ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"ENLAZAR DOS EDIFICIOS INALÁMBRICAMENTE PARA HABILITAR OFICINA PUBLICA DEL BANCO CENTRAL EN LA CIUDAD DE GUAYAQUIL"

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del GRADO de:

INGENIERO EN ELECTRICIDAD.ELECTRONICA

DAVID ALBERTO MENDOZA JAENS

GUAYAQUIL – ECUADOR

AÑO: 2015

AGRADECIMIENTO

Mi agradecimiento a todos quienes hicieron posible finalizar de manera exitosa la Carrera de Ingeniería iniciada hace 37 años en la ESPOL.

En orden de importancia de acuerdo a mis creencias y formación religiosa agradezco a Dios, mis padres, esposa e hijos. A los profesores de la FIEC, muy en especial a los Ingenieros Yapur, Medina, Villao.

A mis compañeros y amigos del Banco Central que siempre hicieron fuerza común por mantener actualizados mis conocimientos y fueron mi apoyo para concluir exitosamente la carrera.

DEDICATORIA

Este trabajo está totalmente dedicado a todas las personas que creyeron en mí, durante todo mi desempeño profesional en las Instituciones donde laboré y en especial a mi familia que siempre me estuvo alentando a graduarme y conseguir un título profesional que avalice todas las labores realizadas.

TRIBUNAL DE SUSTENTACIÓN

Ph.D. Freddy Villao Q.

EVALUADOR

Mg. Miguel Molina

EVUALUADOR

DECLARACIÓN EXPRESA

"La responsabilidad por los hechos, ideas y doctrinas expuestas en este Informe me corresponde exclusivamente; y, el patrimonio intelectual de la misma, a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

(Reglamento de Graduación de la ESPOL).

David Alberto Mendoza Jaéns

RESUMEN

Debido a cambios propuestos por el Gobierno Actual, el Gerente General del Banco Central, debió reubicar al personal que laboraba en las oficinas ubicadas en el edificio principal en 9 de Octubre 200 y Pichincha, donde funcionaba el Dpto. de Coactiva en Guayaquil, ante este inminente cambio la parte tecnológica se vio involucrada en el reto de procurar mantener el nivel de servicio de los funcionarios que fueron reubicados, con la finalidad que desempeñen sus funciones con normalidad, esto implicó asumir retos tecnológicos emergentes y efectivos, para el área de comunicaciones equipo multidisciplinario al cual pertenezco, la población institucional quedó dividida en tres edificios, edificio Ex Suizo, Edificio Ex Previsora y Edificio CFN. En el edificio Ex Previsora, que era la nueva ubicación, se ocuparon los pisos 11, 16 y 17; mientras el Centro de Datos quedó en el edificio CFN.

Para poder mantener el uso de los aplicativos en los tres edificios, se lanzó una fibra óptica entre los edificios CFN y Ex Suizo; y para dar servicio a 50 personas ubicadas en el edificio ex Previsora conservando el nivel de servicio, manejo de aplicativos, correo electrónico y acceso a Internet; implementamos una red inalámbrica, que permita mantener la integridad y seguridad de la información.

Para comunicar los edificios se usó equipos inalámbricos, debido que el cableado usando cable UTP o fibra óptica, no fue posible realizarlo por la situación geográfica de los edificios y los regulaciones que expide el Municipio en las zonas regeneradas. Las investigaciones para implementar la solución se inició en el 2010, utilizando la mejor solución tecnológica para el presente caso, misma que funciona hasta la presente; los usuarios se han incrementado a 200, para lo cual se incrementó una antena adicional, que permitía minimizar los problemas de

interrupción de servicio y lentitud de respuesta. En la actualidad, los usuarios de ambos edificios incrementaron los siguientes servicios:

- Sistema de Video Conferencia Nacional.
- Supervisión y mantenimiento de Control de Acceso y Sistema de Seguridad Electrónica (DVR y cámaras de seguridad).
- Sistema de Administración Documentaria y Digitalización de Documentos.

ÍNDICE GENERAL

INTRODUCCIÓN

Los funcionarios del Banco Central laboramos en un edificio de 16 pisos ubicado en 9 de Octubre 200 y Pichincha desde 1980 hasta el año 2009, en ese año el edificio fue entregado a la CFN. Un grupo de funcionarios, que dan atención a usuarios externos fueron reubicados en los pisos 11, 16 y 17 del edificio Ex Previsora, ubicado en Malecón y 9 de Octubre.

Para seguir desarrollando sus actividades los funcionarios trasladados deben mantener operativos sus sistemas informáticos, entre los cuales se encuentran los programas de Recursos Humanos, sistema de inventarios, aplicativos desarrollados por técnicos de la Institución, sistema de correo electrónico y acceso a Internet. Las actividades que se desarrollan desde equipos computacionales, se deben seguir desarrollando cumpliendo las políticas internas y siguiendo las normas descritas en los procedimientos del Subproceso de Seguridad Informática, por lo cual deben conservar los mismos perfiles de acceso a la red, que como usuarios utilizaban en la ubicación anterior.

Realizamos el levantamiento de información y empezamos a elaborar los cronogramas para comunicar los edificios pues la reubicación tenía carácter de urgente.

Durante el análisis se presentaron tres propuestas técnicas, que inmediatamente las resumo:

La primera opción, fue extender la LAN del BCE utilizando cable UTP blindado, a través de los postes del sector; esta situación no se ejecutó, pues las ordenanzas emitidas por la Administración Municipal a cargo de la Regeneración Urbana en el Centro de Guayaquil, prohíben la instalación de todo tipo de cables aéreos.

