



**UNIVERSIDAD CENTRAL DE VENEZUELA  
FACULTAD DE INGENIERÍA  
ESCUELA DE INGENIERÍA ELÉCTRICA**



**ACTUALIZACIÓN DE LA INFRAESTRUCTURA  
TECNOLÓGICA Y DISEÑO E IMPLANTACIÓN DE LA  
PLATAFORMA DE SEGURIDAD PARA EL CENTRO DE  
ESTUDIOS DE UNA EMPRESA DE TELECOMUNICACIONES**

Trabajo Especial de Grado para Optar al Título de  
Especialista en Telecomunicaciones y Redes de Comunicación de Datos

**Autor:**

Ing. VILLEGAS, Oscar D.

**Tutor:**

**Prof. Vincenzo Mendillo**

Caracas, Diciembre de 2007

## **DEDICATORIA**

A Dios Todopoderoso y la Santísima Virgen María, por ayudarme, iluminarme y guiarme por el camino del bien.

A la memoria de mi abuela Teresa y mi tía Paula, quienes físicamente no están a mi lado, pero que en su vida supieron darme amor y comprensión. Desde donde Dios las tenga sus espíritus me acompañan, protegen y guían mis pasos. A ustedes les dedico este triunfo.

A mis padres, Lucila y Oscar, por darme la vida y estar conmigo en todo momento, por apoyarme incondicionalmente y confiar en mí, por demostrarme que el trabajo y la dedicación traen consigo muchas satisfacciones. Este triunfo también es de ustedes.

A mis hijos: Osdary Carolina y Oscar Alejandro, por ser las personas más importantes en mi vida, por darme la fuerza que me impulsa a seguir adelante, a ustedes les dedico este triunfo.

A mi esposa Raidy Carolina, por todo estos años de amor y amistad que llevamos juntos, por ser paciente conmigo, por entenderme, a tí mujer que has sabido quererme, comprenderme y amarme, este triunfo no es mío sino nuestro. Te amo.

A mis hermanos María Alejandra, José Luis y mis sobrinos Mariagny y Germán, espero que mis logros sean una fuente de inspiración para ustedes, y que logren todas sus metas y objetivos.

**Oscar Darío Villegas.**

## **AGRADECIMIENTOS**

A Dios Todopoderoso, fuente de sabiduría y guía incondicional de mis pasos.

A mis padres, por inculcar en mí valores de ética, disciplina, constancia y perseverancia, para llevar a cabo mis sueños.

A la Universidad Central de Venezuela, casa de estudios que nos acogió y sembró en nosotros la sabiduría y el deseo de superación para lograr nuestra meta. Así mismo, a nuestros profesores por transmitirnos sus conocimientos y hacer de nosotros los profesionales que hoy somos.

Al profesor Ingeniero Vincenzo Mendillo, quien con su experiencia y orientación, me guió por el mejor camino a seguir para la culminar con éxito el Trabajo Especial de Grado.

**Oscar Darío Villegas.**

**UNIVERSIDAD CENTRAL DE VENEZUELA  
FACULTAD DE INGENIERÍA  
ESCUELA DE INGENIERÍA ELÉCTRICA**

**POSTGRADO EN ESPECIALIZACIÓN EN COMUNICACIONES Y REDES  
DE COMUNICACIÓN DE DATOS**

**ACTUALIZACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA Y  
DISEÑO E IMPLANTACIÓN DE LA PLATAFORMA DE SEGURIDAD  
PARA EL CENTRO DE ESTUDIOS DE UNA EMPRESA DE  
TELECOMUNICACIONES**

**Autor:** Ing. Oscar Villegas   **Tutor:** Prof. Vincenzo Mendillo  
Octubre de 2007

**RESUMEN**

El objetivo fundamental del presente Trabajo Especial de Grado es diseñar e implantar un esquema de actualización tecnológica que incluye la red de área local así como el esquema de seguridad, los cuales permitirán mejorar el desempeño de la red, garantizar su disponibilidad y satisfacer la creciente demanda de servicios y recursos, mejorando la seguridad de la información y los tiempos de respuesta de las aplicaciones que apoyan los procesos del negocio de las distintas unidades que conforman el Centro de Estudios de Telecomunicaciones de la Corporación en estudio.

Para la actualización de la infraestructura tecnológica se esbozaron varias soluciones, tales como: la sustitución de equipos de comunicación (*router, hubs, switches*), creación y administración de redes virtuales (VLAN); instalación de cámaras de seguridad, diseño y desarrollo del sitio Web del Centro de Estudios e incorporación de la red LAN al sistema de monitoreo del centro de operaciones de la red.

## ÍNDICE GENERAL

	<u>Pág.</u>
Dedicatoria.....	II
Agradecimientos.....	III
Resumen.....	IV
Índice general.....	V
Índice de anexos.....	IX
Índice de figuras.....	X
Índice de tablas.....	XII
Introducción.....	1
<b>CAPÍTULO I: EL PROBLEMA DE INVESTIGACIÓN</b>	
Planteamiento del problema.....	4
Objetivo general.....	6
Objetivos específicos.....	7
Justificación.....	8
Alcance.....	9
Limitaciones.....	10
Estudio de factibilidad.....	11
<b>CAPÍTULO II: MARCO TEÓRICO</b>	
Antecedentes de la investigación.....	13
Bases teóricas.....	14
Definición general de una red de datos.....	14
Clasificación de las redes.....	14
Redes LAN.....	14
Redes WAN.....	15
Redes MAN.....	15

Topología de red.....	15
Topología física.....	15
Topología estrella.....	16
Topología bus.....	16
Topología anillo.....	17
Topología lógica.....	18
Componentes de una red.....	18
Sistema de cableado.....	18
Servidores de red.....	18
Servidores dedicados.....	18
Servidores no dedicados.....	18
Clientes de la red.....	18
Tarjetas de red.....	18
Sistema operativo de red (NOS).....	18
Shell.....	18
Equipos de red.....	18
Hub.....	18
Switch.....	18
Router (enrutador).....	18
Patch panels.....	18
El modelo OSI.....	18
Estándares de red usados.....	20
VLAN: red de área local virtual.....	20
Segmentación.....	22
Tipos de VLAN.....	23
VLAN por puerto.....	23
Ventajas – desventajas.....	23
VLAN por dirección MAC.....	24

Ventajas – desventajas.....	24
VLAN por protocolo.....	24
Ventajas – desventajas.....	25
VLAN por direcciones IP.....	25
Ventajas – desventajas.....	25
VLAN dinámicas (DVLAN).....	26
Pertenencia a una VLAN.....	26
Etiquetado de VLAN.....	26
Protocolo de compartición para VLAN.....	27
Modos VTP.....	28
Cableado estructurado.....	29
Normas y estándares.....	29
Definición de la estructura de los sistemas de cableado.....	30
Cableado horizontal.....	30
Cableado vertical.....	34
Área de trabajo.....	36
Cuarto de telecomunicaciones.....	38
Armario de telecomunicaciones.....	41
Cuarto de equipos.....	43
¿Qué es la seguridad de la información?.....	44
Objetivo de la seguridad.....	45
Aspectos en la seguridad informática.....	45
La seguridad física.....	48
La seguridad lógica o técnica.....	48
<b>CAPÍTULO III: METODOLOGÍA</b>	
Metodología.....	50
Fases tomadas en consideración para el desarrollo del proyecto.....	51

Fase 1: fase de exploración o análisis del proyecto.....	51
Fase 2: diseño de la solución propuesta.....	51
Fase 3: instalación y pruebas.....	52
Fase 4: web site del centro de estudios.....	52
<b>CAPÍTULO IV: DESARROLLO DEL PROYECTO</b>	
Presentación y análisis de los resultados.....	55
Desarrollo de la fase 1.....	55
Situación actual.....	55
Definición de requerimientos.....	67
Desarrollo de la fase 2.....	68
Diseño.....	68
Adquisición de la solución.....	86
Desarrollo de la fase 3.....	87
Instalación y pruebas.....	87
Desarrollo de la fase 4.....	108
Análisis.....	108
Diseño.....	112
Desarrollo.....	119
Implantación.....	120
<b>CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES</b>	
Conclusiones.....	121
Recomendaciones.....	123
<b>BIBLIOGRAFÍA.....</b>	125
<b>ANEXOS.....</b>	127
<b>GLOSARIO.....</b>	128

## ÍNDICE DE ANEXOS

	<u>Anexo N°.</u>
Plano de equipos planta baja.....	Anexo 1
Plano de equipos piso 1.....	Anexo 2
Plano de equipos piso 2.....	Anexo 3
Plano cableado planta baja.....	Anexo 4
Plano cableado piso 1.....	Anexo 5
Plano cableado piso 2.....	Anexo 6
Ejemplo comentario cableado piso 2.....	Anexo 7
Ejemplo características pc piso 1.....	Anexo 8
Ejemplo resumen puntos de red piso 2.....	Anexo 9
Ejemplo de disponibilidad de puertos switch n° 1 del piso 2.....	Anexo 10
Cámara de vigilancia instalada en el edificio Jan Deketh.....	Anexo 11
Cámara de vigilancia instalada en la entrada principal del edificio Jan Deketh.....	Anexo 12
Cámara de vigilancia instalada en la sotea del edificio Arvelo.....	Anexo 13
Cámara de vigilancia instalada en el piso 2 del edificio Jan Deketh.....	Anexo 14
Cámara de vigilancia instalada en el piso 2 del edificio Jan Deketh.....	Anexo 15
Cámara de vigilancia instalada en el piso 2 del edificio Jan Deketh.....	Anexo 16
Cámara de vigilancia instalada en el piso 2 del edificio Jan Deketh.....	Anexo 17
Vista página Principal.....	Anexo 18
Vista página Información General.....	Anexo 19
Vista página Conocimientos.....	Anexo 20
Vista página Competencias.....	Anexo 21
Vista página Preguntas Frecuentes.....	Anexo 22
Vista página Postulación.....	Anexo 23
Vista página Atención Total.....	Anexo 24

## ÍNDICE DE FIGURAS

	<u>Pág.</u>
Figura II.1. Esquema general de red.....	14
Figura II.2. Topología estrella.....	16
Figura II.3. Topología de bus.....	17
Figura II.4. Topología de anillo.....	17
Figura II.5. LAN tradicional.....	21
Figura II.6. VLAN.....	21
Figura II.7. Diagrama de cableado horizontal.....	31
Figura II.8. Diagrama de cableado vertical.....	35
Figura II.9. Área de trabajo.....	37
Figura II.10. Configuración común área de trabajo.....	38
Figura II.11. Armario de telecomunicaciones.....	42
Figura IV.1. Esquema de red LAN actual del Centro de Estudios de Telecomunicaciones.....	57
Figura IV.2. Cisco Switch Catalyst serie 2950.....	71
Figura IV.3. Cisco Router 1841.....	71
Figura IV.4. Cisco Switch Catalyst serie 3550.....	73
Figura IV.5. Esquema de conexión propuesto para la red LAN del Centro de Estudios de Telecomunicaciones.....	73
Figura IV.6. Esquema de conexión de VLAN.....	75
Figura IV.7. Esquema de conexión del sistema de cámaras de vigilancia.....	78
Figura IV.8. Ubicación de cámaras entrada edificio Arvelo planta baja..	81
Figura IV.9. Ubicación de cámaras entrada edificio Arvelo planta alta..	82
Figura IV.10. Ubicación de cámaras edificio Arvelo azotea 1.....	82
Figura IV.11. Ubicación de cámaras edificio Arvelo azotea 2.....	83
Figura IV.12. Ubicación de cámaras edificio Jan Deketh piso 2.....	84

Figura IV.13. Ubicación de cámaras edificio Jan Deketh piso 1.....	85
Figura IV.14. Ubicación de cámaras edificio Jan Deketh planta baja.....	86
Figura IV.15. Armario de telecomunicaciones principal.....	88
Figura IV.16. Configuración predeterminada para la consola. Hyper Terminal.....	91
Figura IV.17. Configuración de puertos a una VLAN – 1.....	96
Figura IV.18. Configuración de puertos a una VLAN – 2.....	97
Figura IV.19. Configuración de puertos a una VLAN – 3.....	97
Figura IV.20. Servidor de video N° 1 instalado.....	105
Figura IV.21. Incorporación de servidores al Cammanager.....	106
Figura IV.22. Asignación de dirección IP.....	106
Figura IV.23. Canales de frecuencia.....	107
Figura IV.24. Configuración de la opción de backup.....	107
Figura IV.25. Estructura física empleada para el diseño de la Aplicación Web del Centro de Estudios de Telecomunicaciones.....	113
Figura IV.26. Estructura física de la aplicación Web detallando la división estratégica de la página.....	114
Figura IV.27. Diagrama general del sitio Web del Centro de Estudios de Telecomunicaciones.....	115
Figura IV.28. Imágenes en ambiente Corel Draw. 12.....	118
Figura IV.29. Ambiente de trabajo Microsoft FrontPage 2003 en modo código.....	120

## ÍNDICE DE TABLAS

<b>N° de Tabla / Descripción</b>	<b><u>Pág.</u></b>
II.1: VLAN por puerto.....	23
II.2: VLAN por dirección MAC.....	24
II.3: VLAN por protocolo.....	25
IV.1: Características red LAN del Centro de Estudios de Telecomunicaciones.....	56
IV.2: Configuración IBM ThinkCentre MT-M 8141-27S.....	58
IV.3: Configuración IBM ThinkCentre MT-M 8188-37S.....	58
IV.4: Software utilizado en las estaciones de trabajo.....	59
IV.5: Características impresoras de red.....	61
IV.6: Características técnicas Cisco Catalyst 2950.....	69
IV.7: Características técnicas Cisco Catalyst 3550.....	70
IV.8: Características técnicas Cisco Router 1841.....	72
IV.9: Características y cantidad de cámaras de seguridad adquiridas.....	80
IV.10: Requerimientos de hardware.....	111

## INTRODUCCIÓN

Las telecomunicaciones ya tienen más de 100 años. Durante este período, su evolución ha sido asombrosa: las redes telefónicas y las redes de datos se han extendido rápidamente sobre todo el globo y los enlaces se han multiplicado utilizando toda una gama de técnicas de transmisión que la ingeniería ha ido perfeccionando. Las redes de telecomunicaciones se han desarrollado para facilitar el intercambio de información entre puntos separados físicamente y las redes actuales son el fruto de una continua evolución impulsada por los progresos en el campo de la ciencia y la tecnología.

La actualización de los componentes de red (dispositivos, cableado, conectores, entre otros) e incorporación de nuevas tecnologías en una red interna que ya existe dentro de una empresa, permite que los usuarios interactúen, compartan información y recursos, aprovechando las ventajas tecnológicas que éstas tecnologías ofrecen. Esta interacción supone una reconciliación con mundos dispersos: sistemas de información y bases de datos (sistemas de compras, finanzas), documentación técnica (planos, *software*, etc), comunicación (correo electrónico, revistas, publicación, entre otros).

El auge de Internet, el avance de las telecomunicaciones y en el hardware de los computadores han sido importante en los últimos años, abriendo una gran puerta de comunicación que permite a cualquier usuario realizar todo tipo de transacciones en forma remota sin desplazarse de un sitio a otro. Esto no ha sido positivo del todo, debido a que esta gran puerta de comunicación ha quedado abierta también para todo tipo de personajes encargados de buscar fallas en los sistemas de información y aprovechándose de ellos para conseguir información clave de personas y empresas que les pueda causar algún tipo de beneficio. Debido a esto, las empresas a nivel

mundial han centrado sus esfuerzos al fortalecimiento de la seguridad en sus redes internas a través de la incorporación de planes, mecanismos y políticas de seguridad que mitiguen el riesgo de ataques y vulnerabilidades en sus sistemas y redes.

Actualmente existen dos elementos que incrementan la importancia de brindar una adecuada seguridad a la información corporativa por parte de las empresas: la importancia creciente de la información para las empresas y el aumento de los riesgos a la que la misma se ve expuesta. Las empresas pueden llegar a triunfar o morir solamente por la información que manejan, lo que ha llevado a que ésta sea considerada un activo cada vez más valioso, aún cuando no podemos llegar a cuantificarlo adecuadamente.

Esta apertura así como nuevas oportunidades de negocios, mayor eficiencia a las operaciones y/o menos costos de transacción, genera nuevos y más complejos riesgos que se deben mitigar, o por lo menos considerar. También las empresas hoy día manejan información de terceros, por lo tanto, no sólo debe lograr procesar la misma de una manera segura, para impedir pérdida de imagen y/o acciones legales en su contra, sino que la falta de seguridad o la apariencia de ella pueden actuar como un impedimento para concretar negocios.

La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que ellos van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior de la organización ya que estadísticamente se ha demostrado, que la amenaza más importante para nuestros datos, la encontramos dentro de la empresa.

El presente Trabajo Especial de Grado constituye una propuesta para la empresa en estudio, ya que requiere de la actualización tecnológica de su plataforma de red, así como el diseño e implantación de mecanismos de seguridad que garanticen una mayor efectividad y eficiencia en sus procesos. Dicha empresa es un espacio abierto a la innovación e investigación para el mejoramiento técnico, empresarial y del negocio de los empleados que forman parte de la misma. Para ello, se llevan a cabo acciones de formación que apuntan a los objetivos estratégicos de la empresa apoyándose en prototipos tecnológicos.

El presente proyecto está constituido por 5 capítulos, que fueron abordados de manera independiente y que presentan la siguiente estructura:

Capítulo I **Planteamiento del Problema;** se describe el problema de investigación, se establece el objetivo general y los objetivos específicos, además de la justificación y la delimitación.

Capítulo II **Marco Teórico;** se presentan los antecedentes de la investigación, se describe la fundamentación.

Capítulo III **Marco Metodológico;** se describe la metodología utilizada para el desarrollo del proyecto.

Capítulo IV **Presentación y Análisis de los resultados;** Se desarrolla la metodología propuesta fase por fase, presentándose todos los datos recopilados para posteriormente realizar un análisis minucioso de cada resultado obtenido y presentar su interpretación.

Capítulo V **Conclusiones y Recomendaciones;** se presentan las conclusiones obtenidas, conjuntamente con las recomendaciones y anexos correspondientes.

# **CAPÍTULO I**

## **EL PROBLEMA DE INVESTIGACIÓN**

### **PLANTEAMIENTO DEL PROBLEMA**

En vista de las nuevas tendencias de globalización que se presentan en la actualidad y ante la necesidad de proveer de herramientas contemporáneas y eficaces en la consecución de los niveles de desenvolvimiento tecnológico óptimos y adecuados que garanticen y promuevan el desarrollo de las organizaciones se ha hecho necesaria y patente la incorporación de las nuevas tecnologías de información que son representadas a través de la utilización de redes de comunicación. Estas se han convertido en uno de los principales medios de comunicación en la actualidad, por el enorme potencial que representan en el desenvolvimiento de actividades dentro de la sociedad globalizada y el acercamiento que nos permite tal instrumento computacional con los más lejanos ambientes de operaciones, además de colocar al alcance de nuestras manos una infinita cantidad de recursos de invalorable utilidad.

El Centro de Estudios de Telecomunicaciones de la Corporación en estudio, posee una infraestructura tecnológica, la cual presenta una serie de inconvenientes que deben ser solucionados de forma rápida y eficiente, para de esta manera mejorar la disponibilidad y calidad de los diferentes servicios y recursos que se ofrecen internamente, así como el resto de las unidades de la corporación que hacen uso de dicho Centro de Estudios para capacitar al personal en las tecnologías de datos, transmisión, conmutación, energía, red de acceso y sistemas de información.

Los problemas a considerar en la plataforma de redes son los siguientes:

- Demoras en los tiempos de respuesta de las aplicaciones que funcionan en red: salas de PC'S destinadas a la realización de cursos, en donde se simulan ambientes reales relacionados con los servicios que presta la corporación, servicio de correo electrónico, servicios de impresión, servicios web, sistema de gestión SAP R/3, sistemas de aplicaciones propietarias (SISE, Asap, Boss, Siase, Sir) de la organización destinados como ambientes de entrenamientos para el personal de la corporación que asiste a los cursos.
- Insatisfacción por parte de los usuarios en cuanto al tiempo de acceso para las aplicaciones de uso exclusivo para los diferentes cursos que se imparten en el Centro de Estudios de Telecomunicaciones.
- Aumento de la cantidad de computadores destinados a las salas de PC'S, distribuidos en la sede del Centro de Estudios, lo que ha incrementado el tráfico en la red.
- Desactualización de los hub's de la red de área local (LAN), los cuales poseen más de ocho años de uso, siendo obsoletos y sin capacidad de crear redes virtuales (VLAN) que ofrezcan mayor seguridad y descongestión de tráfico.
- Cableado horizontal con estaciones de trabajo funcionando a 10 Mbps y 100 Mbps y un cableado vertical (backbone) operando a 100 Mbps, lo cual representa un cuello de botella.
- Falta de documentación de la red LAN, por lo que es necesario la elaboración de un diagrama que identifique a todos los dispositivos que forman parte de la

red local, para de esta manera identificar más fácilmente cualquier componente que este presentando problemas.

- Falta de un sitio Web corporativo donde se publique información relacionada con el Centro de Estudios de Telecomunicaciones.

En cuanto a los problemas de seguridad se tienen los siguientes:

- No existencia de Redes Virtuales Privadas (VLAN), lo que representa un riesgo para la red local, puesto que el tráfico generado no se encuentra segmentado.
- Desactualización del router principal marca Cisco, serie 1700, el cual posee más de 7 años en uso y no dispone de soporte técnico por parte del proveedor.
- Falta de un sistema de vigilancia a través de cámaras lo cual ayudaría a disminuir los hurtos y garantizar mayor seguridad.

## **OBJETIVO GENERAL**

Actualizar la infraestructura tecnológica e implantar la plataforma de seguridad para el Centro de Estudios de una empresa de Telecomunicaciones, que permita mejorar la prestación de los servicios de red, garantizando su disponibilidad y satisfaciendo la creciente demanda de nuevos servicios, aplicaciones y recursos, mejorando de esta manera el desempeño de la red y los tiempos de respuesta de las aplicaciones que apoyan los procesos del negocio.

## **OBJETIVOS ESPECÍFICOS**

- Análisis de la infraestructura de red actual en el Centro de Estudios de Telecomunicaciones, para definir los límites y alcance que tendrá la actualización propuesta.
- Diseñar el nuevo modelo de red.
- Elaborar los diagramas de red (dispositivos, cableado, PC's).
- Instalar los equipos de red.
- Configurar las Redes Virtuales (VLAN).
- Diseñar el sistema de seguridad a través de cámaras de vigilancia.
- Instalar el sistema de seguridad a través de cámaras de vigilancia.
- Realizar pruebas de conexión de todos los equipos LAN.
- Desarrollar del sitio Web corporativo del Centro de Estudios de Telecomunicaciones.

## JUSTIFICACIÓN

El Centro de Estudios de Telecomunicaciones de la Corporación en estudio, es un espacio abierto a la innovación e investigación para el mejoramiento técnico, empresarial y del negocio del personal que forma parte de su recurso humano. Para ello, se llevan a cabo acciones de formación que apuntan a los objetivos estratégicos de la empresa, apoyándose en prototipos tecnológicos en las áreas de sistemas, datos, transmisión, energía, conmutación y red de acceso. Es por esto que para poder cumplir con las exigencias que sus funciones le confieren, el Centro de Estudios de Telecomunicaciones requiere de la actualización tecnológica de su plataforma de red, así como el diseño e implantación de mecanismos de seguridad que garanticen una mayor efectividad y eficiencia en sus procesos.

El Centro de Estudios de Telecomunicaciones presenta grandes necesidades en la actualización de su plataforma tecnológica existente, ya que existen una serie de aplicaciones que representan ambientes de pruebas reales relacionados con los servicios que presta la corporación, y que presentan graves problemas en sus tiempos de respuesta, ya que los mismos son muy lentos.

Por otro lado, se requiere la actualización de los dispositivos de comunicación de datos (*router, hub*, cableado, conectores, entre otros componentes), ya que con el incremento de las salas de PC'S, ha aumentado el tráfico de la red, lo cual no puede ser satisfecho con la plataforma de redes que se posee actualmente, además de ofrecer bajos parámetros de controles de seguridad.

No obstante, la no existencia de documentación relacionada con la estructura de la red de área local del Centro de Estudios, ocasiona inconvenientes a la hora de ubicar un dispositivo en la red que presenta fallas, por lo que el tiempo de respuesta

para la solución de la misma es más extenso, ocasionando retrasos en procesos. Adicionalmente la falta de instalación de un sistema de vigilancia a través de cámaras de seguridad en el Centro de Estudios facilita la acción de hurtos.

La actualización de la red permitirá la creación y administración de redes virtuales, ampliación de las zonas de seguridad de la red, mejora en los tiempos de respuestas de las aplicaciones, disponibilidad de recursos y servicios e implantación de un sistema de seguridad redundante.

Todo lo expuesto exige que en el Centro de Estudios de Telecomunicaciones se realice la actualización de la plataforma tecnológica y de seguridad de la red local, con el fin de mejorar una serie de funciones y procesos de comunicaciones en sus diferentes áreas, así como la obtención de resultados concretos, inmediatos y favorables para que de esta forma se logre dar cumplimiento a su misión.

## **ALCANCE**

El presente proyecto, se llevará a cabo únicamente en el Edificio Jan Deketh de la sede del Centro de Estudios de Telecomunicaciones ubicado en la ciudad de Caracas, durante el período comprendido entre Enero del 2007 y Septiembre del 2007. La estructura y diseño responderá a los requerimientos y necesidades que allí se determinen bajo un previo estudio.

## LIMITACIONES

- Por razones presupuestarias no se contrató una empresa especializada en realizar análisis de tráfico de red, antes y después de la actualización tecnológica, de forma tal de comprobar estadísticamente las mejoras en los tiempos de respuesta de las aplicaciones, por lo que en análisis de tráfico fue realizado internamente con aplicaciones de uso gratuito.
- Por razones de tiempo, no se pudo contratar a una empresa especializada en seguridad para la realización de un análisis de vulnerabilidades y riesgos que permitiera definir un modelo de seguridad mucho más ajustados a las necesidades del Centro de Estudios.
- No se pudo abarcar las otras dos sedes del Centro de Estudios, por problemas presupuestarios y de tiempo en la finalización del proyecto, por lo que se constituirá una segunda fase de actualización que abarque el resto de los edificios.
- La instalación y configuración de los equipos sólo pudo llevarse a cabo en días feriados, fines de semana o en horario no laboral, ya que la actualización de la red local y del esquema de seguridad afecta la prestación de los servicios.
- Por razones de presupuesto no fue posible contratar una empresa que efectuara la instalación de las cámaras de seguridad en el Centro de Estudios de Telecomunicaciones de la Corporación en estudio.

## **ESTUDIO DE FACTIBILIDAD**

Se realizó un estudio del diseño propuesto, determinándose que el mismo puede ofrecer factibilidad técnica, económica y operacional, en la ejecución de los procesos, dichos estudios de factibilidad son realizados con el propósito de saber en primer grado la capacidad que tiene la Corporación de aceptar el diseño propuesto basándose en las características propias del mismo, sabiendo que ofrecerá beneficios significativos al personal que labora en el Centro de Estudios de Telecomunicaciones de la Corporación en estudio. El estudio de factibilidad de este proyecto se apoya en tres principios básicos: técnica, económica y operacional.

### **Factibilidad Técnica:**

El Centro de Estudios de Telecomunicaciones de la Corporación en estudio, cuenta con la tecnología necesaria para el desarrollo e implantación del nuevo esquema propuesto, ya que los equipos están disponibles en el mercado, al igual que las plataformas computacionales básicas y necesarias para su eficiente elaboración. Estos equipos poseen la capacidad para llevar a cabo un procesamiento y almacenamiento de la información generada en el sistema de redes de datos que se propone. Por otro lado la plataforma propuesta ofrece un manejo adecuado a las exigencias internas.

### **Factibilidad Económica:**

La empresa cuenta con los recursos necesarios para respaldar económicamente el desarrollo del proyecto, con el cual se mejorará considerablemente la calidad y velocidad del servicio, así como ofrecer mayor seguridad a los usuarios que hacen

uso del Centro de Estudios por lo tanto el proyecto se considera económicamente factible.

### **Factibilidad Operativa:**

El diseño propuesto una vez concluido logrará satisfacer todas las expectativas de los usuarios en cuanto a la calidad y velocidad del servicio y reducirá el tiempo de acceso a las aplicaciones usadas para entrenamientos así como las usadas por el personal que labora en dicho Centro de Estudios. Por otro lado ofrecerá mayor seguridad en el desempeño de las funciones, tareas y servicios, mediante la reducción en los tiempos de procesos y el margen de error, y garantizando la eficiencia de las operaciones debido a que la información goza de un alto grado de seguridad y confiabilidad. Todas estas razones hacen factible el desarrollo del proyecto.

## **CAPÍTULO II**

### **MARCO TEÓRICO**

#### **ANTECEDENTES DE LA INVESTIGACIÓN**

Los antecedentes son todo hecho anterior a la formulación del problema que sirve para aclarar, calificar e interpretar el problema planteado. Los antecedentes de esta investigación están conformados por manuales existentes y trabajos realizados anteriormente en la Corporación en estudio, relacionados de una forma u otra con este proyecto.

Con relación a los manuales, se utilizarán los siguientes: Cisco Catalyst Serie 3550-2950. Guía de instalación y configuración. Es un manual de instalación y configuración de los switches de la serie 3500 y 2900 que posee la Gerencia de Operaciones de Red de Corporación en estudio. Este manual representa el estándar de configuración que deben tener los switches a instalarse y la nomenclatura utilizada por ellos para poder adaptarla a la configuración de los nuevos.

Se utilizará el mismo para obtener información sobre los procesos y tareas que se realizan en la Gerencia de Operaciones, específicamente en el área de redes que ayudará al análisis del sistema actual para desarrollar el sistema propuesto adaptándose a los objetivos de la empresa y el área involucrada.

## BASES REÓRICAS

### DEFINICIÓN GENERAL DE UNA RED DE DATOS

Se puede definir, como un sistema de comunicación de datos basado en la interconexión de dispositivos de procesamiento inteligentes e independientes, cuya finalidad primaria consiste en permitir el uso compartido de los recursos instalados en la red (discos, impresoras, fax, archivos, programas, etc.) a través del uso de un protocolo de comunicación común.

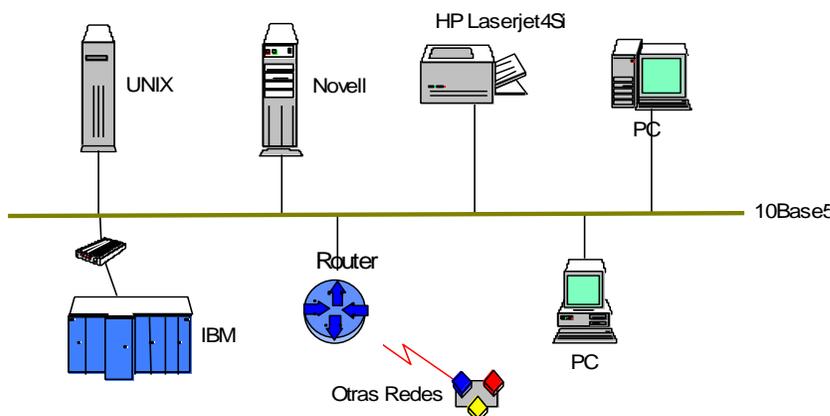


Figura II.1. Esquema general de la red.

### CLASIFICACION DE LAS REDES

Las redes se pueden clasificar de acuerdo a varios criterios como dispersión física de los equipos/nodos de la red, velocidad de transmisión o topología.

- **LAN (Local Área Network):** Se caracteriza porque utiliza medios de transmisión generalmente acotados de muy alta velocidad (2 Mbps hasta 100 Mbps), y por lo general se localizan en espacios físicos reducidos. La mayoría de los estándares

de red local, utilizan un único canal de comunicación que es compartido por todos los nodos de la red y el protocolo de comunicación usado define el método de acceso al canal. Topologías comunes: bus, anillo, entre otras.

- **WAN (Wide Area Network):** Se caracterizan porque utilizan medios de transmisión de baja velocidad (hasta 2 Mbps) y no presenta limitaciones en cuanto a la dispersión geográfica de la red. Cada enlace de comunicación conecta dos nodos de la red (usualmente equipos de conmutación como: routers y bridges), y la comunicación se lleva a cabo sin que el resto de los nodos intervenga (punto-punto). Topologías: asimétricas e irregulares.
- **MAN (Redes de Área Metropolitana):** Las redes de áreas metropolitanas o MAN permiten cubrir un área geográfica de una ciudad entera, pero utilizan tecnología de red de área local en vez de la tecnología de área extensa, es decir, puede alcanzar velocidades semejantes a las redes de área local en un espacio más amplio.

