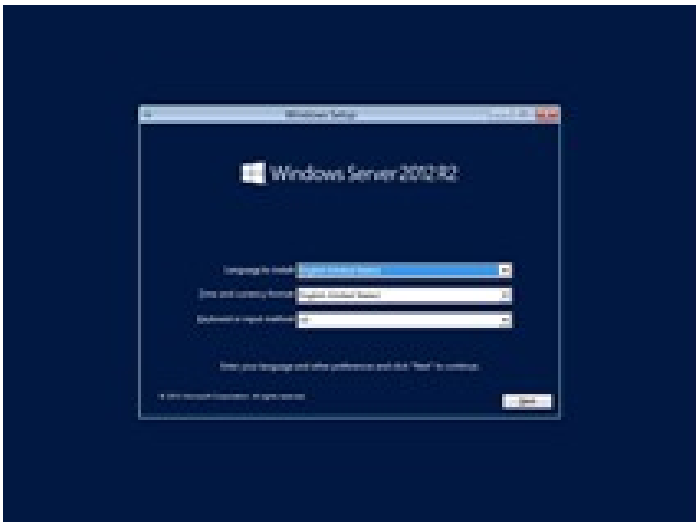


FIGURA N° 35 INSTALACION DE WINDOWS SERVER 2012
Fuente: Propia de los Autores

- ✓ Haga clic en Instalar ahora.
- ✓ Cuando le solicite la clave del producto, escriba la clave del producto.

- ✓ Lea los Términos de licencia. Si los acepta, active la casilla Acepto los términos de licencia y, a continuación, haga clic en Siguiente.
- ✓ Haga Clic en Instalación Personalizada: instalar solo Windows (avanzado).
- ✓ Seleccione la unidad de disco duro donde desea instalar el sistema operativo Windows. Compruebe que todas las unidades de disco duro internas estén disponibles para la instalación. (Para crear una partición a partir de un espacio sin particionar, haga clic en el disco duro que desea particionar, haga clic en Opciones de unidad (avanzadas), haga clic en Nuevo y, a continuación, en el cuadro de texto Tamaño, escriba la partición que desea crear. Por ejemplo, si utiliza el tamaño de partición recomendado de 120 gigabytes (GB), escriba 122880 y, a continuación, haga clic en Aplicar. Una vez creada la partición, haga clic en Siguiente. La partición se formatea antes de continuar la instalación).
- ✓ Una vez terminada la instalación el Sistema Operativo estará listo para configurar.

3.1.4.8.1. Configuración de Windows Server 2012

- ✓ Compruebe la configuración de fecha y hora, si la fecha y hora coincidiera así como la zona horaria no es necesario configurarlo.
- ✓ En la página Elegir el modo de instalación del servidor, realice lo siguiente, elija Instalación limpia para configurar una instalación completamente nueva del software de servidor de Windows Server 2012.
- ✓ En la página Personalice el servidor, escriba el nombre de la organización, un nombre del dominio interno y el nombre del servidor, haga clic en siguiente.

- ✓ En la página Especifique la información de la cuenta de administrador, escriba la información de una nueva cuenta de administrador.
- ✓ En la página Especifique la información de su cuenta de usuario estándar, escriba la información de una nueva cuenta de usuario estándar y, a continuación, haga clic en Siguiente.
- ✓ En la página Mantenga el servidor actualizado automáticamente, seleccione cómo desea recibir actualizaciones de Windows para el servidor y, a continuación, haga clic en Siguiente.
- ✓ La página Actualizar y preparar el servidor muestra el progreso del proceso final de instalación. Esta operación tarda tiempo en realizarse, y el equipo se reiniciará un par de veces.
- ✓ Al finalizar el último reinicio del servidor, aparece la página El servidor está listo para utilizarse. Haga clic en Cerrar.
- ✓ Haga clic en el icono Panel de la pantalla Inicio y, a continuación, en el Panel, realice las tareas de Configurar el servidor en la página Inicio. Estas tareas se deben realizar inmediatamente tras finalizar la instalación de Windows Server 2012.

En la siguiente tabla se definen algunos elementos a tener en cuenta para las tareas de configuración.

