

**ACTUALIZACIÓN DE UNA RED LAN PRIVADA PARA LAS SEDES DE I-
3NET**

FABIAN GERARDO LIZARAZO MORALES.

**UNIVERSIDAD COOPERATIVA DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE TELECOMUNICACIONES
SECCIONAL BOGOTÁ D.C.
FEBRERO, 2016**

**ACTUALIZACIÓN DE UNA RED LAN PRIVADA PARA LAS SEDES DE I-
3NET**

ESPECIALIZACIÓN EN REDES Y TELECOMUNICACIONES
Trabajo de Grado para optar al título de Especialista de
Telecomunicaciones

PRESENTADO

FABIAN GERARDO LIZARAZO

Trabajo de grado para optar al título de Especialista en Redes de
Telecomunicaciones

DIRECTOR

ING. FABIAN BLANCO



UNIVERSIDAD COOPERATIVA DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA DE ESPECIALIZACIÓN EN REDES DE
TELECOMUNICACIONES
SECCIONAL BOGOTÁ D.C.
FEBRERO, 2016
DEDICATORIA

A mi madre que, con su esfuerzo y colaboración, me permitió alcanzar mis metas.

AGRADECIMIENTOS

Al ingeniero Fabian Blanco, director de Post-gradados de la Universidad Cooperativa de Colombia, quien me brindó el espacio para la elaboración de esta propuesta y su asesoría para resolver los inconvenientes que este proyecto presento.

*A mi hija, no llores por un mundo que
lucha, lucha por un mundo que llora.*

TABLA DE CONTENIDO

TABLA DE CONTENIDO 5

<i>LISTA DE FIGURAS.</i>	7
<i>LISTA DE TABLAS.</i>	8
<i>RESUMEN.</i>	9
<i>INTRODUCCIÓN.</i>	10
<i>GLOSARIO.</i>	11
<i>Capítulo I.</i>	13
1.1. Descripción del tema.	13
1.2. Planteamiento del problema.	14
1.3. Justificación.	14
1.4. Objetivos.....	15
1.4.1. Objetivo General.....	15
1.4.2. Objetivos Específicos.	16
<i>Capítulo II.</i>	16
2.1. Marco Teórico.	16
<i>Red privada.</i>	17
<i>Seguridad de la red.</i>	18
<i>Componentes básicos de una red.</i>	18
<i>Protocolo de Internet (IP).</i>	24
<i>Direccionamiento IP.</i>	24
<i>Protocolo de Internet (IPv4).</i>	26
<i>Protocolo de internet (IPv6).</i>	27
<i>Protocolo de resolución de direcciones (ARP).</i>	28
<i>Protocolo de datagrama de usuario (UDP).</i> Protocolo de Configuración de Host Dinámica (DHCP)	28
Protocolo de Configuración de Host Dinámica (DHCP)	29
<i>Cableado estructurado.</i>	30
<i>Cableado vertical, troncal o backbone.</i>	31
<i>Fibra óptica.</i>	33
<i>Wi-Fi.</i>	33
<i>Seguridad y Fiabilidad.</i>	34
2.2. Marco Jurídico.....	35
*ANSI/EIA/TIA-568A.	35
*ANSI/EIA/TIA-569.	36
*ANSI/TIA/EIA-606.	36
*ANSI/TIA/EIA-607.	36
*ISO/IEC 11801.	36
*ISO/IEC 14763-2.	37

<i>Capítulo III.</i>	38
3.1. Análisis del proyecto.	38
3.1.1. Situación actual de la empresa I-3NET.	38
3.1.2. Plano físicos y de red de la sed principal.	40
3.2. Estructura temática.	42
3.2.1. Limitaciones.	42
3.3. Determinación de los requerimientos.	43
3.4. Diseño del proyecto.	47
3.4.1. Topología de la red. Diseño del modelo de direccionamiento y nombramiento.	47
3.4.2. Diseño del modelo de direccionamiento y nombramiento.	47
3.4.3. Selección de protocolos.	52
3.4.4. Desarrollo de estrategias de seguridad de la red.	52
3.4.5. Fase de Diseño Físico.	54
<i>Conclusiones.</i>	60
<i>Bibliografía.</i>	61
<i>Infografía.</i>	62

LISTA DE FIGURAS.

Figura 1. Servidor de archivos	20
Figura 2. Servidor de impresiones	20

Figura 3. Servidor de correo	21
Figura 4. Servidor DHCP	21
Figura 5. Servidor Proxi	22
Figura 6. Servidor web	22
Figura 7. Servidor de autenticación	23
Figura 8. Servidor DNS	23
Figura 9. Servidor de telefonía IP	24
Figura 10. Clase de direccionamiento	26
Figura 11. Cabecera UDP	29
Figura 12. Plano sede principal planta baja.	40
Figura 13. Plano sede principal planta alta.	40
Figura 14. Plano sede principal planta baja red	41
Figura 15. Plano sede principal planta alta red	41
Figura 16. Gabinete actual	42
Figura 17. Selección de Protocolos de Switching y Routing	52
Figura 18. Diseño físico planta baja sede principal.	54
Figura 19. Diseño físico planta alta sede principal	54
Figura 20. Cableado planta baja sede principal	55
Figura 21. Cableado planta alta sede principal	55
Figura 22. Diseño físico planta baja sede ingeniería	56
Figura 23. Diseño físico planta media sede ingeniería	56
Figura 24. Diseño físico planta alta sede ingeniería	57
Figura 25. Diseño red planta baja sede ingeniería	57
Figura 26. Diseño red planta media sede ingeniería	58
Figura 27. Diseño red planta alta sede ingeniería	58
Figura 28. Diseño físico sede Cali	59
Figura 29. Diseño red sede Cali	59

LISTA DE TABLAS.

Tabla 1. Información actual sede principal	38
Tabla 2. Análisis y definiciones de Requerimientos sede principal	44

Tabla 3. Análisis y definiciones de Requerimientos sede ingeniería	45
Tabla 4. Diseño del modelo de direccionamiento.	47
Tabla 5. Direccionamiento de la sede de ingeniería	49
Tabla 6. Direccionamiento sede Cali	51

RESUMEN.

La infraestructura de la empresa **I-3NET** consta de un edificio principal que actualmente cuenta con 2 plantas, las plantas ya se encuentra completamente construidas y operando correctamente, donde se encuentra ubicado la parte

administrativa de la empresa, la siguiente sede se encuentra el departamento de ingeniería el cual consta de 3 plantas, y una sedes más ubicada en la ciudad de Santiago de Cali en el Valle, pero la tecnología que se encuentra instalada, está generando demora en las comunicaciones de las redes, se pretende diseñar una red de datos, altamente eficiente, para evitar la existencia de fallos en la red mediante técnicas de redundancia y comprobación del estado de los equipos.

Esta propuesta tiene como propósito evitar que se presenten fallas de desconexiones, latencias o retardos en la red LAN que afecten la disponibilidad de la red, ya que la cantidad de funcionarios creciente y las diferentes labores deben tener una conexión permanente la cual debe ser confiable y que garantice que todos los servicios se encuentren disponibles en todo momento y en tiempo real.

Se efectuó un Site Survey para identificar las necesidades latentes en cuanto a servicios a prestar, evaluando la infraestructura física y tecnológica para equilibrar la implementación de los equipos. Se presentó una factibilidad correspondiente a las diferentes alternativas que se plantearon para el rediseño de la red, se tomó la más viable garantizando la modernización, eficiencia y confiabilidad de los servicios.

Dentro de la factibilidad se plantea la mejor relación costo beneficio, eficiente y permitir centralizar y garantizar la gestión de la información que fluirá sobre la red a diseñar ya que esto agilizará los procesos y tareas de los funcionarios.

INTRODUCCIÓN.

Desde el nacimiento de la Internet, las redes de comunicaciones han jugado un papel de vital importancia en todas las actividades al interior de las organizaciones tanto a nivel oficial como privado. El activo de mayor importancia en cualquier organización es la información, de ahí que su disponibilidad puede

marcar la diferencia entre el éxito y el fracaso comercial de una compañía en el contexto mundial de mercado abierto.

Diseñar una red siempre ha sido difícil, pero hoy en día la tarea es cada vez más difícil debido a la gran variedad de opciones y es en este punto donde el enfoque de un ingeniero de telecomunicaciones permite centrarse en las principales metas del diseño de una red.

El diseño generado por el ingeniero de la red debe siempre preguntarse. ¿Quién va a usar la red? ¿Qué tareas van a desempeñar los usuarios en la red? ¿Quién va a administrar la red? Igualmente importante ¿Quién va a pagar por ella? ¿Quién va a pagar por mantenerla? Cuando esas respuestas sean respondidas, las prioridades serán establecidas y el proceso del diseño de la red será mucho más productivo.

Es importante tener puntos que sobresalgan en la red como lo son (performance, Volumen proyectado de tráfico, Expansión futura, Seguridad, Redundancia, Compatibilidad, Costo).

Se propone diseñar una red, que cubra las necesidades y que sea amigable, pero sobre todo que permita realizar cambios en la configuración, sin tener que manipular la estructura física del lugar. Este proceso se hace con el fin de optimizar los recursos, pero garantizando la correcta operatividad de cada uno de los puntos.

Como expectativas frente el diseño se espera que la red sea eficiente y sus fallas sean mínimas, con el fin de satisfacer las necesidades del entorno laboral y así poder participar en nuevos proyectos en el mercado de las telecomunicaciones.

GLOSARIO.

ANCHO DE BANDA: Es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período dado. El ancho de banda se indica generalmente en bits por segundo (bps).

BIT: Es el acrónimo Binary digit. (Dígito binario). Un bit es un dígito del sistema de numeración binario. Mientras que en el sistema de numeración decimal se usan diez dígitos, en el binario se usan sólo dos dígitos, el 0 y el 1. Un bit o dígito binario puede representar uno de esos dos valores, 0 ó 1

Byte: Es la unidad fundamental de datos en los computadores, un byte son ocho bits contiguos. El byte es también la unidad de medida básica para memoria, almacenando el equivalente a un carácter, como una letra, un dígito o un signo de puntuación.

DIRECCION IP: Es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red del protocolo TCP/IP

FIBRA OPTICA: Es un medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir.

FIREWALL: Combinación de hardware / software que controla el tipo de servicios permitidos hacia o desde la Intranet.

MASCARA DE SUBRED: Conjunto de bits que excluye redes de una difusión por todo el sistema, en vez de restringir la difusión a una subred

PAQUETE: Unidad de transmisión del nivel de red del estándar Interconexión de sistemas abiertos (OSI) que consta de información binaria que representa datos y un encabezado que contiene un número de identificación, las direcciones de origen y de destino, y datos de control de errores.

PUNTO DE ACCESO: En redes de computadoras es un dispositivo que interconecta dispositivos de comunicación alámbricas para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos.

RED: Es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

RED LAN: Una red de área local, red local o LAN (del inglés *local area network*) es la interconexión de una o varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, con repetidores podría llegar a la distancia de un campo de 1 kilómetro.

RED PRIVADA: Una red privada es una red que usa el espacio de direcciones IP especificadas en el documento *RFC 1918*. A los terminales puede asignársele

direcciones de este espacio de direcciones cuando se requiera que ellas deban comunicarse con otras terminales dentro de la red interna (una que no sea parte de Internet) pero no con Internet directamente. Las redes privadas son bastante comunes en esquemas de redes de área local (LAN) de oficina, pues muchas compañías no tienen la necesidad de una dirección IP global para cada estación de trabajo, impresora y demás dispositivos con los que la compañía cuente. Otra razón para el uso de direcciones de IP privadas es la escasez de direcciones IP públicas que pueden ser registradas. IPv6 se creó justamente para combatir esta escasez, pero aún no ha sido adoptado en forma definitiva.

VPN: Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.¹ Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

SEGURIDAD DE RED: La seguridad de redes es un nivel de seguridad que garantiza que el funcionamiento de todas las máquinas de una red sea óptimo y que todos los usuarios de estas máquinas posean los derechos que les han sido concedidos.

SERVIDOR: Es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.

TCP/IP: Es un modelo de descripción de protocolos de red creado en la década de 1970 por DARPA, una agencia del Departamento de Defensa de los Estados Unidos. Evolucionó de ARPANET, el cual fue la primera red de área amplia y predecesora de Internet. EL modelo TCP/IP se denomina a veces como *Internet Model*, Modelo DoD o Modelo DARPA.

El modelo TCP/IP, describe un conjunto de guías generales de diseño e implementación de protocolos de red específicos para permitir que un equipo pueda comunicarse en una red.

WI-FI: Es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. Los dispositivos habilitados con Wi-Fi, tales como: un ordenador personal, una consola de videojuegos, un Smartphone o un reproductor de audio digital, pueden conectarse a Internet a través de un punto de acceso de red inalámbrica.

Capítulo I.

1.1. Descripción del tema.

La tecnología de telecomunicaciones a lo largo de las últimas décadas de una manera abrumadora han ido constituyéndose en recursos indispensables dentro

de los diferentes campos ya sea investigación, científico, educativo, militar, gubernamental, médico, arquitectura, etc. Por lo que surge la necesidad de interconectarlas entre sí para compartir información y recursos.

En la actualidad las redes informáticas que son un conjunto de computadoras conectadas entre sí mediante algún elemento físico con el propósito de comunicarse y compartir los recursos e información que estas tengan. Las redes informáticas se vienen extendiendo desde una simple red doméstica hasta la famosa red mundial descentralizada que es internet, permitiendo comunicarse de forma remota a cualquier lugar del mundo y ofreciendo uno de los servicios que más éxito ha tenido en Internet.

En este sentido se ha decidido las tecnologías informáticas y de comunicación (TIC), principalmente el diseño de una red privada de ordenadores en el proceso Educativo y de esta manera asumir los retos de la nueva sociedad, ofrecer nuevas y mejores oportunidades de consecución de estudios y contribuir al desarrollo Tecnológico de nuestra sociedad. En consecuencia se ha propuesto un proyecto sobre el diseño de una red privada de ordenadores para las sedes que conforman la empresa **I-3NET**.

1.2. Planteamiento del problema.

Hoy en día las instituciones necesitan de redes sistemáticas para el manejo y el control de los datos. Actualmente **I-3NET** cuenta con una sede principal donde se encuentran todas las áreas de la empresa, y ha encontrado posible la expansión a 2 sedes más, las misma que no están implementadas ni conectadas a la sede principal, la cual cuenta con una red de baja velocidad y con gran cantidad de retardos y saturaciones, por su volumen de trabajo para procesos administrativos y consulta en sus bases de datos, creando congestión en la sede principal, y generando un mal servicio para los usuarios y funcionarios de la misma empresa **I-3NET**.

1.3. Justificación.

I-3NET tendrá una sede a nivel nacional y en Bogotá contará con dos sedes que están conectadas a la sede principal haciendo de esta el core de la red la empresa; la cual cuenta con pequeñas redes para sistematizar todas las labores, llevar el control de algunas tareas administrativas, y el diseño de software y su rendimiento y tecnología implementada es de una calidad baja con un desempeño inestable.