## TOPOLOGIAS DE RED

Los nodos de la red necesitan estar conectados para comunicarse. A la forma en que están conectados se le llama topología. La topología es un aspecto determinante en una red ya que determinan cómo se encuentran interconectados entre sí los equipos. Para cada red se deben definir dos tipos de topologías: la topología lógica y la topología física.

**TOPOLOGÍA FÍSICA:** Define la distribución física de los nodos que conforman la red. En la topología física las estaciones de trabajo de una red se comunican entre sí mediante una conexión física, es decir, busca una adecuada

distribución del cableado. El objeto de la topología es buscar la forma más económica y eficaz de conectarlas, al mismo tiempo, facilita la fiabilidad del sistema, evita los tiempos de espera en la transmisión de los datos, etc. Ejemplo: estrella, bus, anillo.

- **TOPOLOGÍA ESTRELLA:** Todos los nodos se encuentran conectados a un controlador central. Todas las transacciones pasan a través del nodo central, siendo éste el encargado de gestionar y controlar todas las comunicaciones. Por este motivo, el fallo de un nodo en particular es fácil de detectar y no daña al resto de la red, pero un fallo en el nodo central desactiva la red completa.

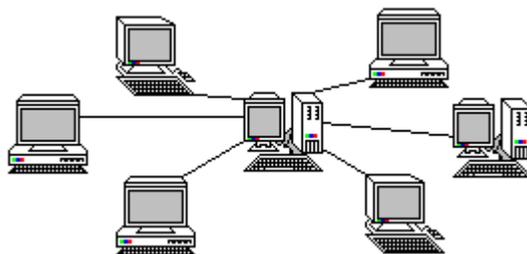


Figura II.2. Topología estrella.

- **TOPOLOGÍA BUS:** Cada computador se conecta a la red en forma lineal uno seguido del otro por medio de un segmento común de cable de red. En este caso no es necesario que un nodo controle la red, salvo para ejercer control sobre los posibles errores que se presenten. El fallo de cualquier nodo no impide que la red siga funcionando normalmente. Todos los nodos de la red se conectan a un troncal de cable denominado bus lineal.

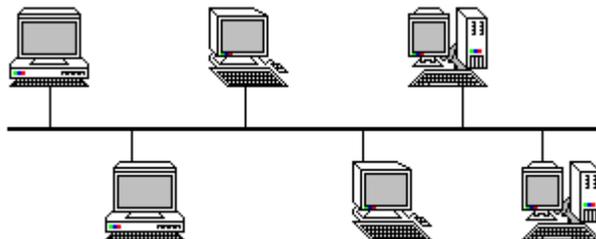


Figura II.3. Topología bus.

- TOPOLOGÍA ANILLO:** Los nodos se conectan configurando un anillo cerrado, de modo que cada estación tiene conexión directa a otros dos. Tiene el inconveniente de que la operación del anillo se interrumpe cuando se avería cualquiera de los enlaces. Los nodos que componen la red están dispuestos en forma circular, el estilo de un bus lineal cerrado en sus extremos.

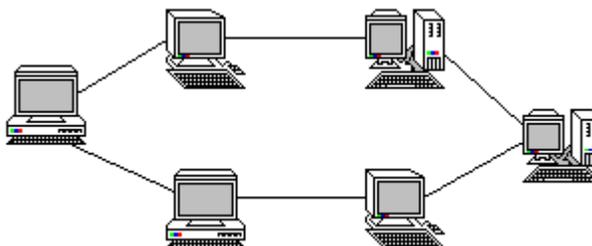


Figura II.4. Topología anillo.

**TOPOLOGÍA LÓGICA:** Define la distribución de los nodos de acuerdo a la ruta lógica que siguen los paquetes en la red. Esta topología está asociada a la funcionalidad y comportamiento del protocolo de red. Por ejemplo, la topología física de Ethernet 10BaseT es estrella o cadena de estrellas, pero su topología lógica es bus.

## COMPONENTES DE UNA RED

- Sistema de cableado.
- Servidores de la red.
- Clientes de la red.
- Tarjetas de red.
- Sistema operativo de red (NOS).
- Estaciones de trabajo.
- Equipos de red.
- *Hubs*.
- *Switchs*.
- *Router* (Enrutador).
- *Patch panels*.

## EL MODELO OSI

El modelo OSI (Open Systems Interconnection) es la propuesta que hizo la Organización Internacional para la Estandarización (ISO) para estandarizar la interconexión de sistemas abiertos. Un sistema abierto se refiere a que es independiente de una arquitectura específica. Se compone el modelo, por tanto, de un conjunto de estándares ISO relativos a las comunicaciones de datos.

- **Las Capas OSI:**
  - **Capa 7 Aplicación:** esta capa atiende a todas las aplicaciones que requieren la red. Permite que varias aplicaciones compartan la red.

- **Capa 6 Presentación:** esta capa se encarga de definir los formatos de los datos y si es necesario, procesarlos para su envío. Este proceso puede ser el de compresión o el de paso a algún sistema de codificación.
- **Capa 5 Sesión:** se encarga de proporcionar diálogo entre aplicaciones finales para el uso eficiente de las comunicaciones. Puede agrupar datos de diversas aplicaciones para enviarlos juntos o incluso detener la comunicación y restablecer el envío tras realizar algún tipo de actividad.
- **Capa 4 Transporte:** esta capa se encarga de que los datos enviados y recibidos lleguen en orden, sin duplicación y sin errores. Puede ser servicio de transporte orientado a conexión (conmutación de circuitos o circuitos virtuales) o no orientado a conexión (datagramas).
- **Capa 3 Red:** esta capa se encarga de vincular los equipos con la red, encaminando los datos hacia sus lugares o direcciones de destino. Para esto, se produce un diálogo con la red para establecer prioridades y encaminamientos.
- **Capa 2 Enlace de datos:** esta capa debe encargarse de que los datos se envíen con seguridad a su destino y libres de errores. Cuando la conexión no es punto a punto, esta capa no puede asegurar su cometido y es la capa superior quien lo debe hacer.
- **Capa 1 Físico:** se encarga de pasar bits al medio físico y de suministrar servicios a la siguiente capa. Para ello debe conocer las características mecánicas, eléctricas, funcionales y de procedimiento de las líneas.

## ESTÁNDARES DE RED USADOS ACTUALMENTE

1. **Ethernet:** Norma o estándar (IEEE 802.3) que determina la forma en que los puestos de la red envían y reciben datos sobre un medio físico compartido que se comporta como un bus lógico, independientemente de su configuración física. Originalmente fue diseñada para enviar datos a 10 Mbps.
2. **Fast Ethernet:** Fast Ethernet, llamado también 100BASEX, es una extensión del estándar Ethernet que opera a velocidades de 100 Mbps, un incremento diez veces mayor que el Ethernet estándar de 10Mbps.
3. **Gigabit Ethernet:** Es una ampliación del estándar Ethernet que consigue una capacidad de transmisión de 1 gigabit por segundo, correspondientes a unos 1000 megabits por segundo de rendimiento contra unos 100 Mbps de Fast Ethernet.
4. **WLAN 802.11:** Es el estándar utilizado para redes inalámbricas (WLANs Wireless Local Area Network), entre los cuales se encuentran: 802.11 = 1Mb, 802.11a = 54 Mb (Ésta trabaja a una frecuencia en el rango de los 5GHz), 802.11b = 11Mb (Trabaja a 2,4 GHz. Conserva compatibilidad con el Estándar Nativo 802.11, de 1Mb), 802.11g = 54 Mb (Trabaja a 2,4 GHz. Puede alcanzar los 108 Mb con dispositivos del mismo fabricante, y en la actualidad se esta hablando de la 802.11n, cuya velocidad de transmisión pudiera llegar a 600Mbps).

## VLAN: RED DE ÁREA LOCAL VIRTUAL

Una red de área local (LAN) está definida como una red de computadoras dentro de un área geográficamente acotada, como puede ser una empresa o una corporación. Uno de los problemas que nos encontramos es el de no poder tener una

confidencialidad entre usuarios de la LAN, también estando todas las estaciones de trabajo en un mismo dominio de colisión el ancho de banda no es aprovechado correctamente. La solución a este problema es la división de la LAN en segmentos físicos los cuales deben ser independientes entre sí, dando como desventaja la imposibilidad de comunicación entre las LANs para algunos de los usuarios de la misma. Una VLAN se encuentra conformada por un conjunto de dispositivos de red interconectados (*hubs*, *bridges*, *switches* o estaciones de trabajo) y se define como un dominio de *broadcast* que pueden estar en el mismo medio físico o bien puede estar sus integrantes ubicados en distintos sectores de una empresa (Figura II.5. y II.6).

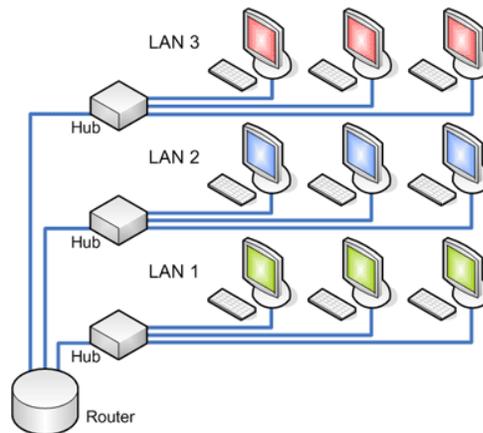


Figura II.5. LAN tradicional.

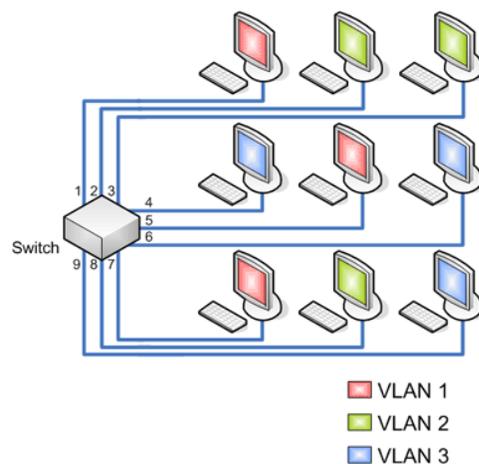


Figura II.6. VLAN.

La tecnología de las VLANs se basa en el empleo de *switches*, en lugar de *hubs*, de tal manera que esto permite un control mas inteligente del tráfico de la red, ya que este dispositivo trabaja a nivel de la capa 2 del modelo OSI y es capaz de dividir el tráfico, para que de esta manera la eficiencia de la red se incremente.

## SEGMENTACIÓN

Con los *switches* se crean pequeños dominios, llamados segmentos o bien se aplica microsegmentación la cual se realiza conectando cada estación de trabajo y cada servidor directamente a puertos de *switch*, teniendo una conexión dedicada dentro de la red, con lo que se consigue maximizar considerablemente el ancho de banda a disposición de cada usuario.

Una de las ventajas que se pueden notar en las VLAN es la reducción en el tráfico de la red, ya que solo se transmiten los paquetes a los dispositivos que estén incluidos dentro del dominio de cada VLAN, una mejor utilización del ancho de banda y confidencialidad respecto a personas ajenas a la VLAN, alto desempeño, reducción de latencia, facilidad para configurar grupos de trabajo. Con el *switch*, el rendimiento de la red mejora en los siguientes aspectos:

- Aísla los “dominios de colisión” por cada uno de los puertos.
- Dedicar el ancho de banda a cada uno de los puertos y, por lo tanto, a cada computadora.
- Aísla los “dominios de *broadcast*”, y que en lugar de uno solo, se puede configurar el *switch* para que existan más “dominios”.
- No importa en donde nos encontremos conectados dentro del edificio de oficinas, si estamos configurados en una VLAN, nuestros compañeros de área, dirección, sistemas, administrativos, entre otros; estarán conectados dentro de

la misma VLAN, y quienes se encuentren en un segmento diferente, podrán “vernors” como una Red de Área Local independiente a las demás.

## TIPOS DE VLAN

### VLAN POR PUERTO

Se configura por una cantidad “n” de puertos en el cual podemos indicar que puertos pertenecen a cada VLAN. Para la Figura 1 tendríamos en el Switch 6 puertos de los cuales el 1 y 5 pertenecen a la VLAN 1; el 2 y 3 a la VLAN 2 y los puertos 4 y 6 a la VLAN 3 como la tabla lo indica (Tabla II.1.).

Puerto	VLAN
1	1
2	2
3	2
4	3
5	1
6	3

Tabla II.1. VLAN por puerto.

#### Ventajas

- Facilidad de movimientos y cambios.
- Multiprotocolo: La definición de la VLAN es independiente del o los protocolos utilizados, no existen limitaciones en cuanto a los protocolos utilizados, incluso permitiendo el uso de protocolos dinámicos.
- Microsegmentación y reducción del dominio de broadcast.

#### Desventajas

- Administración: Un movimiento en las estaciones de trabajo hace necesaria la reconfiguración del puerto del switch al que está conectado el usuario. Esto se puede facilitar combinando con mecanismos de LAN Dinámicas.

## VLAN POR DIRECCIÓN MAC

Los miembros de la VLAN están especificados en una tabla por su dirección MAC (Tabla II.2.).

MAC	VLAN
12.15.89.bb.1d.aa	1
12.15.89.bb.1d.aa	2
1d.15.89.6b.6d.ca	2
12.aa.cc.bb.1d.aa	1

Tabla II.2. VLAN por dirección MAC.

### Ventajas

- Facilidad de movimientos: No es necesario en caso de que una terminal de trabajo cambie de lugar la reconfiguración del switch.
- Multiprotocolo.
- Se pueden tener miembros en múltiples VLANs

### Desventajas

- Problemas de rendimiento y control de broadcast: el tráfico de paquetes de tipo multicast y broadcast se propagan por todas las VLANs.
- Complejidad en la administración: En un principio todos los usuarios se deben configurar de forma manual las direcciones MAC de cada una de las estaciones de trabajo. También se puede emplear soluciones de DVLAN.

## VLAN POR PROTOCOLO

Asigna a un protocolo una VLAN. El *switch* se encarga de dependiendo el protocolo por el cual venga la trama derivarlo a la VLAN correspondiente (Tabla II.3.).

Protocolo	VLAN
IP	1
IPX	2
IP	1

Tabla II.3. VLAN por protocolo

### Ventajas

- Segmentación por protocolo.
- Asignación dinámica.

### Desventajas

- Problemas de rendimiento y control de *broadcast*: Por las búsquedas en tablas de pertenencia se pierde rendimiento en la VLAN.
- No soporta protocolos de nivel 2 ni dinámicos.

## VLAN POR DIRECCIONES IP

Está basado en el encabezado de la capa 3 del modelo OSI. Las direcciones IP a los servidores de VLAN configurados. No actúa como *router*, sino para hacer un mapeo de que direcciones IP están autorizadas a entrar en la red VLAN. No realiza otros procesos con la dirección IP.

### Ventajas

- Facilidad en los cambios de estaciones de trabajo: Cada estación de trabajo al tener asignada una dirección IP en forma estática no es necesario reconfigurar el *switch*.

### Desventajas

- El tamaño de los paquetes enviados es menor que en el caso de utilizar direcciones MAC.
- Pérdida de tiempo en la lectura de las tablas.
- Complejidad en la administración: En un principio todos los usuarios se deben configurar de forma manual las direcciones MAC de cada una de las estaciones de trabajo.

## **VLAN DINÁMICAS (DVLAN)**

Las VLAN dinámicas son puertos del *switch* que automáticamente determinan a que VLAN pertenece cada puesto de trabajo. El funcionamiento de estas VLANs se basa en las direcciones MAC, direcciones lógicas o protocolos utilizados. Cuando un puesto de trabajo pide autorización para conectarse a la VLAN, el *switch* chequea la dirección MAC ingresada previamente por el administrador en la base de datos de las mismas y automáticamente se configura el puerto al cual corresponde por la configuración de la VLAN.

## **PERTENENCIA A UNA VLAN**

La pertenencia a una VLAN define si un dispositivo determinado es miembro de una VLAN. La pertenencia a una VLAN se puede definir de manera estática o dinámica. La forma más habitual es la estática. Cuando la pertenencia se define estáticamente, se basa en el puerto de conmutador al que está conectado el dispositivo. Es el método más sencillo para configurar la pertenencia a una VLAN.

La pertenencia a una VLAN definida dinámicamente se basa en las direcciones MAC del dispositivo. Esta configuración es un poco más complicada, pero permite desplazar los servidores según se desee y que la pertenencia les siga, lo que puede resultar muy útil para empresas que pueden desplazar a sus empleados a menudo o que tienen muchos usuarios conectados a la red mediante portátiles.

## **ETIQUETADO DE VLAN**

El etiquetado de VLAN es un proceso por el que se identifica una trama miembro de una VLAN, de manera que otros conmutadores y enrutadores pueden

decir en qué VLAN se originó la trama. Como resultado, se pueden enviar tramas desde muchas VLAN sobre el mismo puerto físico. Este proceso es llamado compartición (*trunking*). Este proceso es una mejora extremadamente útil que permite ahorrar puertos en conmutadores y enrutadores, ya que por un sólo puerto de compartición (*Trunk*) pueden viajar múltiples VLAN.

Sin embargo, también existen un par de problemas con la compartición. Primero, sobre Ethernet se puede efectuar compartición (*trunking*) sólo con enlaces fast-ethernet o giga-ethernet. Segundo, el etiquetado de VLAN requiere la modificación de la trama Ethernet, lo que significa que todos los conmutadores que participan en el etiquetado de VLAN (al menos en el protocolo ISL: Inter.-Switch Link de Cisco) deben soportar el etiquetado de VLAN. Finalmente se puede efectuar el etiquetado de VLAN de una o dos maneras incompatibles, utilizando el protocolo ISL de Cisco o el IEEE 802.1Q de múltiples fabricantes.

## **PROTOCOLO DE COMPARTICIÓN PARA VLAN**

El protocolo de compartición para VLAN (VTP, VLAN Trunking Protocol) es una característica adicional interesante que se emplea para gestionar las VLAN y que permite asignar definiciones VLAN a múltiples conmutadores de una red. VTP ayuda con las definiciones de las VLAN, permitiendo utilizar números y nombres en las VLAN, para configurar un conmutador independiente y propagarlo por toda la red de la empresa. Obsérvese que VTP no propaga los miembros de las VLAN a todos los conmutadores, sino sólo la definición (nombre, número y otra información básica).

Para llevar a cabo esta proeza, VTP anuncia la información de configuración de la VLAN a todos los puertos compartidos que se encuentren activados. Así, los conmutadores vecinos aprenden cuáles son las VLAN presentes en la red y su

configuración. Entonces estos conmutadores propagan la información de VLAN a otros conmutadores y así sucesivamente.

## **MODOS VLAN TRUNKING PROTOCOL (VTP)**

VTP puede ejecutarse en un conmutador en tres modos:

- a. Cliente. En este modo el conmutador escucha y propaga los mensajes de VTP sobre su dominio de gestión. Efectúa cambios a su configuración VLAN basados en estos mensajes.
- b. Servidor. En este modo, el conmutador también escucha y propaga los mensajes VTP sobre su dominio de gestión, pero además genera nuevos mensajes. Este modo permite modificar directamente la información VLAN en el conmutador, incluyendo añadir y eliminar datos de las VLAN desde el dominio de gestión. Modificar la configuración VTP del dominio de gestión produce la actualización de la configuración del número de revisión. Esta actualización hace que todos los conmutadores del dominio de gestión actualicen su configuración VTP con la nueva información. Apropiadamente, sólo deben existir uno o dos servidores VTP en cada dominio de gestión.
- c. Transparente. En el modo transparente se envía la información VTP, pero se ignoran las configuraciones VLAN contenidas en estos mensajes. La configuración VLAN puede modificarse directamente en un conmutador que se encuentre en el modo transparente, pero esas modificaciones sólo se aplicarán al conmutador local.

## **CABLEADO ESTRUCTURADO**

Un sistema de cableado estructurado consiste de una infraestructura flexible de cables que puede aceptar y soportar sistemas de computación y de teléfono múltiples, independientemente de quién fabricó los componentes del mismo. En un sistema de cableado estructurado, cada estación de trabajo se conecta a un punto central utilizando una topología tipo estrella, facilitando la interconexión y la administración del sistema.

## **NORMAS Y ESTÁNDARES**

### **La Norma EIA/TIA 568-A:**

ANSI / TIA / EIA – 568-A Commercial Building Telecommunications Cabling Standard (October 1995).

Esta norma reemplaza a la EIA/TIA 568 publicada en Julio de 1999. El propósito de la norma EIA/TIA 568-A se describe de la siguiente forma:

Esta norma especifica un sistema de cableado de telecomunicaciones genérico para edificios comerciales que soportará un ambiente multi-producto y multi-fabricante. También proporciona directivas para el diseño de productos de telecomunicaciones para empresas comerciales. El propósito de esta norma es permitir la planeación e instalación de cableado de edificios comerciales con muy poco conocimiento de los productos de telecomunicaciones que serán instalados con posterioridad.

La norma EIA/TIA 568-A especifica los requerimientos mínimos para el cableado de establecimientos comerciales de oficinas. Se hacen recomendaciones para: las topologías, la distancia máxima de los cables, el rendimiento de los componentes, las tomas y los conectores de telecomunicaciones.

Se asume que los edificios tienen las siguientes características:

- Una distancia entre ellos de hasta 3 Km.
- Un espacio de oficinas de hasta 1.000.00 m<sup>2</sup>.
- Una población de hasta 50.000 usuarios individuales.

## **DEFINICIÓN DE LA ESTRUCTURA DE LOS SISTEMAS DE CABLEADO**

La norma EIA/TIA 568-A divide los sistemas de cableado de telecomunicaciones en los siguientes elementos: cableado horizontal, cableado vertical, área de trabajo, armario de telecomunicaciones, cuarto de equipos, instalaciones de entrada, cuarto de entrada de servicio y administración.

### **CABLEADO HORIZONTAL**

Es la porción del cableado que se extiende desde el área de trabajo hasta el armario de telecomunicaciones. El término “horizontal” se utiliza porque típicamente este cableado se desplaza de una manera horizontal en el edificio. Este subsistema conecta el subsistema de estaciones de trabajo con el cuarto donde se hará la administración del piso. Este subsistema es el que genera más análisis y detalle en el diseño por cuanto incide directamente en la conformación arquitectónica del edificio o espacio físico a cablear. En este subsistema se estudian y definen las rutas más adecuadas para distribuir la totalidad del cableado a lo largo de un piso.

El cableado horizontal incluye:

- Los cables horizontales.
- Las tomas/conectores de telecomunicaciones en el área de trabajo.
- La terminación mecánica.
- Las interconexiones horizontales localizadas en el armario de telecomunicaciones.

El cableado horizontal es típicamente el más difícil de mantener debido a la complejidad de trabajo en una oficina en producción. Es sumamente necesario que se tome en cuenta no sólo las necesidades actuales sino las futuras para no causar molestias a los usuarios en el trabajo diario.

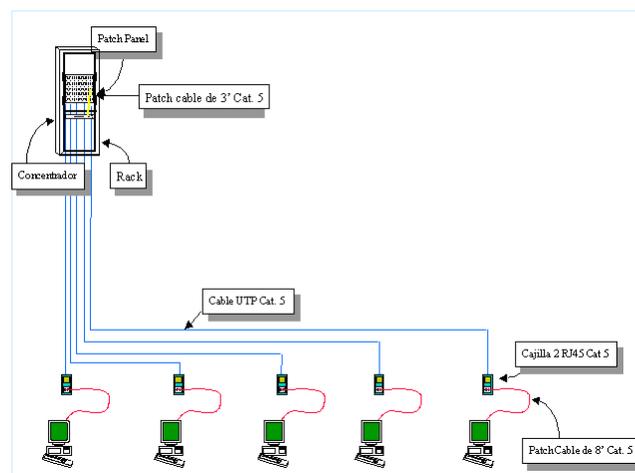


Figura II.7. Diagrama del cableado horizontal.

### Estructura del cableado horizontal

El sistema de cableado horizontal se extiende desde la toma de telecomunicaciones en el área de trabajo a la terminación de conexión horizontal entre diferentes vías en el centro de telecomunicaciones.

- Instalaciones del equipo servidor.
- Cola de empalme del equipo servidor al centro rack principal.
- Colas de conexión de empalme de interconexión/puentes de terminación de conexión entre diferentes vías, incluyendo cables/cables del equipo, no deberían exceder los 6 mts., (20 pies).
- Cable horizontal 90 mts., (295 pies) máx. total.
- F) Toma / conector de telecomunicaciones.

### **Topología cableado horizontal**

La norma EIA/TIA 568-A hace las siguientes recomendaciones en cuanto a la topología del cableado horizontal:

- El cableado horizontal debe seguir una topología estrella.
- Cada toma/conector de telecomunicaciones del área de trabajo debe conectarse a una interconexión en el armario de telecomunicaciones.
- El cableado horizontal en una oficina debe terminar en un armario de telecomunicaciones ubicado en el mismo piso que el área de trabajo servida.
- Los componentes electrónicos específicos de la aplicación (como dispositivos acopladores de impedancia) no se instalarán como parte del cableado horizontal; cuando se necesiten, estos componentes se deben poner fuera de la toma/conector de telecomunicaciones.
- El cableado horizontal no debe contener más de un punto de transición entre cable horizontal y cable plano.
- No se permiten empalmes de ningún tipo en el cableado horizontal.
- Se separan 10 m para los cables del área de trabajo y los cables del armario de telecomunicaciones (cables de parcheo, jumpers y cables de equipo).

- Sin importar el medio físico, la distancia horizontal máxima no debe exceder 90 mts.
- Los cables de interconexión y los cables de parcheo que conectan el cableado horizontal con los equipos o los cables del vertical en las instalaciones de interconexión no deben tener más de 6 m de longitud.
- En el área de trabajo, se recomienda una distancia máxima de 3 m desde el equipo hasta la toma/conector de telecomunicaciones.

#### **Partes del Cableado Estructurado Horizontal:**

1. *Rack*.
2. Concentrador.
3. *Patch panel*.
4. Cable UTP Cat. 5 y 6.
5. Toma doble Rj-45 voz y datos.
6. Estación de trabajo.

#### **Documentación:**

- Se debe establecer una nomenclatura de documentación para cada instalación.
- Todos los cables paneles y salidas deben estar documentados tanto a simple vista como en su interior.
- Deben mantenerse planos y/o diagramas de las instalaciones.
- Se recomienda altamente a grandes instituciones la documentación por medio de bases de datos electrónicas.

## CABLEADO VERTICAL

La norma EIA/TIA 568-A define el cableado vertical (*backbone*) de la siguiente forma:

La función del cableado vertical es la de proporcionar interconexiones entre los armarios de telecomunicaciones, los cuartos de equipos y las instalaciones de entrada en un sistema de cableado estructurado de telecomunicaciones. El cableado vertical consta de:

- Conexión vertical entre pisos (*risers*).
- Las interconexiones principales e intermedias.
- Las terminaciones mecánicas y los cables de parcheo o *jumpers* empleados en la interconexión vertical.
- El vertical incluye también el cableado entre edificios.

Se deben hacer ciertas consideraciones a la hora de seleccionar un cableado vertical:

- La vida útil del sistema de cableado vertical se planifica en varios períodos (típicamente, entre 3 y 10 años); esto es menor que la vida de todo el sistema de cableado de telecomunicaciones (típicamente, varias décadas).
- Antes de iniciar un período de planificación, se debe proyectar la cantidad máxima de cable vertical para el período; el crecimiento y los cambios durante ese período se deben acomodar sin necesidad de instalar cable vertical adicional.
- Se debe planear que la ruta y la estructura de soporte del cable vertical de cobre evite las áreas donde existan fuentes potenciales de emisiones electromagnéticas (EMI).

- Una de las funciones del cableado vertical es proveer la interconexión entre los armarios de telecomunicaciones y las entradas de la instalación en cada piso.

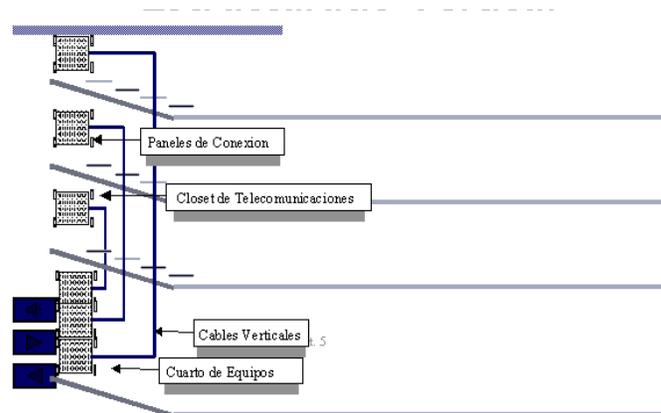


Figura II.8. Diagrama del cableado vertical.

### Topología cableado vertical

La norma EIA/TIA 568-A hace las siguientes recomendaciones en cuanto a la topología del vertical:

- El cableado vertical deberá seguir la topología estrella convencional.
- Cada interconexión horizontal en un armario de telecomunicaciones está cableada a una interconexión principal o a una interconexión intermedia y de ahí a una interconexión principal con la siguiente excepción:
  - Si se anticipan requerimientos para una topología de red bus o anillo, entonces se permite el cableado de conexiones directas entre los armarios de telecomunicaciones.
  - No debe de haber más de dos niveles jerárquicos de interconexiones en el cableado vertical (para limitar la degradación de la señal debido a los sistemas pasivos y para simplificar los movimientos, aumentos o cambios).

- Las instalaciones que tienen un gran número de edificios o que cubren una gran extensión geográfica pueden elegir subdividir la instalación completa en áreas menores dentro del alcance de la norma EIA/TIA 568-A. En este caso, se excederá el número total de niveles de interconexión.
- Solo se debe pasar por una conexión cruzada para llegar a la conexión cruzada principal.
- En ciertas instalaciones, la conexión cruzada del vertical (conexión cruzada principal) bastará para cubrir los requerimientos de conexiones cruzadas.
- Las conexiones cruzadas del vertical pueden estar ubicadas en los armarios de telecomunicaciones, los cuartos de equipos o las instalaciones de entrada.
- No se permiten empalmes como parte del cableado vertical.
- El agua no deberá penetrar el sistema de trayectoria.
- Bandeja, tuberías de protección, manguitos y ranuras penetran los habitáculos un mínimo de 25 mm (1 pulgada).
- Diseñadas para manejar todos los medios reconocidos (tal como se especifica en 568-A).

### **ÁREA DE TRABAJO**

El área de trabajo se extiende desde la toma/conector de telecomunicaciones o el final del sistema de cableado horizontal, hasta el equipo de la estación y está fuera del alcance de la norma EIA/TIA 568-A. El equipo de la estación se puede incluir, pero no se limita a, teléfonos, terminales de datos y computadoras.

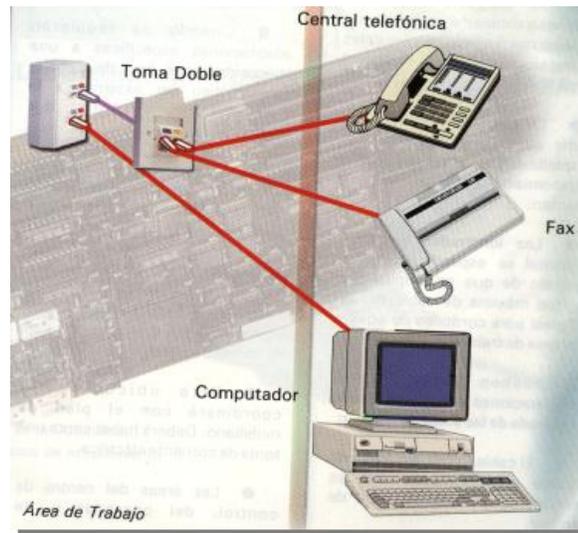


Figura II.9. Área de trabajo.

### Consideraciones acerca del diseño del cableado del área de trabajo

- El cableado de las áreas de trabajo generalmente no es permanente y debe ser fácil de cambiar.
- La longitud máxima del cable horizontal se ha especificado con el supuesto que el cable de parcheo empleado en el área de trabajo tiene una longitud máxima de 3 metros.
- Comúnmente se emplean cables con conectores idénticos en ambos extremos.
- Cuando se requieran adaptaciones específicas a una aplicación en el área de trabajo, éstas deben ser externas a la toma/conector de telecomunicaciones.

### Configuraciones comunes de toma área de trabajo

Se han adoptado dos esquemas de alambrado. Son prácticamente idénticos, salvo que los pares dos y tres están invertidos. T658-A es el esquema preferido porque es compatible con sistemas USOC de 1 ó 2 pares.