TAREA	DESCRIPCIÓN
Obtener actualizaciones para otros productos de Microsoft	Haga clic en esta tarea para tener acceso a un vínculo que ejecuta una herramienta que le permite especificar si desea usar Microsoft Update para obtener automáticamente actualizaciones para Windows Server 2012 Essentials y otros productos de Microsoft como Office.
Agregar cuentas de usuario	Haga clic en esta tarea para ver información breve acerca de cómo agregar cuentas de usuario. Se proporciona un vínculo al **Asistente para agregar cuentas de usuario**. Para obtener más información, vea cómo agregar una cuenta de usuario.
Agregar carpetas de servidor	Haga clic en esta tarea para ver información breve acerca de cómo agregar carpetas de servidor. Se proporciona un vínculo al **Asistente para agregar carpetas**. También se proporciona un vínculo a un tema de ayuda en pantalla acerca del uso de carpetas de servidor. Para obtener más información, vea cómo agregar o mover una carpeta del servidor.
Configurar copia de seguridad del servidor	Haga clic en esta tarea para ver información breve acerca del uso de Copia de seguridad del servidor para proteger sus datos. Se proporciona un vínculo al **Asistente para configuración de copia de seguridad del servidor**. Para obtener más información, vea cómo configurar o personalizar una copia de seguridad del servidor.
Configurar Acceso desde cualquier lugar	Haga clic en esta tarea para ver información breve sobre la característica Acceso desde cualquier lugar de Windows Server 2012 Essentials. Se proporciona un vínculo a la página **Configuración de Acceso desde cualquier lugar**. Para obtener más información, vea cómo Administrar Acceso desde cualquier lugar en Windows Server Essentials.
Configurar notificación de alertas por correo electrónico	Haga clic en esta tarea para ver información breve acerca de la notificación de alertas por correo electrónico. Se proporciona un vínculo a la herramienta **Configurar notificación de alertas por correo electrónico**. Para obtener más información, vea cómo configurar las

	notificaciones de correo electrónico para recibir alertas.
Configurar el servidor multimedia	Haga clic en esta tarea para ver información breve acerca del uso del servidor multimedia para compartir archivos de música, de vídeo y de imagen. Se proporciona un vínculo a la página **Configuración de medios**. También se proporciona un vínculo a un tema de ayuda en pantalla para obtener más información acerca del servidor multimedia. Para obtener más información, vea cómo Administrar medios digitales en Windows Server 2012 Essentials.
Conectar los equipos	Haga clic en esta tarea para ver información breve acerca de cómo conectar un equipo de red al servidor. Para obtener más información, consulte Conectar los equipos al servidor

Tabla Nº 61 TAREAS DE CONFIGURACION A TENER EN CUENTAS
Fuente: Elaborada por los Autores

CAPITULO IV

DISCUSIÓN DE LA HIPOTESIS

Para la contrastación de la hipótesis se ha considerado lo siguiente:

Formulación del Problema:

¿Cómo mejorar la comunicación y seguridad de la información en el Hospital Chancay utilizando tecnología de la información?

Hipótesis:

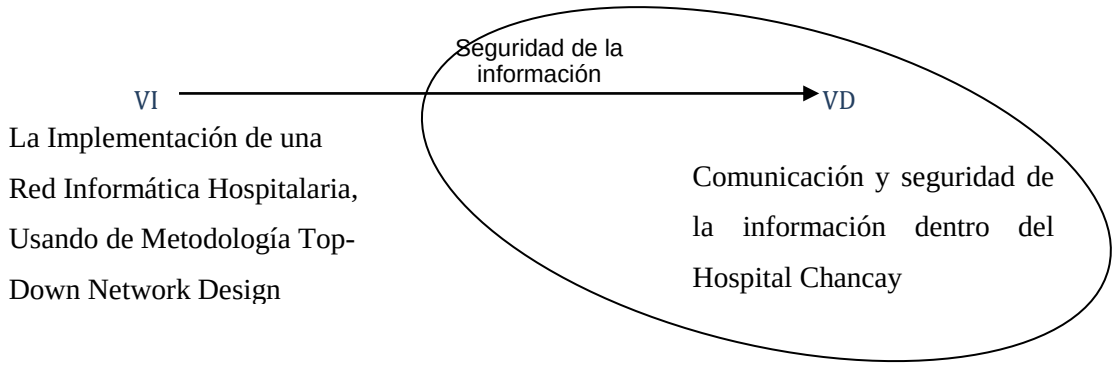
La Implementación de una Red Informática Hospitalaria, Usando de Metodología Top-Down Network Design mejorará la comunicación y seguridad de la información dentro del Hospital Chancay y Servicios Básicos de Salud.

Luego se definen las variables que intervienen en la veracidad o falsedad de la hipótesis:

- Variable Independiente (VI): La Implementación de una Red Informática Hospitalaria, Usando de Metodología Top-Down Network Design

- Variable Dependiente (VD): comunicación y seguridad de la información dentro del Hospital Chancay.

