Capítulo 1

Plan de Implementación de la red Institucional del IEMS

1.1. Objetivo del documento

Establecer de manera detallada el plan de implementación a seguir para la ejecución de las actividades inherentes del proyecto de Red Institucional del Instituto de Educación Media Superior.

1.2. Objetivo del proyecto

El objetivo es el rediseñar la red actual a un esquema seguro, confiable y escalable a futuras tecnologías como telefonía IP y videoconferencias y sobre todo una red que sea de fácil operación.

Para contar con un esquema seguro es necesario cubrir diversas vulnerabilidades con las que cuenta las redes del Instituto actualmente. Entre ellas por mencionar algunas se encuentra la nula administración de los equipos de acceso, la falta de políticas de acceso a servidores, la vulnerabilidad que implican las redes inalámbricas, la falta de homologación de firewalls [2] de las oficinas centrales y planteles y la nula separación de tráfico de acuerdo a máquinas ajenas al Instituto.

Una red confiable es aquella que asegura que el tráfico llega al destino sin pérdida de información. El implementar una red Wide Access Network (WAN) permitirá tener un mejor ancho de banda para la transferencia de archivos críticos como bases de datos, inscripciones, evaluaciones, etc.

Para lograr que la red funcione durante un tiempo prolongado y responda de manera exitosa a cambios tecnológicos, es necesario pensar en escalabilidad. Se requiere una red pensada al crecimiento y que tenga la flexibilidad adecuada para migrar a diferentes tecnologías IP. El diseño basado en Virtual LANs (VLANS), así como el adecuado direccionamiento de la red es fundamental para lograr dicho fin.[2, pag.41]

Es indispensable también que la nueva red sea de fácil administración, porque una red compleja generalmente trae problemas a largo plazo. Si no se automatizan los procesos, la red se vuelve inmanejable, así como también es necesario capacitar constantemente a nuevos trabajadores para que puedan administrar adecuadamente la red.

El proyecto consiste en implementar una red institucional de tipo WAN que considere a cada plantel del IEMS como parte de un segmento de la red Local Area Network (LAN), con lo que se logrará una infraestructura integrada que ofrecerá mejor rendimiento y una administración más eficaz de los recursos y datos.

Así mismo, proveer al IEMS niveles de servicio para la atención de incidentes de seguridad y de red.

[2] Firewall o Cortafuegos es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

1.3. Propuestas tecnológicas de los enlaces

Para lograr una interconexión entre los planteles con el plantel central, se invitó a diferentes empresas a ofrecer soluciones. Entre las opciones sugeridas fueron las siguientes:

- Conexión punto-multipunto mediante enlaces Site-to-Site Internet Protocol Security (IPsec) Virtual Private Network (VPN)
- Conexión tipo malla basada en tecnología Multiprotocol Label Switching (MPLS)
- Conexión punto-multipunto basada en tecnología LAN extendida

La solución mediante enlaces VPN resultó atractiva en cuanto a costos de servicio ya que bastaba con un servicio Asymmetric Digital Subscriber Line (ADSL) para cubrir las necesidades de conexión. Sin embargo era necesaria la instalación de servidores de VPN tanto en los planteles como en las oficinas centrales. La tecnología VPN es ineficiente en cuanto al overhead[3] que se agrega a los paquetes de datos, los encabezados se ven incrementados debido a que se requiere encapsular los Protocol Data Unit (PDU) para ser transmitidos por Internet; esto junto con la asimetría en cuanto a subida y bajada del servicio ADSL traería como consecuencia una lentitud en la transmisión de datos entre planteles y oficinas centrales. Otro aspecto a considerar son aquellos relacionados con la disponibilidad del enlace a Internet. Ya que se haría uso del enlace infinitum (típicamente de 2 **Mb/s!** (**Mb/s!**) por plantel.) con el que ya cuentan los planteles, presentaría problemas de cortes de servicio y lentitud en ciertos periodos.[1, pag.39]

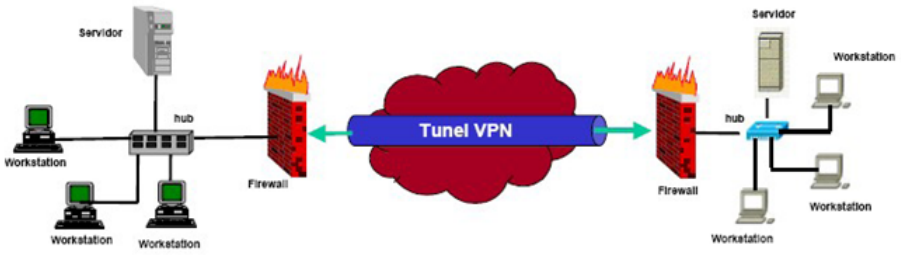

Figura 1.1: Diagrama típico de conexión VPN tipo site to site

Una opción bastante interesante era aquella realizada con tecnología MPLS, que es aquella ofrecida por Teléfonos de México (TELMEX) como su mejor oferta del mercado. Éste tipo de tecnología se adapta perfectamente al proyecto de interconexión porque ofrece conexiones dedicadas y separación de servicios en base al tipo de tráfico. Además que lógicamente los planteles se comportan como una red de tipo malla, donde todos se encuentran interconectados entre ellos.[1, pag.174] El problema con ésta tecnología es que resultó inviable en función de los costos ofrecidos por la empresa TELMEX que superaban por mucho al presupuesto asignado.

La modalidad de enlaces dedicados de LAN to LAN o de LAN extendida ofrece un enlace en el cual el IEMS tiene el control total de los protocolos de comunicación usados en él. En

[3]Overhead es el agregar información extra a los encabezados de los paquetes

éste tipo de enlaces el ancho de banda está dedicado a la transmisión de datos y conserva su capacidad de transferencia o throughput todo el tiempo; en contraste con los enlaces Frame-Relay por ejemplo, que comparten el ancho de banda para transmitir, voz, video y datos generados por otros usuarios del Internet Service Provider (ISP).[4]

La tecnología de LAN extendida basa su funcionamiento en la diferenciación de cada cliente de TELMEX mediante VLANS, el ISP en éste caso TELMEX, crea en su red VLANS para cada cliente a éstas VLANS les asigna un valor llamado Customer VLAN (C-VLAN). El cliente entonces recibe una trama con un "tag.º etiqueta de capa 2. El cliente entonces es el encargado de encapsular el tráfico en la VLAN correspondiente para poder transmitir los datos dentro de la nube del proveedor de servicios. Un punto a recalcar es que se tendría que implementar una red de tipo "HUB and SPOKE.º punto multipunto, esto no garantiza la alta disponibilidad de los enlaces ya que si falla el punto central los planteles del IEMS quedarían sin servicio. Por lo tanto ésta solución debe de acompañarse con enlaces alternos para los planteles que le provean de salida a Internet en caso de falla. Los precios ofrecidos por TELMEX en cuanto a la tecnología de LAN extendida se ajustaban a la partida presupuestal, llegando a un acuerdo de servicio e instalación por parte de la compañía sin ningún costo extra.

[4]CCNA Exploration. [Sitio Web] s.l., United States of America : Publicaciones para Academias Cisco, Cisco Networking Academy, 2009. Acceso a la WAN, 3.1.2 Circuitos Virtuales. http://www.cisco.com/web/learning/netacad/index.html.

1.4. Descripción de la situación actual

1.4.1. Diagramas de Interconexión en oficinas centrales

1.4.1.1. Físico

Las Oficinas centrales del IEMS tienen en sus instalaciones 3 secciones que en éste documento se identificarán como:

- Edificion 1. Planta Alta
- Edificio 1. Planta Baja
- Edificio 2. Telecomunicaciones

A continuación se presenta un diagrama Tridimensional (3D) de las instalaciones:

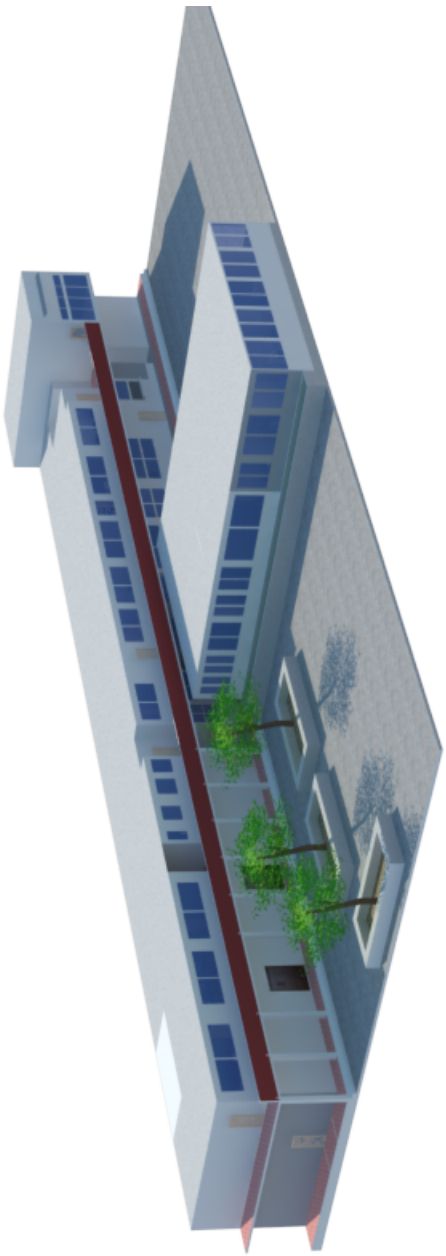

Figura 1.2: Modelo 3D de las oficinas centrales - San Lorenzo

Los cuartos de comunicaciones se encuentran situados en los 3 niveles del inmueble, y brindan servicio el piso que les corresponde con cableado horizontal.

El diagrama 3D se presenta en la figura siguiente:

Figura 1.3: Modelo 3D de las Oficinas centrales - San Lorenzo. Mostrando la ubicación de los cuartos de telecomunicaciones.