El alambrado 10Base-T especifica un conector de 8 contactos, pero usa solamente dos pares. Estos son los pares dos y tres de los esquemas T568-A y T568-B.

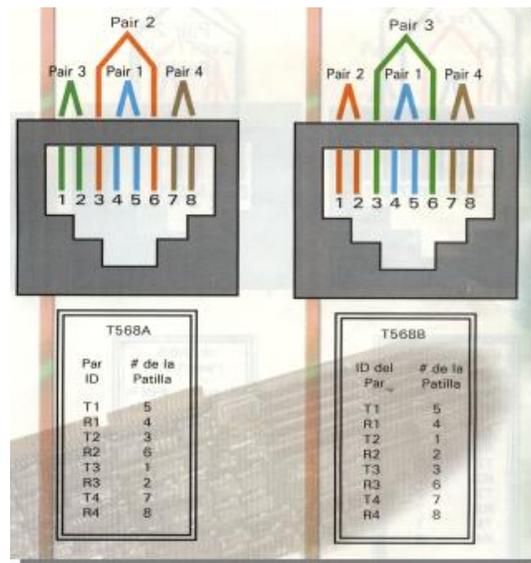


Figura II.10. Configuración común área de trabajo.

## CUARTO DE TELECOMUNICACIONES

Un cuarto de telecomunicaciones es el área en un edificio utilizada para el uso exclusivo de equipo asociado con el sistema de cableado de telecomunicaciones. El espacio del cuarto de comunicaciones no debe ser compartido con instalaciones eléctricas que no sean de telecomunicaciones. El cuarto de telecomunicaciones debe ser capaz de albergar equipo de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado. Todo edificio debe contar con al menos un cuarto de telecomunicaciones o cuarto de equipo.

### Consideraciones de diseño

El diseño de un cuarto de telecomunicaciones depende de:

- El tamaño del edificio.
- El espacio de piso a servir.
- Las necesidades de los ocupantes.
- Los servicios de telecomunicaciones a utilizarse.

### **Cantidad de cuartos de telecomunicaciones**

Debe de haber un mínimo de un cuarto de telecomunicaciones por edificio, mínimo uno por piso, no hay máximo.

- **Altura:** la altura mínima recomendable del cielo raso es de 2.6 metros.
- **Conductos:** el número y tamaño de los conductos utilizados para acceder el cuarto de telecomunicaciones varía con respecto a la cantidad de áreas de trabajo, sin embargo se recomienda por lo menos tres conductos de 100 milímetros para la distribución del cable vertical.
- **Puertas:** La(s) puerta(s) de acceso debe(n) ser de apertura completa, con llave y de al menos 91 centímetros de ancho y 2 metros de alto. La puerta debe poderse desmontar y abrir hacia fuera (o lado a lado). La puerta debe abrir al ras del suelo y no debe tener postes centrales.
- **Polvo y electricidad estática:** se debe evitar polvo y la electricidad estática utilizando piso de concreto, terrazo, loza o similar (no utilizar alfombra). De ser posible, aplicar tratamiento especial a las paredes pisos y cielos raso para minimizar el polvo y la electricidad estática.
- **Control ambiental:** en cuartos que no tienen equipo electrónico la temperatura del cuarto de telecomunicaciones debe mantenerse continuamente (24 horas al día, 365 días al año) entre 10 y 35 grados centígrados. La humedad relativa debe mantenerse menor a 85%. Debe de haber un cambio de aire por hora. En cuartos que tienen equipos electrónicos la temperatura debe

mantenerse continuamente (24 horas al día, 365 días al año) entre 18 y 24 grados centígrados. La humedad relativa debe mantenerse entre 30% y 55%. Debe haber un cambio de aire por hora.

- **Cielos Falsos:** se deben evitar el uso de cielos falsos en los cuartos de telecomunicaciones.
- **Prevención de inundaciones:** los cuartos de telecomunicaciones deben estar libres de cualquier amenaza de inundación. No debe haber tubería de agua pasando por (sobre o alrededor) el cuarto de telecomunicaciones. De haber riesgo de ingreso de agua, se debe proporcionar drenaje de piso. De haber regaderas contra incendio. Suelos: los suelos de los cuartos de telecomunicaciones deben soportar una carga de 2.4 Kg/mt.
- **Iluminación:** se debe proporcionar un mínimo equivalente a 540 lux medido a un metro del piso terminado. La iluminación debe estar a un mínimo de 2.6 metros del piso terminado. Las paredes deben estar pintadas en un color claro para mejorar la iluminación. Se recomienda el uso de luces de emergencia.
- **Localización:** con el propósito de mantener la distancia horizontal de cable promedio en 46 metros o menos (con un máximo de 90 metros), se recomienda localizar el cuarto de telecomunicaciones lo más cerca posible del centro del área a servir.
- **Potencia:** Debe haber tomas de corriente suficiente para alimentar los dispositivos a instalarse en el cuarto de telecomunicaciones. El estándar establece que debe haber un mínimo de dos tomas de corriente dobles de 110V. Deben ser circuitos separados de 15 a 20 amperios. Estas dos tomas de corriente podrían estar dispuestas a 1.8 metros de distancia una de otra. En muchos casos es deseable instalar un cuadro de control eléctrico dedicado al cuarto de telecomunicaciones. La alimentación específica de los dispositivos electrónicos se podrá hacer con un UPS y regletas montadas en los armarios.

- **Seguridad:** se debe mantener el cuarto de telecomunicaciones con llave en todo momento. Se deben asignar llaves a personal que esté en el edificio durante las horas de operación. Se debe mantener el cuarto de telecomunicaciones limpio y ordenado.
- **Requisitos de tamaño:** debe haber al menos un cuarto de telecomunicaciones o cuarto de equipo por piso y por áreas que no excedan los 1000 metros cuadrados. Instalaciones pequeñas podrán utilizar un solo cuarto de telecomunicaciones si la distancia máxima de 90 metros no se excede.
- **Disposición de equipos:** los armarios (racks) deben contar con al menos 82 cm. de espacio de trabajo libre alrededor (al frente y detrás) de los equipos y paneles de telecomunicaciones. La distancia de 82 cm. se debe medir a partir de la superficie más salida del andén.

## **ARMARIO DE TELECOMUNICACIONES**

Los armarios de telecomunicaciones proporcionan varias funciones diferentes a los sistemas de cableado y a menudo son tratados como subsistemas diferentes dentro de la jerarquía de éstos.

Los armarios de telecomunicaciones se consideran por lo general como instalaciones que atienden pisos para distribución de cableado horizontal. También puede usarse para conexiones intermedias y principales entre diferentes vías.

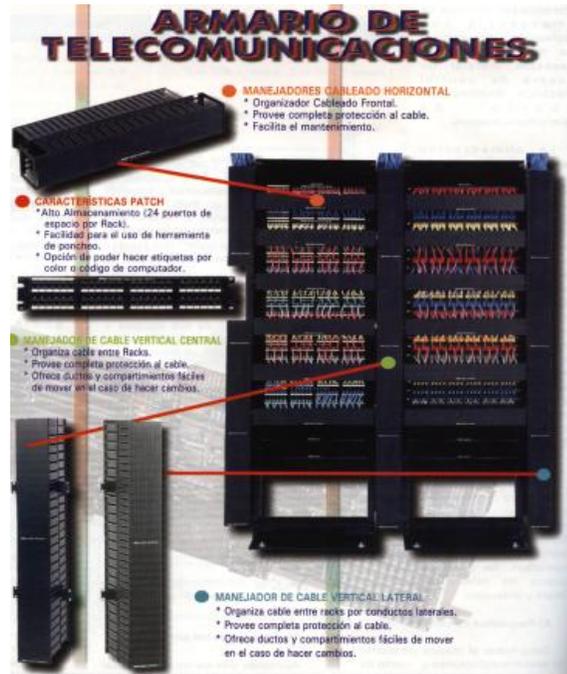


Figura II.11. Armario de telecomunicaciones.

## Diseño

Los armarios de telecomunicaciones deben ser diseñados y aprovisionados de acuerdo a los requerimientos de la norma EIA/TIA 569-A.

- Dedicado a la función de telecomunicaciones.
- No se instalará, pasará a través de o entrará al armario de telecomunicaciones equipo que no tenga que ver estas últimas.
- Armarios múltiples en el mismo piso se interconectarán mediante un mínimo de una tubería de protección (tamaño comercial).

### **Consideraciones de diseño**

- Mínimo un armario por cada piso para alojar equipo de telecomunicaciones / terminaciones de cable.
- Las trayectorias horizontales terminarán en el armario de telecomunicaciones sobre el mismo piso del área atendida.
- Se acomodan a los requisitos de zonas sísmicas.
- La iluminación será de un mínimo de 500 lx (50 bujías pie) y estará montada 2.6 metros (8.5 pies) por encima del piso.
- No se suministrarán techos falsos.
- Tamaño mínimo de la puerta 910 mm (36 pulgadas) de ancho y 2000 mm (80 pulgadas) de alto sin umbral, con bisagras que permitan abrirla hacia fuera, o deslizarla de un lado a otro, o desmontarla, y provista con una cerradura.
- Un mínimo de dos receptáculos de tomas eléctricas dúplex AC, dedicados, a 120V, no conmutados, cada uno en circuitos de ramales separados.
- Acceso al sistema de toma a tierra de telecomunicaciones tal como lo especifica la ANSI/TIA/EIA/607.

### **CUARTO DE EQUIPOS**

El cuarto de equipo es un espacio centralizado de uso específico para equipo de telecomunicaciones tal como central telefónica, equipo de cómputo y/o conmutador de video. Varias o todas las funciones de un cuarto de telecomunicaciones pueden ser proporcionadas por un cuarto de equipo. Los cuartos de equipo se consideran distintos de los cuartos de telecomunicaciones por la naturaleza, costo, tamaño y/o complejidad del equipo que contienen. Los cuartos de equipo incluyen espacio de trabajo para personal de telecomunicaciones. Todo edificio debe contener un cuarto

de telecomunicaciones o un cuarto de equipo. Los requerimientos del cuarto de equipo se especifican en los estándares ANSI/TIA/EIA-568-A y ANSI/TIA/EIA-569.

### **Sistema de Puesta a Tierra y Puenteado para telecomunicaciones**

El sistema de puesta a tierra y puenteado establecido en el estándar ANSI/TIA/EIA-607 es un componente importante de cualquier sistema de cableado estructurado moderno. El sistema de cableado estructurado deberá tener un sistema de tierra totalmente independiente al de la UPS, canaleta, tableros eléctricos y equipos de potencia en general. Un buen sistema de tierra debe incluir 3 elementos de cobre, varilla 99% cobre con una longitud mínima de 1.80 metros, un diámetro de  $\frac{3}{4}$ "', a una distancia igual a la longitud es decir 1.80 metros.

#### **Componentes de un sistema de puesta a tierra:**

1. Conductor de unión para telecomunicaciones.
2. Varilla de puesta a tierra para telecomunicaciones.
3. Sistema medular de puesta a tierra para telecomunicaciones.
4. Varilla de puesta a tierra para instalaciones de telecomunicaciones.
5. Conexiones a la varilla de puesta a tierra para telecomunicaciones.
6. Unión con la estructura metálica del edificio.
7. Conductor para la unión de interconexión de los sistemas modulares de puesta a tierra para telecomunicaciones.

## **¿QUÉ ES LA SEGURIDAD DE LA INFORMACIÓN?**

Es mantener la provisión de información libre de riesgo y brindar servicios para un determinado fin. Es tener bajo protección los recursos y la información con que se

cuenta en la red, a través de procedimientos basados en políticas de seguridad tales que permitan el control de lo actuado.

## **OBJETIVO DE LA SEGURIDAD**

El objetivo de la seguridad en la informática es mantener la integridad, disponibilidad, privacidad, control de acceso y autenticidad de la información manejada por las computadoras así como todos los recursos informáticos involucrados en el ámbito.

## **ASPECTOS EN LA SEGURIDAD INFORMÁTICA**

Existe información que debe o puede ser pública, siendo ésta aquella que puede ser visualizada por cualquier persona, y aquella que debe ser privada, la que sólo puede ser visualizada por un grupo selecto de personas que trabaja con ella. En esta última se debe maximizar el esfuerzo para preservarla de ese modo, reconociendo las siguientes características en la información:

- Crítica: Es indispensable para garantizar la continuidad operativa.
- Valiosa: Es un activo con valor en sí misma.
- Confidencial: Debe ser conocida por las personas que la procesan y sólo por ellas.

La integridad de la información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

La disponibilidad u operatividad de la información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.

La privacidad o confidencialidad de la información es la necesidad de que la misma sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la información puede provocar severos daños a su dueño (por ejemplo conocer antecedentes médicos de una persona) o volverse obsoleta (por ejemplo: los planes de desarrollo de un producto que se “filtran” a una empresa competidora, facilitarán a esta última desarrollar un producto de características semejantes).

El control de acceso sobre la información permite asegurar que sólo los usuarios autorizados pueden decidir cuando y como permitir el acceso a la misma.

La autenticidad permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades.

Adicionalmente pueden considerarse algunos aspectos adicionales, relacionados con los anteriores, pero que incorporan algunos aspectos particulares:

- Protección contra la réplica: mediante la cual se asegura que una transacción sólo puede realizarse una vez, a menos que se especifique lo contrario. No se

deberá poder grabar una transacción para luego reproducirla, con el propósito de copiar la transacción para que parezca que se recibieron múltiples peticiones del mismo remitente original.

- No repudio: mediante la cual se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.
- Consistencia: se debe poder asegurar que el sistema se comporte como se supone que debe hacerlo ante los usuarios que corresponda.
- Aislamiento: este aspecto, íntimamente relacionado con la confidencialidad, permite regular el acceso al sistema, impidiendo que personas no autorizadas hagan uso del mismo.
- Auditoría: es la capacidad de determinar qué acciones o procesos llevarán a cabo en el sistema, así como quién y cuando las realizó.

Cabe definir amenaza, en el entorno informático, como cualquier elemento que comprometa al sistema. Las amenazas pueden ser analizadas en tres momentos: antes del ataque durante y después del mismo. Estos mecanismos conformarán políticas que garantizarán la seguridad de nuestro sistema informático.

- Prevención (antes): mecanismos que aumentan la seguridad (o fiabilidad) de un sistema durante su funcionamiento normal. Por ejemplo el cifrado de información para su posterior transmisión.
- Detección (durante): mecanismos orientados a revelar violaciones a la seguridad. Generalmente son programas de auditoría.

- Recuperación (después): mecanismos que se aplican, cuando la violación del sistema ya se ha detectado, para retornar éste a su funcionamiento normal. Por ejemplo recuperación desde las copias de seguridad (backup) realizadas.

## **LA SEGURIDAD FÍSICA**

Es muy importante ser consciente que por más que una empresa sea la más segura desde el punto de vista de ataques externos, hackers, virus, etc., la seguridad de la misma será nula si no se ha previsto, por ejemplo, como combatir un incendio.

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos aspectos se prevén, otros, como la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de operaciones de la misma, no. Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía red a la misma.

Así, la seguridad física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

## **LA SEGURIDAD LÓGICA O TÉCNICA**

La seguridad lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y a las aplicaciones, permitiéndolo sólo a las personas debidamente autorizadas.

Alguien una vez dijo referente a la seguridad informática “todo lo que no está permitido debe estar prohibido” y esto es lo que debe asegurar la seguridad lógica. Los objetivos que persigue la seguridad lógica son los siguientes; entre otros:

- 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 existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

## **CAPÍTULO III**

### **METODOLOGÍA**

Debido a las características particulares a la que corresponde este tipo de proyectos, y en base a las necesidades, requerimientos y exigencias de las organizaciones o instituciones en las que son llevados a cabo, es necesario adaptar una metodología acorde a estas necesidades, puesto que en la bibliohemerografía consultada no se encontró ninguna metodología formal para este tipo de proyectos.

En consideración a las circunstancias antes expuestas y en vista de la necesidad de ajustarse a las características particulares del proyecto, se ha optado por establecer una adaptación de pasos o fases empleadas en labores semejantes (instalación de redes locales, desarrollo de software), las cuales conllevan al desarrollo apropiado y requerido en las diferentes facetas del proyecto. En este caso particular, se utilizarán diversas técnicas sugeridas por varios autores: Kendall & Kendall, Jonás Montilva (Metodología para el Desarrollo de Hipermedia), Kevin Stoltz, Hernández (Metodología para Sistemas de Planificación de Intranet, 1999, pág. 71-73), Panduit (Metodología para la instalación de cableado estructurado), Cisco Systems, entre otras para obtener una metodología apropiada en la actualización de la infraestructura tecnológica y diseño e implantación de la plataforma de seguridad para el Centro de Estudios de Telecomunicaciones de la Corporación en estudio.

#### **FASES TOMADAS EN CONSIDERACIÓN PARA EL DESARROLLO DEL PROYECTO**

### **FASE 1: FASE DE EXPLORACIÓN O ANÁLISIS DEL PROYECTO.**

- **Situación actual:** En este paso, se debe realizar un estudio formal relacionado con el sistema de comunicación que actualmente se usa, utilizando técnicas de recolección de datos permitiendo así conocer el sistema para realizar con mayor facilidad la construcción de un modelo que mejore las deficiencias y satisfaga todos los requerimientos, tanto actuales como aquellos que se logren identificar.
- **Definición de requerimientos:** Permite identificar las expectativas en cuanto a los servicios prestados y el nivel de desempeño que experimentarán los usuarios con los nuevos equipos, esquemas y configuraciones.

### **FASE 2: DISEÑO DE LA SOLUCIÓN PROPUESTA.**

- **Diseño:** En esta etapa se debe determinar con precisión lo que se desea hacer y justificar el desarrollo de la misma, basándose en la información obtenida en el paso anterior (situación actual), es decir, se procede a la elaboración del diseño del nuevo modelo de red, VLAN, políticas de seguridad, esquema de seguridad a través de cámaras de video.
- **Adquisición de la solución:** Aquí se define el proceso de adquisición de los equipos de la solución propuesta.

### **FASE 3: INSTALACIÓN Y PRUEBAS.**

#### **Instalación y configuración de hardware y software**

La instalación se realiza de acuerdo al diseño de red, diseño de seguridad, configurando toda la plataforma de comunicaciones y seguridad como lo indique el diseño.

### **Pruebas**

Para comprobar el funcionamiento de los equipos y software, se deben definir una serie de pruebas pilotos para la red, seguridad.

### **Elaboración de informes**

Esta actividad consiste en realizar la documentación referente a la instalación de los equipos, configuraciones realizadas en los equipos, políticas, análisis de tráfico y manual de recomendaciones.

## **FASE 4: WEB SITE DEL CENTRO DE ESTUDIOS DE TELECOMUNICACIONES.**

Para el diseño y desarrollo del sitio Web del Centro de Estudios de Telecomunicaciones, se llevaron a cabo mlos siguientes pasos:

### **Paso 1: ANÁLISIS.**

El objetivo de este paso es conocer las necesidades iniciales de la aplicación, definir los parámetros bajo los cuales se debe basar el sistema y finalmente familiarizarse con el dominio de las herramientas a utilizar.

- Descripción del Perfil del Usuario: El objetivo principal de esta etapa es decidir o determinar a que tipo de usuario va dirigido el sistema.

- **Campo de Acción:** Cuando se desarrollan sistemas de información, ya sean tradicionales o aplicaciones Web, es muy importante determinar el alcance o el radio de acción donde tendrá impacto la aplicación.
- **Determinación de requerimientos funcionales:** Esta etapa describe las actividades a ser realizadas por el usuario con la ayuda de la aplicación.
- **Determinación de requerimientos de información:** En esta etapa se identifica la información requerida por el usuario para la realización de sus tareas.
- **Determinación de requerimientos de interacción:** Esta etapa describe las características de la interfaz entre el usuario y el sistema, así como tipos y medios de entradas y salidas de datos requeridos.
- **Determinación requerimientos de desarrollo:** En esta etapa se especifican las herramientas y recursos (hardware y software) requeridas para el desarrollo y operación del sistema.

## **Paso 2: DISEÑO.**

En este paso se diseña la estructura de la intranet, cada una de las unidades que la componen y los ítems que conforman cada una de las unidades. Esta fase culmina con el desarrollo de un prototipo que ilustra la estructura del Web Site y su interacción con el usuario.

- **Diseño de la estructura:** El diseño de la estructura se basa en la descomposición del Web Site en secciones o áreas de desarrollo, la elaboración del modelo conceptual de cada sección y el diseño de la estructura interna de cada una de estas secciones.
- **Diseño de las unidades de información:** El diseño de las unidades de información consiste en la especificación del contenido de cada unidad. Este diseño se basa netamente en la recopilación de datos anteriormente realizada, sirviendo como punto de partida para la realización de cada módulo o unidad de información.

- **Diseño de ítems de información:** El diseño de ítems de información es el paso en el cual se especifica el arte utilizada en la conformación de las unidades de información.

### **Paso 3: DESARROLLO.**

En este paso se procede al ensamblaje de los prototipos anteriormente diseñados de cada una de las unidades de información requeridas para la integración del sistema. Este paso culmina con un ciclo evolutivo y correctivo del sistema.

- **Desarrollo de las unidades de información:** Es la producción de cada uno de los ítems de información que finalmente pasarán a componer el Web Site. Una vez finalizada la producción de ítems las unidades de información deben ensamblarse en el prototipo diseñado anteriormente.
- **Ciclo evolutivo y correctivo:** Este paso consiste en la validación, evolución y aceptación final del proyecto con el objetivo de asegurarse que éste satisface los requerimientos impuestos en la puesta en marcha del proyecto.

### **Paso 4: IMPLANTACIÓN.**

- **Luego de realizar las pruebas, corregir los errores y hacer los ajustes necesarios,** se procede a implantar la aplicación web para su utilización final por parte de los usuarios.

## CAPÍTULO IV

### PRESENTACIÓN Y ANÁLISIS DE LOS RESULTADOS

#### FASE 1: FASE DE EXPLORACIÓN O ANÁLISIS DEL PROYECTO

##### **Situación actual:**

En esta fase se estudió todo lo relativo a la infraestructura tecnológica que se encontraba en funcionamiento en el Edificio Jan Deketh (Edificio Principal) de Centro de Estudios de Telecomunicaciones de la empresa en estudio, a través de técnicas de recolección de datos (entrevistas y observación directa) se identificaron todos los ítems necesarios para luego plantear el diseño de la solución. A continuación se presenta la información referente al levantamiento de información:

#### 1. Red Física:

La red física del Edificio Jan Deketh del Centro de Estudios de Telecomunicaciones de la empresa en estudio, cuenta con una red local, que posee aproximadamente 300 estaciones de trabajo. Esta red está constituida por una red heterogénea con *switches* marca 3Com Superstack II 3300 XM, Netgear JFS524 y concentradores (*hubs*) marca Cisco serie 400 de 24 puertos distribuidos en su planta baja, primer y segundo piso.

Con relación a los *switches* y *hubs*, éstos no forman parte del estándar de equipos utilizados actualmente por la empresa en estudio, y presentan hasta ahora una serie de inconvenientes ocasionando intermitencias y caídas en la red LAN, por otro lado, los *hubs* no están en capacidad de poder soportar una cantidad considerable de

clientes accediendo a aplicaciones simultáneamente. El grado de obsolescencia de estos equipos es del 100%, ya que los equipos están discontinuados por parte del proveedor (3Com, Netgear, Cisco), no cuentan con repuestos y presentan dificultades para recibir el soporte técnico adecuado. En la siguiente tabla se muestra las características principales de la red LAN existente en el Centro de Estudios de Telecomunicaciones de empresa en estudio:

<b>CARACTERÍSTICAS</b>	<b>TIPO</b>
Backbone	Red conmutada colapsada en <i>switches</i> y <i>hubs</i> .
Tipo de red	10/100 base T.
Cableado	UTP nivel 5.
Velocidad	10/100 Mbps.
Conectores	RJ45.
Topología	Configuración estrella.
Método de acceso al medio MAC	Ethernet.
Protocolos	TCP/IP.
Sistemas operativos de red	Microsoft Windows 2003 Server.
Routers	Cisco 1700.
Tipo de <i>switches</i> y <i>hubs</i>	3Com, Netgear, Cisco.

Tabla IV.1. Características red LAN del Centro de Estudios de Telecomunicaciones

A continuación se muestra el esquema actual de la red LAN existente en el Centro de Estudios de Telecomunicaciones de la empresa en estudio:

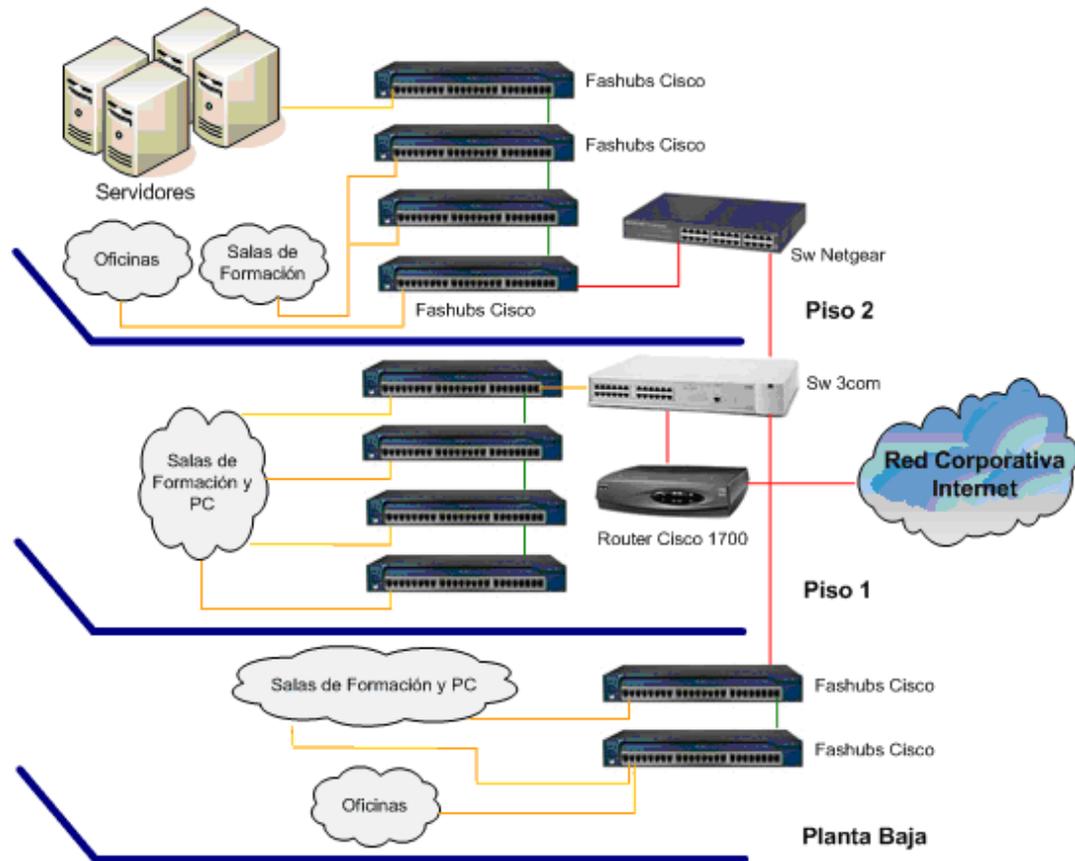


Figura IV.1. Esquema de red LAN actual del Centro de Estudios de Telecomunicaciones

- **Hardware de las estaciones de trabajo de los usuarios:**

En relación a las estaciones de trabajo con que cuentan los usuarios del Centro de Estudios de la empresa en estudio, se disponen de equipos IBM compatible *desktop*. En las siguientes tablas se pueden observar las configuración básicas de cada uno de ellos:

<b>IBM ThinkCentre MT-M 8141-27S</b>		
<b>Características</b>	<b>Procesador</b>	<b>Cantidad</b>
1 Mb de cache. Tarjeta madre Intel 915G Express. Memoria RAM 512 Mb Disco duro 80. GB Tarjeta de video 64 Mb integrada. Unidad de DVD-ROM IDE 16X Floppy de 3.5 Tarjeta de red 10/100 Mbps Tarjeta de sonido Teclado, mouse óptico Monitor IBM 17" pantalla Plana LCD Sistema operativo Windows XP Profesional	Procesador Intel Pentium 4, 3 GHz	32

Tabla IV.2. Configuración IBM ThinkCentre MT-M 8141-27S

<b>IBM ThinkCentre MT-M 8188-37S</b>		
<b>Características</b>	<b>Procesador</b>	<b>Cantidad</b>
1 Mb de cache. Memoria RAM 256 Mb Disco duro 80. GB Tarjeta de video 16 Mb integrada. Unidad de CD-ROM IDE 48X Floppy de 3.5 Tarjeta de red 10/100 Mbps Tarjeta de sonido Teclado, mouse PS2 Monitor IBM 15" Sistema operativo Windows XP Profesional	Procesador Intel Pentium 4, 2.8 GHz	259

Tabla IV.3. Configuración IBM ThinkCentre MT-M 8188-37S

- **Software de las estaciones de trabajo:**

En relación al *software* utilizado en las estaciones de trabajo es importante dividir el utilizado en las oficinas administrativas y las salas de PC'S o salas de formación destinadas para realizar los entrenamientos.

<b>Software utilizado en las estaciones de trabajo</b>	
<b>Oficinas Administrativas</b>	<b>Laboratorios o salas de Formación</b>
Windows XP Proffesional	Ambientes de entrenamientos de aplicaciones propietarias de la Corporación en estudio:
Sap R/3	Sap R/3
Microsoft Office	Sistema integral de la red. (Sir)
Microsoft Outlook	Asap
Antivirus corporativo Trend Micro	Tas
Aplicaciones Web propietarias	Boos
Sapportals	Siscom2k
	Sise.
	Gestores.
	Windows XP.

Tabla IV.4. Software utilizado en las estaciones de trabajo

- **Identificación de los Servidores existentes en el Centro de Estudios de Telecomunicaciones de la empresa en estudio:**

A continuación se describen los servidores de red que se encuentran actualmente funcionando en el Centro de Estudios de Telecomunicaciones, cuyas funciones son las siguientes:

- a. Servidor de aplicaciones (Appli1):

#### **Características**

Marca: HP.

Modelo: Proliant ML300.

Procesador: Dual-Core Intel Xeon 5130 Processor (2.0 GHz, 65 Watts, 1333 FSB)

Disco duro: 2 discos duros de 80 GB y 1 disco de 160 GB.

Memoria RAM: 1 GB.

Sistema operativo: Windows Server 2003 Enterprise Editions.

Utilidad: En este servidor se encuentran aplicaciones desarrolladas internamente para gestionar algunos procesos internos tales como manejo de historiales académicos, gestión de inventario de equipos, gestión con proveedores, entre otros.

b. Servidor Web (WebAppli2):

**Características**

Marca: HP.

Modelo: Proliant ML300.

Procesador: Dual-Core Intel Xeon 5130 Processor (2.0 GHz, 65 Watts, 1333 FSB)

Disco duro: 2 discos duros de 80 GB.

Memoria RAM: 1 GB.

Sistema operativo: Windows Server 2003 Enterprise Editions.

Utilidad: Servidor utilizado para alojar aplicaciones web, así como el sitio web del Centro de Estudios de Telecomunicaciones de la empresa en estudio.

c. Servidor de Impresión (ImpAppli3):

**Características**

Marca: Compaq.

Modelo: Proliant 2500.

Procesador: Pentium III 600MHz. (Cantidad de procesadores: 2).

Disco duro: 4 discos duros de 20 GB.

Memoria RAM: 1 GB.

Sistema operativo: Windows 2000 Server.

Utilidad: Servidor utilizado para gestionar los servicios de impresión a través de impresoras de red instaladas en el Centro de Estudios de Telecomunicaciones de la empresa en estudio.

d. Servidor de Bases de Datos (BasAppli1):

**Características**

Marca: HP.

Modelo: Proliant ML300.

Procesador: Dual-Core Intel Xeon 5130 Processor (2.0GHz, 65 Watts, 1333 FSB)

Disco duro: 2 discos duros de 80 GB.

Memoria RAM: 1 GB.

Sistema operativo: Windows Server 2003 Enterprise Editions.

Utilidad: Servidor utilizado para gestionar los servicios de bases de Datos tiene instalado el manejador de bases de datos SQL Server 2000.

