# UNIVERSIDAD PRIVADA ANTENOR ORREGO

# FACULTAD DE INGENIERÍA

**ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS**


## DISEÑO DE UNA RED DE DATOS PARA EL POLICLINICO SEÑOR DE LOS MILAGROS S.R.L. USANDO METODOLOGÍA TOP DOWN NETWORK DESIGN Y APLICANDO ESTÁNDARES ISO/IEC 27002

**TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO DE COMPUTACIÓN Y SISTEMAS**

ÁREA DE INVESTIGACIÓN:

REDES

**AUTORES:**

Br. GUEVARA PÉREZ, OBED

Br. MIRANDA ZELADA, ARNOLD ANTONIO

**ASESOR:**

ING. JOSÉ MANUEL RODRÍGUEZ MANTILLA

TRUJILLO-PERU
2014

**UNIVERSIDAD PRIVADA ANTENOR ORREGO**

**FACULTAD DE INGENIERÍA**

**ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS**

**TESIS:** **DISEÑO DE UNA RED DE DATOS PARA EL POLICLINICO SEÑOR DE LOS MILAGROS S.R.L. USANDO METODOLOGÍA TOP DOWN NETWORK DESIGN Y APLICANDO ESTÁNDARES ISO/IEC 27002.**

_____

**PRESIDENTE**
Dr. LUIS VLADIMIR URRELO HUIMAN
CIP: 88212

| | |
|---|---|
| **SECRETARIO** | **VOCAL** |
| ING. KARLA MELENDEZ REVILLA | ING. ALBERTIS FLORIAN VIGO |
| CIP: 120097 | CIP: 114879 |

_____

**ASESOR**
ING. JOSÉ RODRIGUEZ MANTILLA
CIP: 139579

# PRESENTACIÓN

**Señores Miembros del Jurado:**

Cumpliendo con los requisitos estipulados en el reglamento de Grados y Títulos de la Universidad Privada Antenor Orrego, para optar el Título de Ingeniero de Computación y Sistemas, sometemos a vuestra consideración la tesis titulada: "**DISEÑO DE UNA RED DE DATOS PARA EL POLICLINICO SEÑOR DE LOS MILAGROS S.R.L. USANDO METODOLOGÍA TOP DOWN NETWORK DESIGN Y APLICANDO ESTÁNDARES ISO/IEC 27002**".

La presente tesis, es el resultado de nuestro esfuerzo, donde hemos plasmado todos los conocimientos y experiencias adquiridas a lo largo de nuestra formación profesional, complementando además con la orientación y apoyo de nuestro asesor y todas aquellas personas que nos aconsejaron y guiaron durante el desarrollo del presente trabajo.

Muy a pesar de todo el entusiasmo y esfuerzo que pusimos para poder alcanzar los objetivos planteados, somos conscientes de que el presente trabajo pudiera tener algunas imperfecciones, por lo cual, invocamos a vuestra comprensión para saber dispensar cualquier error involuntario en el cual pudiéramos haber incurrido.

Los Autores.

**Br. Guevara Pérez Obed** **Br. Miranda Zelada Arnold**

# DEDICATORIA

***A Dios***.
*Por haberme permitido llegar*
*hasta este punto y haberme dado*
*la oportunidad para lograr mis objetivos,*
*conforme a sus propósitos.*

***A nuestros Padres***

*Por la motivación constante*
*que nos han permitido ser unas personas*
*de bien, por los ejemplos*
*de perseverancia y constancia*
*que nos han infundado siempre, por*
*el valor mostrado para salir*
*adelante, pero más que nada, por su amor.*

***A nuestro querido profesor***

*Ing. José Manuel Rodríguez Mantilla, por su apoyo y*
*guía constante en la elaboración y*
*culminación de la presente investigación.*

***Antonio y Obet***

## AGRADECIMIENTO

Al concluir el presente trabajo deseamos expresar nuestro más sincero agradecimiento a quienes hicieron posible la culminación del mismo. A mis familiares y amigos, quienes contribuyeron en nuestra realización profesional y personal. De manera especial a: Dr. Luis Vladimir Urrelo por guiarnos de manera desinteresada en el desarrollo del trabajo de investigación.

Sirva esta oportunidad para testimoniarle el reconocimiento y gratitud a todos los docentes de la Facultad de Ingeniería de Computación y Sistemas de la Universidad Privada Antenor Orrego , que con sus enseñanzas, esfuerzos y sabios consejos contribuyeron a la formación profesional y hacer realidad nuestro propósito de ser profesionales.

Atentamente,

Los autores

## RESUMEN

**"Diseñar una red de datos para el Policlínico Señor de los Milagros SRL usando metodología Top Down Network Desing y aplicando estándares ISO/IEC 27002"**

**Por:**

**Br. Guevara Pérez Obed**

**Br. Miranda Zelada Arnold Antonio**

El Policlínico Señor de Los Milagros se ubica en el Jirón Bolognesi 382 – 386 Trujillo - La Libertad, lleva en el mercado competitivo 16 años brindando servicio en diversas especialidades médicas y laboratorio entre otros. Cuenta con 10 trabajadores en las distintas áreas en la organización.

Actualmente la empresa no cuenta con una red de computadores en la que no se comparten recursos de hardware (impresoras) y software, esto genera demora en la impresión de documentos debido a que todo el laboratorio solo cuenta con una sola impresora.

Dado el siguiente problema se plantea hacer una red de datos con la metodología Diseñar una red de datos usando metodología Top Down Network Desing y aplicando estándares ISO/IEC 27002, que le permitirá interconectar los distintos consultorios que cuenta el laboratorio y además llevar una mejor administración e información de los pacientes, por ello con este proyecto queremos implantar una red de acuerdo a las necesidades que tiene el Policlínico.

Para dar seguridad de información a la empresa se requiere implementar un Estándar de seguridad mediante la Norma ISO 27002, dentro de los equipos que utilizaremos son: Servidores, switch, router, Access point, los cuáles serán configurados para ser administrados.

# ABSTRACT

**"Designing a data network to the Policlínico Señor de los Milagros SRL using Top Down Network Desing methodology and applying standards ISO / IEC 27002"**

**By:**

**Br. Guevara Pérez Obed**

**Br. Miranda Zelada Arnold**

The Policlínico Señor de los Milagros is located on Jiron Bolognesi 382-386 Trujillo - La Libertad, in the competitive market takes 16 years providing service in various medical and laboratory among others. It has 10 employees in different areas in the organization.

Actual mind the company does not have a computer network in which no hardware resources (printers ) and software sharing , this creates delay in printing documents because all the laboratory has only one printer .

Given the following problem to do a data network design methodology with a data network using Top Down Network Desing methodology and applying ISO / IEC 27002 standards, allowing you to interconnect the various locations available to the laboratory and also bring better management and patient information, so with this project we want to implement a network according to the need of the Polyclinic.

Those which will be configured to be managed Servers, switches, router, access point, To provide security for the company's ISO 27002 within the equipment we use are be used.

**INDICE**

**CAPÍTULO II. RESULTADOS**

# INDICE DE FIGURAS

## INDICE DE TABLAS

# INTRODUCCIÓN

El siguiente proyecto está orientado en el área de tecnología de información así como las diferentes tecnologías de comunicación de datos.

El Policlínico Señor de Los Milagros se ubica en el jirón Bolognesi 382 – 386 Trujillo - La Libertad, se dedica al servicio en diversas especialidades médicas y laboratorio entre otros. Se inició en este negocio desde el año 1997,

Actualmente El Policlínico Señor cuneta con un total de 8 computadoras, 1 impresora en el primer piso.

Además adolece de los siguientes problemas desde el punto de vista informático:

- Limitada comunicación entre sus consultorios para la compartición de información debido que no cuenta con acceso a una base de datos.
- La documentación se encuentra en archivos físicos por lo que se requiere un servidor que provea servicios de información a otras áreas.
- Desconocimiento de la importancia de la seguridad de información y requerimientos de implementar políticas de seguridad en la información.

Obteniendo como resultado el siguiente objetivo general; Diseñar una red de datos para el Policlínico Señor de los Milagros SRL usando metodología Topdown Network Desing y aplicando estándares ISO/IEC 27002 y los siguientes objetivos específicos:

- Identificar Objetivos y Necesidades del policlínico mediante entrevistas.
- Diseñar una red lógica aplicando la metodología Top Down Network Design.
- Diseñar un modelo de conectividad, según la metodología TOP DOWN NETWORK DESIGN.
- Establecer políticas de seguridad ISO/IEC 27002 (según el Dominio 5, Objetivo de Control 5.1; Controles 5.1.1; Dominio 7, Objetivo de Control 7.1, 7.2, Controles 7.1.1, 7.1.2; Dominio 11 y Objetivo de Control 11.1, 11.2, 11.4, 11.5; Controles 11.1.1, 11.2.3, 11.4.1, 11.4.6).

El presente trabajo de habilitación está compuesto por los siguientes capítulos:

**CAPÍTULO I FUDAMENTO TEÓRICO,** en este capítulo se describe los conceptos básicos y fundamentos de las diferentes tecnologías de las redes informáticas alambradas, asimismo se establece la normatividad o disposiciones que rigen para el diseño de una red utilizando el sistema de cableado estructurado así como la gestión de seguridad de la información a través de la Norma ISO.

**CAPÍTULO II RESULTADOS,** este capítulo documenta todo los resultados basados en la aplicación de la metodología Top Down, así mismo se detalla el beneficio de implementar la norma ISO 27002 en la Red para la administración de seguridad de la información de la empresa, veremos las tecnologías de redes, haciendo un estudio para encontrar las necesidades y requerimientos de nuestra LAN en concreto. En la segunda fase se abordara el diseño lógico de la red, luego el siguiente apartado se comenta con detalle todas las especificaciones y de los dispositivos que requiere la red para su posterior diseño realizando un análisis de los mismos para su elección, en función a las características y requerimientos técnicos establecidos; además se muestran las distintas alternativas que existen para la selección de los equipos físicos. También se estará realizando políticas de Seguridad de la Información  Y como último apartado se establece un plan de contingencia para soluciones a problemas de la red.

**Capítulo I**

# FUNDAMENTO TEORICO

## 1. MARCO TEORICO
## FUNDAMENTACIÓN TEÓRICA DE LA INVESTIGACIÓN

### 1.1 DEFINICIÓN DE MARCO DE TRABAJO

### 1.2 REDES DE COMPUTADORAS

Una red la constituyen dos o más ordenadores que comparten determinados recursos, sea hardware (impresoras, sistemas de almacenamiento) o sea software (aplicaciones, archivos, datos). Desde una perspectiva más comunicativa, podemos decir que existe una red cuando se encuentren involucrados un componente humano que comunica, un componente tecnológico (ordenadores, televisión, telecomunicaciones) y un componente administrativo (institución o instituciones que mantienen los servicios). En fin, una red, más que varios ordenadores conectados, la constituyen varias personas que solicitan, proporcionan e intercambian experiencias e informaciones a través de sistemas de comunicación (CISCO SYSTEMS, 2004).

### 1.3 DISEÑO FÍSICO

#### 1.3.2 TIPOS DE REDES

##### 1.3.2.1 REDES DE ÁREA LOCAL (LAN)

De acuerdo a Cisco System 2004, una Red de Área Local (Local Área Network - LAN) está constituida por computadoras, tarjetas de interfaz de red, dispositivos periféricos, medios de red y dispositivos de red.

Las LAN permiten a las empresas que emplean tecnologías de computación.

Las LAN están diseñadas para hacer lo siguiente:

- Operar dentro de una zona geográfica limitada.
- Permitir a muchos usuarios acceder a medios de gran ancho de banda.

- Proporcionar conectividad a tiempo completa a los servicios locales.
- Conectar físicamente dispositivos adyacentes.

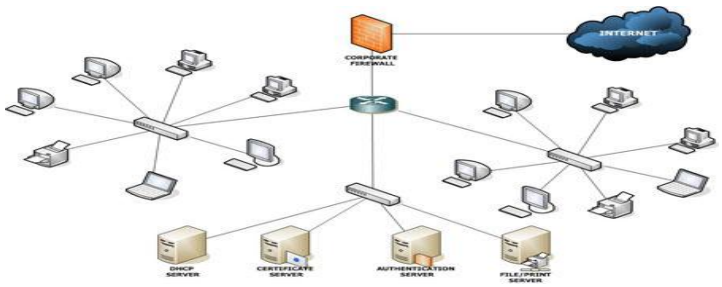



**Figura N° 1 Red LAN (Pcnet, 2011)**

#### 1.3.2.2 REDES DE ÁREA METROPOLITANA (MAN)

De acuerdo a Stallings (2004), como su propio nombre sugiere, las MAN (Metropolitana Área Network) están entre las LAN y las WAN. El interés en las MAN ha sugerido tras ponerse de manifiesto que las técnicas tradicionales de conmutación y conexiones punto a punto usadas en WAN, pueden ser no adecuadas para las necesidades crecientes de ciertas organizaciones.

Mientras que la retransmisión de tramas y ATM prometen satisfacer un amplio espectro de necesidades en cuanto a velocidades de transmisión, hay situaciones, tanto en redes privadas como públicas, que demandan gran capacidad a coste reducido en áreas relativamente grandes.

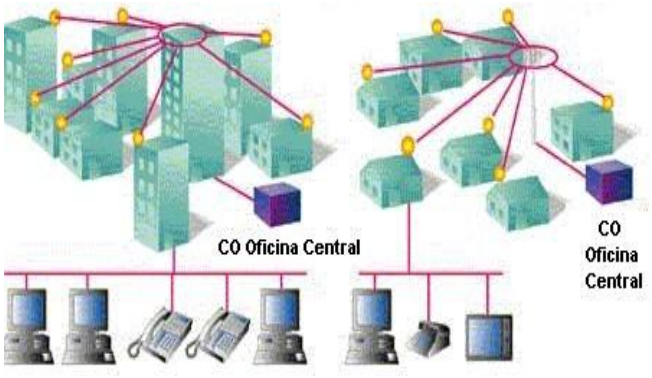



**Figura N° 2Red MAN (LOZANO, 2012)**

### 1.3.2.3 RED DE ÁREA AMPLIA (WAN)

Según Stallings (2004), considera como redes de área amplia a todas aquellas que cubren una extensa área geográfica, requiere atravesar rutas de acceso público y utilizan, al menos parcialmente, circuitos proporcionados por una entidad, proveedora de servicios de telecomunicación.

Generalmente, una WAN consiste en una serie de dispositivos de conmutación interconectados. La transmisión generada por cualquier dispositivo se encaminara a través de estos nodos internos hasta alcanzar el destino.

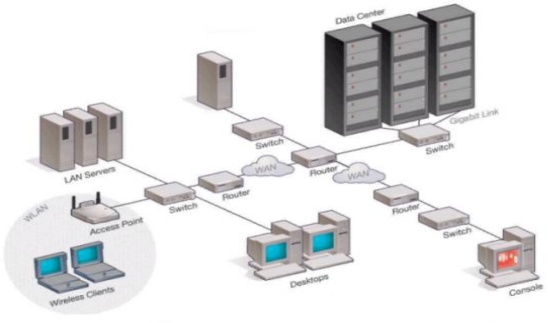



**Figura N° 3Red WAN(Rockalaglam, 2010)**

### 1.3.2.4 REDES INALÁMBRICAS

Según Tanenbaum (1997), puesto que tener una conexión por cable es imposible en autos y aeroplanos, existe mucho interés en las redes inalámbricas. Las computadoras pueden enviar mensajes como guardar registro, y otras cosas. Su capacidad de transmisión es de 1 a 2 Mbps, lo cual es mucho

más lento que las LAN alambradas. Además las tasas de error son mucho más altas y las transmisiones desde diferentes computadoras pueden interferirse.

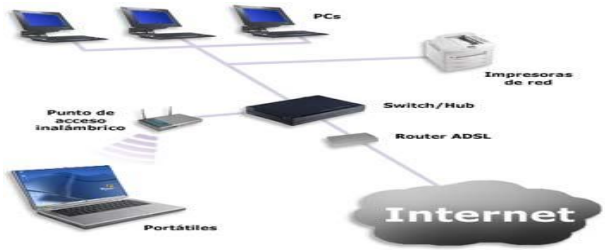



**Figura N° 4 Red Inalámbrica (Michaelcount, 2010)**

### 1.3.3 TOPOLOGÍAS DE REDES

Según Cisco Systems (2004), una topología de red define como están conectadas las computadoras, impresoras, dispositivos de red y otros dispositivos. En otras palabras, la topología define la distribución de los cables y los dispositivos, así como las rutas utilizadas para las transmisiones de datos.

La topología influye enormemente en el funcionamiento de la red, depende de esta la flexibilidad y performance de la red.

Las redes pueden tener una topología física y una topología lógica. La Topología física se refiere a la disposición física de los dispositivos y los medios. Las Topologías físicas más comunes son las siguientes: Bus, Anillo y Estrella. La topología lógica define como acceden los hosts a los medios para enviar datos.

#### 1.3.3.1 TOPOLOGÍA BUS

En una topología bus todas las computadoras en la red comparten el mismo canal de comunicaciones, toda la información circula por ese canal una de ellas recoge la información que le corresponde. Esta estructura es frecuente en las redes de área local.

En una configuración es relativamente fácil controlar el flujo de tráfico entre los distintos equipos, ya que el bus permite

que todas las estaciones reciban todas las transmisiones, es decir una estación puede difundir la información a todas las demás.

La principal limitación de una topología de bus está en el hecho de que suele existir un solo canal de comunicaciones para todos los dispositivos de la red. En consecuencia, si el canal de comunicaciones falla toda la red deja de funcionar.

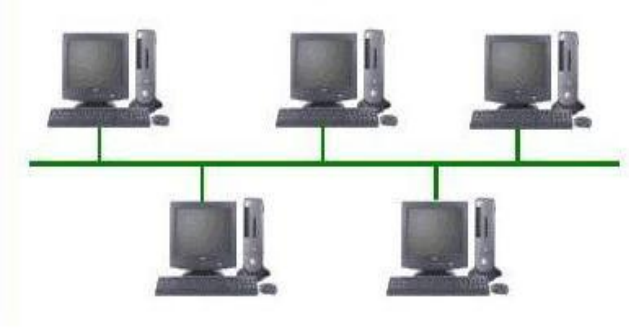


**Figura N° 5 Topología Bus**(Ramos, 2009)

### 1.3.3.2 TOPOLOGÍA ESTRELLA

Es una de las más ampliadas en los sistemas de comunicación de datos. Todo el tráfico emanan del núcleo de la estrella, es el controlador central de la red, por lo general una computadora posee el control total de las computadoras conectadas a la red. El controlador central a la red es responsable de encaminar el tráfico hacia el resto de los componentes; se encarga además de localizar las averías. Esta tarea relativamente sencilla, ya que es posible aislar las líneas para identificar el problema. Si se produce un fallo en una red de las estaciones no repercutirá en el funcionamiento general de la red. Si se produce una falla en el servidor, la red completa se sobrecarga y se viene abajo.

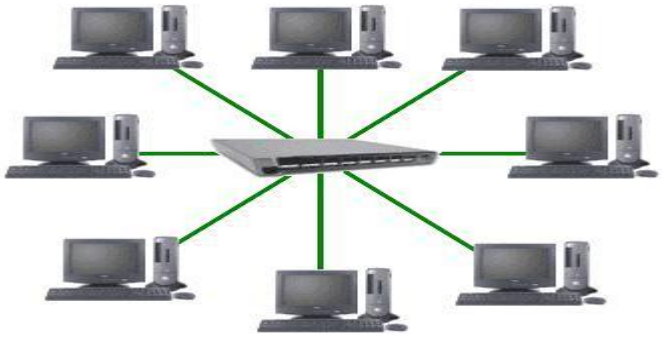


**Figura N° 6 Topología estrella**(R, 2009)

### 1.3.3.3 TOPOLOGÍA EN ANILLO

Todas las estaciones de trabajo están conectadas entre sí formando un anillo, de forma que cada estación solo tiene contacto directo con otras dos.