I-3NET desea ser una institución más competitiva e innovadora, basándose para ello en tecnologías de información para el crecimiento de enseñanza por medio de sus diferentes dependencias, ya sea desde terminales virtuales hasta equipo locales accediendo a Internet.

De este modo se generará un control sistematizado para agilizar procesos, actualizar información, realizar unión y actualización entre áreas. El beneficio económico que recibirá la institución se verá reflejado en los bajos costos de los mantenimientos y puestos de trabajo, más eficientes, pues con Internet podrán ser virtuales, con un mínimo de inversión en las conexiones de Internet.

La seguridad de la información que se maneja dentro de la institución será alta, ya que se incorporarán sistemas de protección no solo a nivel físico sino también lógico, lo cual permitirá proteger los datos, diseños, e información latente en la base de datos de los diferentes socios, que se realizan internamente así como los proyectos que se diseñen, para mantener la autoría por parte de **I-3NET**.

1.4. Objetivos.

1.4.1. Objetivo General.

- Implementar la actualización de una red LAN privada para las sedes de la empresa I-3NET, realizando los diseños físicos y lógicos con el fin de actualizar e instituir la red en las sedes nuevas

1.4.2. Objetivos Específicos.

- Establecer los equipos y dispositivos que se plantean para la implementación de las redes LAN.
- Realizar planos con sus perspectivas medidas de distancia para interconexión de los equipos.
- Establecer la distribución de cada una de las subredes en las plantas físicas de la institución.
- Diseñar la comunicación entre las plantas del edificio de forma segura y con un alto nivel de disponibilidad para evitar cortes en la transmisión de datos.
- Diseñar la comunicación entre las sedes que conforman la empresa de forma segura y con un alto nivel de disponibilidad para evitar cortes en la transmisión de datos.
- Determinar el método más adecuado para la administración y gestión de la red, así como los accesos y privilegios de cada uno de los usuarios dentro de los diferentes servidores.

Capítulo II.

2.1. Marco Teórico.

A continuación se explican los conceptos fundamentales de una red de comunicación y los protocolos para entender el proyecto que se describe en este documento.

Red privada.

Es una red que utiliza los protocolos TCP/IP. Puede tener salida a Internet o no. En el caso de tener salida a Internet, ¹ el direccionamiento IP permite que los hosts con direcciones IP privadas puedan salir a Internet pero impide el acceso a los hosts internos desde Internet. Y en el caso de IPv4 donde las direcciones IP llegaron al límite se creó el protocolo NAT (network address translation), el cual es un protocolo utilizado por los Routers para el intercambio de paquetes de redes diferentes con direcciones incompatibles, como son las privadas y públicas, consiste en cambiar en tiempo real las direcciones de los paquetes transportados, estableciendo la modificación de los paquetes para permitir la ejecución de protocolos que incluyen la información de la direcciones destino y origen dentro de la conversación del protocolo. Dentro de una red privada se pueden configurar todos los servicios típicos de Internet (Web, correo, mensajería instantánea, telefonía IP, etc.) mediante la instalación de los correspondientes servidores. La idea es que las redes privadas se comporten como una red como el internet pero con limitaciones obvias de tamaño lo cual las convertiría en redes intranet.

Este tipo de red tiene un sin número de mejoras para aumentar la rendimiento y la eficiencia de las empresas. Algunas de las formas en que las redes privadas pueden ayudar a las organizaciones son:

- ✓ Suministrar acceso a la información reciente.
- ✓ Mejorar las comunicaciones de la empresa.
- ✓ Mejorar la gestión de recursos humanos.
- ✓ Proveen eficiencias operacionales y administrativas que ahorran tiempo y dinero.
- ✓ Están basadas en estándares de conexión.

¹Andrew S. Tanenbaum: "Redes de Computadoras", Tercera edición, Prentice Hall, México, 1997; p.67.

Existen algunos riesgos y desventajas, que se deben considerar antes de implementar una red privada, por ejemplo:

- ✓ Riesgos de seguridad.
- ✓ Caos potencial, en cuanto al cambio de procesos y sistemas.
- ✓ El crecimiento de la red en usuarios y capacidad.

Seguridad de la red.

Las redes privadas son vulnerables a los ataques de personas que tengan el objetivo de destruir o robar datos empresariales.

Las tecnologías de seguridad de red protegen su red contra el robo y el uso incorrecto de información confidencial de la empresa y ofrecen protección contra ataques maliciosos de virus y gusanos de Internet. Sin ningún tipo de seguridad en red, su empresa se enfrenta a intrusiones no autorizadas, periodos de inactividad de red, interrupción del servicio, incumplimiento de las normativas e incluso a acciones legales.

Las redes privadas requieren varias medidas de seguridad, incluyendo las combinaciones de hardware y software que proporcionan el control del tráfico; la encriptación y las contraseñas para convalidar usuarios; y las herramientas del software para evitar y curar de virus, bloquear sitios indeseables, y controlar el tráfico. El término genérico usado para denominar a una línea de defensa contra intrusos es firewall.

Un *firewall* es una combinación de hardware / software que controla el tipo de servicios permitidos hacia o desde la red privada. Un firewall de un servidor se configura para oponerse y evitar el acceso a los servicios no autorizados. Normalmente está aislado del resto de la red en su propia sub-red de perímetro. De este modo si el servidor es "allanado", el resto de la red no estará en peligro.

Componentes básicos de una red.

- *El ordenador:* La mayoría de los componentes de una red media son los ordenadores individuales, también denominados host; generalmente son sitios de trabajo (incluyendo ordenadores personales) o servidores.
- *Tarjetas de red:* Para lograr el enlace entre las computadoras y los medios de transmisión (cables de red o medios físicos para redes alámbricas e infrarrojos o radiofrecuencias para redes inalámbricas), es necesaria la intervención de una tarjeta de red o NIC (Network Card Interface) con la cual se puedan enviar y recibir paquetes de datos desde y hacia otras computadoras, empleando un protocolo para su comunicación y convirtiendo esos datos a un formato que pueda ser transmitido por el medio. Cada una de estas tarjetas de red le es asignado un identificador único por su fabricante, conocido como dirección MAC (Media Access Control), que consta de 48 bits (6 bytes). Dicho identificador permite direccionar el tráfico de datos de la red del emisor al receptor adecuados.
- *Servidor:* Este ejecuta el sistema operativo de red y ofrece los servicios de red a las estaciones de trabajo.

En la siguiente lista hay algunos tipos comunes de servidores y sus propósitos.

- *Servidor de archivos:* Almacena varios tipos de archivo y los distribuye a otros clientes en la red.

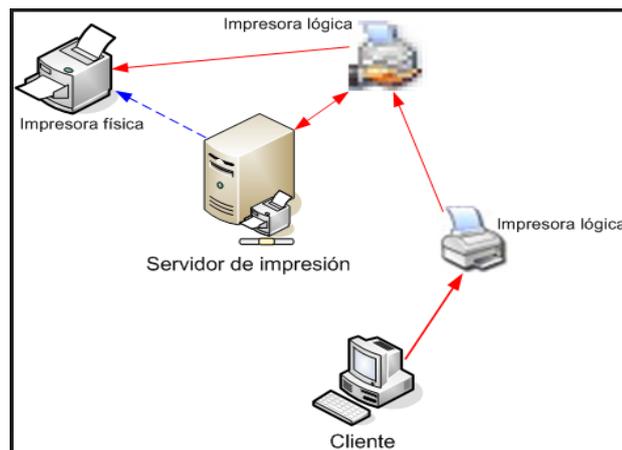
Figura 1. Servidor de archivos



<http://informatechgroup.com/portada/images/stories/servicios/servidor-archivos.jpg>

- *Servidor de impresiones:* Controla una o más impresoras y acepta trabajos de impresión de otros clientes de la red.

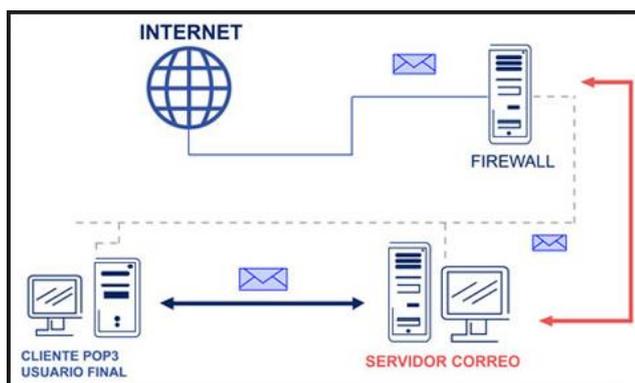
Figura 2. Servidor de impresiones



<https://solucionesinformaticas2011.files.wordpress.com/2011/06/esquema-impresoras.png>

- *Servidor de correo:* Almacena, envía, recibe, en ruta y realiza otras operaciones relacionadas con e-mail para los clientes de la red.

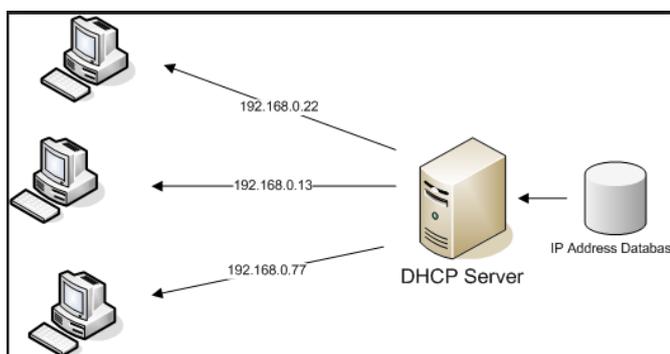
Figura 3. Servidor de correo



<http://s.culturacion.com/wp-content/uploads/2010/11/servidor-de-correo-D1.jpg>

- *Servidor de DHCP*: Protocolo de configuración de host dinámico. Es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración (principalmente, su configuración de red) en forma dinámica (es decir, sin intervención particular). Sólo tiene que especificarle al equipo, mediante DHCP, que encuentre una dirección IP de manera independiente. El objetivo principal es simplificar la administración de la red.

Figura 4. Servidor DHCP

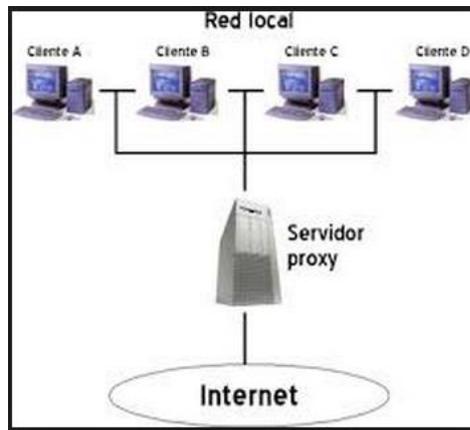


<http://portallinux.es/wp-content/uploads/2015/08/IntroDHCP1.png>

- *Servidor Proxy*: Realiza un cierto tipo de funciones a nombre de otros clientes en la red para aumentar el funcionamiento de ciertas operaciones. También sirve seguridad; esto es, tiene un Firewall (cortafuegos). Permite

administrar el acceso a internet en una red de computadoras permitiendo o negando el acceso a diferentes sitios Web.

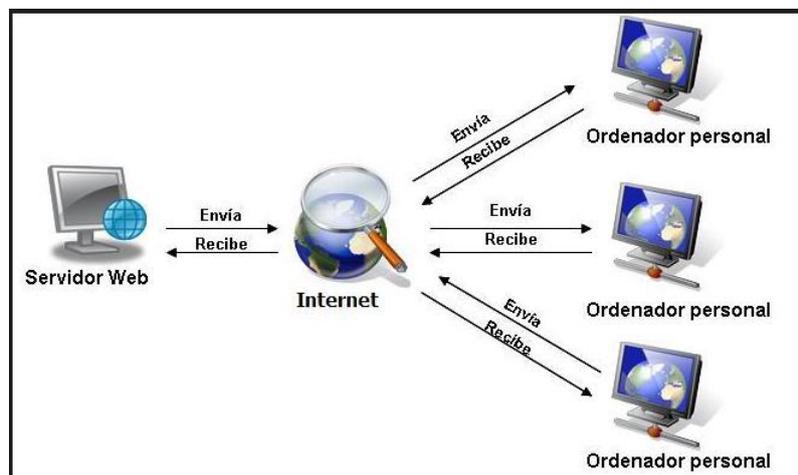
Figura 5. Servidor Proxi



<http://portallinux.es/wp-content/uploads/2015/08/Introproxi.png>

- *Servidor Web:* Almacena documentos HTML, imágenes, archivos de texto, escrituras, y demás material Web compuesto por datos (conocidos colectivamente como contenido), y distribuye este contenido a clientes que la piden en la red.

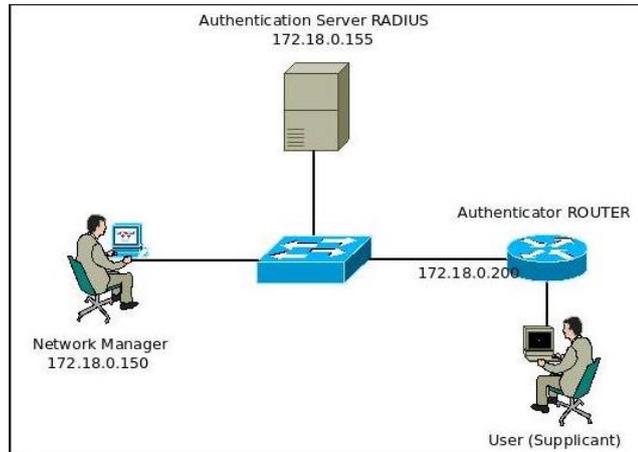
Figura 6. Servidor web



<https://servidores1191.files.wordpress.com/2013/09/internet.jpg>

- *Servidor de Autenticación:* Es el encargado de verificar que un usuario pueda conectarse a la red en cualquier punto de acceso, ya sea inalámbrico o por cable, basándose en el estándar 802.1x y puede ser un servidor de tipo RADIUS.

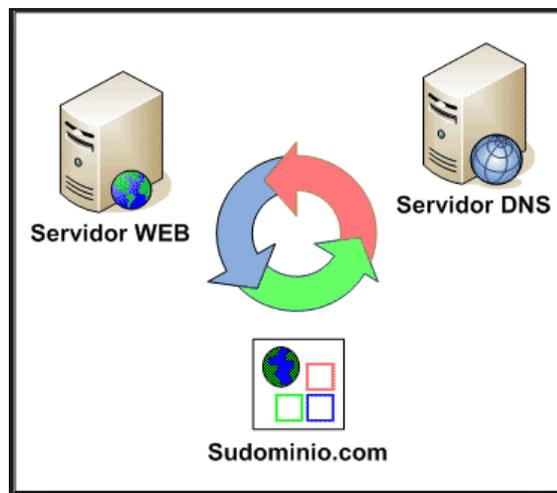
Figura 7. Servidor de autenticación



<http://www.securityartwork.es/wp-content/uploads/2013/12/radius.jpg>

- *Servidor DNS:* Este tipo de servidores resuelven nombres de dominio sin necesidad de conocer su dirección IP.