- **Impresoras de Red:**

El Centro de Estudios de Telecomunicaciones de la empresa en estudio, cuenta con un total de 4 impresoras de red cuyas características se muestran en la tabla siguiente:

<b>Impresoras de Red HP Laserjet 3380</b>	
<b>Características</b>	<b>Cantidad</b>
Funciones: Escaneado en color, impresión en blanco y negro, escaneado en blanco y negro, copiado en blanco y negro, faxes en blanco y negro Velocidad de impresión: 19 ppm Tipo de procesador: Motorola Coldfire® v 4e Velocidad del procesador: 240 Mhz Memoria de Serie: 32 Mb Tipo de digitalización: Escáner plano, ADF, escaneado en color Velocidad de fax (A4): 33,6 kbps (3 seg. por página) Velocidad máxima de copia (negro, A4): 19 ppm Conectividad: Servidor de impresión externo Jet Direct: y servidor de impresión wireless: HP Jetdirect: 170x, 175x, 300x, 380x, 500x, en3700, bt1300	4

Tabla IV.5. Características impresoras de red

## 2. **Red Lógica:**

Actualmente la red dispone de una arquitectura de dominio basada en la tecnología Microsoft Windows 2003 Server llamada XXX.com.ve. Todos los servidores así como los PC's que se encuentran en el Centro de Estudios de Telecomunicaciones de la empresa en estudio, son miembros del dominio principal XXX.com.ve, por otro lado el protocolo de red utilizado es el TCP/IP, con servicios DNS (sistema de nombre de dominios) y WINS (servicio de nombre Internet de Windows).

Por otra parte el Centro de Estudios de Telecomunicaciones de la empresa en estudio, cuenta con un segmento de direcciones IP fijas para ser gestionadas internamente en el caso que se requieran exclusivamente para las diferentes maquetas asociadas a las nuevas tecnologías. Adicionalmente se dispone de un grupo de direcciones IP entregadas por un servidor DHCP. Es importante acotar que las salas de PC'S utilizan las direcciones IP suministradas por dicho servidor.

El rango de direcciones IP certificadas corresponden a los bloques Clase B/128.

- Segmento de Red 163.196.41.128/128

	Red Clase B/128
Dirección:	163.196.41.129
Máscara:	255.255.255.128
Rango de Host:	163.196.41.129
	163.196.41.254
Broadcast:	163.196.41.128
	163.196.41.255

### 3. Red de área amplia WAN:

La red de área amplia (WAN) del Centro de Estudios de Telecomunicaciones de la empresa en estudio, cuenta con un enlace dedicado de 2.048 Mbps, el cual le permite comunicarse con el resto de las sedes que dispone la empresa en estudio a nivel nacional, proporcionando el servicio de Internet y para ello se dispone de un *Router* marca Cisco serie 1700. Es importante mencionar que el centro de Estudios de Telecomunicaciones, hace uso del *firewall* y *proxy* corporativo, los cuales no forman parte del alcance del proyecto.

#### **4. Cuartos de Telecomunicaciones y Cableado Estructurado:**

El Edificio Jan Deketh (planta baja, piso 1 y piso 2) del Centro de Estudios de Telecomunicaciones de la empresa en estudio, dispone de espacios dedicados al alojamiento de los componentes de la red, así como los servidores y componentes del cableado estructurado. Estos espacios se encuentran físicamente acondicionados para asegurar el correcto funcionamiento del sistema. Los servidores cuentan con un sistema de protección en caso de ocurrir interrupciones temporales de energía, lo que evita daños al software y hardware de dichos equipos. El acceso a cada uno de los cuartos de telecomunicaciones se encuentra restringido y las consolas de los servidores permanece bloqueada, lo que impide el acceso por parte de terceros.

Se cuenta con un sistema de canalización que se extiende en forma vertical y horizontal hasta las áreas de oficinas, salas de formación y PC'S mediante el uso de escalerillas, tuberías y canaletas, las cuales cumplen una importante función, ya que garantizan la integridad física del cable, además de cubrir al 100% cada uno de los pisos que conforman el edificio Jan Deketh del Centro de Estudios de Telecomunicaciones.

No existe documentación parcial de planos con la distribución del cableado, así como la conexión de los dispositivos que forman parte de la red. No existe identificación de los puntos de red, lo cual dificulta el desempeño del administrador de la red al momento de llevar a cabo las labores de mantenimiento o detección de fallas de conexión de las estaciones.

El cuarto de telecomunicaciones del piso 2 de la edificación posee un switch Netgear JFS524 con 24 puertos a 100 Mbps y un total de 4 Fasthubs Cisco serie 400 con 24 puertos de 10 Mbps. El cableado de las salas que existe en este piso es UTP

categoría 6, con norma 568B y existen 83 puntos de red, 74 PC'S y 2 impresoras de red en este piso. El switch Netgear está conectado en cascada con cada uno de los 4 Fasthubs Cisco serie 400, utilizando un puerto de 100 Mbps.

El cuarto de telecomunicaciones del piso 1 de la edificación concentra la mayor cantidad de puntos de red, puesto que en este piso se ubican el 94% de los laboratorios de PC'S destinados a realizar los entrenamientos en los sistemas propietarios de la empresa en estudio. Aquí se encuentra un switch 3Com Superstack II con 24 puertos a 100 Mbps, el cual está conectado al router Cisco serie 1700 y un total de 4 Fasthubs Cisco serie 400 con 24 puertos de 10 Mbps. En este piso se encuentran ubicados en la escalerillas del cableado un grupo adicional de 5 Fasthubs Cisco serie 400 de 24 puertos, los cuales distribuyen en cascada las conexiones a una buena parte de los Pc's ubicados en los laboratorios. El cableado en este piso es UTP categoría 5 con norma 568B y existen 191 puntos de red y 186 PC'S en este piso. El switch Netgear está conectado en cascada con cada uno de los 4 Fasthubs Cisco serie 400, utilizando un puerto de 100 Mbps. Todo esto impide garantizar la correcta operación del tráfico de redes ya que representan cuellos de botella y posibles puntos de fallas que se hacen difíciles de detectar.

El cuarto de telecomunicaciones de la planta baja de la edificación posee 2 Fasthub Cisco serie 400 de 24 puertos a 10 Mbps. Uno de ellos está conectado mediante cable UTP al switch 3Com Superstack II de 24 puertos a 100 Mbps. El otro fasthub se encuentra conectado en cascada al primero, estos distribuyen las conexiones a las oficinas administrativas que se ubican en esta planta, la sala de formación y PC'S. El cableado en este piso es UTP categoría 6 con norma 568B y existen 42 puntos de red, 34 PC'S y 2 impresoras de red en este piso. La topología utilizada es en estrella para cada piso de la edificación.

El cableado vertical: se tiene cable UTP categoría 5 con norma 568A. Cada switch está conectado con el núcleo (core) de la red y dicho núcleo esta formado por 2 *switches* Netgear JFS524 y 3Com Superstack II.

Los cuartos de cableado existentes cumplen con el estándar a excepción de algunos componentes que están fuera de la norma (Norma EIA/TIA 568) o discontinuados por los fabricantes. Por otra parte debe sustituirse los componentes de cableado estructurado que existe en algunas salas de PC'S del piso 1 del edificio Jan Deketh del Centro de Estudios, ya que no cumplen con el estándar de marca Panduit establecido por la empresa en estudio.

## 5. Servicios:

Los servicios ofrecidos por el Centro de Estudios de telecomunicaciones de la empresa en estudio, pueden clasificarse o dividirse en función de a quién van dirigidos. Es por esta razón entonces que se tienen los siguientes servicios:

- Servicios Corporativos: estos van dirigidos a los usuarios que pertenecen a la Corporación (empleados) y proveedores (asesores, soporte técnico, etc.). Entre los servicios prestados se tienen: Correo corporativo, acceso vía Internet, sistemas de información: Nómina, Finanzas, entre otros.
- Servicios al Cliente: esta plataforma está orientada a los clientes que hacen uso de los servicios prestados por la Corporación. En su mayoría de realizan pruebas y demostraciones a clientes para lograr realizar ventas exitosas.

## 6. Sistema de Cámaras de Vigilancia.

Actualmente el Centro de Estudios de Telecomunicaciones de la empresa en estudio, no cuenta con un sistema de vigilancia a través de cámaras de video que ofrezcan mayor seguridad física a las personas que laboran y hacen uso de dicho centro, así como el resguardo de los diferentes equipos y componentes que forman parte de la plataforma tecnológica.

## 7. Aplicación Web del Centro de Estudios de Telecomunicaciones de la empresa en estudio:

En necesario crear una aplicación Web relacionada con los servicios que ofrece el Centro de Estudios de Telecomunicaciones a fin de ofrecer toda la información al personal de la empresa.

### Definición de requerimientos:

A continuación se describen en términos generales los requerimientos resultado del levantamiento de información realizado entre los usuarios, administradores y operadores de la plataforma tecnológica del Centro de Estudios de Telecomunicaciones de la empresa en estudio.

- Documentación: Una adecuada documentación de la infraestructura para garantizar un servicio eficiente y una pronta atención a requerimientos y fallas.
- Disponibilidad: Un servicio operativo con un porcentaje de disponibilidad mayor a 80%.

- **Confiabilidad:** Este elemento considerará el problema del transporte de la información a través de la red, mediante la selección adecuada de los elementos de comunicación: protocolos, dispositivos de transmisión, diseño lógico de interconexión, tecnología apropiada, entre otros.
- **Tiempo de Respuesta:** Debido a las características de distribución de procesos y sistemas en arquitectura cliente-servidor. Este es un factor relevante que debe ser tomado en cuenta.
- **Servicio:** En este punto es importante contar con un buen esquema que permita escalabilidad y flexibilidad a la hora de expansiones y/o adiciones de puntos posteriores a la implantación inicial.

A un nivel más detallado, y con el objetivo de cumplir con los aspectos mencionados surgen los siguientes requerimientos:

- Estudio de marcas o fabricantes de equipos con amplia representación y posicionamiento en el mercado tecnológico del país.
- Control de cambios y acceso a la red a través de implantación de funciones de seguridad estándar, tal como la implementación de redes VLAN para la segmentación del tráfico interno de la red.

En cuanto a la infraestructura de comunicaciones:

- Flexible en cuanto a los equipos a conectar a la infraestructura existente.
- Debe ser confiable.
- Debe ser escalable, en cuanto a velocidad e incremento de capacidad
- Permitir su administración a través del protocolo estándar (TCP/IP).
- Soportar técnicas que permitan realizar un uso eficiente del ancho de banda.

- Capacidad instalada para crecimiento flexible en el tiempo, en cuanto a la adición de nuevos dispositivos, equipos y servicios.
- Flexibilidad para realizar la reconfiguración lógica según se requiera.

En cuanto al software:

- Uso eficiente del ancho de banda

En cuanto a la seguridad:

- Permitir el acceso a todas las aplicaciones de la red corporativa, que el usuario tenga autoridad a acceder.
- Garantizar la integridad y confidencialidad de los datos.

## **FASE 2: DISEÑO DE LA SOLUCIÓN PROPUESTA.**

### **1. Red LAN.**

El diseño de la solución planteada para el modelo de red está basada en tecnología Cisco, ya que esta marca forma parte del estándar adoptado por la empresa en estudio, en la implantación de redes Lan en sus diferentes sedes a nivel nacional, a esto se une el hecho de que existe una gran cantidad de personal técnico capacitado para resolver problemas técnicos que puedan presentarse en esta tecnología.

Debido al nivel de obsolescencia de los equipos de datos (*hubs* y *switches*) y en base a las limitaciones que estos presentan, será necesario reemplazarlos en su totalidad por equipos *switches* Cisco modelo 2950, y 3550. Dichos equipos serán compatibles entre sí, lo que hace más fácil la administración y mantenimiento de los

mismos. Una vez instalados y configurados los equipos propuestos será posible entregar la administración de la red LAN del Centro de Estudios de Telecomunicaciones al Centro de Operaciones de Monitoreo Corporativo, desde donde remotamente podrán realizar funciones de monitoreo identificar y prevenir posibles fallas de congestión, errores y tráfico.

A continuación se muestran algunas especificaciones técnicas de los equipos de la serie 2950 Y 3550, así como la cantidad necesarias para la implantación:

<b>Cisco Catalyst 2950 24 puertos</b>		<b>Cantidad</b>
<b>Características</b>		
Peso:	3 kg	15
Memoria RAM:	16 Mb SDRAM	
Memoria Flash:	8 Mb	
Cantidad de puertos:	24 x Ethernet 10Base-T, Ethernet 100Base-TX	
Velocidad de transferencia de datos:	100 Mbps	
Protocolo de interconexión de datos:	Ethernet, Fast Ethernet	
Protocolo de gestión remota:	SNMP, RMON, Telnet	
Modo comunicación:	Semidúplex, dúplex pleno	
Características:	Monitorización en red, capacidad duplex, enlace ascendente, soporte VLAN, activable, apilable	
Cumplimiento de normas:	IEEE 802.3, IEEE 802.3u, IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p, IEEE 802.3x, IEEE 802.1x	
Alimentación:	CA 120/230 V CA 110/220 V $\pm$ 10% ( 50/60 Hz )	
Tecnología de conectividad:	Cableado	
Tamaño de tabla de dirección MAC:	8k de entradas	
Indicadores de estado:	Estado puerto, actividad de enlace, estado de colisión, velocidad de transmisión del puerto, modo puerto duplex, ancho de banda utilización %, alimentación	

Tabla IV.6. Características técnicas Cisco Catalyst 2950

<b>Cisco Switch Catalyst 3550 24 puertos</b>	
<b>Características</b>	<b>Cantidad</b>
Peso: 5 kg Memoria RAM: 64 Mb (instalados) / 64 Mb (máx.) Memoria Flash: 16 Mb (instalados) / 16 Mb (máx.) Cantidad de puertos: 24 x Ethernet 10Base-T, Ethernet 100Base-TX Velocidad de transferencia de datos: 100 Mbps Protocolo de interconexión de datos Ethernet, Fast Ethernet Ranuras vacías: 2 x GBIC Protocolo de gestión remota SNMP 1, SNMP 2, RMON 1, RMON 2, SNMP 3 Modo comunicación: Semidúplex, dúplex pleno Características: Capacidad duplex, enlace ascendente, auto-sensor por dispositivo, Encaminamiento IP, soporte de DHCP, negociación automática, soporte VLAN, activable, apilable Cumplimiento de normas: IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.1w, IEEE 802.1x, IEEE 802.1s Alimentación: CA 120/230 V CA 100/240 V ( 50/60 Hz ) Tamaño de tabla de dirección: MAC 8k de entradas Indicadores de estado: Estado puerto, velocidad de transmisión del puerto, modo puerto duplex	1

Tabla IV.7. Características técnicas Cisco Catalyst 3550

La plataforma propuesta se divide en tres aspectos de la red según los niveles funcionales definidos por Cisco Systems, para redes locales:

### **1. Nivel de Acceso. (SW Capa 2, 10/100Mbps).**

La capa de acceso es el nivel donde los usuarios se conectan a la red. En este nivel se maneja tráfico local entre usuarios y recursos que se encuentran conectados directamente en esta capa, permitiendo la conexión de los segmentos locales al (*backbone*) de la red principal, permitiendo la conexión de puntos locales y distantes de la red en general.

En este nivel la red propuesta provee conexiones Ethernet conmutada de capa 2 (capa de enlace de datos) de 10/100 Mbps directo al usuario, para los apilamientos (stacking) entre equipos pertenecientes al mismo piso. Los equipos que llevarán a cabo esta función son los Cisco Catalyst serie 2950 de 24 puertos (ver figura IV.1).



Figura IV.2. Cisco Switch Catalyst serie 2950

## 2. Nivel de Distribución. (SW Capa 3, 1000Mbps).

La capa de distribución de la red, marca el punto entre la capa de acceso y la capa núcleo (core). La función primaria de esta capa es ejecutar la manipulación de paquetes para funciones de enrutamiento, filtrado y acceso a WAN. La capa de distribución puede verse como la capa que provee “políticas basadas en conectividad”. Para las funciones de enrutamiento y filtrado se seleccionó el equipo *router* 1841 (ver figura IV.2), el cual se encarga de comunicar las distintas subredes y VLAN definidas o por definir en la red.



Figura IV.3. Cisco *Router* 1841

A continuación se muestran algunas especificaciones técnicas del *Router* 1841.

<b>Cisco Router 1841</b>	
<b>Características</b>	<b>Cantidad</b>
Altura: 1.87 in. Ancho: 13.5 in Profundidad: 10.8 in Características: Funcionalidad DHCP, firewall integrado, IP Routing, IPSec, NAT, Uplink, VoIP. Peso: 6.2 lbs Memoria Flash Instalada: 32 Mb Memoria principal instalada: 128 Mb Network protocolos Soportados: DHCP, DNS, FTP, HTTP, SMTP (Simple Mail Transfer Protocol), SNMP, TCP/IP, Telnet. Número de puertos: 4 Soporte de arquitectura de red: Ethernet - 10 Mbps Twisted Pair (10BaseT), Ethernet - 100 Mbps Two-Pair (100BaseTX), Gigabit Ethernet - 1000 Mbps (1000BaseTX) Tipos de Puerto: DB-9, Ethernet-RJ-45, T1, USB - Universal Serial Bus 2.0 Indicadores de Status de Red: Activity Status, Link Status, Power, WAN Speeds Supported: 1 Gbps	1

Tabla IV.8. Características técnicas Cisco Router 1841

### 3. Nivel del Núcleo “Core” (SW Capa 2, 1000Mbps).

El nivel de núcleo (core) es el que se encarga de concentrar las conexiones provenientes de la capa de distribución para permitir la interacción con los servicios de la red, redundancia de conexión y acceso hacia otras rutas de la red. Para este diseño la capa de núcleo se seleccionó el equipo Catalyst serie 3550 (ver figura IV.3), que concentrará la conexión de todo el edificio, ya que ofrece la capacidad de un manejo robusto del ancho de banda de la red, teniendo en cuenta que soportará conexiones hasta 1 Gbps. Tiene orientación modular, lo cual le permite un crecimiento moderado que se ajusta al tamaño actual y futuro (según estimaciones y capacidad física del edificio) de la red del Centro de Estudios de Telecomunicaciones de la empresa en estudio.



Figura IV.4. Switch Cisco 3550

A continuación se presenta el modelo físico propuesto para dar solución a los problemas identificados en la fase del levantamiento de la situación del presente proyecto:

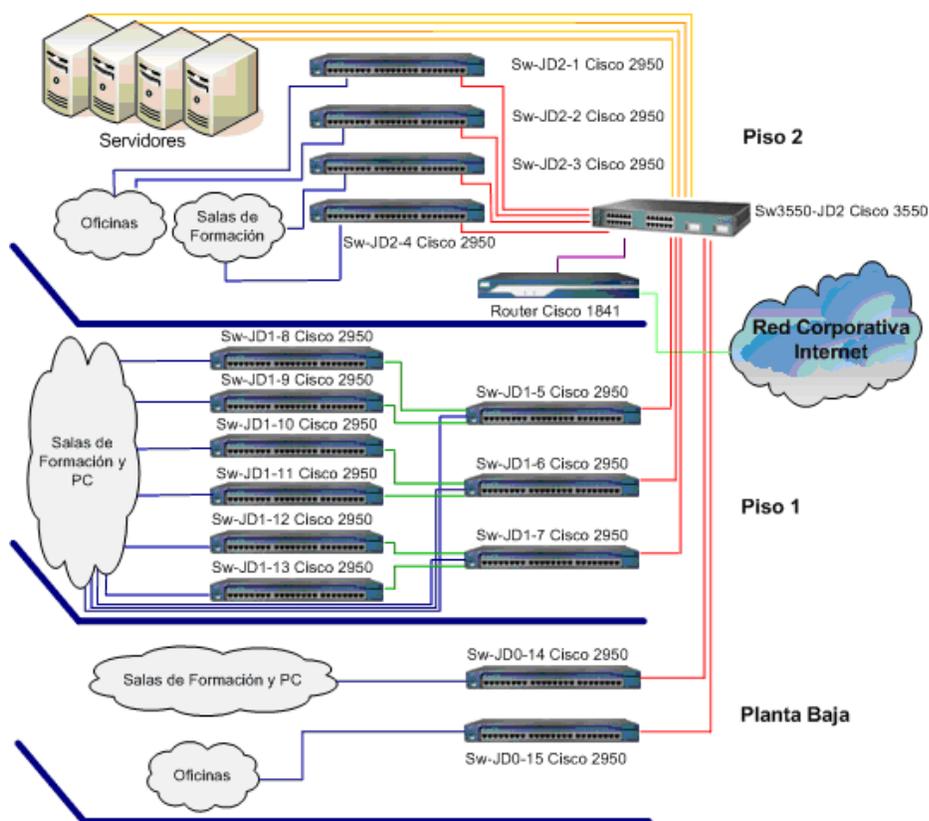


Figura IV.5. Esquema de conexión propuesto para la red LAN del Centro de Estudios de Telecomunicaciones

## 2. Esquema de configuración de VLAN.

Se propone la creación de 3 VLAN diferentes para de esta manera separar completamente a nivel de Ethernet las computadoras de las salas de PC'S, oficinas y servidores. Luego se debe establecer la conexión entre todas las VLANs e Internet a través del *router* con políticas de seguridad adecuadas para cada VLAN.

VLAN propuestas:

- 1.VLAN 1 (Vlan administrativa).
- 2.VLAN 2 (Oficinas).
- 3.VLAN 3 (Salas de Cursos).
- 4.VLAN 4 (Servidores).

Con el objetivo de lograr todo esto se seleccionó el *switch* Cisco Catalyst 3550 como *switch* principal. En este equipo se procederá a la creación y configuración de las VLANs necesarias para brindar protección a nivel de capa 2. Por otro lado es importante mencionar que este *switch* posee funciones de capa 3 que permiten establecer el enrutamiento IP entre todas las VLANs y el *router* Cisco 1841 hacia la red corporativa. En el *switch* Catalyst 3550 también se pueden establecer las políticas de seguridad para el enrutamiento IP entre las VLANs y el *router* principal.

A continuación se presenta el esquema de configuración de VLAN propuesto en el presente proyecto, el cual segmentará la red del Centro de Estudios de Telecomunicaciones para de esta manera aislar el tráfico generado en las oficinas, laboratorios de PC'S y servidores ofreciendo mayor seguridad a los usuarios y mejorando de esta manera significativamente el rendimiento de la red LAN.

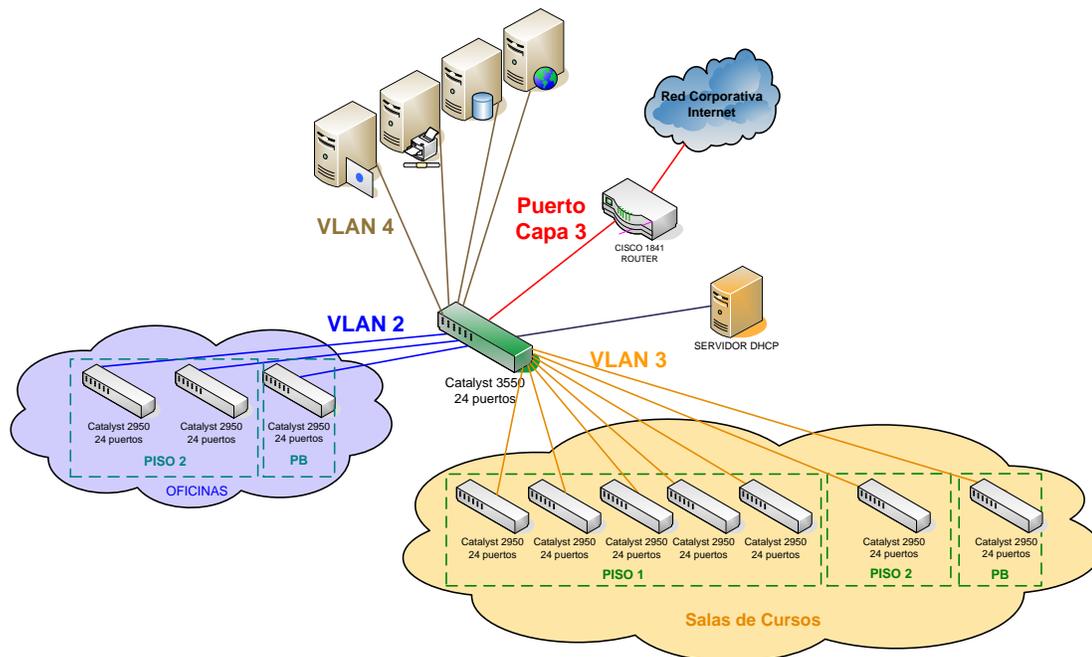


Figura IV.6. Esquema de conexión de VLAN

En el esquema anterior se puede observar que debe existir un servidor DHCP para la VLAN de las salas usadas para impartir cursos debido a que el protocolo DHCP se maneja con mensajes a nivel de Capa 2. La VLAN de servidores y VLAN de oficinas utilizarán direcciones IP fijas del segmento de red asignado.

### 3. Cableado Estructurado y Documentación de la Red LAN.

En relación al cableado estructurado y documentación de la red LAN se determinó en el análisis previo que no existe información alguna de manera que se pueda contar con un soporte de los medios disponibles actualmente para futuros proyectos de cambio o reestructuración del cableado de la red, en este sentido es necesario:

- Diseñar y desarrollar el diagrama de distribución de cableado estructurado de la red LAN actualmente operativa en el Centro de Estudios de Telecomunicaciones, especificando los puntos de red de todo el edificio y asignándole un código para su identificación.
- Especificar un código para la identificación de todos los swiches a instalar en la red LAN.
- Elaborar un plano con la identificación de todos los equipos actualmente conectados a la red LAN del Centro de Estudios de Telecomunicaciones, especificando sus principales características como marca, modelo, configuración IP, procesador y memoria en caso de que aplique.
- Especificar el medio por el cual se realizó el tendido del cable: escalerilla, tubería, tubo plástico flexible, ordenadores verticales y horizontales, entre otros.
- Sustituir el cableado vertical UTP nivel 5 que existe, así como en el piso 1 por cableado nivel 6. Una vez hecha la sustitución del cableado UTP nivel 5 por UTP nivel 6, se contará con una infraestructura de cableado acorde a los futuros requerimientos que se tendrán por parte de la tecnología de equipos, ya que soportará velocidades superiores a los 100 Mbps.

Tanto para la documentación de los equipos como para la documentación del cableado se realizarán los planos correspondientes para cada una de las plantas del edificio; estos planos se realizarán con la ayuda del *software* de Microsoft Visio 2003.

Con respecto al cableado se busca minimizar la tasa de fallas a nivel de puntos de red, así como ampliar el ancho de banda a nivel de estaciones de trabajo. Con la estandarización de la plataforma a cableado UTP nivel 6 se asegura la capacidad de transmisión de 10/100 Mbps en el nivel de acceso (y en un futuro a 1000 Mbps, lo que permitirá soportar los futuros requerimientos de las estaciones de trabajo especializadas: high performance computing). Así como una alta disponibilidad y confiabilidad de los servicios de datos.

Para el recorrido del cableado estructurado dentro de las salas de formación y PC'S se tomó en consideración la ubicación de los cables dentro de las canaletas además de tomar en cuenta una serie de reglas que garantizan un mejor funcionamiento del mismo y que se mencionan en la norma EIA/TIA 568 de las bases teóricas.

#### **4. Sistema de Cámaras de Vigilancia.**

El análisis efectuado en la etapa anterior determinó que el Centro de Estudios de Telecomunicaciones, carece de una infraestructura de cámaras de vigilancia que facilite al personal encargado de la seguridad el proceso de vigilancia de todas las áreas que lo conforman, de tal modo se pueda evitar o minimizar la pérdida de activos y poseer un registro de las actividades realizadas en áreas cuya seguridad se haya visto comprometida.

El sistema de cámaras de vigilancia que se propone consta de 16 cámaras distribuidas estratégicamente en los Edificios Arvelo y Jan Deketh del Centro de Estudios de Telecomunicaciones. Adicionalmente se instalarán 4 servidores de videos que permiten interconectar 4 cámaras a la vez. Estos servidores estarán conectados a

la red Lan del Centro de Estudios de Telecomunicaciones para que a través del software de gestión Cam Manager se pueda observar y gestionar la plataforma.

A continuación se presenta el esquema de conexión del sistema de cámaras de vigilancia propuesto:

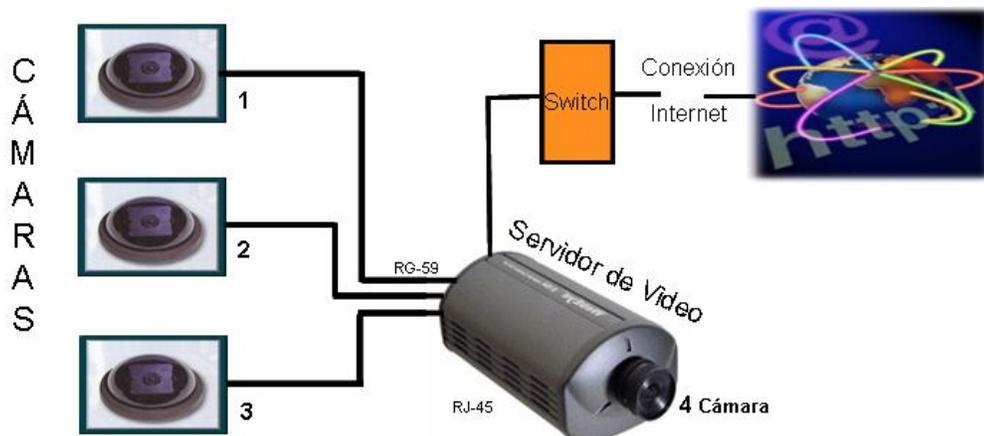


Figura IV.7. Esquema de conexión del sistema de cámaras de vigilancia

El *software* requerido para llevar a cabo la gestión del sistema de cámaras de vigilancia es el CamManager v 1.3.1. Este programa permite monitorear, grabar, reproducir y configurar los servidores de videos desde un equipo servidor destinado para ello. CamManager consta de cinco partes principales: monitoreo, reproducción, copia de seguridad, grabación de programa y alarma. Cada programa puede ser usado por separado:

- **Monitoreo:** La opción de monitoreo se utiliza para ver imágenes en tiempo real a través de las cámaras conectados a la red local o vía Internet. La pantalla de monitoreo puede ser dividida en 1, 4, 7, 10, 13, o 16 canales simultáneamente y soporta resoluciones de 720x486, 360x243, o 180x121.

- **Reproducción:** graba e imprime imágenes específicas, examina las imágenes grabadas en el PC y posee condiciones de búsqueda que pueden ser configuradas tales como cámaras, tiempo o alarmas. Esta opción permite agrandar las imágenes a través de una función digital de foco y soporta el formato de imagen BMP.
- **Copia de seguridad:** esta utilidad sirve para realizar copias de seguridad automáticamente de los datos guardados en los discos duros del servidor. Para ello se designan los parámetros de copia de seguridad y el tiempo de grabación. Se puede programar la duración determinada de la copia de seguridad (por ejemplo de las 12 a.m. a las 4 a.m.). Otra función importante es que se puede programar la supresión automática de archivos almacenados en los discos duros.
- **Grabación de programas:** permite grabar en tiempo real las imágenes procedentes de las cámaras de video.
- **Alarma:** Esta utilidad es opcional y sirve para monitorear el estado de las alarmas producto de la instalación de sensores en los accesos así como detectores de movimientos.

Los requerimientos necesarios para la instalación del software CamManager son los siguientes:

- Sistema Operativo: Microsoft Windows 2000 profesional/XP/Server 2003.
- CPU: Pentium III 600Mhz.
- Memoria: RAM 256 Mb.
- Resolución: 1024x768.
- Espacio de disco duro disponible: 50 megabytes.
- Copia de seguridad: 40 GB.
- Conectar a una red: TCP/IP
- Max conexiones de TCP/IP: 16 por el programa
- Max cámaras de visualización: 16 por el programa

- Max la solución: 720x486
- Pixeles de visualización: 1024x768

En la siguiente tabla se describe las características y cantidad de cámaras de vigilancia que se requieren según en diseño propuesto.