La estructura en anillo es otra configuración bastante extendida, se llama así por el aspecto circular del flujo de datos. En la mayoría de los casos, los retransmite el siguiente anillo. Además una lógica para poner en marcha una red de este tipo es relativamente simple. Cada componente solo ha de llevar a cabo una serie de tares muy sencillas: Aceptar los datos, enviar los a las computadoras conectadas al anillo o retransmitir al próximo componente del mismo.

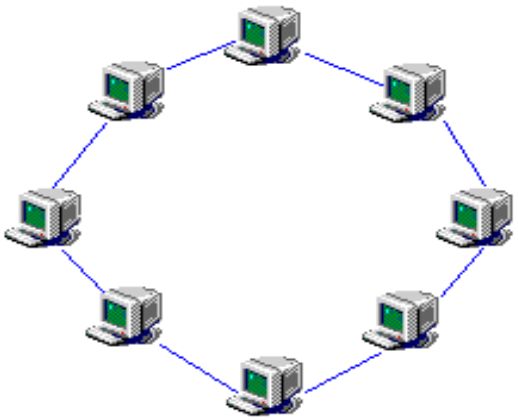


**Figura N° 7 Topología Anillo (Upiinfowarriors, 2010)**

### 1.3.4 COMPONENTES DE UNA RED

Los componentes de una red tienen funciones específicas y se utilizan dependiendo de las características físicas (Hardware) que tienen. Para elegirlos se requiere considerar las necesidades y los recursos económicos de quien se desea conectar a la red, por eso deben conocerse las características técnicas de cada componente de red.

#### 1.3.4.1 SERVIDOR

Son computadoras que controlan las redes y se encargan de permitir o no el acceso de los usuarios a los recursos, también controlan los permisos que determinan si un nodo puede o no pertenecer a la red. La finalidad de los servidores es controlar el funcionamiento de una red y los servicios que realice cada una de estas computadoras dependerán del diseño de la red.

#### 1.3.4.2 ESTACIÓN DE TRABAJO (WORKSTATION)

Es una PC que se encuentra conectada físicamente al servidor por medio de algún tipo de cable. En la mayor parte de los casos esta computadora ejecuta su propio sistema operativo y, posteriormente, se añade al ambiente de la red.

#### 1.3.4.3 TARJETAS O PLACAS DE INTERFAZ DE RED

Toda computadora que se conecta a una red necesita de una tarjeta de interfaz de red (NIC) que soporte un esquema de

red específico, como Ethernet, ArcNet o Token Ring. El cable de red se conectara a la parte trasera de la tarjeta.

#### 1.3.4.4 SISTEMA DE CABLEADO

El sistema de la red está constituido por el cable utilizado para conectar entre si el servidor y las estaciones de trabajo.

#### 1.3.4.5 RECURSOS Y PERIFÉRICOS COMPARTIDOS

Los dispositivos de almacenamiento ligados al servidor, las unidades de discos ópticos, las impresoras, los trazadores, etc.

### 1.3.5 MÉTODO DE TRANSMISIÓN

Una transmisión dada en un canal de comunicaciones entre dos equipos puede ocurrir de diferentes maneras. La transmisión está caracterizada por:

- La dirección de los intercambios.
- El modo de transmisión: el número de bits enviados simultáneamente.
- La sincronización entre el transmisor y el receptor.

Existen 3 modos de transmisión diferentes caracterizados de acuerdo a la dirección de los intercambios.

#### 1.3.5.1 CONEXIÓN SIMPLE

Es una conexión en la que los datos fluyen en una sola dirección, desde el transmisor hacia el receptor. Este tipo de conexión es útil si los datos no necesitan fluir en ambas direcciones (por ejemplo: desde el equipo hacia la impresora o desde el ratón hacia el equipo).

#### 1.3.5.2 CONEXIÓN SEMIDÚPLEX

Es una conexión en la que los datos fluyen en una u otra dirección, pero no las dos al mismo tiempo. Con este tipo de conexión, cada extremo de la conexión transmite uno después del otro. Este tipo de conexión hace posible tener una

comunicación bidireccional utilizando toda la capacidad de la línea.

#### 1.3.5.3 CONEXIÓN DÚPLEX TOTAL

Es una conexión en la que los datos fluyen simultáneamente en ambas direcciones. Así, cada extremo de la conexión puede transmitir y recibir al mismo tiempo; esto significa que el ancho de banda se divide en dos para cada dirección de la transmisión de datos si es que se está utilizando el mismo medio de transmisión para ambas direcciones de la transmisión.

### 1.3.6 CABLEADO ESTRUCTURADO

Es el conjunto de elementos pasivos, flexible, genérico e independiente, que sirve para interconectar equipos activos, de diferentes o igual tecnología permitiendo la integración de los diferentes sistemas de control, comunicación y manejo de la información, sean estos de voz, datos, video, así como equipos de conmutación y otros sistemas de administración.

En un sistema de cableado estructurado, cada estación de trabajo se conecta a un punto central, facilitando la interconexión y la administración del sistema, esta disposición permite la comunicación virtualmente con cualquier dispositivo, en cualquier lugar y en cualquier momento.

#### 1.3.6.1 MEDIOS GUIADOS

##### 1.3.6.1.1 PAR TRENZADO

Lo que se denomina cable de Par Trenzado consiste en dos alambres de cobre aislados, que se trenzan de forma helicoidal, igual que una molécula de DNA. De esta forma el par trenzado constituye un circuito que puede transmitir datos. Esto se hace porque dos alambres paralelos constituyen una antena simple. Cuando se trenzan

los alambres, las ondas de diferentes vueltas se cancelan, por lo que la radiación del cable es menos efectiva. Así la forma trenzada permite reducir la interferencia eléctrica tanto exterior como de pares cercanos.

Un cable de par trenzado está formado por un grupo de pares trenzados, normalmente cuatro, recubiertos por un material aislante.

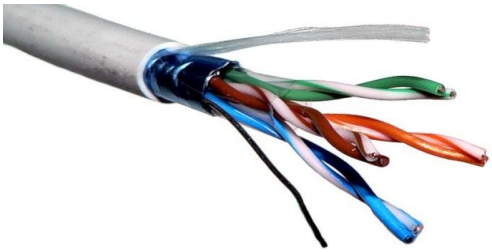


**Figura N° 8 Cable Par Trenzado** (Gutiérrez, 2012)

Los pares trenzados se apantallan. De acuerdo con la forma en que se realiza este apantallamiento podemos distinguir varios tipos de cables de par trenzado, éstos se denominan mediante las siglas UTP, STP y FTP.

**UTP** es como se denominan a los cables de par trenzado no apantallados, son los más simples, no tienen ningún tipo de pantalla conductora. Su impedancia es de 100 ohmios, y es muy sensible a interferencias. Los pares están recubiertos de una malla de teflón que no es conductora. Este cable es bastante flexible.

**STP** es la denominación de los cables de par trenzado apantallados individualmente, cada par se envuelve en una malla conductora y otra general que recubre a todos los pares. Poseen gran inmunidad al ruido, pero una rigidez máxima.

En los cables FTP los pares se recubren de una malla conductora global en forma trenzada. De esta forma mejora la protección frente a interferencias, teniendo una rigidez intermedia.

#### 1.3.6.2 ELEMENTOS DEL CABLEADO ESTRUCTURADO

##### 1.3.6.2.1 CABLEADO HORIZONTAL

Es recomendable la instalación de una canaleta o un subsuelo por el que llevar los sistemas de cableado a cada puesto. Las exigencias de ancho de banda pueden requerir el uso de dispositivos especiales para conmutar paquetes de red, o concentrar y repartir el cableado en estrella. En este nivel se pueden utilizar todos los tipos de cableados mencionados: coaxial, UTP, STP, fibra, etc., aunque alguno de ellos, como el coaxial, presentan problemas por su facilidad de ruptura o su fragilidad, especialmente en los puntos de inserción de <<T>>, con la consiguiente caída de toda la red. Sólo si el sistema se compone de un número reducido de puestos, el cable coaxial puede compensar por su facilidad de instalación. Además, no requiere ningún dispositivo activo o pasivo para que la red comience a funcionar. Subsistema distribuidor o administrador.

##### 1.3.6.2.2 CABLEADO VERTICAL O BACKBONE

Está encargado de comunicar todos los subsistemas horizontales por lo que requiere de medios de transmisión de señal con un ancho de banda elevado y de elevada protección. Para confeccionar un backbone se puede utilizar: cable coaxial fino o grueso (10 Mbps), fibra óptica u otro tipo de medios de transmisión de alta

velocidad. También se pueden utilizar cables de pares, pero siempre en configuración de estrella utilizando concentradores especiales para ello. Los backbones más modernos se construyen con tecnología ATM, redes FDDI o Gigabit Ethernet. Este tipo de comunicaciones es ideal para su uso en instalaciones que requieran de aplicaciones multimedia.

#### 1.3.6.2.3 LOCALIZACIÓN DE CADA PUESTO DE TRABAJO

A cada puesto deben poder llegar todos los posibles medios de transmisión de la señal que requiera cada equipamiento: UTP, STP, fibra óptica, cables para el uso de transceptores y balums, etcétera.

#### 1.3.6.2.4 SUBSISTEMA DE CAMPUS

Extiende la red de área local al entorno de varios edificios, por tanto, en cuanto a su extensión se parece a una red MAN, pero mantiene toda la funcionalidad de una red de área local. El medio de transmisión utilizado con mayor frecuencia es la fibra óptica con topología de doble anillo.

### 1.3.6.3 CABLE UTP CATEGORÍA 6

Cable de categoría 6, o Cat 6 (ANSI/TIA/EIA-568-B.2-1) es un estándar de cables para Gigabit Ethernet y otros protocolos de redes que es backward compatible (compatible con versiones anteriores) con los estándares de categoría 5/5e y categoría 3. La categoría 6 posee características y especificaciones para crosstalk y ruido. El estándar de

cable es utilizable para 10BASE-T, 100BASE-TX y 1000BASE-TX (Gigabit Ethernet). Alcanza frecuencias de hasta 250 MHz en cada par y una velocidad de 1Gbps. El cable contiene 4 pares de cable de cobre trenzado, al igual que estándares de cables de cobre anteriores. Aunque la categoría 6 está a veces hecha con cable 23 AWG, esto no es un requerimiento; la especificación ANSI/TIA-568-B.2-1 aclara que el cable puede estar hecho entre 22 y 24 AWG.

### 1.3.7 DISPOSITIVOS DE CONEXIÓN

#### 1.3.7.1 SWITCH

Según Alcocer (2000), cuando es inicializado el switch, este empieza a reconocer las direcciones MAC que generalmente son enviadas por cada puerto, es decir, cuando llega información al Switch este tiene mayor conocimiento sobre qué puerto de salida es el más apropiado, por lo tanto ahorra una carga("bandwidth") a los demás puertos del switch, esta es una de las principales razones por las cuales en Redes por donde viaja Video o CAD, se procura utilizar Switches para de esta forma garantizar que el cable no sea sobrecargado con información que eventualmente seria descartada por las computadoras finales, en el proceso, otorgando el mayor ancho de banda ("bandwidth") posible a los videos o aplicaciones CAD.

#### 1.3.7.2 ROUTER

Según Alcocer (2000), un router opera en la capa de red del modelo OSI y trabaja mayormente en dicha capa. Estos envían los datagramas para que lleguen a su destino y también cual es la ruta más óptima.

Los routers operan en una capa superior a la de los bridges, por lo cual realizan tareas más sofisticadas, sin embargo son más costosos y complejos para desarrollar.

### 1.3.8 CARACTERÍSTICAS DE RUTEO

- Políticas de enrutamiento. Ruteo estático o dinámico
- Bridging, protocolos panning tree, interfaces multiples bridge, firewall en e lbridge
- Servidores y clientes: DHCP, PPPoE, PPTP,PPP, Relay de DHCP
- Cache: web-proxy, DNS
- Gateway de Hot Spot
- Lenguaje interno descripts

### 1.3.9 HERRAMIENTAS DE MANEJO DE RED

- Ping, trace route.
- Medidor de ancho de banda.
- Contabilización de tráfico.
- SNMP.
- Torch.
- Sniffer de paquetes.

## 1.4 ISO

Las normas ISO surgen como una Normalización nacional e internacional de las empresas, por la necesidad de hacer un mercado estandarizado, donde se logre tener calidad para cumplir con las necesidades y expectativas del cliente. La calidad en los últimos años es un término muy difundido, el cual le da una ventaja competitiva a las empresas mediante la certificación de mecanismos de garantía de la calidad, utilizando las denominadas Normas ISO 9000. Esta norma es una de las más populares en la mayoría de los sectores industriales junto con la norma ISO 14000 relacionada con el medio ambiente.

- **OBJETIVO GENERAL:** Saber y conocer las diferentes Normas Internacionales de garantía de calidad dentro de las organizaciones y diferentes sectores industriales que ayudan a mantener y aumentar la calidad, en los procesos tecnológicos y productivos de la economía; contribuir al desarrollo de las industrias mediante la aplicación de las Normas.(Buenastareas, 2010)

### 1.4.2 ISO/IEC 27000

Es un conjunto de estándares desarrollados o en fase de desarrollo por ISO (International Organization for Standardization) e IEC (International Electro technical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. (Buenastareas, 2010)

### 1.4.3 ISO 17799

El ISO 17799, no es una norma sino que se definirse como una guía en la implementación del sistema de administración de la seguridad de la información, se orienta a preservar los siguientes principios de la seguridad informática:

Confidencialidad. Asegurar que únicamente personal autorizado tenga acceso a la información.

Integridad. Garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas.

Disponibilidad. Asegurar que los usuarios autorizados tendrán acceso a la información cuando la requieran. (Núñez Sandoval, 2012).

### 1.4.4 ISO 27002

Este es el número de la norma 27000 serie de lo que originalmente era la norma ISO 17799 (que a su vez se conocía anteriormente como BS 7799-1).

La norma ISO 27002 fue publicada originalmente como un cambio de nombre de la norma vigente ISO 17799, un código de prácticas para la seguridad de la información. Básicamente se resume cientos de posibles controles y mecanismos de control, que pueden ser implementadas, en teoría, con sujeción a las directrices proporcionadas en la norma ISO 27001.

Los "lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información dentro de una organización" estándar. Los controles reales que figuran en la norma están destinados a atender las necesidades específicas identificadas a través de una evaluación de riesgos formal. La norma también tiene por objeto proporcionar una guía para el desarrollo de "normas de seguridad de la organización y las prácticas eficaces de gestión de la seguridad y para ayudar a construir la confianza en las actividades interinstitucionales". (Buenastareas, 2010)

- **CONTENIDO DE ISO 27002**

  Las secciones de contenido son:

  1. Estructura
  2. Política de Seguridad
  3. Organización de la Seguridad de la Información
  4. Recursos Humanos Seguridad
  5. Gestión de Activos
  6. Control de Acceso
  7. Criptografía
  8. Seguridad física y ambiental
  9. Seguridad de las operaciones
  10. Seguridad en las Comunicaciones
  11. Adquisición de Sistemas de Información, Desarrollo, Mantenimiento
  12. Relaciones con los proveedores
  13. Gestión de Incidentes de Seguridad

14. Información aspectos de seguridad de la Continuidad del Negocio
15. Conformidad, (The ISO 27000, 2013)

### 1.4.5 CONSIDERACIONES DEL ISO 27002: 2005

La propuesta de esta norma, no está orientada a despliegues tecnológicos o de infraestructura, sino a aspectos netamente organizativos, es decir, la frase que podría definir su propósito es "Organizar la Seguridad de la Información", por ello propone toda una secuencia de acciones tendientes al "establecimiento, implementación, monitorización, revisión, mantenimiento y mejora de la gestión de seguridad de la Información"

### 1.4.6 ISO/IEC 27002:2005. DOMINIOS, OBJETIVOS DE CONTROL Y CONTROLES (VER ANEXO 6)

Se usaran las siguientes políticas de seguridad ISO/IEC 27002 (según el Dominio 5, Objetivo de Control 5.1; Controles 5.1.1; Dominio 7, Objetivo de Control 7.1, 7.2, Controles 7.1.1, 7.1.2; Dominio 11 y Objetivo de Control 11.1, 11.2, 11.4, 11.5; Controles 11.1.1, 11.2.3, 11.4.1, 11.4.6).

#### 1.4.6.1 SEGURIDAD FÍSICA Y DEL ENTORNO

Sugiere diseñar una estructura de administración dentro de la empresa, que establezca la responsabilidad de los grupos en ciertas áreas de la seguridad y un proceso para el manejo de respuestas e incidencias. Esta sección considera las políticas generales de la organización y detalla cómo se debe administrar la seguridad de la información dentro de la empresa, Asimismo, define como mantener la seguridad de las instalaciones de procesamiento de información y los activos informáticos accedidos por terceros (proveedores, clientes, etc).

#### 1.4.6.1.1 SEGURIDAD DE LOS EQUIPOS

- Instalación y protección de equipos.
- Suministro eléctrico.
- Seguridad del cableado.
- Mantenimiento de equipos.
- Seguridad de equipos fuera de los locales de la Organización.
- Seguridad en la reutilización o eliminación de equipos.
- Traslado de activos.

### 1.4.6.2 CONTROL DE ACCESO

Detalla los elementos de la compañía (Servidores, Redes, documentos, impresoras, etc.) que deben de ser considerados para establecer un mecanismo de seguridad, manteniendo una protección adecuada, garantizando que reciban un nivel adecuado de protección. En este sentido, los activos deben ser considerados en: confidenciales, Privados, de uso interno y de uso público.

#### 1.4.6.2.1 CONTROL DE ACCESO EN RED

Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para protegerlos contra los abusos internos e intrusos externos. Asimismo establece los diferentes tipos de accesos o privilegios a los recursos de informáticos (sistema operativo, aplicaciones, correo electrónico, internet, comunicaciones, conexiones remotas, etc.) que requiera cada empleado de la compañía y el personal externo que brinda servicios, en concordancia con sus responsabilidades , esto permitirá evitar filtraciones

o actividades no autorizadas, garantizando la información y seguridad de la misma.

En este punto veremos:

- Política de uso de los servicios en red.
- Autenticación de usuario para conexiones externas.
- Identificación de los equipos en las redes.
- Protección de los puertos de diagnóstico y configuración remotos.
- Control de la conexión a la red

### 1.4.7 BENEFICIOS AL APLICAR LA ISO 27002

El aplicar las mejores prácticas nos permitirá mejorar los procesos de negocios alcanzando así estabilidad con respecto a la información, llegando a obtener mejores resultados y minimizando riesgos y tiempo.

Algunos de los beneficios que persigue la Empresa son:

- Si se utiliza un criterio estándar para la configuración y administración de los sistemas de la organización, se puede minimizar la posibilidad de que una debilidad en una de ellos pueda comprometer los controles de acceso de los restantes.
- La organización puede construir una arquitectura de seguridad que permita minimizar las brechas que se puedan registrar entre las amenazas detectadas y los controles existentes, mitigando el riesgo asociado a una eventual ocurrencia de dicha amenaza.
- Se le facilita a la organización la simplificación, estandarización y automatización de los servicios de seguridad.

**1.4.8 IDENTIFICACION DE ACTIVOS** Definamos que es un activo; para la gestión de seguridad de la información, un activo es algo que tiene valor o utilidad, cada activo necesita ser protegido, ya que ellos nos garantizan la continuidad de la organización.

Cada uno de los activos deben de ser identificados apropiadamente y valorados, la ISO clasifica a los activos de la siguiente manera:

- **Activos de Información:** son la base de datos y archivos de datos, documentación del sistema, manuales de usuario, material de entrenamiento, procedimiento de operativos de apoyo, planes de continuidad.
- **Documentos impresos:** documentos impresos, contratos, lineamientos, documentos de la empresa, documentos que contienen resultados importantes de negocio.
- **Activos de software:** software de aplicación, software de sistemas, herramientas de desarrollo.
- **Activos Físicos:** Equipos de comunicación y computación, medios magnéticos, cableado de redes, otros equipos técnicos.
- **Personas:** personal, clientes, suscriptores.
- **Imagen y reputación de la empresa**
- **Servicios:** Servicios de computación y comunicaciones, otros servicios técnicos.