1.4.1.2. Lógico

La topología lógica actual del Instituto se encuentra distribuida en un sólo nivel jerárquico, donde todos los switches se encuentran cascadeados[5]

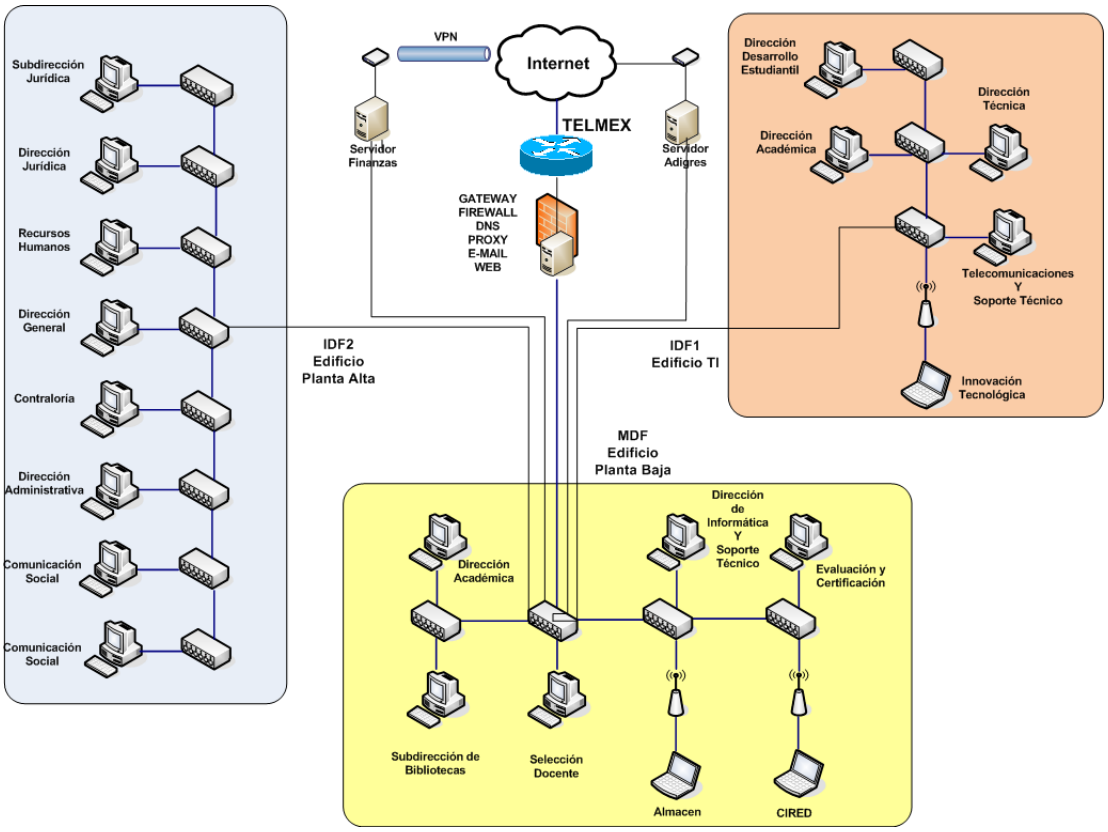

Figura 1.4: Topología Lógica actual en las oficinas centrales

[5]Se le llama cascadear al hecho de conectar uno con otro los switches, típicamente en los switches existen puertos de mayor velocidad designados para dicho fin.

1.4.2. Diagramas de Interconexión en Planteles

1.4.2.1. Físico

Los 18 planteles del Instituto cuentan con una disposición espacial similar, todos cuentan con 2 o 3 edificios conectados entre ellos con fibra óptica. Un diagrama en 3D se presenta a continuación:

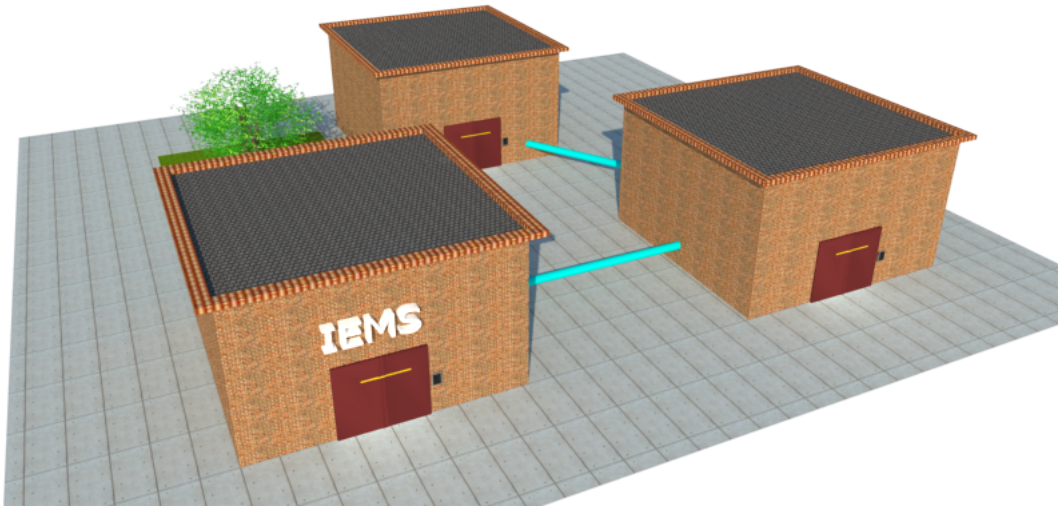

Figura 1.5: Modelo ejemplo de interconexión entre los edificios de los planteles

1.4.2.2. Lógico

Lógicamente los switches de cada plantel se encuentran cascadeados entre ellos. Todos tienen un servidor de filtrado administrado localmente por un administrador de red. Una topología lógica ejemplo de los planteles se encuentra a continuación:

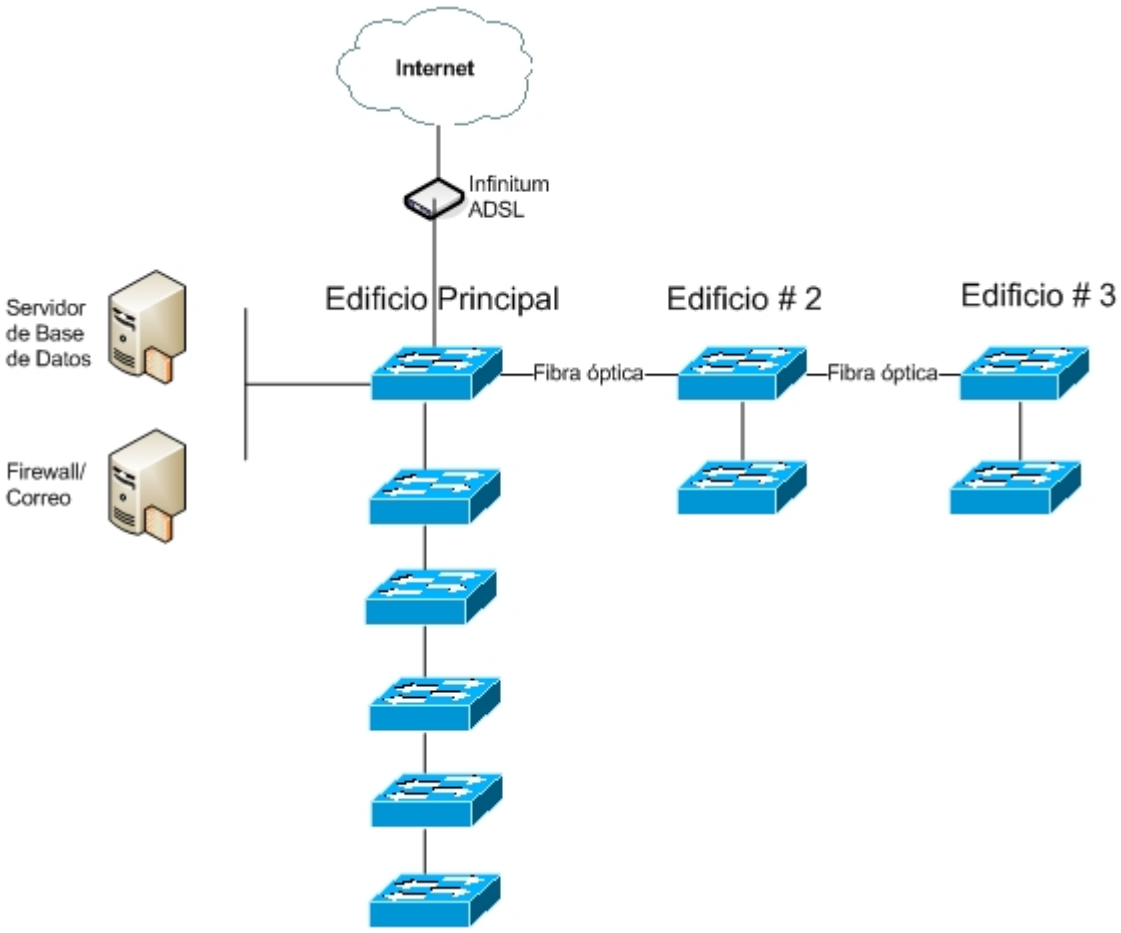

Figura 1.6: Topología lógica actual de los planteles

1.5. Listado de equipos en oficinas centrales

1.5.1. Propietarios de TELMEX

Equipo	Marca	Modelo	Ubicación Física
Módem ADSL	2Wire	2701HG-T Gateway	MDF
Módem ADSL	2Wire	2701HG-T Gateway	MDF
Router	Cisco	2800	MDF

Cuadro 1.1: Listado de equipos en oficinas centrales propietarios de TELMEX

1.5.2. Propietarios del IEMS

1.5.2.1. Edificio 1 - Planta baja

Equipo	Marca	Modelo	Ubicación Física
Switch	3Com	SuperStack3	MDF
Switch	3Com	3300 XM 24 Port	MDF
Switch	Cisco	WS-C2960-24TT-L	MDF
Switch	Cisco	WS-C2960-24TT-L	MDF
Switch	Cisco	WS-C2960-24TT-L	MDF
Switch	3Com	SuperStack3	MDF
AccessPoint	Linksys	WRT320N	Cired
AccessPoint	Linksys	WRT320N-LA	Almacén
AccessPoint	Linksys	WRT320N-V1	Deportes

Cuadro 1.2: Listado de equipos en oficinas centrales propietarios del IEMS. Edificio 1 Planta Baja

1.5.2.2. Edificio 1 - Planta alta

Equipo	Marca	Modelo	Ubicación Física
Switch	Cisco Catalyst 2960	WS-C2960-24TT-L	IDF2
Switch	Cisco Catalyst 2960	WS-C2960-24TT-L	IDF2
Switch	Cisco Catalyst 2960	WS-C2960-24TT-L	IDF2
Switch	3Com	3C16985B	IDF2
Switch	3Com	2226-SFP PLUS	IDF2
AccessPoint	Linksys	WRT320N-V1	Dirección Administrativa

Cuadro 1.3: Listado de equipos en oficinas centrales propietarios del IEMS. Edificio 1 alta

1.5.2.3. Edificio 2

Equipo	Marca	Modelo	Ubicación Física
Switch	3Com	3C16985B	IDF1
Switch	3Com	3C16980A	IDF1
AccessPoint	Linksys	WRT320N-V1	Dirección de Innovación
AccessPoint	Linksys	WRT320N-V1	Telecomunicaciones

Cuadro 1.4: Listado de equipos en oficinas centrales propietarios del IEMS. Edificio 2

1.5.2.4. Servidores

Equipo	Marca	Modelo	Servicio	Ubicación Física
Servidor	LANIX	BRIAN	Web Principal	MDF
Servidor	DELL	POWEREDGE 2900	Web2 Inscripciones	MDF
Servidor	LANIX	BRIAN	Base de Datos Almacén	MDF
Servidor	COMPAQ	EVO	VPN Finanzas	MDF
Servidor	DELL	OPTIPLEX GX 620	Web de Servidor 7	MDF
Servidor	DELL	OPTIPLEX GX 620	VPN de Finanzas2	MDF
Servidor	DELL	POWEREDGE 6800 620	Base de Datos Alumnos	MDF

Cuadro 1.5: Listado de equipos en oficinas centrales propietarios del IEMS. Área de Servidores

1.5.3. Personal que conforma las actividades

El siguiente personal conforma el grupo que estará trabajando a lo largo de cada fase de este proyecto:

Área de Telecomunicaciones: Se encargará de llevar a cabo las fases que conforman el proyecto, desde la planeación, ejecución, seguimiento y control y cierre del proyecto. Dentro de las actividades que se incluyen son: Sondeo de mercado, contratación de proveedor de la solución de interconexión, separación de servicios de red, segmentación de la red LAN de las Oficinas centrales, creación de backbone en oficinas centrales, creación de entorno WAN en Oficinas centrales, supervisión de instalación de enlaces por parte del proveedor de servicios, instalación de firewalls en cada plantel, instalación de HUB receptor de enlaces en oficinas centrales, fase de pruebas, fase de producción, documentación técnica y creación de políticas de acceso a la red.

