ESCUELA POLITECNICA DEL EJÉRCITO

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

"ANÁLISIS Y DISEÑO DE LA RED INALÁMBRICA DE ALTA VELOCIDAD BASADA EN EL ESTÁNDAR WiMAX (IEEE 802.16) PARA LA ESCUELA POLITÉCNICA DEL EJÉRCITO."

Previa a la obtención del Título de:

INGENIERO EN SISTEMAS E INFORMÁTICA

POR: **CÉSAR FRANCISCO CHÁVEZ CEVALLOS**
MIGUEL RAÚL RICLE VARGAS

SANGOLQUI, 30 de Enero de 2006

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por los señores CESAR FRANCISCO CHAVEZ CEVALLOS y MIGUEL RAUL RICLE VARGAS como requerimiento parcial a la obtención del título de INGENIEROS EN SISTEMAS E INFORMATICA

_____
30 de enero de 2006

_____
ING. LOURDES DE LA CRUZ.
DIRECTORA DE TESIS

DEDICATORIA

Dedicada al crecimiento sociocultural de nuestro país basado en el avance tecnológico y la exploración de nuevas fronteras, por un Ecuador competitivo.

CÉSAR FRANCISCO CHÁVEZ CEVALLOS
MIGUEL RAÚL RICLE VARGAS

AGRADECIMIENTOS

Agradecemos a nuestros padres, aquellos que han luchado hombro a hombro como un estudiante más; a nuestra directora de tesis Ingeniera Lourdes de la Cruz, que aparte de sus conocimientos nos entregó su valiosa amistad; a nuestro codirector Ingeniero Fausto Granda por el aliento e incentivo que siempre estuvo presente y a la hermosa ESPE, jamás te olvidaremos.

CÉSAR FRANCISCO CHÁVEZ CEVALLOS
MIGUEL RAÚL RICLE VARGAS

INDICE DE CONTENIDOS

LISTADO DE TABLAS

LISTADO DE CUADROS

LISTADO DE FIGURAS

LISTADO DE ANEXOS

RESUMEN

La nueva tecnología WiMAX (802.16x) está revolucionando las comunicaciones en la actualidad, incrementando distancias y ancho de banda, por lo tanto, la ESPE como una institución de vanguardia debe adoptar esta tecnología como una de sus inversiones para la comunicación entre sedes.

Servicios de punta como voz sobre IP y videoconferencias pueden ser implementados mediante la adopción de esta red en la infraestructura de la ESPE, destacándose de otras universidades y colocándose en un estado de vanguardia en lo que a tecnología se refiere.

Además, costos como el telefónico y el de arrendar un enlace xDSL se verían minimizados ya que esta red propia de la ESPE reemplazaría lo antes mencionado.

Los equipos en la actualidad son escasos y medianamente costosos por el hecho de estar en desarrollo, aunque existen algunas empresas sólidas que han investigado a profundidad y poseen productos robustos para la implementación de esta tecnología.

Una parte importante de esta red es las seguridades y las contingencias que se deben adoptar para que la misma sea lo más eficiente y eficaz en caso de producirse algún tipo de falla, lo cual, se toma muy en cuenta en el presente proyecto.

CAPITULO I: INTRODUCCION

El mundo de las comunicaciones está cambiando día a día en forma acelerada, la necesidad de las organizaciones de mantenerse comunicadas y al día con su información ha hecho que el avance de las telecomunicaciones se desarrolle y crezca de manera rápida en los últimos años.

En la década pasada, la investigación sobre tecnologías de conectividad tuvo un crecimiento importante, especialmente en redes de área local con sistemas de cableado estructurado y el auge de la conectividad inalámbrica con la telefonía celular. Esto ha llevado a las empresas a verse en la imperiosa necesidad de introducir en sus políticas de trabajo la tecnología para mantener su información al día.

La tecnología nos brinda soluciones acordes a las necesidades y presupuestos, pero se debe hacer un análisis en el momento de tomar las decisiones y el mejor camino a seguir, con esto se presentan distintas maneras para formar parte del mundo globalizado de las redes como el Internet, pero simplemente se puede definirlas en dos grandes grupos: soluciones alámbricas e inalámbricas. Cada una con sus ventajas y desventajas, pero a la final brindan conectividad. El costo y los anchos de banda que provee la tecnología alámbrica son los factores de decisión para adoptar o no la misma, pero dentro de estos también aparece la factibilidad física o geográfica y es allí donde aparecen las soluciones inalámbricas de distintos tipos.

La aparición de la telefonía celular revolucionó la mentalidad de la sociedad con respecto a la comunicación, en función del tiempo y lugar donde se encuentre, ahora las personas tienen la conciencia que, donde quiera que se

encuentre, tiene la capacidad de comunicarse con el resto del mundo; este fenómeno se lo denomina “movilidad”. Se denomina movilidad a la capacidad de comunicarse y adquirir información en distintos lugares con el mismo dispositivo. De igual forma que la revolución de las comunicaciones telefónicas tuvo su auge con la telefonía móvil, dentro de las redes de comunicación empresariales, el paso entre las conexiones alámbricas e inalámbricas es muy notorio.

Las comunicaciones inalámbricas cubren las necesidades de comunicación de las empresas o personas especialmente que tienen el problema de acceso físico a las redes ya sean estas al Internet o enlazar redes corporativas local o remotamente. Se podría llegar a pensar en un mundo sin cables pero con los mismos servicios, interesante verdad. Si se transforma el concepto a nivel de procesos es la comparación entre el manejo de documentos en papeles y un sistema de workflow (sistema cero papeles), la misma relación se tiene entre conectividad alámbrica e inalámbrica.

Al desarrollarse las tecnologías inalámbricas y generarse una gran demanda de la adopción de estas, es necesario la creación de estándares que regularicen estos sistemas. Las tecnologías más utilizadas que están estandarizadas por la IEEE son: Bluetooth, WiFi, WiMAX, etc. Cada uno con sus ventajas y debilidades, tratan de cubrir las necesidades tecnológicas de los usuarios.

Tecnologías como WiFi (IEEE 802.11x) son utilizadas últimamente para cubrir las necesidades de redes locales corporativas, basándose en conexiones

seguras con encriptaciones WEP[1] y WPA[2] y soportando los mismos protocolos que FastEthernet, han ido creciendo en el mercado por la baja de sus costos y mejoras en sus servicios, pero aún así no cubre con la completa satisfacción y utilidad para los usuarios, para esto aparecen nuevos avances como la tecnología, WiMAX (802.16x).

La aparición del estándar WiMAX (802.16x), genera una solución para cubrir la necesidad de tecnologías inalámbricas de alta velocidad con buen ancho de banda y largas distancias. En lugares de difícil acceso la solución óptima es la implementación de tecnologías inalámbricas y con el aparecimiento de WiMAX como tecnología que soporta las exigencias de grandes empresas que quieren mantenerse conectadas a la red mundial, el Internet. A su vez estos establecimientos generan necesidades de conectividad internas para enlazar sus dependencias y crecer en su conectividad.

1.1- Justificación

El análisis y diseño de una red inalámbrica para la Escuela Politécnica del Ejército basada en tecnología WiMAX, es la solución más productiva para mejorar el crecimiento tecnológico e intelectual para el establecimiento.

Entre los beneficios principales se tienen los siguientes:

- Escalabilidad de usuarios y de infraestructura de red.
- Disminución del tiempo en la instalación en relación con el cableado estructurado.

[1] Véase en el glosario de términos

[2] Véase en el glosario de términos

- Cobertura total del campus politécnico.
- Tecnología inalámbrica móvil dentro del área de la ESPE.
- Seguridades basadas en encriptación WEP, DES, AES, MAC address.
- Conexión de 124 Mbps y hasta 70 Km. de alcance.
- Gran ancho de banda: una sola estación de base puede admitir de manera simultánea más de 60 empresas con conectividad tipo T1/E1.
- Es independiente de protocolo: puede transportar IP, Ethernet, ATM y más.
- Es compatible con las antenas de telefonía de tercera generación.
- Reutilización de equipos.
- Permite la movilidad corporativa, en casos que las dependencias cambien de ambiente físico.

1.2- Objetivos

1.2.1- Objetivo general

Analizar, diseñar, implementar seguridad y plantear un plan de contingencia de una red inalámbrica de alta velocidad basada en tecnología WiMAX para la Escuela Politécnica del Ejército, optimizando así del ingreso de los usuarios dentro del campus politécnico al Internet, para el crecimiento de la investigación y el desarrollo intelectual de las personas que integran la Institución.

1.2.2- Objetivos específicos

- Analizar la tecnología WiMAX.

- Analizar el sistema actual de la red de la ESPE y proponer el funcionamiento óptimo del mismo basado en requerimientos recopilados.
- Diseñar la red inalámbrica WiMAX tomando en cuenta el aspecto técnico y económico.
- Realizar un plan de implementación.
- Elaborar un plan de seguridades para la red.
- Administrar y gestionar la red.
- Presentar un plan de contingencia para que en caso de que los enlaces principales fallen, la red tenga una alternativa para seguir con el funcionamiento.

CAPITULO II: MARCO TEORICO

2.1- Tecnología inalámbrica de banda ancha

El avance de la tecnología y las necesidades de los usuarios y empresas desarrolladoras, han llevado a un gran salto en el avance de la intercomunicación. La utilización de medios inalámbricos para estar interconectados es ahora la solución óptima para los requerimientos a todo nivel.

Por este crecimiento se presentan tecnologías que satisfacen distintas necesidades en el mercado, estas tecnologías son: 3G, WiFi, WiMAX y UWB. La coexistencia entre estas tecnologías es la predicción de los desarrolladores y esperar que una de ellas sea la principal y maneje el mercado no es seguro.

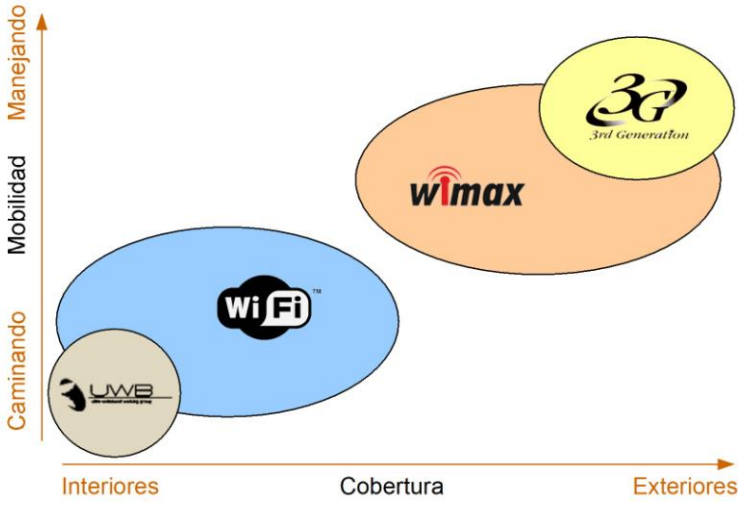


Figura 2.1: Cobertura vs movilidad de estandares inalámbricos[1]

En el siguiente cuadro se muestra las distintas tecnologías inalámbricas existentes en el mercado:

[1] INTEL CORPORATION, Tecnología Inalámbrica de Banda Ancha, http://www.intel.com/cd/network/communications/emea/spa/179913.htm, 2005

Cuadro II.1: Tecnologías inalámbricas[1]

Nombre	Estándar	Uso	Capacidad de proceso	Frecuencia
UWB	802.15.3ª	WPAN	De 110 a 480 Mbps	7,5 GHz
Bluetooth	802.15.1	WPAN	Hasta 720 Kbps	2,4 GHz
WiFi	802.11ª	WLAN	Hasta 54 Mbps	5 GHz
WiFi	802.11b	WLAN	Hasta 11 Mbps	2,4 GHz
WiFi	802.11g	WLAN	Hasta 54 Mbps	2,4 GHz
WiMAX	802.16d	WMAN fija	Hasta 75 Mbps (20 MHz AB)	Sub 11 GHz
WiMAX	802.16e	WMAN portátil	Hasta 30 Mbps (10 MHz)	De 2 a 6 GHz
Edge	2.5G	WWAN	Hasta 384 Kbps	1900 MHz
CDMA2000/1x EV-DO	3G	WWAN	Hasta 2,4 Mbps (aprox. de 300 a 600 Kbps)	400, 800, 900, 1700, 1800, 1900, 2100 MHz
WCDMA/UMTS	3G	WWAN	Hasta 2 Mbps (hasta 10 Mbps con tecnología HSDPA)	1800, 1900, 2100 MHz

Siendo estas las tecnologías que permiten la interconexión con medios inalámbricos, Se debe considerar que banda ancha es aquella tecnología que permite la conexión a Internet de alta velocidad. En nuestro medio erróneamente

[1] INTEL CORPORATION, Tecnología Inalámbrica de Banda Ancha, http://www.intel.com/cd/network/communications/emea/spa/179913.htm, 2005

se considera conexión de alta velocidad a partir de los 64kb de conexión por cualquier medio, puede ser: cable módem, enlaces DSL, enlaces inalámbricos. WiMAX, al ofrecer velocidades de hasta 124Mbps, verdaderamente ofrece una conexión de banda ancha.

2.2- Modulación OFDM

La modulación OFDM consiste en enviar un flujo de información en varías señales portadoras aumentando la cantidad de información enviada en un tiempo determinado. Por ello el tiempo “Tu” de envío de señal aumenta con respecto a la modulación de una sola señal portadora. El retardo de modulación entre cada una de las portadoras hace que la interferencia o eco que exista entre ellas sea mucho menor, por ello, la señal se la considera de alta calidad.

Cada una de las señales portadoras son enviadas en fases distintas generando distintos tonos[1] de señal, los puntos muertos de cada tono coinciden con los puntos muertos de otros tonos (otras señales portadoras desfasadas entre sí), lo que hace cumplir la condición de ortogonalidad. En la figura 2.2 se muestra este concepto gráficamente.

[1] Señal sub-portadora desfasada que va por un mismo símbolo dentro del canal de envío.

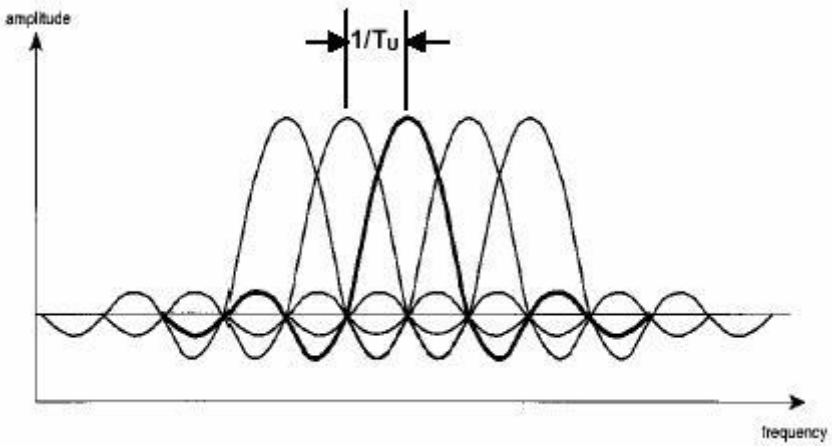


Figura II.2: Espectro de portadoras adyacentes en modulación OFDM[1]

Para que la señal se fortalezca con respecto a los ecos o interferencias entre portadoras a cada uno de los tonos se les agrega un tiempo Δ denominado "intervalo de espera" a la duración de envío "Tu", de tal manera que la duración total del tono "Ts" es:

$$Ts = \Delta + Tu$$

Si una señal llega por dos caminos distintos con un retardo menor al intervalo de espera, la información recibida será la misma si no excede del tiempo útil de envío del tono.

El receptor ignora qué señal le esta llegando en el momento del intervalo de espera, por lo tanto se descarta la interferencia entre tonos, esta ventaja genera una pérdida de capacidad de transmisión del canal en ese momento.

El tiempo Δ se mide en fracciones del tiempo útil de envío de cada tono generando 4 posibles valores:

$$\Delta / Tu = 1/4, 1/8, 1/16, 1/32$$

[1] UNIVERSIDAD POLITECNICA DE MADRID, Alejandro Delgado Gutiérrez, Transmisión de Señales de de TV Digital en el estándar terreno DVB-T, 2002

A continuación se muestra una tabla con los tiempos de transmisión en modulación OFDM para canales de 8MHz.

Tabla II.1: Valores numéricos en modulación OFDM para 8K y 2K en canales de 8 MHz donde K es el número de portadoras[1]

PARAMETRO	8k mode	2k mode
Número de portadoras K	6817	1705
Valor mínimo de portadoras	0	0
Valor máximo de portadoras	6816	1704
Duración de envío Tu	896 µs	224 µs
Tiempo de espera 1/Tu	1116 Hz	4464 Hz
Espacio entre Portadoras K y K-1	7,61 MHz	7,61 MHz

Tras la explicación teórica anterior, para un mejor entendimiento del funcionamiento de OFDM se presenta el siguiente gráfico.

[1] UNIVERSIDAD POLITECNICA DE MADRID, Alejandro Delgado Gutiérrez, Transmisión de Señales de de TV Digital en el estándar terreno DVB-T, 2002

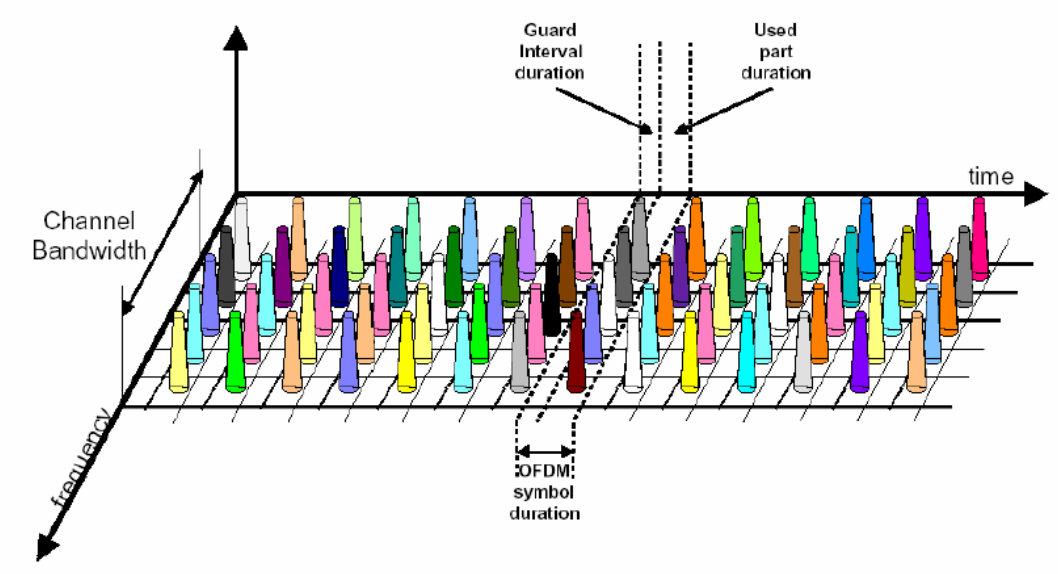


Figura II.3: Distribución de las portadoras con intervalos de espera[1]

En la figura 2.3 se puede visualizar lo siguiente: cada uno de los conos representan diferentes señales portadora K, en un mismo espacio de tiempo se envían distintas señales portadoras, a este se lo llama **Symbol Channel**. El Symbol Channel está compuesto por el tiempo de uso del canal por parte de la señal portadora Kn y el intervalo de espera de envió de Kn+1. Como se puede ver, el único momento donde el canal es subutilizado es en el tiempo muerto entre señales K.

2.2.1- Capacidad de transmisión del canal

No todas las portadoras están moduladas por el envío de datos del canal, se debe tomar en cuenta que según el modo de envió se tiene una capacidad

[1] UNIVERSIDAD POLITECNICA DE MADRID, Alejandro Delgado Gutiérrez, Transmisión de Señales de de TV Digital en el estándar terreno DVB-T, 2002

distinta, por ejemplo, para el modo de 2K se tiene 1512 y para 6K 6048 portadoras útiles para datos.

Según el número de portadoras para transportar datos se puede calcular el Flujo total de datos “Ft”:

$$Ft = fs * v * L$$

Donde:

fs = frecuencia de los símbolos (símbolo/segundo); fs = 1/Ts

Ts = Duración del símbolo

v = número de bits/portadora

L = número de portadoras activas para datos.

La capacidad del canal llamado Flujo Binario Útil, se obtiene de descontar al flujo binario total Ft la redundancia que se genera en la codificación interna y la codificación Reed-Solomon[1] (códigos de corrección de errores), con esto se tiene que:

$$Fu = Ft * r * 188/204 \text{ (bits/seg)}$$

Donde r es la relación de codificación interna.

Ejemplo:

En el caso de transmisión 8K, relación de codificación 2/3, intervalo de espera 1/4 y constelación 64QAM, para canales de 8MHz, se tendrá:

- Duración del Símbolo Ts = Δ + Tu = 1,120 µs

[1] Anónimo, Introducción Al Código De Corrección De Errores, http://personales.mundivia.es/jtoledo/angel/error/error1.htm, 2004

- Frecuencia de los símbolos fs = 1 / Ts = 892,857 símbolos/segundo
- Número de bits/portadora v = 6
- Número de portadoras activas L = 6048
- Flujo Binario total: Ft=32,4 Mbps
- Relación de codificación r = 2/3
- Capacidad del Canal: Fu = 32,4 * 2/3 * 188/204 = 19,90588 Mbps

2.2.2- Tipo de señales portadoras en OFDM

Como se mencionó anteriormente, el número de portadoras que tienen la capacidad de enviar datos no es el total de portadoras enviadas por el canal. Existen otras clases de subportadoras que utiliza el sistema de modulación para enviar y verificar cierta información que permite verificar el envío de información.

2.2.2.1- Portadoras piloto y estructuración en tramas de la señal OFDM

En OFDM los símbolos están compuestos por un número K de elementos o “celdas”, cada uno de ellos corresponden a una portadora. En la señal transmitida existen otras portadoras o “celdas”. A continuación se muestra las subportadoras y su utilidad:

Piloto Continuas “Continual Pilots”, para sincronización del receptor en frecuencia y fase.

Piloto Dispersas “Scattered Pilots”, para regeneración del canal en amplitud y fase del receptor

TPS “Transmission Parameter Signalling” esta portadora envía la información del modo de transmisión utilizado.

Para enviar estas portadoras de una manera adecuada tanto en número como en su distribución, exige transmitir la señal en “Tramas”.

Cada trama, tiene una duración “Tf”, que son 68 símbolos OFDM, que son del 0 al 67. De tal forma que Tf = 68 Ts.

Una “Súper-Trama” está formada por 4 tramas en cualquier modo de transmisión, pero, una “Mega-Trama” esta formada por 32 tramas en el modo 2K y 8 en el 8K.

2.3- Análisis del estándar IEEE 802.16x

El estándar IEEE 802.16 aparece en octubre del 2001 y es publicado el 8 de abril del 2002, orientado para la satisfacción de redes de área metropolitana (MAN’s). El objetivo de este estándar es el complacer a las empresas y usuarios de hogares la necesidad de obtener acceso al Internet por medio de una red inalámbrica pero con banda ancha y a largas distancias o en lugares de difícil acceso, ofreciendo una alternativa en relación a conexiones con T1, DSL, etc., ya que la tecnología inalámbrica brinda la capacidad de llegar a lugares geográficamente de difícil acceso. Las empresas pueden optar ahora con la comodidad de utilizar este estándar para la conexión de redes MAN y dentro de su establecimiento u hogar otros estándares como el IEEE 802.3 para el cableado y 802.11 para redes inalámbricas, ambos locales.

Cuadro II.2: Evolución del estándar IEEE 802.16

ESTANDAR	FECHA APROBACION IEEE	DESCRIPCION
802.16-2001	Abril 2002	Primer estándar relacionado con las redes inalámbricas de área metropolitana
802.16c-2002	Enero 2003	Se añaden detalles para uso de las bandas 10-66 GHz
802.16a-2003	Abril 2003	Se añaden detalles para uso de las bandas 2-11 GHz y modificaciones al funcionamiento de la capa MAC
802.16d-2004	Junio 2004	Recopilación de anteriores estándares e implementación de interfase para acceso a sistemas inalámbricos de banda ancha
802.16e	Finales 2005	Proporciona movilidad al estándar

2.3.1- Frecuencias

Este estándar puede manejar distintas frecuencias, el uso de cada una de ellas se dará según la conveniencia y la necesidad de los usuarios.

2.3.1.1- Bandas de 10 a 66 Ghz

En este rango el entorno físico que presenta el estándar exige línea de vista para su funcionamiento. Lo más común es encontrar anchos de banda de 25 y 28 Mhz. Está orientado a conexiones punto multipunto (PMP) y para empresa medianas y grandes ya que la taza de transferencia se promedia en los 120 Mbps.

2.3.1.2- Bandas inferiores a los 11 Ghz

Debido a su mayor longitud de onda, no es necesaria la línea de vista. La capacidad de poder manejar línea de vista (LOS) o no, pertenece a la capa física y será dada tanto por la banda que se maneje, la calidad de las antenas y la tecnología de transmisión que estas utilizan.

La mayor ventaja de las bandas menores a 11 Ghz es la libertad en permisos para su funcionamiento especialmente las de 5 a 6 Ghz. La dificultad que puede encontrarse es la interferencia con otros artefactos. El mecanismo que tiene para solucionar este problema de interferencia se encuentra en la capa física y es la selección dinámica de frecuencias (DFS).

Cuadro II.3: Designación de nombres de estándares por frecuencias[1]

Designación	Aplicabilidad	Tipo de duplexación
WirelessMAN-SC™	10-66 GHz	TDD/FDD
WirelessMAN-SCa™	Bajo 11 GHz bandas con licencia	TDD/FDD
WirelessMAN-OFDM™	Bajo 11 GHz bandas con licencia	TDD/FDD
WirelessMAN-OFDMA™	Bajo 11 GHz bandas con licencia	TDD/FDD
WirelessHUMAN™	Bajo 11 GHz bandas libres de licencia	TDD

[1] IEEE COMPUTER SOCIETY, Air Interface For Fixed Broadband Wireless Access Systems, 2004

2.3.2- Modelo de Referencia y alcance del estándar

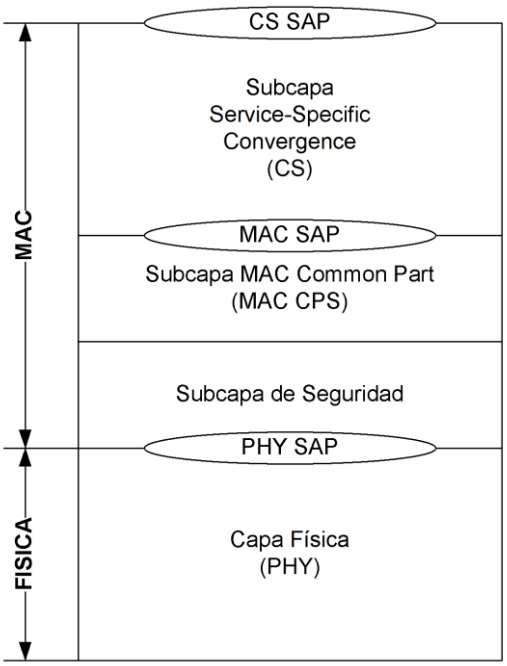


Figura II.4: Capas del estándar IEEE 802.16[1]

Este estándar tiene 2 capas definidas: MAC (control de acceso al medio) y PHY (física).

2.3.2.1- Control de Acceso al Medio (MAC)

Está compuesta por tres subcapas:

- **Service-Specific (CS)**, transforma o mapea la información que viene de la red externa recibida a través de la subcapa de convergencia Service Access Point (SAP) y la envía hacia la MAC Service Data Units (SDU) a través de la MAC Service Data Units

[1] IEEE COMPUTER SOCIETY, Air Interface For Fixed Broadband Wireless Access Systems, 2004

(SAP). Además se encarga del transporte de celdas ATM y paquetes IP.

- **Common Part (CPS),** que recibe los (SDUs) de la MAC Service Data Units (SAP) para clasificarlos y asociarlos al apropiado MAC Service Flow Identifier (SFID) y Connection Identifier (CID).

  Además provee la base de la funcionalidad MAC: acceso al sistema, asignación del ancho de banda, establecer y mantener la conexión.
- **Security,** encargada de la autenticación, intercambio de llaves y encriptación.

2.3.2.2- Física (PHY)

Los datos, el control PHY y las estadísticas son transferidos entre el MAC CPS y la capa física a través del PHY SAP. Esta capa hace referencia a múltiples especificaciones como un apropiado rango de frecuencias y sus debidas aplicaciones.