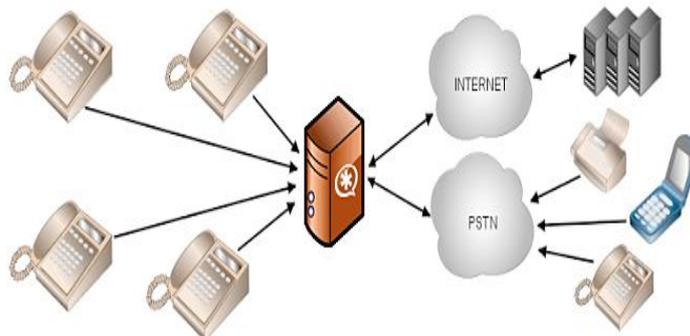
Figura 8. Servidor DNS



<http://www.dnsgratis.es/servidor-DNS.png>

- *Servido de Telefonía IP:* controlar y gestionar comunicaciones de cualquier tipo, ya sean analógicas, digitales o VoIP mediante todos los protocolos VoIP que implementa, permitiendo armar tu propia Central Telefónica en tu organización.

Figura 9. Servidor de telefonía IP



http://images.quebarato.cl/T440x/telefonía+ip+servidores+ip+bases+enrutadoras+santiago+metropolitana+de+santiago+chile__2D1F0C_1.jpg

Protocolo de Internet (IP).

El protocolo de Internet o IP (Internet Protocol) es un protocolo de red no orientado a conexión. Como su nombre indica,² IP es el protocolo por excelencia de Internet, y permite que se envíen y reciban paquetes de datos (también denominados datagramas) entre máquinas conectadas a la red de redes.

IP es un protocolo no confirmado, esto es, cada paquete enviado puede perderse o corromperse en la transmisión sin que la capa de red reciba notificación de ello, ya que no se recibe ninguna información que confirme la correcta recepción de los paquetes (este tipo de paquetes se denominan en inglés Acknowledgement o ACK). Por este motivo, se dice que IP no permite regular la calidad de servicio.

No obstante, sí es posible realizar comunicaciones con control sobre la calidad de servicio en Internet, gracias al uso de protocolos confirmados en las capas superiores, especialmente del protocolo de nivel de transporte denominado TCP, que da nombre al modelo de referencia [TCP/IP] de arquitectura de redes.

Direccionamiento IP.

Las llamadas direcciones IP son las que emplean los routers de Internet para localizar el equipo de destino y poder elegir la mejor ruta disponible para enviar

²Ribera del Loira: "Academia de Networking de Cisco Systems: Guía del segundo año CCNA 3 y 4", Tercera edición, Pearson Educación, 2004

los paquetes. En la versión del protocolo más extendida (IPv4), cada dirección consta de 4 números entre 0 y 255 separados por puntos, que se corresponde con 4 bytes de información (32 bits). Así, un ejemplo de dirección IP sería 192.16.0.8.

Desde el punto de vista de la visibilidad que tienen, las direcciones IP pueden ser:

- *Públicas*, cuando son accesibles directamente desde cualquier punto de Internet, por lo que deben ser únicas para cada máquina.
- *Privadas*, cuando sólo se puede acceder a ellas desde redes privadas como las LAN, por ejemplo. En estos casos, una misma dirección puede ser empleada en todas las redes privadas que sea necesario. Para evitar problemas de asignación, los rangos de IP privadas y públicas están bien diferenciados.

Desde el punto de vista de la asociación de una máquina en particular con una dirección IP en particular, las direcciones pueden ser:

- *Estáticas*, cuando una misma dirección corresponde siempre a la misma máquina.
- *Dinámicas*, cuando en cada conexión a Internet se obtiene una dirección distinta para una misma máquina. Este mecanismo permite optimizar el uso de direcciones para máquinas que no están conectadas permanentemente.

La estructura de las direcciones IP está dividida en 5 clases con sus respectivas gamas de direcciones, identificadas por los bits más significativos como lo muestra (la figura 10).

Figura 10. Clase de direccionamiento



[1http://personales.upv.es/rmartin/Tcplp/imagenes/clases-ip.gif](http://personales.upv.es/rmartin/Tcplp/imagenes/clases-ip.gif)

Protocolo de Internet (IPv4).

El Internet Protocol versión 4 (IPv4) en español: Protocolo de Internet versión 4 es la cuarta versión del protocolo Internet Protocol (IP), y la primera en ser implementada a gran escala. Definida en él RFC 791.

IPv4 usa direcciones de 32 bits, limitándola a $2^{32} = 4.294.967.296$ direcciones únicas, muchas de las cuales están dedicadas a redes locales (LANs). Por el crecimiento enorme que ha tenido Internet (mucho más de lo que esperaba, cuando se diseñó IPv4), combinado con el hecho de que hay desperdicio de direcciones en muchos casos ya hace varios años se vio que escaseaban las direcciones IPv4.

Esta limitación ayudó a estimular el impulso hacia IPv6, que está actualmente en las primeras fases de implantación, y se espera que termine reemplazando a IPv4.

El desperdicio de direcciones IPv4 se debe a varios factores. Uno de los principales es que inicialmente no se consideró el enorme crecimiento que iba a tener Internet; se asignaron bloques de direcciones grandes (de 16,271 millones de direcciones) a países, e incluso a muchas empresas.

Otro motivo de desperdicio es que en la mayoría de las redes, exceptuando las más pequeñas, resulta conveniente dividir la red en subredes. Dentro de cada

subred, la primera y la última dirección no son utilizables; de todos modos no siempre se utilizan todas las direcciones restantes. Por ejemplo, si en una subred se quieren acomodar 80 hosts, se necesita una subred de 128 direcciones (se tiene que redondear a la siguiente potencia de base 2); en este ejemplo, las 48 direcciones restantes ya no se utilizan.

Protocolo de internet (IPv6).

IPv6 (Internet Protocol Versión 6) o IPng (Next Generation Internet Protocol) es la nueva versión del protocolo IP (Internet Protocol). Ha sido diseñado por el IETF (Internet Engineering Task Force) para reemplazar en forma gradual a la versión actual, el IPv4.

En esta versión se mantuvieron las funciones del IPv4 que son utilizadas, las que no son utilizadas o se usan con poca frecuencia, se quitaron o se hicieron opcionales, agregándose nuevas características.

Características del protocolo de internet (IPv6).

- Mayor espacio de direcciones. El tamaño de las direcciones IP cambia de 32 bits a 128 bits, para soportar: más niveles de jerarquías de direccionamiento y más nodos direccionales.
- Simplificación del formato del Header. Algunos campos del Header IPv4 se quitan o se hacen opcionales
- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los Routers, alineados a 64 bits y con una cabecera de longitud fija, más simple, que agiliza su procesamiento por parte del Router.
- Posibilidad de paquetes con carga útil (datos) de más de 65.355 bytes.
- Seguridad en el núcleo del protocolo (IPsec). El soporte de IPsec es un requerimiento del protocolo IPv6.
- Capacidad de etiquetas de flujo. Puede ser usada por un nodo origen para etiquetar paquetes pertenecientes a un flujo (flow) de tráfico particular, que requieren manejo especial por los Routers IPv6, tal como calidad de servicio no por defecto o servicios de tiempo real. Por ejemplo video conferencia.
- Autoconfiguración: la autoconfiguración de direcciones es más simple. Especialmente en direcciones Agregatable Global Unicast, los 64 bits

superiores son seteados por un mensaje desde el router (Router Advertisement) y los 64 bits más bajos son seteados con la dirección MAC (en formato EUI-64). En este caso, el largo del prefijo de la subred es 64, por lo que no hay que preocuparse más por la máscara de red. Además el largo del prefijo no depende en el número de los hosts por lo tanto la asignación es más simple.

- Re-numeración y "multihoming": facilitando el cambio de proveedor de servicios.
- Características de movilidad, la posibilidad de que un nodo mantenga la misma dirección IP, a pesar de su movilidad.
- Ruteo más eficiente en el backbone de la red, debido a la jerarquía de direccionamiento basada en aggregation.
- Calidad de servicio (QoS) y clase de servicio (CoS).
- Capacidades de autenticación y privacidad.

Protocolo de resolución de direcciones (ARP).

El protocolo de resolución de direcciones se emplea para encontrar las direcciones de Hardware (en este caso MAC) usadas por las tarjetas de red a partir de la dirección IP, para este objetivo la fuente envía un mensaje de brocadas (difusión) en el cual se pide que la estación con la IP destino buscada conteste. Esta petición es recibida por todas las estaciones en la red, pero solo es contestada por el host requerido, quien incluye en su mensaje de respuesta su dirección MAC e IP, de tal manera que la fuente ya sabe cómo enviar paquetes a esa estación.

Para evitar el uso excesivo de peticiones ARP, las direcciones MAC e IP se guardan en cada host en una tabla ARP. Cada cierto intervalo de tiempo, entre 5 y 30 minutos, la tabla se refresca.

Protocolo de datagrama de usuario (UDP). Protocolo de Configuración de Host Dinámica (DHCP)

El protocolo de datagrama de usuario UDP está construido sobre el servicio ofrecido por IP para soportar un amplio rango de aplicaciones. ³UDP es un protocolo no orientado a conexión, es decir ofrece a las capas superiores un

³Modelos de referencia, [En línea]. Disponible en:
http://es.wikitel.info/wiki/Modelos_de_referencia, [Consulta: May. 2012].

modo para enviar paquetes de información sin necesidad de establecer previamente una conexión. Es un protocolo no confiable, ya que no ofrece garantías de que los datagramas llegarán a su destino.

El encabezado del segmento UDP es el siguiente:

Figura 11. Cabecera UDP

0	15	16	32
Puerto Fuente		Puerto Destino	
Longitud UDP		UDP checksum	
Datos			

[2http://personales.upv.es/rmartin/Tcplp/cap02s11.html](http://personales.upv.es/rmartin/Tcplp/cap02s11.html)

- *Puerto Fuente*: Identifica la aplicación o proceso particular en el host origen que envía los datos y al cual serán enviadas las respuestas.
- *Puerto de destino*: Este campo contiene el puerto correspondiente a la aplicación del equipo receptor al que se envía.
- *Longitud*: Este campo especifica la longitud total del segmento, con el encabezado incluido. Sin embargo, el encabezado tiene una longitud de 4 x 16 bits (que es 8 x 8 bits), por lo tanto la longitud del campo es necesariamente superior o igual a 8 bytes.
- *Checksum UDP*: Tiene la función de detectar errores en el datagrama. Si la fuente no desea calcular el checksum, este campo debe ser llenado con ceros. Si el resultado del checksum es cero el campo se llena con unos.
- *Datos*: Aquí viajan los datos que se envían las aplicaciones. Los mismos datos que envía la aplicación origen son recibidos por la aplicación destino después de atravesar toda la Red de redes.

Protocolo de Configuración de Host Dinámica (DHCP)

El Protocolo de Configuración Dinámica de Estaciones es un estándar TCP/IP que reduce la complejidad y sobrecarga administrativa que implica la configuración de direccionamiento IP de estaciones.

Cada dispositivo en una red TCP/IP debe tener una dirección IP única para poder acceder a la red y sus recursos. Sin el empleo de DHCP, la configuración IP debe hacerse manualmente en aquellas estaciones que se inician en la red o que se trasladan de una subred a otra. DHCP constituye un mecanismo para asignar direcciones IP a computadores de manera automática, eliminando las limitaciones de la configuración manual de TCP/IP.

Al instalar DHCP en una red, el proceso de configuración TCP/IP se automatiza y administra centralizadamente. El servidor de DHCP mantiene un grupo de direcciones IP y arrienda una dirección IP a cualquier cliente DHCP que se inicia en la red. Dado que las direcciones IP son dinámicas (arrendadas) y no estáticas (asignadas permanentemente), las direcciones que ya no se usen, se devuelven automáticamente al grupo de direcciones asignables para su reasignación.

El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

- a. *Asignación automática.* DHCP asigna una dirección IP permanente al host.
- b. *Asignación dinámica.* DHCP asigna una dirección IP para un periodo de tiempo limitado. Tal dirección de red se llama una lease. Este es el único mecanismo que permite la reutilización automática de direcciones que ya no necesita el host a las que fue asignado.
- c. *Asignación manual o estática.* Asigna una dirección IP a una máquina determinada. Se suele utilizar cuando se quiere controlar la asignación de dirección IP a cada cliente, y evitar, también, que se conecten clientes no identificados.

Cableado estructurado.

El cableado estructurado consiste en el tendido de cables en el interior de un edificio con el propósito de implantar una red de área local. Suele tratarse de cable de par trenzado de cobre, para redes de tipo IEEE 802.3. No obstante, también puede tratarse de fibra óptica o cable coaxial.

En el sistema de cableado estructurado, la infraestructura de cable destinada a transportar, a lo largo y ancho de un edificio, las señales que emite un emisor de algún tipo de señal hasta el correspondiente receptor. Un sistema de cableado estructurado es físicamente una red de cable única y completa, con

combinaciones de alambre de cobre (pares trenzados sin blindar UTP), cables de fibra óptica, bloques de conexión, cables terminados en diferentes tipos de conectores y adaptadores. Uno de los beneficios del cableado estructurado es que permite la administración sencilla y sistemática de las mudanzas y cambios de ubicación de personas y equipos. El sistema de cableado de telecomunicaciones para edificios soporta una amplia gama de productos de telecomunicaciones sin necesidad de ser modificado. Utilizando este concepto, resulta posible diseñar el cableado de un edificio con un conocimiento muy escaso de los productos de telecomunicaciones que luego se utilizarán sobre él. La norma garantiza que los sistemas que se ejecuten de acuerdo a ella soportarán todas las aplicaciones de telecomunicaciones presentes y futuras por un lapso de al menos diez años. Esta afirmación puede parecer excesiva, pero no, si se tiene en cuenta que entre los autores de la norma están precisamente los fabricantes de estas aplicaciones.

El tendido supone cierta complejidad cuando se trata de cubrir áreas extensas tales como un edificio de varias plantas. En este sentido hay que tener en cuenta las limitaciones de diseño que impone la tecnología de red de área local que se desea implantar:

- La segmentación del tráfico de red.
- La longitud máxima de cada segmento de red.
- La presencia de interferencias electromagnéticas.
- La necesidad de redes locales virtuales.

Cableado vertical, troncal o backbone.