Soporte de segundo nivel a los usuarios de los planteles y de primer nivel a los usuarios de oficinas centrales.

Personal	Puesto	Actividad que realiza
Mtro. Hugo Zúñiga Barragán	Director de Informática y Telecomunicaciones	Supervisar las actividades
M.I.S.E. Salim Salomón Torres Medina	Subdirector de Informática y Telecomunicaciones	Supervisar las actividades
Ing. Alberto Ávalos Vélez	Jefe del área de Telecomunicaciones	Dirigir al área de telecomunicaciones, configurar equipos
Ing. Juan Antonio Pérez Vargas	Docente Tutor Investigador	Documentar el avance del proyecto
Ing. Sergio García Sandoval	Enlace	Instalar y cablear, atención a usuarios
Juan José Ponce Domínguez	Líder Coordinador de Proyectos	Diseño y coordinación del proyecto, configurar equipos.

Cuadro 1.6: Personal que conforma las actividades

Jefes de Unidad Departamental de Apoyo Técnico: Entrega de información actualizada sobre la red del plantel que administran, Diagrama Topológico, Identificación de nodos e inventarío de equipos. Apoyo al área de Telecomunicaciones en la instalación y configuración del segmento de red correspondiente a cada uno de ellos. Soporte de primer nivel a los usuarios de los planteles.

TELMEX: Instalación de los enlaces punto a punto de cada uno de los 18 planteles hacia las oficinas centrales e instalación de equipo routeador para salida a internet de 40 Mb/s.

1.6. Descripción de la solución

Ya que el Instituto actualmente se comporta como diferentes redes separadas unas de las otras, para poder interconectarlas es necesario instalar varios equipos en cada plantel y en las oficinas centrales, así como de un proveedor de Internet que interconecte todos los sitios.

Las oficinas centrales del IEMS servirán como nodo concentrador del tráfico que se genere en todos los sitios, así como del tráfico generado en las mismas oficinas. Es por ello que primero debemos de preparar la red de las oficinas centrales para tal transición.

Dichos cambios deberán entonces ser acordes al modelo de buenas prácticas ofrecido por Cisco llamado *Enterprise Composite Model*[2, pag. 15], donde se define una red basada en capas y jerarquías, de acuerdo al tipo de tráfico que se atraviesa por las mismas. A continuación se presenta dicho modelo.

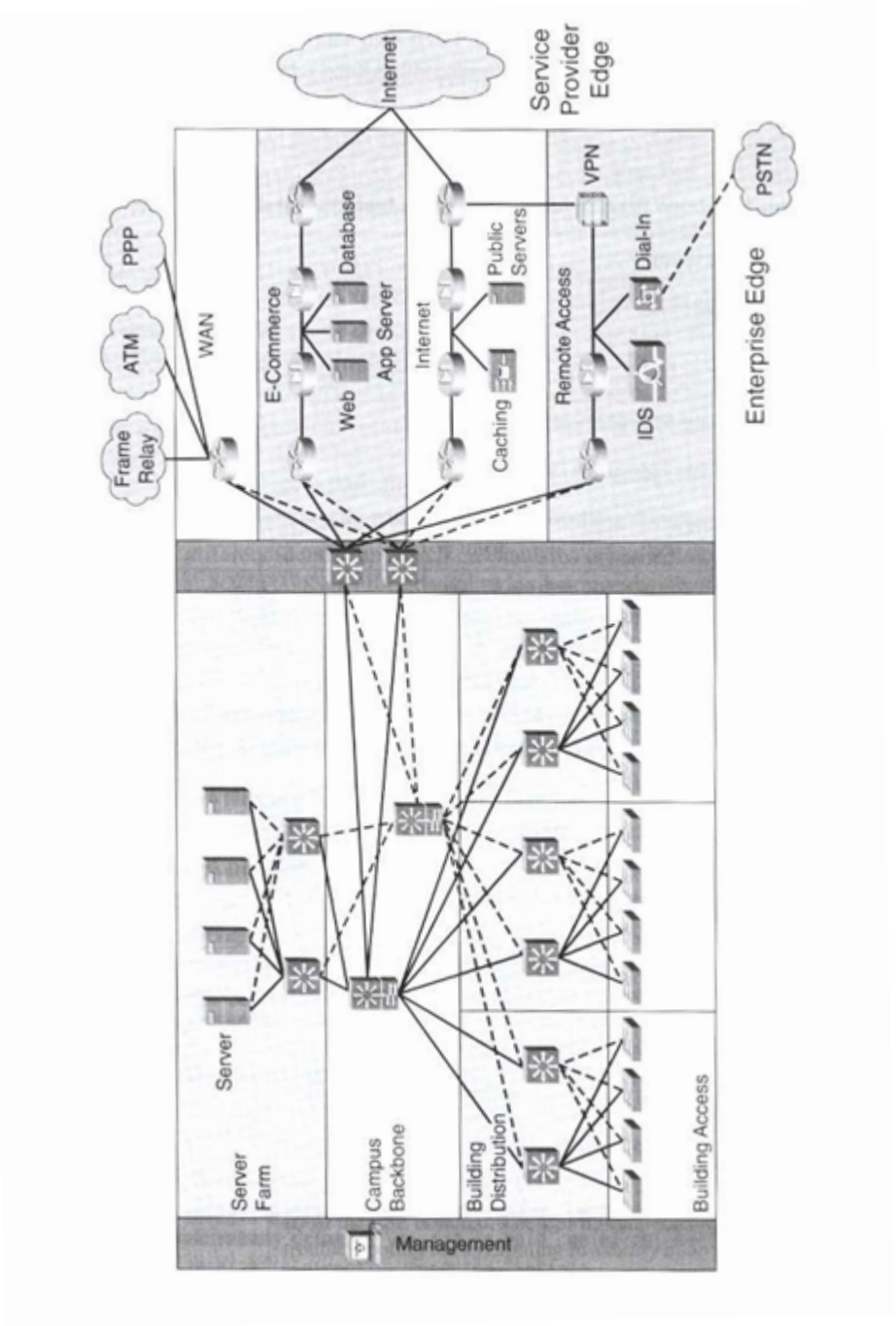

Figura 1.7: Enterprise Composite Model.

Podemos observar en la figura anterior que el modelo se divide en tres secciones:

- Enterprise campus.
- Enterprise edge.
- Service provider edge.

Estas tres secciones deberán estar comprendidas en las oficinas centrales, donde la parte LAN será la capa de acceso, distribución y backbone y el área WAN será entonces la granja de servidores y las conexiones hacia el proveedor de servicios (TELMEX).

Entonces debemos dividir la red central en subredes más manejables mediante VLANS, las VLANS serán definidas en base a la ubicación física de los usuarios de la red, y también separar el tráfico de los usuarios al tráfico de administración.

La red en las oficinas centrales tendrá dos servidores de Dynamic Host Configuration Protocol (DHCP) para manejar las direcciones IP más fácilmente, los servidores se encontraran en alta disponibilidad. Éstos dotarán a las máquinas del IEMS de una dirección IP con privilegios mediante su dirección Media Access Control (MAC), aquellas máquinas nuevas donde su MAC aún no se encuentra registrada en la red se les presentará un portal cautivo[6] indicándoles que deben solicitar el servicio de internet por oficio con los administradores de la red; éstas máquinas sólo tendrán routeo de manera local.

Se tendrá entonces una red jerárquica donde el nivel de acceso serán Switches CISCO administrados en la VLAN de administración (Vlan1), el nivel de distribución serán dos Switches con etherchannel o múltiples enlaces para darle redundancia y mayor capacidad a los enlaces; uno de ellos servirá como servidor VLAN Trunking Protocl (VTP) para mantener consistentemente las VLANS creadas en toda la red. Finalmente el núcleo, Core o Backbone, será provisto de dos firewall-router con Pfsense[7] que usa como sistema operativo FreeBSD, éstos equipos se encargarán de otorgar las direcciones IP a los usuarios y de hacer el routeo intervlan y routeo hacia la WAN con separación de tráfico administrativo, de datos, de voz y de video.

En la WAN de las oficinas centrales se instalará un Switch, dos firewalls en alta disponibilidad y los servidores. El Switch servirá para dividir las VLANS de tráfico administrativo, de datos, de voz, de video y contingencia. Dentro de la VLAN de tráfico administrativo se encontrarán los servidores y los equipos de comunicaciones (VLAN1), dentro de la VLAN de datos (1000) se encontrará todo el tráfico generado por las máquinas del IEMS, las VLANs de voz (2000) y video (3000) quedarán preparadas para hacer cruzar el tráfico generado por teléfonos IP y por las videoconferencias. Finalmente, la VLAN de contingencia (192), proporcionará salida a internet en caso de cualquier contingencia o necesidad de enviar el tráfico a internet por un enlace alterno al principal dotado de 4MB por un módem ADSL.

Los Firewalls estarán instalados con Pfsense al igual que los de las LAN, pero estos firewalls tendrán como servicios el bloqueo de tráfico no deseado desde internet hacia la red,

[6] Un portal cautivo (o captivo) es un programa o máquina de una red informática que vigila el tráfico HTTP y fuerza a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal.

[7] Pfsense es una distribución basada en el sistema operativo FreeBSD que incorpora un firewall/router en un equipo y ofrece una solución similar a equipos comerciales de alto costo y rendimiento. Comenzado en el 2004 a partir de la distribución de m0n0wall. www.pfsense.org.

SNORT[8] para aislar máquinas que violen las políticas, Port Forward para redireccionar las peticiones al puerto 80 hacia el servidor de filtrado y realizará Port Address Translation (PAT)[9].

Por último, la red de los planteles se mantendrá lógicamente igual, sólo se instalará en la punta un servidor firewall-router en Pfsense, que al igual que el de las oficinas centrales se encargará de brindar direcciones IP a los usuarios en base a su perfil, los perfiles se explicarán más adelante en éste documento, en éstas redes de los planteles no se usarán VLANS aún, ya que los Switches 3COM de acceso no se encuentran administrados y están en proceso de renovación por Switches de la marca Cisco.

1.6.1. Propuesta de Interconexión

1.6.1.1. Propuesta - Lógico de la red LAN de las Oficinas Centrales

Podemos observar en la Figura 1.9 la LAN que se implementará en las oficinas centrales, dicha LAN tendrá todos los Switches de la marca Cisco administrados todos ellos con una IP de la VLAN1, ésta VLAN solo será accesible para los administradores de la red.