2.3.3- Funcionamiento de IEEE 802.16

2.3.3.1- La parte física OFDM

La capa física de WirelessMAN-OFDM esta basada en la modulación OFDM. Dirigida principalmente para implementarse en lugares que requieran de accesos fijos como el DSL y cable modem. Soporta sub-canalización en la transmisión (16 canales) basados en TDD y FDD; para la recepción utiliza

Codificación Tiempo-Espacio (STC) y Sistemas de Antenas Inteligentes con Acceso Múltiple por División de Espacio (SDMA).

2.3.3.2- Tipos de encabezados MAC

Existen dos tipos de encabezados MAC: uno genérico y otro que incluye la petición de ancho de banda (BR). En primero es usado para transmitir datos o mensajes MAC, el segundo sirve cuando el cliente remoto (SS) requiere más ancho de banda en la transmisión. La longitud máxima del PDU MAC es de 2048 bytes, incluidos el encabezado, payload y el CRC. Para punto multipunto (PMP) la MAC define ARQ de respuesta rápida, lo que optimiza el uso del ancho de banda.

2.3.3.3- Metodología para ingreso a la red

Para que un SS pueda ingresar a la red debe completar un proceso con la debida BS, que se resume en los siguientes pasos:

- **Sincronización con el canal de recepción,** cuando un SS quiere entrar a la red, escanea un canal en la lista de frecuencias, normalmente un SS es configurado para usar un específico BS con parámetros operacionales dados cuando operan en una banda licenciada. Si el SS encuentra un canal DL y esta disponible para sincronizarse a nivel de capa física, la MAC busca un DCD y un UCD para obtener información de modulación y otros parámetros.
- **Clasificación inicial,** cuando el SS se ha sincronizado con el canal DL y ha recibido el DL y UL MAP para la trama , empieza el proceso de clasificación enviando una petición de clasificación MAC usando

el mínimo poder de transmisión. Si no se recibe respuesta el SS reenvía el mensaje en la trama posterior usando un poder de transmisión mayor. Este proceso se repite hasta encontrar el poder de transmisión óptimo para enviar datos al UL.

- **Capacidad de negociación,** luego de una correcta finalización de la clasificación inicial, el SS envía al BS una descripción de su capacidad de niveles de modulación, esquemas de codificación, tasas y métodos de duplexación. La BS acepta o niega a la SS basándose en sus capacidades antes mencionadas.
- **Autenticación,** luego de la negociación, la BS autentica a la SS y lo provee de una llave para habilitar el cifrado de datos. El SS envía el certificado X.509 de su fabricante y la descripción de los algoritmos de criptografía que soporta. La BS valida la identidad del SS, determina el algoritmo de cifrado y el protocolo que debe usarse y envía una autenticación de respuesta al SS. La respuesta contiene los datos de la clave a ser usada por el SS, continuamente ésta se renueva para mantenerla actualizada.
- **Registro,** luego de una autenticación exitosa, la SS envía un mensaje de registro a la BS, la cual responde a la SS. Este intercambio incluye el soporte para: versión IP, administración del SS, parámetros ARQ, CRC y control de flujo de datos.
- **Conectividad IP,** la SS inicia DHCP (IETF RCF 2131) para obtener la dirección IP y otros parámetros para establecer la conectividad IP, La BS y la SS mantienen la actual fecha y hora usando el protocolo

time of the day (IETF RFC868), entonces la SS descarga los parámetros operacionales usando TFTP (IETF RFC 1350).

- **Creación de la conexión,** el proceso de creación de la conexión es iniciado por la BS, la cual envía un mensaje de petición de servicio a la SS para recibir una confirmación de que la conexión ha sido creada.
- **Clasificación periódica,** en todo el tiempo de la conexión se realiza una clasificación periódica, ajustando el poder de transmisión actual para que la conexión sea lo más óptima posible.

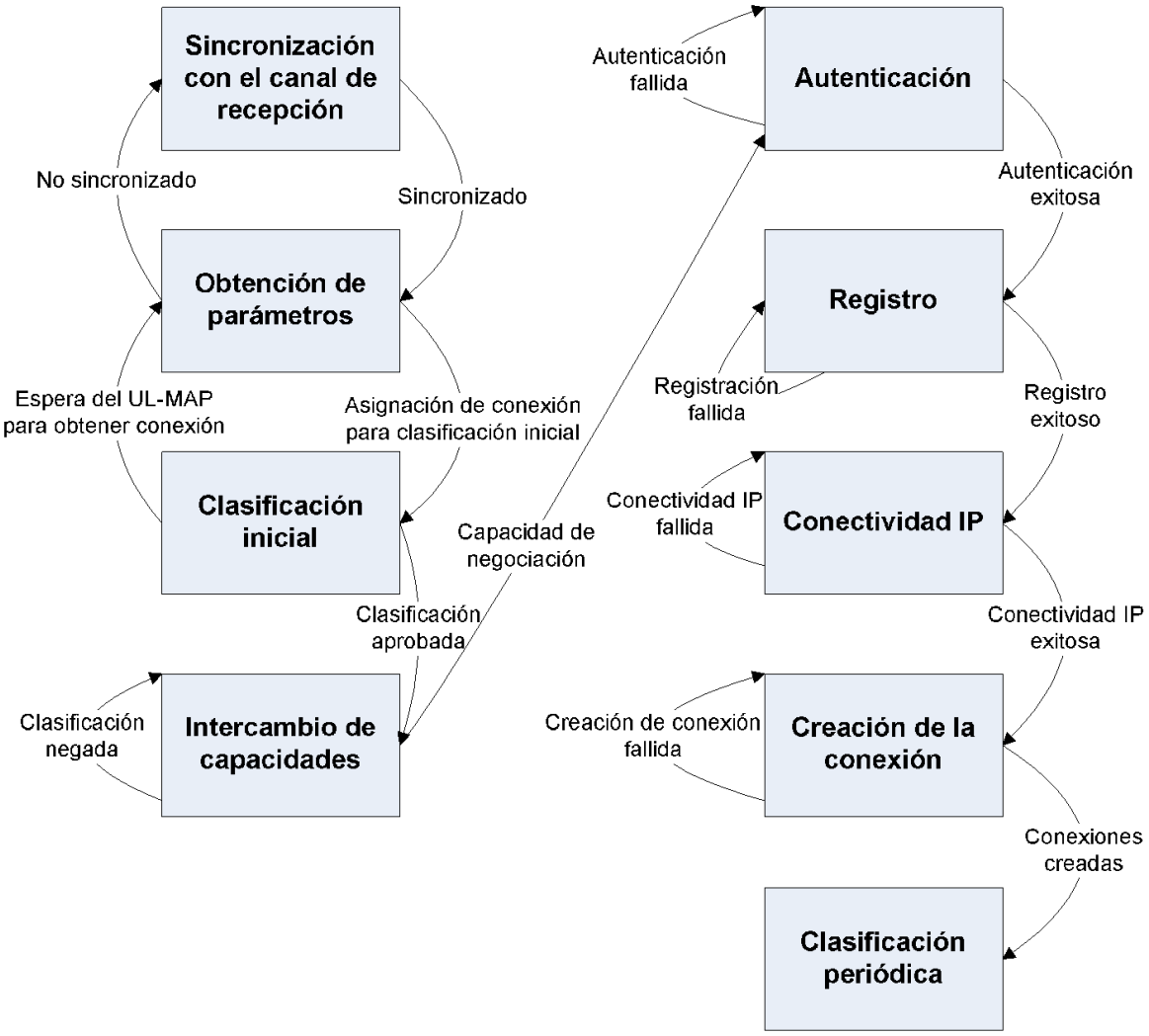


Figura II.5: Proceso de ingreso a la red en IEEE 802.16x[1]

2.3.3.4- Clases de servicio

La capa MAC de 802.16 proporciona diferenciación QoS (Calidad de Servicio) para diferentes tipos de aplicaciones que pueden operar bajo este tipo de redes. Se definen los siguientes tipos de servicio:

[1] INTEL CORPORATION, Intel Technology Journal Vol. 8: WiMAX, 2004

- **Servicios de tipo concesión no solicitada (UGS):** Es designado para soportar servicios con tasa de bits constante (CBR) como: emulación de T1/E1, voz sobre IP (VoIP) sin supresión de silencio.
- **Servicios de tipo sondeo en tiempo real (rtPS):** Designado para soportar servicios en tiempo real que generan paquetes de tamaño variable sobre una base periódica, como video MPEG o VoIP con supresión de silencio.
- **Servicios de tipo sondeo en tiempo no real (nrtPS):** Designado para soportar servicios en tiempo no real que requieren concesión de tamaños de datos variables sobre una base regular, como la transmisión de archivos.
- **Servicios de tipo el mejor esfuerzo (BE),** Aquellos servicios como el usado en la actualidad para navegar por el Internet.

2.3.4- ATM, IPv6, VoIP en 802.16

802.16 soporta diferentes tipos de servicios y protocolos como: ATM, IPv4, IPv6, Ethernet, VLAN's, VoIP, QoS entre otros, proporcionando una gama de posibilidades en cuanto a voz y datos se refiere, adicionalmente, puede funcionar como un backhaul para conectar redes WiFi (802.11x) y hotspots al Internet.

Para soportar estos servicios antes mencionados, 802.16 debe tratar a los diferentes canales del aire como partes separadas a nivel MAC, así por ejemplo, una simple BS puede utilizar dos canales de 10 MHz en paralelo como dos instancias MAC separadas. Este tipo de virtualización es necesario debido a que el uso y la localización del ancho de banda aéreo dependen en gran parte de las

políticas del carrier, de la carga del sistema y del estado de las radiofrecuencias en ese momento.

2.4- La tecnología WiMAX, presente y futuro

Como toda tecnología o estándar tiene un proceso de crecimiento, esto se va dando según las necesidades de los investigadores o de los usuarios que comprometen a las empresas involucradas a permanecer actualizadas.

2.4.1- Presente de WiMAX

Hasta el año 2004 las empresas desarrolladoras no habían hecho sino estudios técnicos más profundos para el estándar que lo rige, en común acuerdo las empresas desarrolladoras ofrecieron la muestra de equipos para poner a prueba con casos de estudio para el año 2005. Hay que tomar en cuenta que los equipos aparecen en el momento que la estructura del estándar es lo suficientemente robusta para satisfacer todos los problemas y necesidades que se presenten.

Como se ha visto en otras tecnologías inalámbricas, especialmente en WiFi (IEEE 802.11x), la flexibilidad de los equipos para adaptarse a las diferentes tecnologías dentro del mismo estándar 802.11a, 802.11b, 802.11g, fueron apareciendo con el transcurso del tiempo; WiMAX, como se mencionó anteriormente, no es una tecnología nueva, sino el desarrollo y mejora de las ya existentes, por lo tanto los equipos desarrollados tienen la capacidad de brindar flexibilidad para los otros estándares inalámbricos en especial con WiFi y la interoperabilidad con sistemas de red con cableado.

En el presente por lo tanto se puede hablar ya de una estandarización real. Se ha llegado ahora a extender el rango de cobertura de 40 a 70 kilómetros, trabajando en bandas de 2 a 11 Ghz, siendo esta común en muchos lugares y por lo tanto no requiere licenciamiento. Válido para topologías PMP sin requerir línea de vista directa. También con bandas de 3.5 y 10.5 Ghz. Las bandas que requieren permisos son 2.5 - 2.7 Ghz en los Estados Unidos y otros países de Latinoamérica. Pero más común son las de 2.4 Ghz y de 5.725 – 5.825 Ghz, que no requieren de licencia de utilización alguna.

WiMAX tiene tecnologías competitivas que tratan de brindar el mismo servicio o características como es el estándar Hiperaccess (>11 Ghz) y HiperMAN (<11 Ghz). Pero el crecimiento de WiMAX ha generado la necesidad de otros estándares en comenzar a armonizar el trabajo con este estándar basándose en la modulación OFDM. Con la tecnología de WiMAX se tiene ciertas características que se pueden satisfacer:

- Por su capacidad de velocidad y ancho de banda, reemplazar enlaces T1 y E1
- Trabaja bajo cualquier protocolo, entre los principales IP y ATM, que a nivel corporativo son los más utilizados.
- Por la característica anterior puede transportar voz sobre IP (VoIP), datos, video.
- Compatibilidad con antenas telefónicas de tercera generación, con la capacidad de apuntar a su emisor constantemente a pesar que se encuentra en movimiento.

En el momento se encuentran 110 empresas inscritas en el WiMAX Forum, siendo los encargados de regir y controlar el desarrollo de esta tecnología. Dentro de las variaciones que están ahora en desarrollo para este estándar es la movilidad de WiMAX con la publicación del estándar IEEE 802.16e, que se espera para Octubre del 2005. Este brindará al usuario la posibilidad de trasportarse sin perder el servicio en el caso que salga del rango de cobertura de su antena proveedora de servicios, ingresando a la siguiente dentro del área geográfica, proceso conocido como “handover”.

2.4.1.1- Tecnología Actual

Las empresas desarrolladoras, esperan tener un estándar robusto para el diseño de equipos de interconexión. La Intel da el primer paso con el chip “Intel WiMAX ProWireless 5116 technology”. Basado en este chip, empresas como Airspan han desarrollado equipos con características con tecnología de alta calidad para brindar soluciones inalámbricas. Airspan es de las empresas más innovadoras dentro del mercado, tienen una muestra de productos que se van a posicionar en el mercado para finales del 2005. Todos los productos pasan por controles de calidad y certificaciones legislados por el WiMAX Forum. Con el módem desarrollado por la Intel, el 5116, la capacidad de interconexión con diferentes tecnologías, tanto WiFi, tecnología inalámbrica, etc. La comercialización de los equipos se pronostican son para inicios del 2006.

2.4.2- El futuro de WiMAX.

El futuro más cercano de WiMAX es la próxima publicación de la actualización al estándar, que va a ser en Octubre la IEEE 802.16e, que se va a basar en la capacidad de generar una tecnología para interconexión de redes inalámbricas con movilidad para los usuarios.

WiMAX tiene previsto su crecimiento en tres fases:

1. En la primera mitad del año 2005, basado en el estándar IEEE 802.16-2004, se tendrán conexiones de banda ancha inalámbricas fijas.
2. En la segunda mitad del año 2005, se cubrirá la parte de instalaciones en interiores, con antenas parecidas a las de tecnología WiFi; tratando con esto de abaratar costos, mejorar espacios y brindar banda ancha en espacios comerciales más reducidos.
3. Después de la publicación del estándar 802.16e que se espera para Octubre del 2005, la capacidad de dispositivos como portátiles de movilizarse sin perder señal iterando con las áreas de servicio, o sea el llamado “handover”.

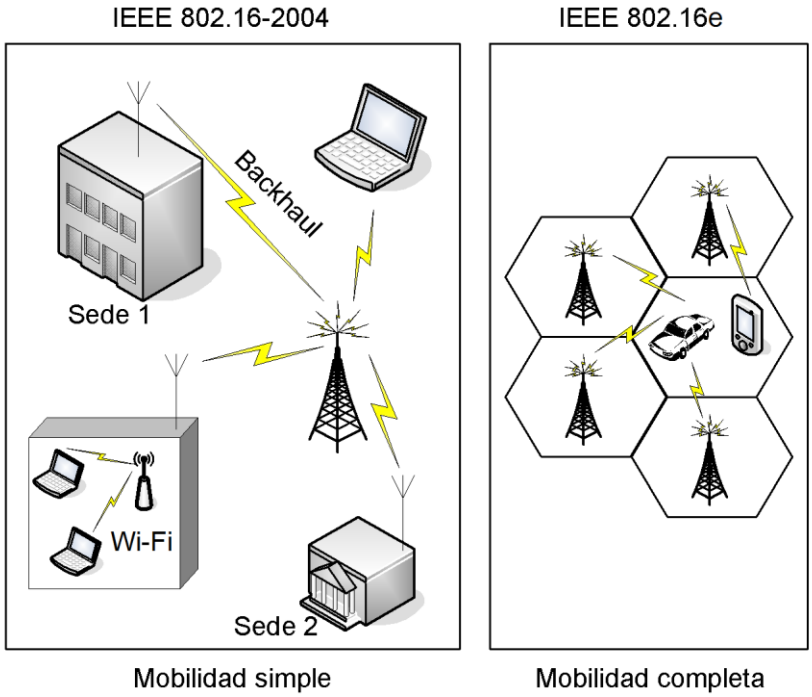


Figura II.6: Evolución de WiMAX[1]

El abaratamiento de costos de instalación y de equipos como toda tecnología se dará transcurrido el tiempo. Todavía no se habla de precios pero si de catálogos de equipos que pueden realizar la conexión.

Pero en sí la orientación o es para reemplazar la fibra ni tecnologías WiFi, sino coexistir con ellas pero para nuevas instalaciones mejorar los costos frente a estas mencionadas.

Como se ha visto en otros estándares como Ethernet (IEEE 802.3), que apareció para tecnologías de velocidades de 10 Mbps, pasado el tiempo, han llegado a tener variaciones y mejoras a ese estándar que no eran calculables desde su inicio sino con la aparición de nuevas tecnologías y necesidades; de la

[1] INTEL CORPORATION, Intel Technology Journal Vol. 8: WiMAX, 2004

misma manera se presentará con IEEE 802.16, irá variando para acoplarse con las necesidades del mercado y según su aceptación se verá el desarrollo de equipos que va a la par con el estándar.

2.5- Análisis comparativo entre tecnologías existentes

En la actualidad, la tecnología brinda diferentes soluciones a nuestros problemas, para realizar una conexión de red en una oficina, no solo se cuenta con diferentes tipos de cableados: UTP, STP, FIBRA, etc., sino también la oportunidad de realizar interconexiones de forma inalámbrica: Bluetooth, WiFi, WiMAX, MobileFi y Telefonía Inalámbrica.

Lo importante es que según las necesidades y requerimientos que se tenga en nuestra red corporativa, realizar la mejor elección tanto para costos y para soporte de tecnología. Ahora en muchos lugares es importante la situación geográfica. En el Ecuador por ejemplo la posibilidad de contratar enlaces de banda ancha en cualquier lugar es todavía un sueño por la tecnología que brindan las operadoras locales; conexiones dentro de edificios antiguos también es un problema para la conexión de un cableado estructurado, es por ello que se debe tomar en cuenta la utilización de tecnología inalámbrica para la solución de estos problemas.

Cuadro II.4: Comparación entre WiMAX y otras tecnologías inalámbricas

	WiMAX 802.16	**WiFi 802.11**	**Mobile-Fi 802.20**	**UMTS y cdma2000**
Velocidad	124 Mbps	11-54 Mbps	16 Mbps	2 Mbps
Cobertura	40-70 Km	300 m	20 km	10 km
Licencia	Si/No	No	Si	Si
Ventajas	Velocidad, Ancho de banda, Movilidad y Alcance	Velocidad y Precio	Velocidad y Movilidad	Rango y Movilidad
Desventajas	Interferencias	Bajo alcance	Precio alto	Lento y caro

Cuadro II.5: Comparación entre WiMAX y las tecnologías celulares

	Celular			**WiMAX**	
	Edge	HSPDA	1xEVDO	802.16-2004	802.16e
Familia tecnológica y modulación	TDMA GMSK y 8-PSK	WCDMA (5 MHz) QPSK y 16 QAM	CDMA2K QPSK y 16 QAM	OFDM/OFDMA QPSK, 16 QAM y 64 QAM	OFDMA QPSK escalable, 16 QAM y 64 QAM
Velocidad máxima de los datos	473 Kbps	10,8 Mbps	2,4 Mbps	75 Mbps (canal de 20 MHz) 18 Mbps (canal de 5 MHz)	75 Mbps (máx.)
Velocidad promedio para el usuario	Velocidad < 130 Kbps	< 750 Kbps inicialmente	< 140 Kbps	1–3 Mbps	80% de rendimiento del modelo de uso fijo
Alcance en exteriores (célula promedio)	2–10 km	2–10 km	2–10 km	2–10 km	2–7 km
Ancho de banda del canal	200 Khz.	5 MHz	1,25 MHz	1,5–20 MHz, escalable	1,5–20 MHz, escalable

Es fácil distinguir en el cuadro la ventaja de WiMAX sobre otras tecnologías, el único inconveniente que se presente sería las dudas sobre las interferencias por manejarse en distintos rangos de frecuencias, pero esto se ve solucionado por tener una flexibilidad en el uso de frecuencias según las interferencias que se encuentren. WiMAX tiene la capacidad de realizar un cambio de frecuencias según la necesidad y el estado de interferencias.

La utilización de modulación OFDM en la mayoría de las tecnologías inalámbricas probadas y ya existentes, hace que WiMAX sea confiable.

Uno de los grandes problemas con la transferencia de radio a largas distancias es la perdida de potencia en la señal, pero ahora con la tecnología de avanzada que se ha desarrollado con la telefonía celular, la capacidad de las antenas de recibir información y decodificarla sin errores ha mejorado notablemente. Y de esto se vale también WiMAX.

Como se puede apreciar, WiMAX utiliza tecnología probada y desarrollada con estándares que ya están en el mercado por lo que WiMAX se convierte en una tecnología estable y si la tecnología que otras inalámbricas utilizan y están en el mercado, WiMAX al mejorar su estándar para soportar mejor ancho de banda, largas distancias y con IEEE 802.16e movilidad, basándose con tecnología ya probada lo hace el mejor estándar inalámbrico para interconexión de redes MAN y próximamente LAN y Móvil.

En el Ecuador la conectividad de las escuelas y colegios, bases de la educación, al mundo de Internet con banda ancha, todavía es muy limitado. Dentro de los motivos fundamentales están: altos costos, situación geográfica y falta de tecnología del proveedor. Estos tres problemas se ven solucionados con

WiMAX, el adquirir un SS para la conexión a uno de los proveedores de Internet inalámbrico va a ser barato, sencillo y físicamente accesible, así se tendría la posibilidad de crecer a nivel país dentro del mundo del Internet.

2.6- Seguridad en sistemas de interconexión

Los datos de los sistemas informáticos están en constante peligro por varias causas: errores de los usuarios o ataques intencionados o fortuitos. Pueden producirse accidentes y ciertas personas con intención de atacar el sistema pueden obtener acceso al mismo e interrumpir los servicios, inutilizar los sistemas o alterar, suprimir o robar información.

Los aspectos donde la información puede sufrir daños son los siguientes:

- **Disponibilidad.-** Es la capacidad de obtener la información en el momento en que se la requiera.
- **Integridad.-** La información debe estar protegida de las modificaciones no permitidas, accidentales o imprevistas.
- **Confidencialidad.-** El sistema contiene información que requiere protección contra la divulgación no autorizada.

La seguridad informática maneja dos conceptos bien definidos como parámetros para hacerla cumplir, estos son: seguridad física y seguridad lógica

Seguridad Física

La seguridad física trata de la protección del hardware y el soporte de datos, también se toma en cuenta los lugares donde se encuentran instalados. Enmarca en sí desastres naturales, incendios, sabotajes, robos y directivas en políticas de seguros sobre los dispositivos.

Seguridad Lógica

La seguridad lógica trata sobre la seguridad en el uso de las aplicaciones (software), protección de datos, procesos y programas, también sobre las políticas de acceso de usuarios a la información.

Cumplidas de manera eficiente estos dos conceptos será fácil manejar auditorías en seguridad.

Para hacer cumplir las seguridades totales dentro de un sistema de red en la ESPE se deben tomar ciertos parámetros o procedimientos a seguir, por lo tanto a continuación mostraremos las fases que cubren el proceso de seguridad para el enlace entre sedes mostrado en capítulos anteriores:

- Análisis de riesgo
- Políticas de seguridad
- Pruebas de intrusión
- Estándar ISO 17799
- Quality of Service (QoS)
- Informática forense

2.7- Análisis de riesgo

Para crear políticas de seguridades de la red, se debe conocer la fuente de las amenazas que generan riesgos, cuales son los recursos que en verdad vale la pena proteger dando importancia unos sobre otros. Todo plan de seguridad es útil únicamente que los esfuerzos por realizar los estudios para generar seguridades sean adoptados e implementados.

Como se ha indicado, lo principal es saber la fuente de donde pueden provenir los problemas y a que parte de nuestra infraestructura afectaría. Para ello está el análisis de riesgo que implica determinar lo siguiente:

- ¿Qué se necesita proteger?
- ¿De que se necesita proteger?
- ¿Cómo protegerlo?

Los riesgos deben clasificarse por nivel de importancia y gravedad de la perdida. No debe terminar en una situación en la que gaste más en proteger algo que es de menor valor para la Institución.

Dentro de este esquema, se pueden reconocer algunos de los componentes estudiados en una Análisis de Riesgos:

- **Riesgo:** es el potencial que tiene una amenaza de explotar las vulnerabilidades asociadas con un activo, comprometiendo la seguridad de éste.
- **Activo:** es un componente relacionado con la información, el cual tiene un valor asignado por la entidad directamente relacionada con éste. Dicho valor representa el nivel de importancia que tiene el activo en el "proceso del negocio".
- **Vulnerabilidad:** es una debilidad en las Tecnologías de Información que hace susceptible un activo a una amenaza.
- **Amenaza:** es un evento, acción o agente que puede comprometer a un activo
- **Impacto:** es la magnitud en que afecta la materialización de un riesgo.

2.8- Políticas de seguridad

Se puede definir política de seguridad de la información como el conjunto de normas, reglas, procedimientos y prácticas que regulan la protección de la información contra la pérdida de confidencialidad, integridad o disponibilidad, tanto de forma accidental como intencionada.

La política de seguridad nos indica:

- Qué hay que proteger.
- Qué principios hemos de tener en cuenta.
- Cuáles son los objetivos de seguridad a conseguir.
- La asignación de cometidos y responsabilidades.

2.9- Encriptación de datos en WiMAX

Para proteger la información la tecnología ha ido a la par con los estudios matemáticos para realizar la encriptación de la información. A continuación se describen los métodos de encriptamiento utilizados en WiMAX, específicamente en equipos citados en la fase de diseño.

2.9.1- AES

AES (Advanced Encryption Standard) es un algoritmo criptográfico usado para la protección de la información, AES puede generar llaves de 128, 192 y 256 bits, y encripta y desencripta información en bloques de 128 bits (16 bytes). A diferencia a de las llaves públicas que utiliza un par de llaves, las llaves simétricas que utiliza AES maneja una misma llave para encriptar y desencriptar información.

La información encriptada retorna en un bloque de cifras que tiene el mismo número de bits que la información que fue ingresada.

El algoritmo AES está basado en permutaciones y sustituciones, donde las permutaciones son el reordenamiento de la información y las sustituciones es el reemplazo de una unidad de información por otra.

Para comparar la eficacia de AES, desde su página web NIST afirma que mientras que el desfasado DES podría actualmente quebrantarse después de varias horas de intento, se necesitarían 149 trillones de años con un algoritmo AES de sólo 128 bits siempre y cuando se crease previamente el equipo adecuado para hacerlo.

2.9.2- DES [1]

DES (Data Encryption Standard) es un esquema de encriptación simétrico. Se basa en un sistema mono alfabético, con un algoritmo de cifrado consistente en la aplicación sucesiva de varias permutaciones y sustituciones. Inicialmente el texto en claro a cifrar se somete a una permutación, con bloque de entrada de 64 bits (o múltiplo de 64), para posteriormente ser sometido a la acción de dos funciones principales, una función de permutación con entrada de 8 bits y otra de sustitución con entrada de 5 bits, en un proceso que consta de 16 etapas de cifrado.

---

[1] LUCIANO MORENO, Criptografía (VII) http://www.htmlweb.net/seguridad/cripto/cripto_7.html), 2005

En general, DES utiliza una clave simétrica de 64 bits, de los cuales 56 son usados para la encriptación, mientras que los 8 restantes son de paridad, y se usan para la detección de errores en el proceso.

Como la clave efectiva es de 56 bits, son posible un total de 2 elevado a 56 = 72.057.594.037.927.936 claves posibles, es decir, unos 72.000 billones de claves, por lo que la ruptura del sistema por fuerza bruta o diccionario es sumamente improbable, aunque no imposible si se dispone de suerte y una gran potencia de cálculo.

Los principales inconvenientes que presenta DES son:

- Se considera un secreto nacional de EEUU, por lo que está protegido por leyes específicas, y no se puede comercializar ni en hardware ni en software fuera de ese país sin permiso específico del Departamento de Estado.
- La clave es corta, tanto que no asegura una fortaleza adecuada. Hasta ahora había resultado suficiente, y nunca había sido roto el sistema. Pero con la potencia de cálculo actual y venidera de los computadores y con el trabajo en equipo por Internet se cree que se puede violar el algoritmo, como ya ha ocurrido una vez, aunque eso sí, en un plazo de tiempo que no resultó peligroso para la información cifrada.
- No permite longitud de clave variable, con lo que sus posibilidades de configuración son muy limitadas, además de permitirse con ello la creación de limitaciones legales.
- La seguridad del sistema se ve reducida considerablemente si se conoce un número suficiente textos elegidos, ya que existe un sistema

matemático, llamado Criptoanálisis Diferencial, que puede en ese caso romper el sistema en 2 elevado a 47 iteraciones.