SUMINISTRO DE CCTV		
ITEM	DESCRIPCIÓN	CANTIDAD
	<p><b>MINIDOMO A COLOR MARCA PELCO MODELO ICS090-CR6</b></p> <ul style="list-style-type: none"> <li>• Integrada CCD 1/4", domo</li> <li>• Lente fijo de 6mm, iris manual.</li> <li>• Puede ser montada en superficies planas o empotradas en cielos rasos</li> <li>• Alta resolución de 480lrv</li> <li>• Modelo auto contenido e intuitivo para fácil instalación</li> <li>• Multivoltaje puede operar con con 24 o 12 vdc</li> <li>• Rotación manual de 360° pan y 180° tilt</li> <li>• Carcaza con domo con cúpula ahumada oscura tipo discreta</li> <li>• Sistema de proceso digital de señales (DSP)</li> <li>• Incluye plato adaptador para techos irregulares</li> <li>• Sensibilidad en escenas de baja iluminación de 1lux.</li> <li>• Incluye Fuente de poder 24VAC, Marca Pelco modelo TF2000 24vac, 20vA</li> </ul>	12
	<p><b>CAMARA FIJA A COLOR PELCO C3700H-2V21A, SERIE CAMERA PACK, MARCA PELCO, CARACTERÍSTICAS DE LA CÁMARA:</b></p> <ul style="list-style-type: none"> <li>• Tecnología SuperHAD</li> <li>• CCD Formato 1/3"</li> <li>• Lente Distancia Focal Variable de 3mm a 8mm</li> <li>• Resolución de de 480 LTV</li> <li>• Autoiris</li> <li>• Cuatro modos de balance de Blancos</li> <li>• Control de ganancia Automática</li> <li>• Selección de Gamma de colores</li> <li>• Compensación de luz trasera</li> <li>• Proceso digital de señales (DSP)</li> <li>• Alta sensibilidad en escenas de baja iluminación de 0,5lux obteniendo 80% de ganancia</li> <li>• Soporta temperaturas desde -10C hasta 60C</li> <li>• Fuente de poder TF2000 24VAC 20vA</li> <li>• Incluye base</li> </ul> <p><b>Incluye carcasa de uso exterior marca PELCO modelo EH2500/MT:</b></p> <ul style="list-style-type: none"> <li>• Tamaño 8", Norma Tipo Nema 4 estándar IP66</li> <li>• Construido en aluminio anodizado</li> <li>• Entradas protegidas para cables y alimentación</li> <li>• Fácil acceso y mantenimiento, incluye soporte o base para montaje en pared, Marca Pelco EM1450.</li> </ul>	4

Tabla IV.9. Características y cantidad de cámaras de seguridad adquiridas

A continuación se presenta los sitios estratégicos donde serán instaladas las cámaras de vigilancia:

### 1. Entrada del edificio Arvelo PB:

- Cámara fija N° 1 (permite visualizar el movimiento de todo el personal que ingresa o sale del edificio).
- Cámara fija N° 2 en pasillo. (permite visualizar el acceso a las maquetas de PB).

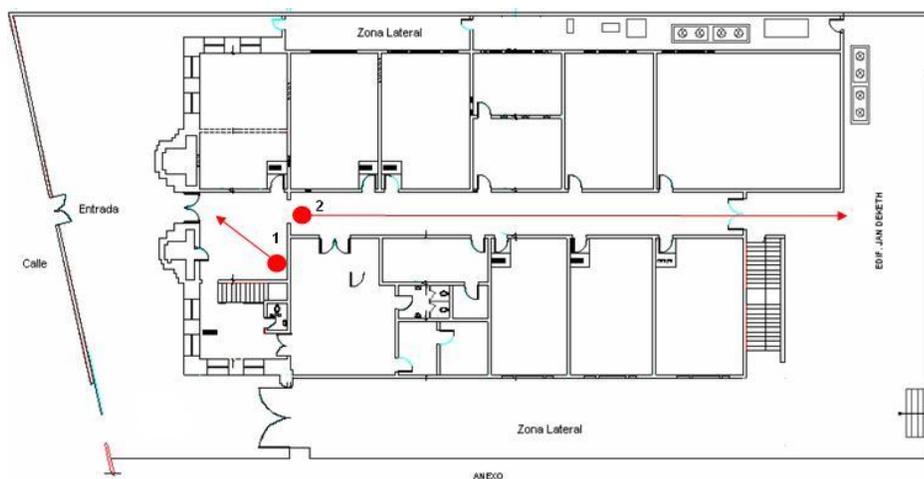


Figura IV.8. Ubicación de cámaras entrada edificio Arvelo planta baja

### 2. Edificio Arvelo planta alta:

- Cámara fija N° 3 (permite visualizar los accesos a las maquetas de la planta alta del edificio).
- Cámara fija N° 4 (permite visualizar el acceso de personas por la escalera proveniente de la entrada del edificio).

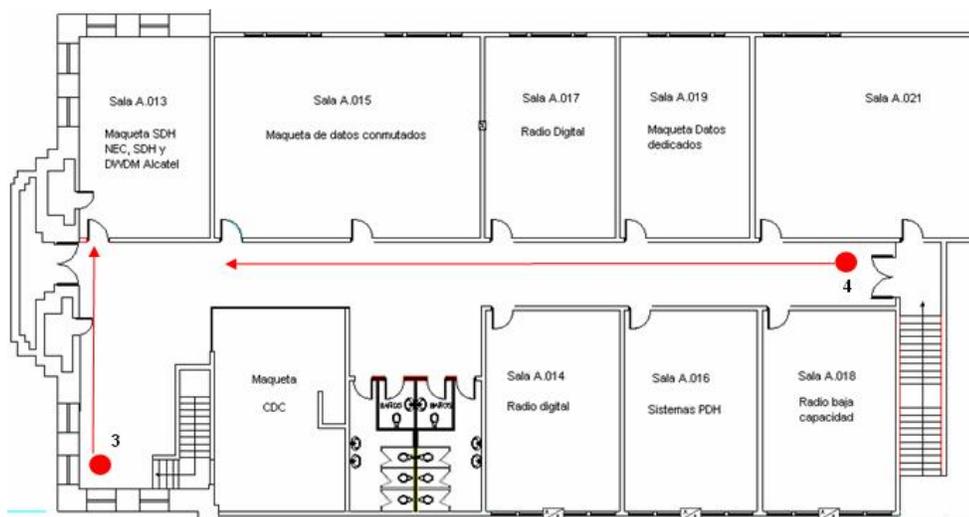


Figura IV.9. Ubicación de cámaras entrada edificio Arvelo planta alta

### 3. Azotea del edificio Arvelo:

- Cámara fija N° 5 (permite visualizar la parte lateral del CET).
- Cámara fija N° 6 (permite visualizar la parte posterior del CET)
- Cámara fija N° 7 (permite visualizar el acceso de personas y vehículos al edificio Arvelo.).
- Cámara fija N° 8 (permite visualizar el acceso al estacionamiento del Centro de Estudios de Telecomunicaciones de la Corporación en estudio).

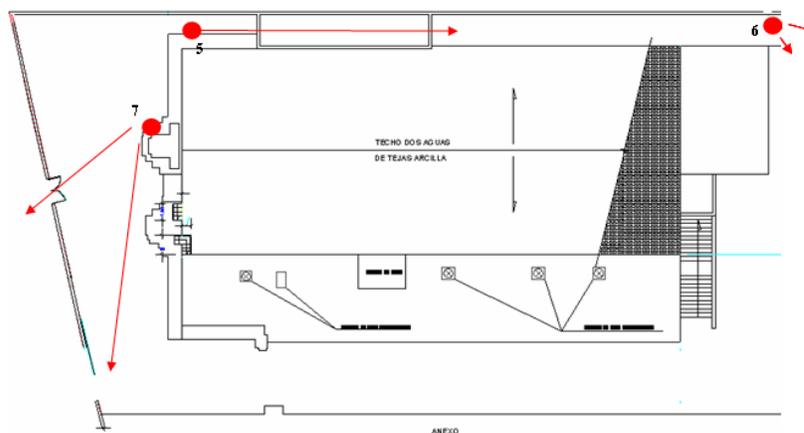


Figura IV.10. Ubicación de cámaras edificio Arvelo azotea 1.

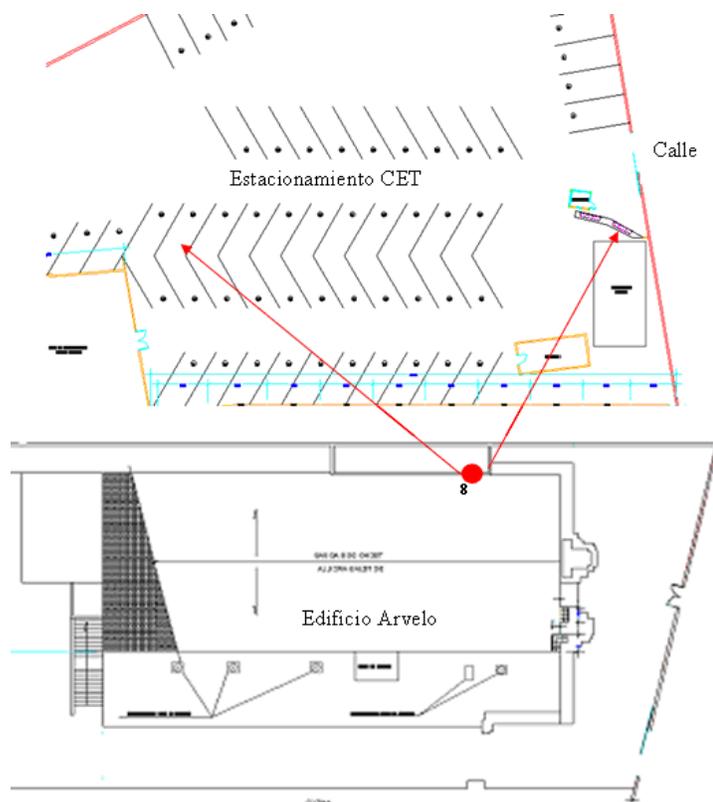


Figura IV.11. Ubicación de cámaras edificio Arvelo azotea 2.

#### 4. Piso 2 Edificio Jan Deketh:

- Cámara fija N° 8 (permite visualizar el acceso a las aulas JD 2.08, 2.09, 2.10 y 2.11).
- Cámara fija N° 9 (permite visualizar el acceso a las aulas JD 2.13- JD 2.17).
- Cámara fija N° 10 (permite visualizar el acceso a la sala JD 2.10 “Sala principal de telecomunicaciones y servidores”).
- Cámara fija N° 11 (permite visualizar el acceso a las oficinas JD 2.01 JD – JD 2.06)

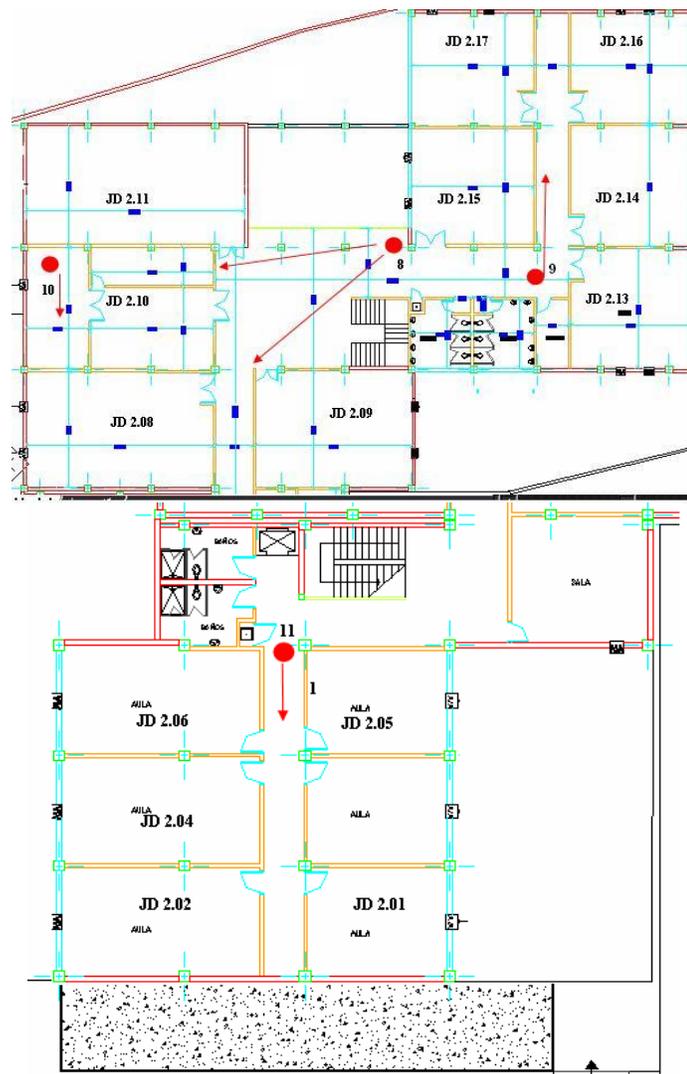


Figura IV.12. Ubicación de cámaras edificio Jan Deketh piso 2

### 5. Piso 1 Edificio Jan Deketh:

- Cámara fija N° 12 (permite visualizar el acceso a las aulas JD 1.08, 1.09, Sala Videoconferencia y JD. 1.11).
- Cámara fija N° 13 (permite visualizar el acceso a las aulas JD 1.13- JD 1.17).
- Cámara fija N° 14 (permite visualizar el acceso a las aulas JD 1.01 JD – JD 1.06).

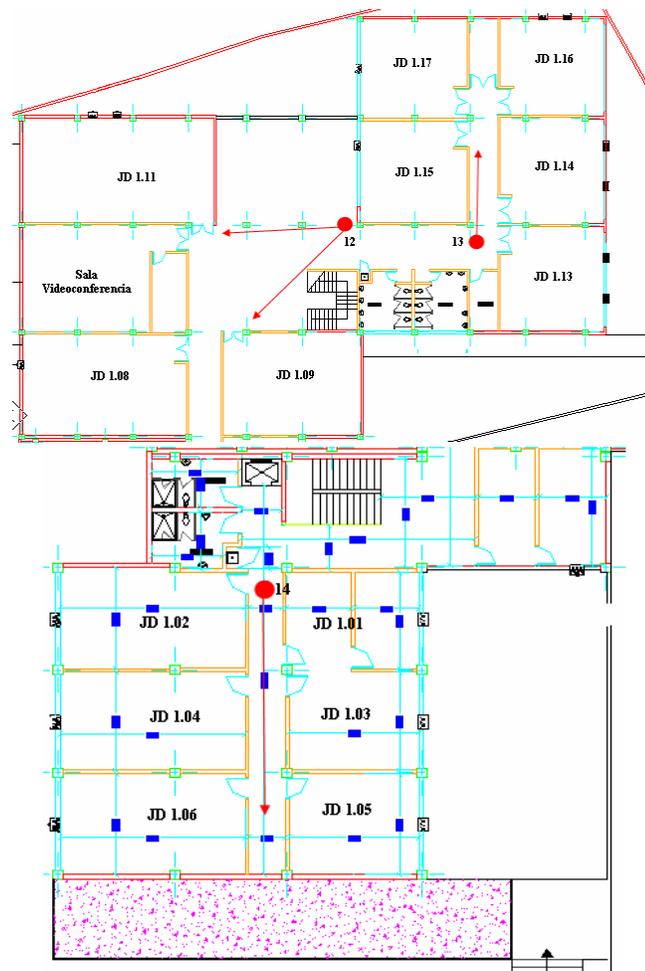


Figura IV.13. Ubicación de cámaras edificio Jan Deketh piso 1

#### 6. Planta Baja Edificio Jan Deketh:

- Cámara fija N° 15 (permite visualizar el acceso al edif. Jan Deketh).
- Cámara fija N° 16 (permite visualizar el acceso al área de almacén y parte posterior del estacionamiento).

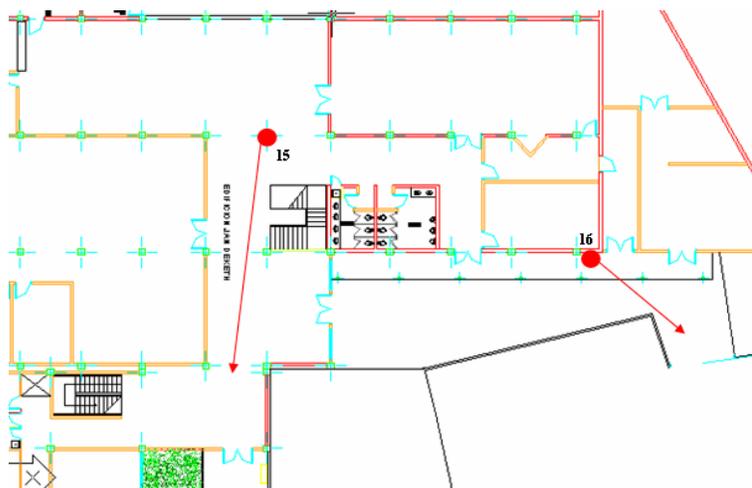


Figura IV.14. Ubicación de cámaras edificio Jan Deketh planta baja

Para la instalación del software de gestión del sistema de cámaras de vigilancia se utilizará el Servidor de Aplicaciones (Appli1), el cual técnicamente posee las características técnicas requeridas por la herramienta. Para poder almacenar las imágenes obtenidas a través de las cámaras de vigilancias en una resolución de pantalla de 360x243 se necesita 1Mb de espacio en disco aproximadamente por cámara por minuto, en este sentido, se requiere contar con un total de espacio en disco duro de 80.640 Gb por semana. Con este espacio se estaría almacenando en disco todas las imágenes detectadas por las 16 cámaras de vigilancia en un horario de 6:30am. a 6:30pm, de lunes a domingo. Se debe configurar el *software* de gestión para que automáticamente elimine la data con 8 días de antigüedad que se encuentre en el servidor, asegurándose de esta manera no exceder el espacio de disco que se tiene previsto en el servidor.

#### **Adquisición de la Solución:**

Una vez hecho los análisis de la situación actual, información y evaluación técnica/económica de beneficios del diseño propuesto, se elaboró un caso de negocios

el cual fue aprobado por la Gerencia del Centro de Estudios. Dicho caso de negocio disponía de toda la información técnica de los equipos y accesorios necesarios para la puesta en marcha del proyecto y fue entregado a la Gerencia de Compras de la empresa en estudio, para la ubicación de los diferentes proveedores, a fin de obtener las cotizaciones respectivas y realizar el análisis de la mejor oferta para la contratación y generación de la orden de compra correspondiente.

Todos los equipos y accesorios necesarios para la implantación del proyecto fueron adquiridos por varias empresas seleccionadas en base a las mejores ofertas en donde participaron 4 proveedores haciendo entrega de los equipos al Centro de Estudios de Telecomunicaciones.

### **FASE 3: INSTALACIÓN Y PRUEBAS**

#### **1. Red LAN.**

En la implantación de la red de área local LAN, los equipos se distribuyeron e instalaron mediante un control de cambios fuera del horario de oficina de la siguiente forma:

#### **Piso 2:**

Se procedió a instalar el equipo *switch* Catalyst 3550 en el cuarto de telecomunicaciones principal ubicado en el piso 2 del edificio Jan Deketh, sustituyendo al equipo *switch* marca Netgear. Este *switch* cumplirá las funciones de equipo principal que tenía el equipo 3Com ubicado en el piso 1 del edificio Jan Deketh. Por otro lado se instalaron 4 *switches* marca Cisco modelo 2950, los cuales sustituyeron a los cuatro Fashub marca Cisco que se encontraban funcionando en este piso. Todos los equipos fueron instalados en un rack 19" marca Panduit con todos sus

elementos de cableado estructurado según la norma establecida por la empresa en estudio. Es importante recordar que la conexión en cascada que se encontraba implantada en el Piso 2 degradaba el desempeño de la red para el acceso a Internet a medida que los equipos se encontraban conectados más abajo de la cascada. Por esta razón, las conexiones en cascadas fueron eliminadas, es decir, los cuatro *Switches* fueron conectados directamente al *switch* principal 3550.

Por otro lado se realizó la mudanza y sustitución del router 1700 que se encontraba en el cuarto de telecomunicaciones del piso 1 del Edificio Jan Deketh por el router marca Cisco modelo 1841, el cual fue instalado en el piso 2 de ese mismo edificio.

En la siguiente figura se puede observar los equipos instalados en el rack ubicado en cuarto de telecomunicaciones principal del piso 2 del edificio Jan Deketh del Centro de Estudios de Telecomunicaciones.



Figura IV.15. Armario de telecomunicaciones principal

**Piso 1:**

En este piso se procedió a instalar 3 switch marca Cisco modelo 2950 conectándolos por medio de cable UTP nivel 6 al switch principal (Cisco 3550) ubicado en el piso 2, adicionalmente se instalaron 6 switch marca Cisco modelo 2950 reemplazando en su totalidad todos los fashub que se encontraban en este piso.

**Planta Baja:**

En la planta baja del edificio Jan Deketh es donde existen menos clientes conectados a la red LAN, por lo que se reemplazaron los Fashub que se encontraban en este piso por 2 *switches* marca Cisco modelo 2950 conectados al switch 3550 por medio de cable UTP nivel 6.

En relación a la seguridad física de todos los equipos instalados la misma se encuentran garantizada, ya que para tener acceso físico a cualquiera de los cuartos de telecomunicaciones (capa de acceso) se necesita la llave y acceso por carnet, adicionalmente se instalaron cámaras de vigilancia que ofrecen mayor seguridad.

**2. Esquema de configuración de los *Switches* y VLAN.**

Para la configuración del switch Cisco Catalyst 3550 (Equipo principal) se utilizaron las siguientes herramientas y programas:

- Cable serial DB-9 - RJ-45 necesario para la configuración por consola. (incluido con el equipo).
- Cable de red directo (no cruzado) Cat 6 con conectores RJ-45
- Software “Cisco Network Assistant” disponible gratuitamente en la página oficial de Cisco: [www.cisco.com](http://www.cisco.com)

- Computador con Windows 2000/XP con software Hyperterminal, un puerto de red Ethernet y un puerto serial (RS-232)

Siempre que sea posible es recomendable reiniciar el switch desde cero para borrar toda la configuración que se le haya hecho anteriormente. En este sentido este procedimiento fue realizado para todos los swiches a instalar:

- Se conectó el *switch* a la corriente alterna y se esperó que los LEDs terminaran de parpadear.
- Se mantuvo presionado el botón MODE que se encuentra en el panel frontal del equipo durante 3 segundos. Todos los LEDs que se encuentran arriba de este botón se colocaron en verde. Una vez que comenzó a parpadear los LEDs se mantuvo presionado el botón por 8 segundos aproximadamente para reiniciar el equipo.

La configuración inicial del equipo se realizó por consola siguiendo los siguientes pasos:

- Se conectó el cable serial a la entrada señalada como CONSOLE (con conector RJ-45) que se encuentra en la parte posterior del equipo y al puerto serial (DB-9) del computador con el que va a configurar el equipo.
- Se abrió el programa *Hyper Terminal* que viene incluido con Windows. Este programa se encuentra haciendo click en la barra de inicio de windows: *Inicio>Programas>Accesorios>Comunicaciones>Hyper Terminal*.
- Se configuró una nueva conexión con el nombre prueba. Luego se seleccionó el puerto de comunicaciones serial que está utilizando (generalmente COM1), Velocidad de 9600 bps, ocho bits de datos, sin paridad, un bit de parada y control de flujo por hardware. Obsérvese la siguiente figura.

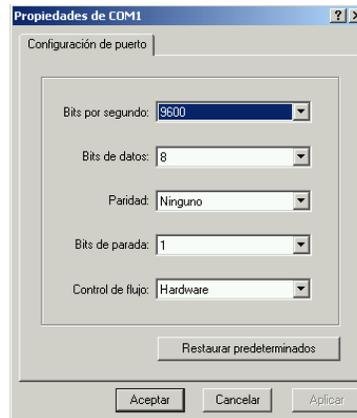


Figura IV.16. Configuración predeterminada para la consola. Hyper Terminal.

- Luego se hizo click en la pantalla principal (pantalla en blanco) y se presionó ENTER. Luego se aceptó configurar el equipo y se fijaron todos los nombres y claves según se fueron presentando. La opción que pregunta si el equipo va a manejar un cluster no fue seleccionada. Un cluster es un conjunto de *switches* que se administran de forma centralizada. Para el caso que se requiere en el Centro de Estudios de Telecomunicaciones, esto no es necesario.
- A continuación se presenta un ejemplo de la configuración de *switch*, por medidas de seguridad no se muestra la configuración real del equipo:

```

host name: Sw3550-JD2.
enable secret: XXXXXXXX.
enable password: XXXXXXXX.
virtual terminal password: XXXXXXXX.
IP: 163.196.41.230.
Subnet mask: 255.255.255.128.

```

- La dirección IP del equipo es la que permite la gestión mediante el software Cisco Network Assistant. Esta IP pertenece a la VLAN 1 (VLAN por

defecto). La VLAN 1 (Administrativa) es la única por la cual es posible gestionar el *switch*, por lo que, por seguridad, debe ser solo accedida por un puerto fijo del *switch* y no se debe usar para más nada. El puerto seleccionado para su administración fue el FastEthernet0/24.

Una vez realizada la configuración inicial del switch se utilizó el Cisco Network Assistant, para la creación de las VLAN según el diseño. Los pasos realizados para colocar en funcionamiento la gestión por CNA fueron los siguientes:

- Se conectó el cable de red directo (Cat5 o 6, RJ-45) desde el computador hasta cualquier puerto del panel frontal del *switch* que pertenezca a la VLAN de gestión (VLAN 1). Como el *switch* está siendo configurado por primera vez, todos los puertos pertenecen a la VLAN de gestión VLAN1.
- Se seleccionó una dirección IP fija al computador que pertenezca a la misma subred que la IP de la VLAN de gestión del switch (VLAN 1) y se fijó su respectiva máscara de subred.
- Se inició el programa CNA y se colocó la IP del switch principal para poder conectarse a él.
- Luego se colocó el nombre de usuario (admin) y la clave que se colocó como *enable secret*. El software desplegó su pantalla principal.

Las VLANs pueden crearse fácilmente tanto por consola como por CNA. Por consola se debe realizar lo siguiente:

- Se debe entrar en modo privilegiado. Para ello se escribió el comando *enable* y luego se introdujo el password asignado XXXXXXXXXXXXX. El prompt debe cambiar de la siguiente forma:

```
sw3550>
a la siguiente forma
sw3550#
```

donde el símbolo numeral indica que se tienen todos los comandos disponibles. (sw3550 es el nombre del switch).

- Ahora debe introducir el comando “vlan database” y el prompt cambia:

```
Sw3550#vlan database
% Warning: It is recommended to configure VLAN from config mode, as
VLAN database mode is being deprecated. Please consult user documentation
for configuring.
sw3550(vlan)#
```

- Para crear las VLANs según el diseño se realizaron los siguientes pasos:

```
Sw3550(vlan)#vlan 2 name Oficinas
VLAN 2 added
Name: Oficinas

Sw3550(vlan)#vlan 3 name Cursos
VLAN 3 added
Name: Cursos

Sw3550(vlan)#vlan 4 name Servidores
VLAN 3 added
Name: Servidores
```

El número que sigue después del comando *vlan* es el identificador de la VLAN.

- Para mostrar todas las VLANs se ejecuta el comando *show*.
- Para eliminar una VLAN se debe ejecutar el comando *no vlan* seguido del número de la VLAN que se desea borrar. Ejemplo:

```
Sw3550(vlan)# no vlan 12
Deleting VLAN 12...
```

```
Sw3550(vlan)#
```

- Para salir de VLAN database se utiliza el comando *exit*:

```
Sw3550(vlan)#exit  
APPLY completed.  
Exiting...
```

Fue necesario asignar una dirección IP a cada VLAN para que se pueda establecer el enrutamiento entre ellas. La dirección IP de cada VLAN será la puerta de enlace de todos los equipos que pertenezcan a ella. Esta dirección IP no pertenece a ningún puerto en específico; configurar una dirección IP a una VLAN es equivalente a agregar un enrutador dentro de la misma VLAN (pero sin ocupar ningún puerto externo del *switch*) con tal dirección IP. Por lo tanto, como este *router* no ocupa ningún puerto del *switch*, todo el enrutamiento se hace internamente dentro del equipo. El enrutamiento se hace entre todas las VLANs y puertos capa 3.

De igual forma las direcciones IP pueden fijarse por comando o mediante la herramienta CNA, ambas de manera muy sencilla. A continuación se muestra la forma como se realizó a través de la ventana de comandos:

```
Sw3550#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z  
Sw3550(config)#
```

Una vez activado el switch en modo de configuración se procedió a ejecutar el comando `interface vlan` seguido del número de la VLAN que desea configurar. Para configurar la VLAN 2, VLAN 3 y VLAN 4 se ejecutan los siguientes comandos:

```
Sw3550(config)#Interface vlan 2  
Sw3550(config-if)#Ip address 163.196.41.210 255.255.255.128  
Sw3550(config-if)#No shutdown
```

```
Sw3550(config-if)#Exit  
Sw3550(config)#
```

```
Sw3550(config)#Interface vlan 3  
Sw3550(config-if)#Ip address 163.196.41.211 255.255.255.128  
Sw3550(config-if)#No shutdown  
Sw3550(config-if)#Exit  
Sw3550(config)#
```

```
Sw3550(config)#Interface vlan 4  
Sw3550(config-if)#Ip address 163.196.41.212 255.255.255.128  
Sw3550(config-if)#No shutdown  
Sw3550(config-if)#Exit  
Sw3550(config)#
```

Finalmente se vuelve a escribir exit para salir del modo de configuración. Es conveniente que durante todo el proceso de configuración siguiente tanto la conexión por consola como la conexión por Ethernet permanezcan habilitadas simultáneamente para una más rápida gestión.

### **VLAN. Configurar puertos.**

La forma más sencilla de agregar puertos a una VLAN es mediante el Cisco Network Assistant. Para ello se seleccionó a la carpeta VLAN>VLAN... y luego en la pestaña de Configure Ports se seleccionó los puertos a configurar presionando el botón Modify. Véase figura IV.16.

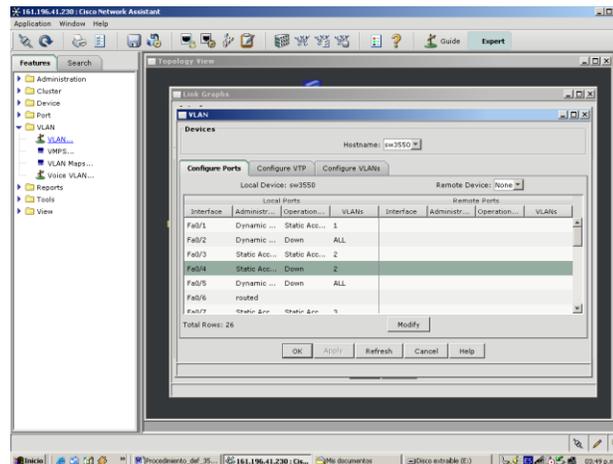


Figura IV.17. Configuración de puertos a una VLAN - 1

A continuación aparece la ventana mostrada en la figura IV.17. En el campo de Administrative Mode se debe seleccionar la opción Static Access para asignar el puerto a una VLAN específica. Esta VLAN se selecciona en el campo Static-Access VLAN. También es posible configurar los puertos de todas las formas mostradas en la figura IV.18. A continuación se presentan las opciones sobre "VLAN trunk":

- **Dynamic Access:** Se utiliza para implementar VLANs basadas en MAC address. Se debe configurar primero una base de datos VTP, un servidor VTP y un switch cliente VTP.
- **Dynamic Auto:** Este puerto se puede convertir en un VLAN Trunk si recibe una solicitud del otro switch al que se encuentra conectado.
- **Dynamic Desirable:** El puerto será un troncal de VLANs solo si el otro puerto al que está conectado así lo permite.
- **ISL Trunk:** El puerto es troncal de VLANs usando el protocolo ISL propietario de Cisco. Puede ser negociable o no.

- 802.1Q Trunk: El puerto es troncal de VLANs siguiendo el protocolo estándar 802.1Q. Se debe usar cuando se desea hacer configurar un VLAN Trunk con un equipo de diferente marca.