El propósito del cableado del backbone es proporcionar interconexiones entre cuartos de entrada de servicios de edificio, cuartos de equipo y cuartos de telecomunicaciones. El cableado del backbone incluye la conexión vertical entre pisos en edificios de varios pisos. El cableado del backbone incluye medios de transmisión (cable), puntos principales e intermedios de conexión cruzada y terminaciones mecánicas. El cableado vertical realiza la interconexión entre los diferentes gabinetes de telecomunicaciones y entre estos y la sala de equipamiento. En este componente del sistema de cableado ya no resulta económico mantener la estructura general utilizada en el cableado horizontal, sino que es conveniente realizar instalaciones independientes para la telefonía y

datos. Esto se ve reforzado por el hecho de que, si fuera necesario sustituir el backbone, ello se realiza con un coste relativamente bajo, y causando muy pocas molestias a los ocupantes del edificio. El backbone telefónico se realiza habitualmente con cable telefónico multipar. Para definir el backbone de datos es necesario tener en cuenta cuál será la disposición física del equipamiento. Normalmente, el tendido físico del backbone se realiza en forma de estrella, es decir, se interconectan los gabinetes con uno que se define como centro de la estrella, en donde se ubica el equipamiento electrónico más complejo.

El backbone de datos se puede implementar con cables UTP o con fibra óptica. En el caso de decidir utilizar UTP, el mismo será de categoría 5 y se dispondrá un número de cables desde cada gabinete al gabinete seleccionado como centro de estrella.

Actualmente, la diferencia de coste provocada por la utilización de fibra óptica se ve compensada por la mayor flexibilidad y posibilidad de crecimiento que brinda esta tecnología. Se construye el backbone llevando un cable de fibra desde cada gabinete al gabinete centro de la estrella. Si bien para una configuración mínima Ethernet basta con utilizar cable de 2 fibras, resulta conveniente utilizar cable con mayor cantidad de fibra (6 a 12) ya que la diferencia de coste no es importante y se posibilita por una parte disponer de conductores de reserva para el caso de falla de algunos, y por otra parte, la utilización en el futuro de otras topologías que requieren más conductores, como FDDI o sistemas resistentes a fallas. ⁴La norma EIA/TIA 568 prevé la ubicación de la transmisión de cableado vertical a horizontal, y la ubicación de los dispositivos necesarios para lograrla, en habitaciones independientes con puerta destinada a tal fin, ubicadas por lo menos una por piso, denominadas armarios de telecomunicaciones.

Se utilizan habitualmente gabinetes estándar de 19 pulgadas de ancho, con puertas, de aproximadamente 50 cm de profundidad y de una altura entre 1.5 y 2 metros. En dichos gabinetes se dispone generalmente de las siguientes secciones:

- Acometida de los puestos de trabajo: 2 cables UTP llegan desde cada puesto de trabajo.

⁴ TIA/EIA-568-B.1-7 Commercial Building Telecommunications Cabling Standard Part 1: General Requirements Addendum 7 - Guidelines for Maintaining Polarity Using Array Connectors

- Acometida del backbone telefónico: cable multipar que puede determinar en regletas de conexión o en “patch panels”.
- Acometida del backbone de datos: cables de fibra óptica que se llevan a una bandeja de conexión adecuada.
- Electrónica de la red de datos: Hubs, Switches, Bridges y otros dispositivos necesarios.
- Alimentación eléctrica para dichos dispositivos.
- Iluminación interna para facilitar la realización de trabajos en el gabinete.
- Ventilación a fin de mantener la temperatura interna dentro de límites aceptables.

Fibra óptica.

La fibra óptica es un medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir. El haz de luz queda completamente confinado y se propaga por el interior de la fibra con un ángulo de reflexión por encima del ángulo límite de reflexión total, en función de la ley de Snell. La fuente de luz puede ser láser o un LED.

Las fibras se utilizan ampliamente en telecomunicaciones, ya que permiten enviar gran cantidad de datos a una gran distancia, con velocidades similares a las de radio y superiores a las de cable convencional. Son el medio de transmisión por excelencia al ser inmune a las interferencias electromagnéticas, también se utilizan para redes locales, en donde se necesite aprovechar las ventajas de la fibra óptica sobre otros medios de transmisión.

Wi-Fi.

Es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. Los dispositivos habilitados con Wi-Fi, tales como: un ordenador personal, una consola de videojuegos, un Smartphone o un reproductor de audio digital, pueden conectarse a Internet a través de un punto de acceso de red inalámbrica. Dicho punto de acceso (o hotspot) tiene un alcance de unos 20 metros (65 pies) en interiores y al aire libre una distancia mayor. Pueden cubrir grandes áreas la superposición de múltiples puntos de acceso.

Seguridad y Fiabilidad.

Uno de los problemas a los cuales se enfrenta actualmente la tecnología Wi-Fi es la progresiva saturación del espectro radioeléctrico, debido a la masificación de usuarios, esto afecta especialmente en las conexiones de larga distancia (mayor de 100 metros). ⁵En realidad Wi-Fi está diseñado para conectar ordenadores a la red a distancias reducidas, cualquier uso de mayor alcance está expuesto a un excesivo riesgo de interferencias.

Un muy elevado porcentaje de redes son instalados sin tener en consideración la seguridad convirtiendo así sus redes en redes abiertas (o completamente vulnerables ante el intento de acceder a ellas por terceras personas), sin proteger la información que por ellas circulan.

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

- WEP, cifra los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos. Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP. WEP codifica los datos mediante una “clave” de cifrado antes de enviarlo al aire.
- Este tipo de cifrado no está muy recomendado, debido a las grandes vulnerabilidades que presenta, ya que cualquier cracker puede conseguir sacar la clave.
- WPA: presenta mejoras como generación dinámica de la clave de acceso. Las claves se insertan como dígitos alfanuméricos.
- IPSEC (túneles IP) en el caso de las VPN y el conjunto de estándares IEEE 802.1X, que permite la autenticación y autorización de usuarios.

⁵Linux wireless LAN support <http://linux-wless.passsys.nl>

- Filtrado de MAC, de manera que sólo se permite acceso a la red a aquellos dispositivos autorizados. Es lo más recomendable si solo se va a usar con los mismos equipos, y si son pocos.
- del punto de acceso: se puede ocultar el punto de acceso (Router) de manera que sea invisible a otros usuarios.
- El protocolo de seguridad llamado *WPA2* (estándar 802.11i), que es una mejora relativa a *WPA*. En principio es el protocolo de seguridad más seguro para Wi-Fi en este momento. Sin embargo requieren hardware y software compatibles, ya que los antiguos no lo son.

Sin embargo, no existe ninguna alternativa totalmente fiable, ya que todas ellas son susceptibles de ser vulneradas.

2.2. Marco Jurídico.

Identificamos las necesidades de la empresa y diseñamos una solución integral que permita satisfacer sus necesidades actuales y futuras, incluyendo tantos equipos activos, tales como switch, router, servidores. Como equipos pasivos que integran la solución de cableado estructurado, fibra óptica y otros tipos de conectividad que permiten integrar los diferentes servicios de voz, datos, internet y video.

El cableado estructurado está diseñado para usarse en cualquier forma, en cualquier lugar, y en cualquier momento. Elimina la necesidad de seguir las reglas de un proveedor en particular, concernientes a tipos de cable, conectores, distancias, o topologías. Permite instalar una sola vez el cableado, y después adaptarlo a cualquier aplicación, desde telefonía, hasta redes locales Ethernet o Token Ring.

La norma central que especifica un género de sistema de cableado para telecomunicaciones

***ANSI/EIA/TIA-568A.**

Las topologías, la distancia máxima de los cables, el rendimiento de los componentes, la toma y los conectores de telecomunicaciones.

Ambos estándares el TIA/EIA 568 y la ISO/IEC 11801 especifican sistemas de cableado para telecomunicación de multipropósito cableado estructurado que es utilizable para un amplio rango de aplicaciones (análogas y de telefonía ISDN, varios estándares de comunicación de datos, construcción de sistemas de control, automatización de fabricación). Cubre tanto cableado de cobre

balanceado como cableado de fibra óptica. El estándar fue diseñado para uso comercial que puede consistir en uno o múltiples edificios en un campus. Fue optimizado para utilidades que necesitan hasta 3 km de distancia, hasta 1 km² de espacio de oficinas, con entre 50 y 50.000 personas, pero también puede ser aplicado para instalaciones fuera de este rango.

***ANSI/EIA/TIA-569.**

Distribución de cableado, backbones, armario de cableado, terminales, canalizaciones.

Norma de construcción comercial para vías y espacios de telecomunicaciones", que proporciona directrices para conformar ubicaciones, áreas, y vías a través de las cuales se instalan los equipos y medios de telecomunicaciones.

***ANSI/TIA/EIA-606.**

Norma de administración para la infraestructura de telecomunicaciones en edificios comerciales.

Proporciona normas para la codificación de colores, etiquetado, y documentación de un sistema de cableado instalado. Seguir esta norma, permite una mejor administración de una red, creando un método de seguimiento de los traslados, cambios y adiciones. Facilita además la localización de fallas, detallando cada cable tendido por características.

***ANSI/TIA/EIA-607.**

Requerimientos de puesta y conexiones a tierra para telecomunicaciones

El propósito principal es crear un camino adecuado y con capacidad suficiente para dirigir las corrientes eléctricas y voltajes pasajeros hacia la tierra. Estas trayectorias a tierra son más cortas de menor impedancia que las del edificio.

***ISO/IEC 11801.**

Cableado de sistemas de TI para las instalaciones del cliente.

El estándar internacional **ISO/IEC 11801** especifica sistemas de cableado para telecomunicación de multipropósito cableado estructurado que es utilizable para un amplio rango de aplicaciones (análogas y de telefonía ISDN, varios estándares de comunicación de datos, construcción de sistemas de control, automatización de fabricación). Cubre tanto cableado de cobre balanceado como cableado de fibra óptica. El estándar fue diseñado para uso comercial que puede consistir en uno o múltiples edificios en un campus. Fue optimizado para utilidades que necesitan hasta 3 km de distancia, hasta 1 km² de espacio de oficinas, con entre 50 y 50.000 personas, pero también puede ser aplicado para instalaciones fuera de este rango. Un estándar correspondiente para oficinas de entorno SOHO (small-office/home-office) es ISO/IEC 15018, que cubre también vínculos de 1,2 GHz para aplicaciones de TV por cable y TV por satélite.

***ISO/IEC 14763-2.**

Administración, documentación y registros.

ISO / IEC 14763-2: 2012 (E) especifica los requisitos para la planificación, instalación y funcionamiento de infraestructuras de cableado y cableado (incluido el cableado, las vías, espacios, puesta a tierra y unión) en apoyo de las normas de cableado genéricos y documentos asociados. Se abordan los siguientes aspectos:

- Especificación de la instalación.
- La garantía de calidad.
- La planificación de la instalación.
- La práctica de la instalación.
- La documentación.
- La administración.
- La prueba.
- La inspección.
- La operación.
- Mantenimiento y reparación.

Capítulo III.

3.1. Análisis del proyecto.

La empresa I-3NET, se encuentra constituida en una sede principal, en la cual se encuentran todas las áreas que la componen, Los niveles tienen una estructura física similar, de tal manera que la división de los puestos y oficinas es casi la misma en las plantas de la sede principal, y su distribución general es la siguiente:

3.1.1. Situación actual de la empresa I-3NET.

- Sede principal y administrativa.
 - 2 plantas.
 - 1 data center.

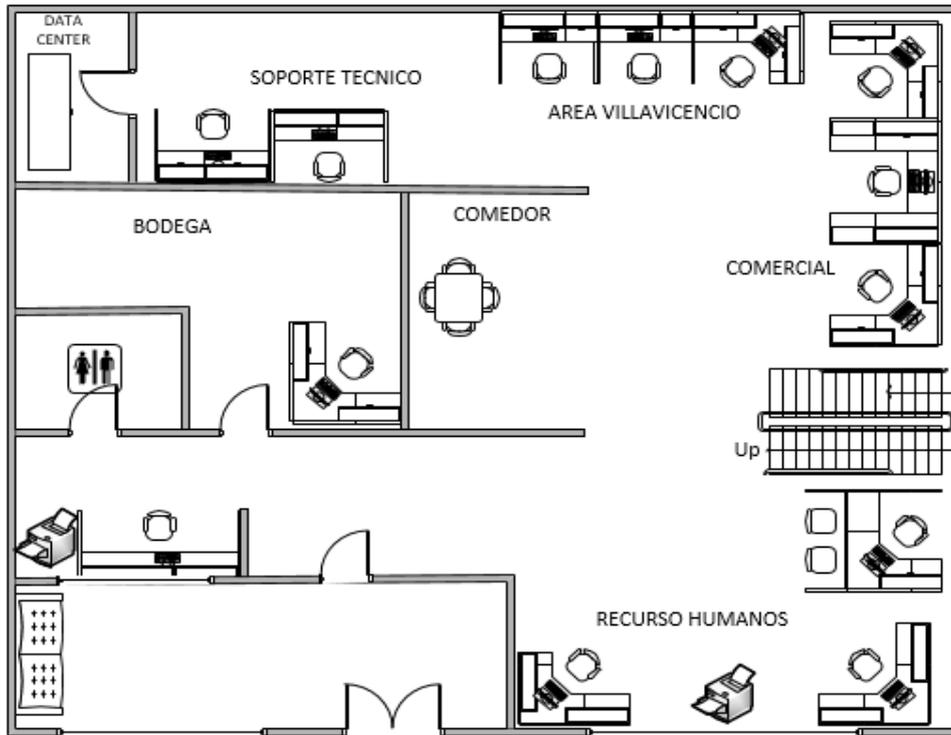
Tabla 1. Información actual sede principal

	ITEM	DETALLE	CANT.	V/UNIT	V/TOTAL
		DETALLE ESTRUCTURADO CAT 7A			
GABINETE	1	Rack Gabinete De Piso 18 Ru 90 Cm Soportetecnologico Racks.	1	480.000,00	\$480.000,00
	2	Patch Panel 48 Puertos Categoria 6 Marca Siemon	1	300.000,00	\$300.000,00
	3	Switch Hp Giga 48 Puertos Adminis L2 Giga 1620-48g.	1	1.808.000,00	\$1.808.000,00
	4	Multitoma Para Rack 8 Salidas Soportetecnologico.	1	71.000,00	\$71.000,00
	5	Servidor Hp Proliant Dl120 G7 Xeon 3.30ghz.	1	2.000.000,00	\$2.000.000,00

CABLEADO	7	574 MTS, 300 Caja de cable Utp 5e Interior Para Redes.	2	104.000,00	\$208.000,00
	8	Cable Rj45 Patch Cord Cat6 2 Metros Certificado.	25	7.000,00	\$175.000,00
EQUIPOS HOST	9	13 Computadores I3, 2GB RAM, 250 GB DD	21	990.000,00	\$20.790.000,00
	10	Impresora Industrial Sharp 337 Imagen Digital	1	1.000.000,00	\$1.000.000,00
	11	Impresora Hp 2545 Multifuncional	3	120.000,00	\$360.000,00
CANAL	12	CANAL DE 10 Mbps. Descripción, GASTO ANUAL	12	120.000,00	\$1.440.000,00
		Velocidad de descarga: Hasta 10.240 Kbps Velocidad de carga: Hasta 2.048 Kbps			
					\$28.982.000,00