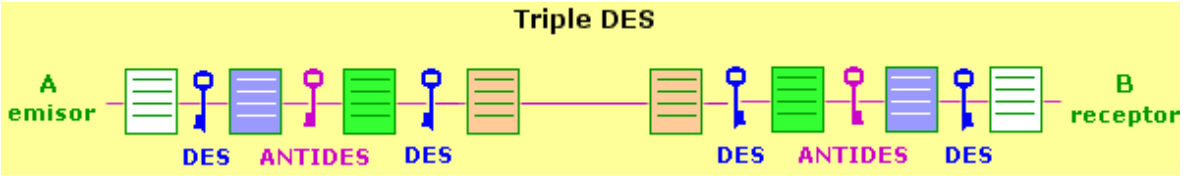
- Entre sus ventajas cabe citar:
- Es el sistema más extendido del mundo, el que más máquinas usan, el más barato y el más probado.
- Es muy rápido y fácil de implementar.
- Actualmente DES ya no es estándar y fue roto en Enero de 1999 con un poder de cómputo que efectuaba aproximadamente 250 mil millones de ensayos en un segundo.

2.9.2.1- Triple DES

Como se ha visto, el sistema DES se considera en la actualidad poco práctico, debido a la corta longitud de su clave. Para solventar este problema y continuar utilizando DES se creó el sistema Triple DES (TDES), basado en tres iteraciones sucesivas del algoritmo DES, con lo que se consigue una longitud de clave de 128 bits, y que es compatible con DES simple.

Este hecho se basa en que DES tiene la característica matemática de no ser un grupo, lo que implica que si se encripta el mismo bloque dos veces con dos llaves diferentes se aumenta el tamaño efectivo de la llave.

Para implementarlo, se toma una clave de 128 bits y se divide en 2 diferentes de 64 bits, aplicándose el siguiente proceso al documento en claro:



1. Se le aplica al documento a cifrar un primer cifrado mediante la primera clave, C1.
2. Al resultado (denominado ANTIDES) se le aplica un segundo cifrado con la segunda clave, C2.
3. Y al resultado se le vuelve a aplicar un tercer cifrado con la primera clave, C1.

Si la clave de 128 bits está formada por dos claves iguales de 64 bits (C1=C2), entonces el sistema se comporta como un DES simple.

Tras un proceso inicial de búsqueda de compatibilidad con DES, que ha durado 3 años, actualmente TDES usa 3 claves diferentes, lo que hace el sistema mucho más robusto, al conseguirse longitudes de clave de 192 bits (de los cuales son efectivos 168), mientras que el uso de DES simple no está aconsejado.

2.10- Pruebas de intrusión

Las pruebas de intrusión permiten saber si el nivel de seguridad que se ha tomado es vulnerable o no, de tal manera, que se puedan hacer modificaciones antes de la puesta en marcha del proyecto.

Los intrusos informáticos utilizan diversas técnicas para romper los sistemas de seguridad de una red. Básicamente buscan los puntos débiles del sistema para poder ingresar.

Los administradores de red de la ESPE deben delegar gente para que hagan el trabajo de “testers”.

Los intrusos cuentan con grandes herramientas como scanners, cracking de passwords, software de análisis de vulnerabilidades, exploits y probablemente

el arma más importante: la ingeniería social. Un administrador cuenta con todas ellas empleadas para bien, los logs, los sistemas de detección de intrusos y los sistemas de rastreo de intrusiones.

Al conjunto de técnicas que se utilizan para evaluar y probar la seguridad de una red se le conoce como “ethical hacking”, uno de los recursos más poderosos con los que se cuenta hoy para generar barreras cada vez más eficaces.

Un test está totalmente relacionado con el tipo de información que se maneja en la institución. Por consiguiente, según la información que deba ser protegida, se determinan las estructuras y las herramientas de seguridad.

El software y el hardware utilizados son una parte importante, pero no única. A ella se le agrega lo que se denomina “políticas de seguridad internas”, descritas anteriormente.

El “Penetration test” o “ethical hacking”, es un conjunto de metodologías y técnicas para realizar una evolución integral de las debilidades de los sistemas informáticos. Consiste en un modelo que reproduce intentos de acceso a cualquier entorno informático de un intruso potencial desde los diferentes puntos de entrada que existan, tanto internos como remotos.

2.11- Informática Forense

Informática forense es el conjunto de herramientas y técnicas que son necesarias para encontrar, preservar y analizar pruebas digitales frágiles, que son susceptibles de ser borradas o sufrir alteración de muchos niveles. Quienes la practican reúnen esos datos y crean una llamada prueba de auditoría para juicios

penales. Buscan información que puede estar almacenada en registros de acceso, registros específicos, modificación de archivos intencionalmente, eliminación de archivos y otras pistas que puede dejar un atacante a su paso.

La idea principal en este tipo de análisis es contar completamente con todo el apoyo del usuario y depende exclusivamente del manejo inmediato que el usuario le haya dado al incidente, ya que al ingresar al sistema o apagar el servidor se puede perder información valiosa para análisis posteriores.

Para este tipo de análisis, se debe recopilar posibles pruebas del ataque y de la ubicación desde donde se realizo, la información modificada, alterada completamente o borrada y los posibles perjuicios al funcionamiento normal de los dispositivos. No está orientada a tomar acciones legales.

CAPITULO III: ANÁLISIS DE LA SITUACION ACTUAL

En un establecimiento universitario como es la ESPE que maneja varias dependencias, sedes y facultades, el estudio de la red se debe orientar a la optimización de recursos y servicios que se prestan a las diferentes áreas mencionadas. Para esto se debe categorizar en tres distintos tipos de redes: LAN, WLAN, WAN.

En todos los casos de estudios se utiliza una metodología para el análisis estructurada de la siguiente manera:

- Evaluación física.
- Determinación de las aplicaciones críticas dentro de la red y parámetros relevantes de tráfico.
- Estimación del uso de la LAN/WLAN incluyendo protocolos y congestión.
- Recomendaciones para el funcionamiento óptimo del sistema de red.

3.1- Análisis del estado de las redes inalámbricas existentes en la ESPE

Toda la información recopilada a continuación ha sido recogida y entregada por la Dirección de Organización y Sistemas de la ESPE.

3.1.1- Redes inalámbricas de área local (WLAN) de la ESPE

En la actualidad, la ESPE no dispone de una red inalámbrica estructurada, siendo la sede Sangolquí la única que posee redes puntuales, distribuidas como se indica en la figura:

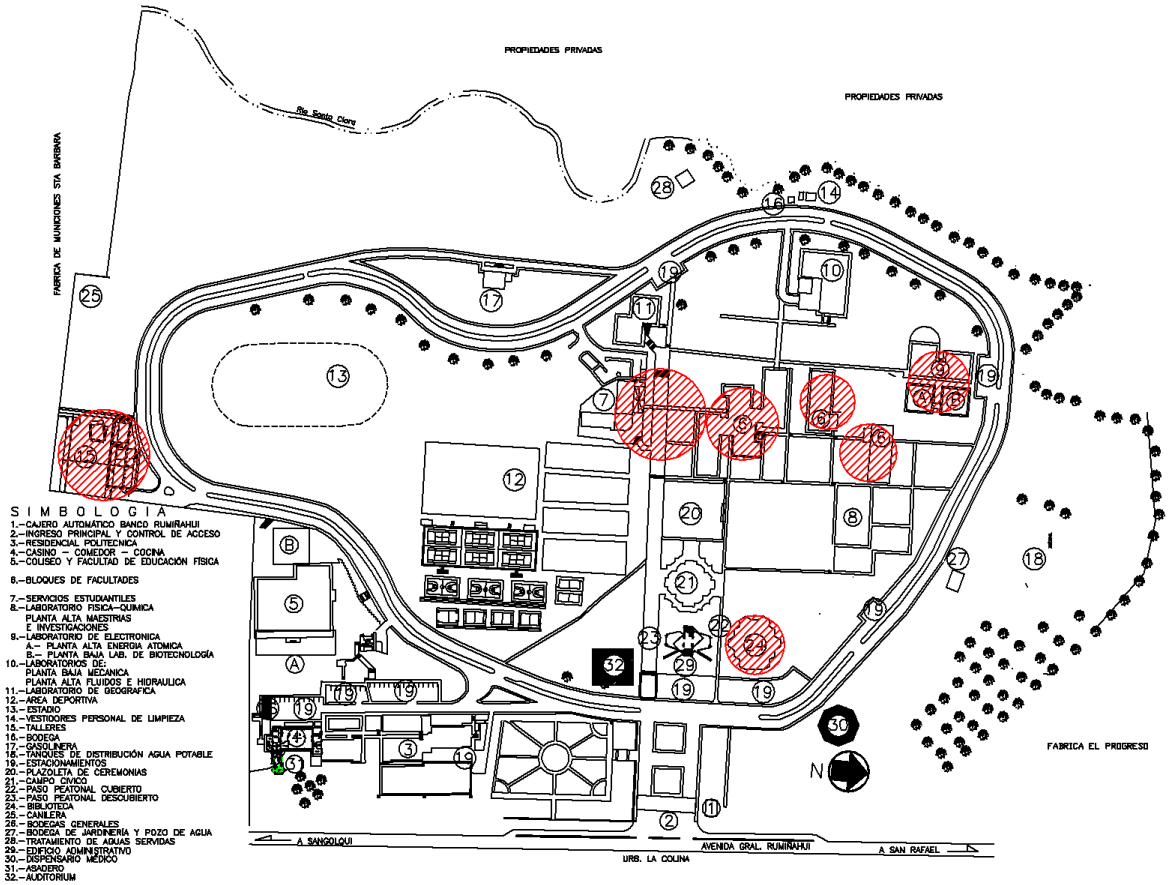


Figura III.1: Ubicación y alcance de redes inalámbricas actuales en el campus Sangolquí

3.1.2- Redes de área local (LAN) de la ESPE

La sede Sangolquí posee un cableado estructurado basado principalmente en fibra óptica entre los edificios principales y dentro de éstos, cable UTP. La figura muestra la estructura general del cableado existente en el campus Sangolquí.

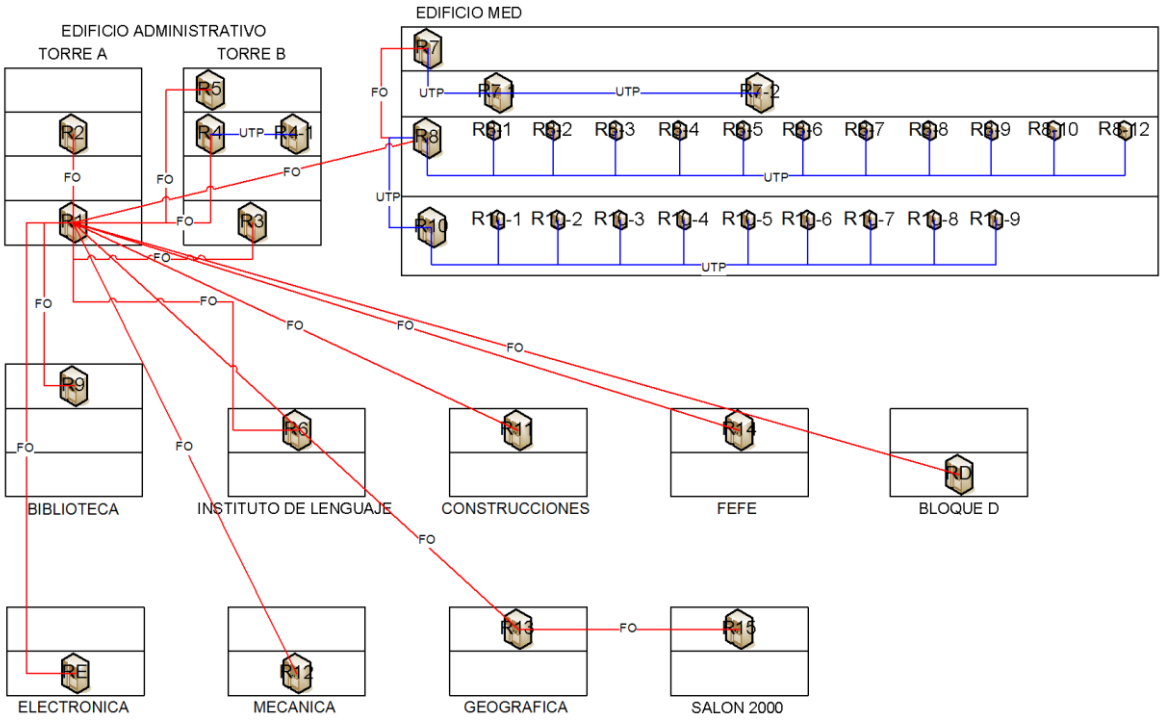


Figura III.2: Diagrama unifilar de la red de datos sede Sangolquí

3.1.3- Enlaces existentes en la actualidad entre sedes de la ESPE

En la actualidad, la ESPE posee conexión entre las sedes, con la limitación del ancho de banda que ofrecen estos canales basados en tecnología xDSL arrendados a la empresa AndinaDatos mediante un pago mensual por este servicio. A continuación se presenta un grafico que detalla las velocidades de transferencia y los equipos que se encuentran en cada una de las sedes.

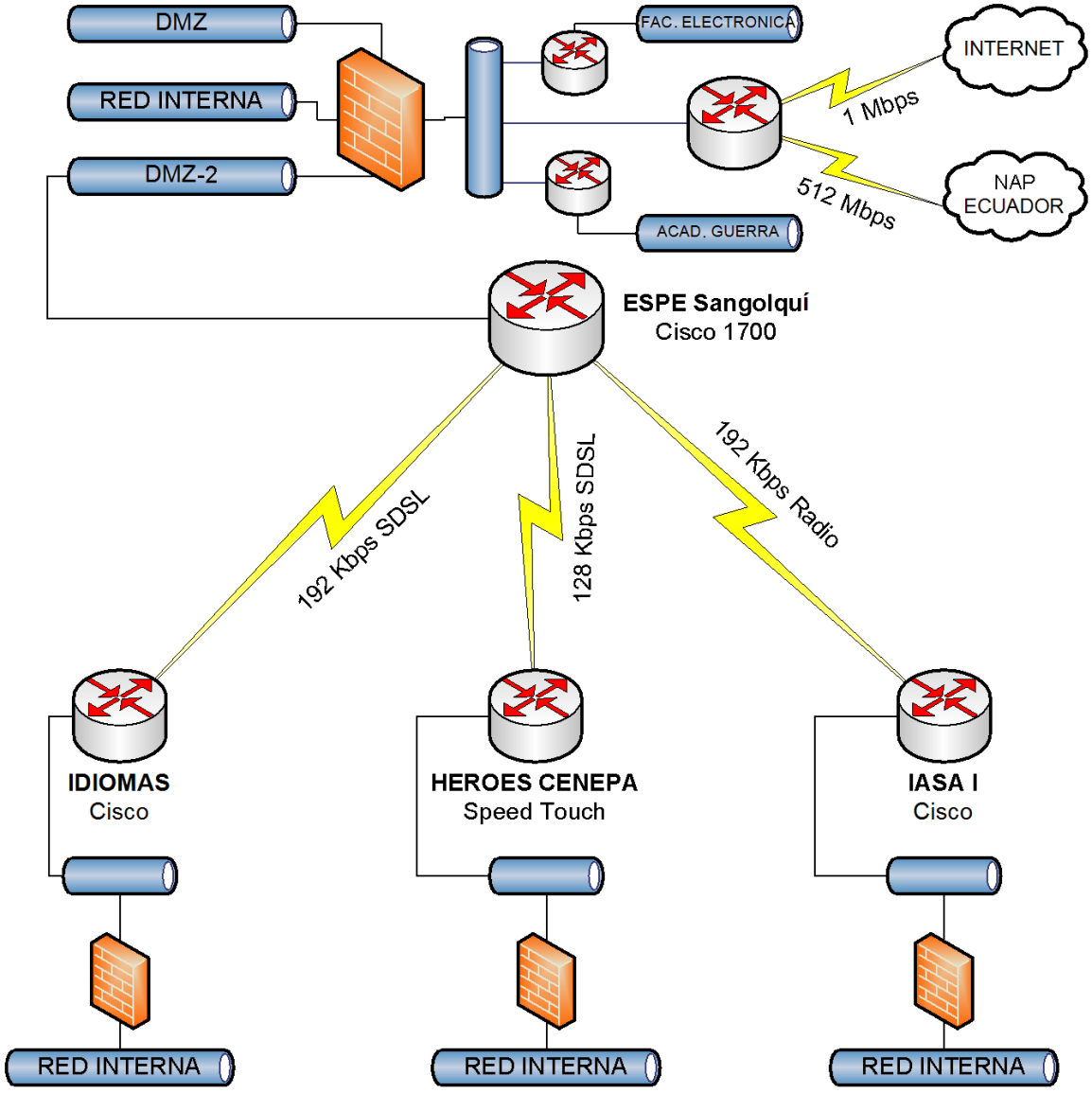
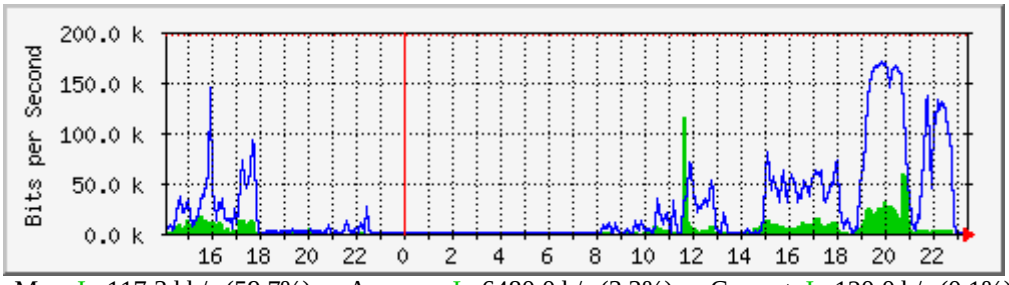


Figura III.3: Diseño lógico de la conectividad con las sedes

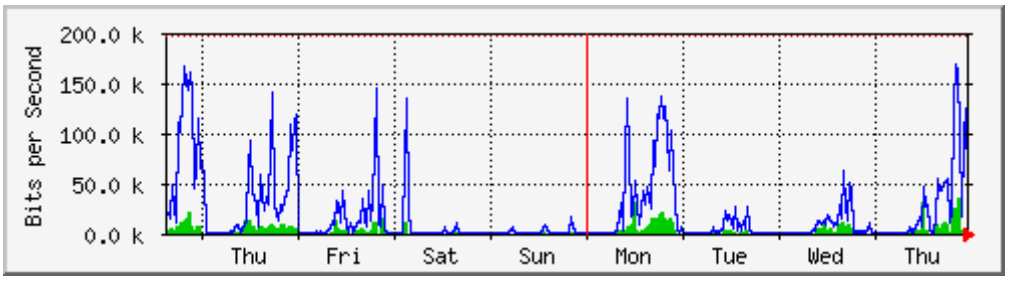
3.1.4- Análisis del tráfico de la red entre sede Sangolquí y sede Idiomas

Los datos presentados a continuación están basados en que la velocidad máxima de recepción y transmisión de datos es igual a 192 Kbps.



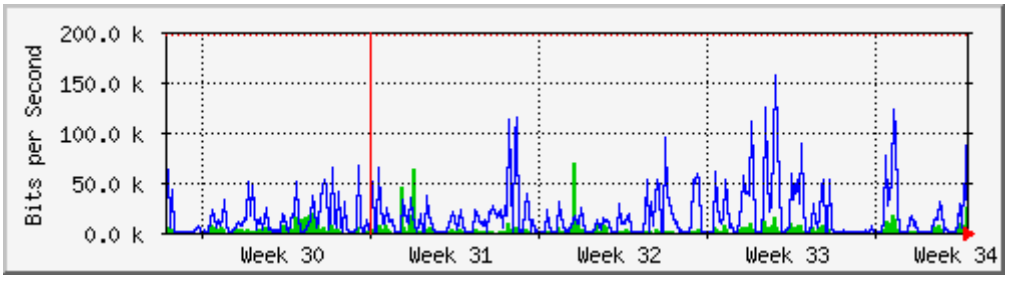
Max In:117.3 kb/s (59.7%) Average In:6480.0 b/s (3.3%) Current In:120.0 b/s (0.1%)
Max Out:171.0 kb/s (87.0%) Average Out:30.3 kb/s (15.4%) Current Out:120.0 b/s (0.1%)

Figura III.4: Tráfico diario entre sedes Sangolquí e Idiomas



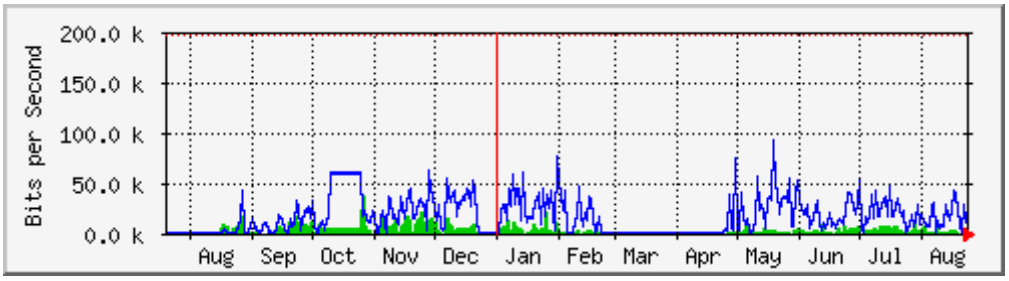
Max In: 36.9 kb/s (18.8%) Average In:3576.0 b/s (1.8%) Current In: 2368.0 b/s (1.2%)
Max Out:168.8 kb/s (85.9%) Average Out:20.6 kb/s (10.5%) Current Out: 47.9 kb/s (24.4%)

Figura III.5: Tráfico semanal entre sedes Sangolquí e Idiomas



Max In: 70.4 kb/s (35.8%) Average In:3848.0 b/s (2.0%) Current In: 27.2 kb/s (13.9%)
Max Out:156.1 kb/s (79.4%) Average Out: 16.7 kb/s (8.5%) Current Out:140.4 kb/s (71.4%)

Figura III.6: Tráfico mensual entre sedes Sangolquí e Idiomas

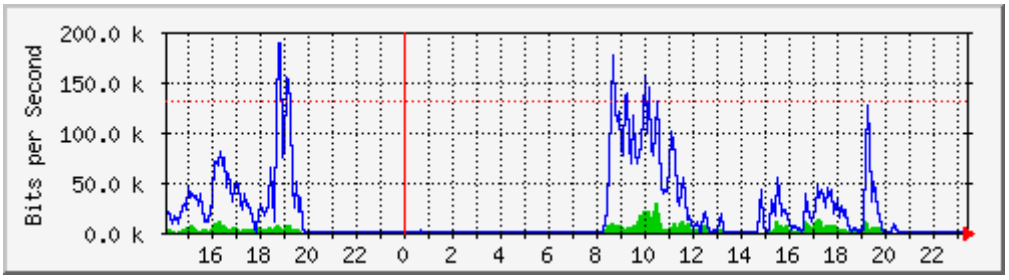


Max In:39.2 kb/s (20.0%) Average In:4488.0 b/s (2.3%) Current In:2744.0 b/s (1.4%)
Max Out:92.6 kb/s (47.1%) Average Out: 19.0 kb/s (9.7%) Current Out:8424.0 b/s (4.3%)

Figura III.7: Tráfico anual entre sedes Sangolquí e Idiomas

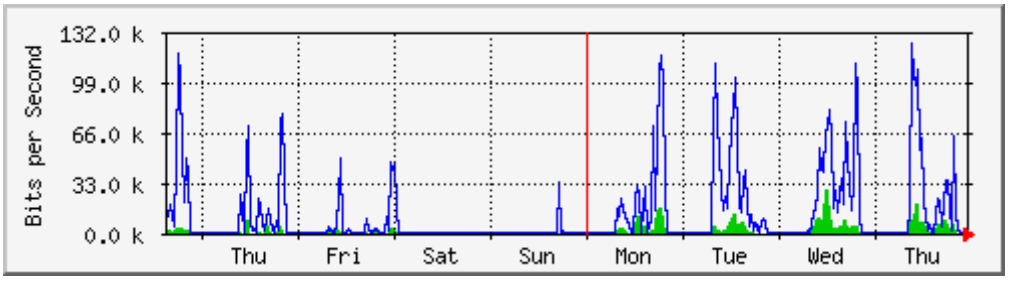
3.1.5- Análisis del tráfico de la red entre sede Sangolquí y sede Héroes del Cenepa

Los datos presentados a continuación están basados en que la velocidad máxima de recepción y transmisión de datos es igual a 128 Kbps.



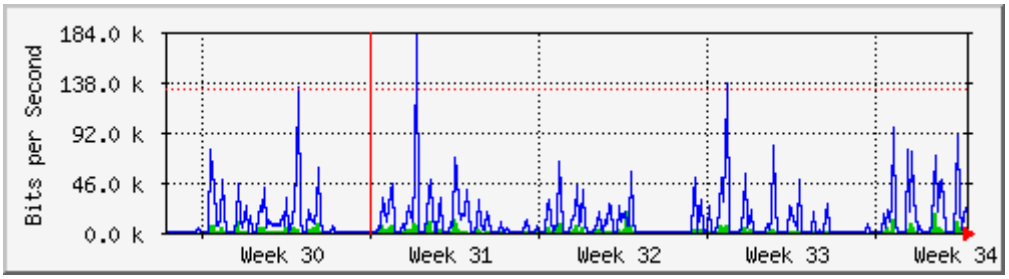
Max In: 30.2 kb/s (23.1%) Average In:4000.0 b/s (3.1%) Current In:920.0 b/s (0.7%)
Max Out:189.1 kb/s (144.3%) Average Out:25.4 kb/s (19.4%) Current Out:656.0 b/s (0.5%)

Figura III.8: Tráfico diario entre sedes Sangolquí y Héroes del Cenepa



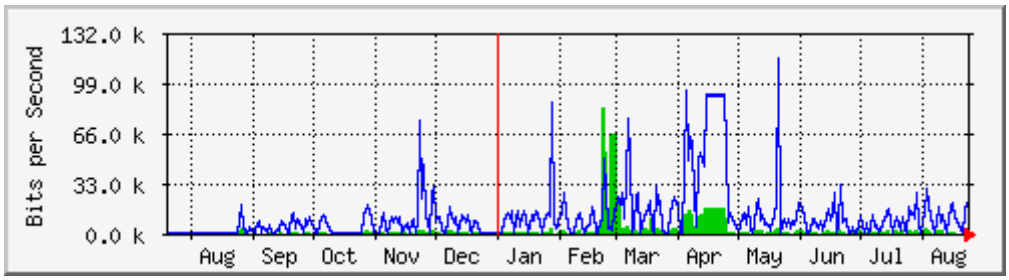
Max In: 29.2 kb/s (22.3%) Average In:1944.0 b/s (1.5%) Current In:936.0 b/s (0.7%)
Max Out:124.2 kb/s (94.7%) Average Out: 12.7 kb/s (9.7%) Current Out:736.0 b/s (0.6%)

Figura III.9: Tráfico semanal entre sedes Sangolquí y Héroes del Cenepa



Max In: 20.9 kb/s (15.9%) Average In:1992.0 b/s (1.5%) Current In:3288.0 b/s (2.5%)
Max Out:180.7 kb/s (137.9%) Average Out: 11.7 kb/s (8.9%) Current Out:20.8 kb/s (15.9%)

Figura III.10: Tráfico mensual entre sedes Sangolquí y Héroes del Cenepa

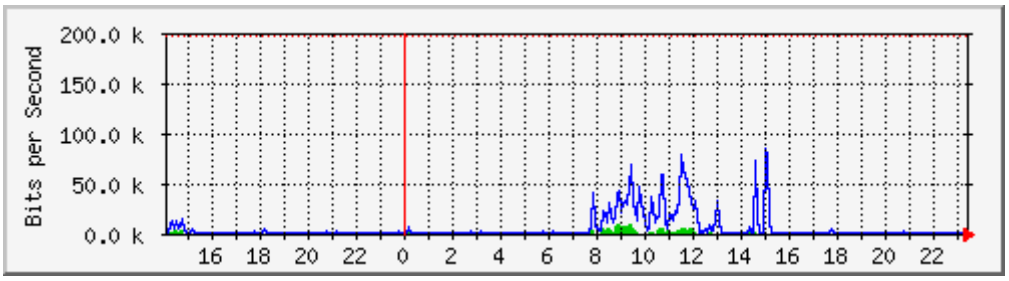


Max In: 83.4 kb/s (63.6%) Average In:3080.0 b/s (2.3%) Current In:4040.0 b/s (3.1%)
Max Out:115.4 kb/s (88.1%) Average Out: 12.9 kb/s (9.9%) Current Out:20.4 kb/s (15.5%)

Figura III.11: Tráfico anual entre sedes Sangolquí y Héroes del Cenepa

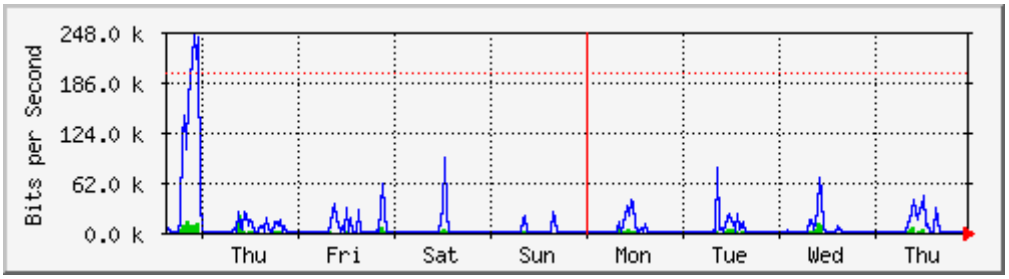
3.1.6- Análisis del tráfico de la red entre sede Sangolquí y sede IASA I

Los datos presentados a continuación están basados en que la velocidad máxima de recepción y transmisión de datos es igual a 192 Kbps.