# Capítulo II

# 2. RESULTADOS

## 2.1 DESCRIPCIÓN GENERAL

### 2.1.1 CRONOGRAMA DE ACTIVIDADES

| Nombre de tarea | Duración | Comienzo | Fin | Predecesoras |
|---|---|---|---|---|
| Recopilación de informacion | 6 días | vie 16/08/13 | vie 23/08/13 | |
| **Fase I: Identificar objetivos y necesidades del cliente** | **22 días** | **sáb 24/08/13** | **lun 23/09/13** | |
| 1. Analizar los objetivos y limitaciones del negocio | 2 días | lun 26/08/13 | mar 27/08/13 | |
| 2. Analizar los objetivos y limitaciones técnicas | 3 días | mié 28/08/13 | vie 30/08/13 | 3 |
| 3.Graficar la red existente | 8 días | lun 02/09/13 | mié 11/09/13 | 4 |
| **Fase II: Diseñar la red lógica** | **19 días** | **jue 12/09/13** | **mar 08/10/13** | |
| 5. Diseñar topología de red | 6 días | mié 25/09/13 | mié 02/10/13 | |
| 6. Diseñar modelo de direccionamiento | 4 días | jue 03/10/13 | mar 08/10/13 | 7 |
| 7. Desarrollar estrategias de seguridad de red según la Norma ISO | 4 días | jue 12/09/13 | mar 17/09/13 | |
| 8. Desarrollar estrategias de mantenimiento de la red según la Norma ISO | 5 días | mié 18/09/13 | mar 24/09/13 | 9 |
| **Fase III: Diseñar la red física** | **36 días** | **lun 23/09/13** | **dom 10/11/13** | |
| 10. Tecnologias y dispositivos de red según la Norma ISO | 7 días | mié 25/09/13 | jue 03/10/13 | 10 |
| **Fase IV: Informe Final de la red** | **53 días** | **vie 04/10/13** | **mar 17/12/13** | |
| 13. Documentar el diseño de red | 6 días | vie 04/10/13 | vie 11/10/13 | |
| Informe completo del diseño de red | 1 día | mar 17/12/13 | mar 17/12/13 | |

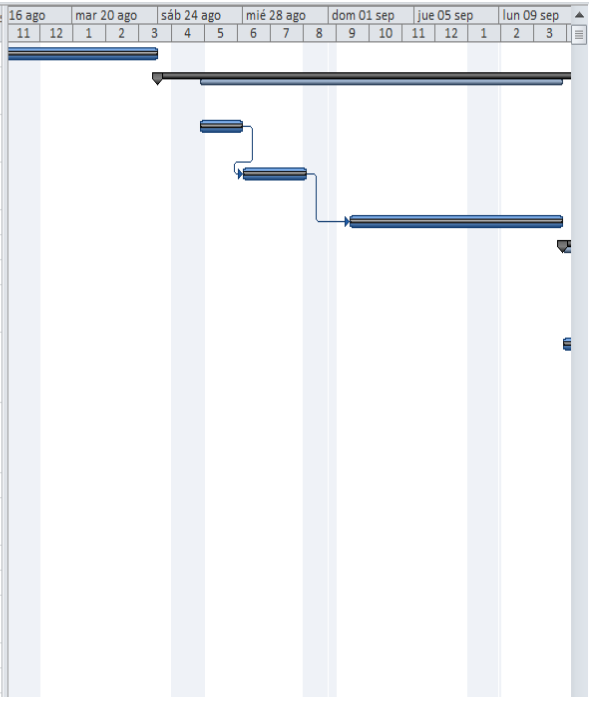



**Figura Nº 9 Cronograma de Actividades**

### 2.1.2 REALIDAD PROBLEMÁTICA

Actualmente el Policlínico Señor de Los Milagros se ubica en el jirón Bolognesi 382 – 386 Trujillo - La Libertad, se dedica al servicio en diversas especialidades médicas y laboratorio entre otros. Se inició en este negocio desde el año 1997, debido al auge de la tecnología y de la macroeconomía se han estado construyendo en Trujillo muchas clínicas y laboratorios, dando un buen servicio al cliente, es por eso que el policlínico en su visión de expandirse empresarialmente y contar con los avances tecnológicos y políticas de seguridad de información, busca actualizar sus servicios haciendo uso de estas tecnologías para mejorar sus servicios e infraestructura. Permitiendo así observar las siguientes debilidades internas, no cuenta con una conexión de red que permita

compartir sus recursos entre sus consultorios y oficinas administrativas teniendo desventajas diarias en la demora de entrega de información de los doctores a sus pacientes. Se puede observar que utiliza la información de sus pacientes por medios extraíbles y documentos físicos, todo el Policlínico no cuenta con la base para un modelo organizacional de red. Haciendo que esta empresa no sea competitiva en el rubro al cual está dirigido. Es por eso que el policlínico se ve en la necesidad de implementar una red estructurada para optimizar sus procesos y estar al nivel competitivo con otras empresas dedicadas a su rubro.

### 2.1.3 DEFINICIÓN DEL PROBLEMA

El Policlínico Señor de los Milagros presenta las siguientes necesidades que demandan una Red de Datos:

- Limitada comunicación entre sus consultorios para la compartición de información debido que no cuenta con acceso a una base de datos.
- La documentación se encuentra en archivos físicos por lo que se requiere un servidor que provea servicios de información a otras áreas.
- Desconocimiento de la importancia de la seguridad de información y requerimientos de implementar políticas de seguridad en la información. ( no cuenta con una Certificación ISO para la seguridad de información)

### 2.1.4 FORMULACIÓN DEL PROBLEMA

¿Cómo planificar el diseño de la interconexión de las áreas del Policlínico “Señor de los Milagros SRL”, usando las Tecnologías de información y según estándares de seguridad de Información?

### 2.1.5 OBJETIVO

#### 2.1.5.1 OBJETIVO GENERAL

Diseño de una red de datos para el Policlínico Señor de los Milagros SRL usando metodología Topdown Network Desing y aplicando estándares ISO/IEC 27002.

#### 2.1.5.2 OBJETIVO ESPECÍFICOS

- Identificar Objetivos y Necesidades del policlínico mediante entrevistas.
- Diseñar una red lógica aplicando la metodología Top Down Network Design.
- Diseñar un modelo de conectividad, según la metodología TOP DOWN NETWORK DESIGN.
- Establecer políticas de seguridad, aplicando estándares ISO/IEC 27002 (según el Dominio 5, Objetivo de Control 5.1; Controles 5.1.1; Dominio 7, Objetivo de Control 7.1, 7.2, Controles 7.1.1, 7.1.2; Dominio 11 y Objetivo de Control 11.1, 11.2, 11.4, 11.5; Controles 11.1.1, 11.2.3, 11.4.1, 11.4.6).

## 2.2 FASE I: IDENTIFICANDO OBJETIVOS Y NECESIDADES DEL CLIENTE

### 2.2.1 ANÁLISIS DE LOS OBJETIVOS Y LIMITACIONES DEL NEGOCIO

- **DATOS EMPRESARIALES**

**Rubro de la Empresa:** Salud Privada

**Razón Social:** Policlínico Señor de los Milagros

**Fecha de Creación:** 22 de diciembre 1973

**Dirección:** Jirón Bolognesi 382 – 386 Trujillo – la Libertad

El Policlínico, debido al constante avance tecnológico y a la evolución de las redes de comunicación y de redes inalámbricas, frente a estas innovaciones se ven obligados a optar por tecnología como fuente de desarrollo, teniéndose en cuenta los sistemas de seguridad que hoy en día es de suma importancia para las empresas.

Actualmente el Policlínico, requiere una red de datos y llevar un control de los usuarios que tienen acceso a internet, así como también darles un mejor servicio a los usuarios, de esta manera accediendo y transmitiendo datos con mayor facilidad, como también mejorar los procesos del Policlínico. Por estos motivos el diseño propuesto tiene una lista de objetivos comerciales que afectará el diseño de la red:

- Aumentar ventajas competitivas frente a otras organizaciones que tienen el mismo rubro de negocio.
- Ofrecer nuevos servicios a los usuarios.
- Construir relaciones y accesibilidad de información a un nuevo nivel, como base para un modelo organizacional de red.
- Evitar una interrupción comercial causada por problemas de seguridad de red.

### 2.2.2 ANÁLISIS DE LOS OBJETIVOS Y LIMITACIONES TÉCNICAS

Teniendo en cuenta que el Policlínico no tiene una Red, y los equipos de cómputo no se encuentran interconectados se sugiere el siguiente análisis.

- **ESCALABILIDAD**

  Teniendo en cuenta la cantidad de computadoras del Policlínico que son 4 computadoras en uso y 12 sin usar en almacén, encontrando un total de 16 computadoras, este diseño deberá soportar un crecimiento de la red permitiéndose incluir nuevos nodos; dejando puertos adicionales en cada área de la empresa para un posible crecimiento del mismo aproximadamente un 50% se

dejaría para el futuro, planteando este objetivo para lograr un diseño lógico jerárquico.

(20%)(N°PC) + [(10% Anual)(N°PC)]*Años

(20% * 16) + (10%*16)*5 Años

3+10= 13 PC

13+16=29 PC

- **DISPONIBILIDAD**

La red estará disponible las 24 horas del día, los 7 días de la semana.

Se calcula con la siguiente fórmula:

**Disponibilidad = (MTBF / (MTBF + MTTR)) X 100**

| **Nombre** | **Acrónimo** | **Calculo** | **Definición** |
|---|---|---|---|
| Tiempo Medio Entre Errores | MTBF | **Horas /N° de Errores** | Duración media de Funcionamiento antes de producirse el Error |
| Tiempo Medio De Recuperación | MTTR | **Horas de g reparación / N° de Errores** | Tiempo medio necesario para reparar y restaurar el servidor después de que se produzca un error |

**Tabla N° 1 Cuadro de Disponibilidad**

Considerando, para que funcione continuamente. Colocamos un punto de control de 24 horas lo que nos da en un mes (30dias) 720 horas (1 mes aproximadamente) Consecutivas, dos errores de una hora durante ese período darían lugar a una disponibilidad de (720 / (720 + 2)) X 100 = (720 / 725) X 100 = 0,9972 X 100 = 99,72 %.

La tasa de disponibilidad de la operatividad de la red será 99.72% por semana lo cual es considerado aceptable por el usuario.

Las restricciones están ligadas a la no operatividad de la red por diferentes causas como por ejemplo siniestros naturales, etc., que no está a nuestro alcance.

- **CONFIDENCIALIDAD:**

  Protección de la información sensitiva de intercepciones no autorizadas.

- **FACILIDAD DE USO:**

  Los usuarios pueden acceder a la red de manera muy fácil y hacer uso de ella en todo momento. Esta red debería ayudara a los colaboradores en los tiempos para determinadas actividades.

- **ADAPTABILIDAD:**

  Indicará si el diseño es flexible, y puede ser adaptado ante algún cambio con nuevas tecnologías y sistemas de información.

### 2.2.3 CARACTERIZAR Y GRAFICAR LA RED EXISTENTE

El Policlínico no cuenta con una red y están funcionando todo los procesos de forma manual y todas sus áreas trabajan de manera aislada; bajo este contexto se describe las diferentes aplicaciones que son utilizadas en la empresa, aplicaciones básicas como Microsoft office 2010, Adobe Reader, y aplicaciones hechas a la medida para diferentes áreas.

#### 2.2.3.1 DESCRIPCIÓN FÍSICA DE LOS EQUIPOS QUE USAN EN EL POLICLÍNICO

El Policlínico cuenta con 4 equipos de cómputos y 3 impresoras activas, distribuidos y con sus respectivas características en cuanto a hardware. A continuación presentamos la siguiente tabla con las computadoras existentes.

| AREA | N° COMPUTADORAS | RAM | PROCESADOR | DISCO DURO |
|---|---|---|---|---|
| **Administración** | 01 | 3 GB | Intel Corei3 2.6 GHz | 500GB |
| **Laboratorios** | 02 | 4GB | Intel Corei3 2.6 GHz | 500GB |
| **Contabilidad** | 01 | 3 GB | Intel Corei3 2.6 GHz | 500GB |

**Tabla N° 2 Computadoras Existentes en Policlínico**

| ÁREA | IMPRESORAS | MARCA | MODELO |
|---|---|---|---|
| **Administración** | 1 | HP | **LaserJet 1536** |
| **Laboratorios** | 1 | HP | **LaserJet 4240** |
| **Contabilidad** | 1 | HP | **CanonMP320** |

**Tabla N° 3 Impresoras Existentes**

| ÁREA | SISTEMA OPERATIVO | APLICACIÓN |
|---|---|---|
| **Administración** | Ms Window7 | Office 2010, Adobe Reader |
| **Laboratorios** | Ms Window7 | Ms Office 2010, Adobe Reader |
| **Contabilidad** | Ms Windows 7 | Ms Office 2010, Adobe Reader. |

**Tabla N° 4 Software en el Policlínico**

### 2.2.4 ANALISIS DEL RIESGO Y LOS REQUERIMIENTOS DEL ISO 27002.

La ISO 27002 requiere que toda organización que plantee un sistema de gestión de seguridad de información (SGSI) e implementación de una Red debe de definir primero el alcance del estándar en la empresa y en base a ese alcance se deben definir todos los activos de información.

Luego se debe de realizar un análisis de riesgo para definir todos los activos y cuales se les puede considerar de mayor riesgo, luego se debe conversar con los respectivos encargados de cada uno de los activos para definir que controles se aplicaran para mitigar dichos riesgos, la ISO 27002 Es un sistema dinámico que obliga a la gerencia

a estar constantemente revisando y definiendo controles, para detectar amenazas vulnerabilidad e iniciar acciones preventivas y correctivas cuando sea necesario.

#### 2.2.4.1 IDENTIFICACIÓN DE REQUERIMIENTO DE SEGURIDAD

Se considerará el dominio 5 de las Políticas de Seguridad de la ISO/IEC 27002. Los requerimientos de seguridad se derivan de tres fuentes esenciales:

- El conjunto de amenazas y vulnerabilidad que pudieran ocasionar pérdidas significativas en la empresa.
- Los requerimientos que deben satisfacerse por la empresa.
- El conjunto único de objetivos, principios y requerimiento para el procesamiento de la información que la empresa requiere.

  Una vez identificado estos se podrá aplicar los controles que satisfagan dichos requerimientos.

#### 2.2.4.2 IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

El daño se puede dar por varias vías ya sea directamente, es decir dañar los datos, o indirectamente puede darse daños a la infraestructura.

Las amenazas pueden originarse de fuentes accidentales o de manera deliberada, para que una amenaza pueda dañar un activo debería explotar la vulnerabilidad del sistema, aplicativo, red, o servicio.

Las amenazas encontradas son:

- Un incendio originado por un corto circuito
- Desastre Natural
- Hackers en el sistema
- Mala instalación de la red
- Errores de los aplicativos
- Robo de los activos del Laboratorio

#### 2.2.4.3 CÁLCULO DE LOS RIESGOS DE SEGURIDAD

El objetivo de la evaluación del riesgo es la de identificar y evaluar el riesgo para poder determinar soluciones. Los riesgos son calculados de una combinación de valores de activos y niveles de requerimiento de seguridad.

La evaluación de riesgo envuelve la sistemática considerando los siguientes aspectos:

- Consecuencia: el daño de la empresa o institución como resultado de un incumplimiento de seguridad de información considerando las potenciales consecuencias de pérdida o fallos de confidencialidad, integridad y disponibilidad de información.
- Probabilidad: la real posibilidad de que tal incumplimiento ocurra a la luz del reinado de amenazas, vulnerabilidad y controles.

Es importante considerar que no existe una manera buena o mala de calcular los riesgos, es por ello que cada institución tiene su propia forma de evaluación de los riesgos considerando cada uno de sus activos, por lo tanto no se puede regir a una norma o ley para poder calcular los riesgos.

**Clasificación de los riesgos:** se clasificarán de la siguiente manera.

- **Sin riesgo:** 0% - 6% → no se han detectado fallos graves
- **Alto potencial:** 7% - 20% → se han detectado fallos de nivel alto.

#### 2.2.4.4 SELECCIÓN DE OPCIONES DE TRATAMIENTO DEL RIESGO

El estándar **ISO 27002:2005** requiere que el tratamiento del riesgo siga cuatro posibles acciones:

- Aplicación de controles apropiados para reducir los riesgos. Los controles tienen que ser identificados. Si los

controles no puedes ser hallados, la firma puede crearlos y documentarlos.

- Aceptar objetivamente los riesgos partiendo del supuesto que satisfacen las políticas de la institución y sus criterios para la aceptación del riesgo.
- Evitar los riesgos.
- Transferir los riesgos asociados a otra parte.
- Hay dos alternativas que se explican:
  - Evitar el riesgo
  - Transferir el riesgo
    - ***Evitar el riesgo:*** Describe cualquier opción donde los activos son transferidos de las áreas de riesgo. Cuando se evalúan la posibilidad de evitar el riesgo, esto debe sopesarse entre las necesidades de la institución y las monetarias.
    - ***Transferir el riesgo:*** Esta opción puede ser la mejor si no se puede reducir los niveles del riesgo. Existen muchas alternativas a considerar en relación a la estrategia de transferencia del riesgo. La transferencia del riesgo podría alcanzarse tomándose una póliza de seguridad. Otra posibilidad podría ser la utilización e servicios de "out sourcing" para que se maneje activos y procesos críticos.

#### 2.2.4.5 SELECCIÓN DE CONTROLES PARA REDUCIR EL RIESGO A UN NIVEL ACEPTABLE

Para reducir el riesgo evaluado, dentro del alcance del sistema de Gestión de Seguridad Informática, considerados los controles de seguridad apropiados y justificados deben ser identificados y seleccionados. Estos controles deben ser seleccionados de ISO 27002:2005. La empresa también puede utilizar el ISO 17799:2005 como guía para la

implementación de los controles, pero deben ser escogidos del ISO 27002:2005.

Especialmente para propósitos de certificación, las relaciones con la evaluación del riesgo deben ser documentadas para justificar la selección de los controles.

Cuando se seleccionan controles para la implementación, un número de factores deben ser considerados, incluyendo:

- Uso de controles.
- Transferencia de usuarios
- Ayuda otorgada a los doctores o usuarios para desempeñar sus funciones.
- Relativa fuerza de los controles
- Tipos de funciones desempeñadas

En término generales, un control podrá satisfacer más de una de estas funciones y lo más que pueda satisfacer mejor.

## 2.3 FASE II: DISEÑO LÓGICO DE LA RED

Esta Segunda Fase se concentra en técnicas para desarrollar una topología para un diseño de red. El diseño de una topología de red es el primer paso en la fase de diseño lógico de la metodología de diseño de red TOP Down.

Diseñando una topología lógica antes de una realización física, usted puede aumentar la probabilidad de encontrar los objetivos de un cliente para escalabilidad, adaptabilidad, e interpretación.

### 2.3.1 SERVICIOS DE LA RED

#### 2.3.1.1 ACTIVE DIRECTORY

Nos permite establecer políticas a nivel de empresa, desplegar programas en muchos ordenadores y aplicar actualizaciones críticas a la organización, almacenara información de una organización en una base de datos central, organizada y accesible.

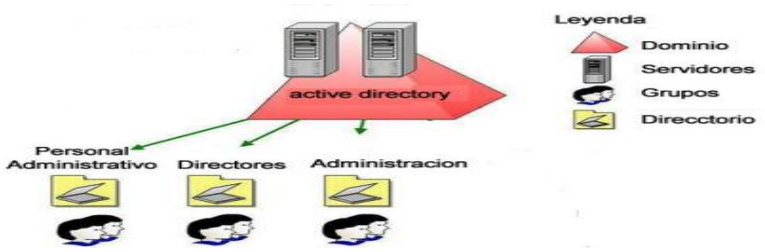



**Figura N° 10 Active Directory**

## 2.3.2 DISEÑANDO TOPOLOGIA DE RED

### 2.3.2.1 SEGURIDAD LÓGICA

La Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."