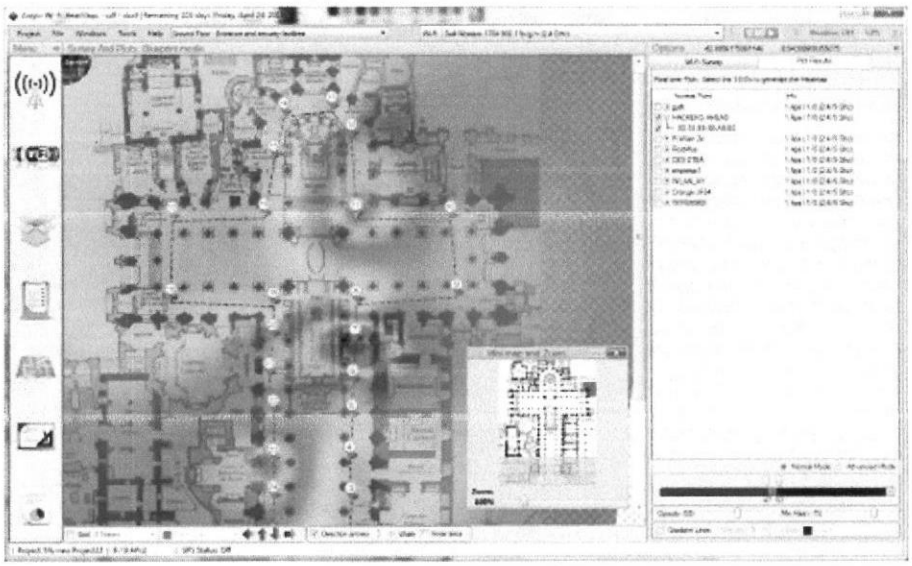
La **segunda opción**, se propuso enlazar los edificios usando fibra óptica subterránea, a través de los ductos existentes; pero tampoco fue factible realizar esta propuesta, debido a que los ductos que unen los edificios de manera subterránea, estaban saturados con cables telefónicos, eléctricos y fibra óptica de las Instituciones financieras y bancarias del sector bancario.

La tercera opción propuesta, consistió en implementar un enlace inalámbrico entre los edificios la misma que resultó ser la más idónea luego del análisis tecnológico realizado, esta solución utiliza TDMA (Time-Division Multiple Access, acceso múltiple de división de tiempo, las características principal es la de preservar todo el ancho del canal, pero lo divide en espacios de tiempo alternados, durante los cuales puede transmitir cada uno una llamada individual. Esta tecnología permite velocidades reales de TCP/IP para exteriores de más de 150 Mbps y consiste en un diseño de vanguardia de hardware de radio, antenas MIMO de estación base de clase portadora, utilizando un potente protocolo TDMA que ofrece velocidad y escalabilidad de red sobre distancias de enlaces de varios kilómetros. (Ubiquitti, 2011).

CAPÍTULO 1

1.1 ANALISIS TECNICO

Una vez que las Autoridades aprobaron la propuesta de implementación del enlace mediante dispositivos wi-fi, iniciamos el levantamiento de información, para definir los parámetros técnicos y los equipos que se debía utilizar para implementar la solución, para conocer los rangos de frecuencia más usados en el sector y evitar conflictos e interferencias se utilizó como site survey el software Acrilic Wifi, tal como se muestra en la Fig. 1.1, con lo que se determinó que la frecuencia menos utilizadas en el sector era 2346, utilizado como umbral RTS en la antena.



Fuente: Pantalla del Software Acrilyc_WiFi

Figura 1.1 : **Site Survey**

Ubicación geográfica de edificios.-

El edificio CFN está ubicado en 9 Octubre 200 entre Pichincha y Pedro Carbo, Latitud 2° 11' 30.95" S, Longitud 79° 52' 49.47" W, este edificio será llamado, "**edificio principal**".

El edificio Ex Previsora está ubicado en 9 Octubre y Malecón. Latitud 2° 11' 32.06" S, Longitud 79° 52' 47.38" W , este edificio será llamado **"edificio secundario"**, es la nueva oficina de los usuarios re-ubicados.

Los edificios están en el centro de Guayaquil, separados por la calle Pichincha.

El edificio CFN tiene toda la infraestructura informática operativa.

El edificio Ex Previsora tiene tres pisos entregados al Banco Central, cuyas oficinas están disponible para ser ocupadas por los funcionarios del área de Recuperación y Liquidación que serán reubicados.

Información de usuarios y aplicativos utilizados.-

La información que maneja cada usuario es variable, pero en promedio se considerará 0.4 Mb correspondiente a sistemas y aplicativos de la Institución; a lo que se debe añadir el uso de Internet e información relacionada.

El objetivo principal es que los usuarios sigan realizando sus actividades, como si aún estuvieran en el edificio principal y que su nueva ubicación no se transforme en un problema para la trasmisión de datos, sabiendo que la Institución presta servicio a usuarios externos.

Análisis técnico para escoger dispositivo de comunicación.

Las condiciones mínimas de funcionamiento del enlace, debían considerar el cumplimento de los siguientes parámetros técnicos:

- Se debía definir nuevos segmentos de red para la nueva ubicación, inicialmente pensamos colocar un firewall y definir un nuevo segmento de red, pero no se dio.
- Latencia mínima.
- Trasmisión de datos sin errores.
- La información debía llegar integra a su destino.

- El ancho de banda de los equipos, debía considerar incremento de servicios y usuarios, sin desmejorar tiempo de respuesta.
- Se debía considerar un plan de contingencia de equipos de comunicación.

Cabe indicar que la Institución implementó enlaces entre oficinas remotos ubicadas dentro del perímetro urbano, pero alejadas del casco comercial por lo que se tomó como punto de partida esos análisis anteriores; aunque el volumen de información y la transaccionalidad de esos enlaces eran diferentes.