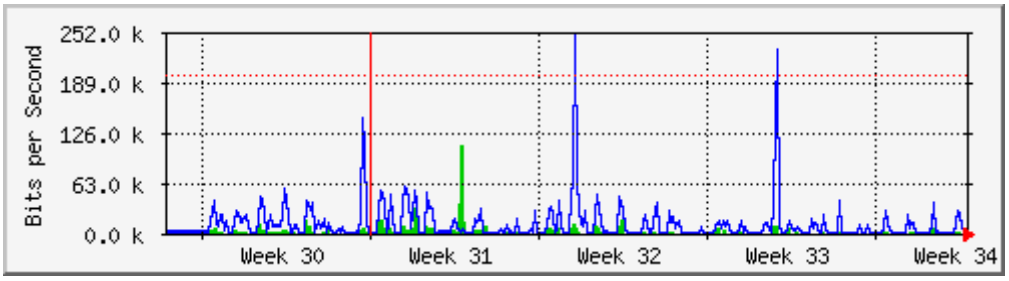
Max In: 10.7 kb/s (5.5%) Average In:1040.0 b/s (0.5%) Current In:216.0 b/s (0.1%)
Max Out:85.7 kb/s (43.6%) Average Out:5432.0 b/s (2.8%) Current Out:240.0 b/s (0.1%)

Figura III.12: Tráfico diario entre sedes Sangolquí e IASA I



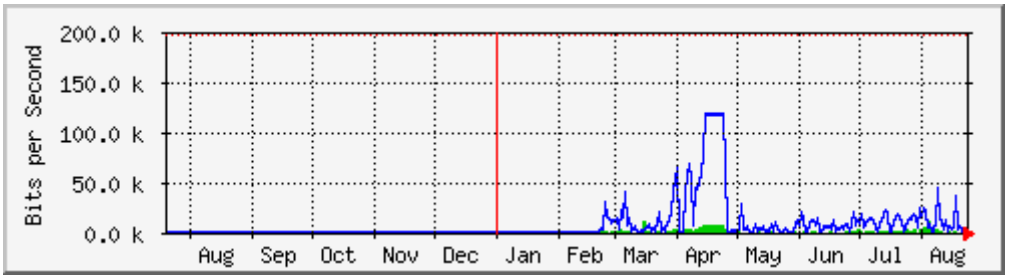
Max In:22.8 kb/s (11.6%) Average In:1232.0 b/s (0.6%) Current In:224.0 b/s (0.1%)
Max Out:247.0 kb/s (125.6%) Average Out:9136.0 b/s (4.6%) Current Out:344.0 b/s (0.2%)

Figura III.13: Tráfico semanal entre sedes Sangolquí e IASA I



Max In: 111.5 kb/s (56.7%) Average In:2856.0 b/s (1.5%) Current In:216.0 b/s (0.1%)
Max Out:251.3 kb/s (127.8%) Average Out: 11.7 kb/s (6.0%) Current Out:456.0 b/s (0.2%)

Figura III.14: Tráfico mensual entre sedes Sangolquí e IASA I



Max In: 12.9 kb/s (6.6%) Average In:1280.0 b/s (0.7%) Current In:1264.0 b/s (0.6%)
Max Out:118.8 kb/s (60.4%) Average Out:9304.0 b/s (4.7%) Current Out:5056.0 b/s (2.6%)

Figura III.15: Tráfico anual entre sedes Sangolquí e IASA I

3.1.7- Requerimientos de servicios proyectados

La ESPE para mantenerse en la vanguardia de la tecnología y brindar a sus estudiantes servicios de calidad, debe proyectar la utilización y entrega de servicios tales como: VoIP y video conferencias (educación virtual). En la actualidad, por los enlaces que tiene con sus sedes, sería imposible implementarlos. A continuación se presentan los requerimientos de red para cada tipo de aplicación.

3.1.7.1- Requerimientos de VoIP

En la actualidad la utilización de este servicio está incrementando notablemente, la reducción de costos para los usuarios es significativa. Instituciones como la ESPE, donde el número de personal administrativo y la necesidad de realizar interconexiones telefónicas entre sedes es extenso, requieren que este servicio sea implementado dentro de sus instalaciones. De acuerdo a la planificación de la ESPE se prevee que en el 2006 se tengan 100 usuarios con VoIP y que el servicio vaya aumentando, por lo que es importante determinar el ancho de banda que utiliza.

Tabla III.1: Ancho de banda requerido para VoIP según los codecs

VoIP Codecs	Ancho de Banda (BW)
G.723.1 CELP	6.3 / 5.3 kbps
G.729 CS-ACELP	8 kbps
G.728 LD-CELP	16 kbps
G.726 ADPCM	16, 24, 32, 40 kbps
G.727 E-ADPCM	16, 24, 32, 40 kbps
G.711 PCM	64 kbps

Teóricamente si se quiere una línea de salida utilizando uno de los codec de alta calidad, que sería el G.711 se necesita un canal de 64Kbps para la llamada, ahora, si se tienen 10 comunicaciones simultaneas, se necesitaría un ancho de banda aproximado de 640 Kbps. La ESPE en la actualidad no podría soportar este servicio. Con WiMAX la conexión que se podría dar en el peor de los casos a 11 Mbps entre las sedes la utilización de 10 canales de comunicación con VoIP no sería un inconveniente y sería soportado por el ancho de banda que brinda esta tecnología.

3.1.7.2- Video conferencia (educación virtual)

Muchas universidades en el mundo han optado por implementar en sus servicios, aulas virtuales donde se pueden recibir cátedras de mucho interés desde distintas ubicaciones, en el caso de la ESPE, muchas veces se realizan congresos, charlas o conferencias en el campus Sangolquí y se excluye de estos beneficios a las otras sedes. Por ejemplo, si en el aula magna se dicta una conferencia que se esta transmitiendo a las otras sedes, el nivel educativo de la Institución crecería notablemente y los conocimientos adquiridos por los alumnos también. El gran inconveniente es tener la infraestructura que soporte estos servicios, actualmente las conexiones DSL con las que cuentan las sedes no permitirían implementar este sistema.

El ancho de banda en la videoconferencia es algo crítico porque se necesita estar seguro del envío y recepción de los datos. Para los enlaces ISDN el ancho de banda necesario puede oscilar entre 128 Kbps y 384 Kbps para cada aplicación sobre IP, mas un 20% correspondiente al control de datos y sesión.

Para video conferencias de alta calidad, como se brindan en Internet 2, se puede hablar de un rango de 2 Mbps a 3 Mbps, y para usos especializados donde la calidad de video es de televisión se requiere de 10 Mbps a 20 Mbps de ancho de banda por sitio.

3.1.8- Proyecciones del uso de red entre sedes

La proyección real a tomar en cuenta son los servicios que se deben brindar como una Institución de Educación Superior, por lo tanto la propuesta y el análisis se enfoca que en 3 años la ESPE debe contar con servicios tales como:

VoIP, educación virtual, aplicaciones distribuidas, sistemas interconectados en tiempo real, sistemas cero papeles entre las sedes, etc.

Los anchos de banda requeridos para cada sede están basados en los servicios proyectados que se presentaron en el capitulo 3.1.7; el número simultáneo de conexiones de acuerdo la cantidad de usuarios de los distintos servicios y la probabilidad que se presenten simultáneamente.

Cuadro III.1: Tasa de transferencia proyectada para Héroes del Cenepa

SERVICIO	**# CONEXIONES SIMULTANEAS**	**AB/CONEXION (Kbps)**	**AB TOTAL (Kbps)**	**AB TOTAL (Mbps)**
VoIP	8	128	1024	1.00
Videoconferencia	4	3072	12288	12.00
Internet	100	16	1600	1.56
Sistemas de información	25	8	200	0.20
TOTAL		**3224**	**15112**	**14.76**

Cuadro III.2: Tasa de transferencia proyectada para Idiomas

SERVICIO	# CONEXIONES SIMULTANEAS	AB/CONEXION (Kbps)	AB TOTAL (Kbps)	AB TOTAL (Mbps)
VoIP	6	128	768	0.75
Videoconferencia	3	3072	9216	9.00
Internet	70	16	1120	1.09
Sistemas de información	20	8	160	0.16
TOTAL		**3224**	**11264**	**11.00**

Cuadro III.3: Tasa de transferencia proyectada para IASA I

SERVICIO	# CONEXIONES SIMULTANEAS	AB/CONEXION (Kbps)	AB TOTAL (Kbps)	AB TOTAL (Mbps)
VoIP	6	128	768	0.75
Videoconferencia	3	3072	9216	9.00
Internet	70	16	1120	1.09
Sistemas de información	15	8	120	0.12
TOTAL		**3224**	**11224**	**10.96**

3.1.8.1- Análisis de proyecciones

De acuerdo al análisis realizado en el ítem anterior se determina que en la infraestructura actual de la ESPE no permite la implementación de nuevos

servicios, por lo que debe adoptar otro tipo de tecnología para la interconexión de sedes. Una de las alternativas más apropiadas es la implementación de una red WiMAX por su cobertura, tasa de transferencia y QoS, entre otras bondades que ésta provee, comparada con otras tecnologías inalámbricas existentes en la actualidad.

3.2- Levantamiento de requerimientos de la Institución

3.2.1- Calculo del tamaño de la muestra para las encuestas [1]

Una fórmula muy extendida que orienta sobre el cálculo del tamaño de la muestra para datos globales es la siguiente:

$$n = \frac{k^2 \times p \times q \times N}{e^2 \times (N-1) + k^2 \times p \times q}$$

Donde:

N: es el tamaño de la población o universo (número total de posibles encuestados).

k: es una constante que depende del nivel de confianza que se asigne. El nivel de confianza indica la probabilidad de que los resultados de la investigación sean ciertos: un 95,5 % de confianza es lo mismo que decir que se puede equivocar con una probabilidad del 4,5%.

Los valores k más utilizados y sus niveles de confianza son:

k	1.15	1.28	1.44	1,65	1,96	2	2,58

[1] FEEDBACK NETWORKS TECHNOLOGIES, Errores frecuentes en las encuestas: ¿Cómo calcular la muestra correcta?, http://www.feedbacknetworks.com/cas/experiencia/sol-preguntar-calcular.htm, 2005

Nivel de confianza 75% 80% 85% 90% 95% 95,5% 99%

e: es el error muestral deseado. El error muestral es la diferencia que puede haber entre el resultado que se obtiene preguntando a una muestra de la población y el que se obtendría si se preguntase al total de ella.

p: es la proporción de individuos que poseen en la población la característica de estudio. Este dato es generalmente desconocido y se suele suponer que p=q=0.5 que es la opción más segura.

q: es la proporción de individuos que no poseen esa característica, es decir, es 1-p.

$$n = \frac{k^2 \times p \times q \times N}{e^2 \times (N-1) + k^2 \times p \times q}$$

n: es el tamaño de la muestra (número de encuestas que se deben hacer).

Así, para nuestro caso, la ecuación queda con los siguientes valores:

k = 1,15 siendo un tema nuevo el conocimiento a profundidad es bajo.

p = 75% basándose en pre-encuestas, es la cantidad de personas que conocen el tema.

q = basándose en pre-encuestas, es la cantidad de personas que no conocen el tema.

N = 7000 es el número de usuarios potenciales para el sistema a implementarse.

e = 5% como estándar para temas de investigación.

Dados estos valores se tiene:

$$n = \frac{1.15^2 \times 75 \times 25 \times 7000}{0.05^2 \times (7000-1) + 1.15^2 \times 75 \times 25}$$

Y el valor de n es: 97,8154635 por lo tanto se deben realizar 98 encuestas.

3.2.2- Encuesta orientada a usuarios de la Red de la ESPE

Al realizar una encuesta a los usuarios se obtienen datos cuantitativos para conocer: la conformidad, utilidad y nuevos requerimientos que tiene la infraestructura y servicios que brinda la ESPE en su red informática.

3.2.2.1- Objetivos

- Conocer la apreciación de los usuarios sobre la situación actual de la red de la ESPE.
- Determinar la utilización de tecnología inalámbrica.
- Evaluar el conocimiento del usuario acerca de la tecnología WiMAX.
- Analizar el criterio de los usuarios sobre la implementación de tecnología inalámbrica para la optimización de la red de la ESPE.

3.2.2.2- Enfoque y tipo de encuesta

Esta encuesta esta enfocada a la obtención de datos cuantitativos del concepto que tienen los usuarios acerca de los servicios de la red informática de la ESPE y así realizar el estudio óptimo para la utilización de tecnología WiMAX.

Para el cumplimiento de esto se realizarán preguntas cerradas a fin de conseguir datos concretos.

3.2.2.3- Calendario y alcance de la encuesta

Se realizará a todo el departamento de Redes perteneciente a Organización y Sistemas de la ESPE, profesores y alumnos de la facultad de Ingeniería en Sistemas y usuarios del Internet en la biblioteca y laboratorios especializados.

El proceso de encuesta se realizó el día jueves 13 de octubre de 2005.

3.2.2.4- Formato de la encuesta

El formato de la encuesta se encuentra detallado en el Anexo A.

3.2.2.5- Resultados de la encuesta

- **Pregunta 1**

  ¿Ha utilizado usted la red de la ESPE?

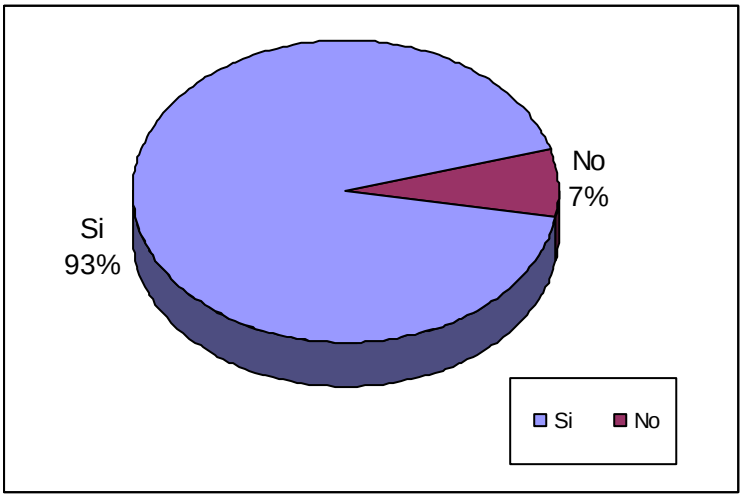


Figura III.16: Resultados pregunta 1

- **Pregunta 2**

  ¿Que servicios de la red de la ESPE ha utilizado?

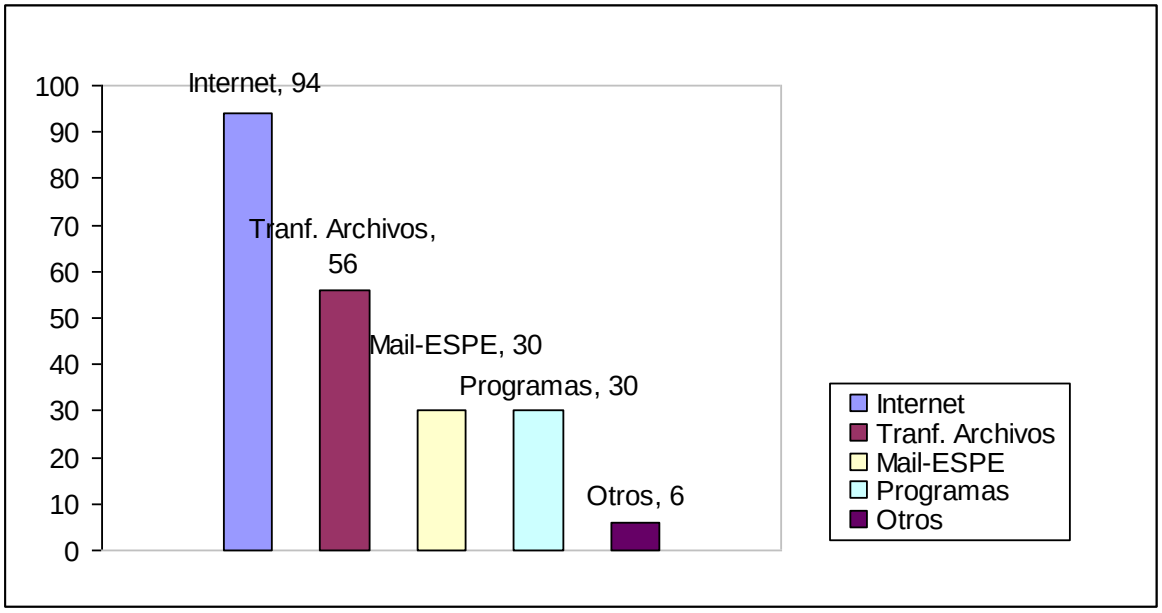


Figura III.17: Resultados pregunta 2

- **Pregunta 3**

  ¿Cómo considera usted el funcionamiento de la red informática interna de la ESPE?

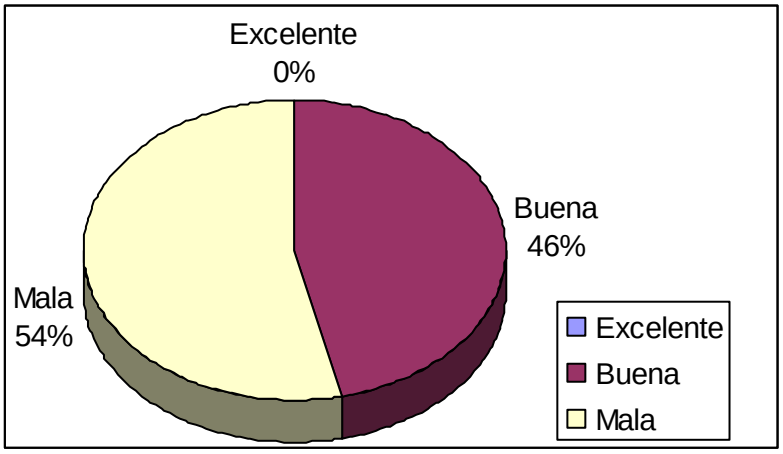


Figura III.18: Resultados pregunta 3

- **Pregunta 4**

  ¿Ha tenido acceso a la red inalámbrica de la ESPE?, en el caso de ser no marque uno de los motivos.

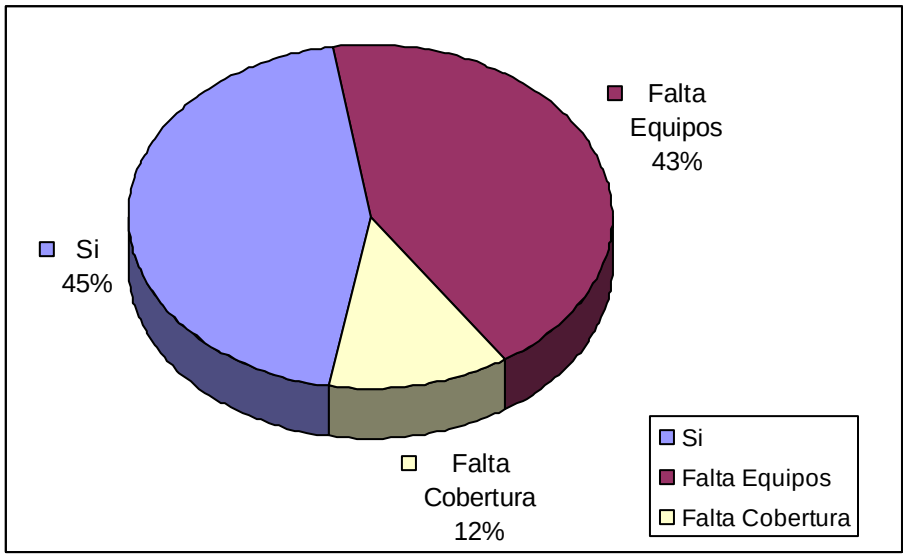


Figura III.19: Resultados pregunta 4

- **Pregunta 5**

  La cobertura de la red inalámbrica de la ESPE es:

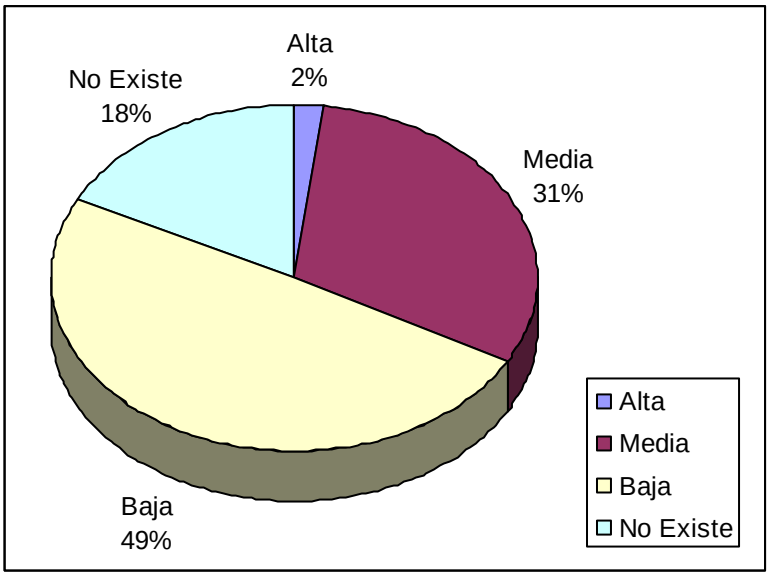


Figura III.20: Resultados pregunta 5

- **Pregunta 6**

  ¿Cuál de estos servicios considera usted que la ESPE debería brindar a los usuarios de su red informática?

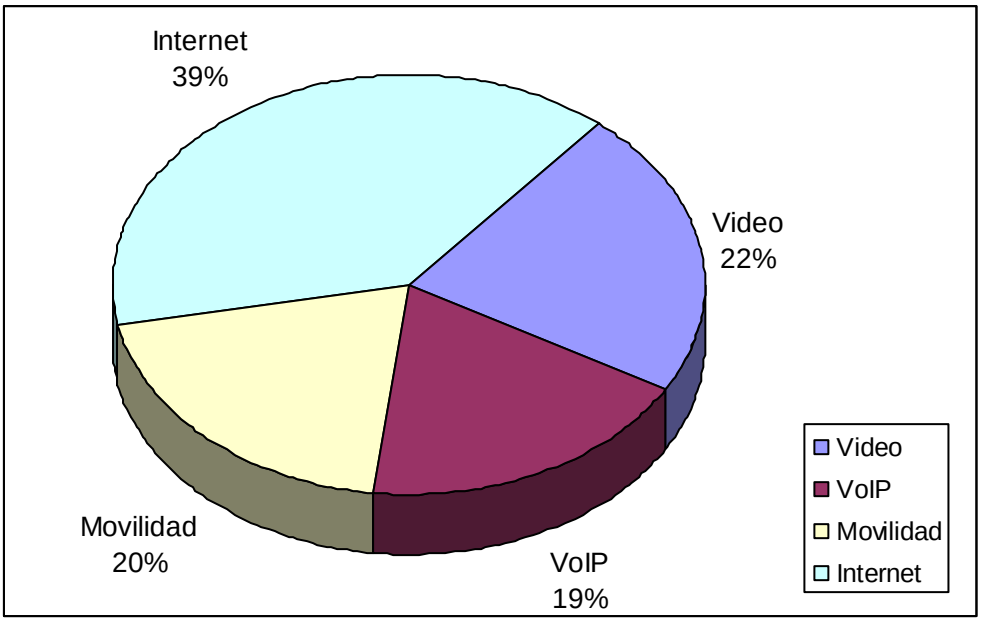


Figura III.21: Resultados pregunta 6

- **Pregunta 7**

  ¿Sabia que Tecnología WiMAX es tecnología inalámbrica de alta velocidad con gran ancho de banda para largas distancias?

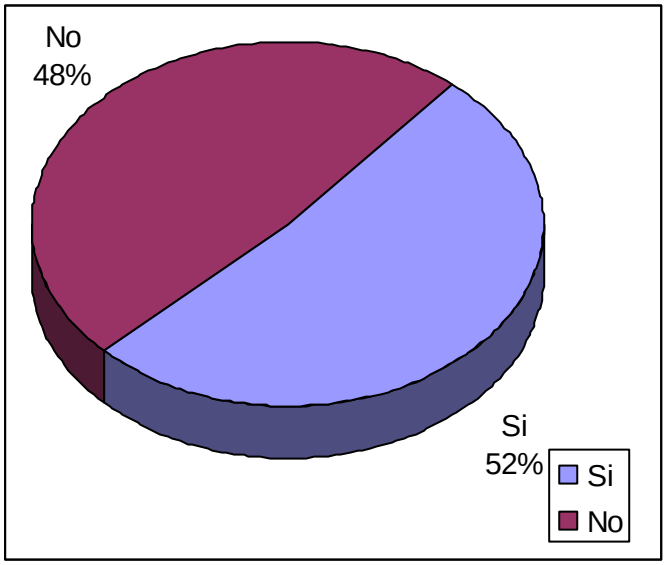


Figura III.22: Resultados pregunta 7

- **Pregunta 8**

  ¿Que uso le daría a una red WiMAX?

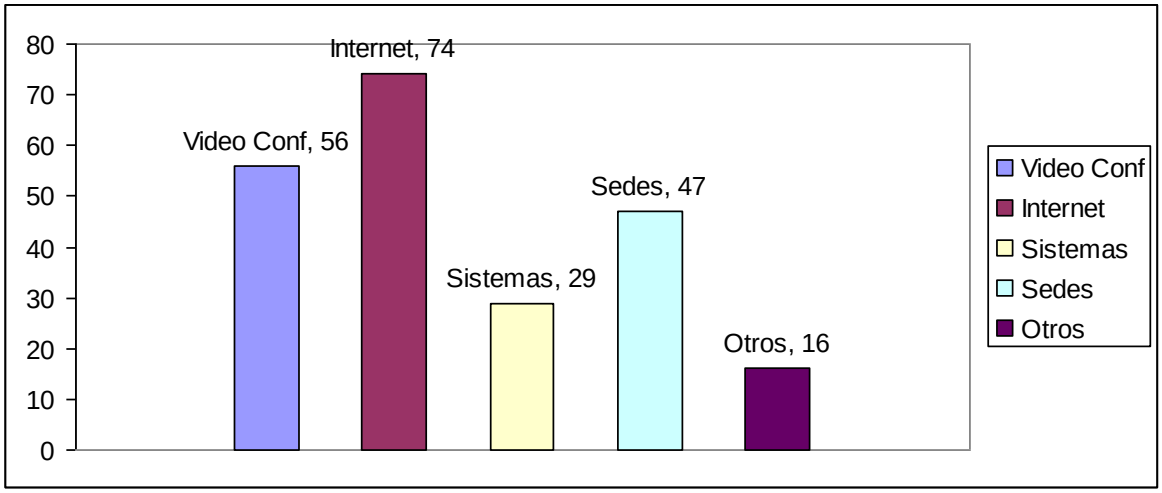


Figura III.23: Resultados pregunta 8

3.2.2.6- Análisis de los resultados obtenidos

A continuación se presenta el cumplimiento de los objetivos haciendo el análisis de cada uno de los resultados obtenidos de las preguntas.