Los objetivos que se plantean serán:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

  Esta fase describe de cuatro características de topología de red: Jerárquica, Modular, redundancia y seguridad, todas estas características pueden ser aplicadas a campus como a empresas.

Para el desarrollo de este proyecto se decidió utilizar la topología Jerárquica la cual se divide en tres capas:

- **Una Capa Core:** Router y Switch de alta velocidad que son optimizados para una buena disponibilidad y performance.
- **Una Capa de Distribución:** Puntos de accesos inalámbricos y Switch para la implementación de políticas.
- **Una Capa de Acceso:** Que une en la parte inferior a usuarios vía switch.

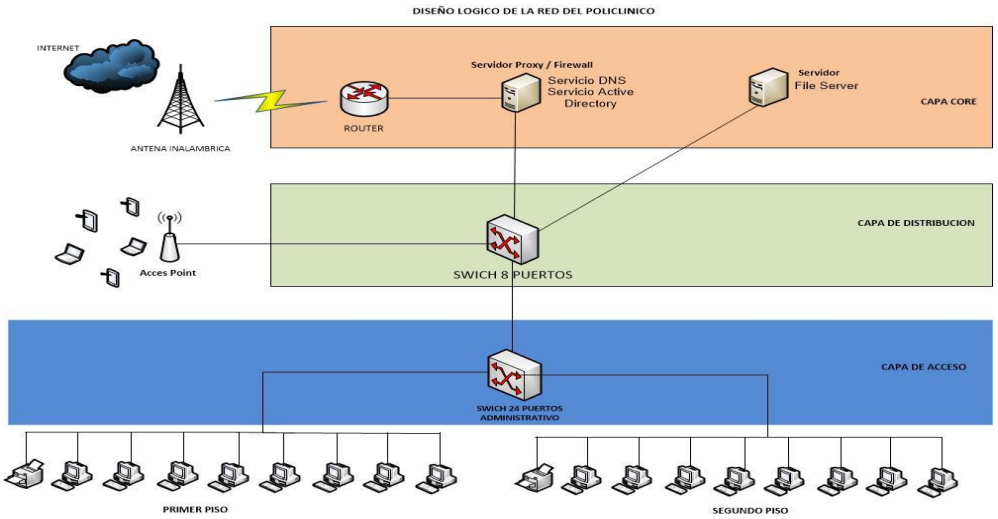



**Figura N° 9Diseño Lógico Propuesto Para El Policlínico**

La topología propuesta es de tipo jerárquico, de esa forma, si el policlínico decide crecer entonces cumpliríamos con el objetivo técnico de escalabilidad, puesto que crecería de acuerdo a la necesidad; en la actualidad se dividiría en 2 subredes las cuales serían administrativo y servidores. Como se muestra en el diagrama y así cumple la disponibilidad ya antes planteada.

### 2.3.3 DISEÑAR MODELO DE DIRECCIONAMIENTO

#### 2.3.3.1 DISEÑO DE DISTRIBUCIÓN DE IP'S DE LA RED

Para la asignación de IP a los equipos y dispositivos, usaremos la clase C para tipos de IP, siguiendo el formato 192.168.1.x, donde tendremos hasta un máximo de 253 direcciones para vincularse con la red. La dirección IP de la puerta de enlace del Router será 192.168.1.1 y las demás direcciones serán como se muestra en la tabla.

***Distribución de IP de la Red***

| N° | Subred | Nombre de Subred | Rango de IP | Dirección de IP | | Broadcast |
|---|---|---|---|---|---|---|
| 1 | 192.168.1.0 | **Servidor** | 192.168.1.0 - 192.168.1.63 | Servidor Proxy / Firewall | 192.168.1.1 | 192.168.1.63 |
| | | | | | 192.168.1.2 | 192.168.1.63 |
| | | | | | 192.168.1.3 | 192.168.1.63 |
| | | | | Servidor DNS y Archivos | 192.168.1.4 | 192.168.1.63 |
| | | | | | 192.168.1.5 | 192.168.1.63 |
| 2 | 192.168.1.64 | **Administrativo** | 192.168.1.64 – 192.168.1.127 | PC01 | 192.168.1.65 | 192.168.1.127 |
| | | | | PC02 | 192.168.1.66 | 192.168.1.127 |
| | | | | PC03 | 192.168.1.67 | 192.168.1.127 |
| | | | | PC04 | 192.168.1.68 | 192.168.1.127 |
| | | | | PC05 | 192.168.1.69 | 192.168.1.127 |
| | | | | PC06 | 192.168.1.70 | 192.168.1.127 |
| | | | | PC07 | 192.168.1.71 | 192.168.1.127 |
| | | | | PC08 | 192.168.1.72 | 192.168.1.127 |
| | | | | PC09 | 192.168.1.73 | 192.168.1.127 |
| | | | | PC10 | 192.168.1.74 | 192.168.1.127 |
| | | | | PC11 | 192.168.1.75 | 192.168.1.127 |
| | | | | PC12 | 192.168.1.76 | 192.168.1.127 |
| | | | | PC13 | 192.168.1.77 | 192.168.1.127 |
| | | | | PC14 | 192.168.1.78 | 192.168.1.127 |
| | | | | PC15 | 192.168.1.79 | 192.168.1.127 |
| | | | | PC16 | 192.168.1.80 | 192.168.1.127 |

**Tabla N° 5 Direccionamiento IP Propuesto**

### 2.3.4 ESTABLECIENDO POLÍTICAS DE SEGURIDAD APLICANDO NORMA ISO 27002

Teniendo en cuenta que el Policlínico no cuenta con estándares de seguridad se está considerando el objetivo cuatro de la presente tesis Establecer políticas de seguridad ISO/IEC 27002 (según el Dominio 5, Objetivo de Control 5.1; Controles 5.1.1; Dominio 7, Objetivo de Control 7.1, 7.2, Controles 7.1.1, 7.1.2; Dominio 11 y Objetivo de Control 11.1, 11.2, 11.4, 11.5; Controles 11.1.1, 11.2.3, 11.4.1, 11.4.6). Cuando se tenga diseñado el modelo lógico de la red, se deberán tener en cuenta los equipos que se estarán utilizando (Servidor, computadoras, Switch, router, etc.) así mismo la persona encargadas de supervisar y mantener el cuidado de la red deberá tener en cuenta lo siguiente:

#### 2.3.4.1 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Se ha considerado implementar los controles que aseguren la reducción de los riesgos a un nivel aceptable.

Hay muchas formas de gestionar los riesgos y este documento proporcionará ejemplos de enfoques habituales. Sin embargo hay que reconocer que ciertos controles no son aplicables para todos los sistemas o entornos de información y pueden no ser de aplicación en todas las organizaciones.

Cierto número de controles se consideran principios orientativos que proporcionan un punto de partida para implementar la seguridad de la información. Se apoyan en requisitos legislativos esenciales o se considera la mejor práctica habitual para conseguir dicha seguridad.

Los controles que se consideran esenciales para esta empresa desde un punto de vista legislativo comprenden:

- La protección de los datos de carácter personal y la intimidad de las personas.
- La salvaguarda de los registros de la organización
- Los derechos de la propiedad intelectual.

Los controles que se consideran comunes para la mejor práctica habitual para conseguir la seguridad de la información comprenden:

- La documentación de la política de seguridad de la información
- La asignación de responsabilidades de seguridad, estas las dará la gerencia
- La información y capacitación para la seguridad de la información del personal que se encargara de supervisar la red
- El riesgo de las incidencias de seguridad
- La gestión de la continuidad del negocio

Estos controles pueden aplicarse a la mayoría de las organizaciones y los entornos.

### 2.3.5 GESTIÓN DE ACTIVOS

Se ha tomado en cuenta el domino (7), Objetivo de control (7.1) (7.2), controles (7.1.1; 7.1.2), (7.2.1) teniendo lo siguiente:

#### 2.3.5.1 RESPONSABILIDAD SOBRE LOS ACTIVOS

- Todos los activos de información del policlínico tienen un propietario (médico).
- Cada propietario clasificará la información dentro de uno de los niveles sensitivos que dependen de obligaciones legales, costos, políticas institucionales y necesidades de la empresa.
- El propietario es responsable por la protección de esta información.
- El propietario definirá cuáles usuarios pueden acceder a sus datos.
- El propietario es responsable de sus datos
- La seguridad de los mismos tiene que estar de acuerdo al nivel de sensibilidad.

#### 2.3.5.2 CLASIFICACIÓN DE LA INFORMACIÓN

Para mantener la seguridad de la información del Policlínico se ha considerado clasificar la información considerando cuatro niveles.

- Información Pública.
- Información Interna.
- Información confidencial.
- Información secreta.

El más bajo (Pública) es el menos sensitivo y el más alto (Secreta) es para los procesos o datos más importantes. Cada nivel es un súper conjunto del nivel previo.

Por ejemplo, si un sistema está clasificado como clase confidencial, entonces el sistema debe seguir las directivas de la clase Pública, Interna y Confidencial.

Si un sistema contiene datos de más de una clase sensitiva, debe ser clasificado de acuerdo a la necesidad de los datos confidenciales en el sistema.

### 2.3.6 CONTROL DE ACCESO

Se ha considerado el Dominio 11 y Objetivo de Control 11.1; 11.2; 11.4

#### 2.3.6.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO

##### 2.3.6.1.1 POLITICA DE CONTROL DE ACCESO

- Todos los trabajadores deben ser autenticados.
- Los trabajadores deben ser capaces de modificar los datos que pertenecen a ellos y sólo podrán consultar los datos que pertenecen a otros usuarios siempre y cuando estos datos estén clasificados como información pública o interna.

- Se permite el acceso al sistema como administrador privilegiado solo vía consola o desde las estaciones que se defina.
- Se debe de controlar el acceso de los usuarios a todos los objetos en el sistema (archivos, impresoras, dispositivos, base de datos, comandos, aplicaciones, etc.).
- No se permite a los trabajadores conocer el acceso otorgado a otros usuarios.
- Identificar la información de acuerdo a la clasificación de sensibilidad previamente definida.
- El sistema debe proveer un control de acceso obligatorio.
- Sólo el administrador debe tener la capacidad de conectarse a los recursos del sistema en modo privilegiado para realizar tareas administrativas.

#### 2.3.6.2 GESTION DE ACCESO DE USUARIO

- Las cuentas de usuarios deben existir sólo para el personal autorizado.
- Cada usuario debe ser identificado por un nombre y pertenecer a un grupo dentro del sistema operativo o a un rol dentro de la base de datos.
- Los usuarios y grupos deben ser administrados por el administrador de la base o su delegado, pero no por los usuarios en sí.
- Cada usuario debe tener solamente una cuenta sobre el sistema operativo.
- Las cuentas como usuario huésped no son permitidas.

- No se debe permitir cuentas a las cuales se accede de un grupo de usuarios.
- La pantalla inactiva por un periodo de 15 minutos debe ser reactivada con un password de protección.
- Los usuarios deberán ser informados de acciones que violan la seguridad.

#### 2.3.6.3 CONTROL DE ACCESO A LA RED

##### 2.3.6.3.1 POLÍTICA DE USO DE LOS SERVICIO EN RED

- Documentación de configuración de la Red
- Documentar y autenticar cualquier sujeto en la red institucional.
- Si es posible debe haber un solo mecanismo de ingreso para los usuarios, evitando múltiples nombres de usuarios y passwords.
- En las redes de acceso restringido, el cableado no debe pasar a través de redes públicas, su conducción debe ser protegida y los puntos de conexión deben estar disponibles sólo a las personas autorizadas. el cableado debe ser inspeccionado y certificado.
- La red se requiere disponible las 24 horas del día, los 6 días de la semana. El horario de mantenimiento será el día domingo de 18:00 a 22:00 horas.
- Monitorear los errores y desempeño de la Red, tomar acciones preventivas antes de que ocurran interrupciones serias de la red.
- Se debe de tener una etiqueta que contenga la siguiente información y debe ser pegadas en todas las maquinas durante la instalación: nombre del equipo, fabricante, modelo de la

máquina, dirección IP, dirección MAC, identificar del nodo en el cableado (si la topología de la red lo permite), fecha de vencimiento de la garantía y número de teléfono de la línea de ayuda o seguridad.

- La firewall debe cumplir con políticas de seguridad y debe ser regularmente monitoreado y auditado.

#### 2.3.6.3.2 POLÍTICAS DE RESPALDO Y RECUPERACIÓN DE SERVIDORES APLICACIONES

- Definir al responsable que realizará los respaldos y la restauración.
- Los respaldos de información confidencial deben almacenarse en lugares con acceso restringido. Todos los respaldos deben ser contabilizados. Las cintas o discos viejos deben de ser destruidos.
- Se debe realizar un respaldo de cada uno de los logs de las aplicaciones.
- Se debe realizar un respaldo de los usuarios y conexiones a la base de datos.

#### 2.3.6.3.3 POLÍTICAS DE RESPALDOS Y RECUPERACIÓN DE LA BASE DE DATOS

- Sólo los DBA pueden realizar las tareas de respaldar y recuperar información.
- Los respaldos deben de hacerse regularmente y algunos de estos respaldos deben almacenarse en otra instalación.
- Se debe realizar un respaldo diario de los datos.

- Se debe realizar un respaldo diario de los datafile.
- Realizar un respaldo semanal de los redologs.
- Probar policitas de restauración cada mes.
- Documentar el tiempo de restauración esperado para varios escenarios de desastre.

#### 2.3.6.4 REDES

Información confidencial:

- Los datos confidenciales transmitidos sobre redes públicas deben ser encriptados.

#### 2.3.6.5 RESPONSABILIDAD PERSONAL DE REDES

- El personal encargado de la Red es responsable por la destrucción de cintas o discos defectuosos o viejos.

#### 2.3.6.6 CONTROL DE LA CONEXIÓN DE LA RED:

- Un trabajador del Policlínico no puede conectar una maquina a cualquier red excepto la LAN local
- El acceso a redes externas debe hacerse a través de un firewall.
- El firewall deben ser instalados y mantenidos por el encargado o responsable del mantenimiento de la Red.

#### 2.3.6.7 MÓDEMS

- Los empleados no deben tener módems en sus máquinas.
- El acceso Dial-in a la LAN del Policlínico es permitido solo para el encargado de la administración de la Red. Todos los accesos Dial-in deberán hacerse vía servidores seguros con mecanismos de password de una vez.

#### 2.3.6.8 CORREO ELECTRÓNICO

- La información clasificada como interna puede enviarse dentro de la compañía sin encriptación. La información

clasificada como confidencial debe ser encriptado. La información clasificada como secreta no puede ser transmitida vía correo electrónico.

- los trabajadores deben estar al tanto de los riesgos de abrir documentos con macros, archivos postcript y programas de instalación recibidos vía correo electrónico.
- Debe considerarse un esquema que permita la autenticación del emisor/receptor de información clasificada como confidencial. Por ejemplo, uso de firmas digitales.

#### 2.3.6.9 INTERNET

Debido a su carencia de estructura y controles, el internet debe evitar los siguientes riesgos:

- Revelación de información confidencial.
- La red institucional puede ser penetrada por hackers de internet.
- La información puede ser cambiada o borrada.
- El acceso a los sistemas podría ser negado a una sobrecarga del sistema.

Si los doctores van a tener acceso al internet, ellos deben estar al tanto de los riesgos y la política institucional en cuanto a consideraciones de uso de internet.

- Todos los accesos hacia el internet deben hacerse sobre Gateway de la empresa los cuales han sido certificados.
- Tienen acceso a internet personal administrativo, gerencia, técnicos.
- El software cliente de internet permitido puede ser el internet Explorer.
- No usar el acceso a internet para visualizar o descargar material pornográfico, descargar software peligroso o no licenciado, uso privado excesivo, etc.

### 2.3.6.10 POLITICA DE FIREWALL PARA INTERNET

- La política de firewall y su configuración deben ser documentadas correctamente.
- Los equipos de firewall deben estar sujetos a un monitoreo regular y una auditoria anual.
- La cuenta del administrador debe usar sesiones de login encriptadas.
- Instalar los equipos de firewall de modo seguro. Todos los servicios del sistema operativo no necesarios deben detenerse.
- Mantener registros históricos de todas las auditorias de seguridad.
- Deben haber y estar disponibles estadísticas de uso.
- Todos los accesos al internet desde la red de la empresa deben hacerse sobre proxys localizadas en un firewall.
- Ningún usuario debe ser capaz de ingresar directamente a los equipos de firewall.
- Debe chequearse regularmente (cada mes) la exactitud e integridad de los archivos localizados en los equipos de firewall.

### 2.3.6.11 POLÍTICAS DE PASWORDS

La identidad de los usuarios sobre el sistema está dada por la combinación del nombre de usuario y del password.

Los passwords deben cumplir los siguientes requerimientos:

- Tener una longitud de 8 caracteres.
- Tener al menos un carácter numérico, alfabéticos y caracteres especiales como "_&*.".
- No debe ser fácil de recordar. Por ejemplo, no debe ser igual al nombre del usuario.
- Debe ser fácil de digitar rápidamente, para que sea difícil de mirar por un observador.

- Deben ser validos por una rutina de verificación. La rutina de verificación debe de validar que el password cumpla con los requerimientos mencionados.

En la definición de los passwords evitar el uso de:

- Nombres como: esposa, padre, canción, amigo mes, día, pueblo, mascota.
- Palabras del diccionario común
- Una serie de letras o números idénticos.
- Secuencias de palabras obvias, como: "unodos"

Para la definición de passwords se sugiere:

- Escoger una línea de una canción, poema o cualquier párrafo y usar solo las primeras letras de un grupo de palabras.
- Juntar pequeñas palabras con un carácter de subrayado ("_").
- Inventarse un acrónimo (siglas).

Para asegurar la privacidad de los passwords, tomar en cuenta lo siguiente:

- No escribir en un lugar visible, o revelarlo por e.mail.
- No de su password a otra persona.
- No compartir el passwords del administrador.
- Informarle a los usuarios en detalle el éxito o el peligro de que su password sea revelado, un usuario bien educado es la mejor manera de asegurar buenas opciones de passwords.
- El passwords, de acuerdo a su novel de sensibilidad está clasificado como información secreta.
- Los passwords deben ser almacenados en una forma encriptada. La encriptación debe ser solida, que resista el forcejeo de la desencriptación.
- El password encriptado no debe estar embedido dentro del software tanto cuanto sea posible.

- El sistema debe chequear el contenido del password de acuerdo a las reglas definidas previamente, antes de aceptar el password.
- Solamente el usuario puede cambiar su password.
- Proveer un proceso que permita generar un nuevo password al usuario en caso de olvidos de su password, de modo similar a cuando ingresa por primera vez.

  En el tiempo de vida de los passwords considerar:
- El tiempo máximo de vigencia para los passwords es de 1 año. El usuario debe tener un periodo de gracia de 5 días de tal forma que en este lapso de tiempo el usuario pueda cambiar su password. Si no lo hace, entonces su cuenta expirará.

#### 2.3.6.12 POLÍTICAS GENERALES DE SOFTWARE

- El software no licenciado no debe ser usado.
- Los programas de juegos no son permitidos en las estaciones de trabajo de los usuarios.

#### 2.3.6.13 DIRECTIVAS PARA EL CENTRO DE CÓMPUTO

Se deben de cumplir las siguientes directivas para el área de cómputo

- Todos los dispositivos del centro de cómputo deben estar limpios y etiquetados.
- El cableado debe estar limpio, bien arreglado y etiquetado, tal que las conexiones no puedan ser accidentalmente desconectadas o rotas.
- Debe haber un diagrama con la ubicación de los equipos y dispositivos instalados en el centro de cómputo.

- El transporte de los medios eléctricos (cintas, repuestos, discos) debe hacerse considerando medidas que eviten dañarlos.