Las VLAN 100, 200 y 300 separarán el dominio de broadcast en 3 partes y estarán asignadas en función de la ubicación física de los equipos terminales.

Existirá una VLAN 400 para dispositivos de telefonía IP, actualmente el conmutador es de telefonía tradicional, es un Private Branch Exchange (PBX) Panasonic TDE200, y cuenta con aproximadamente 120 extensiones analógicas y 2 extensiones con teléfonos IP. Éste PBX entonces tiene la capacidad de manejar extensiones IP, actualmente sólo se está utilizando en dos teléfonos, pero si se desea agregar más extensiones de éste tipo se debe de adquirir un licenciamiento lo cual resulta poco atractivo. Se planea una migración a telefonía IP utilizando un servidor con Asterisk[10].

[8] Snort es un sniffer de paquetes y un detector de intrusos basado en red

[9] Port Address Translation (PAT) es una característica del estándar NAT, que traduce conexiones TCP y UDP hechas por un host y un puerto en una red externa a otra dirección y puerto de la red interna. Permite que una sola dirección IP sea utilizada por varias máquinas de la intranet. Con PAT, una IP externa puede responder hasta a 64000 direcciones internas.

[10] Asterisk es un programa de software libre (bajo licencia GPL) que proporciona funcionalidades de una central telefónica (PBX). Como cualquier PBX, se puede conectar un número determinado de teléfonos para hacer llamadas entre sí e incluso conectar a un proveedor de VoIP o bien a una RDSI tanto básicos como primarios.

En algunos casos también se hará uso de dispositivos inalámbricos en modo Wireless Switch, en éste modo no existe una IP para administrarlos y el DHCP que otorgará las direcciones serán los firewall Routers, para lograr éste tipo de Access Points transparentes se debe de conectar el enlace WAN en un puerto LAN del Switch. De la siguiente forma:

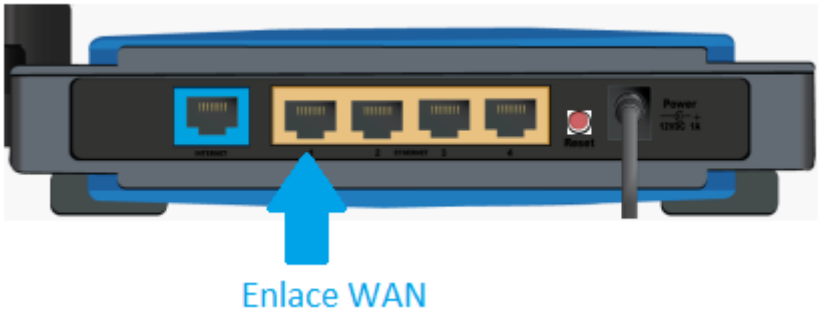

Figura 1.8: Conexión de Access Point en modo Wireless Switch

Estos usuarios inalámbricos estarán en una VLAN independiente y abierta e insegura, el portal cautivo en el Firewall-Router les indicará que están accesando bajo su riesgo y que no existirá conexión a los servidores, éste servicio no tendrá filtrado alguno y está pensado para aquellos que traen laptops al Instituto. El ancho de banda estará limitado a 1 Mb/s para todos los usuarios.

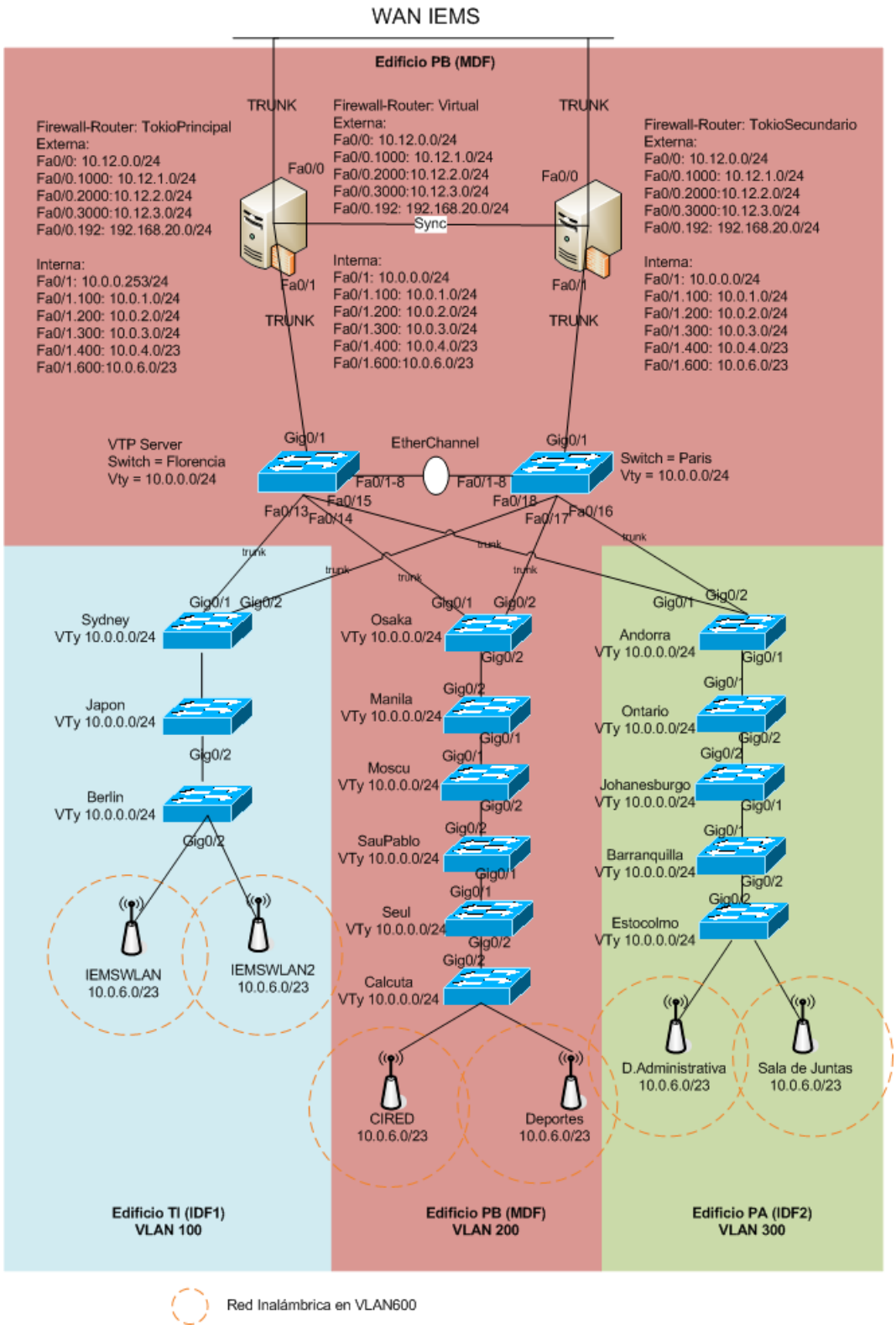

Figura 1.9: Diseño nuevo de la red LAN en las oficinas centrales

1.6.1.2. Propuesta - Lógico de la red WAN en Oficinas Centrales

La WAN de las oficinas centrales se encuentra compuesta de diversos equipos repartidos en las oficinas centrales, equipos del proveedor de servicios y equipos en los planteles.

El diagrama lógico de la WAN se encuentra dividido para su comprensión en 2 figuras, la Figura 1.10 donde se hace énfasis en las oficinas centrales y la Figura 1.12 donde se presenta ya a los planteles integrados.

En la figura 1.10 se pueden observar a los Firewall TokioPrincipal y TokioSecundario, estos firewalls proveen a la LAN de las oficinas centrales de IP mediante DHCP. Así también éstos tienen conexión en su tarjeta WAN a un Switch llamado México. Los firewall routean los paquetes en base a origen de IP, determinando si los paquetes serán enrutados nuevamente a la LAN, si los paquetes provienen de un dispositivo que genera tráfico de datos y deben ser enrutados a la VLAN1000, si provienen de un dispositivo como un teléfono IP y deben cruzar a la WAN por la VLAN 2000 o si dichos paquetes deberán atravesar a la WAN por la VLAN 3000 debido a que fueron generados por un equipo de videoconferencia. Éste esquema de separación de tráfico en base a VLAN provee la facilidad de crear reglas de Quality of Service (QoS).

El Switch llamado México tiene todas las VLANS de la WAN, éste Switch se encuentra físicamente dividido en dos, en el esquema sólo se señala uno para facilitar la comprensión. El Switch se puede administrar en la VLAN1 y a ésta VLAN1 sólo es accesible por los administradores de las oficinas centrales.

Los equipos Firewall-Principal y Firewall-Secundario son los más importantes de toda la red y al igual que los llamados Tokio, éstos se encontrarán en alta disponibilidad y su sistema operativo será FreeBSD. Éstos firewall Router serán los responsable de realizar el PAT desde adentro hacia afuera de la red, asignación de ancho de banda de internet a oficinas centrales y planteles, balanceo en las salidas de internet (sólo de ser requerido), bloqueo desde direcciones provenientes de Internet, routeo inter-vlan, routeo desde y hacia los diferentes planteles, servidor principal de Domain Name System (DNS), direccionamiento de los paquetes dirigidos al puerto 80 hacia el servidor de filtrado (port-forward), servidor Intrusion Detection System (IDS) e Intrusion Prevention System (IPS) mediante SNORT para bloquear usuarios que violen las políticas de la red como uso de torrents[11] bloqueo de programas mediante Layer7[12] y finalmente logs o registro de tráfico y consumo de ancho de banda.

Como podemos observar existirán dos servicios de internet uno de 4 Mb/s y otro de 40 Mb/s, esto con el fin de utilizar el enlace 4 Mb/s sólo en caso de extrema urgencia, el enlace principal será entonces el de 40 Mb/s y será limitado por los firewalls de 2 Mb/s a cada plantel y de 4 Mb/s a los servidores y oficinas centrales.

[11] Torrent es el archivo generado por el protocolo BitTorrent diseñado para el intercambio de ficheros de igual a igual (en inglés: peer-to-peer o P2P). El protocolo BitTorrent fue desarrollado originalmente por el programador Bram Cohen y está basado en software libre.

[12] Referido a la capacidad de realizar un análisis profundo del tráfico, esto quiere decir que se puede analizar hasta la capa 7 del modelo OSI.