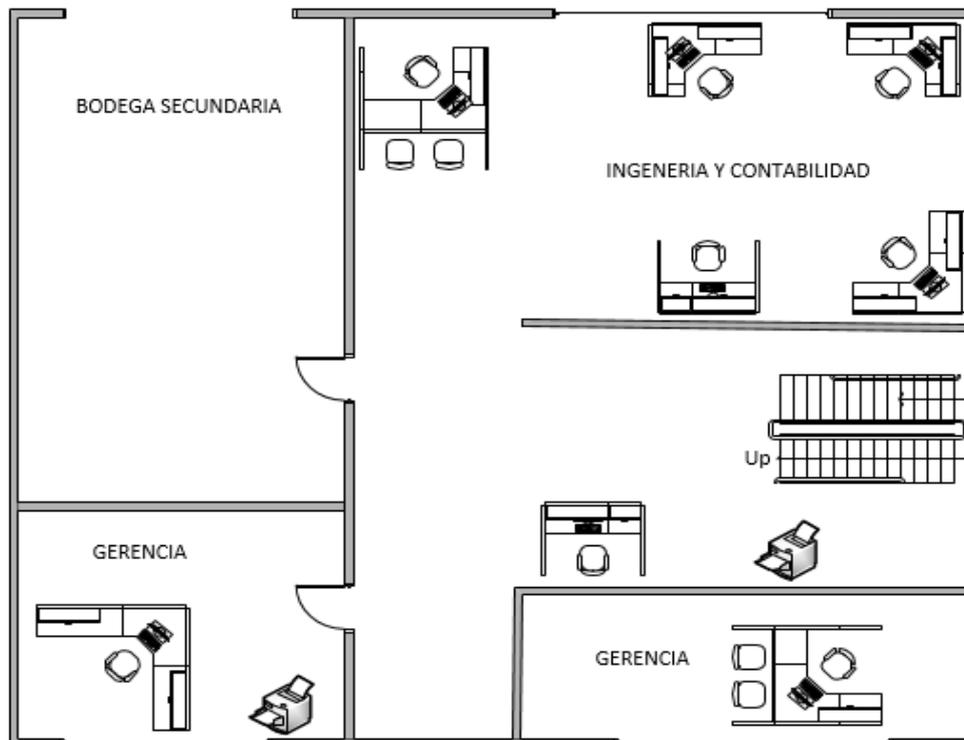
3.1.2. Plano físicos y de red de la sed principal.

Figura 12. Plano sede principal planta baja.



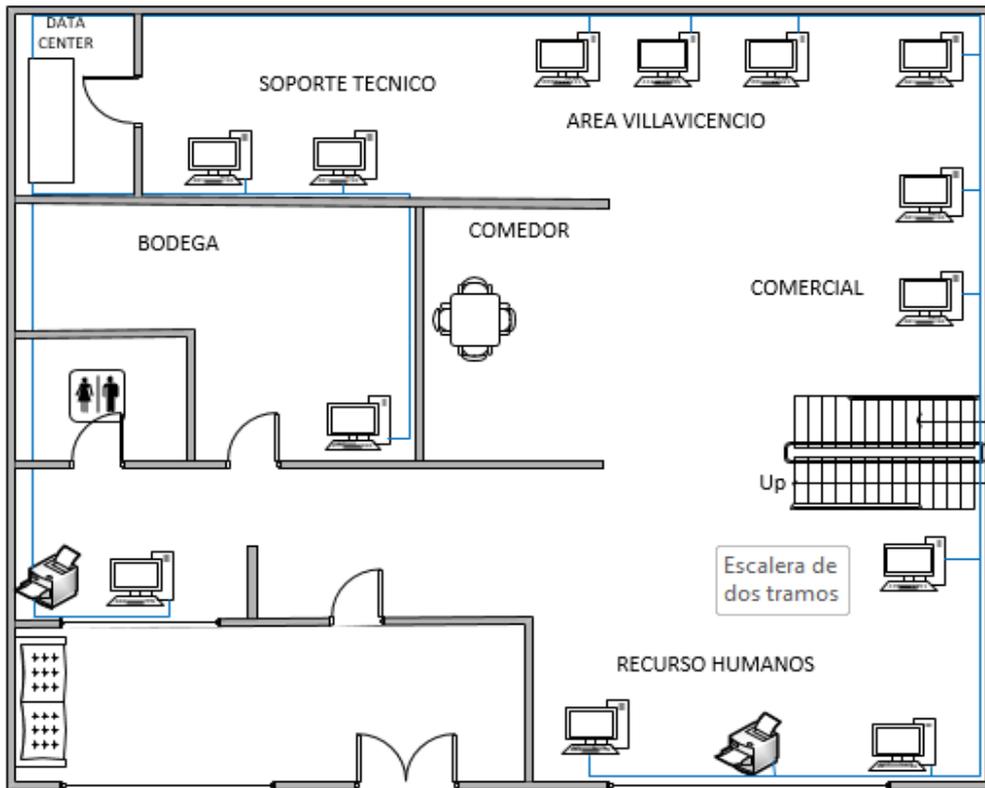
Lizarazo F. Plano empresa I-3NET. Realizado Microsoft Visio.

Figura 13. Plano sede principal planta alta.



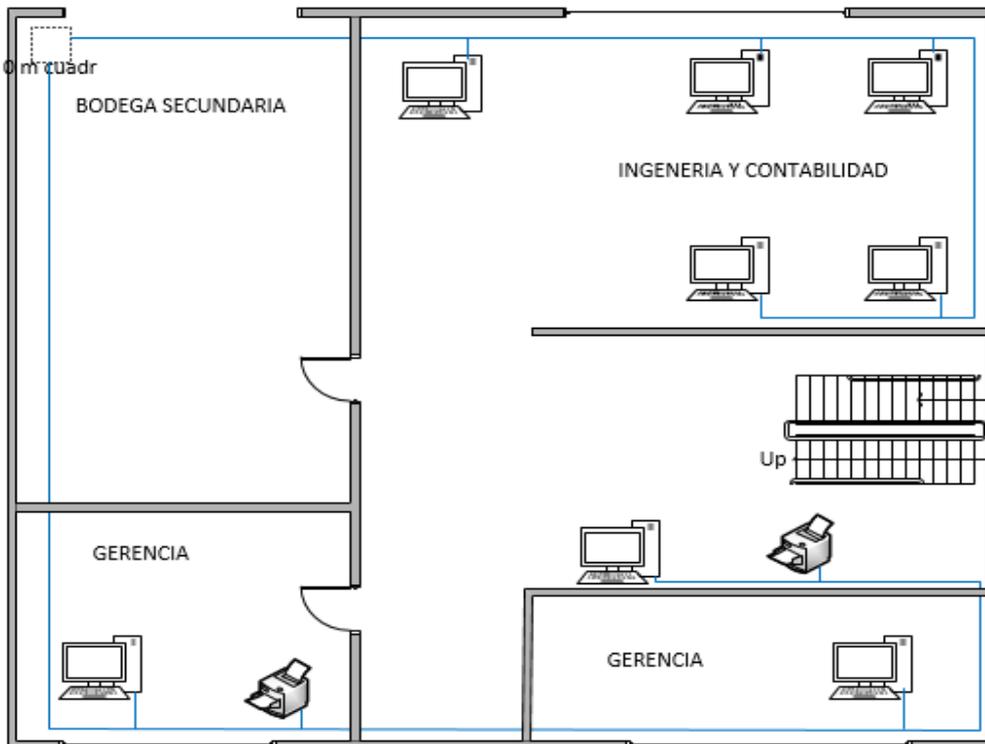
Lizarazo F. Plano empresa I-3NET. Realizado Microsoft Visio.

Figura 14. Plano sede principal planta baja red



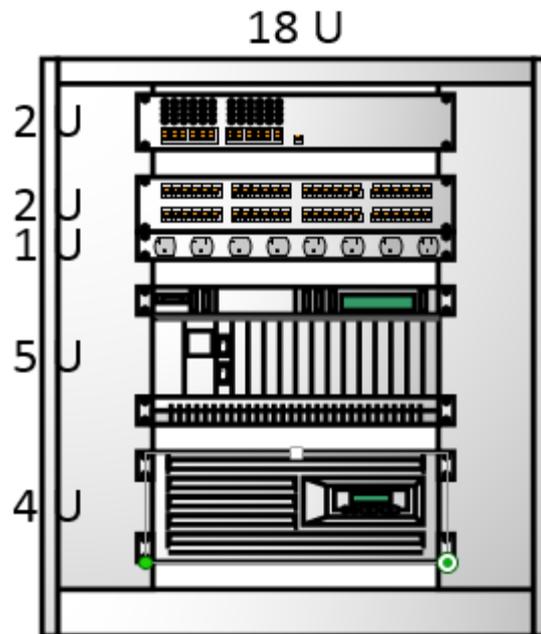
Lizarazo F. Plano red empresa I-3NET. Realizado Microsoft Visio.

Figura 15. Plano sede principal planta alta red



Lizarazo F. Plano red empresa I-3NET. Realizado Microsoft Visio.

Figura 16. Gabinete actual



Lizarazo F. Gabinete empresa I-3NET. Realizado Microsoft Visio.

3.2. Estructura temática.

Aunque se pretende actualizar el diseño de una red privada de ordenadores para la sede principal de **I-3NET**, no solo se hará en la parte física como son el cableado y los equipos que conforman una red, si no se agilizará en la parte lógica usando redes virtuales VLAN's, VPN's y configuraciones más inteligentes para los servidores, los cuales ofrecerán más servicios a la red adicionamos al diseño más servicios como telefonía IP, y seguridad con cámaras IP.

3.2.1. Limitaciones.

Teniendo en cuenta que el edificio no cuenta con una planta eléctrica o un sistema de ups; por lo tanto no hay garantía del funcionamiento de la red en el 100% del tiempo ya que el funcionamiento de la red está sujeto al fluido eléctrico de la empresa prestadora de este servicio. Por otro lado tenemos los equipos de cómputo que con el pasar de tiempo, la empresa no tuvo la precaución de actualizar su plataforma, por tal motivo muchos de los procesos que ejecutan los equipos son lentos y varios de estos equipos tienen un bajo acceso a la red. Considerando la expansión de la empresa no se programó el crecimiento de la red en host de servicio Asimismo como el ancho de bando ya no es suficiente

para cubrir las necesidades de comunicación, suele producirse el fenómeno denominado cuello de botella, provocando disminución en el rendimiento del sistema e impactando de manera negativa en las operaciones. Las redes hoy en día ofrecen más servicios que la simple comunicación de host a un servidor para guardar información, los servicios de telefonía IP no se han implementado, y la empresa no cuenta con seguridad perimetral. Los servidores no tienen la capacidad suficiente para desarrollar más servicios que los de host.

3.3. Determinación de los requerimientos.

- Garantizar puntos de red para cada uno de los terminales existentes en las plantas de cada una de las sedes según sea la distribución física que tiene la empresa. Por medio del cambio del cableado, actualizando la categoría y certificando cada uno de los puntos de red que soportaran la plataforma ya sea host, telefonía IP o Cámaras IP.
- Elaborar un diseño para actualizar la red privada que permita implementar la tecnología de red tipo anillo, con una interconexión eficaz y eficiente, asegurando que la red sea redundante.
- Establecer los accesos y privilegios de manera jerárquica a las diferentes áreas de la institución. Por medio de VLAN's y segmentando la red por áreas.
- Contratar un BW de 50 Mbps, con el cual aseguraremos la satisfacción de las necesidades de comunicación y servicios adicionales
- Implementar zonas de red Wi-Fi.
- Implementar servidor de impresoras.
- Implementar servidor de VoIP.
- Implementar seguridad perimetral, por medio de cámaras IP.
- La proyección del proyecto de red planteado, para la institución vendría a solucionar, en gran medida, muchos de los problemas que actualmente las sedes presenta respecto al manejo de información, permitiéndole a quienes allí laboran poder acceder a ésta de manera más rápida, eficiente y confiable.

Si bien es cierto que existe en la planta física del edificio, algunos elementos que podrían facilitar la implementación de una red, debe reconocerse que en la existencia de equipos de computación con los que cuenta la sede principal presentan serias carencias que deberán ser corregidas necesariamente para que la red a diseñar no encuentre en ello un obstáculo.

A continuación se enumeran los ítems de los requerimientos que se desean instalar.

Tabla 2. Análisis y definiciones de Requerimientos sede principal

	ITEM	DETALLE	CANT.	V/UNIT	V/TOTAL
		DETALLE ESTRUCTURADO CAT 7A			
GABINETE	1	Gabinete Rack 19" De Piso De 180 Cms Ru 40 Inrp180	1	1.674.000,00	\$1.674.000,00
	2	Patch Panel Cat6a 48 Puertos Categoría 6a Jack Rj45 Qpcom	2	1.245.000,00	\$2.490.000,00
	3	Switch Hp 48 Puertos Giga Sfp Administrable J9775a 2530-48g	2	4.728.100,00	\$9.456.200,00
	4	Multitoma Para Rack 8 Salidas Soportetecnologico.	2	71.000,00	\$142.000,00
	5	Servidor Cisco Nac3315-500-k9 Core 2 Quad - 4 Gb - 1T	1	9.274.500,00	\$9.274.500,00
	6	Pantalla De Portátil Lcd 14.1 Hp, Tecaldo gabinete.	1	180.000,00	\$180.000,00
CABLEADO	7	1170 MTS, Cable Utp Cat 6a Rollo X 305 Metros Amp Certificado.	4	660.000,00	\$2.640.000,00
	8	Cable Rj45 Patch Cord Cat6 2 Metros Certificado.	62	7.000,00	\$434.000,00

EQUIPOS HOST	9	PORTATIL ASUS I7 X555I PROCESADOR INTEL CORE TM i7 451OU SISTEMA OPERATIVO WINDOWS 8.1 MEMORIA DDR3L 1600 MHz SDRAM, 8 GB SDRAM	33	1.500.000,00	\$49.500.000,00
	10	Impresora Industrial Sharp 337 Imagen Digital	2	1.000.000,00	\$2.000.000,00
	11	Impresora Hp 2545 Multifuncional	6	120.000,00	\$720.000,00
CANAL	12	CANAL DE 1 Gbps. Descripción, GASTO ANUAL	12	290.000,00	\$3.480.000,00
					\$81.990.700,00

Tabla 3. Análisis y definiciones de Requerimientos sede ingeniería

	ITEM	DETALLE	CANT.	V/UNIT	V/TOTAL
		DETALLE ESTRUCTURADO CAT 7A			
GABINETE	1	Gabinete Rack de Piso De 180 Cms Ru 40 Inrp180	1	1.674.000,00	\$1.674.000,00
	2	Patch Panel Cat6a 48 Puertos Categoria 6a Jack Rj45 Qpcom	1	1.245.000,00	\$1.245.000,00
	3	Switch Hp 48 Puertos Giga Sfp Administrable J9775a 2530-48g	1	4.728.100,00	\$4.728.100,00
	4	Multitoma Para Rack 8 Salidas Soportetecnologico.	1	71.000,00	\$71.000,00
	5	Pantalla De Portátil Lcd 14.1 Hp, Tecaldo gabinete.	1	180.000,00	\$180.000,00
CABLEADO	6	665 MTS, Cable Utp Cat 6a Rollo X 305 Metros Amp Certificado.	3	660.000,00	\$1.980.000,00
	7	Cable Rj45 Patch Cord Cat6 2 Metros Certificado.	32	7.000,00	\$224.000,00
EQUIPOS HOST	8	PORTATIL ASUS I7 X555I PROCESADOR INTEL CORE TM i7 451OU SISTEMA OPERATIVO WINDOWS 8.1	12	1.500.000,00	\$18.000.000,00

		MEMORIA DDR3L 1600 MHz SDRAM, 8 GB SDRAM			
	9	Impresora Industrial Sharp 337 Imagen Digital	1	1.000.000,00	\$1.000.000,00
	10	Impresora Hp 2545 Multifuncional	4	120.000,00	\$480.000,00
CANAL	11	CANAL DE 20 Mbps. Descripción, GASTO ANUAL	12	150.000,00	\$1.800.000,00
					\$31.382.100,00

3.4. Diseño del proyecto.

3.4.1. Topología de la red. Diseño del modelo de direccionamiento y nombramiento.

Para este proyecto se implementara una topología de estrella, puesto que esta se adapta más a las necesidades del proyecto, centralizando su cableado, y permitiendo diferenciar los servicios que se pretenden montar. Y a su vez, esta topología será implementada en todas sedes de la empresa.