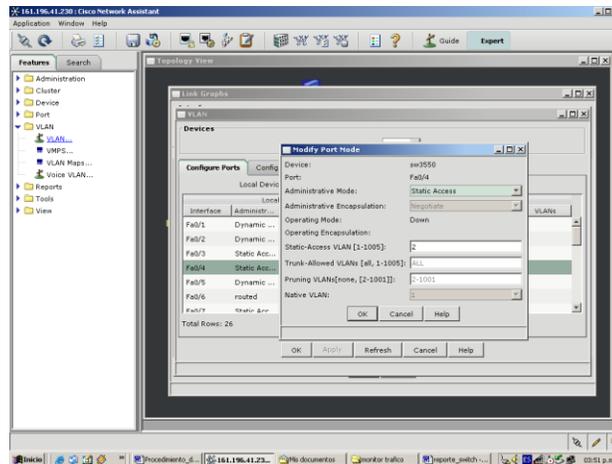


Figura IV.18. Configuración de puertos a una VLAN - 2

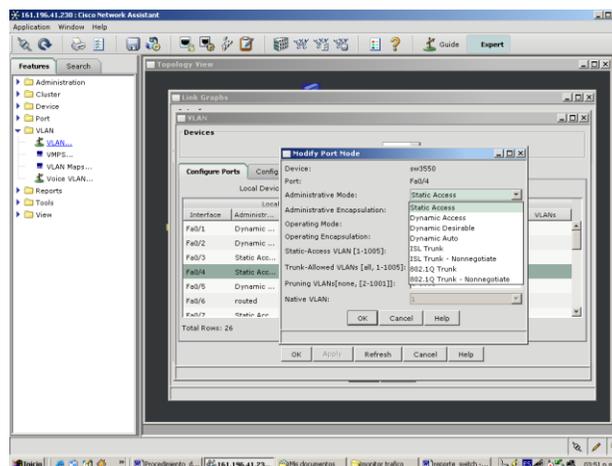


Figura IV.19 Configuración de puertos a una VLAN - 3

El switch Catalyst 3550 de Cisco ha salido al mercado con diferentes versiones de software. Existen dos tipos de software interno:

- SMI (Standard Multilayer Interface)  
Solo a partir de la versión 12.1 (11) EA1 soporta funciones básicas de capa 3.
- EMI (Enhanced Multilayer Interface)  
Todas las versiones poseen funciones de capa 3.

El enrutamiento IP es una función de capa 3 por lo que el switch debe tener el software EMI o SMI a partir de la versión 12.1 (11) EA1. La versión del software del switch puede verificarse rápidamente en el CNA.

La habilitación del enrutamiento IP es conveniente realizarse por consola. En este sentido es necesario contar con todos los privilegios activados. Para activar todos los permisos se escribió el comando enable y luego se introdujo el password que se fijó como XXXXXXXXXXXXX. El prompt cambió de la siguiente forma:

```
sw3550>  
a la siguiente forma  
sw3550#
```

donde el símbolo numeral indica que se tienen todos los comando disponibles. (sw3550 es el nombre del switch). Luego para habilitar el enrutamiento se ejecutó el siguiente comando:

```
sw3550# Ip routing
```

Para verificar que el servicio de enrutamiento quedó en funcionamiento ejecute:

```
sw3550#show running-config
```

debe aparecer entre muchas otras cosas:

```
i  
ip subset-zero  
ip routing  
i
```

Una vez creadas las VLAN en el switch principal 3550 la asignación de puertos quedó de la siguiente forma:

VLAN creadas en el *switch* principal 3550:

- 1.VLAN 1 (Vlan administrativa). VLAN por defecto, Puerto de gestión N° 24.
- 2.VLAN 2 (Oficinas). Puertos asignados: 21 al 23.
- 3.VLAN 3 (Salas de Cursos). Puertos asignados: 17-20
- 4.VLAN 4 (Servidores). Puertos asignados: 13 al 16.

Como es necesario agrupar usuarios de la misma VLAN que se encuentran ubicados en diferentes zonas del edificio Jan Deketh, es necesario utilizar en los *switches* un enlace troncal. Para que los *switches* envíen información sobre las VLAN que tienen configuradas a través de enlaces troncales es necesario que las tramas sean identificadas con el propósito de saber a que VLAN pertenecen. A medida que las tramas salen del *switch* son etiquetadas para indicar a que VLAN corresponden. Esta etiqueta es retirada una vez que entra en el *switch* de destino para ser enviada al puerto de VLAN correspondiente.

Un puerto de *switch* que pertenece a una VLAN determinada es llamado puerto de acceso, mientras que un puerto que transmite información de varias VLANS a través de un enlace punto a punto es llamado puerto troncal. Todos los puertos troncales que se configuraron en cada uno de los *switches* instalados fueron configurados en el puerto N° 2 de cada *switch*.

Para evitar que todas las VLANS viajen por el troncal es necesario quitarla manualmente. La información de todas la VLANS creadas viajara por el enlace trocal automáticamente, la VLAN 1 que es la VLAN por defecto o nativa lleva la información de estado de los puertos. También es la VLAN de gestión. El resumen de

la información brindada por un show VLAN que se muestra a continuación se observa la asociación de las respectivas VLAN, con sus puertos asociados:

```
switch#show vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/24.
2 Oficinas	active	Fa0/21, Fa0/22, Fa0/23.
3 Cursos	active	Fa0/17, Fa0/18, Fa0/19, Fa0/20.
4 Servidor	active	Fa0/13, Fa0/14, Fa0/15, Fa0/16.

Para la configuración de los *switches* de cada piso se siguieron los siguientes pasos:

1. Se definió una nomenclatura para identificar los *switches* dependiendo del lugar donde se encuentran. Así el *switch* con “Sw-JD2-1”, es un *switch* modelo 2950 que se encuentra en el piso 2 y es el número 1 en cluster.
2. Se definieron los *password* de consola, de telnet y de enable para el acceso de los mismos.
3. Se describieron los puertos por punto físico de la red.
4. Se colocó un número IP para administración remota.
5. Se definió la VLAN a la que pertenece con su dominio VTP.
6. Se definió el puerto trunk “switchport trunk encapsulation”, en cada uno de los *switches* instalados.

El siguiente paso consistió en configurar la interfaz hacia el *router*. Para ello se asignó un puerto que va conectado al *router* principal hacia Internet (u otra red). Todos los paquetes cuyos destinos no pertenezcan a ninguna de las subredes

(VLANs) conectadas al *switch* serán enrutadas por esta interfaz hacia el *router* principal.

Para configurar el puerto de salida se procedió a entrar en modo de configuración de igual manera como se explicó en el punto anterior. Luego se ejecuta el comando Interface FastEthernet (o GiEthernet) seguido del número del puerto. Este puerto no puede pertenecer a ninguna VLAN.

```
Sw3550(config)#Interface fastethernet 0/10
Sw3550(config-if)#No switchport
Sw3550(config-if)#Ip address 163.196.41.213 255.255.255.128
Sw3550(config-if)#No shutdown
Sw3550(config-if)#exit
Sw3550(config)#
```

El commando no *switchport* indica que ese puerto es capa 3. La dirección IP que se le asignó es 163.196.41.213.

Finalmente se ordena que todo destino desconocido (e inalcanzable) debe ser enrutado al *router* principal. El *router* principal debe estar en la misma subred que el puerto configurado anteriormente. En el ejemplo anterior se le fijo al puerto la dirección IP 163.196.41.213 suponiendo que el *router* principal al que está conectado directamente este puerto tiene asignada la dirección 163.196.41.214. Ahora se indica que todo destino inalcanzable por el *switch* (que no pertenece a ninguna de sus VLANs) debe ser enrutado al *router* principal:

```
Sw3550(config)#Ip route 0.0.0.0 0.0.0.0 163.196.41.213
```

En ningún momento se indica por cual puerto del *switch* van a ser enrutados los paquetes sino que solo se indica la dirección IP del *router* principal. Esto se debe a que el *switch* directamente sabe que ese destino solo puede ser alcanzado por aquel

puerto cuya dirección IP pertenezca a la misma subred que el router principal. El *router* principal puede estar conectado a un puerto capa 3 o a una VLAN con IP asignada. Por razones de seguridad y rendimiento es conveniente que el router se encuentre conectado a un puerto capa 3.

A partir de este punto el Catalyst 3550 está en capacidad de enrutar satisfactoriamente entre todas las VLANs y hacia el *router* principal. Se realizaron pruebas usando el protocolo ICMP (ping) para verificar que todo se encuentra operativo.

**IMPORTANTE:** Fue necesario configurar el *router* principal para que envíe los paquetes a la dirección del puerto capa 3 al cual se encuentra conectado, ya que el *switch* solo enrutará si los paquetes son dirigidos hacia la IP de la interfaz (sea VLAN o puerto capa 3).

### **3. Cableado Estructurado y Documentación de la Red Lan.**

El primer paso que se realizó fue la elaboración de los planos del edificio Jan Deketh del Centro de Estudios de Telecomunicaciones. Para ello se procedió a la toma de medidas de todo el edificio mediante el uso de una cinta métrica de 5 metros de longitud. Luego se realizó el plano a escala 1:10 mediante el empleo del software Microsoft Visio Profesional 2003.

A continuación se comenzó con la sustitución del cableado UTP nivel 5 ubicado en el piso 1 por cableado nivel 6 en cada una de las salas de PC'S. Este trabajo se realizó en horario no laboral y fines de semana para no interrumpir las operaciones del Centro de Estudios de Telecomunicaciones. El cableado UTP nivel 5 fue retirado de la escalerilla de distribución y se colocó el cableado nuevo nivel 6, dirigiéndose todo el cableado hasta un solo punto de concentración ubicado en la sala de cableado

JD-1.12 del piso 1 del edificio Jan Deketh. Para llevar a cabo esta sustitución se utilizaron 25 bobinas de cable UTP nivel 6 aproximadamente, más de 400 conectores RJ-45 marca Panduit, 200 *patch cord*, 9 *patch panels*, 2 *racks*, entre otros accesorios. El cableado vertical UTP categoría 5 que existía para interconectar los *switches* con el equipo principal (core) fue también reemplazado por UTP categoría 6.

Posteriormente se procedió a tomar la información de todas las computadoras e impresoras conectadas a la red. Los datos tomados para las computadoras fueron: marca, modelo, velocidad CPU, memoria RAM, capacidad de disco duro, velocidad de la tarjeta de red, dirección IP (en caso de ser manual, sino se especifica "por DHCP") y máscara de subred. Los datos de la impresoras fueron solo dirección IP, modelo y marca. Se realizó un plano para cada una de las plantas del edificio con la distribución de todos los equipos y sus características los cuales se presentan en los anexos 1, 2 y 3 respectivamente.

También se realizó un plano para cada una de las plantas del edificio con la distribución de todos los equipos y sus características principales, los cuales se presentan en los anexos 4, 5 y 6 respectivamente. Por otro lado los anexos 7 y 8 muestran las características de algunos de los equipos que se encuentran disponibles en los planos de equipos.

Para realizar el diagrama de cableado se procedió a identificar todo el recorrido del cableado de red del edificio, especificando el medio por el que se hizo (escalerilla, canaleta de pared, etc.). Para ello se utilizó una escalera en las áreas donde el cableado se ocultaba por encima del "cielo raso". Se ubicaron además todos los puntos de red disponibles. Se realizó un plano especificando todo el recorrido del cableado y los puntos de red, a los cuales se les asignó una codificación para su más fácil identificación. Este plano además especifica los puntos por donde el cableado pasa entre diferentes pisos.

Por otro lado se elaboró un conjunto de tablas resumen de todos los equipos, puntos de red y disponibilidad de puertos por *switches* que existen en cada uno de los pisos del edificio Jan Deketh del Centro de Estudios de Telecomunicaciones. Algunos ejemplos se pueden observar en los anexos 9 y 10.

Todos los planos mostrados en las figuras mencionadas anteriormente se encuentran disponibles en el CD-ROM anexo al proyecto. Es necesario disponer del software Microsoft Visio para que los mismos puedan ser visualizados.

Es importante destacar que, con la ayuda del plano de cableado realizado se tomó en cuenta la longitud de los todos los cables con el objetivo de comprobar que ninguno excediera la longitud máxima de 100 metros para Fast Ethernet 100BaseT. La máxima longitud que se encontró con los recorridos del cable actual es menor a los 78 metros (77,6 mts).

Finalmente se realizaron todas las pruebas de cada uno de los puntos de red instalados nuevos con los probadores de cables respectivos, corrigiendo las fallas y asegurándose de encontrarse operativos.

#### **4. Sistema de Cámaras de Vigilancia.**

Una vez diseñado y aprobado el sistema de cámaras de vigilancia, se procedió a realizar la instalación de las mismas en cada uno de los sitios estratégicos ubicados en los planos de los edificios. Dicha instalación abarcó el cableado eléctrico y de datos el cual se realizó a través de cable coaxial RG59 utilizando 2 bobinas de cable para tal fin.

Se instalaron 4 servidores de video en su totalidad distribuidos de la siguiente manera:

- Servidor de video N° 1: Instalado en la sala de servidores y cableado estructurado del piso 2 del edificio Jan Deketh.
- Servidor de video N° 2: Instalado en la sala de cableado estructurado del piso 1 del edificio Jan Deketh.
- Servidor de video N° 3: Instalado en el piso 1 del edificio Arvelo.
- Servidor de video N° 4: Instalado en el piso 2 del edificio Arvelo.

En la siguiente figura IV.20, se observa el servidor de video N° 1 instalado en la sala de servidores y cableado estructurado del piso 2 del edificio Jan Deketh.



Figura IV.20 Servidor de Video N° 1 instalado

En los anexos 11, 12, 13 y 14 se muestran algunas de las cámaras de vigilancia instaladas en los edificios Jan Deketh y Arvelo del Centro de Estudios.

Finalizada la instalación de las cámaras se procedió a realizar la instalación de la aplicación Cammanager en el Servidor de Aplicaciones (Appli1). Para iniciar la gestión de las cámaras fue necesario el establecimiento de un *password*.

Posteriormente se agregó cada uno de los 4 servidores de video instalados, la siguiente figura muestra la información solicitada para la incorporación de los servidores a la aplicación Cammanager.

Figura IV.21 Incorporación de Servidores al Cammanager

Posteriormente cada servidor de video fue configurado con una dirección IP, tal y como se muestra en la figura teniendo disponible 2 opciones de configuración (Fija o DHCP)

Figura IV.22 Asignación de dirección IP

Cada servidor de video maneja 4 cámaras de vigilancia a través de canales (Frecuencias) tal y como se indica en la siguiente figura:



Figura IV.23 Canales de frecuencia

Una vez instalados todos los servidores de video y agregadas todas las cámaras de vigilancia se procedió a configurar la opción de backup para iniciar el proceso de grabación en el servidor, en la siguiente figura se muestra el proceso.

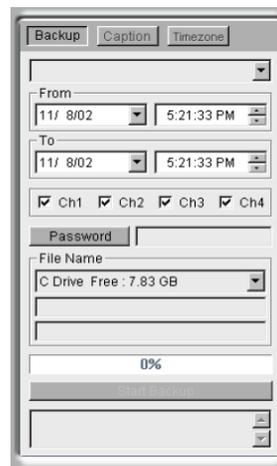


Figura IV.24 Configuración de la opción de backup

Una vez realizada la configuración del backup y ya instaladas todas las cámaras se procedió a realizar las pruebas pertinentes, resolviendo los problemas de sincronización y quedando operativas las 16 cámaras de vigilancia. Por último se pueden observar en los anexos 15, 16 y 17 las imágenes del funcionamiento de algunas de las cámaras de vigilancia ya instaladas y configuradas.

## **FASE 4: SITIO WEB DEL CENTRO DE ESTUDIOS DE TELECOMUNICACIONES DE LA EMPRESA EN ESTUDIO.**

### **Paso 1: ANÁLISIS.**

#### **☐ Descripción del Perfil del Usuario**

Los usuarios potenciales del sitio Web del Centro de Estudios de Telecomunicaciones estarán integrados por todos los empleados de la empresa, puesto que la información contenida en la aplicación es de carácter interna, significativa y útil para todas las gerencias y unidades que conforman la empresa en estudio.

#### **☐ Campo de Acción**

El ambiente donde el sitio Web será utilizado, está constituido por la estructura física organizacional de la empresa en estudio y cada una de sus sedes a nivel nacional, así que, como requerimiento, sólo se necesita que los usuarios estén autenticados a la red e intranet corporativa y dispongan de un computador y un navegador para poder visualizar las páginas, permitiendo que la aplicación pueda ser accedida a desde cualquier parte de la empresa, lo que le da un radio de acción a nivel nacional.

#### **☐ Determinación de requerimientos funcionales**

El usuario final podrá utilizar el sitio Web del Centro de Estudios de Telecomunicaciones para diferentes actividades, las cuales se mencionan a continuación:

- Como Unidad Informativa acerca de las políticas, procesos, instructivos, directivas, lineamientos organizacionales de la corporación en materia de Formación.
- Como herramienta para la búsqueda de información referente eventos tecnológicos, programación de cursos, lineamientos, gestión de formación, recomendaciones, normativas, entre otras. Así mismo, le permitirá al personal acceder y conocer información referente a los contactos que existen para canalizar los requerimientos en materia de formación.
- Como medio de información acerca del Centro de Estudios de Telecomunicaciones referente a sus objetivos, metas, logros, entre otros.

El sitio Web del Centro de Estudios de Telecomunicaciones, lo que persigue es concentrar en un solo medio la mayor información, para facilitar de esta forma el acceso a la información de todo el personal de la corporación.

Para el buen funcionamiento de la aplicación, el usuario debe poseer un Navegador de páginas Web conocido (Internet Explorer, Netscape, Firefox), preferiblemente el Internet Explorer en su versión 6.0 o superior, esto por razones de compatibilidad entre productos.

#### **☐ Determinación de requerimientos de información**

Cabe destacar que para que el usuario obtenga el mayor beneficio del sitio Web del Centro de Estudios de Telecomunicaciones, debe conocer el entorno de navegación Web de la intranet corporativa, puesto que allí se encuentra el link hacia

la aplicación, por otro lado debe poseer conocimientos básicos acerca de la estructura organizativa de la Corporación, lo que le facilitará el acceso, manejo y búsqueda de información.

#### ▣ **Determinación de requerimientos de interacción**

El diseño y desarrollo del sitio Web del Centro de Estudios de Telecomunicaciones, se realizó en base a las políticas de la Gerencia de Identidad de Marca de la empresa, la cual establece un conjunto de estándares a ser utilizados tales como el tipo y tamaño de la letra, colores, logotipos, formas, entre otros aspectos, por lo que la misma busca crear un ambiente amigable y estándar entre los usuarios y la intranet Corporativa.

En este aspecto se presentan básicamente tres tipos de interacción con la Aplicación Web del Centro de Estudios de Telecomunicaciones:

1. **Interacción del usuario y el sitio Web:** ocurre cuando los usuarios, acceden a la información registrada en la aplicación en busca de información publicada en la misma.
2. **Interacción del sitio Web con el administrador:** se presenta cuando el administrador de la aplicación ingresa, elimina, modifica o actualiza la información de la misma.
3. **Interacción del usuario con los módulos de consultas:** sucede cuando los usuarios dirigen a los módulos de consultas destinados a la extracción de información concreta tales como archivos que contienen presentaciones de eventos de formación, programación, lineamientos, entre otros.

## ■ Determinación requerimientos de desarrollo

Para el diseño, desarrollo e implantación del sitio Web se hizo necesario la utilización de un conjunto de requerimientos técnicos y operacionales que se describen a continuación:

### 1) Requerimientos de Hardware

Tanto para el diseño como desarrollo del sitio Web fue necesario establecer una arquitectura cliente/servidor, la cual permite el desarrollo de la página Web en el servidor utilizado para alojar las páginas del sistema, y la utilización de las estaciones de trabajo para visualizar, consultar y actualizar la Aplicación Web final. Esta arquitectura cliente/servidor no requiere de hardware especial, aunque es recomendable que el servidor y la estación de trabajo posean las características de hardware descritas a continuación:

	Servidor	Estación de Trabajo
Procesador	Pentium IV de 3.0 Mhz	Pentium IV 2.8 Mhz INTEL
Memoria RAM	≥ 512 Mb	≥ 256 Mb
disco duro	> 80 Gb	40 Gb
Controlador de disco	E-IDE o SCSI	E-IDE o SCSI
Tarjeta gráfica	SUPER-VGA ≥ 64Mb	SVGA ≥ 32Mb
CD-ROM	52X	52X
Tarjeta de red	PCI 10/100Mbps	10/100 Mbps

IV.10: Requerimientos de Hardware

### 2) Requerimientos de Software.

Para el desarrollo del sitio Web del Centro de Estudios de Telecomunicaciones fue necesario trabajar con la herramienta Microsoft **FrontPage2003**, incluido en el paquete de Office2003, la cual permite la creación de sitios web utilizando tecnologías como HTML, controles de Active X, programación

de páginas Active Server Page (ASP) a través de los lenguajes Vbscript, Javascript y páginas de estilos CCS.

FrontPage2003 opera con el modelo Cliente/Servidor, por lo que fue necesario trabajar en el Servidor con el sistema operativo **Windows 2003 Server**, conjuntamente con el Servidor Web **Internet Information Server (IIS) 6.0**, el cual incluye una amplia gama de funciones administrativas para controlar sitios Web y el servidor Web. La razón por la cual no se uso el servidor Web Apache es porque en el servidor Web, se encuentran otras aplicaciones funcionando con IIS y no es posible levantar ambos servicios ya que entran en conflicto. En cuanto al diseño del arte de la Aplicación Web se utilizaron los programas: **Corel Draw 12, Flash Macromedia 2006 MX, Paint, Photo Editor**.

Para las estaciones de trabajo fue necesario contar con el sistema operativo Windows XP, por su versatilidad en el manejo del entorno Web. Por último, se empleo Navegador de Microsoft **Internet Explorer 6.0** para visualizar las páginas contenidas en la aplicación.

## **Paso 2: DISEÑO.**

### **☐ Diseño de la Estructura.**

El sitio Web del Centro de Estudios de Telecomunicaciones está constituido por diversas secciones, las cuales presentan la misma estructura física diferenciándose sólo en la información contenida en cada uno de los mismos y que será mostrada en un marco principal establecido para ello.

El diseño de la estructura física utilizada para el desarrollo de la aplicación cumple con un conjunto de lineamientos establecidos por la Gerencia de Identidad de Marca de la Corporación, en donde involucra el uso de un área predeterminada para la colocación del Logo de la Corporación, así como la colocación de imágenes representativas de la sede de dicho centro, al igual que el nombre de la Gerencia a la que pertenece el Centro de Estudios de Telecomunicaciones, por otro lado en la parte central se encuentran los *link* hacia las secciones contenidas en aplicación.

A continuación se muestra la estructura física general usada en el desarrollo de la Aplicación Web del Centro de Estudios de Telecomunicaciones:

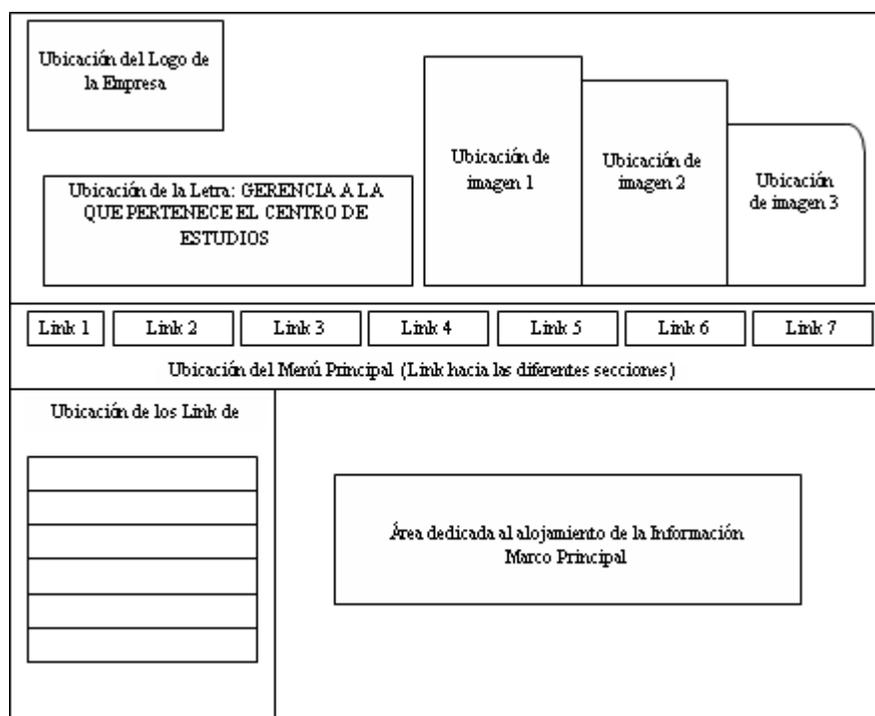


Figura IV.25. Estructura física empleada para el diseño de la Aplicación Web del Centro de Estudios de Telecomunicaciones

A continuación se presenta la estructura física donde se puede observar las áreas descritas anteriormente:



Figura IV.26. Estructura física de la aplicación Web detallando la división estratégica de la página

Cabe destacar que todas las páginas que forman parte del sitio Web del Centro de Estudios de Telecomunicaciones se encuentran estructuradas de esta forma, en total las áreas que conforman la aplicación son:

1. Unidad principal del sitio “Home”.
2. Información general.
3. Conocimientos.
4. Competencias.
5. Preguntas frecuentes.
6. Postulación.
7. Formación atención total.

El sitio Web del Centro de Estudios de Telecomunicaciones está integrado por 7 unidades. Estas fueron organizadas según la siguiente figura:

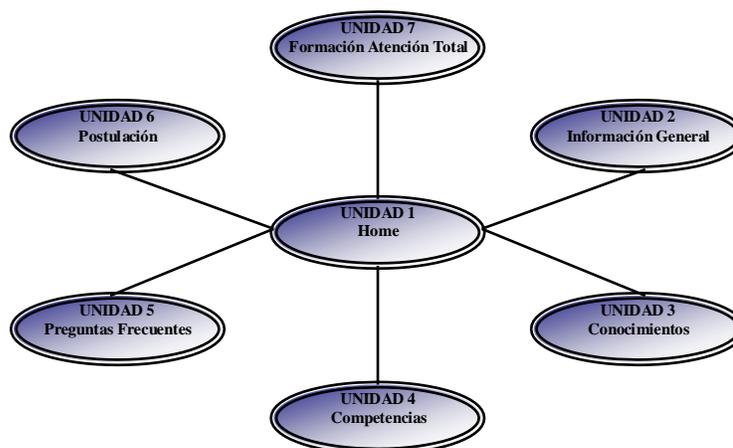


Figura IV.27. Diagrama general de la aplicación Web del Centro de Estudios de Telecomunicaciones

#### ▣ Diseño de las Unidades de Información

En el diseño de las Unidades de Información, se especifica el contenido de cada unidad descritas anteriormente. Ya se hizo referencia de las áreas que componen la Aplicación Web del Centro de Estudios de Telecomunicaciones. A continuación se procederá a describir cada una de las áreas y alguno de los aspectos utilizados para su desarrollo.

**Unidad 1 (Home):** Se trata de la página principal del sitio Web del Centro de Estudios de Telecomunicaciones, desde esta unidad es posible acceder a cada una de las unidades o secciones de la aplicación, puesto que se encuentran todas las conexiones hacia las otras unidades desarrolladas. Además tiene como propósito contener en su espacio central, información referente a la visión y misión de dicho Centro de Estudios, así como lineamientos, productos y servicios, programación de entrenamientos, dirección del centro y eventos cualquier actividad de interés para la empresa en estudio. Esta página puede visualizarse en la sección correspondiente a los anexos, (Anexo N° 18).

**Unidad 2 (Información General):** Esta unidad muestra información de carácter general sobre algunos procesos internos del Centro de Estudios tales como:

- Procesos relacionados con la participación del personal de la corporación en los ciclos de cine foros, películas a proyectar, programación, postulación a los foros, planillas de inscripción, guías de selección y análisis de películas y personas de contactos. Esta página está conformada por un contenido definido por texto, imágenes, presentaciones y links, que las harán atractivas a todos los usuarios de la aplicación.
- Información relacionada a las políticas de solicitud de viáticos existentes en la corporación. En esta sección los usuarios podrán descargar las planillas de solicitud de anticipo de viáticos así como la planilla de liquidación de los mismos.
- Información relacionada a las diversas estrategias emprendidas por la corporación en cuanto a iniciativas sociales y ciudadanas que impactan de manera positiva en atención a los sectores más vulnerables del país.
- Información referida al sistema de aprendizaje activo Moviltraining, a través del cual se dispone de más de 2000 cursos en línea que pueden ser realizados por cualquier empleado de la corporación.
- Información de nuestros contactos de RRHH a nivel nacional los cuales sirven de apoyo en los procesos de formación.

Esta página puede visualizarse en la sección correspondiente a los anexos, (Anexo N° 19 ).

**Unidad 3 (Conocimientos):** Esta unidad está destinada a brindar información referente al tema de conocimientos, el cual responde de manera directa a las necesidades de comprensión de procedimientos, contexto de trabajo, métodos, instrumentos, equipos y tecnologías. Esta página puede visualizarse en la sección correspondiente a los anexos, (Anexo N° 20 ).

**Unidad 4 (Competencias):** Esta unidad está dedicada a ofrecer información relacionada al tema de competencias, el cual incluye características personales que predicen y producen un desempeño excelente en un contexto específico. Estas características se evidencian a través de conductas que se presentan en diversas situaciones, con frecuencia y asociadas a los mejores resultados. Esta página puede visualizarse en la sección correspondiente a los anexos, (Anexo N° 21 ).

**Unidad 5 (Preguntas Frecuentes):** Esta unidad está dedicada a ofrecer información sobre las preguntas más frecuentes relacionadas con los procesos de identificación de necesidades de formación (IOF) y el Plan Individual de Desarrollo (PID Competencias y Conocimientos). Esta página puede visualizarse en la sección correspondiente a los anexos, (Anexo N° 22).

**Unidad 6 (Postulación):** En esta sección se muestra información referente al proceso de postulación del personal de la corporación a las acciones de formación de tipo voluntaria, internacional y nacional, así como recomendaciones a los supervisores para garantizar la adecuada distribución de las actividades de formación de sus equipos de trabajo y la oportuna asistencia de todos los integrantes del grupo a sus acciones de formación, en función de la dinámica del negocio. Esta página puede visualizarse en la sección correspondiente a los anexos, (Anexo N° 23).

**Unidad 7 (Formación Atención Total):** Esta sección esta dedicada a ofrecer información relacionada con el Proyecto Atención Total que lideriza la Corporación el cual busca satisfacer un conjunto de requerimientos de tipo tecnológico ideando para ello un esquema de formación basado en e-learning y cursos presénciales. Esta página puede visualizarse en la sección correspondiente a los anexos, (Anexo N° 24).

- ▣ **Diseño de ítems de información:** El diseño de ítems de información es el paso en el cual se especifica el arte y/o estética utilizada en la conformación de las unidades de información.

Como primer paso en la elaboración del sitio Web del Centro de Estudios de Telecomunicaciones se utilizó los items suministrados por la Gerencia de Identidad de Marca, la cual establece las pautas para el diseño de sitios web dentro de la Corporación, de manera de contar con un estándar para la construcción de aplicaciones web en temas como logos, tipo y tamaño de letras, colores, espacios, formas, entre otros aspectos. Para la elaboración de cada gráfico se utilizaron varios programas de manejo y diseño de imágenes tales como: Corel Draw 12, Paint, Photo Editor. A continuación se muestran algunos gráficos realizados:

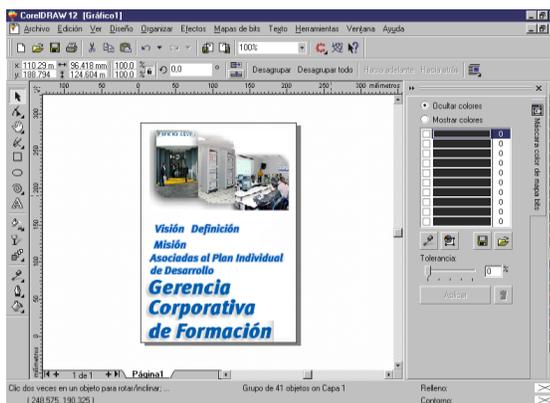


Figura IV.28. Imágenes en ambiente Corel Draw 12

### **Paso 3: DESARROLLO.**

Hasta este momento se cuenta con los prototipos de cada una de las unidades que formarán parte del sitio Web del Centro de Estudios de Telecomunicaciones, esta fase es la que se encarga del ensamblaje de cada uno de los sub-sitios para conformar de esta manera la aplicación.

- ▣ **Desarrollo de las Unidades de Información:** Luego de establecer el diseño del prototipo se procedió al ensamblaje del proyecto lo que arrojará como resultado final la culminación del proyecto. Con la finalización del desarrollo de las unidades de información el proyecto entrará en el ciclo evolutivo y correctivo por su período de vida.

Ya planteado el diseño de las páginas html y htm se procedió con el ensamblaje y programación de cada una de las páginas que componen el sitio Web del Centro de Estudios de Telecomunicaciones se utilizó como editor de paginas HTML el programa de Microsoft **FrontPage2003**, donde se combino código html, javascript y páginas de estilo css. Luego de diseñado el modelo de las unidades se introdujo la información perteneciente a cada unidad, así como también los respectivos enlaces (Link) correspondientes a las demás páginas, siguiendo el esquema planteado en la fase de diseño. En la siguiente figura se puede apreciar el ambiente de trabajo utilizado para este fin:





## CAPÍTULO V

### CONCLUSIONES

Una vez finalizadas todas las fases del proyecto y tomando en cuenta los objetivos de la investigación, se pueden concluir varios puntos que se mencionan a continuación:

- Se logró identificar las principales necesidades y requerimientos de información más necesarios en el Centro de Estudios de Telecomunicaciones, así como también todos los implementos tanto de hardware como de software necesarios para la actualización de la infraestructura tecnológica, lo que garantiza grandes beneficios al nivel de comunicación y gestión puesto que las características que presentan todos éstos implementos seleccionados son de gran calidad y rendimiento.
- El diseño e implantación del sitio Web del Centro de Estudios de Telecomunicaciones, constituye una completa herramienta, puesto que introduce mecanismos y recursos interactivos que permiten el manejo, administración, catalogación y enriquecimiento permanente de la información existente, logrando de esta manera que la empresa sea más eficiente y eficaz.
- El Centro de Estudios de Telecomunicaciones cuenta ahora con una red LAN óptima, ya que se rige bajo las normas internacionales de cableado estructurado EIA/TIA/568, y de esta forma garantiza el buen funcionamiento de una plataforma.

- Se logró mejorar los tiempos de respuesta en un 90%, lo cual satisface el creciente uso de las aplicaciones cliente/servidor, aplicaciones internas, acceso Internet, envío y recepción de correo interno, entre otros.
- La utilización de *switches* permitió segmentar la red, limitando tráfico de *broadcast* y proporcionando mayor seguridad, control y redundancia entre dominios individuales de *broadcast*. Por otro lado se eliminaron los cuellos de botella que se formaban con los *hubs* que se encontraban instalados, aumentando de esta manera el ancho de banda y la velocidad de transmisión.
- La creación de VLAN permiten una actividad de difusión (*broadcast*) controlada, además de proporcionar seguridad de grupos de trabajo.
- Al contar con una LAN 100% conmutada, se logró incorporar a la gestión del Centro de Operaciones de la Red, el cual se encuentra en constante monitoreo, registrando y alertando sobre cualquier falla o eventualidad que pueda ocurrir, logrando minimizar los tiempos de respuestas a la hora de resolver las fallas.
- Se cuenta con una documentación actualizada de la red LAN, a nivel de cableado estructurado, equipos, diagramas de interconexión lo cual permite identificar fácilmente cualquier componente que este presentando problemas.
- El diseño e implantación del sistema de vigilancia a través de cámaras de video ofrece mayor seguridad física garantizando el resguardo de los diferentes equipos, componentes que forman parte de la plataforma tecnológica y minimizando las incidencias de seguridad.

## RECOMENDACIONES

Una vez realizado el proyecto de actualización de la infraestructura tecnológica y diseño e implantación de la plataforma de seguridad para el Centro de Estudios de Telecomunicaciones, es oportuno hacer una serie de recomendaciones que fortalezcan el mismo y sirvan de base para futuras investigaciones.

- Mantener actualizados los planos de distribución de cableado y equipos, manteniendo la ubicación de los puntos de datos así como actualizar cualquier modificación en la configuración de los *switches*. Los planos deben estar a disposición de los técnicos de cableado, a fin de poder consultar en ellos las dudas atendiendo de forma más eficiente las posibles fallas que puedan presentarse.
- En caso de adquirir nuevos implementos de red para futuras ampliaciones se recomienda seguir las normas descritas para la instalación del cableado estructurado para de esta forma garantizar el buen funcionamiento de la red.
- Mantener los cuartos de cableado en óptimas condiciones bajo los estándares establecidos. No utilizar los cuartos de cableado como depósitos de equipos que puedan obstaculizar el normal desenvolvimiento de las tareas por parte del equipo de técnicos en redes.
- Crear y mantener actualizado el sitio web del Centro de Estudios de Telecomunicaciones.
- Analizar la infraestructura del resto de los edificios que forman parte del Centro de Estudios de Telecomunicaciones a fin de evaluar su actualización en cuanto a equipos de redes y el cableado en general.

- Ejecutar un mantenimiento preventivo, periódico y continuo, tanto del hardware como del software, al ser implementado el nuevo sistema.
- Realizar un mantenimiento preventivo, periódico y continuo, al sistema de vigilancia a través de las cámaras instaladas en los diferentes edificios del Centro de Estudios.
- Monitorear constantemente la información registrada por las cámaras de vigilancia en el servidor destinado para ello, a fin de detectar y notificar cualquier irregularidad a la unidad de seguridad.
- Velar por el cumplimiento de las medidas de seguridad físicas con la finalidad de impedir la entrada de intrusos y evitar hurtos internos.
- Mantener entrenados al personal técnicos de cableado y analistas de redes, en materia de cableado, infraestructura y *switches* Cisco, para así obtener un mayor aprovechamiento de los equipos y tecnologías existentes.
- Realizar todos los trámites necesarios para colocar redundancia en el centro (core) de la red, es decir adquirir otro equipo equivalente al Cisco 3550, para tener un respaldo y si es necesario balanceo de carga.

## BIBLIOGRAFÍA

Afergan, M., Darnell, R., Farrar, B. y Otros. (1998). Programación en Web 6 en 1. México: Prentice-Hall Hispanoamericana, S.A.

Montilva, J. (1998). Sistemas de Información Web: Fundamentos y Aspectos Metodológicos. Memorias del IV Congreso Nacional sobre Multimedia y Videoconferencia. (p. 1).

Senn, J. (1992). *Análisis y Diseño de Sistemas de Información.* México: McGraw Hill

Stoltz, Kevin (1995).- Todo acerca de Redes de Computación. Prentice – Hall Hispanoamericana.

Cantv (2005). Cisco Catalyst 2950 – 3550. Guía de Instalación y configuración. Revisión 2. Caracas, Venezuela.

Kendall, K. & Kendall, J. (1991). Análisis y Diseño de Sistemas. México: Prentice-Hall. México.

Chávez, Feliciano. “Plataformas Tecnológicas Para Redes de Datos”. Centro de Estudios de Telecomunicaciones - CANTV. Caracas, 2000.

Cisco System. Interconnecting Cisco Network Devices. Volumen 1 y 2. Versión 2.1. Student Guide. Capítulo 6: Addressing and Routing, Página 6-5. San Francisco, EEUU, 2003.

Cisco System. Interconnecting Cisco Network Devices. Volumen 1 y 2. Versión 2.1. Student Guide. Capítulo 6: Addressing and Routing, Página 6-6. San Francisco, EEUU, 2003.