Del levantamiento de información, en lo referente a cantidad y tipo de usuarios, clase de información a transmitir, volumen de información y frecuencia, obtuvimos parámetros que nos permitieron escoger el equipo con mayor eficiencia en el mercado, para nuestra situación en particular.

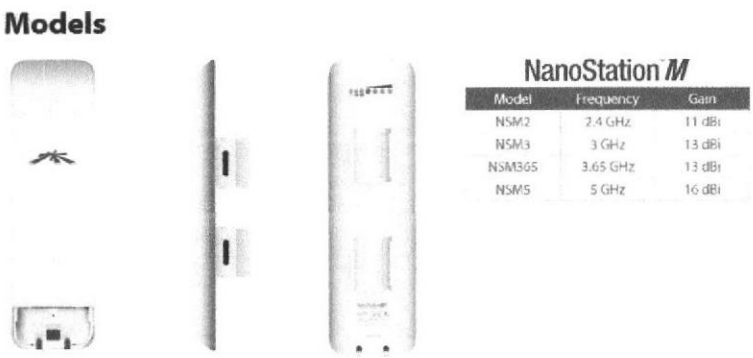
Teniendo en cuenta los servicios y cantidad de información que se debía trasmitir, se buscó soluciones que cumplan las mejores prácticas de comunicación inalámbrica, normas Itil, Iso 27000.

Se consideró la ubicación física en los edificios, que iban a alojar los equipos, para escoger el modelo, pues los edificios están ubicados entre otros edificios de gran altura.

Con los datos de los usuarios calculamos parámetros tales como, ancho de banda, ganancia, potencia máxima de salida, tipo de antena, tanto para la estación de origen, como para la de destino.

Basados en los cálculos planteados, pruebas y experiencias al implementar enlaces de comunicaciones similares para comunicar Espacios Culturales administrados por la Institución, decidimos utilizar las antenas Nano M5, fabricadas por Netware Ubiquiti, mostradas en la fig. 1.2 equipos que de acuerdo a las referencias técnicas, habían sido probados en situaciones ambientales y físicas similares a nuestro caso, con resultados altamente eficientes.

Las antenas Nano, tienen las siguientes ventajas de funcionamiento:



Fuente: DataShet del Fabricante

Figura 1.2: **Modelos Antenas**

- Es un dispositivo WI-FI que funciona como Router.
- Puede ser usado como cliente o como AP.
- Si se lo usa como receptor de datos los resultados tienen el 100% de efectividad.
- No los afectan los cambios climáticos, agua, sol viento, etc.
- El modelo M5 escogido cubre hasta 20 Km, por la gran potencia del dispositivo.

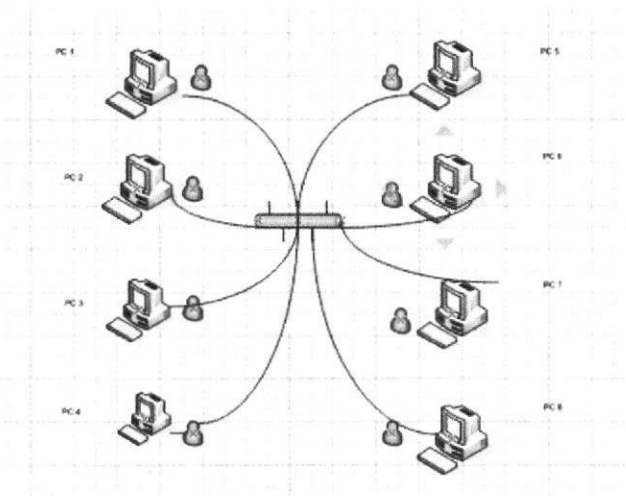
- La frecuencia a la que trabaja el Nano/m5, para esas fechas no estaba saturada, no así modelos anteriores como el m1 y m2, por lo que no afectarían interferencias provocadas por otros dispositivos inalámbricos instalados en la zona.
- Son configurables, tal como los Router; se definieron parámetros de comunicación de acuerdo a nuestra necesidad.
- En el panel de configuración se puede monitorear y configurar los siguientes parámetros:
  - Tiempo que lleva encendido el equipo
  - Forma como se lo ha instalado (vertical, horizontal, o inclinado).
  - Direcciones IP de la Lan y de los dispositivos wi-fi.
  - Permiten ejecutar ping.
  - Permite alinear antenas.
  - Monitorear estado de la conexión.
  - Realizar pruebas de velocidad de transferencia.
  - El software permite monitorear todas las redes existentes en el medio.
  - La potencia es configurable, para evitar los ruidos e interferencias, por la cercanía entre equipos de alta potencia.

Configuración e instalación de los dispositivos

Conociendo las bondades técnicas de las antenas Nano M5, se procedió a:

- Configurar el dispositivo, con las direcciones IP correspondientes a los siguientes equipos:
- Servidor al que se va conectar en el edifico CFN.
- Gateway de salida hacia el nuevo segmento de red.
- Habilitación y definición de SSID y WAP2 - PSK para dar seguridad a la trasmisión de datos.
- Parámetros de ubicación física del dispositivo.
- Configurar el dispositivo nano m5, con las direcciones IP de:
- Nuevo segmento de red.
- Gateway de salida hacia edificio "A".
- Parámetros de ubicación física del dispositivo.
- Instalar el dispositivo de comunicación en la terraza del edificio CFN y conectarlo al swicht que lo enlaza con la red de la Institución.
- Instalar el dispositivo de comunicación en la ventana del piso 11 del edificio "B" y conectarlo al switch que lo enlaza con la red de equipos del nuevo segmento de red.
- Alinear las antenas.

- Simultáneamente, se elaboró el cableado estructurado para los 50 usuarios iníciales del nuevo segmento de red, a los que se les configuró los parámetros de comunicación correspondientes, de acuerdo a lo mostrado en la fig 1.3.