3.4.2. Diseño del modelo de direccionamiento y nombramiento.

Para el proyecto realizaos el siguiente direccionamiento para las sedes de I-3NET.

- Direccionamiento para la sede principal.

En la sede principal se encuentra el core de la compañía, y la segmentamos en las diferentes áreas las cuales discriminamos en la tabla 3.

Tabla 4. Diseño del modelo de direccionamiento.

DIRECCIONAMIENTO IP SEGMENTADO SEDE PRINCIPAL.			
AREA	HOTS NECESARIOS	DATOS	DIRECCIONAMIENTO
TELEFONIA IP	17	Network	192.168.0.0
		Bitmask	27
		Netmask	255.255.255.224
		Wildcardmask	0.0.0.31
		Host range	192.168.0.1
			192.168.0.30
		Broadcast address	192.168.0.31
total IP addresses	30		
CAMARAS	12	Network	192.168.0.32
		Bitmask	27
		Netmask	255.255.255.224
		Wildcardmask	0.0.0.31
		Host range	192.168.0.33-
			192.168.0.62
		Broadcast address	192.168.0.63
total IP addresses	30		
IMPRESORAS	10	Network	192.168.0.64
		Bitmask	28
		Netmask	255.255.255.240
		Wildcardmask	0.0.0.15

		Host range	192.168.0.65-
			192.168.0.78
		Broadcast address	192.168.0.79
		total IP addresses	14
COMERCIAL	7	Network	192.168.0.80
		Bitmask	28
		Netmask	255.255.255.240
		Wildcardmask	0.0.0.15
		Host range	192.168.0.81-
			192.168.0.94
		Broadcast address	192.168.0.95
		total IP addresses	14
SOPORTE	5	Network	192.168.0.96
		Bitmask	28
		Netmask	255.255.255.240
		Wildcardmask	0.0.0.15
		Host range	192.168.0.97-
			192.168.0.110
		Broadcast address	192.168.0.111
		total IP addresses	14
RECURSOS HUMANOS	5	Network	192.168.0.112
		Bitmask	28
		Netmask	255.255.255.240
		Wildcardmask	0.0.0.15
		Host range	192.168.0.113-
			192.168.0.126
		Broadcast address	192.168.0.127
		total IP addresses	14
GERENCIA	4	Network	192.168.0.128
		Bitmask	29
		Netmask	255.255.255.248
		Wildcardmask	0.0.0.7
		Host range	192.168.0.129-
			192.168.0.134
		Broadcast address	192.168.0.135
		total IP addresses	6
CONTABILIDAD	3	Network	192.168.0.136
		Bitmask	29
		Netmask	255.255.255.248
		Wildcardmask	0.0.0.7
		Host range	192.168.0.137-
			192.168.0.142
		Broadcast address	192.168.0.143

RECEPCION Y BODEGA	2	total IP addresses	6
		Network	192.168.0.144
		Bitmask	29
		Netmask	255.255.255.248
		Wildcardmask	0.0.0.7
		Host range	192.168.0.145-
			192.168.0.150
		Broadcast address	192.168.0.151
total IP addresses	6		

- Direccionamiento de la sede de ingeniería.

En la sede principal se encuentra el core de la compañía, y la segmentamos en las diferentes áreas las cuales discriminamos en la tabla 3.

Tabla 5. Direccionamiento de la sede de ingeniería

DIRECCIONAMIENTO IP SEGMENTADO SEDE INGENIERIA			
AREA	HOTS NECESARIOS	DATOS	DIRECCIONAMIENTO
TELEFONIA IP	12	Network	192.168.0.0
		Bitmask	27
		Netmask	255.255.255.224
		Wildcardmask	0.0.0.31
		Host range	192.168.0.1-
			192.168.0.30
		Broadcast address	192.168.0.31
		total IP addresses	30
CAMARAS	8	Network	192.168.0.32
		Bitmask	28
		Netmask	255.255.255.240
		Wildcardmask	0.0.0.15
		Host range	192.168.0.33-
			192.168.0.46
		Broadcast address	192.168.0.47
		total IP addresses	14
RECEPCION Y TECNICOS	4	Network	192.168.0.48
		Bitmask	28
		Netmask	255.255.255.240
		Wildcardmask	0.0.0.15

		Host range	192.168.0.49-
			192.168.0.62
		Broadcast address	192.168.0.63
		total IP addresses	14
DRIVE TEST	3	Network	192.168.0.64
		Bitmask	29
		Netmask	255.255.255.248
		Wildcardmask	0.0.0.7
		Host range	192.168.0.65-
			192.168.0.70
		Broadcast address	192.168.0.71
		total IP addresses	6
TERCERIZACION	3	Network	192.168.0.72
		Bitmask	29
		Netmask	255.255.255.248
		Wildcardmask	0.0.0.7
		Host range	192.168.0.73-
			192.168.0.78
		Broadcast address	192.168.0.79
		total IP addresses	6
GERENCIA	2	Network	192.168.0.80
		Bitmask	29
		Netmask	255.255.255.248
		Wildcardmask	0.0.0.7
		Host range	192.168.0.81-
			192.168.0.86
		Broadcast address	192.168.0.87
		total IP addresses	6

- Direccionamiento sede de Santiago de Cali.

En la sede principal se encuentra el core de la compañía, y la segmentamos en las diferentes áreas las cuales discriminamos en la tabla 4.

Tabla 6. Direccionamiento sede Cali

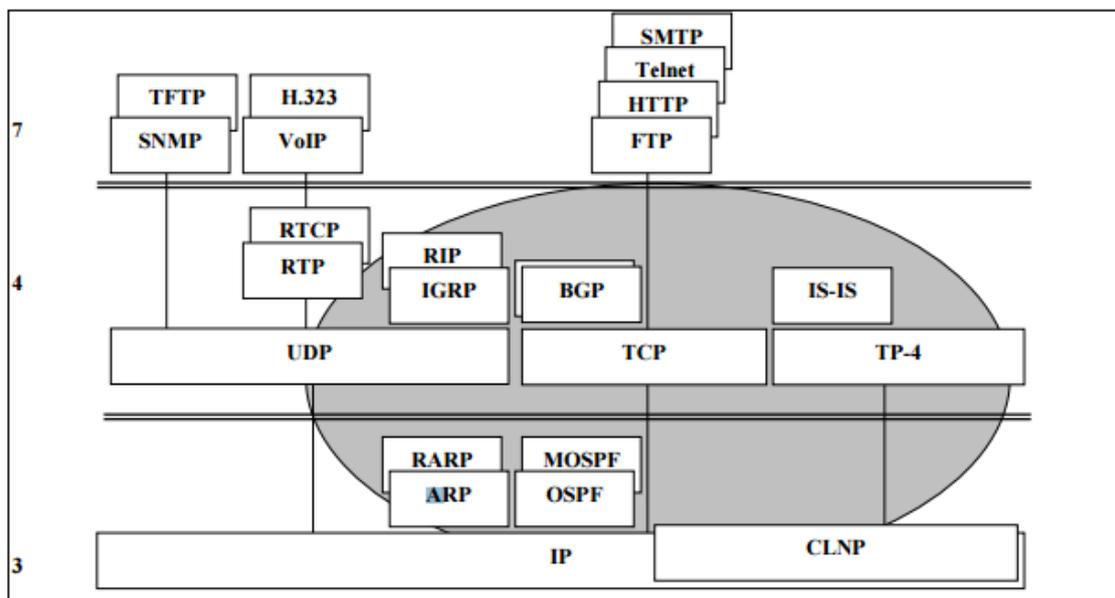
DIRECCIONAMIENTO IP SEGMENTADO SEDE CALI			
CAMARAS	4	Network	192.168.0.0
		Bitmask	29
		Netmask	255.255.255.248
		Wildcardmask	0.0.0.7
		Host range	192.168.0.1-
			192.168.0.6
		Broadcast address	192.168.0.7
total IP addresses	6		
TELFONIA IP	3	Network	192.168.0.8
		Bitmask	29
		Netmask	255.255.255.248
		Wildcardmask	0.0.0.7
		Host range	192.168.0.9-
			192.168.0.14
		Broadcast address	192.168.0.15
total IP addresses	6		
COMPUTADPORES	3	Network	192.168.0.16
		Bitmask	29
		Netmask	255.255.255.248
		Wildcardmask	0.0.0.7
		Host range	192.168.0.17-
			192.168.0.22
		Broadcast address	192.168.0.23
total IP addresses	6		
IMPRESORA	2	Network	192.168.0.24
		Bitmask	30
		Netmask	255.255.255.252

	Wildcardmask	0.0.0.3
	Host range	192.168.0.25-
		192.168.0.26
	Broadcast address	192.168.0.27
	total IP addresses	2

3.4.3. Selección de protocolos.

A continuación ilustramos los protocolos a utilizar en la red.

Figura 17. Selección de Protocolos de Switching y Routing



http://www.spw.cl/08oct06_ra/doc/REDES%20WAN%20IP-ATM/ProtocolosderoutingenIP.pdf

3.4.4. Desarrollo de estrategias de seguridad de la red.

La magnitud y nivel requerido de seguridad en un sistema de red depende del tipo de entorno en el que trabaja la red, en general la seguridad en una red requiere establecer un conjunto de reglas, regulaciones y políticas que no dejan nada al azar. El primer paso para garantizar la seguridad de los datos es implementar las políticas que establecen los matices de la seguridad y ayudan al administrador y a los usuarios a actuar cuando se producen modificaciones, esperadas como no planificadas, en el desarrollo de la red.

3.4.4.1. Autenticación y dominio.

En un ambiente de dominio, hay uno o más “servers” que cumplen la función de Controladores de Dominio, una de cuyas funciones principales es Autenticar.

Algo que habrán notado seguramente, es que con los sistemas operativos actuales como clientes, hay que crear una cuenta de máquina en el dominio, inclusive con los servidores miembros. Los equipos tienen cuenta en el dominio, se autentican durante el proceso de inicio, a partir de lo cual se arma un canal seguro de comunicación que servirá para el transporte de las credenciales de autenticación de los usuarios que accedan a los recursos del mismo.

3.4.4.2. Equipamiento de seguridad.

El mantenimiento de la seguridad de los datos es proporcionar seguridad física para el hardware de la red. La magnitud de la seguridad requerida depende de:

- El tamaño de la empresa.
- La importancia de los datos.
- Los recursos disponibles.

Al tener una topología de estrella, que es un gran sistema centralizado, la seguridad en los servidores debe de ser garantizada, contra amenazas accidentales o deliberadas. Se creara un data center con lo cual la parte física debe de tener un nivel básico de seguridad y acceso restringido.

3.4.4.3. Seguridad lógica.

Para garantizar la seguridad perimetral de la parte lógica de la red se instalaran cortafuego (firewalls) es un sistema de seguridad, normalmente una combinación de hardware y software, que está destinado a proteger la red de una organización frente a amenazas externas que proceden de otra red, incluyendo Internet.

Se instalara un anti-virus el cual protegerá la red de amenazas internas de la red.

3.4.5. Fase de Diseño Físico.

Figura 18. Diseño físico planta baja sede principal.