MANERA PRESENCIAL



Para la comprobación de la hipótesis se realizó lo siguiente, los datos obtenidos fueron usando la red actual y simulando el comportamiento de la red que se piensa implementar:

- ✓ Se tomó los tiempos que demoran los usuarios en acceder, transferir y la duración de sus transferencias haciendo uso de la red ya sea en la Intranet e Internet.
- ✓ Se tomó el tiempo que demoran los usuarios en obtener respuesta de las diferentes áreas de la institución.

Comprobación de Hipótesis			
Acceso a la información en las Áreas	**Red Actual (Segundos)**	**Simulador (Segundos)**	**Ahorro (Segundos)**
Dirección General	9,53	2,16	7,37
Oficinas de Administración	25,92	9,25	16,67
Oficina de Computo	11.96	6.50	5.46
Oficina de Estadística	16,93	1,18	15,75
Oficina de Planeamiento	26,36	3,29	23,07
Oficina de S.G.	36,42	6,23	30,19
Tópico	20.00	6,06	13,94
Farmacia	19,3	6,32	12,98
Admisión	22,35	8,32	24,03
Hospitalización Materno	29,4	6,2	23,2
Servicio de Emergencia	10.0	3.0	7.0
Hospitalización	45,84	4,49	41,35
Total (seg)	**274,01**	**63**	**211.01**

Tabla Nº 62 COMPROBACIÓN DE HIPOTESIS
Fuente: Elaborada por los Autores

Comprobación de Hipótesis			
Actividades	**Red Actual (Segundos)**	**Simulador (Segundos)**	**Ahorro (Segundos)**
Avg. Transfer Duration	5,47	1,83	3,64
Avg. Cache Hit Duration	0,07	0,01	0,06
Avg. Cache Miss Duration	9,09	3,44	5,65
Total (Segundos)	**14,63**	**5,28**	**9,35**

Tabla Nº 63 COMPROBACIÓN DE HIPOTESIS
Fuente: Elaborada por los Autores

Prueba Estadística

Para verificar la comprobación de la hipótesis se aplicará la prueba estadística t – Student que se puede describir como aquella que se utiliza en un modelo en el que una variable explicativa (var. independiente) intenta explicar una variable respuesta (var. dependiente) con el fin de evaluar el tiempo de respuesta de acceso antes y después de las pruebas de laboratorio.

Así tenemos que la hipótesis estadística es la siguiente:

Ho: $\mu_a > \mu_d$

Ha: $\mu_a \leq \mu_d$

Siendo:

μ_a : La media antes de las pruebas de laboratorio propuesta en el diseño.

μ_d: La media después de las pruebas de laboratorio propuesta en el diseño.

La fórmula que se va a utilizar es la siguiente:

$$t = \frac{\overline{X_a} - \overline{X_d}}{\sqrt{\frac{S_a^2}{N_a} + \frac{S_d^2}{N_d}}}$$

Siendo:

$\overline{X_a}$: El promedio de los tiempos antes de las pruebas de laboratorio propuesta en el diseño, habiendo obtenido el valor de 27,401.

$\overline{X_d}$: El promedio de los tiempos después de las pruebas de laboratorio propuesta en el diseño, habiendo obtenido el valor de 6,3.

S_a^2 : La varianza de los tiempos antes de las pruebas de laboratorio propuesta en el diseño, habiendo obtenido el valor de 107,614.

S_d^2 : La varianza de los tiempos después de las pruebas de laboratorio propuesta en el diseño, habiendo obtenido el valor de 12,917.

N_a : La cantidad de tiempos antes de las pruebas de laboratorio propuesta en el diseño, habiendo obtenido el valor de 10.

N_d : La cantidad de tiempos después de las pruebas de laboratorio propuesta en el diseño, habiendo obtenido el valor de 10.

Tenemos X_{ai} que representa los tiempos antes de pruebas de laboratorio propuesta en el diseño tal que X_{ai} = {9.53, 25.92, 45.84, 16.93, 26.36, 36.42, 31.96, 19.3, 32.35, 29.4}, para un valor de i desde 1 hasta 10 y X_{dj} que representa los tiempos después de las pruebas de laboratorio propuesta en el diseño tal que X_{dj} = {2.16, 9.25, 4.49, 1.18, 3.29, 9.23, 12.56, 6.32, 8.32, 6.2}, para un valor de i desde 1 hasta 10.