Fuente: Elaborado por el autor

Figura 1.3 **Diseño de Red**

- Pruebas de trasmisión de datos a los sistemas, correo institucional y salida al Internet en tiempo real de los usuarios del nuevo segmento.

Permiso de funcionamiento (SENATEL)

Con la finalidad de cumplir con el marco legal, que permite la implementación de una red inalámbrica, se solicitó a Senatel el permiso de uso de frecuencias, para lo cual se entregó la siguiente información, correspondiente a los parámetros de funcionamiento de los dispositivos de comunicación que forman parte de la red inalámbrica. (Ver Anexos)

Los datos de los equipos que se utilizaron en la implementación de la red inalámbrica que unió los edificios mencionados, como se muestra en las tablas 1.1 y 1.2.

Tabla 1.1: **Datos de la Antena**

Características Técnicas	Antena 1	Antena 2
Marca	Ubiquiti	Ubiquiti
Modelo	15-211	15-211
Rango de Frecuencias (Mhz)	5470-5725	5470-5725
Tipo	Panel	Panel
Impedancia (ohmios)	50	50
Polarización	Vertical	Vertical
Ganancia (dbd)	12.85	12.85
Azimut de radiación Máxima (°)	117.78	297.78
Angulo de elevación (°)	16.08	16.08
Altura Base Antena (mts)	15	36

Fuente: Datashet del Fabricante

Tabla 1.2: **Datos de los Equipos**

Tipo de Estación	**Fija**	**Fija**
Marca	Ubiquiti	Ubiquiti
Modelo	Nanostation 5	Nanostation 5
Ancho de Banda	20 Mhz	20 Mhz
Tipo de Modulación	OFDM	OFDM
Velocidad de Trasmisión (Kbps)	25.000	25.000
Potencia de salida (watts)	0.5	0.5
Rango de Operación (Mhz)	5470 - 5825	5470 - 5825
Sensibilidad (dbm)	´-86 dBm	´-86 dBm
Máx desviación de frecuencia (khz)	15.0	15.0

Fuente: Datashet del Fabricante

El primer piso que ocuparon los funcionarios fue el piso 11 del edificio Ex Previsora, por lo que colocamos una antena en la ventana del piso 4to del edificio CFN enlazada con una antena ubicada en el piso 11 del edificio Ex Previsora.

Luego se incrementó la cantidad de usuarios y se los ubicó en el piso 16 del edificio Ex Previsora, e inicialmente se utilizó el mismo enlace, pero la velocidad de trasmisión disminuyó y se incrementó el tiempo de respuesta, por lo que decidimos implementar otro enlace de igual característica que el anterior, por lo que montamos otra antena en el piso 4to del edificio CFN enlazada con otra ubicada en el Piso 16 de la Previsora.

De esta manera se creó dos enlaces alternos, balanceando el uso de los canales y mejorando la perfomance, adicionalmente se creó un anillo de redundancia, uniendo las antenas del piso 11 con las del 16 mediante cable UTP, para que en caso de

falla de uno de los enlaces, toda la carga transaccional viaje por el canal que permanezca activo.

Protección de la red inalámbrica.-

La antena NANO incluye como parámetros configurables, sistemas para proteger la antena y la información que se transmitirá, estos parámetros se escogerán de acuerdo a la necesidad de precautelar los datos institucionales. (Penalva, 2009)

Seguridades de la conexión de red.-

El **SSID** (**S**ervice **S**et **ID**entifier) es un nombre incluido en todos los paquetes de una red (Wi-Fi) para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres que la mayoría de las veces son alfanuméricos (aunque el estándar no lo especifica, así que puede consistir en cualquier carácter). Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

Existen algunas variantes principales del SSID. Las redes ad-hoc, que consisten en máquinas cliente sin un punto de acceso, utilizan el BSSID (**B**asic **S**ervice **S**et **ID**entifier); mientras que en las redes en infraestructura que incorporan un punto de acceso, se utiliza el ESSID (Extended Service Set Identifier). Nos podemos referir a cada uno de estos tipos como SSID en términos generales. A menudo al SSID se le conoce como nombre de la red.

Uno de los métodos más básicos de proteger una red inalámbrica es desactivar la difusión (broadcast) del SSID, ya que para el usuario medio no aparecerá como una red en uso. Sin embargo, no debería ser el único método de defensa para proteger

una red inalámbrica. Se deben utilizar también otros sistemas de cifrado y autentificación.

Wi-Fi Protected Access, llamado también ***WPA*** (en español «Acceso Wi-Fi protegido») es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo, Wired Equivalent Privacy (WEP). Los investigadores han encontrado varias debilidades en el algoritmo WEP (tales como la reutilización del vector de inicialización (IV), del cual se derivan ataques estadísticos que permiten recuperar la clave WEP, entre otros). WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. WPA fue creado por la Wi-Fi Alliance (Alianza Wi-Fi).

WPA adopta la autenticación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red. Para no obligar al uso de tal servidor para el despliegue de redes, WPA permite la autenticación mediante una clave precompartida, que de un modo similar al WEP, requiere introducir la misma clave en todos los equipos de la red.

WPA2 (*Wi-Fi Protected Access 2* - Acceso Protegido Wi-Fi 2) es una versión mejorada, creada para corregir las vulnerabilidades detectadas en WPA.

WPA2 está basada en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de "migración", no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i.