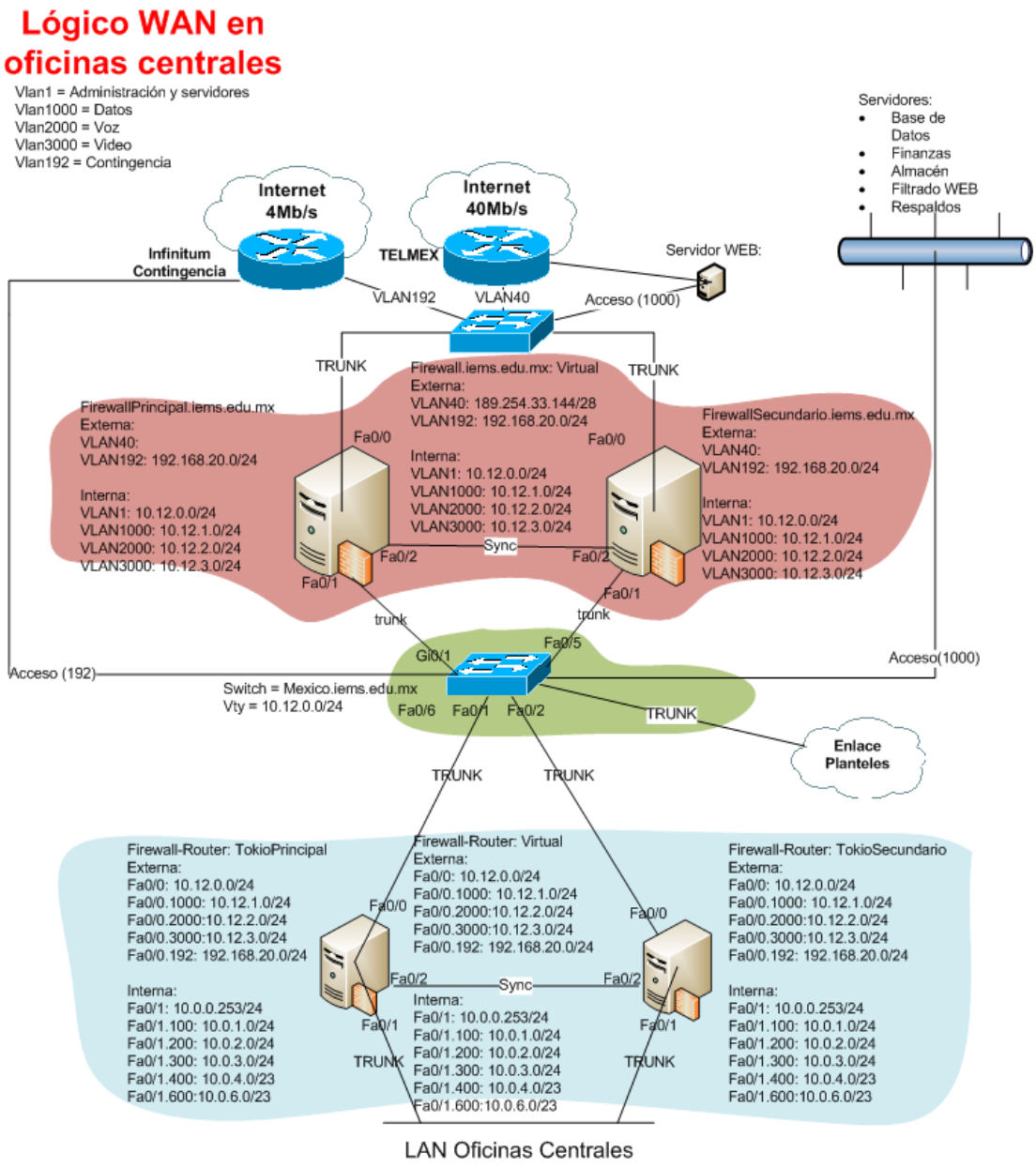

Figura 1.10: Diseño Nuevo de la red WAN en las oficinas centrales

1.6.1.3. Propuesta - Lógico de la red LAN de los planteles

La red LAN de los planteles son actualmente un conjunto de Switches no administrados de la marca 3Com que dan servicio a un máximo de 150 máquinas, 3 servidores y un gateway[13] típicamente el mismo ADSL otorgado por Telmex de la marca 2Wire.

La red de voz y datos de cada uno de los planteles se encuentra a cargo de los Jefes de Unidad Departamental de Apoyo Técnico (JUDs), ellos son entonces los responsables de atender las peticiones que se generen del servicio ahí otorgado, de aplicar las reglas que él considere pertinentes en cuanto al filtrado y seguridad de la red, de otorgar el direccionamiento a las máquinas de la manera que desee, etc.

El esquema traerá cambios a la manera en que la red se administra y se comporta y por consiguiente cambiarán las funciones que cada uno de los JUDs tiene actualmente, ésta reestructuración deberá entonces de ser acompañada de un manual de administración definiendo las nuevas tareas del administrador de red, lo que estará y no a su alcance.

En la figura 1.11 se observa el diagrama a seguir en los planteles, éste esquema pretende contemplar a todos los usuarios y dispositivos que podrían utilizar la red de voz y datos. Se dividieron entonces en 9 perfiles que se definen en la siguiente tabla:

[13] Puerta de enlace

Perfil	Característica	Usuarios Pertenecientes	Segmento
0	DHCP activado, donde a todos los nuevos usuarios se les asigna dirección IP, Sólo routeo local sin salida a internet. Se presenta un portal cautivo donde se indica que tienen conectividad limitada, dicho portal se encuentra en el firewall del plantel de manera local	Todos aquellos que se desea que no tengan salida a internet y sólo acceso local. Aquellos que no importa si tienen dirección IP dinámica.	10.X.0.0/24
1	Dirección IP fija en base a MAC. Salida a internet sólo a páginas Institucionales del IEMS (de tipo 4) (*.iems.edu.mx, *iems.df.gob.mx) y correos personales (yahoo, hotmail, gmail, unam).	A consideración del JUD del plantel.	10.X.1.0/24
2	Dirección IP fija en base a MAC. Salida a internet restringida de tipo 2. (Bloqueo a páginas pornográficas, videos, descargas, etc).	Administrativos. Profesores.	10.X.2.0/24
3	Dirección IP fija en base a MAC. Salida a internet restringida de tipo 3. (Bloqueo a páginas pornográficas, videos, descargas, etc).	Laboratorio de Computo	10.X.3.0/24
4	Dirección IP fija en base a MAC. Salida a internet restringida de tipo 3. (Bloqueo a páginas pornográficas, videos, descargas, etc).	Laboratorio de Internet	10.X.4.0/24
5	Dirección IP fija en base a MAC. Salida a internet restringida de tipo 3. (Bloqueo a páginas pornográficas, videos, descargas, etc).	Laboratorio de Cotic	10.X.5.0/24
6	Dirección IP fija en base a MAC. Salida a internet sin restricciones (de tipo 1).	JUDs de sistemas para fines de prueba. Invitados al plantel que desean internet para exponer, etc.	10.X.6.0/24
7	Dirección IP fija en base a MAC. Salida a internet sin restricciones pero siempre monitoreada (de tipo 1).	Servidores locales. Impresoras.	10.X.7.0/24
8	Dirección IP fija en base a MAC. Solo routeo telefónico de Voz sobre IP.	Teléfonos IP.	10.X.8.0/24
9	Dirección IP fija en base a MAC. Solo routeo de Video.	Máquinas que realicen Videoconferencias	10.X.9.0/24

Cuadro 1.7: Características de perfiles definidos en la propuesta para la red LAN de los planteles

En la tabla anterior se puede observar el tipo de filtrado, éste tipo define que tan restrictivo es el DansGuardian.

El DansGuardian es un software de control de contenidos, diseñado para controlar el acceso a sitios web. Incluye un filtro de virus, importante en sistemas Windows, es usado principalmente en instituciones de educación, gobierno y empresas. Se caracteriza por su alto grado de flexibilidad y adaptación de la implementación.

DansGuardian se instala en un ordenador (servidor) con el sistema operativo GNU/Linux, y filtrará contenidos de webs solicitadas por el resto de ordenadores (independientemente del sistema operativo que tengan instalado). Para filtrar contenido usa comparación de caracteres, filtro Pictures (PICS) y filtro por Uniform Resource Locator (URL).

El mecanismo de filtrado se explica de mejor manera en la sección "Filtrado web con DansGuardian"

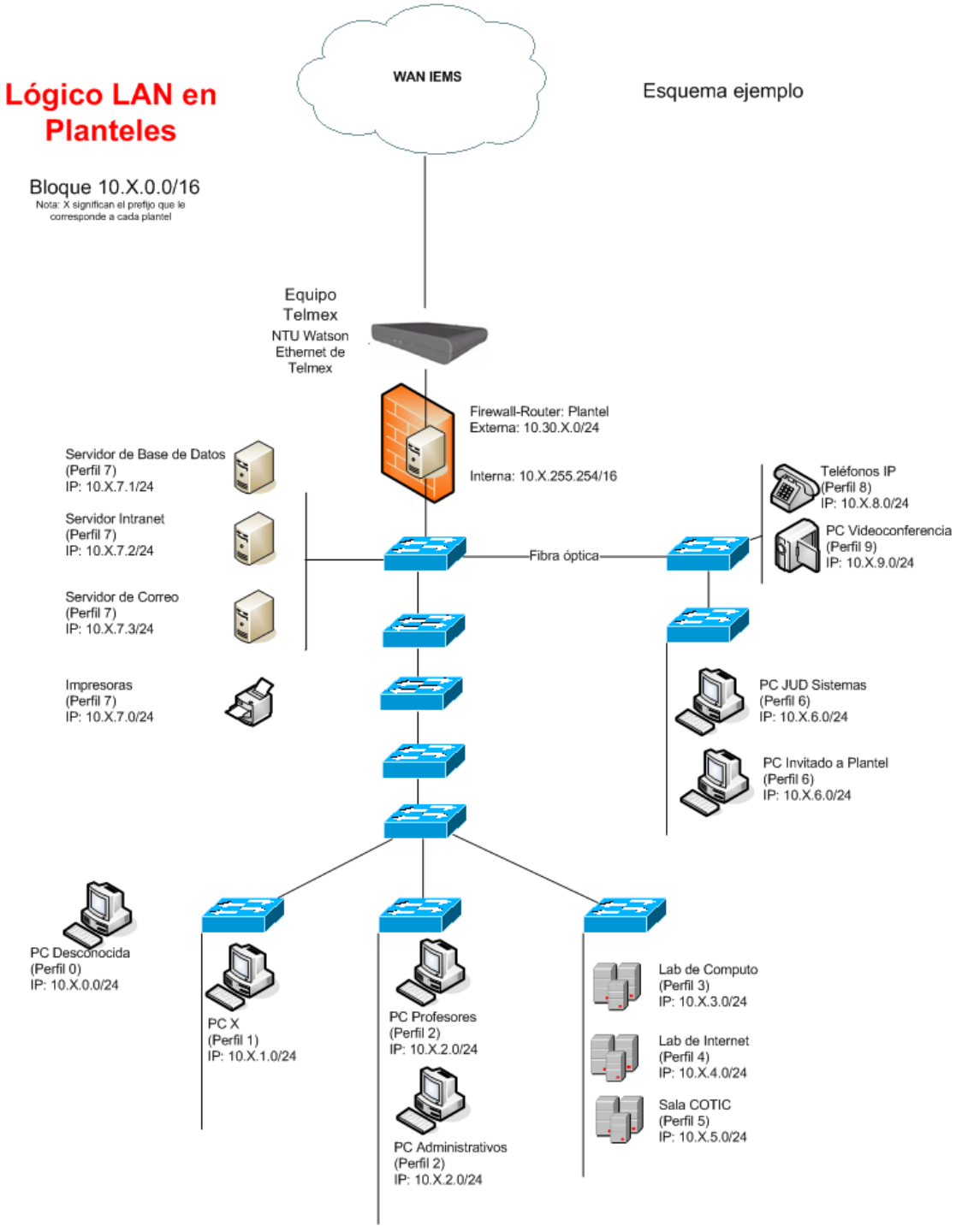

Figura 1.11: Diagrama lógico ejemplo de la nueva red LAN en los planteles

1.6.1.4. Propuesta - Lógico de la Red Institucional

La red institucional integrará entonces las redes de las oficinas centrales, de cada uno de los planteles y de los servidores, con lo que el bloque de direcciones será 10.0.0.0/8.