Calculando se obtiene un valor de t = 6,07

El valor tabular de t al 95% de confianza con 9 grados de libertad es: 1.833, obteniéndose el siguiente gráfico:

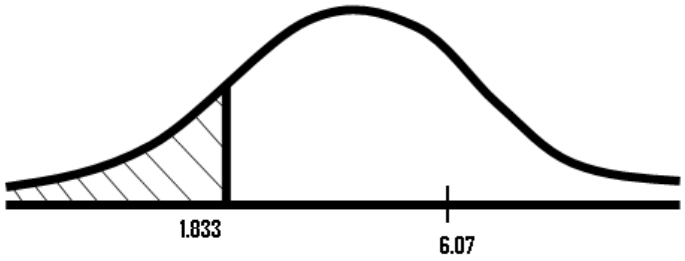


Figura. Nº 36 DISTRIBUCIÓN T
Fuente: Elaborada por los Autores

Del gráfico se puede observarse que el valor calculado es mayor que el valor tabular ubicándose en la zona de aceptación, por lo que se acepta Ho: $\mu_a > \mu_d$ comprobándose estadísticamente que la media de los tiempos antes de las pruebas de laboratorio propuesta en el diseño es mayor que la media de los tiempos después de las pruebas de laboratorio, con lo cual podemos afirmar que la hipótesis cumple con los requisitos propuesto en el diseño.

V. CONCLUSIONES

1. Se documentó la realidad técnica problemática por la viene atravesando el Hospital Chancay y Servicios Básicos de Salud, con respecto a la trasmisión de información entre sus diversas Áreas, Departamentos, Unidades y Servicios.
2. Se analizaron e identificaron y documentaron, las necesidades y requerimientos de los usuarios a través de técnicas de recopilación de información (lluvia de ideas), donde participaron activamente los trabajadores del Hospital Chancay y Servicios Básicos de Salud.
3. Se realizó el inventario de la red existente, permitiéndonos, determinar hardware, software, materiales y herramientas informáticas existentes en el Hospital de Chancay: 37 Laptop, 132 Computadores, 35 Impresoras Láser, 28 Impresoras de Punto FX 890, 87 Licencias de Windows XP, 38 Licencias de Windows 7 Starter, 7 Licencias Windows 8, 123 Licencias de Microsoft Office 2010, 2 Lan Tester, 5 Multitester, 2 Estaciones de Soldadura, 3 Juegos de Destornilladores.
4. El diseño lógico de la red nos permitió determinar la necesidad de Servidores y Dispositivos de comunicación de red: 3 Servidores, 1 Switch Core, 2 Switch Distribución, 13 Switch de Acceso y 3 Modem.
5. Se elaboró el diseño físico de red tomando en cuenta la norma técnica peruana NTP-ISO/IEC 17799:2007 EDI, permitiendo la distribución y administración en la comunicación de equipos, estableciendo 6 Directivas de Contraseña, 3 Directivas de Bloqueo de Cuentas, 8 Directivas de Auditoria, 9 Directivas de Derecho de Usuario y 12 Directivas de Seguridad.
6. Se estableció el plan de implementación para los servicios de red como: DNS, DHCP, DA, SERVICOS DE CORREO y FIREWALL/PROXY de seguridad basado en ISA SERVER 2006.
7. El uso de la metodología Top Down Network Design, nos garantiza, el éxito de la implementación de la Red Informática Hospitalaria, beneficiándose ampliamente el Hospital Chancay, que solucionará su problema de seguridad y rapidez en la trasmisión de su información entre sus diversas Unidades, Áreas, Departamentos, y Servicios.

VI. RECOMENDACIONES

1. Se recomienda a la Oficina de Planeamiento e Inversión (OPI), gestionar los recursos, ante las instituciones encargadas de brindar el financiamiento, para cristalizar este proyecto en beneficio del Hospital Chancay y Servicios Básicos de Salud.

2. Para una aplicación exitosa de las directivas de la norma NTP-ISO/IEC 17799-2007 se recomienda capacitar al personal que utiliza y administra la red, debiendo llevarse a cabo, capacitaciones constantes durante el periodo de transición, con la finalidad de que los usuarios asimilen los cambios que surgirán al culminar el proyecto.

3. Poner en práctica los controles de seguridad y las directivas propuestas en este trabajo, para evitar los incidentes de seguridad, garantizando el desempeño y funcionamiento óptimo de la red.