- **Situación actual de la red de la ESPE**

Con la pregunta 1 (figura 3.18) y 2 (figura 3.19) se puede observar que el porcentaje de personas que utilizan la red de la ESPE es del 93%, quiere decir que el conocimiento del funcionamiento de la red es bastante aceptable, también soportados por las respuestas de la pregunta dos donde se ve claramente que la utilización del Internet y transferencia de archivos son los usos principales dentro de la red.

Se debe tomar en cuenta que la utilización del Internet es la base para ampliar el conocimiento, y si los usuarios no tienen satisfacción en su fuente de información principal no generan buenos resultados.

Con estas dos premisas de las preguntas anteriores, se puede medir el grado de conformidad que tienen los estudiantes en la pregunta 3.

En la pregunta 3 (figura 3.20) se muestra la realidad de la situación actual para el estudiantado. Es difícil asimilar que en una universidad de prestigio como la ESPE, el rango de “excelente” para categorizar a su red tenga un 0% y el mayor sea un 54% correspondiente a “mala”.

Ahora, se debe analizar lo siguiente: si en el campus Sangolquí donde se tiene mayor ancho de banda para los alumnos existe inconformidad, ¿cómo debe ser en las sedes?

- **Utilización de tecnología inalámbrica**

En la pregunta 4 (figura 3.21) se analiza que porcentaje de personas utilizan actualmente medios inalámbricos para ingresar a la red, el 45% de los encuestados dicen que si han utilizado la infraestructura inalámbrica, lo importante es que el 55% no ha utilizado ya sea por falta de equipos un 43% y falta de cobertura el 12%. Esto demuestra que en si la infraestructura de la red inalámbrica no cumple con los requerimientos y expectativas de los usuarios. Si se analiza que principalmente se habla de falta de equipos, quiere decir que la inversión de la ESPE para que la tecnología inalámbrica sea adoptada por el alumnado no ha sido alta.

Con la pregunta 5 (figura 3.22) se puede apreciar que las personas que han utilizado o que conocen la red inalámbrica de la ESPE, consideran que la cobertura para cumplir sus necesidades es “baja” con el 48%, “media” 31%, “no existe” el 18%, que ratifica los datos de la pregunta 4 y lo más crítico, que el sólo el 2% considera que la cobertura es alta.

En la ESPE, se debe tomar en cuenta que al tener un área extensa de estudio es muy importante tener cobertura total, así, el alumnado tiene la

capacidad de discernir información en el momento que la requiera sin necesidad de acceder a un aula o laboratorio especializado.

- **Conocimiento de WiMAX**

En la pregunta 7 (figura 3.24) se puede observar que el 52% de los encuestados conocen sobre la tecnología. Entonces, la mitad de los usuarios de la red de la ESPE conocen de tecnologías de punta, capaz de mejorar la calidad de servicio que tienen al momento y que al adoptar esta tecnología no generaría rechazo.

- **Criterios para la optimización**

Las preguntas 6 (figura 3.23) y 8 (figura 3.25) son orientadas a la optimización de la red de la ESPE, ya que servicios como: VoIP, video conferencias (educación virtual), sistemas educativos, movilidad y enlace entre sedes; no se encuentran en la actualidad funcionando por falta de soporte de tecnología y optimización de la red actual.

3.2.2.7- Conclusiones generales de la encuesta

Es fácil observar el grado de disconformidad por parte de los usuarios con respecto a la situación actual de la red de la ESPE.

La ESPE debe procurar llegar al grado de la excelencia en el servicio que brinda a sus alumnos (su principal cliente), adoptando tecnología capaz de soportar servicios que respalden el nivel de enseñanza que la Institución brinda actualmente.

Es claro que los usuarios desean llegar a disponer de video conferencias, Internet de alta velocidad, VoIP y sistemas educativos.

Estos servicios con la tecnología que actualmente la ESPE maneja entre sedes es imposible de brindar, por esto, se encuentra justificada la implementación de tecnología WiMAX que nos permitirá brindar estos y otros servicios entre sedes.

3.2.3- Entrevista enfocada a la alta gerencia y mandos medios de la ESPE

Al realizar una entrevista se tiene un panorama claro sobre el pensamiento de la innovación de tecnologías dentro de la ESPE, así como la situación actual, tomando en cuenta los principales involucrados en el área administrativa de la red y altos mandos que toman las decisiones para la implantación de tecnologías.

3.2.3.1- Objetivos

- Conocer el grado de conformidad del funcionamiento operativo de la red interna de la ESPE.
- Conocer la capacidad de inversión para implementar nueva tecnología que optimice la conectividad de la ESPE.
- Determinar cuál es la visión a futuro respecto a tecnologías de interconectividad a implementar en la ESPE.
- Analizar la escalabilidad de la infraestructura de la red de la ESPE para próximas innovaciones.
- Determinar el nivel de conocimiento acerca de la tecnología WiMAX en el área administrativa de redes de la ESPE.

3.2.3.2- Enfoque y tipo de entrevista

Al tabular la entrevista se pretende: obtener datos cualitativos de manera que justifique la implementación de la tecnología WiMAX y conocer los conceptos que maneja el personal que administra la situación actual de la red de la ESPE. Para esto se debe tomar en cuenta una entrevista de tipo abierta para adquirir distintos conceptos, luego agruparlos a fin de tener una imagen general y lograr una conclusión clara.

3.2.3.3- Calendario de la entrevista

Se realizó a todo el departamento de Redes perteneciente a Organización y Sistemas de la ESPE, profesores del área de telecomunicaciones de la facultad de Ingeniería en Sistemas de la ESPE, Rectorado, Vicerrectorado Académico, Financiero y Administrativo de la ESPE.

El proceso de entrevista se realizó el día 13 de julio de 2005

3.2.3.4- Preguntas hacia los entrevistados

1. Nombre del entrevistado, cargo y departamento.
2. ¿Considera que el servicio de la red de datos de la ESPE es bueno, malo o excelente? ¿Por qué?
3. ¿Qué servicios debería ofrecer la red de datos de la ESPE?
4. ¿Qué presupuesto está destinado al área de redes de la ESPE para inversión en tecnología?
5. ¿Cuál es su visión de la red informática de la ESPE en los próximos dos años?
6. ¿Cuál es la importancia que tiene una red de datos inalámbricos en la ESPE?

7. ¿Sabia que la tecnología inalámbrica WiMAX implementa alta velocidad con gran ancho de banda para largas distancias?
8. ¿Qué uso le daría en la ESPE a la tecnología WiMAX?
9. ¿Considera usted que la ESPE se encuentra a la vanguardia de la tecnología en el área de comunicaciones?

3.2.3.5- Resultados de las entrevistas

Las entrevistas se realizaron a responsables del área de redes de distintas dependencias de la ESPE como son los laboratorios especializados, el área de redes y telecomunicaciones del departamento de Organización y Sistemas, la Facultad de Sistemas entre otros.

A continuación se lista las personas entrevistadas:

NOMBRE	CARGO	DEPENDENCIA
Ing. Walter Fuertes	Subdecano	Facultad de Sistemas
Ing. Lourdes De La Cruz	Planificadora	Facultad de Sistemas
Ing. Fausto Granda	Administración de Telecomunicaciones	Organización y Sistemas
Ing. Darwin Aguilar	Coordinador de redes	Organización y Sistemas
Sr. Ramiro Pulgar	Administrador de Seguridades	Organización y Sistemas
Sr. Luis Buri	Laboratorista	Laboratorios de Computación

Luego de realizadas las entrevistas, las cuales están anexadas como archivo digital a la presente tesis, se concluye lo siguiente:

- Existe el presupuesto suficiente para implementar este proyecto en un futuro cercano, ya que la ESPE dispone de una asignación destacable de dinero para redes y telecomunicaciones.

- Las autoridades tienen total disposición para implementar un proyecto de este tipo, ya que incrementará sustancialmente la calidad y los servicios que se brinden a las sedes.
- Se tiene claro que esta red se puede aprovechar para los propósitos mencionados en las encuestas como son las videoconferencias y VoIP.
- La ESPE tiene como uno de sus objetivos principales invertir en todo momento en tecnología de punta, como es el caso del presente proyecto.
- Existen algunos problemas en la red actual de la ESPE, principalmente Internet, el cual es muy lento y mal administrado hacia las sedes y los puntos de acceso inalámbricos, que son escasos y de poca cobertura.
- En cuanto a puntos de red, la ESPE posee una infraestructura que rebasa los requerimientos, teniendo así al menos un punto de red por cada persona que la integra, lo cual la coloca en una posición élite.

CAPITULO IV: Diseño de la Red

4.1- Requerimientos técnicos de la ESPE

Luego de analizar las encuestas y entrevistas, se llega a la conclusión de que la ESPE en la actualidad no posee una infraestructura adecuada para realizar el crecimiento tecnológico que desea dar.

Por un lado, el alto costo mensual de los enlaces actuales y por otro el insignificante ancho de banda que éstos brindan, imposibilitan totalmente la implementación de las nuevas tecnologías requeridas.

Se puede resumir que las necesidades esenciales de la ESPE, según los resultados anteriores son:

- Aumento del rendimiento y nivel académico de los alumnos mediante la educación virtual basada en videoconferencias entre sedes.
- Reducción de costos de líneas telefónicas mediante la implementación de voz sobre IP (VoIP).
- Optimizar el funcionamiento del Internet en general.

Los requerimientos técnicos para implementar estas tecnologías, como se explica en el Capítulo II, son básicamente una tasa de transferencia alta y diferenciación de servicios (ToS). Por lo tanto, la solución mediante la tecnología WiMAX es la más adecuada para la implementación de los servicios requeridos por la Institución.

4.2- Configuraciones

Tomando en cuenta los costos y el óptimo funcionamiento de la red, se presentan dos configuraciones.

La primera optimiza el factor costo, llevando este rubro al mínimo valor a cambio de una posible “inestabilidad” por la reducción del ancho de banda en comparación a la segunda configuración, la cual, contraria a la anterior, valora principalmente la conectividad por un precio más alto.

4.2.1- Primera configuración

En esta configuración se optimiza la cantidad de equipos mediante una topología punto-multipunto en la torre de repetición ubicada en la loma de Puengasí.

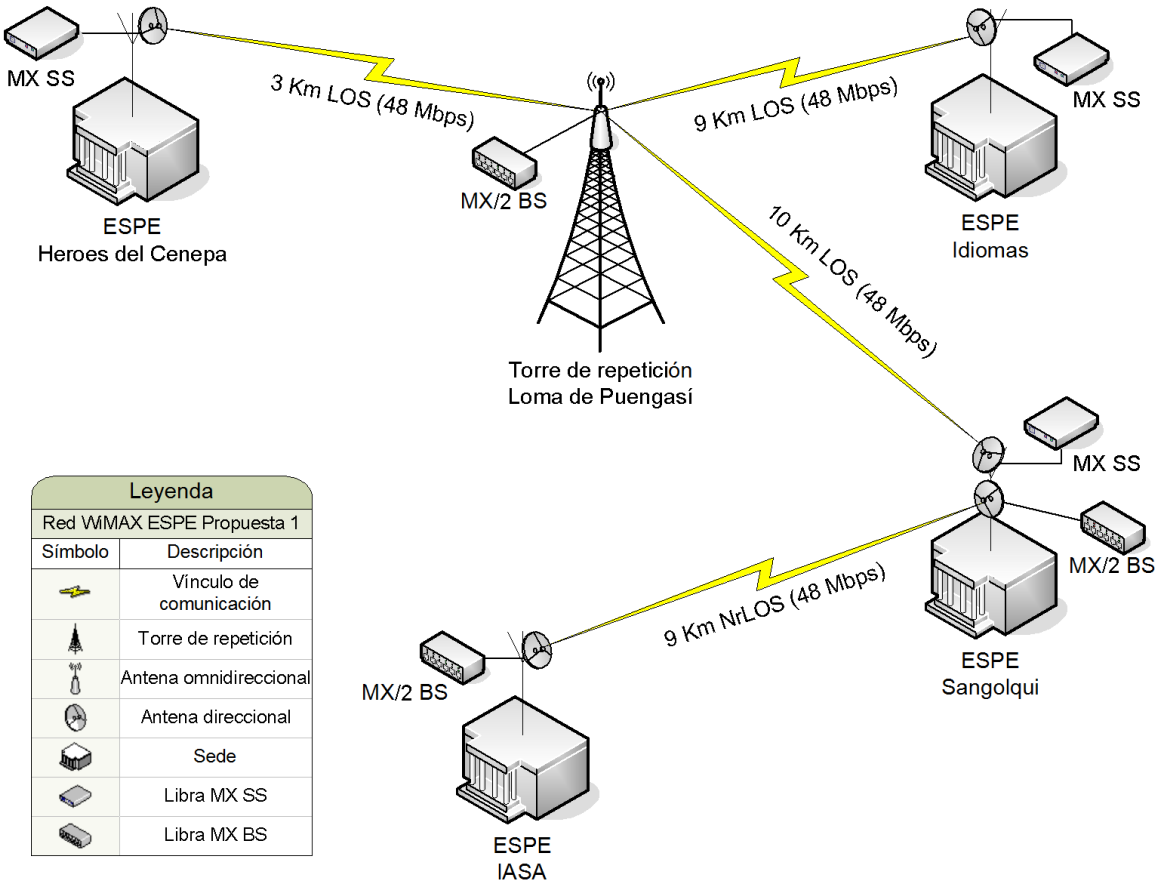


Figura IV.1: Diagrama de red primera configuración

4.2.1.1- Ventajas

La gran ventaja de esta configuración es su costo, ya que con un solo equipo y una sola antena en la loma de Puengasí se resuelve el problema de la repetición desde Quito hacia Sangolquí.

4.2.1.2- Desventajas

Genera tres inconvenientes:

- Problemas de seguridad, ya que en topología punto-multipunto es más fácil el acceso como suscriptor, ya que el equipo esta preparado para aceptar conexiones entrantes como un punto de acceso inalámbrico, lo que no sucede en la configuración punto-punto.
- Genera una reducción del ancho de banda, ya que si las dos Sedes Idiomas y Héroes del Cenepa están transmitiendo a toda su capacidad hacia Sangolquí, esto es a 48 Mbps, se genera un cuello de botella, ya que este último enlace es de 48 Mbps y no de 96 Mbps que sería lo adecuado para que no exista un congestionamiento de red, como se explica en la figura 4.2

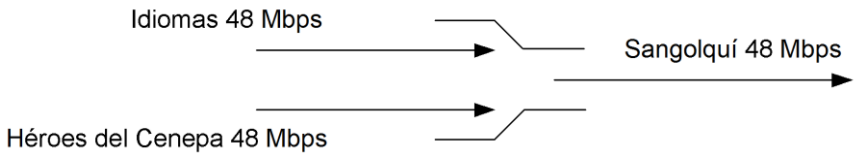


Figura IV.2: Cuello de botella que se genera en la primera configuración

- Falta de redundancia, ya que si existe algún fallo en un equipo principal, podría ocasionar que toda la red colapse.

4.2.1.3- Costo

El costo aproximado de esta configuración, limitándose a lo que equipos se refiere, se detalla en el cuadro 4.1

Cuadro IV.1: Valor estimado primera configuración

DESCRIPCION	CANT.	PRECIO UNITARIO	PRECIO TOTAL
Libra MX Suscriber Station	3	$ 1 532.97	$ 4 598.91
Libra MX/2 Base Station	3	$ 2 489.19	$ 7 467.57
Tarjetas expansión Libra MX BS	3	$ 924.87	$ 2 774.61
Antena direccional 32 dBi	5	$ 219.99	$ 1 099.95
Antena omnidireccional 15 dBi	1	$ 89.95	$ 89.95
Supresores de rayos para antenas	6	$ 29.99	$ 179.94
	T O T A L:		$ 16 210.93

4.2.2- Segunda configuración

Esta configuración da prioridad a la funcionalidad óptima de la red, tomando en cuenta anchos de banda adecuados y redundancia en algunos de los enlaces, corrigiendo las desventajas presentadas en la configuración anterior a cambio de una inversión más alta.

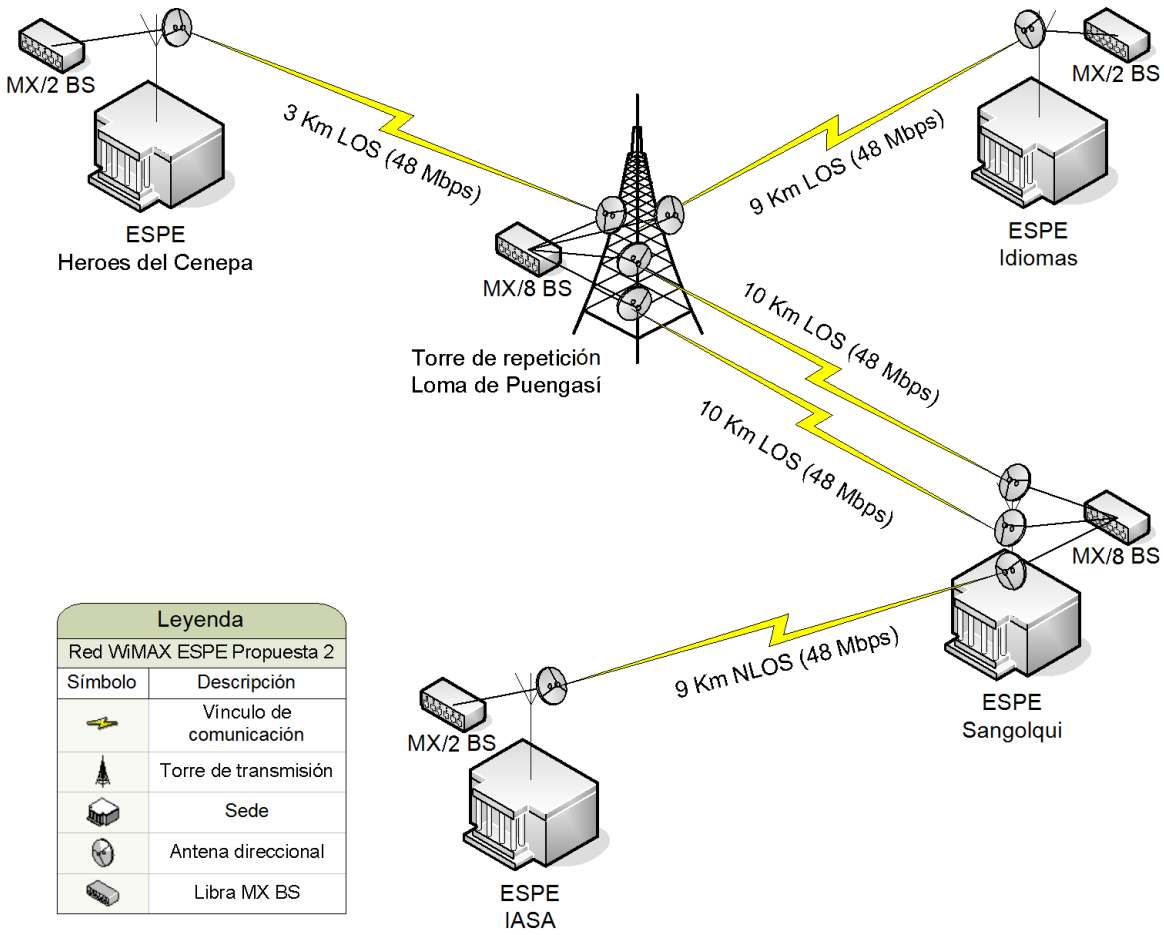


Figura IV.3: Diagrama de red segunda configuración

4.2.2.1- Ventajas

Entre las principales ventajas que este modelo presenta se pueden citar las siguientes:

- Existe redundancia en el enlace hacia Sangolquí, lo que genera un enlace más estable, ya que si uno de ellos falla, el otro puede sustentar la conexión hasta su restablecimiento.
- La redundancia anterior también genera un aumento del ancho del banda, ya que se tienen dos enlaces de 48 Mbps que juntos hacen uno

de 96 Mbps, lo que soluciona el problema del cuello de botella de la configuración anterior.

- En cuanto a seguridad, ésta se incrementa al usar la topología punto-punto, ya que los equipos no están en modo de aceptar conexiones de suscriptores, como si lo están en topología punto-multipunto.

4.2.2.2- Desventajas

La única desventaja presentada en esta configuración es el costo de la inversión, lo cual se recompensa con la funcionalidad óptima de la red.

4.2.2.3- Costo

El costo aproximado de esta configuración, limitándose a lo que equipos se refiere, es el siguiente:

Cuadro IV.2: Valor estimado segunda configuración

DESCRIPCION	CANT.	PRECIO UNITARIO	PRECIO TOTAL
Libra MX/2 Base Station	3	$ 2 489.19	$ 7 467.57
Libra MX/8 Base Station	2	$ 4 867.23	$ 9 734.46
Tarjetas expansión Libra MX BS	10	$ 924.87	$ 9 248.70
Antena direccional 32 dBi	10	$ 219.99	$ 2 199.90
Supresores de rayos para antenas	10	$ 29.99	$ 299.90
	T O T A L:		$ 28 950.53

4.2.3- Análisis de las alternativas y determinación de la mejor opción

Presentadas las características detalladas de cada configuración, se debe adoptar una para implementar en el diseño.

En el cuadro 4.3 se resume y compara ambas opciones resaltando los puntos más relevantes para ser tomados en cuenta.

Cuadro IV.3: Comparación entre propuestas

	Primera Configuración	**Segunda Configuración**
Seguridad	Media	Alta
Ancho de Banda	Bajo	Optimo
Redundancia	No	Si
Costo	Medio	Alto

Como se puede apreciar, el único inconveniente presentado por la segunda opción versus la primera es el costo, el cual, según las entrevistas realizadas a las autoridades respectivas, están dispuestos a asumir a cambio de la funcionalidad óptima que ésta presenta.

Basándose en el análisis anterior, se toma la segunda configuración como la base para el diseño de la red WiMAX para interconectar las sedes aledañas de la ESPE.

4.3- Diseño

4.3.1- Características de diseño

4.3.1.1- Frecuencia de operación

Una parte importante del diseño es la banda en la que trabajarán los equipos de comunicaciones, ya que como se explico con anterioridad, se necesita de licencia para operar en la frecuencia de 3 - 5 GHz en nuestro país.

Luego de una investigación en la SENATEL, organismo Estatal encargado de la administración del espectro de frecuencia en nuestro país, se determinó que la banda de 3 GHz ya está otorgada casi en su totalidad a varias empresas de telecomunicaciones nacionales, por lo tanto, se debe utilizar la banda de 5 GHz que todavía está disponible.

El costo por el uso de la banda de 5 GHz, por cada enlace es aproximadamente de USD 200, en la configuración se tiene 4 enlaces, por lo que da un total de USD 800 anuales; USD 67 mensuales versus los casi USD 4000 mensuales que la ESPE paga por servicio de interconexión de sedes en la actualidad.

4.3.1.2- Calidad de servicio

Los datos que se transmitirán por esta red se basan en calidad de servicio por el tipo de información que se maneja, principalmente: videoconferencia y VoIP, es por esto que todos los equipos involucrados deben soportar este tipo de servicios.

En la sede Sangolquí, se dispone de equipos que soportan en su totalidad calidad de servicio, por lo que en esta sede no habría problema. No así en las otras sedes donde se deben adquirir los equipos necesarios para proveer de calidad de servicio de manera interna.

4.3.2- Equipos WiMAX

En la actualidad las empresas que producen equipos de comunicaciones inalámbricas basados en la tecnología WiMAX son pocas, de las mas conocidas podemos citar dos: AirSpan y Wi-LAN.

Luego de un análisis de disponibilidad y conveniencia de equipos, la empresa Wi-LAN posee los equipos más apropiados para el presente proyecto.

Wi-LAN posee una línea de productos llamados LibraMX que funcionan bajo el estándar WiMAX. Cuentan con tres tipos de equipos, con características generales y técnicas que se detallan a continuación:

- **Libra MX/2 Base Station**

Figura IV.4: Libra MX/2 Base Station

  - Es el equipo más económico.
  - Ideal para un sistema redundante punto-punto, o para sistemas punto-multipunto.
  - Total compatibilidad con equipos MX/8 y MX/16.
  - Con chasis tipo 1U soporta hasta 2 extensiones.
  - Tasa de transferencia de hasta 96 Mbps por cada equipo.

- **Libra MX/8 Base Station**

Figura IV.5: Libra MX/8 Base Station

  - Totalmente escalable, con chasis tipo 4U soporta hasta 6 extensiones.
  - Compatibilidad con equipos MX/2 y MX/16.
  - Posee slots de control, de alarma y redundancia de suministro eléctrico.
  - Tasa de transferencia de hasta 288 Mbps por cada equipo.

- **Libra MX/16 Base Station**

Figura IV.6: Libra MX/16 Base Station

  - Escalabilidad al máximo, con chasis tipo 8U soporta hasta 6 extensiones redundantes (12 extensiones simples).
  - Compatibilidad con equipos MX/2 y MX/8.
  - Posee slots de control, de alarma y redundancia de suministro eléctrico.
  - Tasa de transferencia de hasta 576 Mbps por cada equipo.

Además de estas características generales, todos los equipos poseen las siguientes especificaciones técnicas:

Cuadro IV.4: Especificaciones técnicas de los equipos LibraMX [1]

RADIO SPECIFICATIONS	
Output Power (Antenna Port)	BPSK, QPSK: 26dBm; QAM16: 26dBm, QAM64: 23dBm
Frequency Bands	5.4 - 5.6 GHz initially, future WiMAX bands
PHY Technology	Turbo W-OFDM Sector - Turbo W-OFDM
	WiMAX Sector - WiMAX/802.16-2004 256 FFT
Coverage	NLOS, NrLOS, LOS
Range	Up to 30 km PtMP; Up to 75 km PtP
Modulation Rates	BPSK, QPSK, QAM16, QAM64
Duplexing Format	FDD/TDD, HDX/FDX option
Throughput (Raw/Effective)	Turbo W-OFDM & WiMAX Sectors - 47 / 35 Mbps (QAM64, 7MHz, FDX)
	Turbo W-OFDM Backhaul - 96 / 72 Mbps (QAM64, 14MHz, FDX)
Channel Size	Turbo W-OFDM Sector - 3.5 / 7 MHz
	Turbo W-OFDM Backhaul - 3.5 / 7 / 14 MHz
	WiMAX Sector - 3.5 / 7 MHz
IF Frequency	465 MHz
IF Cable Loss	9 Db
Antenna	Non-integrated Sectoral - 60°, 90°, 120°, 360° (omni)
RF Connector	N Connector
Certification	ETSI, SRRC, SIRIM
NETWORK SUPPORT	
Network Connection	10/100 Base T, for sector blades, Gigabit Ethernet for Ethernet Switch Blade, E1/T1 option, VoIP option
VLAN Compliance	Yes, IEEE 802.1q
CIR/MBR	Yes
Bridge Functionality	Yes
Network Filtering	MAC address, IP address, Ip subnet
QoS Support	Turbo W-OFDM Sector - IP TOS
	WiMAX Sector - IP TOS, Best Effort, Non-Real-Time, Real-Time, Continuous Grant
Topologies	Point-to-Point, Point-to-Multipoint
Number of Subscriber Stations per Sector	2047
SECURITY	
Data Scrambling	Turbo W-OFDM Sector – Proprietary
	WiMAX Sector - DES/AES
Data Security Password	Yes
Configuration Security	Yes

1 Wi-LAN Inc., LibraMX Specifications, http://www.wi-lan.com/products/libramx.htm

MANAGEMENT	
Remote Management	Telnet, SNMP
Remote Access Management	From the wired LAN or from the wireless link
Local Management	Port RS 232 Serial Port
Software Upgrade	Remote upgradable, over the air

4.3.2.1- Tarjetas de expansión

Son la base de los equipos LibraMX, ya que hacia cada una de éstas van conectados antena e interfase de red cableada. De acuerdo a la capacidad del equipo, se puede ir aumentando estas tarjetas para incrementar ancho de banda según la necesidad de la red.

Figura IV.7: Tarjetas de expansión para equipos LibraMX

4.3.2.2- Partes de los equipos

Cada equipo se conforma de las partes mencionadas y dispuestas de acuerdo como se muestra en la figura 4.5, a excepción del LibraMX/2 que no posee redundancia de alimentación eléctrica ni módulo de alarma.