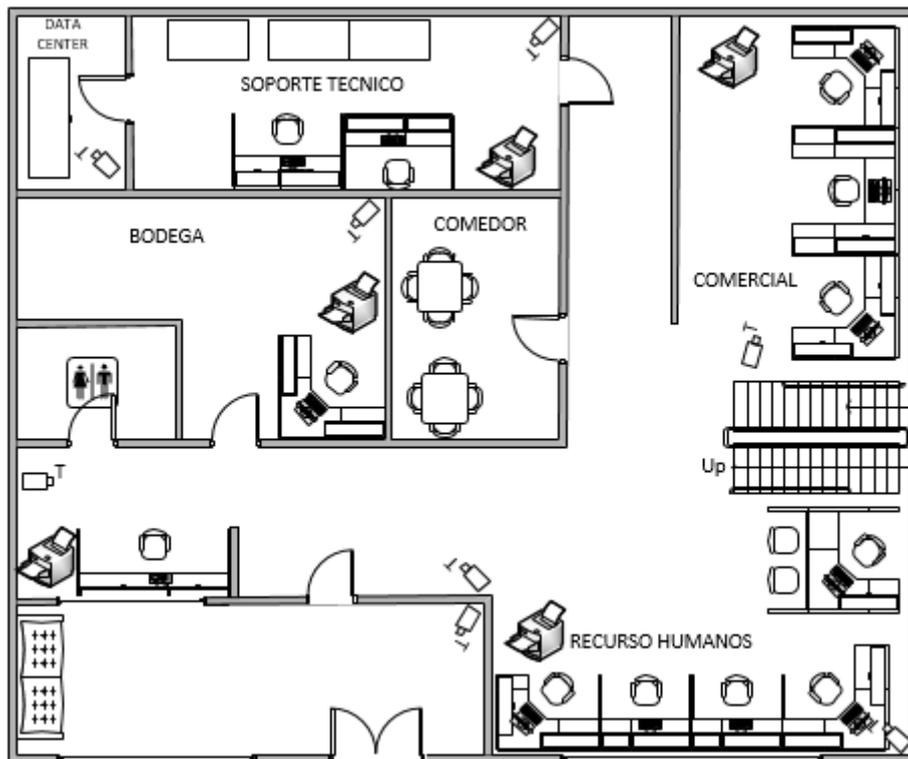


Figura 19. Diseño físico planta alta sede principal

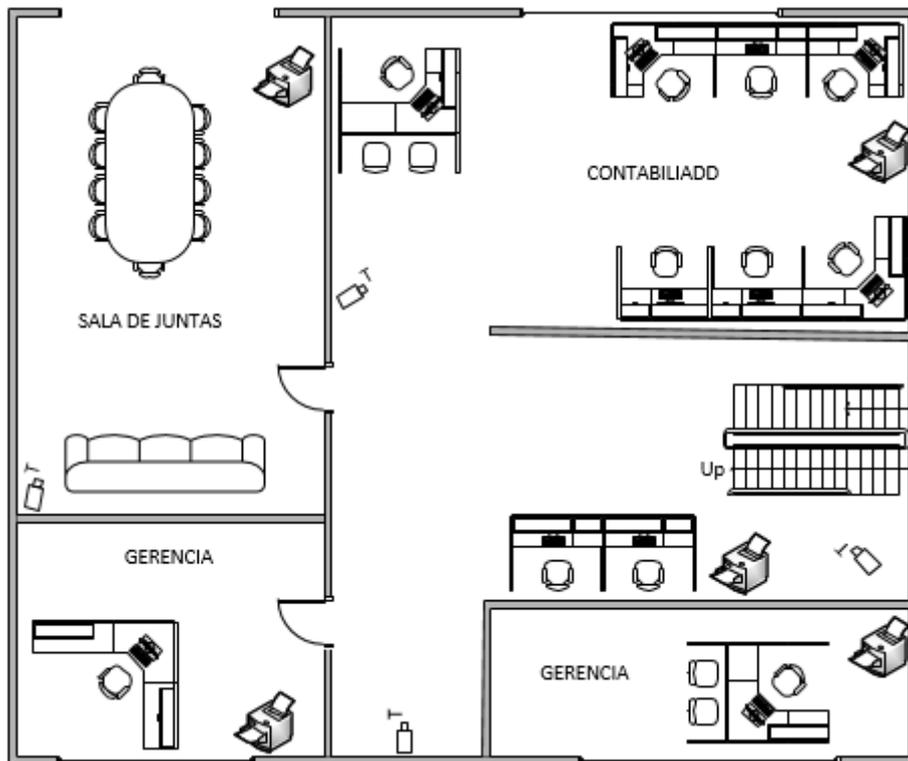


Figura 20. Cableado planta baja sede principal

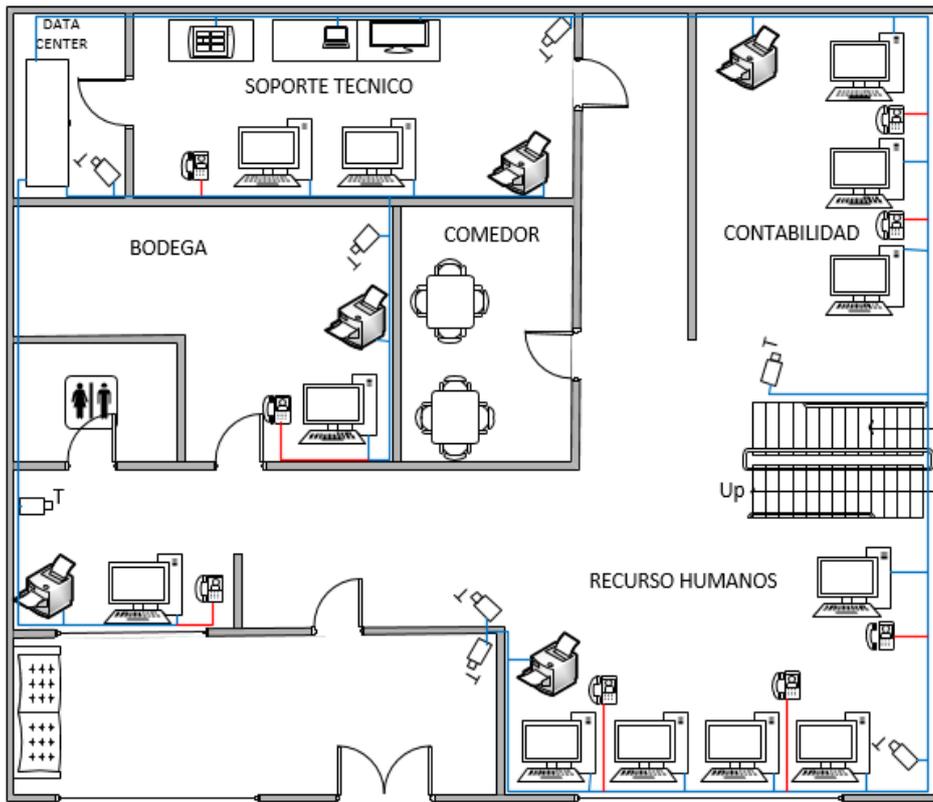


Figura 21. Cableado planta alta sede principal

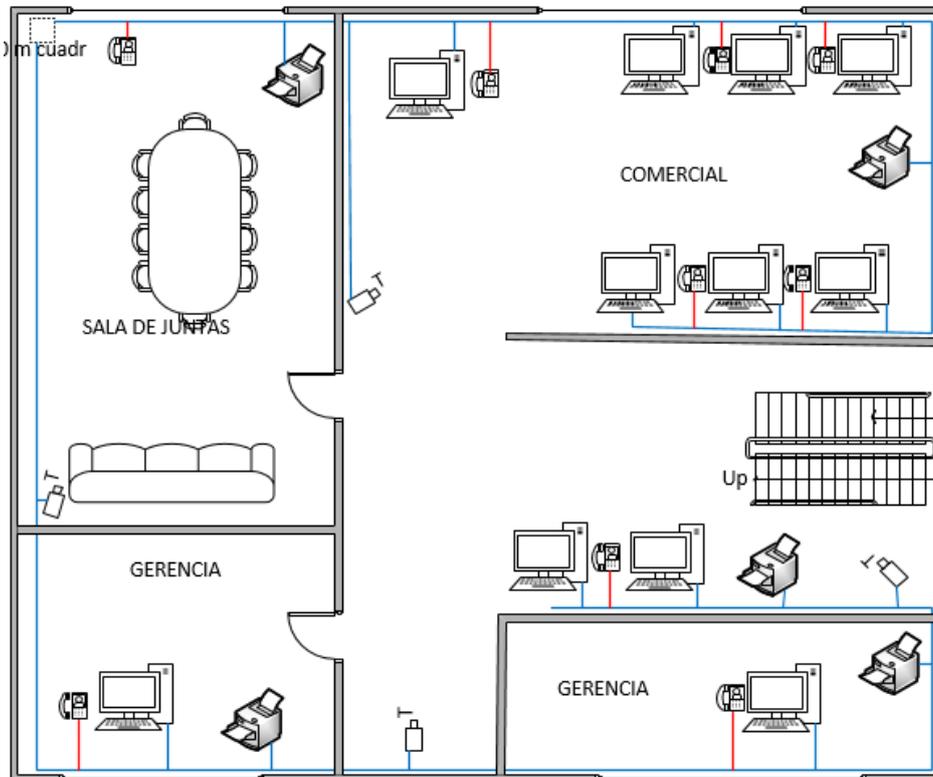


Figura 22. Diseño físico planta baja sede ingeniería

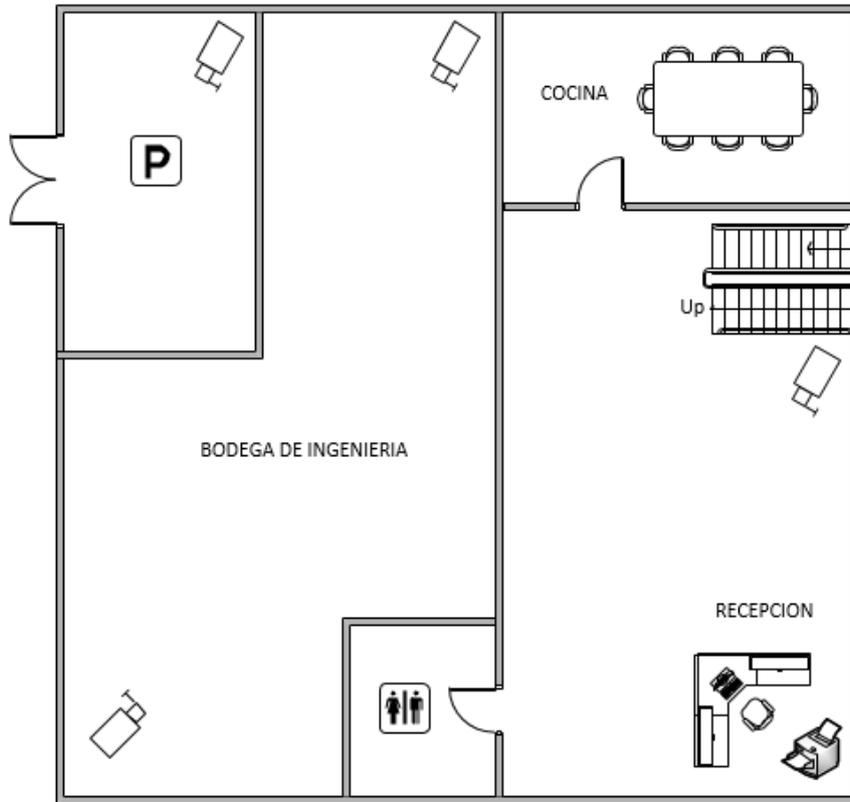


Figura 23. Diseño físico planta media sede ingeniería

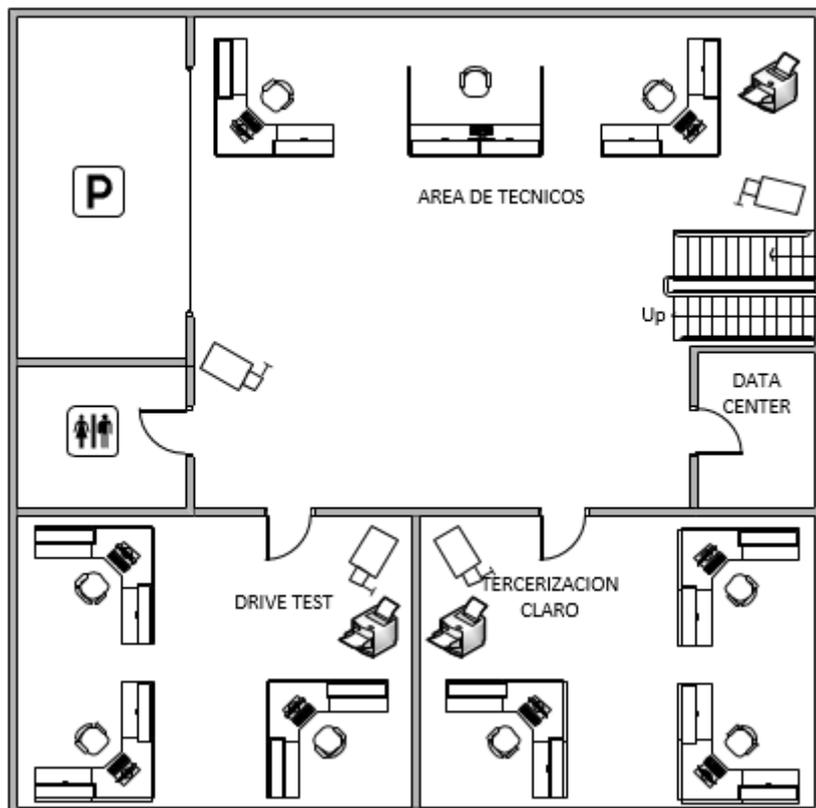


Figura 24. Diseño físico planta alta sede ingeniería

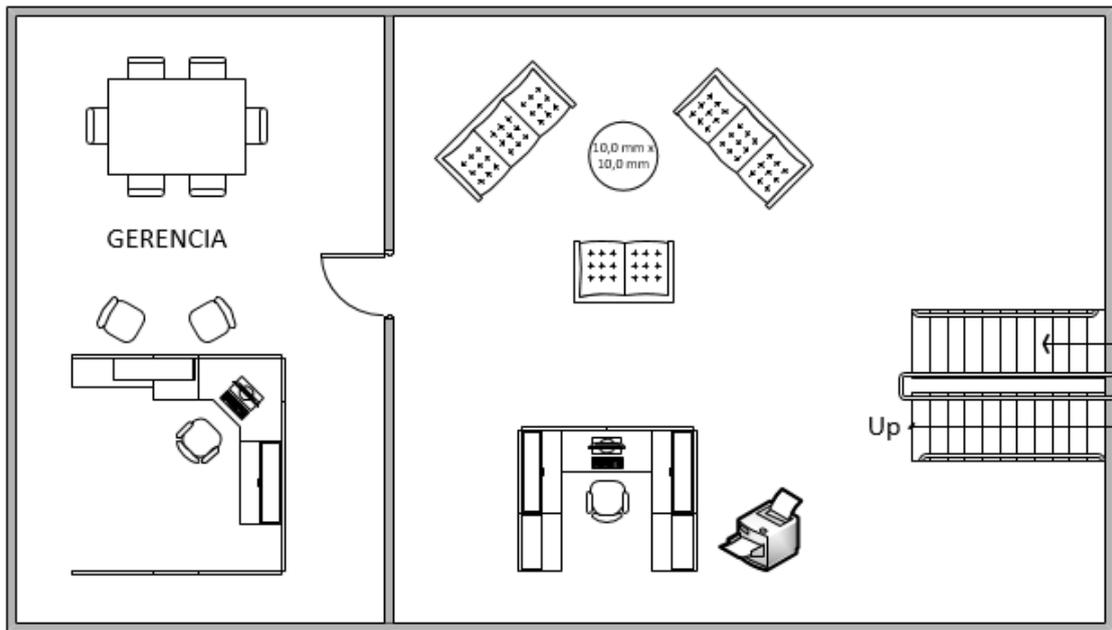


Figura 25. Diseño red planta baja sede ingeniería

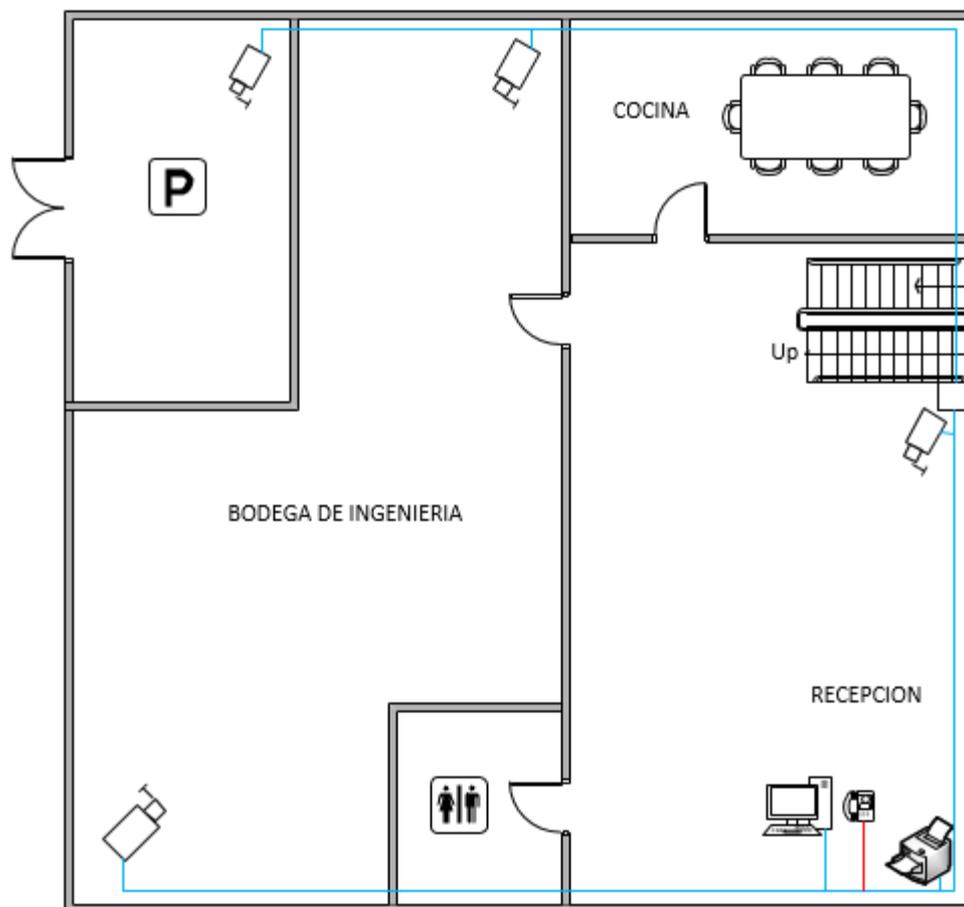


Figura 26. Diseño red planta media sede ingeniería

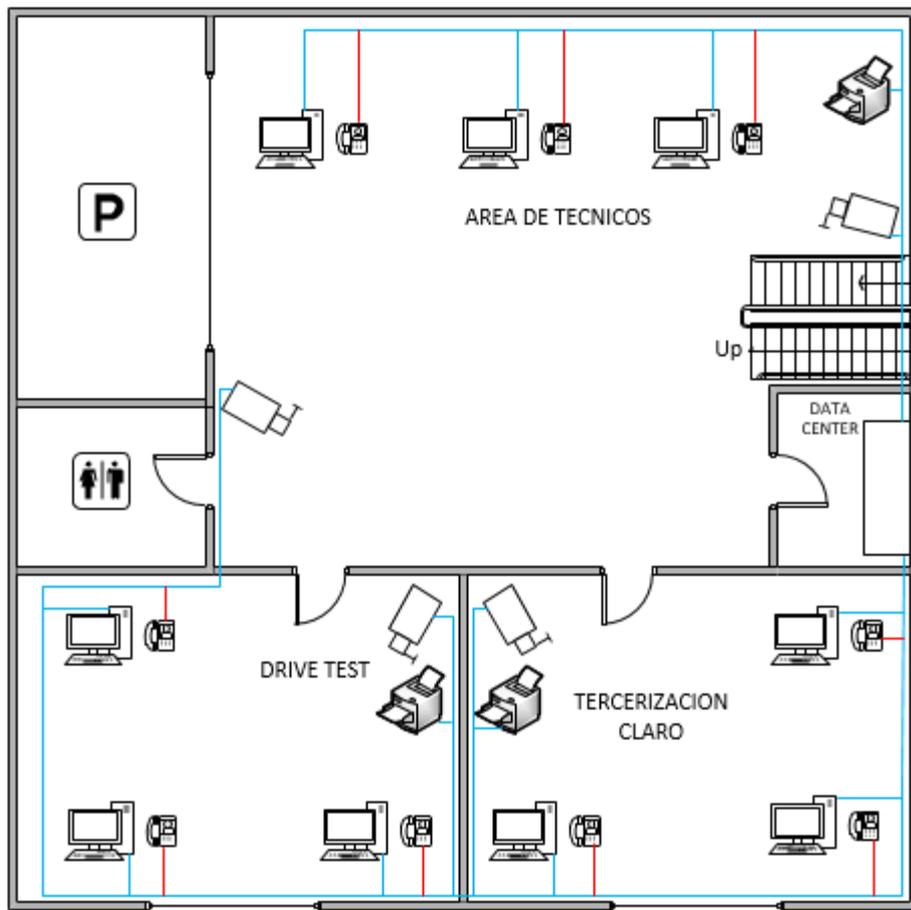


Figura 27. Diseño red planta alta sede ingeniería

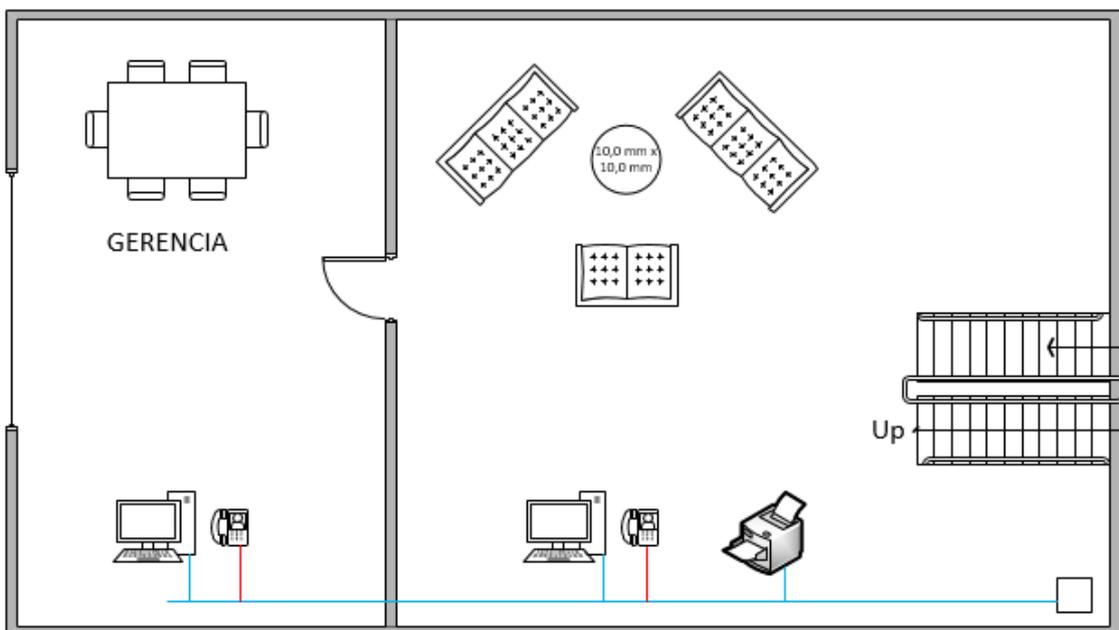


Figura 28. Diseño físico sede Cali

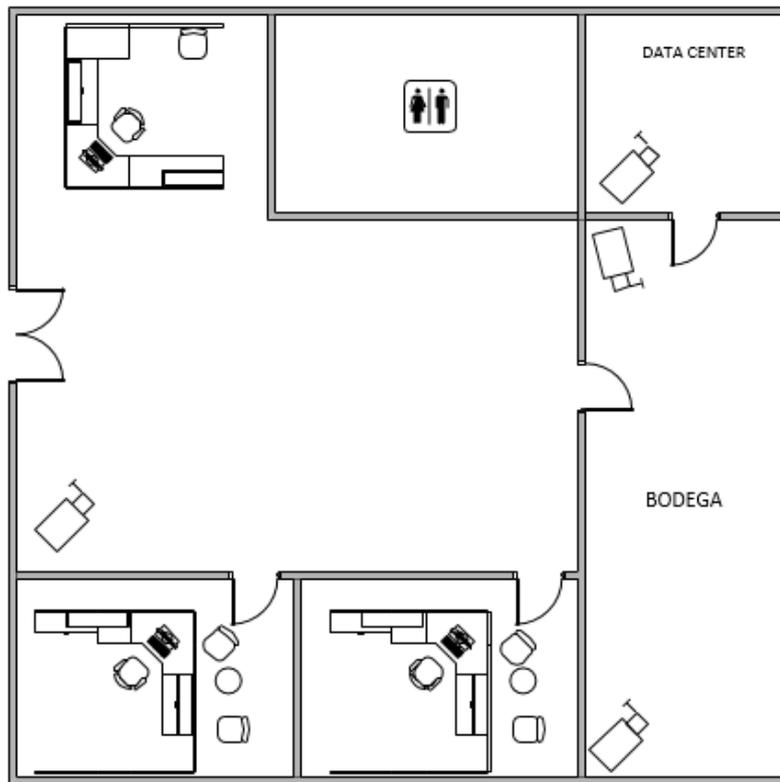
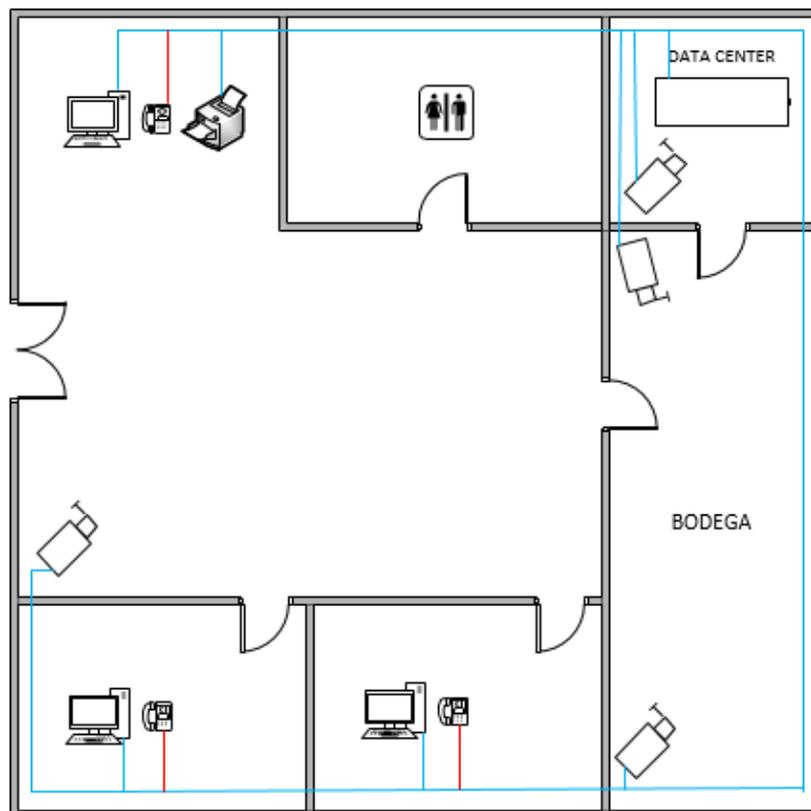


Figura 29. Diseño red sede Cali



Conclusiones.

El proyecto que realice ha contribuido de manera muy importante para identificar y resaltar los puntos que hay que cubrir y considerar para llevar a cabo una implementación exitosa de las tecnologías en TI. Nos deja muchas cosas importantes que reflexionar y muchas otras las ha reforzado como puntos angulares para llevar a cabo una buena implementación.

Dentro de los puntos considerados tienen más importancia dentro de un proyecto de esta naturaleza el detectar cuáles son las necesidades reales de las personas que trabajan día a día con los sistemas, que los procesos operativos de una empresa, definiendo la causa real del problema, y de esta forma aclarar los beneficios económicos, laborales y operativos que se pretenden alcanzar con la implementación de un sistema nuevo, de manera que las personas dentro de la empresa sepan cómo se verán beneficiadas.