## 2.4 FASE III: DISEÑO FÍSICO DE LA RED

### 2.4.1 DISEÑO FISICO DE LA RED PROPUESTA

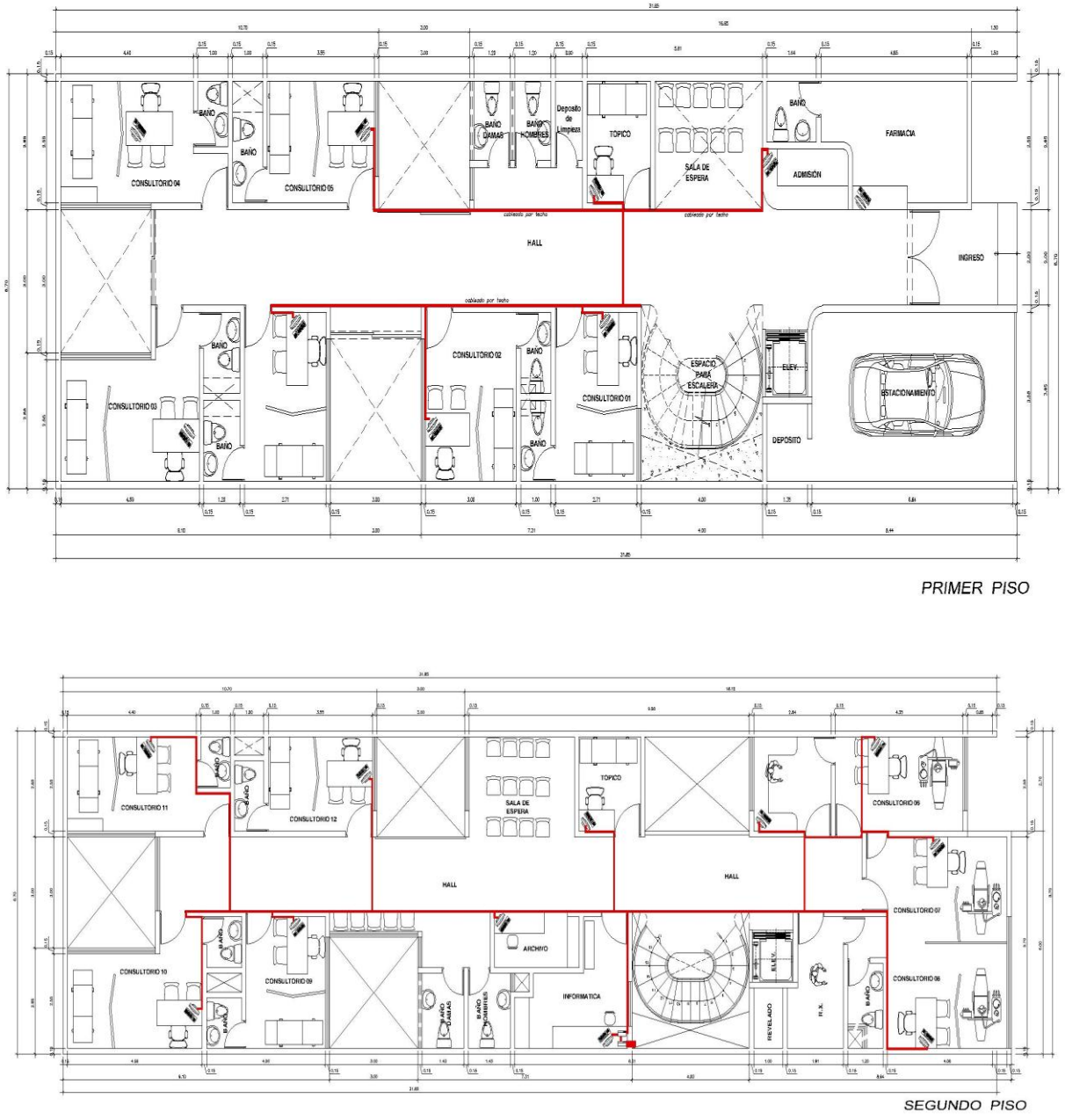



**Figura N° 10 Diseño Físico de La Red Del Policlínico**

### 2.4.2 SELECCIONAR TECNOLOGÍAS Y DISPOSITIVOS PARA LA RED

El sistema de cableado estructurado usan topología de tipo estrella extendida en donde todas las áreas de trabajo se enrutan hacia un punto principal, es por eso que en esta tesis se considera lo siguiente:

#### 2.4.2.1 TOPOLOGÍA

Para el desarrollo de este proyecto se utilizara la Topología Estrella bajo un esquema de cableado estructurado terminando este, en el cuarto de comunicaciones, se usara esta topología por las siguientes razones:

- Por el tamaño del Edificio que es grande amplio y de 3 plantas
- Permite la manejabilidad de la red
- Permite aumentar el número de dispositivos sin interrumpir el funcionamiento de la red.

#### 2.4.2.2 CABLEADO A UTILIZAR SEGÚN EIA/TIA 568B

Según EIA/TIA 568 B – 1.2 nos recomienda usar un cable UTP Categoría 6 y operaran con conectividad RJ45 la norma recomienda dos RJ45en cada lugar de trabajo, para unir el cuarto de comunicaciones hasta las rosetas, para la construcción de los latiguillos para conectar los Patch Panel con los Switchs y para la construcción de PatchCord que conectan las rosetas con los usuarios.

#### 2.4.2.3 DISPOSITIVOS DE RED

Los dispositivos a emplear según el cableado son: las rosetas las cuales deben ser de categoría 6 y por supuesto los latiguillos desde la roseta a cada pc. Un patch panel, el cual debe ser de categoria 6 y los latiguillos de esta hasta el switch.

Se determina la calificación de los dispositivos de acuerdo a un factor de ponderación establecido en función a sus características y necesidades técnicas de la red calificándose con un determinado peso ponderativo para así poder elegir el dispositivo de la marca especifica que se acerque o cumpla con dichos requerimientos técnicos. El siguiente Factor de ponderación nos ayudara a sopesar las características del producto en cuestión y requerimientos técnicos.

Factor de ponderación:

1. Malo
2. Regular
3. Bueno
4. Muy bueno
5. Excelente

Este proceso se aplica en las tres capas descritas en el diseño lógico, para su mejor estudio se detalla capa por capa comparando los productos de diferentes marcas o fabricantes.

#### 2.4.2.4 SWITCH

##### 2.4.2.4.1 PARA LA CAPA DE ACCESO

Para la capa de acceso se propone 1Switch de 24 puertos; se propone 3 Switch de 24 puertos de tres marcas diferentes, entre ellas tenemos Cisco, HP/3Com, D-Link y según sus características técnicas y en función a los requerimientos técnicos en la red se deberá elegir la mejor o una combinación de las tres realizando una comparación ponderativa.

| CARACTERISTICAS | FABRICANTES DE SWITCH | | |
|---|---|---|---|
| | D-LINK DES-1210-28P | HP V1910-24G | CISCO SF300-24 |
| **Protocolo y modo de comunicación** | 4 | 3 | 4 |
| **Velocidad de Transmisión** | 4 | 2 | 4 |
| **Espacios de expansión** | 3 | 2 | 3 |
| **Facilidad de Instalación** | 4 | 3 | 4 |
| **Fiabilidad** | 3 | 2 | 3 |
| **Rendimiento** | 4 | 2 | 4 |
| **Costo y Garantía** | 4 | 4 | 3 |
| **TOTAL** | 26 | 18 | 25 |

**Tabla N° 6 Ponderación para la Capa de acceso**

Para esta capa del proyecto se ha elegido los productos de marca D-LINK de acuerdo al cuadro comparativo, por las siguientes razones:

- Por su costo y Garantía de sus productos en cuanto a Switch
- Por ser fáciles de instalar
- Por incluir variedad de marcas reconocidas en el mercado y que sean compatibles en su implementación en el proyecto.
- Por tener un rendimiento de acuerdo a los estándares establecidos y estar a la par de productos como Cisco.
- Por su desempeño eficiente en esta capa en pequeñas y medianas redes existentes.

- Por ofrecer un amplio servicio técnico para soporte de sus productos.

#### 2.4.2.4.2 PARA LA CAPA DE DISTRIBUCIÓN

Para la capa de distribución del proyecto de red del Policlínico se propone 1 Switch en total de 8 puertos de tres marcas diferentes como son HP, D-Link, Cisco y según sus características técnicas se deberían elegir la marca mejor o una combinación de las tres realizando una comparación ponderativa.

| CARACTERISTICAS | FABRICANTES DE SWITCH | | |
|---|---|---|---|
| | D-LINKDGS-1210-10P | HP PS1810-8G, 8 RJ-45 GbE | CISCOSF300-08 |
| **Protocolo y modo de comunicación** | 3 | 3 | 4 |
| **Velocidad de Transmisión** | 3 | 2 | 4 |
| **Espacios de Expansión** | 3 | 3 | 4 |
| **Facilidad de Instalación** | 3 | 3 | 3 |
| **Fiabilidad** | 3 | 2 | 4 |
| **Rendimiento** | 3 | 3 | 4 |
| **Costo y Garantía** | 3 | 3 | 3 |
| **TOTAL** | 21 | 19 | 26 |

**Tabla N° 7 Ponderación para la capa de Distribución**

Para esta capa del proyecto se ha elegido los productos de marca HP de acuerdo al cuadro comparativo se especifica las siguientes razones:

- Por justificar su costo con el alto rendimiento del producto.
- Por ofrecer un amplio servicio técnico para soporte de productos HP
- En cuanto a rendimiento citar que este switch se encuentra diseñado principalmente para ser utilizado en grupos de trabajo que requieran conexiones de 10/100/1000 Mbps seguras, fiables y disponibles en todo momento sin bloqueos del dispositivo ni saturaciones en los momentos de máxima demanda de red.

#### 2.4.2.4.3 PARA LA CAPA CORE

Para la capa core se propone usar 2 Servidores con la finalidad de asegurar el acceso constante a los recursos, crear un cluster de Alta Disponibilidad y permitiendo la administración de la red y dar privilegios a los usuarios.

Para este proceso se tomara en cuenta la configuración mínima necesaria en cuanto a hardware se refiera para poder implementar los servicios requeridos en la red como son:

#### 2.4.2.4.4 SERVIDOR DE ARCHIVOS/DNS/ACTIVE DIRECTORY/ FIREWALL/PROXY

En esta parte se describe los requerimientos en cuanto a hardware se refiere para poder implementar el Servidor de Archivos, incluyendo el servidor DNS, Firewall/Proxy y el Controlador

de Dominio requeridos en este proyecto. Hemos elegido tres marcas para su estudio y evaluación como son IBM, DELL y HP que de acuerdo a sus características técnicas de sus productos pasamos a describir para luego elegir el Servidor adecuado para el proyecto.

| CARACTERISTICAS | MARCA DE SERVIDOR | | |
|---|---|---|---|
| | **HP** | **DELL** | **IBM** |
| **Configuración de hardware** | 4 | 3 | 3 |
| **Velocidad de Procesador** | 4 | 3 | 3 |
| **Memoria RAM** | 4 | 3 | 3 |
| **Escalabilidad** | 4 | 3 | 2 |
| **Garantía y Costo** | 4 | 4 | 4 |
| **Velocidad de respuesta Disco Duro (N° rpm)** | 4 | 4 | 4 |
| **TOTAL** | 24 | 19 | 18 |

**Tabla N° 8 Ponderación Servidor de Archivos**

#### 2.4.2.4.5 CUARTO DE COMUNICACIONES

El cuarto de comunicaciones o de equipos se instalara en el primer piso y constara de 5.m de largo, de ancho de 4m y 2.6 m de alto y está diseñado según lo establecido en la norma EIA/TIA 568-B y EIA/TIA 569 del Sistema de Cableado estructurado, y apoyándonos en la norma ISO 27002. En este cuarto de Comunicaciones se encuentran los equipos de conexión (Switch y Router). 1 Patch Panel de 24 puertos marca SATRA, así como los diferentes servidores conectados a los equipos de conexión.

#### 2.4.2.4.6 SUBSISTEMA DE PUESTA A TIERRA

El pozo a tierra se encuentra en la parte derecha, patio del Policlínico y consta de una jabalina de cobre, tipo Coperweld de 0.5 Ohm. Todas las salidas eléctricas para las computadoras estarán polarizadas y llevadas a una tierra común; del mismo modo todos los componentes metálicos tanto de la estructura como del cableado estarán debidamente llevados a tierra para evitar descargas por acumulación de estática. Además se debe de tomar en cuenta la ubicación del subsistema de Puesta a Tierra ya que se encuentra dentro de una zona transitable, se debe tomar las precauciones del caso como señalizar la zona de alto peligro, y dar la seguridad del caso ante las posibles descargas de corriente eléctrica.

#### 2.4.2.4.7 SELECCIÓN DE TECNOLOGÍAS Y DISPOSITIVOS PARA ACCES POINT

Para la solución inalámbrica utilizaremos el estándar 802.11 g ya que es un estándar que nos brinda una velocidad teórica máxima de 54Mb/s y es compatible con los estándares 802.11b.

En consecuencia los equipos que se utilizaran para este proyecto deberán trabajar con el estándar 802.11 b/g/n y utilizar la banda de 2.4 Ghz.

## Selección del Hardware a utilizar (Access Point)

| Especificaciones AP | PICOSTATION 2HP Ubiquiti | SENAO ENGENIUS EOC-5611 | **Cisco Aironet1300** |
|---|---|---|---|
| Potencia de Transmisión | 13 dbi | 13 dbi | 13 dbi |
| Estándares | 802.11 b/g | 802.11 a/b/g | 802.11 b/g |
| Costo del Equipo | s/ 300.00 | s/ 350.00 | s/1382.40 |
| Antena | Interna / Externa | Interna / Externa | Interna / 2 Externas |
| Temperatura de Operación | -20 °C a 70 °C | -20 °C a 70 °C | -30 °C a 55 °C |
| Seguridad | WEP Encryption 64/128/152 bit WPA/WPA2 Personal(WPA-PSK usando TKIP o AES) WPA/WPA2 Enterprise usando(WPA-EAP) 802.1x | WEP Encryption 64/128/152 bit WPA/WPA2 Personal(WPA-PSK usando TKIP o AES) WPA/WPA2 Enterprise usando(WPA-EAP) 802.1x Authenticador SSID oculta en broadcast 802.1Q Vlan MAC filtering | WEP Encryption 64/128/152 bit WPA/WPA2 Personal(WPA-PSK usando TKIP o AES) WPA/WPA |
| Alcance | 40 km | 10 km | 10 – 30 km |
| Garantía | 1 año | 1 año | 1 año |
| Potencia de Salida | 1000 mw | 500 mw | 400 mw |
| Rango de Frecuencia | 2.4 Ghz | 2.4 Ghz y 5.8 Ghz | 2.4 Ghz y 5.8 Ghz |
| RESULTADO | ACEPTABLE | PARA OTRAS CONDICIONES | COSTO ELEVADO |

**Tabla N° 9 Cuadro de comparación de Tecnologías (Access – Point)**

### 2.4.3 PLANO DE DISTRIBUCIÓN PROPUESTO DEL CABLEADO DE LA RED

En el siguiente plano se propone establecer la ubicación exacta y su respectivo cableado horizontal por las canaletas, las respectivas rosetas que conectaran a los usuarios finales en la red así como la respectiva entrada de la señal de Internet mediante acceso inalámbrico. Toda esta distribución se realiza teniendo en cuenta la normatividad existente para la instalación del Cuarto de comunicaciones **(ANS/TIA/EIA-568-B y ANSI/TIAEIA-569)** así también de la administración para la infraestructura de telecomunicaciones **(ANSI/TIA/EIA-606),** y por último el estándar que establece los requerimientos de puesta a tierra **(ANSI/TIA/EIA-607).**

| AREA | DISTANCIA PARCIAL | DISTANCIA TOTAL |
|---|---|---|
| **Administración** | 3 m x 5m | 15 m |
| **Recepción** | 3 m x 5m | 15 m |
| **Consultorios** | 3 m x 5m | 15 m |
| **Total de cable** | | **300 m** |

**Tabla N° 10 Áreas y Distancias Totales**

### 2.4.4 ESTUDIO DE COSTOS PARA LA REALIZACIÓN DE LA RED

#### 2.4.4.1 EQUIPOS DE CONECTIVIDAD

| DESCRIPCIÓN | CANTIDAD | PRECIO | TOTAL |
|---|---|---|---|
| D-LINK | 1 unid. | S/.1700 | S/.1700 |
| HPSwitch | 1 unid. | S/.279 | S/.279 |
| **SUBTOTAL** | | **S/.1979** | |

**Tabla N° 11 Cuadro de los costos de los Equipos de conectividad**

### 2.4.4.2 METRAJE DE CABLE UTP CATEGORÍA 6

| PISO | CANTIDAD DE CABLE | N° PUNTOS |
|---|---|---|
| **Primer Piso** | 260m. | 8 |
| **Segundo Piso** | 100 m. | 8 |
| **TOTAL : 440 mt** | | 16 |

**Tabla N° 62 Cuadro para calcular el metraje a utilizar**

Según Los Planos el local tiene un metraje de 100 metros cuadrados y por cada laboratorio un excedente de 2 metros * 8 PC nos da igual a 160 metros de cable por cada consultorio

Cantidad de Rollos a Utilizar = 1 ½ rollo (1 rollo tiene 305 metros) se utilizará

- Numero de Conectores =Número de puntos * 2

  **16 puntos * 2 = 32 conectores.**

  Número de rosetas = Número de puntos /2

  **16 puntos / 2 = 8 rosetas.**

### 2.4.4.3 CABLE Y CONECTORES

| DESCRIPCIÓN | CANTIDAD | PRECIO | TOTAL |
|---|---|---|---|
| **Cable UTP Categoría 6** | 1 1/2 | S/. 360.00 | S/. 540.00 |
| **Conectores Categoría 6** | 32 | S/. 2.50 | S/. 80.00 |
| **Rosetas Categoría 6** | 8 | S/. 25.00 | S/. 200.00 |
| **Jacks Categoría 6** | 8 | S/. 15.00 | S/. 120.00 |
| **TOTAL** | | **S/. 940.00** | |

**Tabla N° 13 Cuadro de los costos de los Cables y Conectores**

#### 2.4.4.4 SERVIDORES

| DESCRIPCIÓN | CANTIDAD | PRECIO | TOTAL |
|---|---|---|---|
| **Servidor HP ProLiant ML370 Gen6** | 2 unid. | S/.10900 | S/.21800 |
| **TOTAL** | | **S/.21800** | |

**Tabla N° 7Cuadro de los costos de los Servidores**

#### 2.4.4.5 PRESUPUESTO TOTAL

| MATERIAL Y/O SERVICIO | COSTO |
|---|---|
| **Equipos de conectividad** | **S/.1979** |
| **Cables y conectores** | **S/. 940.00** |
| **Servidores (físicos)** | **S/.10900** |
| **TOTAL** | **S/.** |

**Tabla N° 8Cuadro de Presupuesto Total**

### 2.4.5 PLAN DE CONTINGENCIA PARA SOLUCIONES A PROBLEMAS

Se enfoca las contingencias relacionadas con fallas menores que se suscitan en el normal funcionamiento de la red de información.

#### 2.4.5.1 ÁREA DE REDES Y COMUNICACIONES

La ocurrencia de fallos en la red, puede darse en alguno de los componentes de la misma como:

- Equipos y enlaces de comunicaciones
- Acceso a internet
- Servidores de red
- Estación de trabajo
- Equipos de impresión

El fallo de un componente es factible ser focalizado de manera precisa, dado que cada uno de ellos le corresponde brindar un servicio, el mismo que en caso de ocurrencia de errores, deniega el servicio para el cual fue implementado.

#### 2.4.5.2 EQUIPOS DE ENLACE DE COMUNICACIÓN

##### 2.4.5.2.1 Fallas

- Equipos remotos no pueden acceder a aplicaciones de los servidores.
- Los equipos de monitoreo no detectan a los equipos remotos.

##### 2.4.5.2.2 Acciones a tomar

- Asegúrese que los equipos de comunicación estén encendidos (router, switch, etc)
- Ejecute el comando ping en el Pront del sistema, a fin de verificar comunicación con la inter fase LAN.
- En primer lugar verificamos que el puerto LAN del firewall de intranet se encuentre activo y la comunicación con este esté en buen estado, para lo cual ejecutamos el comando:
  Ping puerto LAN del firewall.
- En caso de no tener respuesta afirmativa verificar cables de comunicación y verificar estado de la firewall. Si la respuesta es afirmativa, se debe de comprobar que la comunicación con el router esté activa, para lo cual ejecutamos el comando:
  Ping para el caso de la PC de Administración
  Ping para el caso de la PC de Laboratorio

- En caso de no tener resultados positivos verifique cable de conexión del router al firewall.