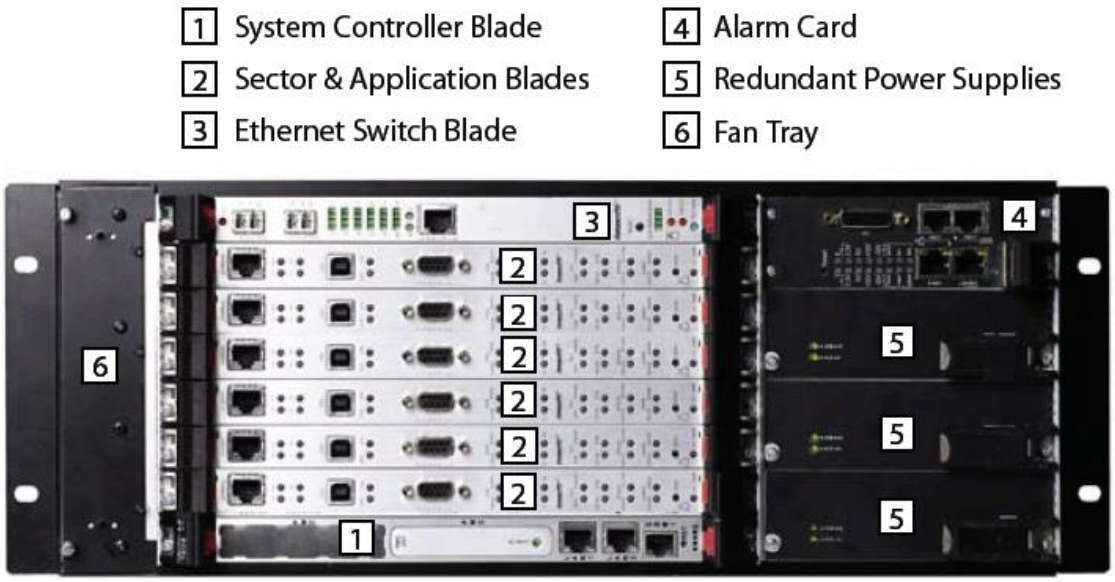


Figura IV.8: Distribución de partes del equipo LibraMX

4.3.2.3- Antenas

Las antenas son de tipo panel, con tecnología inteligente, la cual localiza al cliente y focaliza con mayor potencia la señal hacia el punto donde éste se encuentra. En nuestro caso, por ser la red punto-punto, no existen clientes sino únicamente bases.

Figura IV.9: Antena para equipos LibraMX

4.3.3- Equipos WiFi

D-Link DWL-2100AP [1]

El D-Link DWL-2100AP es un Access Point Inalámbrico potenciado, perteneciente a la línea AirPlus XtremeG de D-Link, que responde al estándar 802.11g, operando con un de ancho de banda 108Mbps, y que gracias al nuevo Chip de Atheros puede alcanzar un througput quince veces superior -15x* exclusivo de D-Link- que una red Wireless tradicional de 11Mbps.

[1] D-LINK LATINAMERICA, Descripción DWL-2100AP, http://www.dlinkla.com/home/productos/descripcion.jsp?id=3&idp=497&sm=4&sf=13, 2004

Figura IV.10: Access Point DWL-2100AP

El DWL-2100AP interopera en forma transparente con cualquier producto D-Link Air, D-Link AirPlus, D-Link AirPlus G+ y D-Link Airpremier AG o con cualquier producto de otros vendedores, bajo el estándar 802.11b y por supuesto con el estándar 802.11g. En conjunto con las altas tasas de transferencia, un muy buen nivel de seguridad, hacen del DWL-2100AP la solución ideal para la nueva tecnología, además de proteger las inversiones wireless ya hechas.

El Access Point AirPlus XtremeG DWL-2100AP incorpora mecanismos adicionales de seguridad, tales como WiFi Protected Access (WPA) y 802.1x, que en conjunto con un servidor Radius proporcionan un mayor nivel de Seguridad.

Cuadro IV.5: Especificaciones técnicas del equipo DWL-2100AP

Estándar	IEEE 802.11g
	IEEE 802.11b
	IEEE 802.3 Ethernet/ IEEE 802.3u FastEthernet
Puerta	1 x RJ-45, 100Base-TX
Seguridad	Encriptación 64/128/152 bits WEP
	802.1x
	WPA

Tasa de Transferencia y Técnicas de Modulación	802.11g : D-Link 108Mbps, 54Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 9Mbps, Auto Fallback
	802.11b : 11 Mbps, 5.5 Mbps, 2 Mbps, 1 Mbps, Auto Fallback
Rango de Cobertura Valores nominales	Hasta 100 mts. In-door
	Hasta 400 mts. Out-door
	Factores del entorno pueden afectar adversamente los rangos de cobertura.
Antena	Externa desmontable con conector RSMA
	Sistema de Antena Giratoria; dipolo con ganancia de 2 dBi
Rango de Frecuencia	2.400 – 2.4835 GHz
Técnicas de Modulación	- 802.11g: BPSK, QPSK, 16QAM, 64QAM, OFDM
	- 802.11b: DQPSK, DBPSK y CCK
Arquitectura de Red	Soporta Modo Estructurado (Comunicaciones de redes alambradas vía Access Point con Roaming)
Modos de Operación	Access Point
	Wireless Bridge
	Point-to-Point
	Point-to-Multipoint
	Client Access Point
	Repeater
Leds de Diagnóstico (Verde)	- WAN
	- LAN (10/100Mbps)
	- WLAN
Método de acceso	CSMA/CA con ACK
Administración	Web Based
	DHCP Cliente/Servidor

4.3.4- Diagrama de red WiMAX

El siguiente diagrama basa su funcionalidad en topología punto-punto con redundancia en cada conexión.

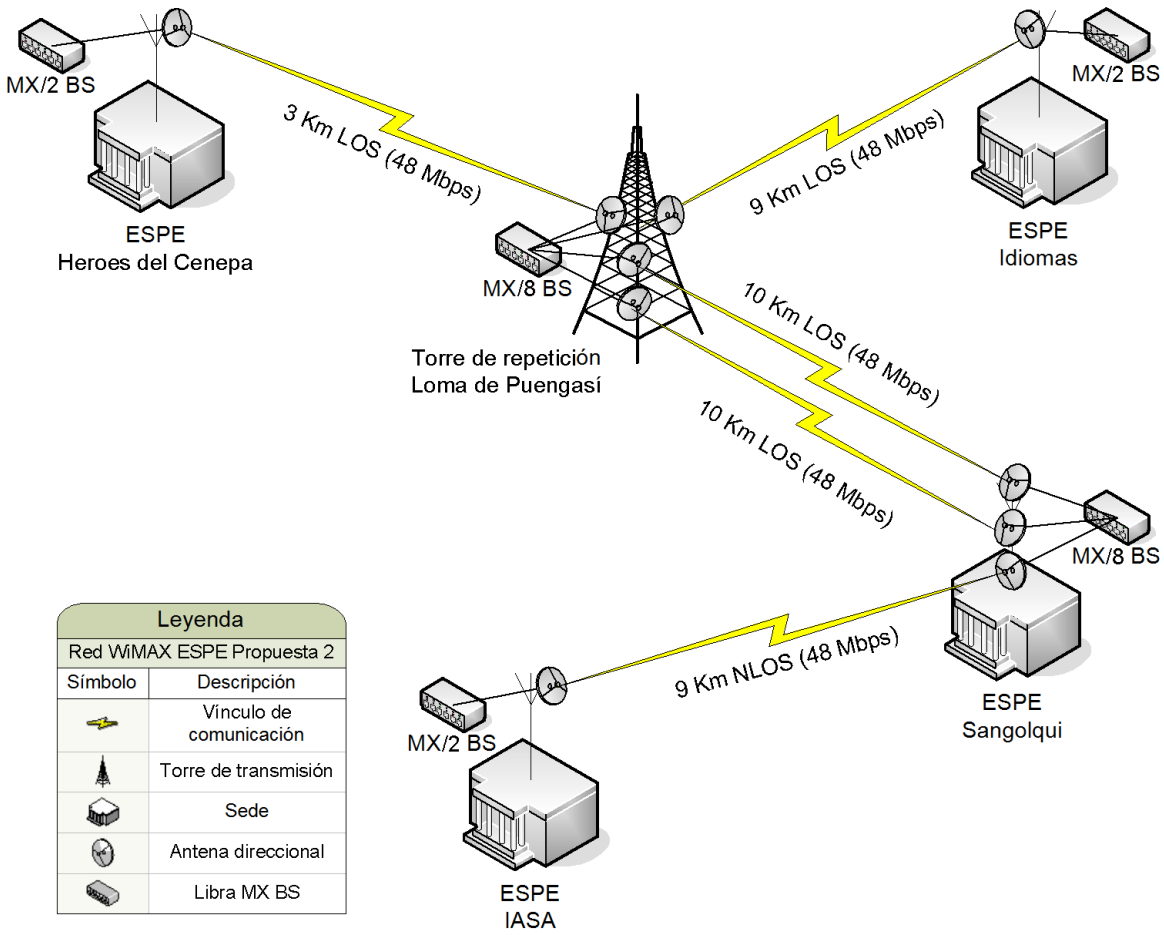


Figura IV.11: Diagrama general del modelo de red WiMAX

4.3.4.1- Descripción del modelo general de red

Este diagrama propuesto es totalmente escalable, pudiendo adicionar módulos de expansión de acuerdo a la necesidad en cualquiera de los equipos mencionados, lo que implementa redundancia y aumenta el ancho de banda.

ESPE Héroes del Cenepa

En esta sede se colocará un equipo LibraMX/2 Base Station con una tarjeta de expansión, la cual se conecta mediante línea de vista hacia la torre de repetición.

ESPE Idiomas

Esta sede posee una configuración muy similar a la anterior, colocando un equipo LibraMX/2 Base Station con una tarjeta de expansión, el cual se conecta mediante línea de vista hacia la torre de repetición.

Torre repetidora

En esta ubicación se coloca un equipo LibraMX/8 Base Station con 4 tarjetas de expansión, las dos primeras se conectan mediante línea de vista hacia las sedes: ESPE Héroes del Cenepa y ESPE Idiomas; las dos últimas se conectan con línea de vista hacia la ESPE Sangolquí, así, se tiene redundancia para aumentar el ancho de banda y por seguridad en caso de fallos.

Una solución para que la ESPE no tenga que incurrir en todos los gastos que implica la construcción de la torre repetidora, es la de alquilar un espacio en una ya existente, ya que en este lugar hay mas de una docena. El costo mensual del alquiler del espacio para una antena y el equipo oscila entre los USD 100.

ESPE Sangolquí

La ESPE Sangolquí debe implementar un equipo LibraMX/8 Base Station con 3 tarjetas de expansión, las dos primeras se conectan hacia la torre de repetición con la redundancia antes mencionada, y la última hacia la sede IASA I.

ESPE IASA I

En IASA I se coloca un equipo LibraMX/2 Base Station con una tarjeta de expansión que se conecta sin con línea de vista casi directa hacia ESPE Sangolquí.

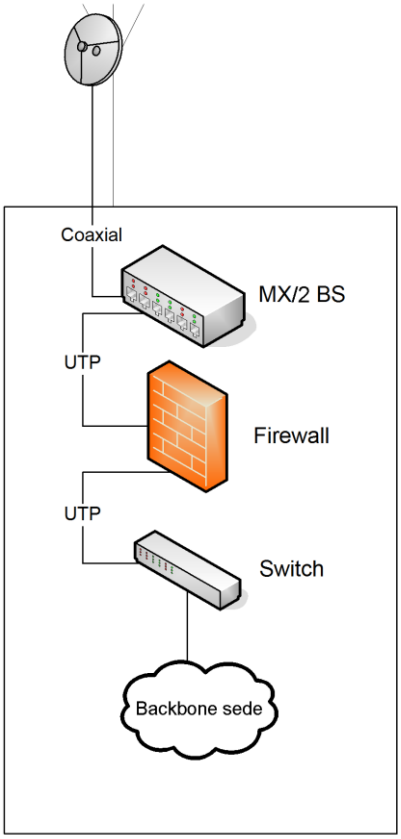


Figura IV.12: Detalle de conexión final para cada sede

4.3.5- Diagrama de red WiFi

Se presenta una alternativa de solución inalámbrica basada en tecnología WiFi para la parte interna de la ESPE por su bajo precio y su popularidad en la actualidad. El siguiente diagrama representa los puntos donde se debe colocar un punto de acceso inalámbrico para cubrir la mayor parte del campus Politécnico de la ESPE Sangolquí, un modelo similar quedaría para cada una de las sedes para implementar puntos de acceso inalámbricos para los clientes finales.

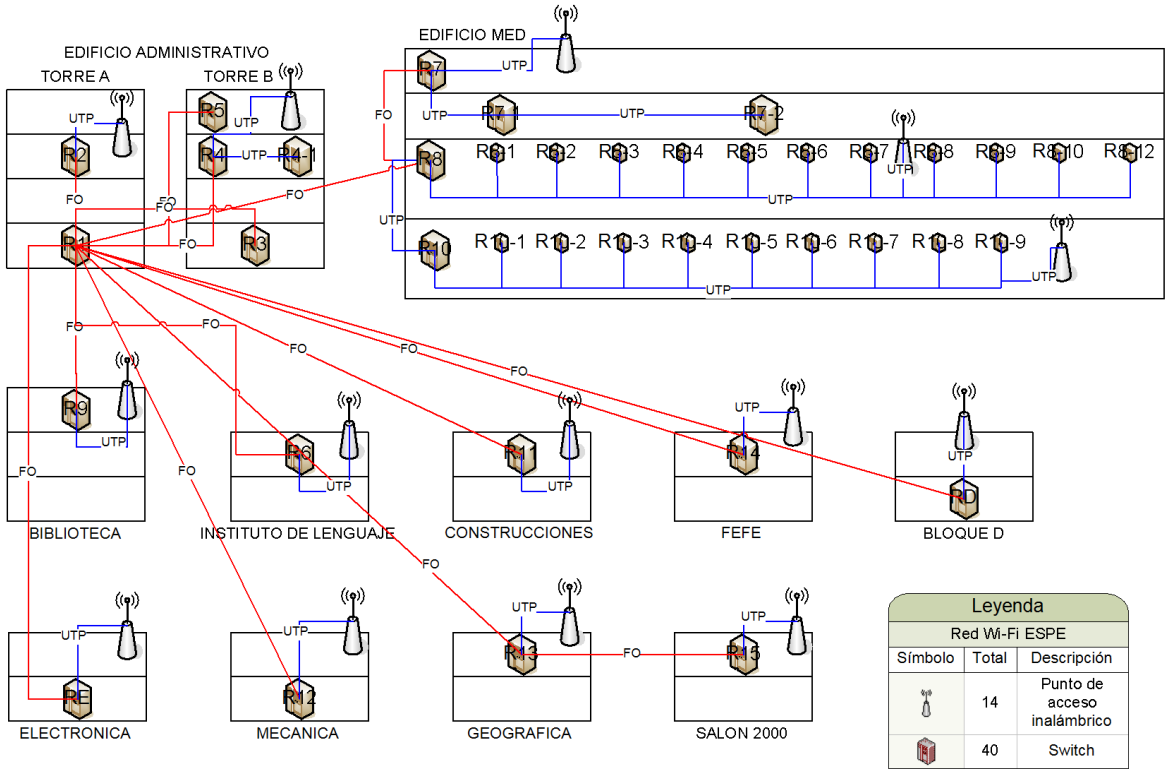


Figura IV.13: Diagrama de red WiFi ESPE Sangolquí

Lo que se puede apreciar en el diagrama, es que se han colocado puntos de acceso inalámbricos con antenas omnidireccionales de 7dBi en cada uno de los edificios de la Institución. Para cubrir la parte exterior como son canchas, parqueaderos, etc. se debe colocar un punto de acceso con una antena de 15dBi en la parte alta del edificio central que dará cobertura de alrededor de un radio de 600 m en exteriores.

4.4- Plan de implementación de la red

Al iniciar un proceso de implementación de una red, se debe tomar en cuenta varios aspectos. En este caso, se tienen procesos que son separados para

su desarrollo uno de otro, entonces se pueden ejecutar de manera paralela, así se administra de mejor forma el recurso tiempo.

4.4.1- Cronograma

Basándose en el análisis anterior, se elabora un cronograma de actividades para la implementación de esta manera:

Tabla IV.1: Cronograma de implementación de la red WiMAX en la ESPE

DESCRIPCION	RESPONSABLE	1 semana	2 semana	3 semana	4 semana	5 semana	6 semana	7 semana	8 semana	9 semana	10 semana	11 semana	12 semana
Petición importación de equipos y llegada	ESPE												
Pruebas de equipos	Técnicos y ESPE												
Adquisición licencia de la banda	ESPE y SENATEL												
Arrendamiento de la torre repetidora	ESPE												
Configuración de equipos en cada ubicación	Técnicos y ESPE												
Pruebas de conectividad	Técnicos y ESPE												
Pruebas de seguridades	Técnicos y ESPE												
Pruebas de servicios	Técnicos y ESPE												

Se puede apreciar en la tabla anterior que aproximadamente se necesitan 12 semanas, equivalentes a 3 meses calendarios, para la implementación del proyecto. La actividad que mas sujeta a cambios está es la segunda ya que los equipos no se encuentran en stock en nuestro país debido a su el elevado costo,

por lo que se debe anticipar su importación desde el exterior con un tiempo prudente.

4.4.2- Descripción de actividades

- **Pruebas de equipos**

Con esta actividad se comprueba la conectividad y el alcance de los equipos de manera real, así como también los anchos de banda y servicios. Estas pruebas deben realizarse principalmente entre la torre repetidora y la sede Sangolquí donde es la parte mas crítica de la red.

- **Petición de importación de equipos**

Se realiza la petición a la empresa de los equipos para que haga la importación de todo lo necesario para la implementación de la red. Esta actividad se debe realizar, de ser posible, con mucha anticipación ya que los equipos no existen en stock en nuestro país.

- **Adquisición licencia de la banda**

Como la banda en la que funcionan estos equipos (3-5 GHz) requiere licencia para su utilización, se la debe solicitar en la Secretaría Nacional de Telecomunicaciones, para lo cual se deben entregar algunos documentos como:

  - Descripción técnica detallada de los servicios que soportará la red, especificando el tipo de información que cursará sobre ella.
  - Diagrama funcional de la red, que indique claramente los elementos activos y pasivos de la misma, describir su funcionamiento basado en el diagrama.

- Gráfico esquemático de la red a instalarse, el cual debe estar asociado a un plano geográfico en el que se indiquen la trayectoria del medio físico de transmisión o los enlaces radioeléctricos que se van a utilizar. Dicho gráfico deberá contener las direcciones exactas de las instalaciones.
- Especificaciones técnicas del equipamiento a utilizarse y de los medios físicos que se emplearían. Incluir una copia de los catálogos técnicos.
- Indicar los recursos del espectro radioeléctrico requeridos, especificando la banda en la cual se va a operar, así como los requerimientos de ancho de banda.
- Requerimiento de conexión.

- **Arrendamiento de la torre repetidora**

En la loma de Puengasí existen algunas torres repetidoras en la actualidad, por lo tanto se debe limitar a arrendar una de éstas, ya que la colocación de una nueva torre usada únicamente para nuestra red implica gastos altos e innecesarios.

Se deben colocar las antenas con sus debidas conexiones y seguridades contra rayos en la parte superior de la torre, y en la base, los equipos de telecomunicaciones y de suministro eléctrico como UPS y reguladores de voltaje.

Cabe indicar que la gran mayoría de torres que se arriendan, incluyen los servicios de electricidad y UPS.

- **Configuración de equipos en cada ubicación**

Las configuraciones deben empezar por la torre de repetición y la sede Sangolquí en paralelo, por ser la parte principal de la red, luego las sedes restantes siguiendo el siguiente esquema de configuración de los equipos:

- Instalación de la red eléctrica y UPS.
- Configuración de equipos de comunicaciones:
  - Selección de banda a trabajar.
  - Selección de modo a operar: punto-punto o punto-multipunto.
  - Configuración de seguridades y filtros: MAC, DES/AES, etc.
  - Configuración de calidad de servicios QoS, asignación de anchos de banda y prioridad de cada tipo de paquete que se transmita por la red.
  - Configuración de la potencia de la antena.
- Colocación y orientación de las antenas.
- Pruebas generales de conectividad.

- **Pruebas de conectividad**

En esta etapa se realizan todo tipo de pruebas de conectividad y ancho de banda de cada uno de los enlaces, transmitiendo datos para simular casos extremos del uso de la red y comprobar cual será el comportamiento de la misma en caso de darse este tipo de situaciones.

Es importante realizar estas pruebas de conectividad en relación al medio ambiente, por ejemplo con lluvia, niebla, o calor extremo.

- **Pruebas de seguridades**

Esta etapa es importante, ya que se debe intentar burlar las seguridades configuradas en toda la red y a todo nivel, esto es, no limitarnos únicamente a la

parte lógica sino también a la física. Algunos puntos importantes en esta actividad son:

- Tratar de capturar paquetes que se transmiten por la red, de lograr esto, descifrar su encriptación para poder entender lo que se transmite.
- Tratar de ingresar a la red como un cliente.
- Utilizar el software de monitoreo de la red permitiendo el ingreso de intrusos de prueba para verificar que éste los localice y notifique.
- Hacer pruebas de fallas eléctricas, cortando la energía en la torre de repetición y en las sedes para comprobar como responden los UPS y otros dispositivos eléctricos, y por cuánto tiempo realmente pueden sostener el enlace.

En los capítulos 5 y 6 se detalla con profundidad el tema de seguridades y las pruebas de vulnerabilidades que se deben realizar al la red.

- **Pruebas de servicios**

Se deben probar todos los servicios que la red debe brindar como VoIP, videoconferencia, Internet, sistemas internos de la ESPE, etc.

Los dos primeros servicios son los que más calidad requieren, por lo tanto, se deben hacer pruebas de situaciones extremas, realizando de manera simultánea llamadas IP, videoconferencias, transmisión de datos, logrando así valores reales el en cuanto al desempeño máximo que la red nos brinda.

4.5- Plan de administración y gestión de la red

Esta parte está enfocada al método de administración de la red, cuando la misma se encuentre en total funcionamiento. Existen algunos programas

diseñados específicamente para este propósito pero en su totalidad son enfocados para redes WiFi por el momento. A continuación se presenta una lista de algunos de ellos.

- Solarwinds
- Loriot
- CiscoWorks Wireless LAN Solution Engine (WLSE)
- Netasyst
- Network Stumbler
- WiFi Manager

Luego de analizar algunos de éstos programas, se presentan dos opciones, CiscoWorks Wireless LAN Solution Engine (WLSE) y WiFi Manager.

4.5.1- CiscoWorks Wireless LAN Solution Engine (WLSE)

CiscoWorks WLSE es una aplicación centralizada basada en niveles de sistema para manejar y controlar una infraestructura entera de la línea Cisco Aironet WLAN.

Características y ventajas:

- Reduce los gastos de implementación y operación
- Simplifica la operación diaria y la administración gerencia de pequeñas y grandes redes Aironet
- Maximiza la seguridad de la red:
    - Detecta, localiza, y elimina puntos de acceso y redes ad-hoc no autorizadas
    - Asegura el uso constante de las políticas de la seguridad.

- Mejoran funcionamiento y disponibilidad de la WLAN:
    - Detecta interferencias de RF.
    - Optimiza la cobertura y configuraciones.
    - Monitorea el funcionamiento y las fallas.
- Ahorra tiempo y recursos:
    - Automatiza la configuración de los access points y bridges Cisco Aironet
    - Ayuda a determinar la selección óptima de la antena y las configuraciones de los access point, como el poder de transmisión y la selección del canal.

4.5.2- WiFi Manager

WiFi Manager es un software diseñado para empresas que poseen redes inalámbricas con una administración y seguridad centralizadas. Realza la disponibilidad y la seguridad de las WLAN implementando un continuo control de la red, así como del espectro de frecuencia. WiFi Manager puede detectar casi todas las amenazas inalámbricas importantes incluyendo intrusiones, sniffers, ataques DoS, y vulnerabilidades. También ahorra tiempo permitiendo configurar cientos de access points con un solo comando. Con WiFi manager se tendrá control completo sobre los dispositivos inalámbricos, así como su espacio aéreo.

Como se mencionó anteriormente, éstos programas son diseñados para redes WiFi, pero el funcionamiento básico del mismo soporta una red WiMAX ya

que se basa en la administración del espectro de frecuencia, interferencias y monitoreo SNMP que son iguales para ambos tipos de redes.

CAPITULO V: Plan de Seguridades

Un plan de seguridades esta diseñado para ayudar a los responsables de la seguridad de un sistema o área de una organización a desarrollar una estrategia para proteger la disponibilidad, integridad y confidencialidad de la información en los enlaces a las sedes del diseño del capítulo anterior.

Análisis de riesgos

Como se describió en el marco teórico, a continuación se definirá separando en áreas físicas y lógicas que se pueden presentar en la interconexión.

Vulnerabilidades físicas

Las vulnerabilidades físicas responden a todo aquello que tenga que ver con el hardware que permite la interconexión de la red. Tomando en cuenta el diseño del capítulo anterior estos son los dispositivos físicos que requieren implementación de alguna seguridad por cualquier causal de riesgo:

- Antenas
- Cable de antenas
- Equipos de comunicación
- Cables eléctricos
- Cable de datos
- Torres de comunicación
- Servidores

Por lo tanto, los riesgos que pueden causar un desastre a estos elementos físicos son los siguientes:

- Caída de rayos en las torres de comunicación
- Movimientos telúricos de gran intensidad

- Lluvia
- Fuertes vientos
- Incendios
- Temperaturas extremas
- Erupción de volcanes
- Accidentes de avión
- Manipulación indebida por el ser humano
- Robo
- Apagones de luz

Vulnerabilidades lógicas

Son aquellas falencias en el sistema que hay proteger para proteger los servicios, aplicaciones, datos, en general la información que es enviada por la red de datos. Quiere decir que los riesgos que se presentan son aquellos que pueden generar falencias en cualquiera de los anteriores nombrados, por lo tanto a continuación listamos la parte lógica de la red que puede ser afectada.

- Servicios de red
- QoS
- Enlace entre sedes
- Velocidad de transferencia
- Pérdida de paquetes
- Aplicaciones críticas

Estos elementos de lógicos de red pueden ser afectados por la activación de los siguientes riesgos:

- Temperaturas extremas

- Manipulación indebida por el ser humano
- Ingreso de intrusos a la red
- Apagones de luz
- Interferencia de otras señales
- Alta congestión en los enlaces entre sedes
- Alta congestión de la LAN de cada sede
- Atenuación de la señal
- Todos los problemas que generen daños físicos a los dispositivos listados anteriormente.

La información de las vulnerabilidades lógicas y físicas se resume en el siguiente cuadro:

Cuadro V.1: Recursos afectados y sus causales de riesgo

RECURSO AFECTADO	CAUSAS DE ACTIVACIÓN DE RIESGOS
Medios de comunicación y enlace, torres y antenas en estaciones terrenas y sedes	Caída de rayos en las torres de comunicación
	Movimientos telúricos de gran intensidad
	Lluvia
	Fuertes vientos
	Incendios
	Temperaturas extremas
	Erupción de volcanes
	Accidentes de avión
	Manipulación indebida por el ser humano
	Robo
Servidores en las sedes	Movimientos telúricos de gran intensidad
	Incendios
	Temperaturas extremas
	Erupción de volcanes
	Accidentes de avión
	Manipulación indebida por el ser humano

RECURSO AFECTADO	CAUSAS DE ACTIVACIÓN DE RIESGOS
	Robo
	Ingreso de intrusos a la red
	Apagones de luz
Configuraciones de red	Ingreso de intrusos a la red
	Apagones de luz
Información, datos, paquetes	Manipulación indebida por el ser humano
	Robo
	Ingreso de intrusos a la red
	Apagones de luz
	Interferencia de otras señales
Servicios de red, aplicaciones, QoS, tasa de transferencia, enlace entre sedes	Ingreso de intrusos a la red
	Apagones de luz
	Alta congestión en los enlaces entre sedes
	Alta congestión de la LAN de cada sede
	Atenuación de la señal
	Interferencia de otras señales

Estas causales de riesgos mencionadas en el cuadro anterior se subdividen, como dijimos inicialmente, en vulnerabilidades físicas y lógicas por lo tanto para el tratamiento de cada una las manejaremos por esta división.

De tal manera que una vez respondidas las preguntas ¿Qué se debe proteger? y ¿de que se necesita proteger?. Se hará el análisis para dar soluciones a estos problemas basándose en políticas de seguridad.

5.1- Políticas de seguridad

Basada en la información recopilada en las vulnerabilidades físicas y lógicas se tiene la protección ante cada uno de los posibles riesgos.

5.1.1- Caída de rayos en torres de comunicación

La estructura de construcción de las torres de comunicación tienen instalación a tierra, generalmente son diseñadas para soportar las inclemencias del clima.