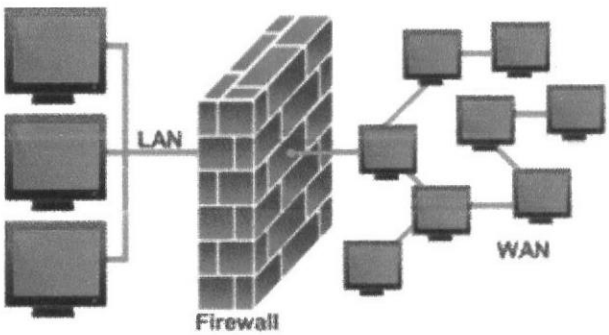
Los fabricantes comenzaron a producir la nueva generación de puntos de accesos apoyados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES (Advanced Encryption Standard). Con este algoritmo será posible cumplir con los requerimientos de seguridad del gobierno de USA - FIPS140-2. "WPA2 está idealmente pensado para empresas tanto del sector privado cómo del público. Los productos que son certificados para WPA2 le dan a los gestores de TI la seguridad que la tecnología cumple con estándares de interoperatividad". Si bien parte de las organizaciones estaban aguardando esta nueva generación de productos basados en AES es importante resaltar que los productos certificados para WPA siguen siendo seguros de acuerdo a lo establecido en el estándar 802.11i.

Considerando las opciones de configuración, con la finalidad de proteger el enlace inalámbrico habilitamos el SSID y el WPA2-PSK.

Escogimos encriptación WPA2-PSK por ser más robusta y presentar un nivel más complicado de violentar, comparada con la opción WPA, misma que era más sencilla de hackear por tener una cadena de bits limitada. En cambio la tecnología WPA2-PSK combina la tecnología anterior con una nueva llave de encriptación cuya longitud es de 63 caracteres; otra característica que presenta este tipo de encriptación es la obligatoriedad del cambio frecuente de la clave de acceso, lo cual impide a los hackers trabajar libremente en el intento de violación de las redes inalámbricas.

Protección de la Información.-

Un **cortafuegos** (***firewall***) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas, como se muestra en la fig. 1.4.



Fuente: Elaborado por el autor

Figura 1.4 **Red Firewall**

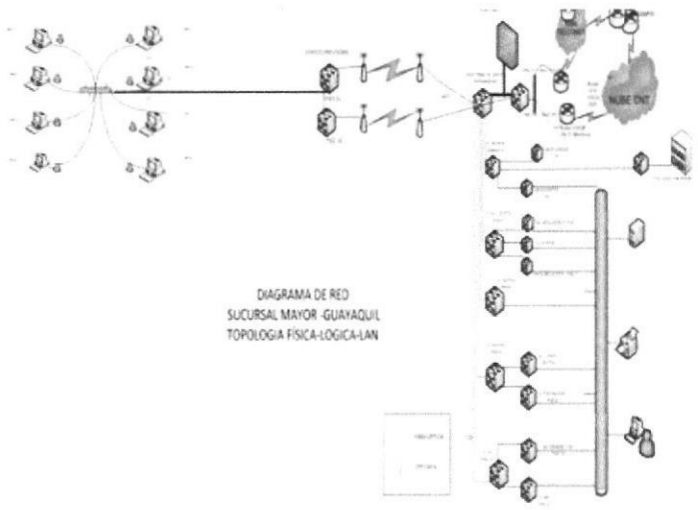
Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o en una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la

intranet pasan a través del firewall, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar el firewall a una tercera red, llamada zona desmilitarizada *o* DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un firewall correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

Para nuestro caso se añadió los usuarios a FORTINET, dispositivo de capa 4, que actúa como Router, Firewall, Proxy, Antispam (control de contenido, control de navegación y antipishing). En la fig. 1.5 se muestra el Diagrama de red.



Fuente: Elaborado por el autor

Figura 1.5 **Diagrama de Red**

CAPÍTULO 2

2.1 SERVICIOS DE TI INCORPORADOS.

Luego de la implementación del cableado estructurado, creación de un nuevo segmento de red, configuración de equipos de comunicación, instalación de las antenas en cada edificio, alineamiento de las antenas, la comunicación entre servidores y usuarios de ambos edificios se desarrolló de manera satisfactoria.

En la actualidad, existen 200 usuarios conectados a los que se han incrementado otras áreas de la Institución y la comunicación se realiza de manera eficiente, no hay pérdida de información, no hay retraso en el envío de paquetes, no se han vulnerado las seguridades implementas.

Por lo que el resultado de la implementación del enlace inalámbrico se constituye en un éxito total.

Segmento de red funcionando con 200 usuarios.

Los servicios disponibles para los usuarios son los siguientes:

- Aplicativos administrativos, control de inventarios, recursos humanos, sistema de cobro coactivo, sistema gestión legal.
- Correo electrónico, plataforma Lotus Notes.
- Navegación a Internet.
- Portal Corporativo de Servicios.
- Sistema de Control de Asistencia y Vacaciones.

Sistemas adicionales implementados.

De esta manera, se cumplió el requerimiento solicitado; pero los usuarios a medida que la tecnología avanza, solicitan nuevos servicios, por esta razón se implementó los servicios de:

- Video Conferencia Nacional
- Seguridad electrónica, a través de DVR y cámaras de seguridad ubicadas en lugares estratégicos, para dar seguridad al personal y a la información física.
- Control de Acceso para áreas restringidas, donde se guardan valores y documentos reservados.

CAPÍTULO 3

3.1 CONFIGURACION Y MONITOREO DE LAS ANTENAS

Operatividad del Servicio.-

Para tener un rendimiento eficiente del enlace debemos considerar dos puntos relevantes:

1. Verificar la línea de vista entre los sitios donde colocaremos las antenas.
2. Realizar un análisis de las frecuencias mas utilizadas (saturadas)del sector donde se implementará el enlace inalámbrico, para definir el umbral de frecuencia de operación de nuestro enlace.

A continuación mostraré pantallas de configuración y afinamiento de parámetros de funcionamiento de las antenas Nano 5, para tener una idea más clara del funcionamiento.