#### 2.4.5.3 ACCESO A INTERNET

##### 2.4.5.3.1 Fallas

- Los consultorios no tienen acceso a internet
- El monitor de internet reporta fallos

##### 2.4.5.3.2 Acciones a tomar

- Asegúrese que los equipos de comunicaciones para internet están encendidos, esto es: router de internet, radio de comunicaciones.
- Desde el pront de la PC, ejecute telnet al router, con la finalidad de verificar estado de los puertos de comunicación y del enlace, para esto ejecutamos el comando:
  telnet servidor de internet
- Passwords para ingreso como administrador de los diferentes routers.
- De no existir resultados positivos verificar el cable de conexión del router al switch.

#### 2.4.5.4 SERVIDOR DE RED

Los servicios de red que son proveídos por servidores locales son: DHCP y DNS

##### 2.4.5.4.1 FALLAS EN SERVIDORES DE DHCP Y DNS

- No existe comunicación entre las diferentes máquinas de la red LAN
- Ninguna de las estaciones de trabajo tiene asignado una dirección IP

##### 2.4.5.4.2 Acciones a tomar

- Verifique que el equipo servidor este encendido

- Verifique que el equipo servidor esté conectado a la red
- Verifique que la configuración de acceso a redes, del equipo, se encuentre bien.
- Verifique que el servidor de DHCP server se encuentre iniciado
- En caso de no tener respuesta positiva con todas estas acciones es necesario verificar configuración o definitivamente reconfigurar el servicio.

#### 2.4.5.5 FALLAS EN EL SERVIDOR DNS

- Al intentar comunicación con otros equipos, utilizando el nombre de alto nivel del equipo destino, obtenemos el mensaje Host no reconocido.

##### 2.4.5.5.1 Acciones a tomar

- Verificar si el equipo servidor de DNS se encuentra encendido.
- Verificar que el equipo servidor se encuentre conectado a la red.
- Verifique que la configuración de acceso a red del equipo se encuentre bien.
- Verificar que el servido de DNS se encuentre iniciado
- En caso de no tener respuesta positiva con todas estas acciones es necesario verificar configuración o definitivamente reconfiguración del servicio

#### 2.4.5.6 ESTACION DE TRABAJO

Dado que las estaciones de trabajo son usuarias de todos los servicios de red, así como las aplicaciones que se hacen,

existen mayor cantidad de parámetros por verificar, tanto en la parte de comunicaciones como de acceso a aplicaciones.

#### 2.4.5.6.1 FALLAS EN COMUNICACIONES

- No visualiza ningún computador perteneciente al grupo de la estación.
- No se tiene asignada una dirección IP
- No se tiene respuesta utilizando nombres de alto nivel.

#### 2.4.5.6.2 Acciones a tomar

- Verificar el pacthcord se encuentre conectado a tarjeta de red y al punto de datos del cableado estructurado.
- Ejecutar el comando ipconfig en el Pront del sistema, a fin de obtener información de dirección IP, default gateways, etc.
- Si no se tiene respuesta positiva al requerimiento anterior, se debe habilitar en cada uno de los clientes de los servicios la configuración automática, a fin de obtener estos parámetros del servidor.

### 2.4.5.7 EQUIPOS DE IMPRESIÓN

#### 2.4.5.7.1 FALLAS DE IMPRESIÓN

- Al realizar el envío de impresión a una impresora de red, esta no es detectada por la maquina origen.
- No se encuentra ninguna impresora instalada en un computador personal.
- Es detectada la impresora de red pero no se produce la impresión.

#### 2.4.5.7.2 ACCIONES A TOMAR

- Verifique que la impresora de red se encuentre encendida.

- Ejecute el comando ping en el pront del sistema, a din de verificar comunicación con la impresora de red: C;/ > ping <DIR IP - IMPRESORA>
- Verificar que la impresora tenga disponibilidad de papel.
- Ejecutar en la impresora una impresión a prueba y de seteo de la impresora, si la impresora ha cambiado sus parámetros de configuración, volver a realizar la configuración utilizando como procedimiento el respectivo manual de instalación de la impresora.
- Verificar que el software de impresión de la impresora local, no haya cambado sus parámetros de configuración.

**Capítulo III**

# DISCUSIÓN DE LOS RESULTADOS

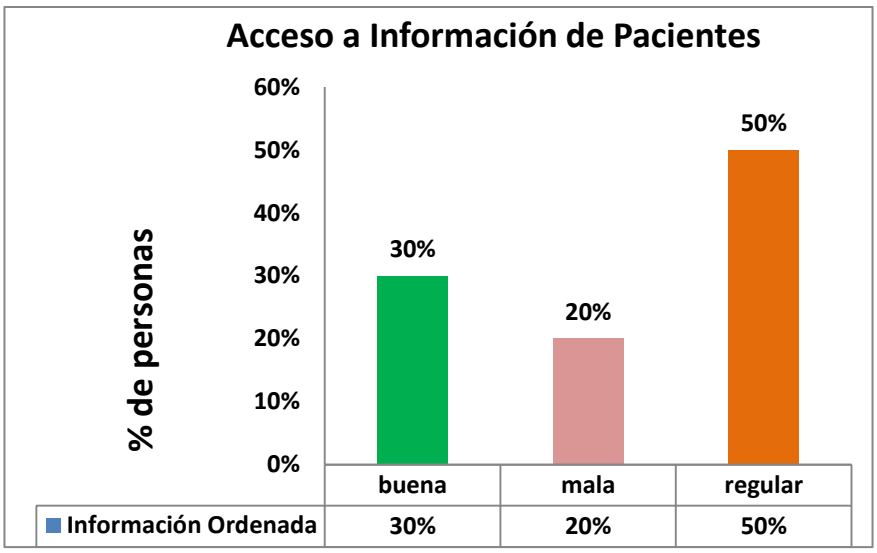
En este capítulo se presenta la discusión de los resultados obtenidos en la investigación.

- Al aplicar los dominios de control 5 y 11 de la ISO 27002, se ha recopilado la información de los Activos y funciones de la empresa dando como resultado el apoyo a definir políticas de seguridad, con la descripción de las acciones que se deben realiza para salvaguardar la integridad de los trabajadores y clientes en el policlínico.
- Mediante una encuesta tomada de la ISO 27002, nos ha permitido poyar en la gestión de proteger datos de los pacientes del Policlínico, teniendo como resultado, el cumplimiento de la Ley Nro. Nº 29733, Ley de Protección de Datos Personales DECRETO SUPREMO Nº 003-2013-JUS artículo 2 numeral 6 de la Constitución Política del Perú.
- Por medio de una encuesta se pudo ver que la norma ISO, nos ha permitido unificar los trabajos de los doctores con otras áreas del policlínico, lo que se establece una sistemática de trabajo y se deja de lado la improvisación, lo cual se espera reducir el 86% lo cual se toma al buscar la información de los pacientes.

| ¿Encuentra usted la información de los clientes de manera ordenada? | ¿Cómo calificaría el tiempo que le toma en almacenar la información del paciente? | ¿Cree usted que interconectando en red las computadoras del policlínico mejorarían los procesos de almacenamiento y búsqueda de pacientes? | ¿Tiene conocimiento de políticas de seguridad del policlínico? | ¿Cree usted que los datos de los pacientes son seguros? | ¿Los equipos están protegidos sobre posibles amenazas físicas y ambientales? | cuantos pacientes atiende |
|---|---|---|---|---|---|---|
| regular | regular | buena | no | regular | regular | 16 |
| regular | buena | buena | no | regular | regular | 14 |

| | | | | | | |
|---|---|---|---|---|---|---|
| mala | regular | buena | no | regular | regular | 12 |
| mala | regular | buena | no | buena | buena | 11 |
| regular | regular | regular | no | mala | regular | 15 |
| buena | buena | regular | no | buena | mala | 16 |
| regular | regular | buena | no | buena | regular | 12 |
| regular | mala | buena | no | regular | buena | 11 |
| buena | regular | buena | si | regular | regular | 10 |
| buena | regular | regular | si | regular | regular | 12 |

| Etiquetas de fila | Cuenta de ¿Encuentra usted la información de los clientes de manera ordenada? | Cuenta de ¿Encuentra usted la información de los clientes de manera ordenada ?2 |
|---|---|---|
| buena | 30% | 3 |
| mala | 20% | 2 |
| regular | 50% | 5 |
| **Total general** | **100.00%** | **10** |



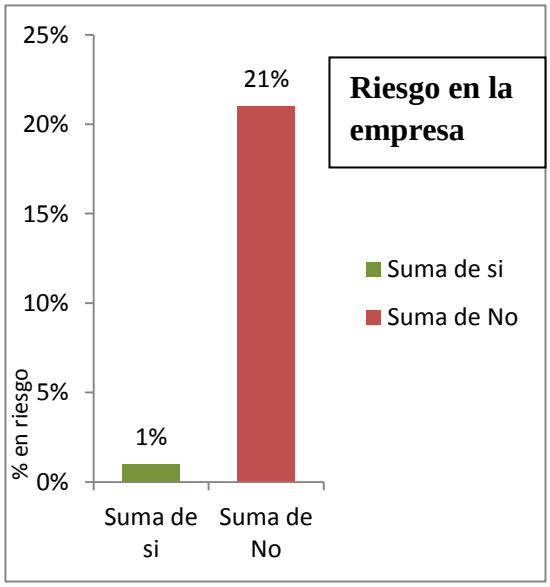

Encontramos un 50% quienes consideran que la información que se busca de un paciente es regular cuando se realiza de manera manual, se ha logrado unificar los trabajos del policlínico reduciendo este porcentaje a un 30% con la implementación de la red.

- Para los controles de accesos a la red se ha diseñado políticas de uso de servicios de red (según el punto 2.3.6.3) se espera tener como resultado una red disponible las 24 horas del día, los 6 días de la semana. El horario de mantenimiento será el día domingo de 18:00 a 22:00 horas.

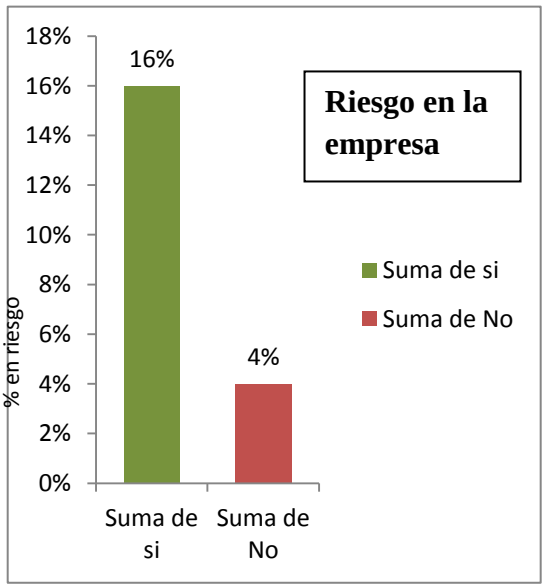
- Al aplicar el dominio 7 de la Norma ISO 27002 nos ha dado como resultado apoyar en políticas de responsabilidad para un mejor manejo de los Activos del Policlínico ver puno (2.3.5.1).

- La certificación ISO se aplicó una guía de levantamiento de información de riesgo el cual nos dio como resultado una mejora del 16% en el diseño e implementación de la Red ante una crisis encontrada en 21%.

| Si está protegido | No está protegido |
|---|---|
| 1% | 21% |
| 1 | 21 |




| Si está protegido | No está protegido |
|---|---|
| 16% | 4% |
| 1 | 21 |



# CONCLUSIONES

1. El Formato 001 del Anexo 1, el cual se diseñó para controlar los riesgos de la empresa en el diseño de la red, nos ha permitido procesar, documentar e identificar los Objetivos y las Necesidades del policlínico.

2. Mediante el análisis y diseño se logró implementar el modelo lógico de la red con ayuda de la metodología Top Down Network design.

3. El aplicar los estándares ISO/IEC 27002 (según el dominio 5, dominio 7 y dominio 11) se ha permitido obtener un manual de información con respectos a los activos del Policlínico, para archivarlos en caso de una auditoria externa.

4. Del análisis de 20 encuestas obtenidas se ha podido diseñar políticas de seguridad de Información, política de respaldo de Red, política de internet, políticas de password, Políticas de Firewall y un plan de contingencias en caso de alguna falla o siniestro, estás permitirán tener también un mayor control sobre todos los activos que maneja el policlínico a un 100%.

## RECOMENDACIONES

- Para establecer la selección del hardware y software se deberá crear cuadros comparativos en función a los diversos requerimientos técnicos y necesidades de la Empresa y de acuerdo a las características que cumpla con dichos requerimientos.

- Se recomienda seguir todos los puntos señalados en el proyecto al momento de instalar la Red para que se cumpla todas las características de las Norma ISO/IEC 27002 ISO/IEC 27002 (según el Dominio 5, Objetivo de Control 5.1; Controles 5.1.1; Dominio 7, Objetivo de Control 7.1, 7.2, Controles 7.1.1, 7.1.2; Dominio 11 y Objetivo de Control 11.1, 11.2, 11.4, 11.5; Controles 11.1.1, 11.2.3, 11.4.1, 11.4.6).

- Es importante dejar siempre documentado la instalación, o los cambios que se realicen, para facilitar el mantenimiento del administrador y para ayudar en futuras capacitaciones al nuevo personal que administrara la red.

- Se deberá de realizar una capacitación a todos los trabajadores del Policlínico con el propósito de mejorar la utilización de la Red y su uso en la gestión de servicios.

- La Persona encargada de la red deberá realizar un monitoreo frecuente, para el buen desempeño de la misma es por eso que se creado un historial de modificaciones ver anexo1 cuadro 4.

- Para la implementación de la red se deberá usar una Pc estándar con los requerimientos necesarios para instalar el Windows server 2008 que cumplirá las función de un file server, directorio activo y entre otros servicios necesarios para empresa.

## REFERENCIAS BIBLIOGRAFICAS


- The ISO 27000, D. (2 de ENERO de 2013). *27000.org*. Recuperado el 20 de OCTUBRE de 2013, de 27000.org: http://www.27000.org/
- ENCICLOPEDEA. (10 de 09 de 2013). *Domain Name System*. Recuperado el 10 de 09 de 2013, de Domain Name System: http://es.wikipedia.org/wiki/Domain_Name_System
- PAT, L. (24 de JUNIO de 2013). *IP reference*. Recuperado el 09 de 09 de 2013, de IP reference: http://ipref.wordpress.com/2008/11/28/modelo-jerarquico-de-red/
- CISCO SYSTEMS, I. (2004). *GUÍA DEL PRIMER AÑO. CCNA 1 Y 2 Tercera Edicion España.* MADRID: PEARSON EDUCACION.
- COMPUTING. (08 de 09 de 2013). *ACM Computing Empleo Website*. Recuperado el 08 de 09 de 2013, de ACM Computing Empleo Website: http://computingcareers.acm.org/
- FEDERICO REINA TORANZO, J. A. (Marzo de 2009-2013). *Universidad de Sevilla.* Recuperado el 23 de Agosto de 2013, de Universidad de Sevilla: http://www.forpas.us.es/aula/hardware/dia4_redes.pdf
- García Trejo, J. (2006-2013). *Digitecnia S.A. de C.V*. Recuperado el 20 de SETIEMBRE de 2013, de Digitecnia®: http://www.icono-computadoras-pc.com/redes-cableadas.html
- GOWEX, G. (20 de Enero de 2009-2013). *telcommunity*. Recuperado el 13 de Agosto de 2013, de Grupo Gowex: http://www.telcommunity.com/productos-wifi/recursos/
- METODOLOGIASREDES. (24 de mayo de 2013). *metodologiaspararedes.com.* Recuperado el 22 de Octubre de 2013, de metodologiaspararedes.com: http://metodologiaspararedes.blogspot.com/
- NÚÑEZ SANDOVAL, A. (2 de julio de 2012). *Enterate en Linea.com*. Recuperado el 26 de Setiembre de 2013, de Enterate en Linea.com: http://www.enterate.unam.mx/Articulos/2005/febrero/seguridad.htm
- Oppenheimer, P. (2011). *Top-down Network Design* (3era Edicion ed.). USA: Cisco Press: Cisco Systems.
- Ruben Fuentes BS, M. (2013). *YO PROFESOR.* Recuperado el 10 de 9 de

2013, de YO PROFESOR: http://yoprofesor.ecuadorsap.org/wp-content/uploads/2013/05/manual_redes.pdf

- SOFT, S. (2012). *SKYWARD SOFT COM*. Recuperado el SETIEMBRE de 2 de 2013, de SKYWARD SOFT COM: http://www.skyward-soft.com/iptrafficmonitor.html
- TABARES RODRIGUEZ, P. (3 de SETIEMBRE de 2012). *cables para RED*. Recuperado el 2013 de 08 de 2013, de cables para RED: http://cables-para-red.blogspot.com/2012/09/cables-para-red-tipos-caracteristicas.html
- WORDPRESS, W. (23 de Marzo de 2012). *gentegeek.com*. Recuperado el 8 de Agosto de 2013, de gentegeek.com: http://www.gentegeek.com/sl-sp-ventajas-desventajas/
- Br. Guerra Moya, Gary Antony, Br. Oruna Lara, Marco Antonio, Diseño de una red de datos para el diario nuevo norte usando la metodología Topdown Network Design, UPAO, 2012.
- Oppenheimer, Priscilla. (2011). Top-Down Network Design (3ª edición ed.). Indianapolis ,USA: Cisco Press
- CISCO SYSTEMS, I. (2004). GUÍA DEL PRIMER AÑO. CCNA 1 Y 2 Tercera Edicion España. MADRID: PEARSON EDUCACION.
- Stallings, William. (2004). Comunicaciones y Redes de Computadoras, 7 edición, Person Educación S.A., Madrid, España.
- Tanenbaum, Andrew S. (2003). *Redes de Computadoras* (4ª edición ed.). (G. T. Mendoza, Ed.) Mexico, Mexico: Pearson Education.

# ANEXOS

**ANEXO 1**
**ENCUESTA 1**

## GESTIÓN DE INFORMACIÓN DEL POLICLINICO

1. ¿Cuántas computadoras tiene el Policlínico?

   _____

2. ¿Cuántas computadoras están interconectadas en Red en el Policlínico?

   _____

3. ¿De qué manera el policlínico realiza sus procesos de registro clientes, citas consultas médicas y entrega de resultados clínicos?

   _____

4. ¿Conoce usted de servidores?

   _____

5. ¿Creé usted que una Red de datos ayudara en la gestión de información de los pacientes?

   _____

6. ¿El policlínico tiene pensado en expandirse a futuro?

   _____

7. ¿El policlínico tiene pensado en certificarse?

   _____

8. ¿Qué tipo de certificado busca?

   _____

9. ¿El policlínico tiene normas o políticas de seguridad?