Cisco System. Interconnecting Cisco Network Devices. Volumen 1 y 2. Versión 2.1. Student Guide. Capítulo 12: Establishing Serial Point-to-Point Connections. San Francisco, EEUU, 2003.

### **PÁGINAS WEB VISITADAS**

Desarrolladores web. Disponible en: <http://www.lawebdelprogramador.com>

Microsoft. (2007). Microsoft Latino Americana. [On-Line] disponible en: <http://www.microsoft.com/latam/>

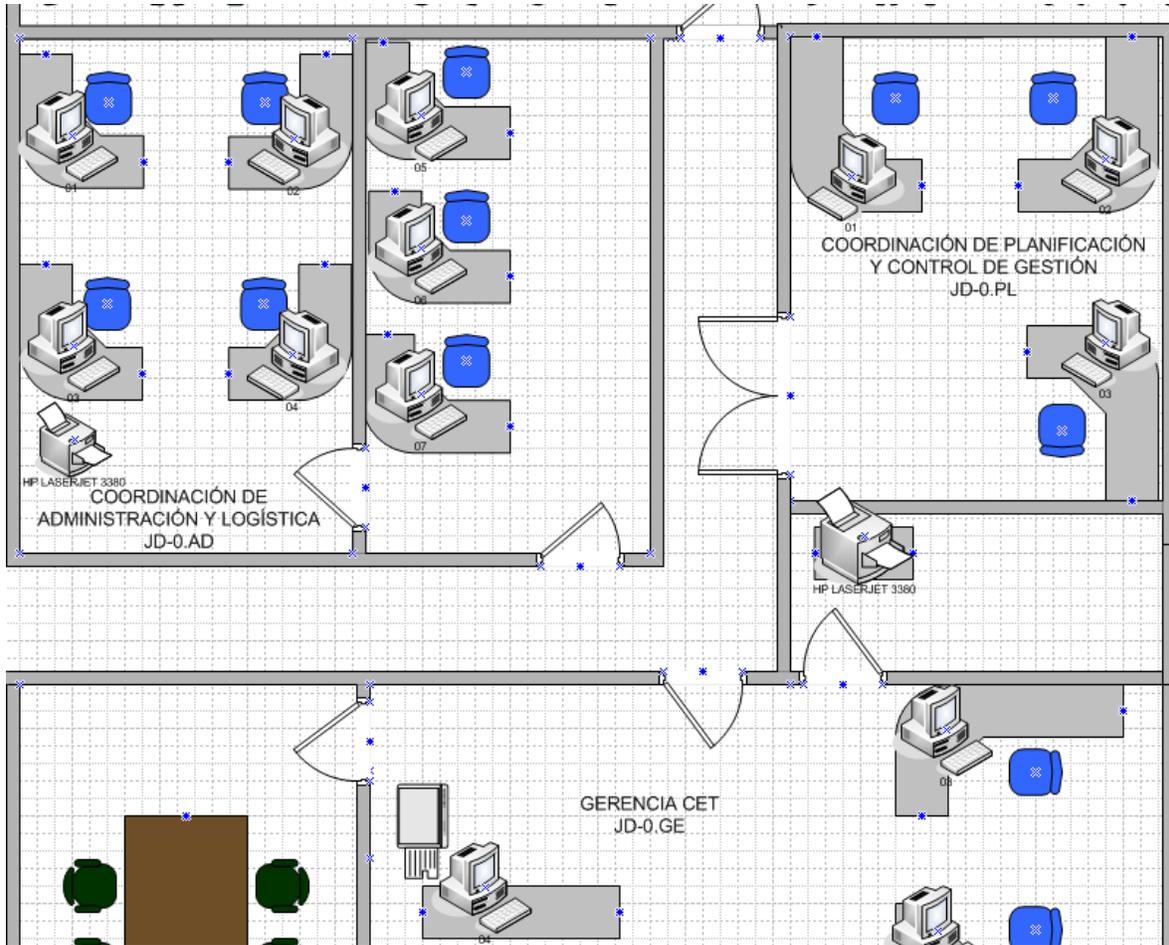
Network Solutions. (1999). Tutoriales. [On-Line] disponible en: <http://tutoriales.hypermart.net/cgi-bin/buscar/url/srch.cgi>

Cisco Systems (2007). Documentos de Soportes [On-Line] disponible en: [http://www.cisco.com/en/US/support/tsd\\_documentation.html](http://www.cisco.com/en/US/support/tsd_documentation.html)

Ministerio de Educación, Cultura y Deportes de Espana. [On-Line] disponible en: <http://w3.cnice.mec.es/tecnologica/experto/ip/index.htm>

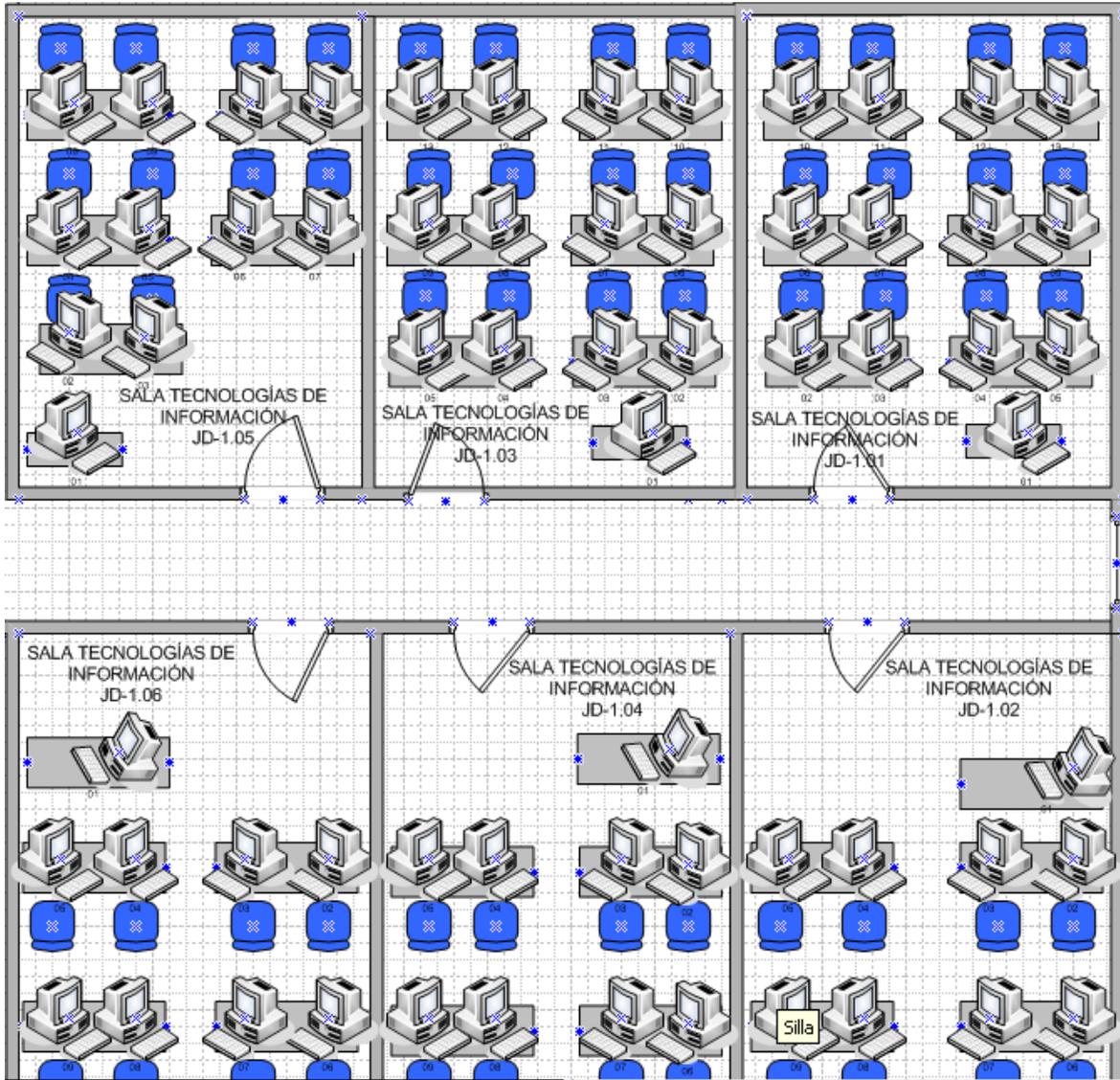
# **ANEXOS**

**ANEXO 1**  
**PLANO DE EQUIPOS PLANTA BAJA**

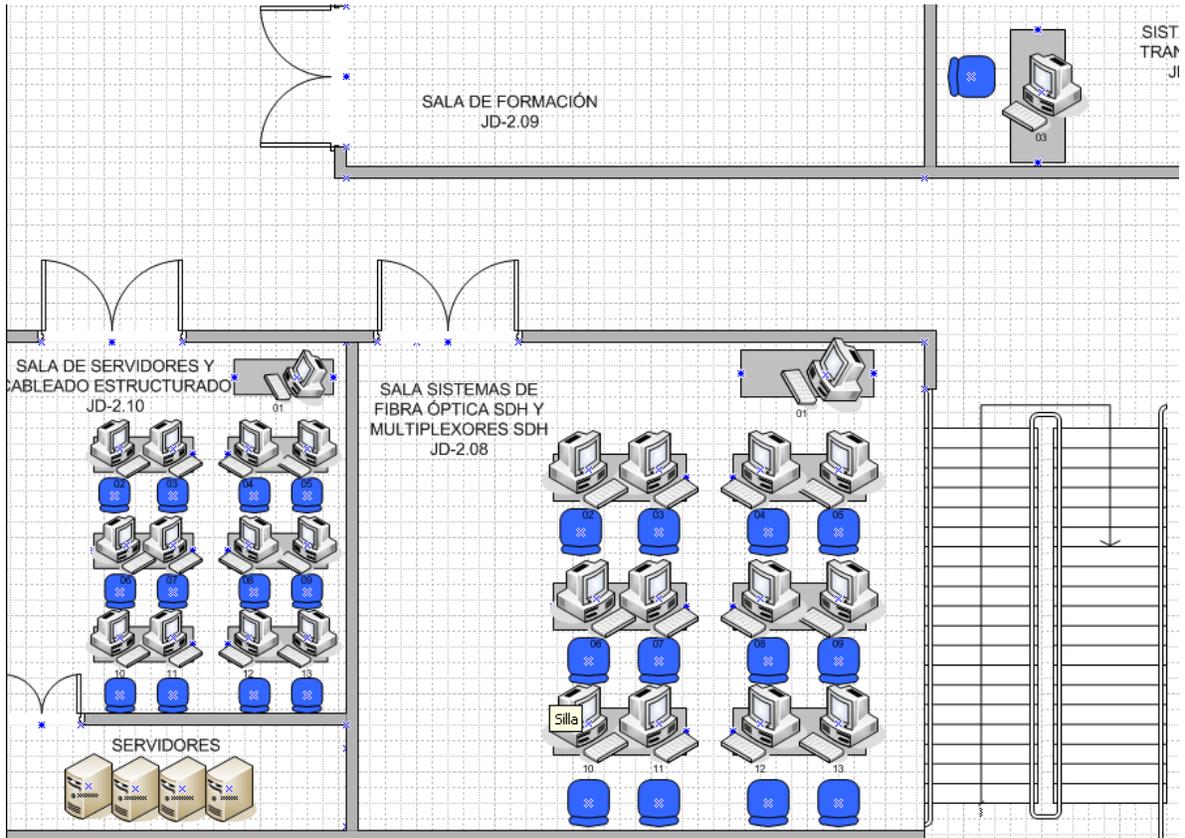


## ANEXO 2

### PLANO DE EQUIPOS PISO 1

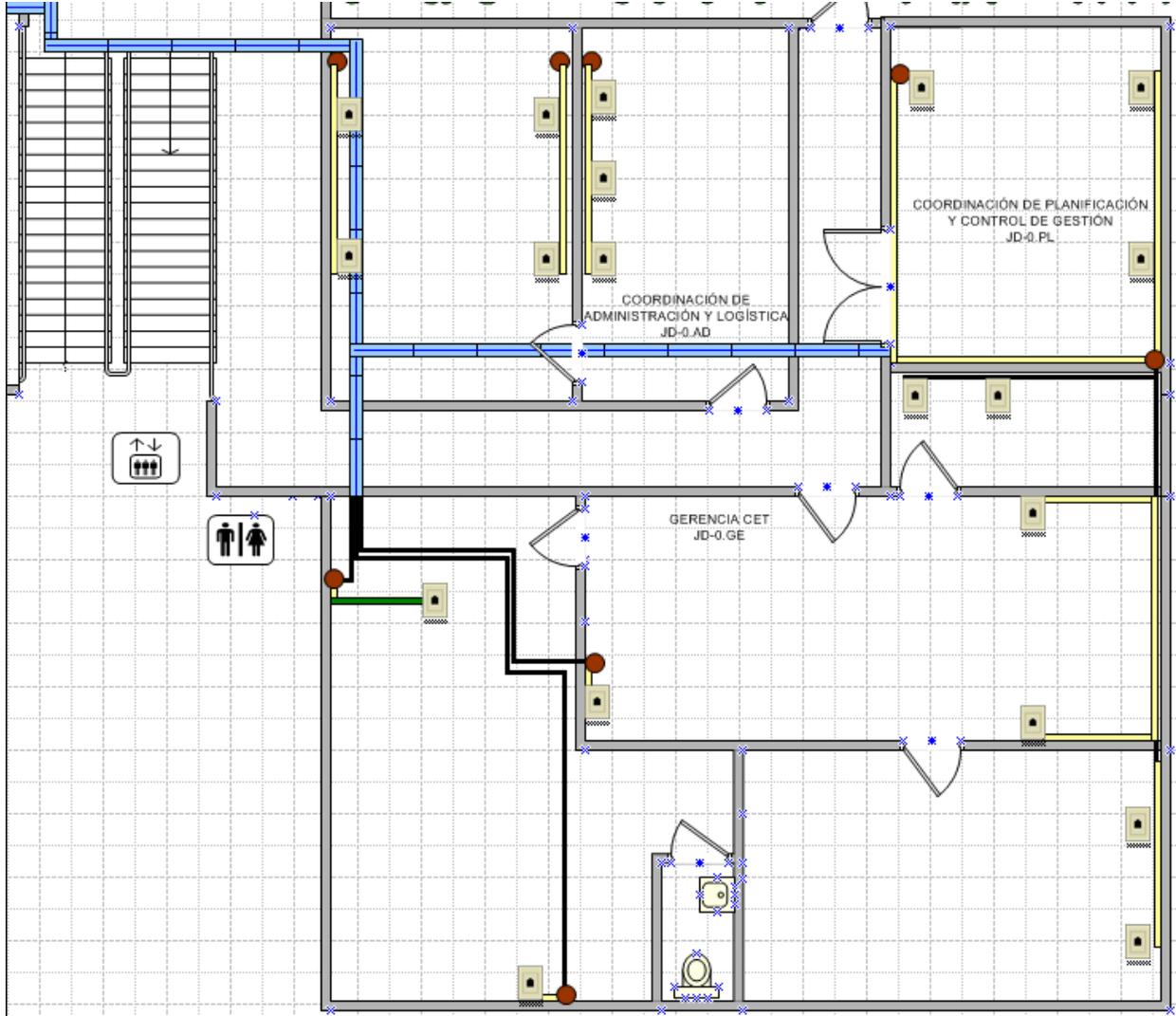


**ANEXO 3**  
**PLANO DE EQUIPOS PISO 2**

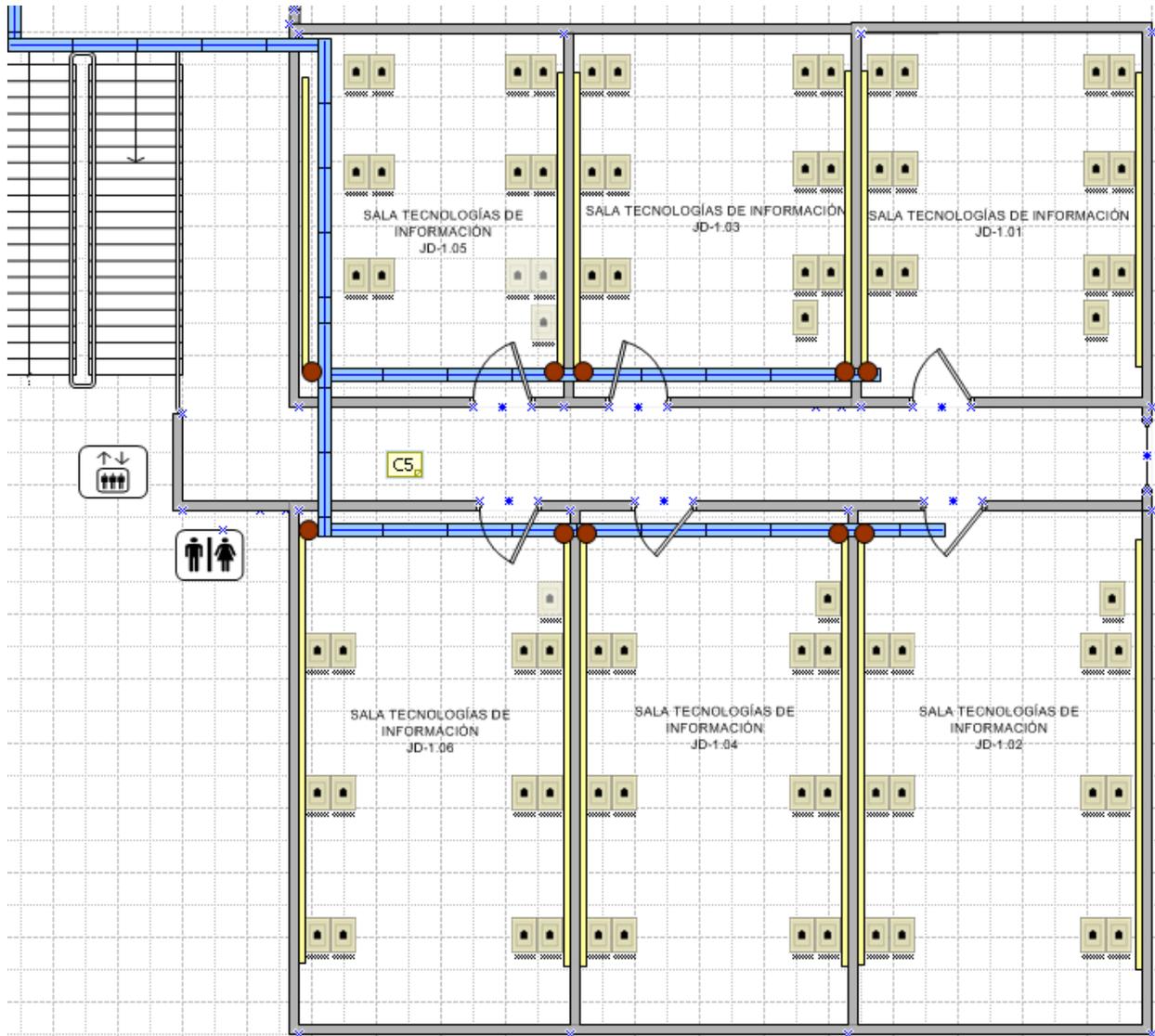


# ANEXO 4

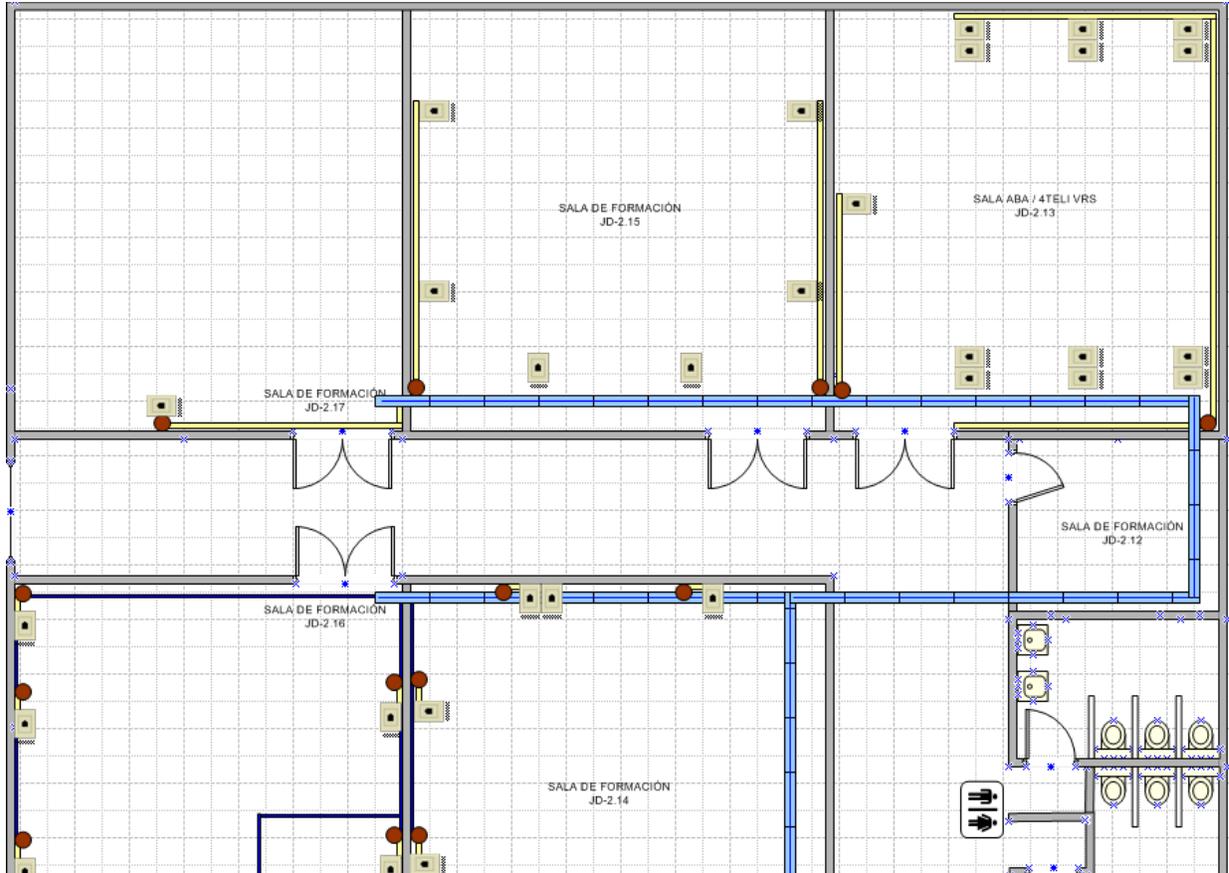
## PLANO CABLEADO PLANTA BAJA



**ANEXO 5**  
**PLANO CABLEADO PISO 1**

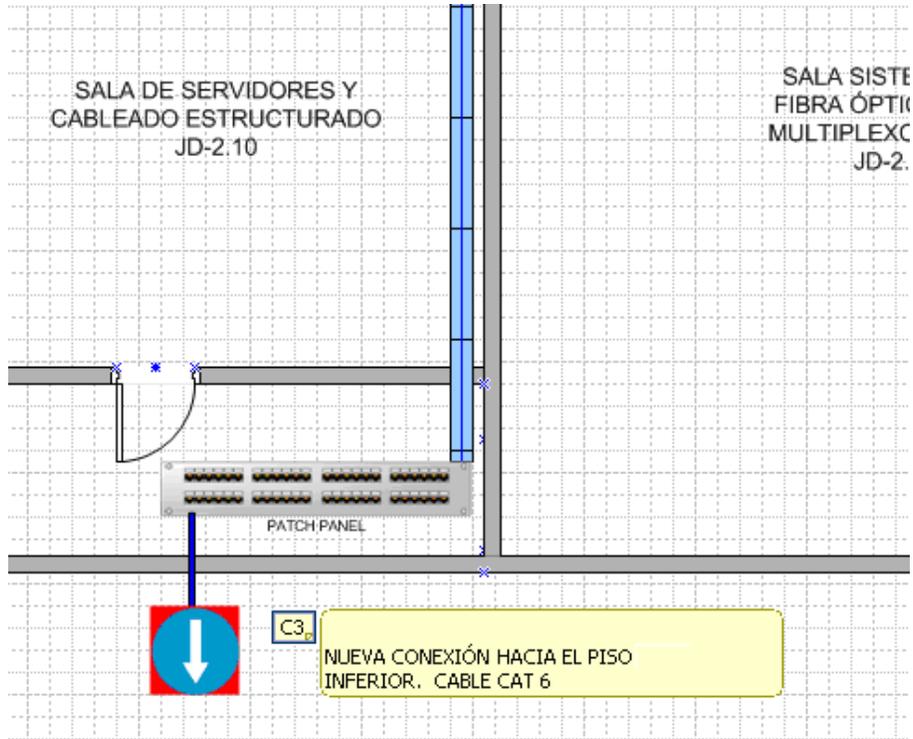


**ANEXO 6**  
**PLANO CABLEADO PISO 2**



## ANEXO 7

### EJEMPLO COMENTARIO CABLEADO PISO 2



## ANEXO 8

### EJEMPLO CARACTERÍSTICAS PC PISO 1

Custom Properties - PC.406	
Número de activo	
Número de serie	KCZMST4
Ubicación	JD-2.05
Edificio	JAN DECKET, PISO 2
Sala	TECNOLOGÍAS DE INFORMACIÓN
Fabricante	IBM
Número de producto	
Número de pieza	MT-M 8188-375
Descripción del producto	IBM ThinkCentre (color negro)
Nombre de red	
Dirección IP	163.196.41.143
Máscara de subred	255.255.255.0
Interfaz administrativa	
Número de puertos	1
Cadena de comunidad	
Descripción de red	Tarjeta de red 10/100/1000 Mbps
Dirección MAC	
CPU	PENTIUM 4 DE 2.8 GHz
Memoria	256 MB de RAM
Sistema operativo	Microsoft Windows XP
Capacidad del disco duro	60 GB
Departamento	

TECNOLOGÍAS DE INFORMACIÓN JD-2.05

COORDINACIÓN DE PLANIFICACIÓN Y CONTROL DE GESTIÓN JD-2.01

SISTEMAS DE RED DE ACCESO Y ENERGÍA JD-2.04

SISTEMAS DE DATOS JD-2.02

## ANEXO 9

### EJEMPLO RESUMEN PUNTOS DE RED PISO 2

CÓDIGO	OFICINA/SALA	PC CONECTADO	DIRECCIÓN IP	CONECTADO AL SWITCH	Nº PUERTO
JD-2.01-001	JD-2.01. COORD. PLANIFICACIÓN Y CONTROL DE GESTIÓN	KCDH5GW	163.196.41.167	Sw-JD2-1	2
JD-2.01-002	JD-2.01. COORD. PLANIFICACIÓN Y CONTROL DE GESTIÓN	KCDZ1NF	163.196.41.166	Sw-JD2-1	3
JD-2.01-003	JD-2.01. COORD. PLANIFICACIÓN Y CONTROL DE GESTIÓN	KZDZBTN	163.196.41.169	Sw-JD2-1	4
JD-2.01-004	JD-2.01. COORD. PLANIFICACIÓN Y CONTROL DE GESTIÓN	KCZM5V2	163.196.41.168	Sw-JD2-1	5
JD-2.02-005	JD-2.02. SISTEMAS DE DATOS.	KCDH5MC	163.196.41.165	Sw-JD2-1	6
JD-2.02-006	JD-2.02. SISTEMAS DE DATOS.	KCDH6BW	163.196.41.164	Sw-JD2-1	7
JD-2.02-007	JD-2.02. SISTEMAS DE DATOS.	KCDH6HP	163.196.41.163	Sw-JD2-1	8
JD-2.02-008	JD-2.02. SISTEMAS DE DATOS.	KCZM6HO	163.196.41.162	Sw-JD2-1	9
JD-2.02-009	JD-2.02. SISTEMAS DE DATOS.	KCZM5N3	163.196.41.161	Sw-JD2-1	10
JD-2.02-010	JD-2.02. SISTEMAS DE DATOS.	KCZM5NO	163.196.41.160	Sw-JD2-1	11
JD-2.02-011	JD-2.02. SISTEMAS DE DATOS. (Impresora de Red)	QSB44371	163.196.41.184	Sw-JD2-1	12
JD-2.04-012	JD-2.04. SISTEMAS DE RED DE ACCESO Y ENERGÍA	ZKZM6G7	163.196.41.159	Sw-JD2-1	13
JD-2.04-013	JD-2.04. SISTEMAS DE RED DE ACCESO Y ENERGÍA	ZCDH5HP	163.196.41.158	Sw-JD2-1	14
JD-2.04-014	JD-2.04. SISTEMAS DE RED DE ACCESO Y ENERGÍA	ZKZM5V9	163.196.41.157	Sw-JD2-1	15
JD-2.04-015	JD-2.04. SISTEMAS DE RED DE ACCESO Y ENERGÍA	ZCZM5P1	163.196.41.156	Sw-JD2-1	16
JD-2.04-016	JD-2.04. SISTEMAS DE RED DE ACCESO Y ENERGÍA	KCZM5XO	163.196.41.155	Sw-JD2-1	17
JD-2.04-017	JD-2.04. SISTEMAS DE RED DE ACCESO Y ENERGÍA	ZCZN1T4	163.196.41.154	Sw-JD2-1	18
JD-2.05-018	JD-2.05. TECNOLOGÍAS DE INFORMACIÓN	KCDZ9RL	163.196.41.175	Sw-JD2-1	19
JD-2.05-019	JD-2.05. TECNOLOGÍAS DE INFORMACIÓN	KCDZ8MB	163.196.41.176	Sw-JD2-1	20

## ANEXO 10

### EJEMPLO DE DISPONIBILIDAD DE PUERTOS DEL SWITCH N° 1 DEL PISO 2

DESCRIPCIÓN DEL SWITCH	Nº PUERTOS	DISPONIBILIDAD
Sw-JD2-1	1	Usado
Sw-JD2-1	2	Usado
Sw-JD2-1	3	Usado
Sw-JD2-1	4	Usado
Sw-JD2-1	5	Usado
Sw-JD2-1	6	Usado
Sw-JD2-1	7	Usado
Sw-JD2-1	8	Usado
Sw-JD2-1	9	Usado
Sw-JD2-1	10	Usado
Sw-JD2-1	11	Usado
Sw-JD2-1	12	Usado
Sw-JD2-1	13	Usado
Sw-JD2-1	14	Usado
Sw-JD2-1	15	Usado
Sw-JD2-1	16	Usado
Sw-JD2-1	17	Usado
Sw-JD2-1	18	Usado
Sw-JD2-1	19	Usado
Sw-JD2-1	20	Usado
Sw-JD2-1	21	Usado
Sw-JD2-1	22	Usado
Sw-JD2-1	23	Usado
Sw-JD2-1	24	Usado

***ANEXO 11***

***CÁMARA DE VIGILANCIA INSTALADA EN EL EDIFICIO JAN DEKETH***



***ANEXO 12***

***CÁMARA DE VIGILANCIA INSTALADA EN LA ENTRADA PRINCIPAL DEL EDIFICIO JAN DEKETH***



### ***ANEXO 13***

#### ***CÁMARA DE VIGILANCIA INSTALADA EN LA SOTEA DEL EDIFICIO ARVELO***



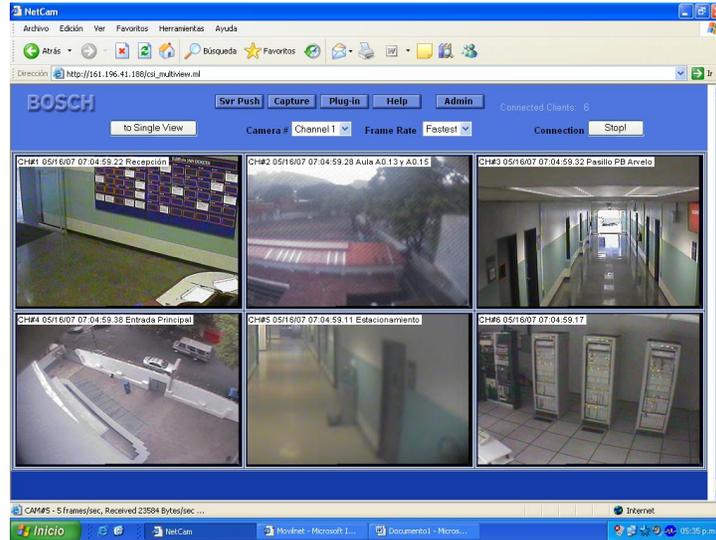
### ***ANEXO 14***

#### ***CÁMARA DE VIGILANCIA INSTALADA EN EL PISO 2 DEL EDIFICIO JAN DEKETH***



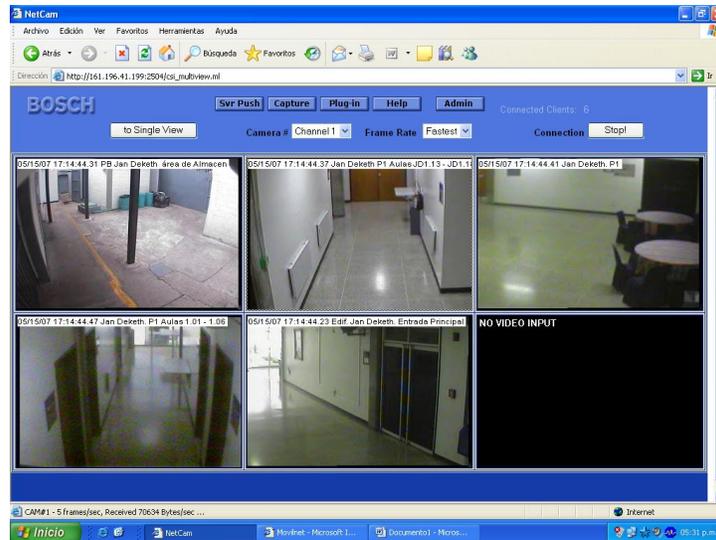
## ANEXO 15

### CÁMARA DE VIGILANCIA INSTALADA EN EL PISO 2 DEL EDIFICIO JAN DEKETH



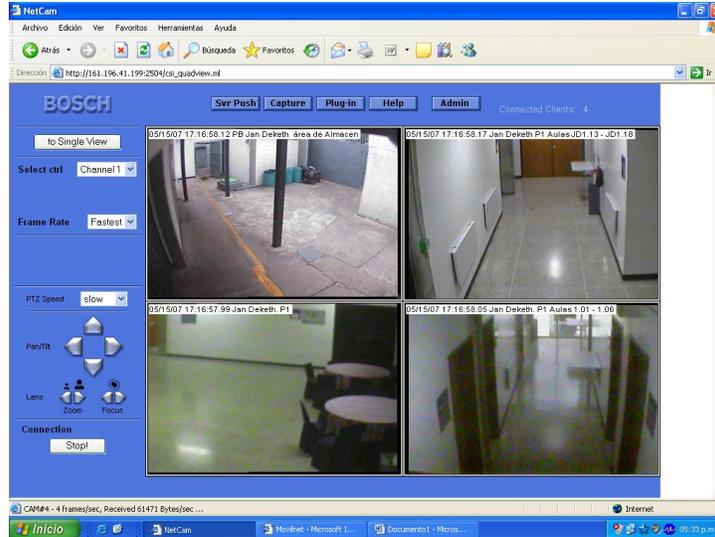
## ANEXO 16

### CÁMARA DE VIGILANCIA INSTALADA EN EL PISO 2 DEL EDIFICIO JAN DEKETH



## ANEXO 17

### CÁMARA DE VIGILANCIA INSTALADA EN EL PISO 2 DEL EDIFICIO JAN DEKETH



## ANEXO 18

### VISTA PÁGINA PRINCIPAL



## ANEXO 19

### VISTA PÁGINA INFORMACIÓN GENERAL

The screenshot shows a web browser window displaying the 'Gerencia Corporativa de Formación' website. The page is titled 'Información general' and features a navigation menu with options: Home, Información general, Conocimientos, Competencias, Preguntas frecuentes, and Postulación. The main content area is divided into several sections:

- Cine foros**: A list of categories including Viajes, Responsabilidad social, Movitraining, and Contactos de RRHH.
- Cineforos**: A list of items to project, including:
  - Películas a proyectar
  - Programación
  - Proceso de postulación
  - Planilla de postulación
  - Guía de selección y Análisis de películas
  - Registro en el PID de Acciones No formales
  - Personas contacto
- Proceso de postulación**: A section for participants in the Region Capital, detailing the steps for participating in the cine forum cycle.
- Películas a proyectar**: A section displaying movie posters for 'Capitán de Ebla y Genes', 'Chocolat', 'Hotel Rwanda', 'Troja', 'Oraciones de fuego', and 'Arraigados'.

## ANEXO 20

### VISTA PÁGINA CONOCIMIENTOS

The screenshot shows a web browser window displaying the 'Gerencia Corporativa de Formación' website, specifically the 'Conocimientos' page. The page features a navigation menu with options: Home, Información general, Conocimientos, Competencias, Preguntas frecuentes, Postulación, and Formación Atención total. The main content area is divided into several sections:

- Definición**: A section defining knowledge as the response to direct needs of the work environment, including procedures, context, methods, instruments, and technologies.
- Conocimientos cubiertos**: A section detailing the requirements for competent execution of a position.
- Conocimientos no cubiertos**: A section detailing the requirements for competent execution of a position.
- Niveles de conocimientos**: A section detailing the requirements for competent execution of a position.

## ANEXO 21

### VISTA PÁGINA COMPETENCIAS



## ANEXO 22

### VISTA PÁGINA PREGUNTAS FRECUENTES



## ANEXO 23

### VISTA PÁGINA POSTULACIÓN

The screenshot shows a web browser window displaying the 'Gerencia Corporativa de Formación' website. The page title is 'Gerencia Corporativa de Formación'. The main navigation menu includes 'Home', 'Información general', 'Conocimientos', 'Competencias', 'Preguntas frecuentes', 'Postulación', and 'Formación Atención Total'. The 'Postulación' section is active, featuring a sidebar with links: 'Gestión de entrenamiento', 'Recomendaciones', 'Ventajas', and 'Proceso inscripción en línea'. The main content area is titled '¿Cómo postularme para una acción presencial Nacional e Internacional?' and lists 'Acciones de formación voluntarias' and 'Acciones de formación abiertas', with sub-categories for 'Nacionales' and 'Internacionales'. An image of a modern office space is visible in the top right.

## ANEXO 24

### VISTA PÁGINA ATENCIÓN TOTAL

The screenshot shows a web browser window displaying the 'Estrategia de Formación Atención Total' website. The page title is 'Estrategia de Formación Atención Total'. The main navigation menu includes 'Home', 'Información general', 'Conocimientos', 'Competencias', 'Preguntas frecuentes', 'Postulación', and 'Formación Atención Total'. The 'Formación Atención Total' section is active, featuring a sidebar with links: 'Modalidades de Formación', 'Rol del tutor de formación', 'Rol del facilitador', 'Cronograma', 'Plan de Formación', 'Unidades', 'Usuarios finales', 'Área de soporte (help desk)', and 'Archivo de noticias'. The main content area is titled '¿Cuáles serán las modalidades de Formación en Atención Total?' and describes 'Educación en línea' and 'Presenciales'. An image of a person working at a computer is visible in the top right.

## GLOSARIO DE TÉRMINOS

**10BASE-T.** Se trata del estándar IEEE 802.3 para ethernet con una velocidad de transmisión de 10 Mbps que utiliza un cable UTP (par trenzado sin apantallar), 10BASE-T utiliza una topología en estrella, que es más robusta y ofrece más seguridad, pero que requiere un dispositivo central común.

**ANCHO DE BANDA.** Diferencia entre las frecuencias más altas y más bajas disponibles para las señales de red. Asimismo, la capacidad de rendimiento medida de un medio o protocolo de red determinado.

**ANSI.** American National Standards Institute. Un grupo que certifica a organizaciones que desarrollan estándares en Estados Unidos para la industria del proceso de la información. Los grupos acreditados por ANSI participan en la definición de los estándares del protocolo de red.

**APLICACIÓN.** Un programa de PC, como un procesador de textos o una hoja de cálculo electrónica; o bien, un grupo de secuencias de comandos y componentes ASP que realizan esas tareas.

**APLICACIÓN WEB.** Elementos que conforman un sitio Web o una porción distinta de un sitio Web organizados en un directorio raíz virtual.

**AUTENTICACIÓN.** Con respecto a la seguridad, la verificación de la identidad de una persona o proceso.

**ATM.** (Asynchronous Transfer Mode). Una tecnología de red, que transfiere paquetes de datos para el posterior reenvío de diferentes tipos de información (Video, datos, entre otros).

**ATENUACIÓN.** Pérdida de energía de la señal de comunicación.

**BACKBONE.** Núcleo estructural de la red, que conecta todos los componentes de la red de manera que se pueda producir la comunicación.

**BROADCAST.** Paquete de datos enviado a todos los nodos de una red. Los broadcasts se identifican por una dirección broadcast. Comparar con multicast y unicast. Ver también dirección broadcast, dominio de broadcast y tormenta de broadcast.

**BPS.** Bits por segundo, es una medida de la velocidad con que se transmiten los datos.

**BROWSER (NAVEGADOR).** Software del cliente, que se utiliza para buscar informaciones en las distintas páginas WEB; Netscape y Microsoft Internet Explorer son los más populares.

**BYTE.** Un caracter de información, usualmente de ocho bits.

**CABLE DE FIBRA ÓPTICA.** Medio físico que puede conducir una transmisión de luz modulada. En comparación con otros medios de transmisión, el cable de fibra óptica es más caro, pero por otra parte no es susceptible a la interferencia electromagnética, y permite obtener velocidades de datos más elevadas. A veces se denomina fibra óptica.

**COLISIÓN.** En Ethernet, el resultado de dos nodos que transmiten simultáneamente. Las tramas de cada dispositivo impactan y se dañan cuando se encuentran en el medio físico.

**CONFIABILIDAD.** Proporción entre los mensajes de actividad esperados y recibidos de un enlace. Si la relación es alta, la línea es confiable. Utilizado como métrica de enrutamiento.

**CONGESTIÓN.** Tráfico que supera la capacidad de la red.

**CONMUTACIÓN.** Proceso de tomar una trama entrante de una interfaz y enviarla a través de otra interfaz.

**DATAGRAMA.** (datagram) La unidad transmitida entre un par de módulos de internet. El Protocolo Internet provee para transmitir bloques de datos, llamados datagramas, desde el origen a destinos. El Protocolo Internet no provee una facilidad para comunicación confiable. No hay reconocimientos ya sea extremo a extremo o escala por escala. No hay control de errores para los datos, solamente un checksum (chequeo de suma) en el encabezado. No hay retransmisiones. No hay control de flujo. Véase IP.

**DIRECCIÓN IP.** Dirección del Protocolo de Internet. Una dirección única que identifica a un equipo host en una red. Identifica a un equipo como una dirección de 32 bits que es única en una red TCP/IP. Una dirección IP se suele representar en una notación decimal con puntos que indica cada octeto (ocho bits o un byte) de una dirección IP como su valor decimal y separa cada octeto con un punto. Por ejemplo: 102.54.94.97.

**DIRECCIÓN DE RED.** Dirección de capa de red que se refiere a un dispositivo de red lógico, en lugar de físico. También denominada dirección de protocolo.

**DIRECCIÓN DE SUBRED.** Parte de una dirección IP especificada como la subred por la máscara de subred.

**DIRECCIÓN DESTINO.** Dirección de un dispositivo de red que recibe datos. Ver también dirección origen.

**DIRECCIÓN MAC.** (Control de Acceso al Medio). Dirección de capa de enlace de datos estandarizada que se necesita para cada puerto o dispositivo que se conecta a una LAN. Otros dispositivos de la red usan estas direcciones para ubicar dispositivos específicos en la red y para crear y actualizar las tablas de enrutamiento y las estructuras de los datos. Las direcciones MAC tienen 6 bytes de largo, y son controladas por el IEEE. También se denominan direcciones de hardware, dirección de capa MAC o dirección física. Comparar con dirección de red.

**DIRECCIÓN MULTICAST.** Dirección única que se refiere a múltiples dispositivos de red. Sinónimo de dirección de grupo. Comparar con dirección broadcast y dirección unicast. Ver también multicast.

**DIRECCIÓN ORIGEN.** Dirección de un dispositivo de red que envía datos.

**DOMINIO.** Una colección de equipos definida por el administrador de una red que comparten una base de datos de directorios común. Un dominio proporciona acceso a las cuentas de usuario y las cuentas de grupo centralizadas mantenidas por el administrador del dominio. Cada dominio tiene un nombre único.

**DNS.** El Domain Name System (sistema de nombres de dominio) es un mecanismo usado en el Internet para traducir nombres de servidores a direcciones.

**ENCABEZADO.** (header) La porción de un paquete precediendo los datos propiamente dichos, contiene las direcciones de origen y destino, además de campos para chequeo de errores.

**ESTÁNDAR.** Conjunto de reglas o procedimientos de uso generalizado o de carácter oficial.

**ETHERNET.** Un estándar de redes para los niveles "hardware" y "data link". Hay dos tipos de Ethernet: Digital/Intel/Xerox (DIX) y IEEE 802.3.

**EXTENSIONES DE SERVIDOR DE FRONTPAGE.** Un grupo de archivos instalados en un servidor Web para conceder a ese servidor la capacidad de proporcionar funcionalidad especial de Microsoft FrontPage. Con las extensiones de servidor de FrontPage, los administradores pueden ver y administrar un sitio Web mediante una interfaz gráfica. Además, los autores pueden crear, modificar y exponer páginas Web en IIS de forma remota.

**FAST ETHERNET.** Se basa en una extensión de la especificación IEEE 802.3. Ver también Ethernet. varias especificaciones de Ethernet de 100-Mbps. Fast Ethernet ofrece un incremento de velocidad diez veces mayor que el de la especificación de Ethernet 10BaseT, aunque preserva características tales

**FIREWALL.** Router o servidor de acceso, o varios routers o servidores de acceso, designados para funcionar como búfer entre redes de conexión pública y una red privada. Un router de firewall utiliza listas de acceso y otros métodos para garantizar la seguridad de la red privada.

**FORMMANAGER.** Usado para crear conjuntos de formularios controlados por eventos, por ejemplo, formularios de entrada de datos con los modos Examinar, Modificar e Insertar.

**FORMULARIO.** En la publicación en Web, una página o parte de una página Web que el usuario completa y devuelve al servidor para su procesamiento.

**FTP.** File Transfer Protocol. El protocolo de alto nivel estándar de Internet para transferencia de archivos desde una computadora a otra.

**GIF.** Formato de intercambio de gráficos. Un formato de archivo de gráficos desarrollado a mediados de los 80 por CompuServe y utilizado en la presentación de imágenes gráficas de calidad fotográfica en las pantallas de los equipos. Ahora se suele utilizar en Internet.

**GB.** Gigabyte. Una unidad de almacenamiento de datos cuyo tamaño representa 2 elevado a la 30 (1,073,741,824), expresado comúnmente como mil millones de bytes. Header Véase encabezado.

**GBPS.** (gigabytes por segundo). Medida de velocidad de transferencia.

**HIPERTEXTO.** Texto estándar dentro de las páginas Web, se comporta de la misma manera que el texto convencional con la única manera que contiene Hipervínculos a otros documentos Web.

**HIPERVÍNCULOS.** Vínculos directos incluidos en páginas Web que permiten a los usuarios pasar de un documento a otro relacionado sin en donde resida este en Internet.

**HOME PAGE.** Página principal en un servidor y es la primera página que el usuario ve cuando se conecta con la dirección del servidor Web.

**HUB.** (Concentrador) Dispositivo para el tratamiento de datos que permite encaminar hacia un computador central, a través de una sola línea de transmisión, los mensajes procedentes de los terminales asociados.

**HTML.** Hypertext Markup Language.

**HTTP.** Hypertext Transfer Protocol (Transport según Expansión).

**IEEE.** Institute for Electrical and Electronics Engineers. Asociación profesional que define estándares y especificaciones.

**IEEE802.** Estos son los estándares para la conexión física y eléctrica de LAN's desarrollado por IEEE.

**IEEE802.3 BASE5.** Especificación de la IEEE que iguala en antiguo producto de AT&T StarLAN.

**INTERNET.** Abreviatura inglesa de internetwork. Un conjunto de redes de equipos diferentes conectadas mediante gateways que se encargan de la transferencia de datos y la conversión de mensajes de la red que los envía a los protocolos usados por la red que los recibe. Estas redes y gateways usan el conjunto de protocolos TCP/IP.

**IIS (Internet Information Server).** Permite configurar una máquina con el sistema operativo Windows NT como servidor Web, FTP y Gopher.

**INTERNET EXPLORER.** Navegador de la casa de Software Microsoft usado para el recorrido de la World Wide Web.

**IP.** Internet Protocol. El protocolo a nivel de red para el Internet. Es un protocolo datagrama para intercambio de paquetes definido en el RFC.

**ISL (inter.-switch link).** Es un protocolo propietario de Cisco para interconectar multiples switches y mantener información VLAN, tales como tráfico entre switches. ISL proporciona capacidades VLAN en puertos FastEthernet en modo full o half duplex. Se ejecuta en puertos Trunk y es altamente recomendado. ISL funciona en la capa 2 del modelo OSI, encapsulando la trama con una cabecera y un CRC. Además es independiente del protocolo que se utilice en la capa superior.

**ISO (Organización Internacional para la Normalización).** Organización internacional que tiene a su cargo una amplia gama de estándares, incluyendo aquellos referidos al networking. ISO desarrolló el modelo de referencia OSI, un modelo popular de referencia de networking.

**JAVASCRIPT.** Un lenguaje de secuencias de comandos que evolucionó a partir del lenguaje LiveScript de Netscape y que se hizo más compatible con Java. Utiliza una página HTML como interfaz.

**JPEG.** Joint Photographic Expert Group (Grupo de expertos en fotografía). Un estándar internacional ampliamente aceptado para la compresión de archivos de imágenes en color, utilizado a veces en Internet.

**MAC (Control de Acceso al Medio).** Parte de la capa de enlace de datos que incluye la dirección de 6 bytes (48 bits) del origen y del destino, y el método para obtener permiso para transmitir. Ver también capa de enlace de datos y LLC.

**MÁSCARA DE SUBRED.** Máscara utilizada para extraer información de red y subred de la dirección IP.

**MULTICAST.** Paquetes únicos copiados por una red y enviados a un conjunto de direcciones de red. Estas direcciones están especificadas en el campo de dirección del destino. Comparar con broadcast y unicast.

**NAT (traducción de direcciones de red).** Mecanismo que reduce la necesidad de tener direcciones IP exclusivas globales. NAT permite que las organizaciones cuyas direcciones no son globalmente exclusivas se conecten a la Internet transformando esas direcciones en espacio de direccionamiento enrutable global. También denominado traductor de dirección de red.

**NIC (tarjeta de interfaz de red).** Tarjeta que brinda capacidades de comunicación de red hacia y desde un computador. También denominada adaptador

**NAVEGADOR.** Software cliente usado para la búsqueda de paginas colocadas en el Web.

**PÁGINA DINÁMICA.** Una página Web creada automáticamente basándose en la información proporcionada por el usuario.

**PÁGINA ESTÁTICA.** Páginas HTML preparadas antes de recibir la petición y enviadas al cliente cuando las solicita. Esta página no requiere ninguna acción especial cuando se solicita.

**PING (búsqueda de direcciones de internet).** Mensaje de eco ICMP y su respuesta. A menudo se usa en redes IP para probar el alcance de un dispositivo de red.

**KB. Kilobyte.** Una unidad de almacenamiento de datos cuyo tamaño representa 2 elevado a la 10 (1,024), expresado comúnmente como mil bytes.

**KBPS.** Kilo Bist por segundo, se refiere a miles de Bist por segundo.

**LAN** Local Area Network. Una red que toma ventaja de la proximidad de las computadoras para ofrecer comunicaciones relativamente más eficientes u de más alta velocidad que redes de largo alcance o área amplia.

**MAN.** (Metropolitan Area Network)

**MB** Megabyte. Una unidad de almacenamiento de datos cuyo tamaño representa 2 elevado a la 20 (1,048,576), expresado comúnmente como un millón de bytes.

**MBPS.** Mega Bist por Segundo o millones de Bist por segundo.

**NETWORK.** Red. Es un grupo de dispositivos de cómputo interconectados entre sí para propósitos de comunicación.

**NIC.** Network Information Center. Una organización que provee a los usuarios de red con información acerca de servicios provistos por la red.

**NOS.** Network Operating System. El software que controla los recursos de la red, así como la distribución de los archivos, correo electrónico, impresión, dispositivos de seguridad, entre otros.

**NÚMERO DE SUBNET** (subnet number) Una parte de la dirección Internet que designa una subnet. Es ignorado para los propósitos del enrutamiento de Internet pero es usado para enrutamiento intranet.

**OSI.** Open Systems Interconnection. Un grupo de protocolos designados para ser un método estándar internacional para conectar computadoras y redes diferentes. Europa ha hecho la mayor parte del trabajo desarrollando OSI y probablemente lo usará tan pronto como sea posible.

**OSI.** Reference Model El modelo de referencia OSI es un "croquis" de OSI que define sus siete capas y sus funciones. Algunas veces usado para ayudar a describir otras redes.

**PC.** Personal Computer.

**PROTOCOLO.** Es una descripción formal de formatos de mensajes y las reglas que dos computadoras deben seguir para intercambiar esos mensajes. Los protocolos pueden describir detalles de bajo nivel de interfaces máquina a máquina (por ejemplo, el orden en que los bits y los bytes se envían sobre un cable) o intercambios a alto nivel entre programas de asignación (por ejemplo, la forma en que dos programas deben transferir un archivo a través del Internet),.

**REDUNDANCIA.** En interconexión (internetwork), duplicación de dispositivos, servicios o conexiones, de modo que, en caso de que se produzca una falla, los dispositivos, servicios o conexiones redundantes puedan realizar el trabajo de aquellos en los que se produce la falla. 2.

**RENDIMIENTO.** Velocidad de la información que llega a, y posiblemente pase a través de, un punto determinado del sistema de red.

**RFC.** La serie de documentos de Internet Request for Comments. Los RFCs son notas de trabajo de la investigación en internet y la comunidad en desarrollo. Un documento en estas series puede ser esencialmente cualquier tópico relativo a la

comunicación de computadoras y puede ser cualquier cosa desde un reporte de juntas a la especificación de un estándar.

**ROUTER.** Dispositivo de capa de red que usa una o más métricas para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes de una red a otra basándose en la información de capa.

**SEGMENTO.** Sección de una red que está rodeada de puentes, routers o switches 2. En una LAN que usa topología de bus, un circuito eléctrico continuo que a menudo está conectado a otros segmentos similares a través de repetidores. 3. En la especificación TCP, una unidad única de información de capa de transporte. Los términos datagrama, trama, mensaje y paquete también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

**SERVIDOR.** (server) Una computadora que comparte sus recursos, tales como impresoras y archivos, con otras computadoras en la red. Un ejemplo de esto es un servidor Network File System (NFS) el cual comparte su espacio en disco con una o más estaciones de trabajo que pueden no tener discos locales.

**SITIO WEB.** Conjunto de una o más aplicaciones web organizadas bajo un único dominio. Se utilizan para reflejar la imagen de una organización en la Internet y publicar información tanto interna como de dominio público.

**SOFTWARE CISCO IOS** (sistema operativo de internetnetwork). Software de sistema de Cisco que proporciona funcionalidad, escalabilidad y seguridad comunes a todos los productos bajo la arquitectura CiscoFusion. El software Cisco IOS permite la instalación y administración centralizada, integrada y automatizada de internetnetwork,

garantizando al mismo tiempo la compatibilidad con una amplia variedad de protocolos, medios, servicios y plataformas.

**SPANNING TREE.** Subconjunto sin bucles de una topología de red de Capa 2 (conmutada).

**SMTP (Simple Mail Transfer Protocol).** El protocolo estándar de Internet para transferir mensajes de correo electrónico de una computadora a otra.

**SWITCH.** Es un dispositivo electrónico de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconnection). Un Switch interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

**TRAMA.** Agrupamiento lógico de información enviada como unidad de capa de enlace de datos a través de un medio de transmisión. A menudo se refiere al encabezado y a la información final, utilizadas para la sincronización y control de errores, que rodean los datos del usuario contenidos en la unidad. Los términos datagrama, mensaje, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

**TIEMPO DE DISEÑO.** El periodo de tiempo durante el cual un usuario construye una aplicación en el entorno de desarrollo agregando controles, estableciendo las propiedades de los controles o los formularios etc. Por el contrario, durante el tiempo de ejecución, un usuario interactúa con la aplicación.

**TCP.** Transmission Control Protocol. Un protocolo de la capa transporte para Internet. Es un protocolo de flujo orientado a la conexión, definido por el RFC 793.

**TCP/IP.** Transmission Control Protocol/Internet Protocol. El protocolo default usado por sistemas Unix para rutear paquetes de información sobre una red de área local o amplia. Es el protocolo estándar en que está basado Internet. Esta abreviatura se refiere al grupo de protocolos de aplicación y transporte que corren sobre IP.

**TELNET.** El protocolo estándar de Internet para el servicio de conexión remota. TELNET permite a un usuario en un sitio interactuar con un sistema remoto de tiempo compartido en otro sitio como si la terminal del usuario estuviera conectada directamente a la computadora remota.

**UDP.** User Datagram Protocol. Un protocolo para la capa transporte para el Internet. Es un protocolo datagrama que añade un nivel de confiabilidad y multiplexión a los datagramas IP. Está definido en RFC 768.

**USUARIO.** Persona que utiliza un computador o sistema informático, pero que no es especialista en informática, ni dispone de instrucciones específicas para su utilización.

**URL.** Uniform Resource Locator, denominación estándar de la dirección en la World Wide Web, por ejemplo <http://www.pnptech.com/>

**UTP.** Acrónimo de Unshielded Twisted Pair, par trenzado no apantallado; se trata de un cable fino muy utilizado en las instalaciones de cables de redes.

**UPS.** Equipos electrónicos especiales que, mediante un sistema de baterías, puede seguir suministrando corriente alterna después de haber ocurrido un apagón sin que lo detecten los equipos conectados a ellos.

**VLAN (LAN virtual).** Grupo de dispositivos de una LAN que están configurados (usando el software de administración) de tal modo que se pueden comunicar como si estuvieran conectados al mismo cable, cuando, en realidad, están ubicados en una serie de segmentos de LAN distintos. Debido a que las LAN virtuales están basadas en conexiones lógicas en lugar de físicas, son extremadamente flexibles.

**WAN** Wide Area Network. (Red de Área Extensa).

**WWW** World Wide Web. Sistema basado en hipermedia para organizar información dentro de Internet. Contiene archivos que incluyen texto, imágenes y sonido.