Pantallas de configuración de las Antenas NANO

Todos los parámetros de los equipos son configurables por software, adjunto pantallas de configuración de los principales, que me permiten afinar el sistema al mejor funcionamiento.

Algunos de los parámetros configurables son:

- Umbral RTS
- Datos Multicast
- Control EIRP
- Umbral de sensibilidad
- Velocidad de LAN
- Modo de Red
- Elegor modo de operación del equipo: Router , AP.

Reportes de rendimiento de las antenas

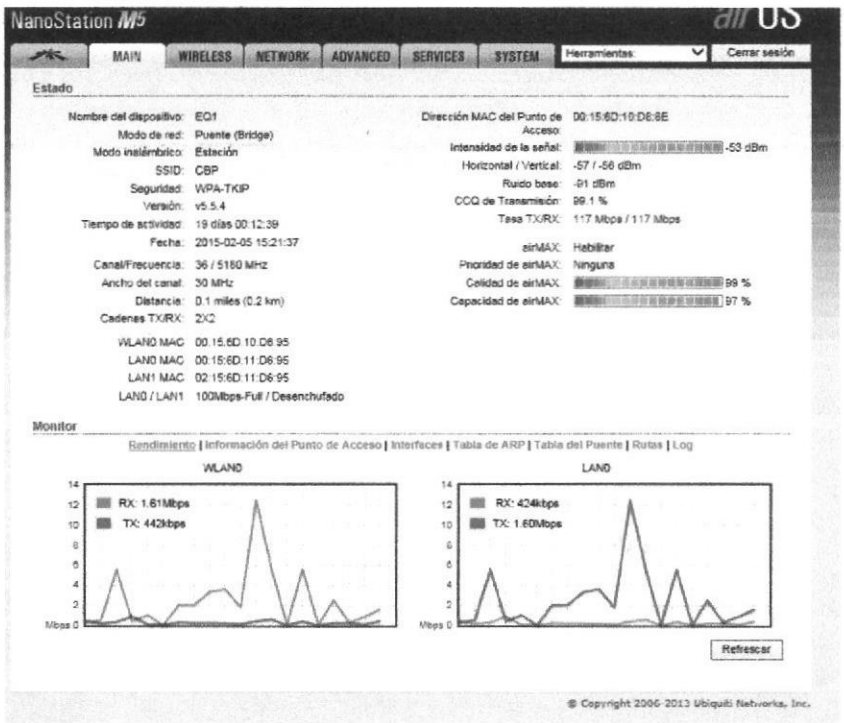
Ahora que las antenas están en producción, es posible monitorear el uso y rendimiento de cada parámetro.

- Intensidad de la señal.
- Rendimiento de la Red
- Información del Punto de acceso.

- Tabla ARP.
- Ruido Base.
- Rutas.

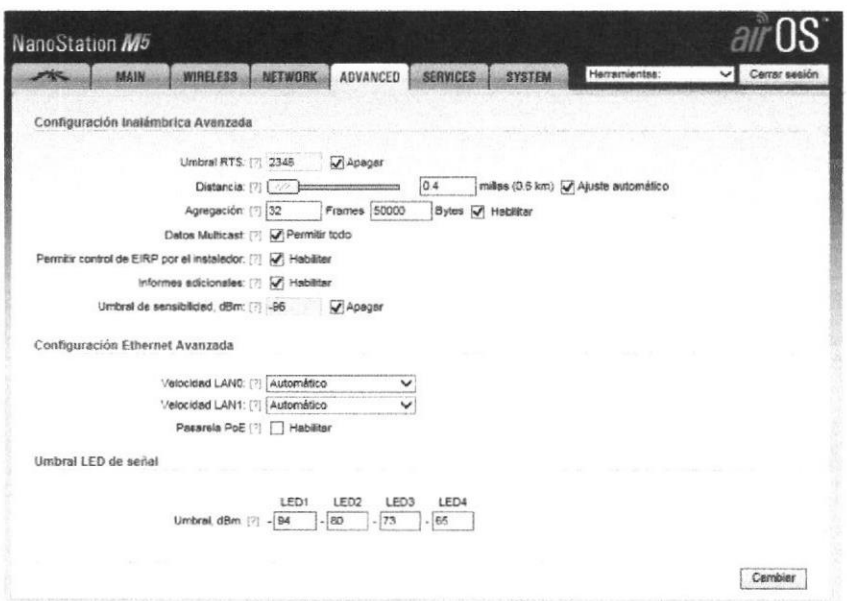
El software de la Antena, permite monitorear la calidad de la señal, para si es necesario cambiando los parámetros de potencia, umbrales de frecuencia, rendimiento y uso de canales de comunicación, de esta manera mejoramos los servicios de trasmisión de datos y evitamos la saturación de los mismos.

La antena incorpora en su parte posterior un juego de led´s, que nos permite visualizar la potencia de la señal y mediante el software Airmax propietario de las antenas Ubiquiti cambiamos parámetros y optimizamos el uso del canal y minimizamos las interferencias. En las fig. 3.1, 3.2, 3.3 y 3.4 se muestra las diferentes pantallas de configuración y monitoreo, analizadas a diario por el administrador del software Airmax, este software permite el monitoreo y configuración de las antenas de comunicación Ubiquiti Nano Station M5.