4. Realizar periódicamente pruebas de funcionalidad entre cliente y servidor en todo el sistema para garantizar una correcta acción preventiva, asegurando la disponibilidad y performance.

5. Impulsar la necesidad de documentar el historial técnico de cada componente de la Red Informática Hospitalaria, fuente esencial para un correcto seguimiento del Plan de Mantenimiento programado a cada uno de los equipos.

6. Fomentar la implementación de nuevas tecnologías en la infraestructura de la red Informática Hospitalaria como: Telefonía Ip, ya que no implicara grandes modificaciones en su estructura física.

VII. REFERENCIAS BIBLIOGRÁFICAS

1. Wikipedia, Agosto 2013;"IEEE Instituto de Ingenieros Eléctricos y Electrónicos" [En Línea] Disponible en: http://es.wikipedia.org/wiki/ieee
2. Top-Down-Network-Design-3rd-Edition, Enero 2013; [En Línea] Disponible en: http://www.valleytalk.org/wp-content/uploads/2013/01/top-down-network-design-3rd-edition.pdf
3. Redes de Datos, Agosto 2008; "Ing. José Joskowicz; Instituto de Ingeniería Eléctrica, Facultad de Ingeniería, Universidad de la República Montevideo, Uruguay [En Linea] Disponible en: http://iie.fing.edu.uy/ense/asign/redcorp/material/2008/Redes%20de%20Datos%202008.pdf
4. Wikipedia, 20 Noviembre 2013; "Red de Computadoras"[En Línea] Disponible en: http://es.wikipedia.org/wiki/Red_de_computadoras
5. Wikipedia, Noviembre 2014; "Servidores"[En Línea] Disponible en: http://es.wikipedia.org/wiki/Servidor
6. Wikipedia, Noviembre 2014; "Modelo_OSI"[En Línea] Disponible en: http://es.wikipedia.org/wiki/Modelo_OSI
7. Wikipedia, Noviembre 2014; "Modelo_TCP/IP"[En Línea] Disponible en: http://es.wikipedia.org/?title=Modelo_TCP/IP
8. Wikipedia, Noviembre 2014; "WI-FI"[En Línea] Disponible en: http://es.wikipedia.org/wiki/Wi-Fi
9. Wikipedia, Octubre 2013; "Windows_Server_2012" [En Línea] Disponible en: http://es.wikipedia.org/wiki/Windows_Server_2012
10. Cisco Press& Priscilla Oppenheimer, Agosto 2010; Top-Down Network Design, Tercera Edición.
11. Redes de Datos, Noviembre 2014; "Redes de Datos" [En Línea] Disponible en: http://definicion.de/red-de-datos/#ixzz2yJ4vNPov
12. Wikitel Info, Octubre 2014; "Redes de Datos" [En Línea] Disponible en: http://wikitel.info/wiki/Redes_de_datos