El filtrado de páginas Red, malla, telaraña (WEB) se realizará de manera centralizada y todos los planteles deberán seguir el esquema LAN anteriormente propuesto de lo contrario el filtrado WEB y el acceso a los servidores se verá afectado.

En la punta WAN de cada uno de los planteles se configurará una IP del tipo 10.30.X.2 donde la X corresponderá a la asignada en la sección "Direccionamiento"de éste documento; éste tráfico deberá de estar contenido en la Service Provider VLAN (S-VLAN) otorgada por el proveedor de servicios. Del otro lado del enlace, en las oficinas centrales, habrá un servidor llamado "HUB"que recibirá cada uno de los enlaces, quitará la S-VLAN de cada uno de los planteles y redireccionará el tráfico agregando la VLAN correspondiente; si es de datos, de voz o de video.

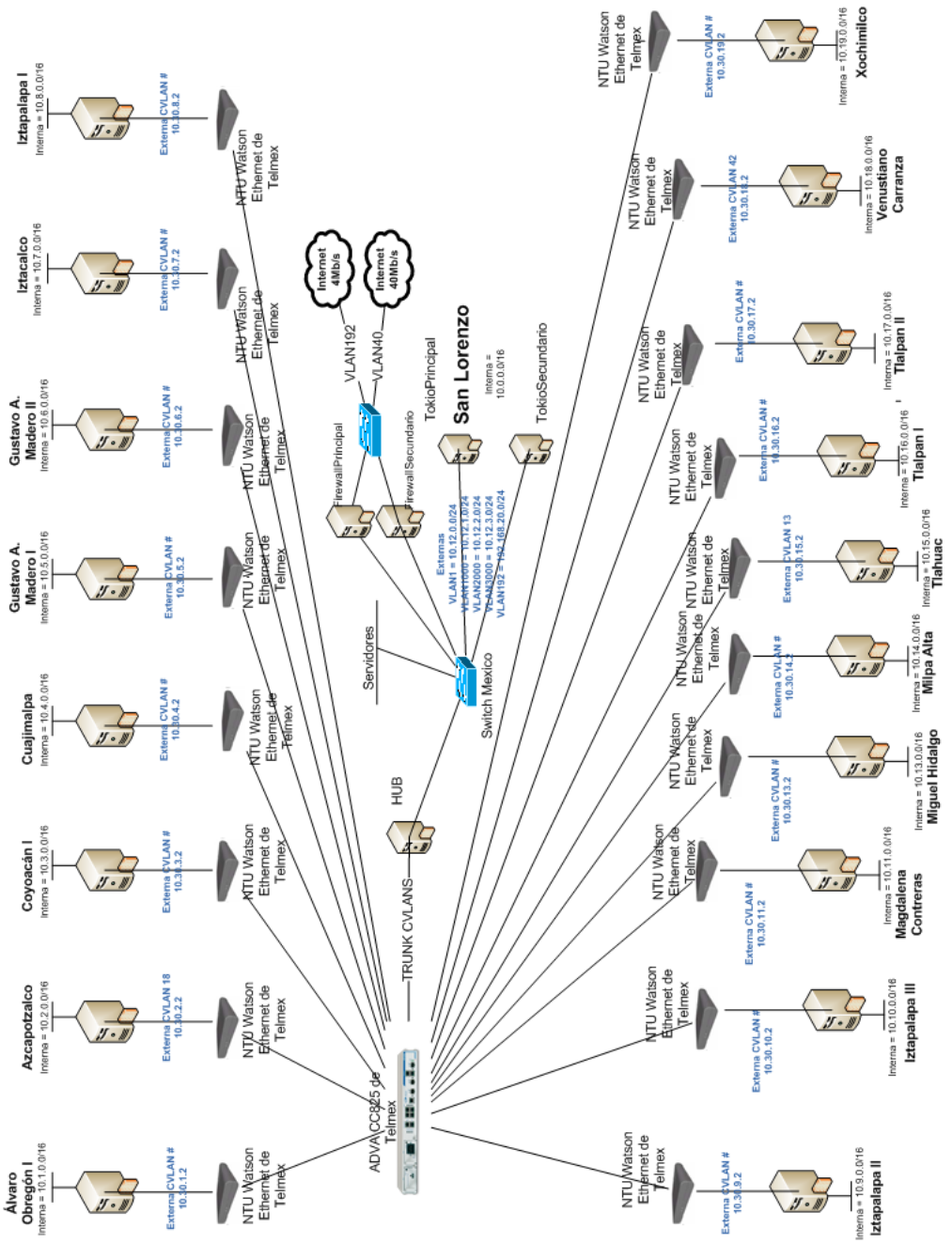

Figura 1.12: Diseño de la red Institucional del IEMS

1.6.2. Equipos nuevos requeridos en la estructura actual

Equipo	Marca	Modelo	Nombre	Ubicación física
Servidor	DELL	POWEREDGE 2900	TokioPrincipal	MDF
Servidor	DELL	POWEREDGE 2900	TokioSecundario	MDF
Servidor	DELL	POWEREDGE 2900	FirewallPrincipal	MDF
Servidor	DELL	POWEREDGE 2900	FirewallSecundario	MDF
Servidor	DELL	-	HUB	MDF
Servidor	DELL	-	FiltradoWEB	MDF
Switch	Cisco	Catalyst 2960 WS-C2960-24TT-L	Mexico	MDF
18 Servidores	-	-	-	En planteles

Cuadro 1.8: Equipos nuevos requeridos en la estructura actual

1.7. Relación de Actividades

1. Separación de Servicios en oficinas centrales - San Lorenzo.
2. Segmentación de la Red de las oficinas centrales - San Lorenzo.
3. Implementación de Esquema de Seguridad en oficinas centrales - San Lorenzo.
4. Creación de segmento WAN en oficinas centrales - San Lorenzo.
5. Configuración de salida a internet de 40 Mb/s - San Lorenzo.
6. Instalación de ADSL en WAN Oficinas Centrales para contingencias. - San Lorenzo
7. Generación de políticas de acceso a la red.
8. Instalación y configuración de servidor de filtrado WEB - San Lorenzo.
9. Instalación de equipos provistos por TELMEX en cada plantel y oficinas centrales.
10. Configuración de Red de cada plantel en base al nuevo direccionamiento.
11. Instalación de Firewall-Router en cada plantel.
12. Pruebas de conectividad.
13. Instalación de servidor de monitoreo.
14. Instalación de servidor de Reportes.
15. Generación de Entorno de Producción.

1.7.1. Detalle de actividades

Actividad	Separación de Servicios en oficinas centrales - San Lorenzo
Justificación	Realizar la separación de los servicios de red del IEMS, ya que actualmente se encuentran integrados en un mismo equipo de cómputo. Lo que dificulta la administración y vulnera de manera crítica la disponibilidad de los servicios.
Descripción:	Se pretende tener servidores independientes donde residirán cada uno de los servicios de red con lo que cuenta el instituto. Tener en diferentes equipos el servidor de DHCP, DNS, Correo Institucional y WEB.
Inicio:	Fecha: 01/ 10/2010 Localidad: Oficinas San Lorenzo
Fin:	Fecha: 31/10/2010 Localidad: Oficinas San Lorenzo
Resultados:	Tener servidores administrados de forma independiente, los cuales tendrán sus propias configuraciones y esquemas de seguridad

Cuadro 1.9: Detalle de actividades. Separación de servicios en oficinas centrales - San Lorenzo.

Actividad	Segmentación de la Red de las oficinas centrales - San Lorenzo.
Justificación	Segmentación de los equipos de red de las oficinas centrales por ubicación física mediante VLANS, y así tener 3 segmentos independientes y separados uno del otro. Esto permitirá establecer los mecanismos para que el broadcast de la red no sea tan extenso y así la red tenga mejor rendimiento. Las VLANS tendrán también la finalidad de canalizar el tráfico hacia el destino de manera más eficiente; bloqueando el tráfico hacia la VLAN de administración de los equipos dándole con esto seguridad a la red.
Descripción:	Establecer seis segmentos en la red de datos del IEMS de acuerdo a la división física y de servicios que presenta la red, la primera segmentación se realizará para la planta Baja del Edificio 1 (VLAN200), la segunda segmentación para la planta Alta del Edificio 1 (VLAN300) y la tercera se creará con el Edificio 2 del Instituto (VLAN100). Una cuarta red será para la VLAN de voz y los equipos de voz sobre IP (VLAN400). Una quinta para equipos inalámbricos (VLAN600). Finalmente una sexta para la administración de la red y los equipos de comunicaciones como Switches y routers.
Inicio:	Fecha: 01/ 11/2010 Localidad: Oficinas San Lorenzo
Fin:	Fecha: 30/11/2010 Localidad: Oficinas San Lorenzo
Resultados:	Creación de VLAN 1, 100, 200, 300, 400, 600. En una configuración Router on a stick”

Cuadro 1.10: Detalle de actividades. Segmentación de la Red de las oficinas centrales - San Lorenzo.

Actividad	Implementación de Esquema de Seguridad en oficinas centrales - San Lorenzo.
Justificación	Contar con una red segura de intrusiones y ataques informáticos, mediante la filtración de peticiones indebidas. Aunado con la separación mediante VLANS; Esto se logrará instalando un firewall en FreeBSD que estará en la punta de la red que filtrará peticiones de diversos rangos de IP bien conocidos que se encuentran en diversos países. Administración de Switches y Routers en la VLAN1. El bloqueo local de pings y peticiones a la VLAN de administración (VLAN1).
Descripción:	Instalación de un firewall que servirá como un filtro que evitará los accesos no permitidos desde Internet. Así como la configuración PAT en dicho equipo para la traducción y enmascaramiento de direcciones locales. Creación de Access Control List (ACL) para bloqueo de tráfico hacia VLAN de administración.
Inicio:	Fecha: 01/12/2010 Localidad: Oficinas San Lorenzo
Fin:	Fecha: 15/12/2010 Localidad: Oficinas San Lorenzo
Resultados:	Un esquema de seguridad que permitirá que los datos dentro del IEMS se encuentren seguros en la red.

Cuadro 1.11: Detalle de actividades. Implementación de Esquema de Seguridad en oficinas centrales - San Lorenzo.