Las antenas y equipos de comunicación serían los más afectados por la caída de rayos, por ello existen dispositivos llamados “supresores de rayos”. Estos supresores de rayos hacen que el rayo se desvíe a tierra por medio de una conexión directa lo que libera de problemas a los dispositivos. El costo de estos dispositivos es 200 USD.

5.1.2- Movimientos telúricos de gran intensidad

Frente a este problema las torres de comunicación suelen ser generalmente antisísmicas. Pero sobre todo los equipos tienen que estar físicamente asegurados en RACKS asegurados al piso. El costo promedio de un RACK de comunicación es de 200 USD.

Los servidores son parte de la seguridad total de las redes de la ESPE. Como estos servidores se encuentran dentro de las instalaciones de la institución entonces se debe acoplar con el sistema actual de seguridad de estos dispositivos.

5.1.3- Lluvia, fuertes vientos

Las antenas de comunicación son diseñadas para exteriores.

Los cables que conectan a las antenas y van a los dispositivos también son diseñados para exteriores por lo tanto no tienen ningún problema. Cualquier falla

será asumida por el fabricante o distribuidor, por lo tanto el costo para solucionar este problema viene dado por la compra de los equipos.

Se debe asegurar las antenas con los mismos dispositivos que vienen para colocarlos en las antenas. Este tipo de problema se soluciona simplemente con una buena instalación de los equipos.

5.1.4- Incendios, robos, erupción de volcanes, accidentes de avión, manipulación física del ser humano

Aunque estos casos son distintos se los trata de igual manera. Si ocurre un incendio dentro de las instalaciones y afectan a los equipos es obvio que no habrá solución con respecto a los mismos. Lo que se debe hacer para tener protegido contra todas estas inclemencias es contratar un seguro para todos los equipos que intervengan en la interconexión, basado en el costo total de el diseño mostrado en el capítulo anterior. Esto no va a solucionar el problema del enlace en caso de perderlo sino para recuperar los equipos.

Para asegurar que no se roben los equipos se debe poner seguridades físicas en la estación terrena como guardianes si es que no lo hubiese y un cerramiento alrededor de la misma.

Para ingresar a las estaciones terrenas sólo pueden hacerlo con documentación asignada por el director de Organización y Sistemas de la ESPE. Quiere decir que sin un memo a nombre del técnico que realice la visita no puede ingresar hasta el área de equipos.

En la estación terrena y en el departamento de redes se debe llevar una bitácora de visitas del personal que realiza las inspecciones a los equipos donde conste: fecha, responsable, técnico,

Se debe tener un inventario documentado de los equipos de comunicaciones, detallando el nombre del responsable del área física como de los equipos en si.

5.1.5- Temperaturas extremas

Esto se soluciona tanto en el área de servidores como en cuarto de comunicaciones de estaciones terrenas poniendo aire acondicionado capaz de satisfacer los requerimientos del fabricante.

5.1.6- Apagones de luz

La instalación de sistemas de soporte eléctrico llamados UPS debe ir acorde con la cantidad de amperaje utilizado en esta área. Se debe instalar UPS que permitan mantener la energía por lo menos 1 hora.

5.1.7- Interferencia de otras señales

Como se mencionó en el marco teórico, WiMAX tiene la capacidad de seleccionar la frecuencia dinámicamente DFS (dynamic frecuency selection). En los equipos descritos en el diseño se debe configurar esta opción así no existen colisiones o problemas con otras señales

Si se trabaja con una banda licenciada entonces es muy poco probable la colisión con otras señales de otras redes. En la sección Descripción de actividades del Capítulo 4 se describe este proceso.

5.1.8- Ingreso de intrusos a la red

El ingreso de intrusos a la red trata no solo de hackers o personas mal intencionadas sino también de elementos que puedan capturar la señal de la información y hacerla de uso público.

Existen varios métodos para no permitir el ingreso de intrusos a la red y a la configuración de equipos. Este proyecto trata de la seguridad de la información dentro de la red diseñada, quiere decir que el manejo de seguridades e intrusión de otras personas al resto de redes que pertenecen a la institución la manejaran los administradores del área de redes.

5.1.9- Ingreso a los equipos de comunicación

Cada equipo tiene cuentas de administración con sus respectivas claves. Internamente en la ESPE se maneja cierto formato para la asignación de éstas. Estas claves deben ser renovadas cada 30 días, y no pueden ser iguales a las 3 últimas claves asignadas. Para cada dispositivo la clave tiene que ser distinta e independiente a las otras.

Los equipos administrables remotamente, tendrán levantado un puerto que asigne el administrador del sistema tanto en el firewall como el equipo en sí. La forma de administración que manejan los equipos analizados en el diseño son:

remotamente utilizando telnet y SNMP, localmente por el puerto RS 232 e inalámbricamente con un equipo que tenga un suscriber a la base station.

Por seguridad, una vez puesta en marcha la red, se debe respaldar las configuraciones de cada equipo en un archivo, para que en caso de presentarse una desconfiguración grave, se pueda acudir a éste y resolver el problema de marea rápida.

5.1.10- Confidencialidad e integridad de la información

La información debe ser protegida cualquiera sea el grado de importancia. Dentro de WiMAX se maneja una capa de seguridad que permite la administración de los paquetes de tal manera que salen ya encriptados en el momento del envío hasta su recepción. Al igual que cualquier otro protocolo los paquetes de información pasan por fases de encriptación, autenticación e intercambio de llaves ya sean públicas o privadas dependiendo del protocolo.

En el caso de los equipos analizados en la sección 4.3.1, se tiene que manejan la siguiente seguridad:

- Data Scrambling (cifrado de datos): Encriptación DES/AES
- Security configuration (Seguridad para configuración)
- Data password (clave para datos)

En muchos dispositivos inalámbricos como los access points, se tiene el problema que cualquier persona que se encuentra dentro del rango y con un dispositivo para conexión a redes inalámbricas, en el caso de WiMAX los suscriber station, aparece el nombre del dispositivo (SSID) entre sus redes

disponibles, quiere decir que el SSID del dispositivo es público. Esta opción debe ser desactivada como otra medida de precaución.

5.1.11- Disponibilidad de la información

La disponibilidad de información es la capacidad del usuario de recibir y enviar los datos que solicita o que requieres en el momento indicado. Una vez controlada la información física y lógica con respecto a los dispositivos, se deben tomar políticas de cómo administrar los paquetes, servicios y usuarios.

5.1.12- Atenuación de la señal

Este problema se puede presentar en días muy congestionados de lluvia o extremo calor. Al diseñar la red se toma en cuenta que WiMAX y los equipos a utilizarse trabajan hasta 70 Km. con línea de vista y la distancia máxima entre los enlaces es de 10 Km., no se presentarán problemas. Técnicamente la tecnología WiMAX fue diseñada exclusivamente para cubrir esta falencia en otras tecnologías inalámbricas.

5.1.13- Manipulación indebida por el ser humano a nivel lógico

La principal falla en el funcionamiento de los equipos suele ser la mala configuración y falta de conocimiento de los administradores sobre la utilización de los equipos y de la tecnología implementada.

Se debe capacitar de manera eficiente al personal que vaya a ser el responsable del manejo o administración de la red.

Generar un listado de las personas que son capacitadas para el manejo y no permitir emitir permisos para otras personas para el ingreso hacia los equipos.

La parte de intrusos mal intencionados a la red ya fue analizado anteriormente.

Pruebas de intrusión

En las pruebas de intrusión existen varias técnicas, en el caso de redes inalámbricas se recomienda el Ethical Hacking.

5.1.14- Ethical Hacking

El ethical hacking es acceder a los equipos informáticos de la organización analizada e intentar obtener los privilegios del administrador del sistema, logrando así realizar cualquier tarea sobre esos equipos. También se podrán definir otros objetivos secundarios que permitan realizar pruebas puntuales sobre algunos ámbitos particulares de la empresa.

Los procesos a seguir para el ethical hacking son los siguientes:

- Planeamiento de las pruebas externas y/o internas con los administradores de la red de la ESPE.
- Tests de penetración de los firewalls
- Tests de intrusión en ruteadores y otros elementos de la red
- Tests de las capacidades de detección de ataques
- Evaluación de las políticas de seguridad y de su aplicación real
- Reporte de las pruebas y resultados, con evaluación y recomendaciones

Todos estos pasos la ESPE debe realizar para todas las redes e interconexiones de la institución; no sólo del área que está por implementarse a menos que se hayan realizado pruebas recientes para cerciorarse que la seguridad de todas las áreas se encuentran en óptimas condiciones.

En el caso del enlace WiMAX que se esta presentando, las pruebas de intrusión se las debe dar a:

- Firewalls que intervienen en el enlace de cada una de las sedes
- Switches que intervienen en el enlace de cada una de las sedes
- Protocolos de encriptación DES/AES
- Señales enviadas entre cada sede
- Aplicaciones y servicios a brindar en los enlaces

5.1.14.1- Planeamiento de pruebas con los administradores de la red de la ESPE.

Se pondrá a prueba el enlace sin realizar la interconexión entre la red interna de la institución.

El administrador de las redes en el departamento de organización y sistemas de la ESPE delegará la persona responsable para todas las pruebas que se necesiten realizar.

Estas pruebas se deben realizar por un mes, continuamente, a fin de tener una visualización real del funcionamiento de los sistemas.

Todas las pruebas se deben realizar en paralelo utilizando las siguientes herramientas para cada una de las pruebas:

5.1.14.2- Tests de penetración de los firewalls, de intrusión en ruteadores y capacidad de detección de ataques.

Para realizar todos estos test orientados a evaluar el nivel de seguridad en el que se encuentra la red diseñada, se lo realizará mediante un software que permita realizar un análisis de varios aspectos que nos pueden detallar en donde se puede estar fallando y se debe reforzar las políticas de seguridad.

En este documento recomendamos utilizar el software **GFI LANGuard.**

GFI LANguard Network Security Scanner [1]

GFI LANguard Network Security Scanner (**GFI LANguard N.S.S.**) es una herramienta que permite a los administradores de red realizar rápida y fácilmente una auditoría de seguridad de red. GFI LANguard N.S.S. crea informes que pueden ser utilizados para resolver problemas de seguridad de la red. Además puede realizar la administración de actualizaciones de seguridad. Al contrario que otros escáneres de seguridad, GFI LANguard N.S.S. no creará un 'bombardeo' de información, que es virtualmente imposible de seguir. En su lugar, ayudará a resaltar la información más importante. Además proporciona hipervínculos a sitios de seguridad para averiguar más sobre estas vulnerabilidades. Utilizando análisis inteligente, GFI LANguard N.S.S. recoge información sobre los equipos como nombres de usuario, grupos, recursos compartidos, dispositivos USB, dispositivos inalámbricos y otra información sobre un Dominio Windows. Además de esto, GFI LANguard N.S.S. también identifica vulnerabilidades específicas como problemas de configuración de servidores FTP, exploits en

[1] GFI SOFTWARE, GFI Development Group, http://www.gfi.nu/es/lannetscan/lanscan6manual_es.pdf, 2005

Servidores Microsoft IIS y Apache Web o problemas en la configuración de la política de seguridad Windows, más otros muchos potenciales problemas de seguridad.

Este software nos va a permitir analizar lo siguiente:

- Encuentra servicios y puertos TCP y UDP abiertos
- Detecta vulnerabilidades CGI, DNS, FTP, Correo, RPC y otras
- Detecta dispositivos inalámbricos.
- Detecta usuarios maliciosos y en “puertas traseras” (backdoors)
- Detecta recursos compartidos abiertos y enumera quién tiene acceso a estos recursos junto con sus permisos.
- Enumera grupos, incluyendo los miembros de grupos.
- Enumeración de usuarios, servicios, etc.
- Enumera dispositivos de red e identificación del tipo de dispositivo (Cableado, Inalámbrico, Virtual)
- Puede realizar Análisis Programados.
- Actualiza automáticamente las Comprobaciones de vulnerabilidad de seguridad.
- Habilidad para detectar la falta de actualizaciones críticas y service packs del sistema operativo.
- Habilidad para detectar la falta de actualizaciones críticas y service packs de aplicaciones soportadas.
- Capacidad de guardar y cargar resultados de análisis.
- Habilidad de comparar análisis, para enterarse de posibles nuevos puntos de entrada.

- Identificación de Sistema operativo.
- Resultados en HTML, XSL y XML.
- Auditoría SNMP y MS SQL.
- Lenguaje de comandos compatible Vbscript comprobaciones de vulnerabilidad a medida.
- Módulo SSH que permite la ejecución de sobre equipo Linux/Unix.
- Analiza varios equipos al mismo tiempo.

Luego de haber realizado si es necesario cambios dentro de las políticas de seguridad se debe realizar las mismas pruebas cada 3 meses para confirmar su buen funcionamiento.

Con estos datos derivados del análisis que nos entrega el software se tienen las pruebas de intrusión que requerimos para brindar de la mejor manera la seguridad de los enlaces.

5.2- Estándar ISO 17799

La ESPE como Institución educativa de alto nivel, debe proyectarse a una certificación para la seguridad de su información, la ISO 17799. Siendo este proceso un tema aparte de estudio que el proyecto actual.

5.3- Quality of Service (QoS)

La tecnología WiMAX brinda total soporte para calidad de servicio, lo importante es que todos los dispositivos de la red tengan esta característica.

5.4- Informática forense

En el caso de la ESPE, con el mismo software que se recomendó anteriormente se puede realizar este proceso de seguridad. También con la instalación de Active Directory o paquetes de auditoría como el SMS de Microsoft, se puede detectar varias anomalías a nivel de software que pueden afectar al desempeño de la red interna de la institución.

CAPITULO VI: Plan de Contingencias de Comunicaciones

"Entendemos por plan de contingencia el conjunto de procedimientos alternativos a la operativa normal de cada empresa, cuya finalidad es la de permitir el funcionamiento de ésta, aún cuando alguna de sus funciones deje de hacerlo por culpa de algún incidente tanto interno como ajeno a la organización".[1]

El hecho de preparar un plan de contingencia no implica un reconocimiento de la ineficiencia en la gestión de la empresa, sino todo lo contrario, supone un importante avance a la hora de superar todas aquellas situaciones descritas con anterioridad y que pueden provocar importantes pérdidas, no solo materiales sino aquellas derivadas de la paralización del negocio durante un período más o menos largo.

Dentro de las empresas donde la necesidad de sistemas informáticos es crucial para su funcionamiento, se debe tomar en cuenta los riesgos que se pueden presentar, los cuales al ejecutarse, se convertirían en desastres. En la ESPE, la utilización de sistemas de conectividad tiene un alto nivel de requerimientos a nivel de usuarios de distintas áreas.

Al realizar la interconexión de las sedes se debe tomar en cuenta que los servicios que se utilicen dependerán de la calidad del enlace que se provea.

Con el plan de contingencia se realiza la investigación de cuales son los riesgos que pueden generar posibles desastres y a su vez las medidas a tomar para que la ejecución de estos riesgos sea casi nula y esencialmente el plan de contingencia servirá para cuando estos riesgos se conviertan en desastres, los

[1]Anónimo, ¿Está su empresa preparada ante incidentes imprevistos? http://www.virusprot.com/Art4.html

sistemas sigan funcionando orientados a satisfacer en ese momento los requerimientos básicos de los usuarios.

Desastre

Un desastre es la ejecución de un riesgo, esto genera la interrupción del sistema informático ya sean redes o software por un lapso de tiempo. Dependiendo del tiempo, cantidad y tipo de información, se puede su considerar su gravedad: baja, mediana, alta e irrecuperable.

Estos riesgos pueden originar desastres por distintos actores:

- Medio ambiente.
- Tecnología.
- Ser humano.

Independiente de cual sea el origen de estos desastres llevan al mismo punto, inestabilidad en el sistema de información.

Según un análisis del personal administrativo encargado del control de esta área se determina cual de estos riesgos, al ejecutarse, se transforma en “problema” o “desastre”.

6.1- Metodología para el plan de contingencia

Como todo proyecto, se debe realizar un análisis estructurado a fin de tomar en cuenta todos los factores y tratarlos adecuadamente.

A continuación se muestran las fases a seguir para documentar el plan de contingencia:

- Evaluación.
- Planificación.

- Pruebas de viabilidad.
- Ejecución.
- Recuperación.

6.1.1- Fase de evaluación

La fase de evaluación indicará que riesgos, parámetros, áreas, personal, procesos y ambientes que se deben tomar en cuenta para elaborar el plan de contingencia. De esta manera lo que se busca en la fase de evaluación es lo siguiente:

- Constitución del grupo de desarrollo del plan.
- Identificación de riesgos o funciones críticas.
- Definición y documentación de los posibles escenarios con los que se puede encontrar para cada elemento o función crítica.
- Análisis del impacto del desastre en cada función crítica.
- Definición de los niveles mínimos de servicio.
- Identificación de las alternativas de solución.
- Evaluación de la relación coste/beneficio de cada alternativa.

6.1.1.1- Grupo de desarrollo del plan

En este caso la documentación será responsabilidad de los elaboradores de este documento. Luego, para cada una de las responsabilidades que se van a asignar, se documentará recomendaciones, pero al final el director del proyecto de implementación o del departamento de Organización y Sistemas de la institución será el encargado en delegar estas.

Por lo tanto el director del desarrollo del plan deberá ser la persona que dirija el proyecto delegada en el área de Organización y Sistemas de la ESPE.

6.1.1.2- Identificación de riesgos o funciones críticas

Las funciones críticas suelen ser aquellos elementos de la institución o funciones que puedan ser críticos ante cualquier eventualidad o desastre, jerarquizarlos por orden de importancia dentro de la organización.

En este caso, serían a nivel de hardware los elementos físicos y dispositivos que permiten la interconexión y a nivel lógico los servicios que se proveen a cada sede.

Estos elementos son los nombrados anteriormente en el plan de seguridades, listados a continuación de manera jerárquica, en orden descendente, separados en elementos físicos y elementos lógicos:

Elementos físicos:

- Equipos de comunicación
- Antenas
- Cable de antenas
- Cables eléctricos
- Cable de datos
- Torres de comunicación
- Servidores

Elementos lógicos:

- Enlace entre sedes
- Servicios de red

- QoS
- Pérdida de paquetes
- Velocidad de transferencia
- Aplicaciones críticas
- Configuración de equipos

6.1.1.3- Definición y documentación de los posibles escenarios con los que se puede encontrar para cada elemento o función crítica

Los riesgos son analizados tomando en cuenta el diseño de la red. Estos riesgos que se corren son generados por desastres de 3 tipos:

- Medio ambiente
- Tecnología
- Ser humano

Estos parámetros son los mismos que los que se encuentran en el plan de seguridades, donde las vulnerabilidades se convierten en riesgos en esta sección separados de la siguiente manera:

Medio ambiente

Aquellos producidos por desastres naturales o inclemencias del medio ambiente. Tras el análisis se concluye que los siguientes generan un factor de riesgo:

- Caída de rayos en las torres de comunicación
- Movimientos telúricos de gran intensidad
- Lluvia
- Fuertes vientos

- Incendios
- Temperaturas extremas
- Erupción de volcanes
- Accidentes de avión
- Apagones de luz accidentales

Ser Humano

Aquellos producidos por la mano del hombre. Tras el análisis se concluye que los siguientes generan un factor de riesgo:

- Manipulación indebida por el ser humano
- Robo
- Apagones de luz
- Ingreso de intrusos a la red

Tecnología

Aquellos producidos por falencias tecnológicas o falta de optimización de recursos informáticos. Tras el análisis se concluye que los siguientes generan un factor de riesgo:

- Interferencia de otras señales
- Alta congestión en los enlaces entre sedes
- Alta congestión de la LAN de cada sede
- Atenuación de la señal
- Interferencia de otras señales
- Apagones de luz
- Mal funcionamiento de equipos

Basándose en esta información, se realizó el cuadro 5.1.

6.1.1.4- Análisis del impacto del desastre en cada función crítica y alternativas de solución

Consiste en realizar un análisis del impacto de cada problema sobre cada una de las funciones críticas del diseño.

En este caso, basándose en la información obtenida de los posibles riesgos en el plan de seguridades se tiene el siguiente cuadro.

Cuadro VI.1: Análisis de impacto

FUNCIONES AFECTADAS	RIESGO GENERADOR	SOLUCIÓN	TIEMPO DE ACCIÓN	TIEMPO DE EJECUCIÓN	TIEMPO TOTAL PARA CONTINUIDAD
Problemas de funcionamiento de los equipos	Caída de rayos en las torres de comunicación	Ejecución del seguro contratado para los equipos y utilizar hasta la reposición de los mismos el enlace DSL de respaldo	30 min	7 días	7 días 30 min
	Movimientos telúricos de gran intensidad				
	Lluvia				
	Fuertes vientos				
	Incendios				
	Temperaturas extremas				
	Accidentes de avión				
	Manipulación indebida por el ser humano				
	Defectos de fabricación	Ejecución de garantía de los equipos y utilizar hasta la reposición de los mismos el enlace DSL de respaldo	2 hrs	7 días	7 días 2 hrs
Alteración en las configuraciones	Caída de rayos en las torres de comunicación	Cargar la configuración respaldada del equipo respectivo	30 min	2 hrs	2 hrs 30 min
	Manipulación indebida por el ser humano				
	Ingreso de intrusos a la red	Revisar la política de seguridad sobre integridad de la información y cambiar las claves actuales de acceso	2 días	3 días	5 días

FUNCIONES AFECTADAS	RIESGO GENERADOR	SOLUCIÓN	TIEMPO DE ACCIÓN	TIEMPO DE EJECUCIÓN	TIEMPO TOTAL PARA CONTINUIDAD
Problemas en la instalación de las antenas	Movimientos telúricos de gran intensidad	Realizar una inspección técnica para la revisión de la instalación de los equipos. El técnico debe tener la capacidad de realizar pruebas para confirmar el enlace	30 min	1 día	1 día 30 min
	Fuertes vientos				
	Manipulación indebida por el ser humano				
	Accidentes de avión	Ejecución del seguro contratado para los equipos y utilizar hasta la reposición de los mismos el enlace DSL de respaldo	30 min	7 días	7 días 30 min
Deterioro de los cables y conectores	Lluvia	Realizar una inspección técnica para la revisión de estos elementos. El técnico debe tener la capacidad de realizar pruebas para confirmar el enlace	3 días	5 días	8 días
	Fuertes vientos				
	Manipulación indebida por el ser humano				
	Temperaturas extremas				
	Robo	Ejecución del seguro contratado para los equipos y utilizar hasta la reposición de los mismos el enlace DSL de respaldo	30 min	7 días	7 días 30 min
Daño en estación terrena	Lluvia	En el caso qua la estación terrena no sea de la ESPE, solicitar al propietario su arreglo, si esto no es posible, buscar otra estación cercana para continuidad del enlace. Si es de propiedad de la ESPE, reparar los daños y ejecutar el seguro contratado, en ambos casos se utilizar el enlace DSL de	3 días	15 días	18 días
	Fuertes vientos				
	Incendios				
	Accidentes de avión		1 día	5 días	6 días

FUNCIONES AFECTADAS	RIESGO GENERADOR	SOLUCIÓN	TIEMPO DE ACCIÓN	TIEMPO DE EJECUCIÓN	TIEMPO TOTAL PARA CONTINUIDAD
		respaldo hasta la solución del problema			
Pérdida total de comunicación	Movimientos telúricos de gran intensidad	Si los desastres naturales son muy graves, se tendrá que revisar las prioridades del plan de contingencia con respecto al resto de la institución, esta pérdida total de la comunicación se verá solucionada con la ejecución de todas las medidas mencionadas por el resto de desastres.	No calculable	No calculable	No calculable
	Incendios				
	Temperaturas extremas				
	Erupción de volcanes				
	Accidentes de avión				
	Ingreso de intrusos a la red	Revisar la política de seguridad sobre integridad de la información y cambiar las claves actuales de acceso, luego cargar las configuraciones respaldadas en el momento de la instalación adoptando las nuevas políticas de seguridad	2 días	3 días	5 días
Deficiencia en los servicios, seguridad y perdida, retraso o alteración de la información	Manipulación indebida por el ser humano	Realizar una inspección técnica para la revisión de la instalación de los equipos. El técnico debe tener la capacidad de realizar pruebas para confirmar el enlace	1 día	2 días	3 días
	Ingreso de intrusos a la red	Revisar la política de seguridad sobre integridad de la información y cambiar las claves actuales de acceso, luego cargar las	1 día	5 días	6 días

FUNCIONES AFECTADAS	RIESGO GENERADOR	SOLUCIÓN	TIEMPO DE ACCIÓN	TIEMPO DE EJECUCIÓN	TIEMPO TOTAL PARA CONTINUIDAD
		configuraciones respaldadas en el momento de la instalación adoptando las nuevas políticas de seguridad			
	Alta congestión en los enlaces entre sedes	Cambiar las políticas de administración de red para proveer de QoS. Realizar un análisis de tráfico referido a los servicios que se están brindando y adoptar nuevas políticas de administración basándose en este análisis	1 día	5 días	6 días
	Alta congestión de la LAN de cada sede	Revisar plan de contingencia para las redes locales de cada sede	1 día	15 días	16 días
	Atenuación de la señal	Investigar causales para la atenuación de la señal: medio ambiente, interferencia, etc. Si no existen resultados que puedan mostrarse como causales de este problema entonces procurar hacer un análisis sobre los dispositivos en especial antenas que se utilizan en el enlace si es necesario incrementar la potencia de envió de la señal	1 día	5 días	6 días
	Interferencia de otras señales	Revisar las configuraciones con respecto a la frecuencia que se utiliza en el enlace	30 min	1 día	1 día 30 min

FUNCIONES AFECTADAS	RIESGO GENERADOR	SOLUCIÓN	TIEMPO DE ACCIÓN	TIEMPO DE EJECUCIÓN	TIEMPO TOTAL PARA CONTINUIDAD
Apagones de luz	Caída de rayos	Se debe inicialmente saber si es por problemas de: suministro energético público, desastre o falta de energía de estación terrena. En el primer caso se debe reportar el corte de luz a la empresa eléctrica y en el resto de situaciones enviar el personal necesario para superar este inconveniente.	2 hrs	4 hrs	6 hrs
	Fallas eléctricas	Si el sistema de soporte eléctrico de UPS ha culminado su ciclo de cobertura, considerar la utilización del medio alternativo que es el sistema de conexión DSL	30 min	7 días	7 días 30 min

6.1.1.5- Definición de los niveles mínimos de servicios

Actualmente la ESPE cuenta con 2 servicios que se brindan entre sedes que son: Internet y sistema escolástico.

Como se ha analizado en este documento, se debe proyectar a implementar servicios como: videos conferencias, VoIP. Actualmente estos servicios no están activos, pero se pretende que con la implementación de una red WiMAX esto sea posible.

En el departamento de organización y sistemas, nos indica que el servicio que debe siempre estar activo es el sistema escolástico especialmente en época de matrículas. Luego la utilización del Internet es fundamental para el sistema de enseñanza.

Si se implementa VoIP es un servicio muy importante pero al poder tener en paralelo las líneas de comunicación normales pues se podría prescindir en el momento de un desastre y por último quedaría video conferencia.

Por lo tanto se ha categorizado del 1 al 5 la prioridad siendo 1 la de más alta.

Cuadro VI.2: Prioridad de aplicaciones en caso de desastres

APLICACIÓN	PRIORIDAD
Sistema escolástico	1
Internet	2
VoIP	3
Video Conferencia	4

Basado en este cuadro de prioridades se realiza el plan de continuidad de servicios.

Plan de continuidad de servicios

El plan de continuidad de servicios lo que genera es la documentación para poder brindar en caso de desastres los servicios mínimos que requieren las sedes.

6.1.1.5.1 Requerimientos mínimos de enlace

El servicio que se presta actualmente a las sedes son: el sistema escolástico e Internet. Si se toma en cuenta las proyecciones de servicios a 3 años que se realizó en el capítulo anterior, se debe tener los siguientes enlaces para cada sede:

Cuadro VI.3: Proyección de la tasa de transferencia por sedes a 3 años

SEDE	TASA DE TRANSFERENCIA
Héroes del Cenepa	14.76 Mbps
Idiomas	11.00 Mbps
IASA I	10.96 Mbps

Basado en estos datos, se debe tener una conexión alternativa de respaldo con alguno de los operadores que nos brinden un servicio de xDSL como el proveedor de servicios actual y si el presupuesto lo permite la adquisición de equipos de redundancia. Lo importante, por cuestiones económicas, es negociar con el proveedor de estos servicios que se haga el cobro por el tiempo utilizado, no por un costo o contrato mensual.

Con estos enlaces se puede soportar el sistema escolástico y el Internet en las sedes siendo estos los servicios actuales.