Para llevar a cabo un proyecto como este al máximo de su aplicación, se deberá capacitar a los usuarios de los nuevos sistemas, si hacemos todo correctamente para desarrollar e implementar los sistemas pero no le damos herramientas a la gente para que trabaje con ellas es muy probable que todo el trabajo realizado se venga abajo y encuentren la manera de realizar sus tareas sin usarlas; haciendo que todos los beneficios que se tenían en mente no solo no se cumplan sino que tal vez empeoren.

Esta experiencia ha mostrado cómo es posible diseñar y aplicar un aprendizaje basado en la práctica y conocimiento, con el fin de servirse de todas las herramientas para solucionar problemas, no solo en las TI, si no en varios aspectos del ámbito personal y laboral.

Bibliografía.

HUIDOBRO MOYA, JOSÉ MANUEL. TELECOMUNICACIONES. TECNOLOGÍAS, REDES Y SERVICIOS. 2ª EDICIÓN ACTUALIZADA. RA-MA EDITORIAL. 2014.

ARIGANELLO ARIGANELLO, ERNESTO. REDES CISCO. GUÍA DE ESTUDIO PARA LA CERTIFICACIÓN CCNA ROUTING Y SWITCHING. RA-MA EDITORIAL. 2014.

Evelio Martínez Martínez & Arturo Serrano Santoyo. FUNDAMENTOS DE TELECOMUNICACIONES Y REDES. COVER GENTE. 2013.

Infografía.

- [1]. <http://informatechgroup.com/portada/images/stories/servicios/servidor-archivos.jpg> 11-10-2015
- [2]. <https://solucionesinformaticas2011.files.wordpress.com/2011/06/esquema-impresoras.png> 11-10-2015
- [3]. <http://s.culturacion.com/wp-content/uploads/2010/11/servidor-de-correo-D1.jpg> 11-10-2015
- [4]. <http://portallinux.es/wp-content/uploads/2015/08/IntroDHCP1.png> 11-10-2015
- [5]. <http://portallinux.es/wp-content/uploads/2015/08/Introproxi.png> 11-10-2015
- [6]. <https://servidores1191.files.wordpress.com/2013/09/internet.jpg> 11-10-2015
- [7]. <http://www.securityartwork.es/wp-content/uploads/2013/12/radius.jpg> 11-10-2015
- [8]. <http://www.dnsgratis.es/servidor-DNS.png> 11-10-2015
- [9]. http://images.quebarato.cl/T440x/telefonía+ip+servidores+ip+bases+enrutadoras+santiago+metropolitana+de+santiago+chile__2D1F0C_1.jpg 11-10-2015
- [10]. http://www.gestioip.net/cgi-bin/subnet_calculator.cgi 11-10-2015