   _____

**ENCUESTA 2**

**DISEÑO DE UNA RED DE DATOS**

Encuesta aplicada a los encargados de la recepción de los pacientes del Policlínico Señor de los Milagros

| Nro. | **PREGUNTAS** | **RESPUESTA** |
|---|---|---|
| 1 | ¿Encuentra usted la información de los clientes de manera ordenada a la hora de buscarla? | BUENA |
| | | REGULAR |
| | | MALA |
| 2 | ¿Cómo calificaría el tiempo que le toma en almacenar la información del paciente? | BUENA |
| | | REGULAR |
| | | MALA |
| 3 | ¿Cree usted que interconectando en red las computadoras del policlínico mejorarían los procesos de almacenamiento y búsqueda de pacientes? | BUENA |
| | | REGULAR |
| | | MALA |
| 4 | ¿Tiene conocimiento de las políticas de seguridad del policlínico? | SI |
| | | NO |
| 5 | ¿Cree usted que los datos de los pacientes son seguros? | BUENA |
| | | REGULAR |
| | | MALA |
| 6 | ¿Los equipos están protegidos sobre posibles amenazas físicas y ambientales? | BUENA |
| | | REGULAR |
| | | MALA |
| 7 | ¿A cuántos pacientes atiende? | |

**RESULTADOS BASADO EN LA: RESPUESTA DE 10 PERSONAS DE LA POBLACIÓN TOTAL DE 20**

| ¿Encuentra usted la información de los clientes de manera ordenada a la hora de buscarla? | ¿Cómo calificaría el tiempo que le toma en almacenar la información del paciente? | ¿Cree usted que interconectando en red las computadoras del policlínico mejorarían los procesos de almacenamiento y búsqueda de pacientes? | ¿Tiene conocimiento de políticas de seguridad del policlínico? | ¿Cree usted que los datos de los pacientes son seguros? | ¿Los equipos están protegidos sobre posibles amenazas físicas y ambientales? | cuantos pacientes atiende |
|---|---|---|---|---|---|---|
| regular | regular | buena | no | regular | regular | 16 |
| regular | buena | buena | no | regular | regular | 14 |
| mala | regular | buena | no | regular | regular | 12 |
| mala | regular | buena | no | buena | buena | 11 |
| regular | regular | regular | no | mala | regular | 15 |
| buena | buena | regular | no | buena | mala | 16 |
| regular | regular | buena | no | buena | regular | 12 |
| regular | mala | buena | no | regular | buena | 11 |
| buena | regular | buena | si | regular | regular | 10 |
| buena | regular | regular | si | regular | regular | 12 |

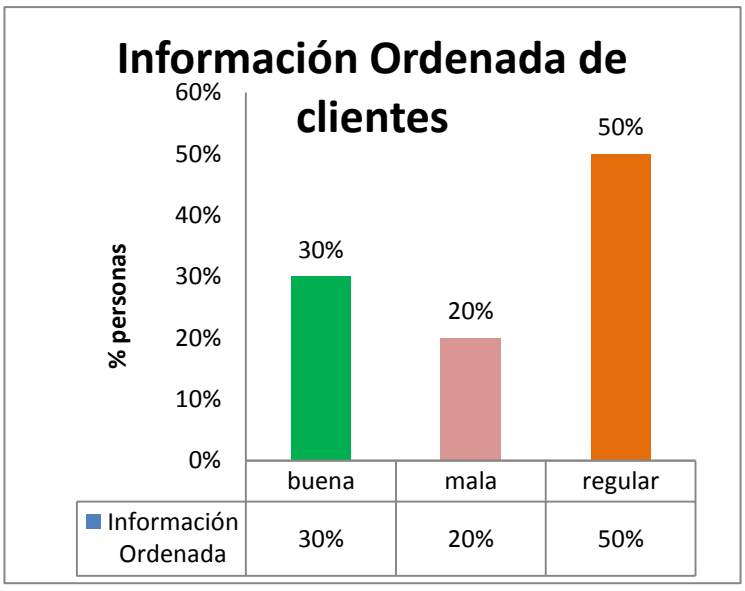
**Tabla N° 9 Tabla encuesta para el diseño de una Red.**

## Cuadros Estadísticos de los Resultados de la Encuesta Obtenida del Policlínico "Señor de Los Milagros"

### 1. Buscar información de un paciente

Esta grafica representa la búsqueda de información de un paciente sin el uso de un sistema de Red, observamos que el 50% de los enfermeras informan que se realiza de manera regular debido a que tienen muchas veces que esperar a que el doctor llegue para poder buscar la información

Sin duda estos valores nos demuestran que existe una gran deficiencia en todos los procesos que se tengan para obtener información de los pacientes.

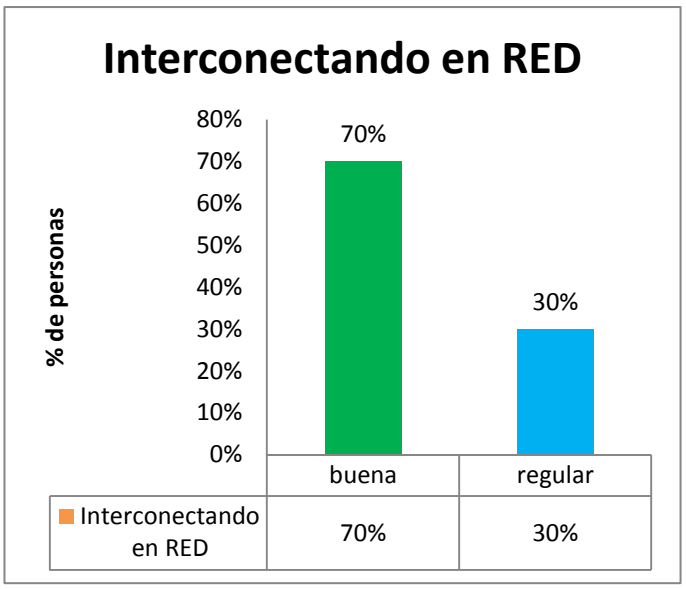


## 2. Interconectando en red las computadoras

| Etiquetas de fila | ¿Cree usted que interconectando en red las computadoras del policlínico mejoran los procesos de almacenamiento y búsqueda de pacientes? | TOTAL |
|---|---|---|
| buena | 70% | 7 |
| regular | 30% | 3 |
| **Total general** | **100.00%** | **10** |

Esta grafica representa el mejoramiento de los procesos de información de los pacientes teniendo 70% buena aceptación por parte de los encargados del policlínico

Sin duda estos valores nos demuestran que existe una correcta forma de procesar la información de los pacientes.



### 3. Formato para levantamiento de Información de riesgo en la empresa

| **Formato - 001** | | Puntuación total de las protecciones encontradas. | |
|---|---|---|---|
| Nro. | Preguntas | si | no |
| 1 | ¿La empresa está autorizada por una ley? | si | |
| 2 | ¿Todos los trabajadores están autenticados? | | no |
| 3 | ¿Se tiene controlado el acceso de los usuarios a los lugares no establecidos? | | no |
| 4 | ¿Proceden los datos de fuentes accesibles al público? | | no |
| 5 | ¿Se han seguido los pasos necesarios para la Protección de Datos de los pacientes en los ficheros o tratamientos de datos personales? | | no |
| 6 | ¿Sólo el administrador tiene la capacidad de conectarse a los recursos del sistema? | | no |
| 7 | ¿Se ha publicado la de manera visible las políticas de seguridad? | | no |
| 8 | ¿Se adoptan, en su caso, las garantías necesarias para el tratamiento de datos con finalidades históricas, científicas o estadísticas? | | no |
| 9 | ¿Existen mecanismos y procedimientos mal implementados y que no se sujetan a las normas establecidas? | | no |
| 10 | ¿El servidor de BD es accesible físicamente por personal no autorizado? | | no |
| 11 | ¿Se tiene documentación de configuración de la Red? | | no |
| 12 | ¿El cableado de la red pasar a través de las redes públicas? | | no |
| 13 | ¿La red se encuentra protegida según las normas establecidas? | | no |
| 14 | ¿Se monitorean los errores y desempeño de la Red? | | no |
| 15 | ¿La firewall cumple con políticas de seguridad y esta regularmente monitoreado? | | no |
| 16 | ¿Las BD tienen respaldo de seguridad? | | no |

| | | | |
|---|---|---|---|
| 17 | ¿La información clasificada como interna se envía dentro de la compañía sin encriptación? | | no |
| 18 | ¿Los Gateway de la empresa han sido certificados? | | no |
| 19 | ¿Se tiene historial de todas las auditorias de seguridad? | | no |
| 20 | ¿Se cuenta con proxy localizada en un firewall? | | no |
| 21 | ¿Todos los dispositivos de cómputo etiquetados? | | no |
| 22 | ¿Se utilizó la Norma EIA/TIA 568 B – 1.2 para la construcción de la red? | | no |
| | | Total 1 | 21 |

| si | No |
|---|---|
| 1 | 21 |

| | |
|---|---|
| **RIESGO** | Nivel Alto Riesgo |

Se pudo detectar un riesgo alto en el policlínico del 21% lo que se bajara a un nivel de riesgo bajo es decir a un nivel de 0.5%

## 4. Historial de modificaciones

| **Fecha** | **Versión** | **Creado por** | **Descripción de la modificación** |
|---|---|---|---|
| 10/01/2013 | 0.1 | Antonio Miranda | Descripción básica del documento |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**ANEXO 2**

**SWICHT PARA LA CAPA DE ACCESO**

**CARACTERISTICAS SWITCH DLINK DES-1210-28P, 24**

**Especificaciones**

| CARACTERISTICAS | DESCRIPCION |
|---|---|
|  | **Switch Web Smart D-Link DES-1210-28P, 24 RJ-45 10/100/1000 Mbps PoE, 2 RJ-45 LAN GbE.** |
| MARCA | DLINK |
| MODELO | **DES-1210-28P** |
| PUERTOS | 24 puertos 10/100/1000 |
| ESTANDARES | Estandard IEEE 802.3 10BASE-T<br>Estandard IEEE 802.3u 100BASE-TX<br>Estandard IEEE 802.3x control de flujo en modo full-dúplex |
| PRINCIPALES CARACTERISTICAS | -Web-BasedGui<br>-Soporta Ipv4<br>-Cli<br>-Telnet Server<br>-UserAccount<br>-Trusted Host<br>-Configuration File Upload/Download<br>-Firmware File Backup/Upgrade<br>-Dhcp Auto-Configuration |
| SEGURIDAD | -802.1x port-basedaccess control<br>-d-link safeguardengine<br>-portsecurity<br>-broadcaststorm control<br>-mac estática<br>-dhcp server screening<br>-arpspoofingpreventionssl |
| MODO DE COMUNICACION | Full-Dúplex, permite proteger a los usuarios frente a posibles pérdidas de datos durante la transmisión en la red. |
| ESPECIFICACION FISICA | - Dimensiones (producto): 440 (Largo) x 210 (Ancho) x 44 (Alto) mm<br>- Peso CE: 2.993 kg |

**Tabla N° 10 DLINK 1210-28P**

## CARACTERISTICAS SWITCH HP V1910-24G

| CARACTERISTICAS | DESCRIPCIÓN |
|---|---|
|  | **SWITCH HP V1910-24G RJ-45 LAN GbE, 4 SFP GbE** |
| MARCA | HP |
| MODELO | **V1910-24G** |
| PUERTOS | 24 puertos 10/100 Mbps |
| ESTANDARES | IEEE 802.3 10BASE-T<br>IEEE 802.3u 100BASE-TX<br>IEEE 802.3ab 1000BASE-T |
| PRINCIPALES CARACTERISTICAS | • 24 puertos RJ-45 10/100 de detección automática (IEEE 802.3 tipo 10Base-T, IEEE 802.3u tipo 100Base-TX), dúplex: semi o completo. |
| SEGURIDAD | • UL 60950; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1-03 |
| DESCRIPCIÓN | El HP V1910-24G es un switch 10/100/1000 de 24 puertos, sin bloqueo y sin administración diseñado para oficinas pequeñas a medianas. Este switch de clase empresarial, que se puede instalar en un rack, puede colocarse en el armario de cableado o como unidad autónoma.<br>El switch viene pre-configurado para una instalación rápida y fácil, utilizando económicos cables de cobre. Su auto-negociación ajusta la velocidad del puerto con la del dispositivo de comunicación. Cualquiera de los 24 puertos del switch puede ofrecer Ethernet 10BASE-T para usuarios con requerimientos promedio de ancho de banda, o Fast Ethernet100BASE-TX para usuarios de potencia con conexiones de red más nuevas. Para simplificar la conexión de cables, los 26 puertos detectan automáticamente el tipo de cable Ethernet (MDI/MDIX). |

**Tabla N° 11 HP V1910-24G**

**CARACTERISTICAS CISCO SF300-24**

| CARACTERISTICAS | DESCRIPCIÓN |
|---|---|
|  | **Cisco SF300-24, Capa 2 / 3, 24 RJ-45 10/100, 4 RJ-45 LAN GbE, 2 SFP** |
| MARCA | CISCO |
| MODELO | **SF300-24** |
| PUERTOS | 24 Puertos10/100/1000BASE-T |
| VLAN(S) | Compatible |
| ESTANDARES | IEEE 802.3<br>IEEE 802.3u<br>IEEE 802.3ab<br>IEEE 802.3ad LACP<br>IEEE 802.1s STP múltiple<br>IEEE 802.1X Autenticación de acceso a puertos |
| PRINCIPALES CARACTERISTICAS | -1 unidad de rack (RU) interruptor independiente<br>-Ofrece servicios de inteligencia a la red borde<br>-Ideal para la migración de redes troncales Gigabit sobre cobre en la capa de acceso |
| SEGURIDAD | Protocolo Secure Shell (SSH)<br>Capa de sockets seguros (SSL)<br>IEEE 802.1X (función de Autenticador)<br>Aislamiento de capa 3<br>Perímetro de VLAN privada (PVE) con aislamiento de capa 2 y comunidad VLAN<br>Prevención de Denegación de servicios (DoS) |

**Tabla N° 12 Cisco SF300-24**

**ANEXO 3**

**SWICHT PARA LA CAPA DE DISTRIBUCION SWITH HP 1400-8G**

| CARACTERISTICAS | DESCRIPCIÓN |
|---|---|
|  | **HP PS1810-8G, 8 RJ-45 GbE** |
| MARCA | HP |
| MODELO | **PS1810-8G** |
| PUERTOS | 8 puertos 10/100/1000 Mbps |
| ESTANDARES | IEEE 802.1p Priority; IEEE 802.3ab 1000BASE-T; IEEE 802.3i 10BASE-T; IEEE 802.3u 100BASE-X; IEEE 802.3x Flow Control; IEEE 802.3z 1000BASE-X |
| PRINCIPALES CARACTERISTICAS | 8 RJ-45 autosensing 10/100/1000 ports(IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T), Media Type: Auto-MDIX, Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only<br>Memory and processor: 512 KB flash, packet buffer size: 512 KB<br>Latency: 100 Mb Latency: < 8.0 µs (LIFO 64-byte packets); 1000 Mb Latency: < 3.6 µs (LIFO 64-byte packets)<br>Throughput: up to 23.8 million pps (64-byte packets)<br>Switching capacity: 32 Gbps |
| CONFIGURACION | Auto Matico |

**Tabla N° 13 HP 1400-8G**

**CARACTERISTICAS DLINK SWITCH DGS-1210-10P**

| CARACTERISTICAS | DESCRIPCIÓN |
|---|---|
|  | **D-LINK DGS-1210-10P** |
| MARCA | DLINK |
| MODELO | **DGS-1210-10P** |
| PUERTOS | 8 puertos NWay de 10/100/1000Mbps |
| ESTANDARES | IEEE 802.3 10Base-T Ethernet<br>IEEE 802.3u 100Base-TX FastEthernet<br>IEEE 802.3ab 1000Base-T GigabitEthernet |
| METODO DE ACCESO | CSMA/CD |
| SEGURIDAD | CUL (UL 60950)<br>LVD (EC 60950) |
| MODO DE COMUNICACION | 10/100Mbps HalfDuplex o FullDuplexNWay auto-negotiation.<br>2000Mbps FullDuplex |
| OTROS | Es una excelente opción para pequeños grupos de trabajo, ya que permite conectar en forma simple cualquier puerta de 10Mbps, 100Mbps ó 1000Mbps, satisfaciendo las demandas de tráfico de cualquier usuario. |

**Tabla N° 14 D-LINK DGS-1210-10P**

**CARACTERISTICAS DE SWITCH CISCO SF300-08**

| CARACTERISTICAS | DESCRIPCIÓN |
|---|---|
|  | **CISCO SF300-08** |
| MARCA | **CISCO** |
| MODELO | **SF300-08** |
| PUERTOS | 10Base-T, 100Base-TX, 1000Base |
| ESTANDARES | IEEE 802.1P |
| OTROS | El CISCOSwitch 8 busca automáticamente la velocidad de conexión más rápida, los puertos 10/100/1000 con detección automática se ajustan automáticamente a la velocidad de los dispositivos de la red comunicando a 1000, 100 o 10 Mbps, de forma que el conmutador puede acomodar toda una gama de aplicaciones para grupo de trabajo. |

**Tabla N° 15 CISCO SF300-08**

**ANEXO 4**
**SERVIDORES DE A RCHIVOS/DNS/ FIREWALL/PROXY**

**CARACTERISTICAS DE SERVIDOR DE ARCHIVOS IBM**

| CARACTERISTICAS | DESCRIPCIÓN |
|---|---|
|  | IBM System x3400 7976 - Quad-Core Xeon E5420 2.5 GHz. |
| MARCA | IBM System x3400 7976 - Quad-Core Xeon E5420 2.5 GHz. |
| MODELO | Servidor |
| FACTOR DE FORMA | Torre – 5U |
| DIMENSIONES(ANCH,PROF,ALT) | 21.8 cm x 74.7 cm x 44 cm |
| ESCABILIDAD DEL SERVIDOR | 2 Vía |
| PROCESADOR | 1 x Intel Quad-CoreXeon E5420 / 2.5 GHz ( Quad-Core ) |
| CARACTERISTICAS PRINCIPALES DEL PROCESADOR | Tecnología de memoria extendida Intel 64 , Intel ExecuteDisable Bit, tecnología de visualización Intel. |
| MEMORIA CACHE | 12 MB L2 |
| MEMORIA RAM | 12 MB |
| CONEXION DE REDES | Adaptador de red - PCI Express - Ethernet, Fast Ethernet, Gigabit Ethernet |
| CONTROLADOR GRAFICO | PCI - ATI ES1000 - 16 MB |

**Tabla N° 16 SERVIDOR DE ARCHIVOS IBM**

## CARACTERISTICAS DE SERVIDOR DE ARCHIVOS HP

| CARACTERISTICAS | DESCRIPCIÓN |
|---|---|
|  | **Servidor HP ProLiant ML370 G6** |
| MARCA | HP |
| MODELO | **PROLIANT ML370 G6E5649** |
| TIPO | SERVIDOR |
| FACTOR DE FORMA | MICRO ATX TOWER 4U |
| PROCESADOR | Intel ® Xeon ® E5649 (6 núcleo, 2,53 GHz, 12 MB L3, 80W |
| MEMORIA RAM | 6 GB DDR3 |
| CONTROLADOR DE RED | LAN GbE NC375i de 4 puertos |

**Tabla N° 17 SERVIDOR DE ARCHIVOS HP**

## CARACTERISTICAS DE SERVIDOR DE ARCHIVOS DELL

| CARACTERISTICAS | DESCRIPCIÓN |
|---|---|
|  | SERVIDOR DELL POWEREDGE 840 |
| MARCA | DELL |
| MODELO | POWEREDGE 840 |
| TIPO | SERVIDOR |
| TARJETA DE INTERFAZ DE RED | Una tarjeta NIC Broadcom Gigabit2 integrada;<br>Una tarjeta opcional NIC Intel x4 PCIe Gigabit2 de doble puerto;<br>Una tarjeta opcional NIC Intel PCIe Gigabit2 de doble puerto;<br>Broadcom x1 PCIe Gigabit2 Opcional<br>NIC con TOE Broadcom x4 PCIe Gigabit2 opcional |
| PROCESADOR | Procesador de secuencia de un solo núcleo Intel Xeon® 3000 de hasta 2,66 GHz;<br>Procesador de un solo núcleo Intel Pentium® D de 2,8 GHz;<br>un procesador Intel Celeron D de 2,8 GHz |
| MEMORIA | Memoria SDRAM de 512 MB-8 GB con ECC y DDR-2 533/667 |
| COMPARTIMIENTO DE DISCO DURO | 4 SATA o SAS conectables en marcha/de acceso frontal o con cableado de 3,5"<br>1 CD, CD/DVD-ROM, combinado de CD-RW/DVD opcionales de 5,25"<br>1 TBU interna opcional de media altura de 5,25"<br>1 unidad de disquete de 3,5" |