6.1.2- Planificación del plan de contingencia

Se debe planificar como realizar la documentación del plan de contingencia y su validación para el momento de necesitarse.

Documentación del plan de contingencia

Esta fase de la planificación consta de las siguientes partes:

- Objetivo del plan
- Modo de ejecución
- Tiempo de duración
- Costes estimados
- Recursos necesarios
- Evento a partir del cual se pondrá en marcha el plan

6.1.2.1- Objetivo del plan de contingencia

Documentar las acciones a tomarse en el momento que cualquiera de las medidas de seguridad implementadas sea vulnerada y los riesgos se conviertan en desastres.

6.1.2.2- Modo de Ejecución

El Plan de Contingencia debe ser de completo conocimiento a los responsables en el área de redes. De tal manera que en el momento que alguno de los desastres se presente se tenga perfecto conocimiento que es lo que hay que hacer.

Principalmente se van a tener delegados para cada una de las áreas involucradas, a continuación se detallará que áreas son las que se deben tomar en cuenta para su administración.

- Hardware
- Software
- Áreas Físicas
- Marcos Legales
- Área Administrativa

Quedando el siguiente cuadro de resumen de las áreas y los riesgos que se involucran.

Cuadro VI.4: Administración de riesgos por áreas

AREA	RIESGO
Marcos Legales	Ejecución de garantía de los equipos y utilizar hasta la reposición de los mismos el enlace DSL de respaldo
	Ejecución del seguro contratado para los equipos y utilizar hasta la reposición de los mismos el enlace DSL de respaldo
	En el caso qua la estación terrena no sea de la ESPE, solicitar al propietario su arreglo, si esto no es posible, buscar otra estación cercana para continuidad del enlace. Si es de propiedad de la ESPE, reparar los daños y ejecutar el seguro contratado, en ambos casos se utilizar el enlace DSL de respaldo hasta la solución del problema
	Si los desastres naturales son muy graves, se tendrá que revisar las prioridades del plan de contingencia con respecto al resto de la institución, esta pérdida total de la comunicación se verá solucionada con la ejecución de todas las medidas mencionadas por el resto de desastres.
Software	Cargar la configuración respaldada del equipo respectivo
	Revisar la política de seguridad sobre integridad de la información y cambiar las claves actuales de acceso
	Revisar la política de seguridad sobre integridad de la información y cambiar las claves actuales de acceso, luego cargar las configuraciones respaldadas en el momento de la instalación adoptando las nuevas políticas de seguridad

AREA	RIESGO
	Cambiar las políticas de administración de red para proveer de QoS. Realizar un análisis de tráfico referido a los servicios que se están brindando y adoptar nuevas políticas de administración basándose en este análisis
	Revisar las configuraciones con respecto a la frecuencia que se utiliza en el enlace
Hardware	Realizar una inspección técnica para la revisión de la instalación de los equipos. El técnico debe tener la capacidad de realizar pruebas para confirmar el enlace
	Revisar la política de seguridad sobre integridad de la información y cambiar las claves actuales de acceso, luego cargar las configuraciones respaldadas en el momento de la instalación adoptando las nuevas políticas de seguridad
	Investigar causales para la atenuación de la señal: medio ambiente, interferencia, etc. Si no existen resultados que puedan mostrarse como causales de este problema entonces procurar hacer un análisis sobre los dispositivos en especial antenas que se utilizan en el enlace si es necesario incrementar la potencia de envío de la señal
	Se debe inicialmente saber si es por problemas de: suministro energético público, desastre o falta de energía de estación terrena. En el primer caso se debe reportar el corte de luz a la empresa eléctrica y en el resto de situaciones enviar el personal necesario para superar este inconveniente.
	Si el sistema de soporte eléctrico de UPS ha culminado su ciclo de cobertura, considerar la utilización del medio alternativo que es el sistema de conexión DSL
Administrativos	Revisar plan de contingencia para las redes locales de cada sede

6.1.2.3- Tiempo de Duración

El tiempo de duración del plan de contingencia va directamente relacionado con el plan de seguridad ya que esta basado en este.

Una vez generadas las políticas de seguridad se recomienda que sean evaluadas cada 3 meses.

Si estas generan alguna variante, se deberá tomar en cuenta esta parte también en el plan de contingencia.

Un nuevo plan de contingencia deberá ser documentado una vez que se genere un nuevo plan de seguridades.

6.1.2.4- Recursos Necesarios y costes estimados

El plan de contingencia descrito esta conformado por los siguientes recursos:

- Recursos humanos
- Recursos legales
- Recursos tecnológicos
- Documentación
- Capacitación
- Recursos financieros

6.1.2.4.1 Recursos Humanos y responsabilidades

Es el personal encargado tanto de la elaboración, ejecución, mantenimiento y auditoría del plan de contingencia por lo tanto como recurso humano se necesita:

- Coordinador del plan de contingencia.- Encargado de la administración del plan en todas sus fases.
- Grupo de trabajo para la elaboración.- Encargado de la elaboración y documentación del plan. (2 personas)
- Grupo de trabajo para el mantenimiento.- Junto al auditor y el coordinador se encargan de realizar las modificaciones necesarias para el buen funcionamiento del plan (2 perdonas)

- Auditor para el plan de contingencia.- Revisa la documentación desde la fase de ejecución del plan.

Cuadro VI.5: Responsabilidades de acción en el plan de contingencia

ACCIÓN DEL PLAN DE CONTINGENCIA	RESPONSABLE
Ejecución del seguro contratado para los equipos y utilizar hasta la reposición de los mismos el enlace DSL de respaldo	Coordinador
	Grupo Mantenimiento
Ejecución de garantía de los equipos y utilizar hasta la reposición de los mismos el enlace DSL de respaldo	Coordinador
	Grupo Mantenimiento
Cargar la configuración respaldada del equipo respectivo	Grupo Elaboración
	Grupo Mantenimiento
Revisar la política de seguridad sobre integridad de la información y cambiar las claves actuales de acceso	Auditor
	Coordinador
	Grupo Elaboración
	Grupo Mantenimiento
Realizar una inspección técnica para la revisión de la instalación de los equipos. El técnico debe tener la capacidad de realizar pruebas para confirmar el enlace	Coordinador
	Grupo Mantenimiento
Realizar una inspección técnica para la revisión de estos elementos para la interconexión. El técnico debe tener la capacidad de realizar pruebas para confirmar el enlace	Coordinador
	Grupo Mantenimiento
En el caso qua la estación terrena no sea de la ESPE, solicitar al propietario su arreglo. Si esto no es posible, buscar otra estación cercana para continuidad del enlace. Si es de propiedad de la ESPE, reparar los daños y ejecutar el seguro contratado, en ambos casos se utilizar el enlace DSL de respaldo hasta la solución del problema	Coordinador
	Grupo Mantenimiento
	Grupo Elaboración
Si los desastres naturales son muy graves, se tendrá que revisar las prioridades del plan de contingencia con respecto al resto de la institución, esta pérdida total de la comunicación se verá solucionada con la ejecución de todas las medidas mencionadas por el resto de desastres.	Auditor
	Coordinador
Cambiar las políticas de administración de red para proveer de QoS. Realizar un análisis de tráfico referido a los servicios que se están brindando y adoptar nuevas políticas de administración basándose en este análisis	Auditor
	Grupo Elaboración
Revisar plan de contingencia para las redes locales de cada sede	Coordinador
	Agente Externo
Investigar causales para la atenuación de la señal: medio ambiente, interferencia, etc. Si no existen resultados que	Auditor
	Grupo

ACCIÓN DEL PLAN DE CONTINGENCIA	RESPONSABLE
puedan mostrarse como causales de este problema entonces procurar hacer un análisis sobre los dispositivos en especial antenas que se utilizan en el enlace si es necesario incrementar la potencia de envío de la señal	Mantenimiento
Revisar las configuraciones con respecto a la frecuencia que se utiliza en el enlace	Auditor
	Grupo Elaboración
Se debe inicialmente saber si es por problemas de: suministro energético público, desastre o falta de energía de estación terrena. En el primer caso se debe reportar el corte de luz a la empresa eléctrica y en el resto de situaciones enviar el personal necesario para superar este inconveniente.	Coordinador
Si el sistema de soporte eléctrico de UPS ha culminado su ciclo de cobertura, considerar la utilización del medio alternativo que es el sistema de conexión DSL	Coordinador
	Grupo Mantenimiento
Elaboración y documentación	Coordinador
	Grupo Elaboración

6.1.2.4.2 Recursos Legales

En los recursos legales se debe tomar en cuenta lo siguiente:

- Ejecución de pólizas de seguros
- Garantías de los equipos
- Restricciones de uso de frecuencias contratadas; y
- Contratación de áreas físicas en el caso de ser necesario
- Contratación de servicios de interconexión con operadoras locales

Este marco legal es muy importante ya que es aquel que permite la ejecución del plan de contingencia. Por ejemplo, si en cierto caso uno de los equipos tiene defectos de fabricación y las garantías no han sido debidamente tratadas; otro caso podría ser si se sustraen algún dispositivo, se debe realizar

basado en un marco legal bien definido el reclamo para que el seguro responda ante el siniestro.

6.1.2.4.3 Recursos tecnológicos

Para una adecuada utilización del plan de contingencias se debe tener un respaldo tecnológico que permita la recuperación, detección, corrección y documentación de los errores. Basado en estos recursos tecnológicos, el auditor tendrá la capacidad de realizar un análisis exhaustivo y, acompañado al grupo de mantenimiento, realizar las respectivas correcciones si fuese necesario.

Para este propósito se debe tener el siguiente soporte tecnológico:

- Espacio de almacenamiento digital donde se tengan los respaldos de las configuraciones de red
- Reportes de errores en la transferencia de información
- Puertos de comunicación libres en cada sede para la utilización de enlaces DSL
- Herramientas y dispositivos necesarios para realizar correcciones y pruebas
- Enlaces telefónicos convencionales a cada una de las sedes
- Sistema de alertas de errores detectados dentro de la red y en áreas físicas como son: alarmas, mails informativos, alertas digitales, sistemas de seguridad eléctricos, cámaras de vigilancia, etc.
- Capacidad de acceso a todas las áreas para el administrador o coordinador del plan de contingencia como son: claves de acceso a dispositivos y áreas físicas

Estos recursos tecnológicos apuntan a brindar a las personas encargadas, detectar, analizar, corregir y documentar los casos de desastre o riesgo que se presenten en la estructura de red diseñada.

6.1.2.4.4 Documentación

El proceso de documentación del plan de contingencia no solo se refiere al modo de actuar ante un desastre, sino también, el registrar aquellos acontecimientos que generen un caos en el funcionamiento de la red. Dentro de la documentación se debe llevar:

- Registro de acciones legales que se presenten
- Bitácoras de mantenimientos o reparaciones de áreas afectadas
- Almacenamiento de reportes que generen los sistemas de control
- Registro de cambios y modificaciones al plan de contingencia y al diseño

6.1.2.4.5 Capacitación

La capacitación del personal que controle la información generada en el plan de contingencia es muy importante. Sin una buena capacitación ninguno de los recursos anteriores sería útil. Se debe capacitar a los interventores del plan de contingencia en las siguientes áreas:

- Diseño de red planteado
- Tecnología WiMAX y redes inalámbricas en general
- Sistemas de reportes y control de red
- Marco legal para enfrentar problemas legales
- Equipos que intervienen en el diseño

- Administración de redes
- Administración de sistemas de información
- Administración de QoS

Dependiendo de la responsabilidad que tenga en el plan de contingencia se deberá adquirir los conocimientos necesarios.

6.1.2.4.6 Recursos financieros

Los recursos financieros realizan el soporte económico para poder poner en marcha cualquiera de las acciones listadas en el plan de contingencia de tal manera que se debe realizar una aproximación del costo que acarrea la ejecución de cualquiera de las medidas a tomarse para la continuidad del negocio:

6.1.2.5- Puesta en marcha del plan

El plan de contingencia esta diseñado para poner en marcha a partir que el sistema se encuentre el la fase de pruebas y mantenimiento.

6.1.3- Pruebas de viabilidad

Para las pruebas de viabilidad del plan de contingencia se deben generar simulacros de ciertos problemas que se pueden presentar.

Estas pruebas de viabilidad se van a generar en la fase de pruebas y mantenimiento.

A nivel de dispositivos de hardware se debe realizar lo siguiente:

- Averiguar en que tiempo el distribuidor cubriría las garantías de los equipos.

- Comprobar la seriedad de los seguros y revisar el tiempo que se demoraría en ejecutarse la póliza.
- Hacer pruebas a los técnicos encargados de las reparaciones de los equipos y capacitarlos también.
- Realizar pruebas para analizar el tiempo de demora para asistir los siniestros.

A nivel de software la principal prueba de viabilidad se va a realizar cuando se ejecute el ethical hacking descrito en el plan de contingencia. Al encontrar situaciones de ese tipo se debe medir lo siguiente:

- Tiempo que se requiere para cargar las configuraciones respaldadas a los equipos
- Tiempo que se requiere para cambiar las configuraciones actuales, y definir nuevas políticas de contingencia
- Tiempo que se requiere para detectar el problema y solucionarlo
- En el caso de necesitar realizar un cambio de frecuencia se debe tomar en cuenta el tiempo de recuperación hasta contratar la nueva.

Los tiempos descritos anteriormente son estimados. Con estas pruebas de viabilidad se generan resultados reales y positivos para respaldo del sistema a implementar.

Todas estas pruebas deben ser documentadas de manera que se pueda describir cuales fueron las acciones tomadas. Se recomienda realizar bitácoras de trabajo.

También se debe tomar en cuenta que estas pruebas no solo se deben realizar una sola vez sino cada cierto período de tiempo, se recomienda que sea

cada 6 meses o cuando las políticas de seguridad y contingencia sean alteradas o modificadas.

6.1.4- Ejecución y recuperación

6.1.4.1- Ejecución

En esta fase se debe tener muy presente que el plan no busca resolver la causa del problema, sino asegurar la continuidad de las tareas críticas de la empresa.

6.1.4.2- Recuperación

Los datos afectados por el siniestro que pudiesen haber quedado desactualizados o corruptos, deben corregirse usando los procedimientos ya definidos.

En general, la reiniciación del proceso normal no implica la cancelación del alternativo, salvo que deban utilizarse los mismos recursos. Si esto no es así, durante cierto tiempo, los procesos deberían ejecutarse en paralelo para asegurar que la reiniciación de la operación normal es correcta y, ante cualquier defecto, continuar con el de contingencia.

Una vez finalizado el plan, es conveniente elaborar un informe final con los resultados de su ejecución cuyas conclusiones pueden servir para mejorar éste ante futuras nuevas eventualidades.

CAPITULO VII: Conclusiones y Recomendaciones

1. La evolución de la tecnología va a la par de las necesidades, el problema de los cables hizo que el advenimiento de sistemas inalámbricos se acelere. Lo importante es que exista interoperabilidad entre redes cableadas e inalámbricas. Sería complicado si cada tecnología que aparece sea incompatible con la existente ya que se debería invertir grandes cantidades de dinero.

2. La modulación OFDM ha venido desarrollándose varios años por lo tanto es suficientemente robusta, de tal manera que la forma de comunicación que utiliza la tecnología WiMAX es efectiva. Al optimizar el uso del canal basándose en la ortogonalidad de las señales es más fácil la detección y corrección de errores y permite implementar QoS. Es muy importante darse cuenta que la sub utilización del canal solo se da en el momento que se introduce el “intervalo de espera” para diferenciar cada una de las portadoras en la transmisión OFDM.

3. El estándar IEEE 802.16x es la evolución de otros estándares como los de la familia 802.11x. Cubriendo las falencias que se presentaban en el momento de la interconexión y seguridad de la transferencia. El estándar 802.16 supera el problema de interferencias con el mencionado DFS (Dynamic Frecuency Selection), selección dinámica de frecuencias.

4. Un punto a destacar muy importante contrario a otras tecnologías inalámbricas es el manejo de capas para la transmisión y recepción de paquetes. Esto permite asegurar la integridad de la información especialmente al poseer una sub-capa de seguridades que se encarga de la autenticación, procesamiento e intercambio de llaves.

5. Si bien la tecnología WiMAX ha generado grandes resultados en el momento de cubrir necesidades como distancias y atenuación, el principal propósito para superar a otros estándares inalámbricos, es el poder implementar movilidad entre los dispositivos (handover), la variación 802.16e del estándar trata de cubrir este vacío que han generado otras tecnologías de su clase.

6. En el campus Sangolquí es la única sede donde se encuentra en funcionamiento una red inalámbrica. La implementación de una red WiMAX para beneficio directo de los usuarios como son personal administrativos y estudiantes no es óptimo por los costos que implica los equipos suscriptores. Por esto, el hecho que WiMAX sea basado en tecnologías inalámbricas ya conocidas como WiFi, permite la interconexión con lo existente actualmente. Además, se debe tomar en cuenta que no sólo Internet y un sistema escoláticos son los servicios que debería obtener una sede sino también video conferencias, e-learning, VoIP.

7. Se recomienda la utilización e implementación de tecnología WiMAX a fin de abaratar costos y principalmente de manera inmediata mejorar los servicios que se brindan a las diferentes sedes.

8. Las dos propuestas de configuración presentadas soportan las necesidades ya estudiadas de los servicios que se deberían implementar. Aunque la primera propuesta se acoplaría a estas necesidades, la segunda nos haría tomar en cuenta que, si se tiene un buen diseño es más fácil su administración, seguridad y corrección de errores. Es muy importante tomar en cuenta que lo que más se debe cuidar es el no perder la conectividad entre las sedes.

9. Se conoce que hay empresas que ya han contratado ciertas frecuencias que son parte de este estudio. Siendo este el caso se debe sub contratar las bandas a estas empresas o averiguar si el ejército o gobierno no tiene reservadas para el uso de universidades o Instituciones militares como la ESPE.

10. En el momento de hacer pruebas se debe realizar poniendo en caso crítico a los enlaces. Si se toma en cuenta factores como: medio ambiente, distancias, paquetes, servicios, etc., las pruebas resultaran un dato muy similar a los que se obtiene una vez funcionando los sistemas. Es muy importante al instalar y hacer las pruebas también ir de la mano con el proceso de seguridades y plan de contingencias.

11. El control de acceso a los lugares críticos donde se encuentran los equipos o respaldos es muy importante, se debe tomar en cuenta que si físicamente se tienen problemas ninguna de las seguridades lógicas tendrá validez. Así como

se invierte para la implementación tanto en equipos como en documentación, se debe invertir en seguridades y en planes de contingencia.

12. Se deben revisar las políticas de seguridad cada lapso de tiempo, se recomienda que sea cada 6 meses o cuando los planes de contingencia dicten que se deben revisar las políticas de seguridad.

13. Por supuesto uno de los procesos más importantes a seguir en el momento de adoptar los sistemas de seguridad es la capacitación a los usuarios y la administración de la red.

14. La adopción dentro de la institución del estándar 17799 es fundamental para un desempeño eficaz de los sistemas de información que maneja la ESPE, no solo para efectos de este proyecto sino para todo el sistema interno de la institución.

15. Si se tiene la proyección de tener VoIP, Video Conferencias e Internet para todas las sedes, entonces se debe basar en esto para el proceso de administración de desastres. Siempre se debe documentar los cambios y las acciones que se hayan tomado en el momento de ejecución de un riesgo, también si las políticas de seguridad varían, generarán cambios para el plan de contingencia.

BIBLIOGRAFÍA

- Alejandro Delgado Gutiérrez. (2002). Transmisión de Señales de de TV Digital en el estándar terreno DVB-T. Universidad Politécnica de Madrid.
- Anónimo. (2004). Introducción Al Código De Corrección De Errores. http://personales.mundivia.es/jtoledo/angel/error/error1.htm
- Roger B. Marks. (2004). Developing the IEEE 802.16 **WirelessMAN**® Standard for Wireless Metropolitan Area Networks. http://grouper.ieee.org/groups/802/16/index.html
- Feedback Networks Technologies. (2005). Errores frecuentes en las encuestas: ¿Cómo calcular la muestra correcta? http://www.feedbacknetworks.com/cas/experiencia/sol-preguntar-calcular.htm
- D-Link LatinAmerica. (2004). Descripción DWL-2100AP. http://www.dlinkla.com/home/productos/descripcion.jsp?id=3&idp=497&sm=4&sf=13
- Wi-LAN Inc. (2005). LibraMX Specifications. http://www.wi-lan.com/products/libramx.htm
- Airspan Communications, Ltd. (2005). Products Overview. http://www.airspan.com/products_main.aspx
- Luciano Moreno. (2005). Criptografía (VII) http://www.htmlweb.net/seguridad/cripto/cripto_7.html
- GFI Development Group. (2005). LanGuard Description http://www.gfi.nu/es/lannetscan/lanscan6manual_es.pdf
- Internet Solutions. (2005). Seguridad Informática. http://www.internet-solutions.com.co/seginformatica.html
- Anónimo. (2004). ¿Está su empresa preparada ante incidentes imprevistos?

http://www.virusprot.com/Art4.html

- Intel Corporation. (2005). Tecnologías inalámbricas de banda ancha. http://www.intel.com/cd/network/communications/emea/spa/179913.htm
- Intel Corporation. (2005). Conectividad de la banda ancha. http://www.intel.com/cd/personal/computing/emea/spa/entertainment/broadband/index.htm
- Intel Corporation. (2005). Intel and WiMAX. http://www.intel.com/standards/case/case_wimax.htm
- Eliot Weinman. (2005). WiMAX Trends: State of the Industry. http://www.wimaxtrends.com/articles/excerpt/e100205a.htm
- Beth Cohen and Debbie Deutsch. (2003). 802.16: A Look Under the Hood. http://www.wi-fiplanet.com/tutorials/article.php/10724_3068551_3
- Advento Networks. (2005). Cálculos para enlaces wireless. http://www.e-advento.com/tecnologia/calculos.php
- Micro Alcarria. (2004). Cálculos para realizar un enlace gíreles. http://www.microalcarria.com/miscelanea/calculos_enlace_wireless
- Leo DaCruz. (2005). Wimax, la Internet inalámbrica del futuro http://www2.noticiasdot.com/publicaciones/2005/0205/1802/noticias180205/noticias180205-21.htm
- Intel Corporation. (2005). WiMAX en la India. http://www.intel.com/espanol/update/contents/wi11041.htm
- Victor E. Cappuccio. (2004). Plan de Contingencia para sistemas informáticos http://www.ilustrados.com/publicaciones/EplpVpEEkVSEGPFgcg.php

GLOSARIO DE TERMINOS

AAS Adaptive Antenna Systems, sistemas de antenas inteligentes.

AES Advanced Encryption Standard, encriptación de datos avanzada.

ARQ Automatic Repeat Request, petición de repetición automática.

Backhaul Backbone de redes inalámbricas.

BE Best Effort Services.

BR Bandwidth Request, petición de ancho de banda.

BS Base Station, estación base.

CBR Constant Bit Rate, tasa de transferencia constante.

CS Service-Specific Convergence Sublayer, capa de convergencia de servicios

DCD DL Channel Descriptor, descriptor del canal DL.

DES Data Encryption Standard, encriptación de datos estándar.

DFS Dinamic Frecuency Selection, selección de frecuencia dinámica.

DL Downlink, recepción.

DSL Digital Subscriber Line, línea de suscripción digital.

Ghz Gigahertz, gigaherzios.

IEEE Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Eléctricos Y Electrónicos.

IP Internet Protocol, protocolo de Internet.

LAN's Local Area Networks, redes de área local.

LOS Line Of Sight, línea de vista.

MAC Medium Access Control, control de acceso al medio.

MAN Metropolitan Area Networks, redes de área metropolitana.

NLOS Non line of sight, sin línea de vista.

NrLOS Near Line of Sight, línea de vista casi directa.

nrtPS Non-Real-Time Polling Services.

OFDM Orthogonal Frequency Division Multiplexing, Multiplexación por división ortogonal de frecuencia.

PDU Package Data Unit, unidad de paquete de datos.

PHY Physical, física.

PtMP Point to Multi-Point, conexiones punto-multipunto.

PtP Point to Point, conexión punto-punto.

Polling Sondeo, forma de control en redes de comunicaciones.

QoS Quality of Service, calidad de servicio.

rtPS Real-Time Polling Services.

SAP Service Access Point, punto de acceso a servicio.

SDMA Spatial Division Multiple Access, Acceso Múltiple por División de Espacio.

SS Subscriber Station, estación remota.

STC Space Time Coding, codificación espacio-tiempo.

UCD UL Channel Descriptor, descriptor del canal UL.

UGS Unsolicited Grant Services, concesión de servicios no solicitados.

UL Uplink, envío.

VoIP Voice over IP, voz sobre IP.

WEP Wired Equivalency Privacy, privacidad equivalente a cableado

WiFi Wireless Fidelity, fidelidad inalámbrica.

WiMAX Worldwide Interoperability for Microwave Access, Interoperabilidad Mundial para Acceso por Microondas.

WPA WiFi Protected Access, acceso protegido WiFi

ANEXOS

Anexo A- Formato de la encuesta realizada a los usuarios de la red de la ESPE

Facultad de Ingeniería en Sistemas e Informática
GRADO DE SATISFACCIÓN Y CONOCIMIENTO DE LOS USUARIOS
DE LA RED DE DATOS DE LA ESPE

OBJETIVO:

Determinar el grado de satisfacción y conocimiento de los usuarios de la red de datos de la ESPE.

INSTRUCCIONES

Lea detenidamente las preguntas y respóndalas con total franqueza marcando con una "x" las opciones de su agrado.

DATOS DE IDENTIFICACIÓN			**FECHA:**
FACULTAD:	**NIVEL:**	**EDAD :**	**SEXO:** O Femenino O Masculino

1. Ha utilizado usted la red de la ESPE?	O Si O No Porqué? _____ _____
2. Que servicios de la red de la ESPE ha utilizado?	O Internet O Transferencia de Archivos O Mail - ESPE O Programas en red O Otros : _____
3. ¿Cómo considera usted el funcionamiento de la red informática interna de la ESPE?	O Excelente O Buena O Mala O Porqué? _____ _____
4. ¿Ha tenido acceso a la red inalámbrica de la ESPE?, en el caso de ser no marque uno de los motivos?	O Si O No (indique el porque) Falta equipos Falta cobertura
5. La cobertura de la red inalámbrica de la ESPE es:	O Alta O Media O Baja O No existe
6. ¿Cuál de estos servicios considera usted que la ESPE debería brindar a los usuarios de su red informática?	O Video conferencia entre las sedes O Telefonía IP para las sedes O Movilidad para los clientes O Internet de alta velocidad
7. Sabia que Tecnología WiMAX es: Tecnología inalámbrica de alta velocidad con gran ancho de banda para largas distancias	O Si O No
8. ¿Que uso le daría a una red WiMAX?	O Video conferencia O Internet O Sistemas administrativos O Conexión Sedes O Otros _____

BIOGRAFIA

CESAR CHAVEZ

Mi nombre completo es César Francisco Chávez Cevallos, nací en la hermosa ciudad de Quito, capital del Ecuador.

Mis estudios primarios los realicé en el Colegio Borja No 2, los secundarios en el Colegio Básico Marista y la especialización en el Colegio Diversificado Marista obteniendo la especialización de Físico-Matemático con una calificación promedio general de 16.07

Mis estudios superiores los empecé en la ESPE en marzo de 2000 y egresé de la misma en febrero de 2005 con un promedio general de 16.33.

Actualmente trabajo en mi propia empresa que brinda soluciones mediante Tecnologías de Información.

Esta debe incluir el lugar y la fecha de nacimiento, las instituciones en las que cursó los estudios, los títulos obtenidos (con fechas) y los honores obtenidos (no más de una página).

MIGUEL RICLE

Soy Miguel Raúl Ricle Vargas, nací en quito. Mi madre Quiteña y mi padre Porteño (Argentino). Mis estudios escolares y secundarios fueron en el colegio T.W.Anderson, obteniendo el bachillerato en ciencias de la informática, con un promedio general de 17 en el año de 1998.

Curse un año en la Facultad de Ingeniería en la Universidad de Buenos Aires y en el año 2000 ingresé a la ESPE.

Tras 5 años de estudio concluí la carrera de ingeniería obteniendo un promedio de calificaciones al egresar de 16,69.

Actualmente tengo mi propia empresa de brinda soluciones de tecnología de información y Gerencio el área de producción de una empresa de mubles cormados llamada CRONIC Cromo y Niquel del Ecuador.

HOJA DE LEGALIZACION DE FIRMAS

ELABORADO POR

_____
Miguel Raúl Ricle Vargas

_____
César Francisco Chávez Cevallos

DECANO DE LA FACULTAD DE INGENIERIA

_____
Tcrn. De E.M. Marco Quintana

Sangolquí, 30 de enero de 2006