Actividad	Creación de segmento WAN en oficinas centrales - San Lorenzo.
Justificación	Creación de una red WAN dentro de las oficinas centrales, en preparación a la futura instalación de los enlaces a los planteles. En dicho segmento se definirán cinco VLANS, Una para administración VLAN1), una para tráfico de datos (VLAN1000), otra para tráfico de voz (VLAN200), otra para video (VLAN3000) y otra para contingencias (VLAN192). Esto permitirá tener aislado el tráfico y agregar además de seguridad, calidad de servicio al tráfico más importante y que requiere de menos latencia. En dicho segmento WAN se tendrán a los servidores del IEMS que serán accesibles a los planteles y a las oficinas centrales. De esta forma el tráfico no tendrá que ingresar a ninguna red local ni de las oficinas centrales ni de los planteles.
Descripción:	Implementar dos servidores en las oficinas centrales que servirán como routeadores y servidores de DHCP, dichos servidores redireccionarán el tráfico de acuerdo al tipo de tráfico que se está generando en la LAN. Los servidores se encontrarán configurados en failover para alta disponibilidad. Instalar un Switch Cisco Catalyst en la WAN que tendrá configurados los puertos en las VLANS correspondientes. Migrar los servidores a la VLAN1 en la WAN. Ajustar el Firewall montado anteriormente para el nuevo esquema; así como instalar un segundo en failover para proveer de alta disponibilidad. Configurar en dichos servidores las políticas de acceso a sitios no seguros en internet. Habilitar PAT.
Inicio:	Fecha: 15/12/2010 Localidad: Oficinas San Lorenzo
Fin:	Fecha: 15/01/2011 Localidad: Oficinas San Lorenzo
Resultados:	Se crearán 5 VLANS: - VLAN1: Tráfico de administración - VLAN1000: Tráfico de datos. - VLAN2000: Tráfico de voz - VLAN3000: Tráfico de video - VLAN192: Tráfico hacia contingencia.

Cuadro 1.12: Detalle de actividades. Creación de segmento WAN en oficinas centrales - San Lorenzo.

Actividad	Configuración de la salida a internet de 40 Mb/s - San Lorenzo.
Justificación	Es necesario que la salida a internet de 40 Mb/s contratada por TELMEX esté configurada adecuadamente para que todos las Personal Computer (PC) del IEMS puedan hacer uso de ella.
Descripción:	Configurar el Switch que está en la salida a internet con dos VLANS la VLAN 40 y la VLAN 192, la VLAN 40 hará uso del enlace de 40 Mb/s y la VLAN192 la del infínitum de 4Mb/s. Habilitar PAT en el firewallprincipal y secundario para que traduzca las IP de la red local en las públicas de los 40 Mb/s. Así como es indispensable limitar el ancho de banda para las oficinas centrales de 4 Mb/s y de cada plantel a 2 Mb/s.
Inicio:	Fecha: 01/01/2011 Localidad: Oficinas San Lorenzo
Fin:	Fecha: 15/01/2011 Localidad: Oficinas San Lorenzo
Resultados:	Lograr la salida internet tanto de las PC como de los servidores del instituto, teniendo un plan de contingencia para hacer uso del infínitum.

Cuadro 1.13: Detalle de actividades. Configuración de la salida a internet de 40 Mb/s - San Lorenzo.

Actividad	Instalación de WAN ADSL en oficinas centrales para contingencias - San Lorenzo.
Justificación	Se instalará una salida alterna a internet mediante un enlace infinitum con el que ya cuenta el Instituto de 4 Mb/s, dicho enlace será sólo usado en contingencia, si el enlace principal falla.
Descripción:	Se conectará en la VLAN192 del Switch ubicado en la WAN un equipo infínitum ADSL de 4 Mb/s para darle una salida en caso de contingencia del enlace principal de 40 Mb/s, éste enlace será sólo utilizado cuando sean requerido.
Inicio:	Fecha: 01/01/2011 Localidad: Oficinas San Lorenzo
Fin:	Fecha: 15/01/2011 Localidad: Oficinas San Lorenzo
Resultados:	Se tendrá una alternativa de internet limitado en ancho de banda para cualquier eventualidad o proceso crítico que se presente en el enlace principal.

Cuadro 1.14: Detalle de actividades. Instalación de WAN ADSL en oficinas centrales para contingencias - San Lorenzo.

Actividad	Generación de políticas de acceso a la red.
Justificación	Toda máquina que desee hacer uso de la red deberá de cumplir con las normas que se definan en el documento de políticas.
Descripción:	Se redactará un documento el cual contenga las políticas que deberán cumplir las máquinas que deseen hacer uso de la red institucional. Lo que el usuario podrá y no realizar.
Inicio:	Fecha: 01/01/2011 Localidad: Oficinas San Lorenzo
Fin:	Fecha: 31/05/2011 Localidad: Oficinas San Lorenzo
Resultados:	Un documento que defina las políticas de uso de la red el cual contenga de manera clara lo que un usuario puede realizar al hacer uso de la red, así como de las penalizaciones, si existiesen, del mal uso que se pueda dar.

Cuadro 1.15: Detalle de actividades. Generación de políticas de acceso a la red.

Actividad	Instalación y configuración de servidor de filtrado WEB - San Lorenzo.
Justificación	Es necesario que las máquinas del IEMS pasen a través de un filtrado de sitios WEB, ya que el uso indebido de la red puede traer problemas no sólo de seguridad sino también de ancho de banda.
Descripción:	El servidor estará instalado con Debian[14] y DansGuardian, el DansGuardian se instala junto con Squid[15] en la misma máquina y escucha las peticiones por algún puerto definido por el administrador de la red. Una vez que una petición llega al servidor éste lo compara con las políticas definidas en él y decide si el sitio es bloqueado o no. Se definirán 4 perfiles de filtrado cada uno con diferentes niveles de bloqueo. Estos perfiles permitirán una mejor flexibilidad. Una máquina se identificará con su dirección IP.
Inicio:	Fecha: 15/01/2011 Localidad: Oficinas San Lorenzo
Fin:	Fecha: 15/02/2011 Localidad: Oficinas San Lorenzo
Resultados:	Se logrará un mejor uso del ancho de banda con el que cuenta el Instituto, así como permitirá llevar un registro de las páginas que se visitan en el IEMS para fines estadísticos.

Cuadro 1.16: Detalle de actividades. Instalación y configuración de servidor de filtrado WEB - San Lorenzo.

Actividad	Instalación de equipos provistos por TELMEX en cada plantel y oficinas centrales.
Justificación	En las oficinas centrales dichos equipos serán los que proveerán de salida a internet, así como de la conectividad hacia cada plantel. En cada plantel se instalará uno y servirá de enlace hacia las oficinas centrales de san Lorenzo.
Descripción:	TELMEX se encargará de instalar la infraestructura necesaria tanto en las oficinas centrales como en cada plantel, dicha infraestructura será supervisada por el área de telecomunicaciones del Instituto y por los JUDs de cada plantel.
Inicio:	Fecha: 01/01/2011 Localidad: Oficinas San Lorenzo
Fin:	Fecha: 31/05/2011 Localidad: Oficinas San Lorenzo
Resultados:	Se tendrán instalados los equipos de TELMEX en las oficinas centrales y en cada plantel del IEMS.

Cuadro 1.17: Detalle de actividades. Instalación de equipos provistos por TELMEX en cada plantel y oficinas centrales.

Actividad	Configuración de Red de cada plantel en base al nuevo direccionamiento.
Justificación	Se otorgará a cada plantel de un bloque de direcciones IP que serán aquellas con las que deberán configurar su red local.
Descripción:	Los jefes de unidad departamental de cada plantel serán los encargados de configurar los equipos de la red local con el bloque de direcciones otorgado por el área de telecomunicaciones. Así como serán responsables de direccionar los servicios locales para que las máquinas de los planteles tengan acceso a los recursos compartidos, y servicios que se ofrezcan en cada plantel.
Inicio:	Fecha: 01/01/2011 Localidad: Oficinas San Lorenzo
Fin:	Fecha: 31/05/2011 Localidad: Oficinas San Lorenzo
Resultados:	Cada plantel tendrá un bloque único de direcciones con el que saldrán a la WAN y poder ubicar de mejor manera de dónde proviene el tráfico.

Cuadro 1.18: Detalle de actividades. Configuración de Red de cada plantel en base al nuevo direccionamiento.

Actividad	Instalación de Firewall-Router en cada plantel.
Justificación	Dicho servidor estará instalado en la punta de cada red local de cada plantel. Éste servidor estará en FreeBSD y redireccionará el tráfico de acuerdo a su característica o prioridad. También será un servidor de DHCP para la mejor administración de IPs. El servidor bloqueará el tráfico indeseado desde la WAN hacia dentro del plantel.
Descripción:	Implementar un servidor en cada plantel que servirá como routeador y servidor de DHCP, dicho servidor dotará a cada usuario del plantel una IP correspondiente a su perfil el cual define las páginas que puede o no visitar el usuario. Aquellos usuarios que no estén registrados en el firewall o que se hayan puesto la IP de manera manual en la se les presentará un portal cautivo indicándoles las políticas del uso de la red y la necesidad de contactarse con el área de sistemas del plantel. El servidor tendrá dos niveles de administración, para acceso remoto del área de telecomunicaciones de las oficinas centrales y para los jefes de unidad departamental de cada plantel.
Inicio:	Fecha: 01/04/2011 Localidad: Oficinas San Lorenzo y cada plantel
Fin:	Fecha: 31/05/2011 Localidad: Oficinas San Lorenzo y cada plantel
Resultados:	Se conectará un servidor en cada plantel que estará dando servicio de DHCP a los usuarios de cada plantel, así como se encargará de routear el tráfico hacia la VLAN correspondiente en la WAN.

Cuadro 1.19: Detalle de actividades. Instalación de Firewall-Router en cada plantel.

Actividad	Pruebas de conectividad.
Justificación	Son las realizadas una vez instalados los servidores en cada plantel y los equipos provistos por TELMEX.
Descripción:	Observar el ancho de banda otorgado por los enlaces mediante el uso de IPERF[16], desde las oficinas centrales hacia cada plantel. Generar peticiones a servidores en las oficinas centrales. Generar tráfico WEB.
Inicio:	Fecha: 01/04/2011 Localidad: Oficinas San Lorenzo y cada plantel
Fin:	Fecha: 31/05/2011 Localidad: Oficinas San Lorenzo y cada plantel
Resultados:	Se requerirá de ayuda de cada jefe de unidad departamental para realizar dichas pruebas que permitirán la generación de una tabla de ancho de banda que será comparada a la que actualmente se tiene. Se ajustará cualquier imprevisto causado por la transición al nuevo esquema de red.

Cuadro 1.20: Detalle de actividades. Pruebas de conectividad.

Actividad	Instalación de servidor de monitoreo.
Justificación	Es importante tener en una red un servidor de monitoreo que permita generar una respuesta más oportuna a cualquier incidente que se genere en la red institucional. Se requiere de un servidor que sea capaz de monitorear a todos los equipos de comunicaciones y servidores de manera centralizada y que sea un punto de partida para cualquier diagnóstico de un probable incidente. Debe éste ser quien genere una alarma en el momento en que un servicio se detenga.
Descripción:	Implementar un servidor de monitoreo con SolarWinds[17] en la red WAN que sea accesible a los equipos de las oficinas centrales y planteles.
Inicio:	Fecha: 01/06/2011 Localidad: Oficinas San Lorenzo y cada plantel
Fin:	Fecha: 30/06/2011 Localidad: Oficinas San Lorenzo y cada plantel
Resultados:	Instalar un servidor en SolarWinds con diversos niveles de administración, accesible a los responsables de la administración de la red.