**Tabla N° 18 SERVIDOR DE ARCHIVOS DELL**

**ANEXO 5**

**PICOSTATION 2HP CARACTERISTICAS**

| CARACTERISTICAS | DESCRIPCIÓN |
|---|---|
|  | Picostation 2HP WIRELESS AP, OUTDOOR 6DBI 802.11b/g 800mW, 1000mw. |
| **MARCA** | Ubiquiti Networks |
| **MODELO** | 2HP |
| **ESPECIFICACIONES DEL PROCESADOR** | Torre – 5U |
| **MEMORIA** | 21.8 cm x 74.7 cm x 44 cm |
| **INTERFAZ DE RED** | 2 Vía |
| **CERTIFICACIONES** | 1 x Intel Quad-CoreXeon E5420 / 2.5 GHz ( Quad-Core ) |
| **CUMPLIMIENTO DE LAS NORMAS ROHS** | Tecnología de memoria extendida Intel 64 , Intel ExecuteDisable Bit, tecnología de visualización Intel. |
| **MÉTODO DE LA ENERGÍA** | 12 MB L2 |
| **TEMPERATURA DE FUNCIONAMIENTO** | 12 MB |
| **FUENTE DE ALIMENTACIÓN** | Adaptador de red - PCI Express - Ethernet, Fast Ethernet, Gigabit Ethernet |
| **POTENCIA** | 800 mw – 1000mw |

**Tabla N° 19 Picostation 2HP**

**SENAO ENGENIUS EOC-5611 CARACTERISTICAS**

| CARACTERISTICAS | DESCRIPCIÓN |
|---|---|
|  | ACCES POINT EOC-5611<br>Dual 5 GHZ Y 2.4 GHZ |
| **MARCA** | EnGenius |
| **MODELO** | EOC-5611 |
| **MCU/RF** | Atheros AR2313 + AR5112 |
| **MEMORIA** | 32 MB SDRAM |
| **INTERFAZ DE RED** | 10/100 Fast Ethernet RJ-45.<br>Botón de reseteo.<br>Antena Switch( interno y externo).<br>2 Conectores SMA (para 2.4 GHz y 5.8 GHz). |
| **CERTIFICACIONES** | FCC Part 15C/15B/15E,EN301 893,EN 301 489-1/-17,EN60950,IC Certification |
| **Indicadores LED** | Potencia / Estado<br>LAN (10/100 Mbps)<br>WLAN (Wireless es hasta)<br>3 x enlace de calidad (modo de puente de cliente)<br>Verde:Buena calidad<br>Amarillo:De calidad apenas aceptable<br>Rojo: Mala calidad |
| **MÉTODO DE LA ENERGÍA** | Active Ethernet (Powerover Ethernet) de propiedad de diseño PoE<br>Adaptador 24V / 1 A DC |
| **POTENCIA** | Direcional de 13 dBi |

**Tabla N° 20 SENAO ENGENIUS EOC-5611**

**Cisco Aironet 1300 CARACTERISTICAS**

| CARACTERISTICAS | DESCRIPCIÓN |
|---|---|
|  | ACCES POINT EOC-5611<br>Dual 5 GHZ Y 2.4 GHZ |
| **MARCA** | Cisco Systems |
| **MODELO** | 1310 Outdoor Access Point/Bridge |
| **Protocolo de gestión remota** | SNMP 1 , SNMP 2 , Telnet , HTTP |
| **Protocolo de interconexión de datos** | IEEE 802.11b , IEEE 802.11g |
| **Velocidad de transferencia de datos** | 54 Mbps |
| **Algoritmo de cifrado** | LEAP , TLS , PEAP , TTLS , WPA |

**Tabla N° 21 Cisco Aironet 1300**

## ISO/IEC 27002:2005. Dominios (11), Objetivos de control (39) y Controles (133)

CLIC SOBRE CADA CONTROL PARA MÁS INFORMACIÓN

Versión actualizada de esta lista en: http://www.iso27000.es/download/ControlesISO27002-2005.pdf

5. POLÍTICA DE SEGURIDAD.
- 5.1 Política de seguridad de la información.
  - 5.1.1 Documento de política de seguridad de la información.
  - 5.1.2 Revisión de la política de seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Compromiso de la Dirección con la seguridad de la información.
  - 6.1.2 Coordinación de la seguridad de la información.
  - 6.1.3 Asignación de responsabilidades relativas a la seg. de la informac.
  - 6.1.4 Proceso de autorización de recursos para el tratamiento de la información.
  - 6.1.5 Acuerdos de confidencialidad.
  - 6.1.6 Contacto con las autoridades.
  - 6.1.7 Contacto con grupos de especial interés.
  - 6.1.8 Revisión independiente de la seguridad de la información.
- 6.2 Terceros.
  - 6.2.1 Identificación de los riesgos derivados del acceso de terceros.
  - 6.2.2 Tratamiento de la seguridad en la relación con los clientes.
  - 6.2.3 Tratamiento de la seguridad en contratos con terceros.

7. GESTIÓN DE ACTIVOS.
- 7.1 Responsabilidad sobre los activos.
  - 7.1.1 Inventario de activos.
  - 7.1.2 Propiedad de los activos.
  - 7.1.3 Uso aceptable de los activos.
- 7.2 Clasificación de la información.
  - 7.2.1 Directrices de clasificación.
  - 7.2.2 Etiquetado y manipulado de la información.

8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 8.1 Antes del empleo.
  - 8.1.1 Funciones y responsabilidades.
  - 8.1.2 Investigación de antecedentes.
  - 8.1.3 Términos y condiciones de contratación.
- 8.2 Durante el empleo.
  - 8.2.1 Responsabilidades de la Dirección.
  - 8.2.2 Concienciación, formación y capacitación en seg. de la informac.
  - 8.2.3 Proceso disciplinario.
- 8.3 Cese del empleo o cambio de puesto de trabajo.
  - 8.3.1 Responsabilidad del cese o cambio.
  - 8.3.2 Devolución de activos.
  - 8.3.3 Retirada de los derechos de acceso.

9. SEGURIDAD FÍSICA Y DEL ENTORNO.
- 9.1 Áreas seguras.
  - 9.1.1 Perímetro de seguridad física.
  - 9.1.2 Controles físicos de entrada.
  - 9.1.3 Seguridad de oficinas, despachos e instalaciones.
  - 9.1.4 Protección contra las amenazas externas y de origen ambiental.
  - 9.1.5 Trabajo en áreas seguras.
  - 9.1.6 Áreas de acceso público y de carga y descarga.
- 9.2 Seguridad de los equipos.
  - 9.2.1 Emplazamiento y protección de equipos.
  - 9.2.2 Instalaciones de suministro.
  - 9.2.3 Seguridad del cableado.
  - 9.2.4 Mantenimiento de los equipos.
  - 9.2.5 Seguridad de los equipos fuera de las instalaciones.
  - 9.2.6 Reutilización o retirada segura de equipos.
  - 9.2.7 Retirada de materiales propiedad de la empresa.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.
- 10.1 Responsabilidades y procedimientos de operación.
  - 10.1.1 Documentación de los procedimientos de operación.
  - 10.1.2 Gestión de cambios.
  - 10.1.3 Segregación de tareas.
  - 10.1.4 Separación de los recursos de desarrollo, prueba y operación.
- 10.2 Gestión de la provisión de servicios por terceros.
  - 10.2.1 Provisión de servicios.
  - 10.2.2 Supervisión y revisión de los servicios prestados por terceros.
  - 10.2.3 Gestión del cambio en los servicios prestados por terceros.
- 10.3 Planificación y aceptación del sistema.
  - 10.3.1 Gestión de capacidades.
  - 10.3.2 Aceptación del sistema.
- 10.4 Protección contra el código malicioso y descargable.
  - 10.4.1 Controles contra el código malicioso.
  - 10.4.2 Controles contra el código descargado en el cliente.
- 10.5 Copias de seguridad.
  - 10.5.1 Copias de seguridad de la información.
- 10.6 Gestión de la seguridad de las redes.
  - 10.6.1 Controles de red.
  - 10.6.2 Seguridad de los servicios de red.
- 10.7 Manipulación de los soportes.
  - 10.7.1 Gestión de soportes extraíbles.
  - 10.7.2 Retirada de soportes.
  - 10.7.3 Procedimientos de manipulación de la información.
  - 10.7.4 Seguridad de la documentación del sistema.
- 10.8 Intercambio de información.
  - 10.8.1 Políticas y procedimientos de intercambio de información.
  - 10.8.2 Acuerdos de intercambio.
  - 10.8.3 Soportes físicos en tránsito.
  - 10.8.4 Mensajería electrónica.
  - 10.8.5 Sistemas de información empresariales.
- 10.9 Servicios de comercio electrónico.
  - 10.9.1 Comercio electrónico.
  - 10.9.2 Transacciones en línea.
  - 10.9.3 Información públicamente disponible.
- 10.10 Supervisión.
  - 10.10.1 Registros de auditoría.
  - 10.10.2 Supervisión del uso del sistema.
  - 10.10.3 Protección de la información de los registros.
  - 10.10.4 Registros de administración y operación.
  - 10.10.5 Registro de fallos.
  - 10.10.6 Sincronización del reloj.

11. CONTROL DE ACCESO.
- 11.1 Requisitos de negocio para el control de acceso.
  - 11.1.1 Política de control de acceso.
- 11.2 Gestión de acceso de usuario.
  - 11.2.1 Registro de usuario.
  - 11.2.2 Gestión de privilegios.
  - 11.2.3 Gestión de contraseñas de usuario.
  - 11.2.4 Revisión de los derechos de acceso de usuario.
- 11.3 Responsabilidades de usuario.
  - 11.3.1 Uso de contraseñas.
  - 11.3.2 Equipo de usuario desatendido.
  - 11.3.3 Política de puesto de trabajo despejado y pantalla limpia.
- 11.4 Control de acceso a la red.
  - 11.4.1 Política de uso de los servicios en red.
  - 11.4.2 Autenticación de usuario para conexiones externas.
  - 11.4.3 Identificación de los equipos en las redes.
  - 11.4.4 Protección de los puertos de diagnóstico y configuración remotos.
  - 11.4.5 Segregación de las redes.
  - 11.4.6 Control de la conexión a la red.
  - 11.4.7 Control de encaminamiento (routing) de red.
- 11.5 Control de acceso al sistema operativo.
  - 11.5.1 Procedimientos seguros de inicio de sesión.
  - 11.5.2 Identificación y autenticación de usuario.
  - 11.5.3 Sistema de gestión de contraseñas.
  - 11.5.4 Uso de los recursos del sistema.
  - 11.5.5 Desconexión automática de sesión.
  - 11.5.6 Limitación del tiempo de conexión.
- 11.6 Control de acceso a las aplicaciones y a la información.
  - 11.6.1 Restricción del acceso a la información.
  - 11.6.2 Aislamiento de sistemas sensibles.
- 11.7 Ordenadores portátiles y teletrabajo.
  - 11.7.1 Ordenadores portátiles y comunicaciones móviles.
  - 11.7.2 Teletrabajo.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.
- 12.1 Requisitos de seguridad de los sistemas de información.
  - 12.1.1 Análisis y especificación de los requisitos de seguridad.
- 12.2 Tratamiento correcto de las aplicaciones.
  - 12.2.1 Validación de los datos de entrada.
  - 12.2.2 Control del procesamiento interno.
  - 12.2.3 Integridad de los mensajes.
  - 12.2.4 Validación de los datos de salida.
- 12.3 Controles criptográficos.
  - 12.3.1 Política de uso de los controles criptográficos.
  - 12.3.2 Gestión de claves.
- 12.4 Seguridad de los archivos de sistema.
  - 12.4.1 Control del software en explotación.
  - 12.4.2 Protección de los datos de prueba del sistema.
  - 12.4.3 Control de acceso al código fuente de los programas.
- 12.5 Seguridad en los procesos de desarrollo y soporte.
  - 12.5.1 Procedimientos de control de cambios.
  - 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 12.5.3 Restricciones a los cambios en los paquetes de software.
  - 12.5.4 Fugas de información.
  - 12.5.5 Externalización del desarrollo de software.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Control de las vulnerabilidades técnicas.

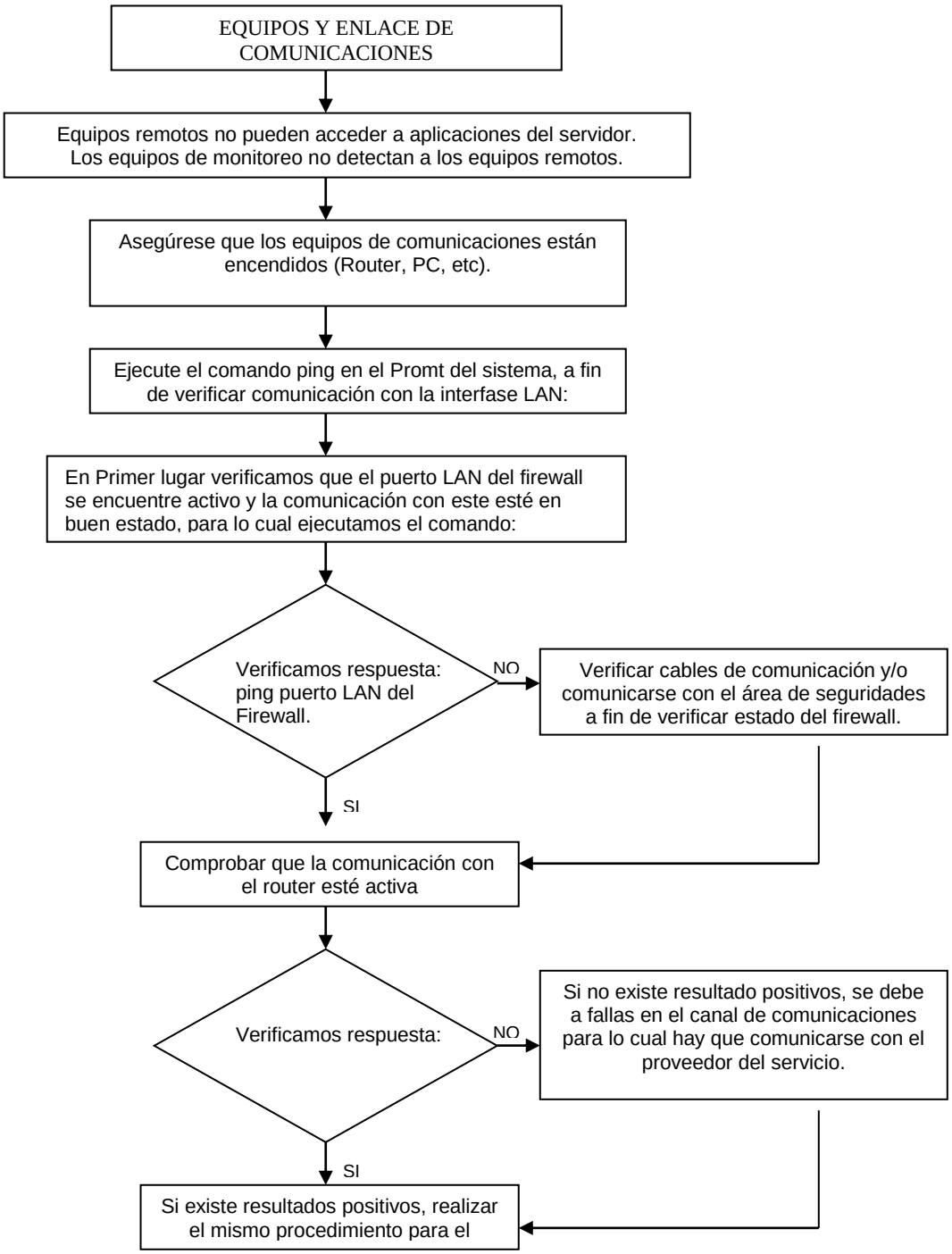
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 13.1 Notificación de eventos y puntos débiles de seguridad de la información.
  - 13.1.1 Notificación de los eventos de seguridad de la información.
  - 13.1.2 Notificación de puntos débiles de seguridad.
- 13.2 Gestión de incidentes y mejoras de seguridad de la información.
  - 13.2.1 Responsabilidades y procedimientos.
  - 13.2.2 Aprendizaje de los incidentes de seguridad de la información.
  - 13.2.3 Recopilación de evidencias.

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
  - 14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
  - 14.1.2 Continuidad del negocio y evaluación de riesgos.
  - 14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
  - 14.1.4 Marco de referencia para la planificación de la cont. del negocio.
  - 14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.

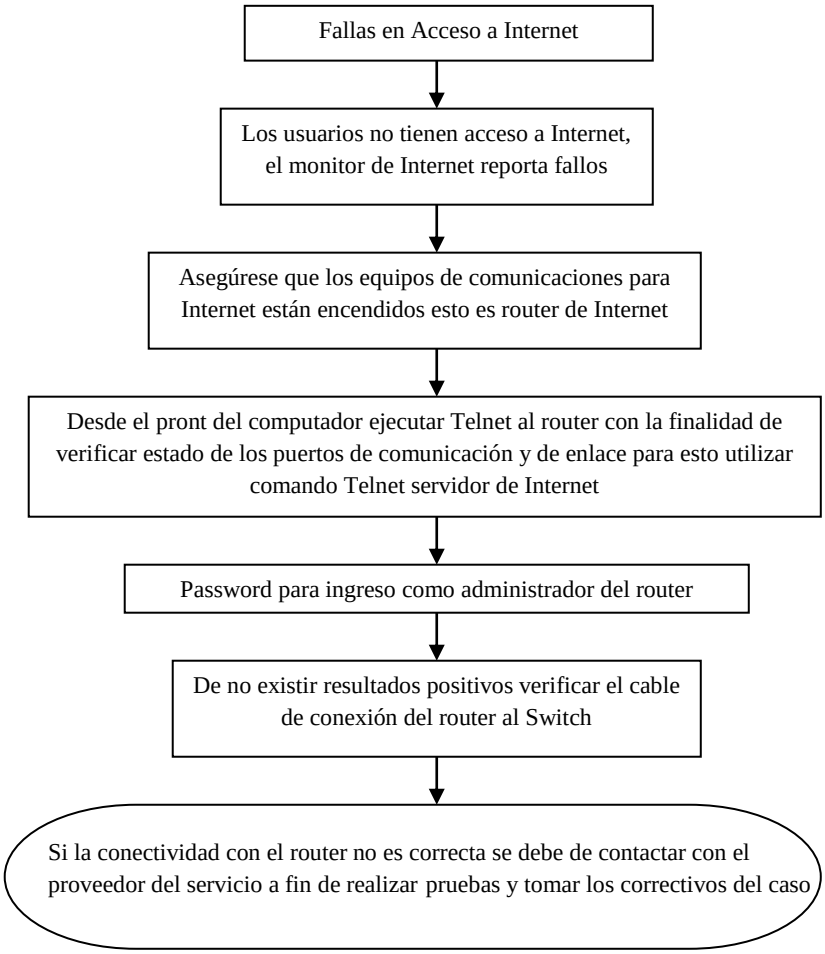
15. CUMPLIMIENTO.
- 15.1 Cumplimiento de los requisitos legales.
  - 15.1.1 Identificación de la legislación aplicable.
  - 15.1.2 Derechos de propiedad intelectual (DPI).
  - 15.1.3 Protección de los documentos de la organización.
  - 15.1.4 Protección de datos y privacidad de la información de carácter personal.
  - 15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.
  - 15.1.6 Regulación de los controles criptográficos.
- 15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.
  - 15.2.1 Cumplimiento de las políticas y normas de seguridad.
  - 15.2.2 Comprobación del cumplimiento técnico.
- 15.3 Consideraciones sobre las auditorías de los sistem. de información.
  - 15.3.1 Controles de auditoría de los sistemas de información.
  - 15.3.2 Protección de las herramientas de auditoría de los sist. de inform.

**ANEXO 7**

# 1. DIAGRAMA DE FLUJO EQUIPOS Y ENLACES DE COMUNICACIONES



## 2. DIAGRAMA DE FLUJO FALLAS DE ACCESO A INTERNET



# 3. DIAGRAMA DE FLUJO FALLAS EN SERVIDOR DHCP