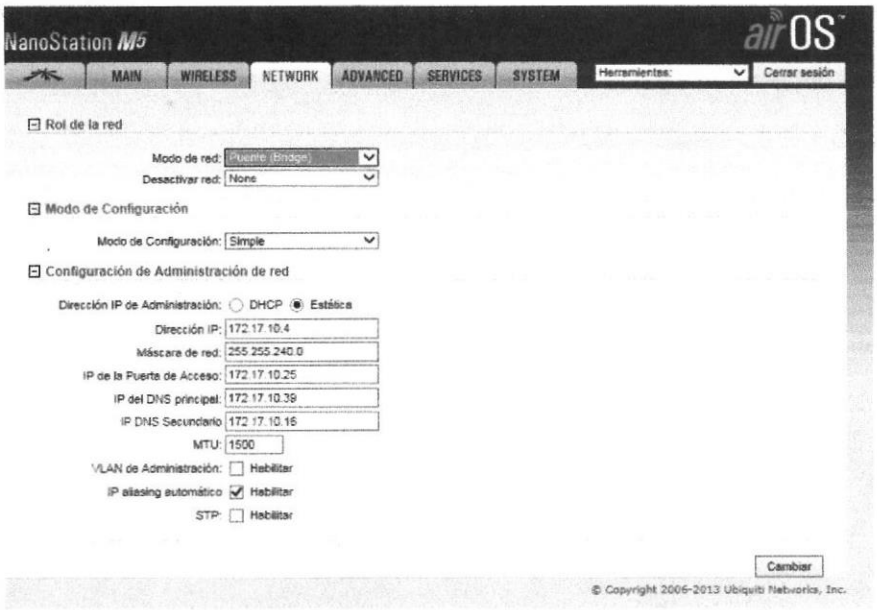
Fuente: Pantalla de Monitoreo del Software

Fig. 3.1 **Configuración de Antenas**



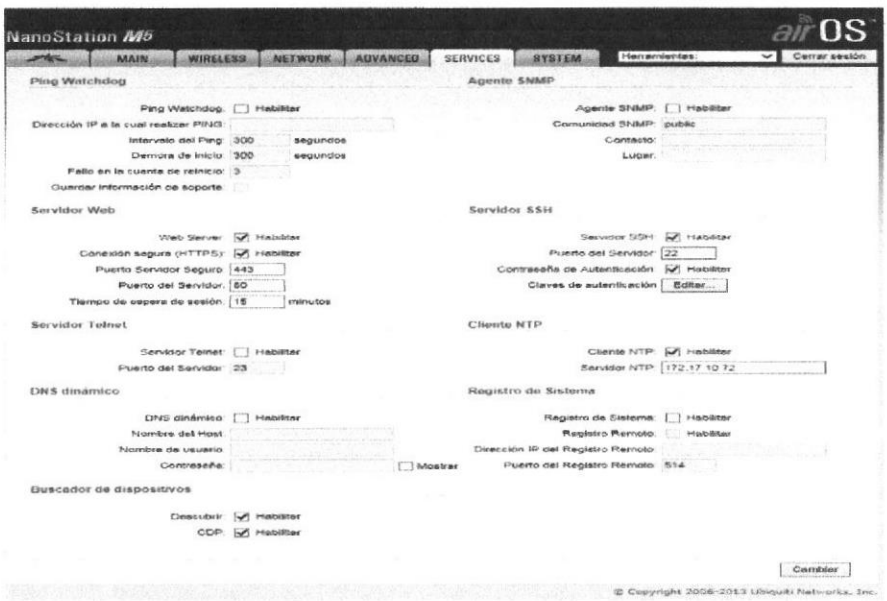
Fuente: Pantalla de Configuración del Software

Fig. 3.2 **Configuración de Frecuencia**



Fuente: Pantalla de Configuración del Software

Fig. 3.3 **Configuración de Dirección IP**



Fuente: Pantalla de Configuración del Software

Fig. 3.4 **Configuración de NTP**

CONCLUSIONES

1. El presente informe ha sido desarrollado omitiendo los datos técnicos, para precautelar la seguridad de la información de la Institución, misma que a todo empleado público se prohíbe hacer pública, en cumplimiento del compromiso de confidencialidad firmado con la Institución.

2. Realizamos las actividades para implementar el presente proyecto, cuyo rendimiento ha sido satisfactorio y útil durante 5 años.

3. Es necesario indicar, que el segmento de red implementado, a través de la Intranet Institucional, tiene acceso a los servicios de Base de Datos e información de los servidores ubicados en Casa Matriz (Quito).

4. El proyecto que dio una eficiente solución al requerimiento, se costeó aproximadamente con $ 42.000 dólares, desglosado de la siguiente manera.

I.	Equipos de comunicación inalámbrica y accesorios	$ 15.000
II.	100 puntos de voz y datos (incluye materiales)	$ 15.000
III.	50 puntos eléctricos, polarizados, UPS 10 KVA	$ 12.000

RECOMENDACIONES

1. Todo proyecto cuya solución involucre un enlace inalámbrico, debe configurar algoritmos cifrados y encriptados para proteger el enlace y los usuarios deben estar conectados a un firewall de última tecnología para garantizar el contenido de la información que se va a trasmitir.

2. Antes de poner en producción enlaces inalámbricos, se debe realizar pruebas de campo y penetración, que permitan dar a los usuarios seguridad, confidencialidad y legitimidad de los datos e información que reside en los servidores.

3. Para prevenir el ataque de hackers, cada vez que se realice un proyecto, donde se maneja información reservada y sensible, el equipo multidiciplinario que el diseño e implementa la solución, debe estar conformado por personal de: soporte técnico y comunicaciones, seguridades informáticas, base de datos, firma electrónica, desarrollo de aplicaciones y auditoria informática; para cubrir las posibles vulnerabilidades y los sistema e información sea segura, confiable e inviolable.

BIBLIOGRAFIA

Ref. # 1: Acosta, M. (2000). *Nuevo Derecho Mercantil.* Ciudad de México: Porrúa.

Ref. # 2 Esteban, J. R. (2009). *Criptografía.* Buenos Aires: Unilibro.

Ref. # 3 Penalva, C. (2009). *Seguridad Criptográfica.* Madrid: Montana.