Cuadro 1.21: Detalle de actividades. Instalación de servidor de monitoreo.

Actividad	Instalación de servidor de Reportes.
Justificación	Requerido para dar atención y seguimiento a reportes de incidentes en la red. Dichos reportes serán generados por los usuarios de la red y atendidos por los administradores. Un servidor de reportes es necesario para poder medir el tiempo que tarda en resolverse un incidente desde que se genera hasta que se resuelve. Es un mecanismo para calcular la productividad de los administradores de red.
Descripción:	Implementar un servidor de reportes en la WAN que será programado por el área de sistemas del IEMS y accesible para usuarios y administradores de red.
Inicio:	Fecha: 01/06/2011 Localidad: Oficinas San Lorenzo y cada plantel
Fin:	Fecha: 30/06/2011 Localidad: Oficinas San Lorenzo y cada plantel
Resultados:	Contar con un servidor donde se pueda generar reportes a incidentes y solicitudes de la red de datos. Una manera fehaciente de medir la productividad y el tiempo de respuesta.

Cuadro 1.22: Detalle de actividades. Instalación de servidor de Reportes.

Actividad	Generación de Entorno de Producción.
Justificación	Entrega formal de la red con la documentación generada durante el proyecto.
Descripción:	Otorgar la documentación generada durante el proyecto a la Dirección de Informática y Telecomunicaciones del IEMS. Generación de políticas de manera formal para definir aquellas máquinas que tienen acceso a ciertos recursos de red y privilegios. Definición de responsabilidades del área de sistemas, telecomunicaciones y jefes de unidad departamental. Generación de manuales simples para procedimientos comunes.
Inicio:	Fecha: 01/07/2011 Localidad: Oficinas San Lorenzo y cada plantel
Fin:	Fecha: 31/07/2011 Localidad: Oficinas San Lorenzo y cada plantel
Resultados:	Otorgar todos los medios que permitirán a la red operar de manera correcta.

Cuadro 1.23: Detalle de actividades. Generación de Entorno de Producción.

1.8. Premisas ajustadas a la situación real

- Asegurar el funcionamiento de los diferentes servidores donde se instalaron los servicios del IEMS, en base al nuevo direccionamiento.
- Redistribución de equipos de telecomunicaciones en los diferentes Intermediate Distribution Frame (IDF) para la implementación del nuevo esquema en San Lorenzo.
- Llevar a cabo las tareas de afectación del servicio en ventanas de mantenimiento. Teniendo en cuenta los procesos críticos del Instituto como inscripciones, evaluaciones, pagos de nómina y respaldos de bases de datos.
- Generar manuales y talleres de aprendizaje de administración de la nueva red a los jefes de unidad departamental de cada área.

1.9. Responsabilidades

Telecomunicaciones

- Llevar a cabo la administración, planeación, ejecución, seguimiento y finalización de la implementación de la Red Institucional del IEMS.
- Documentar todos los cambios realizados.
- Generar manuales para uso de los administradores.
- Presentar una propuesta de las políticas de uso de la red, como privilegios de acceso a servidores y páginas de Internet.
- Dar soporte de segundo nivel a los usuarios de los planteles y de primer nivel a los de las oficinas centrales.
- Realizar respaldos continuos de configuración de los servidores y equipos de comunicaciones que formen parte de la red. Firewalls, Routers, Switches, Access Points.

Jefes de Unidad Departamental (JUDs)

- Preparar la red para la migración.
- Cambiar las direcciones IP de los equipos de la red en base al direccionamiento otorgado por telecomunicaciones.
- Mantener la seguridad basada en otorgar privilegio sólo a aquellas máquinas que son propietarias del IEMS.
- Dar soporte de primer nivel a los usuarios de su propio plantel que requieran ayuda con un servicio de red.

1.10. Riesgos

- Afectación de los servicios de red en las migraciones al nuevo esquema de plataforma de red
- Modificación a la topología planeada por falta de equipos de telecomunicaciones o servidores.
- Retraso en tiempos y fechas por eventualidades y procesos críticos del IEMS que requieran asignación de fechas específicas (inscripciones, huelgas, eventos).
- Retraso en tiempos y fechas generados por la instalación de los servicios del proveedor de servicios (TELMEX).
- Generación de descontento debido al nuevo esquema de filtrado WEB, así como ajuste del servidor debido a falsos positivos.

1.11. Direccionamiento

1.11.1. Bloque de direcciones IP para las redes LAN en Oficinas centrales y planteles

No de Plantel	Plantel	Dirección de Red	Prefijo
1	Oficinas Centrales	10.0.0.0	16
2	A. Obregón	10.1.0.0	16
3	Azcapotzalco	10.2.0.0	16
4	Coyoacán	10.3.0.0	16
5	Cuajimalpa	10.4.0.0	16
6	Gustavo A Madero I	10.5.0.0	16
7	Gustavo A Madero II	10.6.0.0	16
8	Iztacalco	10.7.0.0	16
9	Iztapalapa I	10.8.0.0	16
10	Iztapalapa II	10.9.0.0	16
11	Iztapalapa III	10.10.0.0	16
12	M. Contreras	10.11.0.0	16
13	M. Hidalgo	10.13.0.0	16
14	Milpa Alta	10.14.0.0	16
15	Tláhuac	10.15.0.0	16
16	Tlalpan I	10.16.0.0	16
17	Tlalpan II	10.17.0.0	16
18	V. Carranza	10.18.0.0	16
19	Xochimilco	10.19.0.0	16

Cuadro 1.24: Bloque de direcciones IP para las LAN en oficinas centrales y planteles.

1.11.2. Direccionamiento para la red LAN de las Oficinas Centrales

No de VLAN	Nombre	Tipo	Dirección	Prefijo
1	VLAN1	Administración	10.0.0.0	24
100	VLAN100	Edificio de TI	10.0.1.0	24
200	VLAN200	Edificio planta baja	10.0.2.0	24
300	VLAN300	Edificio planta alta	10.0.3.0	24
400	VLAN400	Voz	10.0.4.0	24
600	VLAN600	Inalámbricos	10.0.6.0	24

Cuadro 1.25: Direccionamiento para la LAN de las oficinas centrales.

1.11.3. Direccionamiento para la red WAN

No de VLAN	Nombre	Tipo	Dirección	Prefijo
1	VLAN1	Administración	10.12.0.0	24
1000	VLAN1000	Datos	10.12.1.0	24
2000	VLAN2000	Voz	10.12.2.0	24
3000	VLAN3000	Video	10.12.3.0	24
192	VLAN192	Contingencia	192.168.20.0	24

Cuadro 1.26: Direccionamiento para la red WAN parte 1

No. de plantel	Plantel	Equipo	Dirección VLAN 1	Dirección VLAN 1000	Dirección VLAN 2000	Dirección VLAN 3000
0	Oficinas centrales	TokioPrincipal	10.12.0.98	10.12.1.98	10.12.2.98	10.12.3.98
1	Oficinas centrales	TokioSecundario	10.12.0.99	10.12.1.99	10.12.2.99	10.12.3.99
2	Oficinas centrales	TokioVirtual	10.12.0.100	10.12.1.100	10.12.2.100	10.12.3.100
3	Oficinas centrales	HUB	10.12.0.180	10.12.1.180	10.12.2.180	10.12.3.180
4	A. Obregón	Firewall-Router	10.30.1.2	N/A	N/A	N/A
5	Azcapotzalco	Firewall-Router	10.30.2.2	N/A	N/A	N/A
6	Coyoacán	Firewall-Router	10.30.3.2	N/A	N/A	N/A
7	Cuajimalpa	Firewall-Router	10.30.4.2	N/A	N/A	N/A
8	Gustavo A Madero I	Firewall-Router	10.30.5.2	N/A	N/A	N/A
9	Gustavo A Madero II	Firewall-Router	10.30.6.2	N/A	N/A	N/A
10	Iztacalco	Firewall-Router	10.30.7.2	N/A	N/A	N/A
11	Iztapalapa I	Firewall-Router	10.30.8.2	N/A	N/A	N/A
12	Iztapalapa II	Firewall-Router	10.30.9.2	N/A	N/A	N/A
13	Iztapalapa III	Firewall-Router	10.30.10.2	N/A	N/A	N/A
14	M. Contreras	Firewall-Router	10.30.11.2	N/A	N/A	N/A
15	M. Hidalgo	Firewall-Router	10.30.13.2	N/A	N/A	N/A
16	Milpa Alta	Firewall-Router	10.30.14.2	N/A	N/A	N/A
17	Tláhuac	Firewall-Router	10.30.15.2	N/A	N/A	N/A
18	Tlalpan I	Firewall-Router	10.30.16.2	N/A	N/A	N/A
19	Tlalpan II	Firewall-Router	10.30.17.2	N/A	N/A	N/A
20	V. Carranza	Firewall-Router	10.30.18.2	N/A	N/A	N/A
21	Xochimilco	Firewall-Router	10.30.19.2	N/A	N/A	N/A

Cuadro 1.27: Direccionamiento para la red WAN parte 2

Nota: La VLAN192 sólo reside en las oficinas centrales y será utilizada mediante routeo en los equipos FirewallPricipal y FirewallSecundario.

1.12. Recomendaciones

El proyecto está diseñado para ser ejecutado por diversas áreas del IEMS así como por parte de la empresa TELMEX, por lo tanto es indispensable la documentación de cualquier cambio realizado en el diseño del mismo, dicha documentación servirá entonces para llevar un mejor control.

Es indispensable también llevar a cabo buenas prácticas como mantener los sitios de trabajo limpios y ordenados, con el cableado identificado por color si es posible, con nodos etiquetados, Switches nombrados con una etiqueta y su correspondiente IP de administración; finalmente es importante tener instalado y funcionando un aire acondicionado.

El diseño del proyecto está pensado para funcionar al 100 % con equipo de la marca Cisco, por lo que se deberán de adquirir nuevos equipos conforme se requieran de dicha marca.

El cambio de contraseñas deberá ser periódico para así mantener los equipos seguros.

La asignación de los bloques de IP se llevará a cabo por el área de Telecomunicaciones del Área Central, por lo que cualquier requerimiento de implementación en los planteles deberá ser autorizado por el área central.

1.13. Conclusión

Se establece mediante éste documento los pasos a seguir para implementar la red Institucional del IEMS, así como las responsabilidades de cada área involucrada en dicho proyecto.

El esquema de red presentado se basa en las condiciones actuales y las necesidades del Instituto; así como de las posibilidades de adquisición de nuevos servidores y equipos de comunicaciones.

Se presenta también, el direccionamiento de red que tendrán los equipos y podrá ser modificado sólo si las condiciones ofrecidas por la empresa TELMEX cambian, como la tecnología utilizada para los enlaces.