ANEXOS

ANEXO A

IMÁGENES DEL ESTADO DEL CABLEADO DE LAS INTALACIONES

Figura. Nº 37 SERVIDORES HP-G6
Fuente: Propia de los Autores

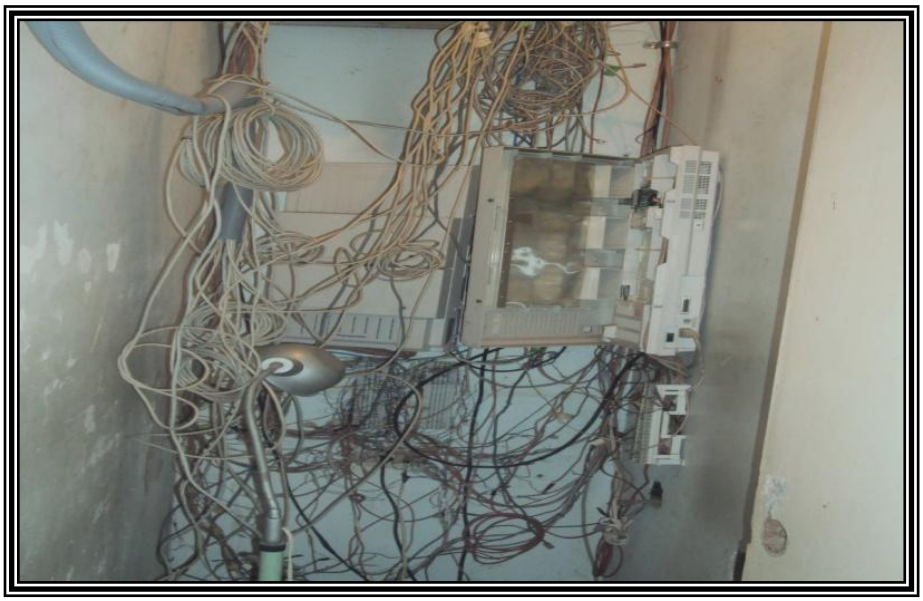


Figura. Nº 38 CENTRAL DE COMUNICACIONES
Fuente: Propia de los Autores

ANEXO A

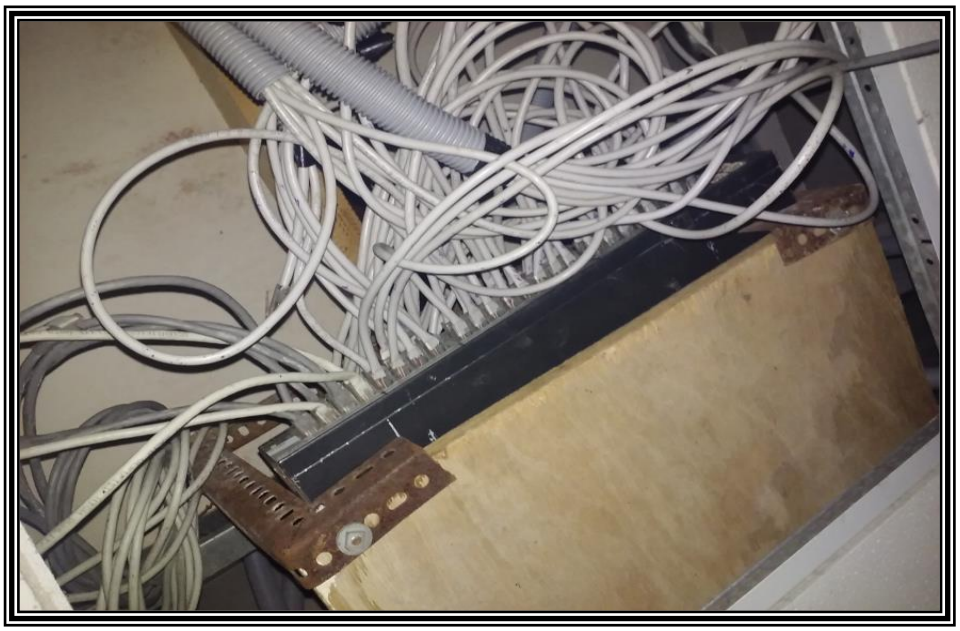


Figura. Nº 39 SWICHT AREA DE COMUNICACIONES
Fuente: Propia de los Autores

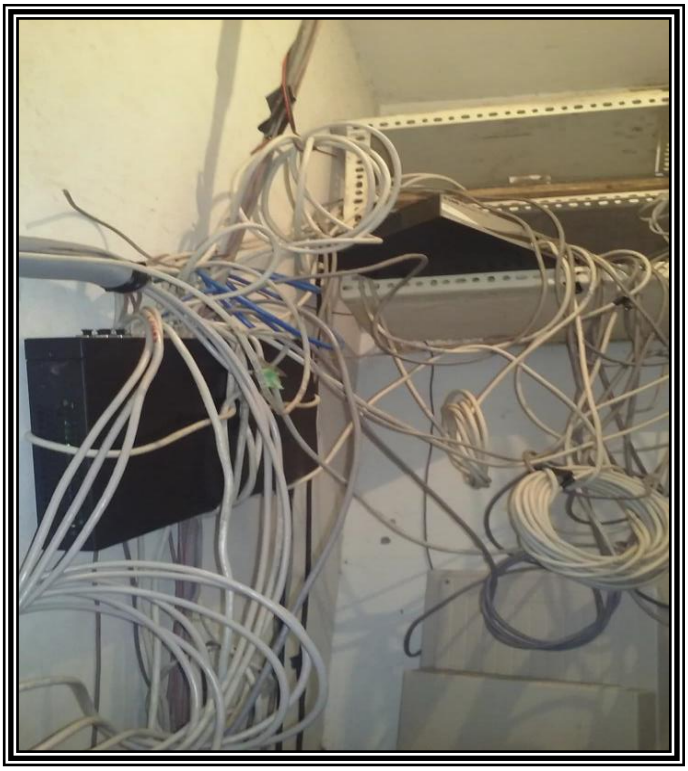


Figura. Nº 40 SWICHT AREA DE ALMACEN
Fuente: Propia de los Autores