Ref. # 4 Ubiquitti. (10 de Noviembre de 2011).

http://dl.ubnt.com/datasheets/nanostationm/nsm_ds_web.pdf. Recuperado el 20 de Febrero de 2012,

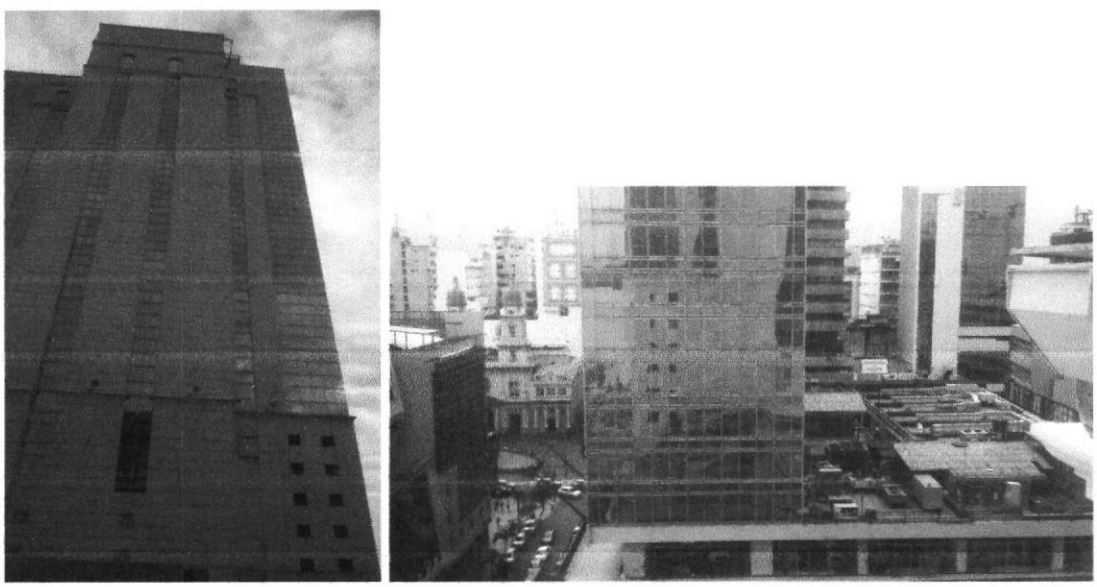
Ref. # 5
http://dl.ubnt.com/datasheets/nanostationm/nsm_ds_web.pdf :

Ref. # 6

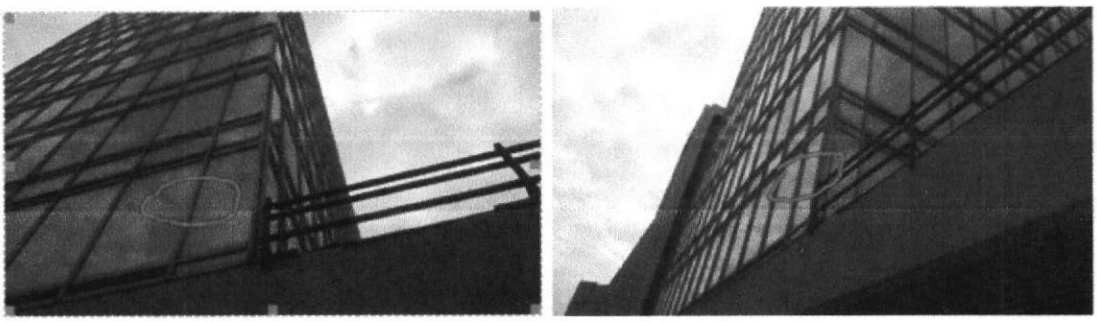
http://dl.ubnt.com/datasheets/nanostationm/nsm_ds_web.pdf

ANEXOS

Cap. Anexos Figura#10 - Edificio CFN y Edificio Ex Previsora



Cap. Anexos Figura#11 - Edificio Ex Previsora - CFN



Cap. Anexos Figura#12 Piso 4to Edif. CFN Inst. de 2 Antenas

Cap. Anexos Figura#13 - Piso 11 Edif. Ex previsora Inst. De 2 Antenas

Overview

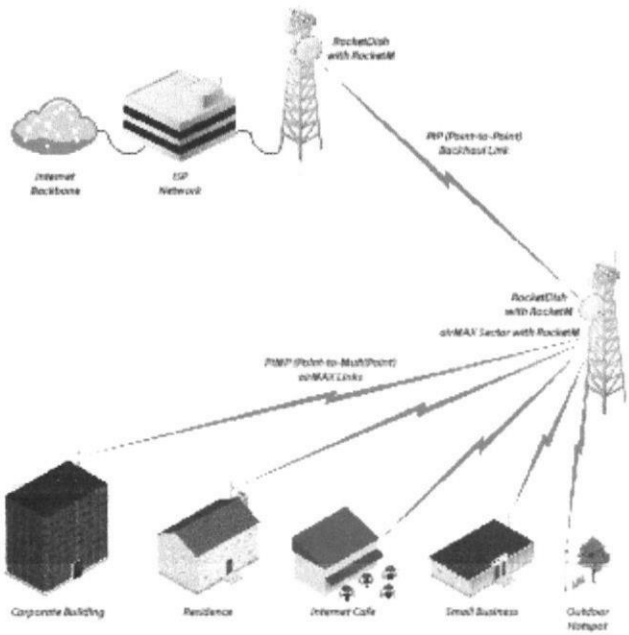
Sector Coverage

The airMAX Sector Antenna is a Carrier Class 2x2 Dual Polarity MIMO Sector Antenna that was designed to seamlessly integrate with RocketM radios (RocketM sold separately).

Pair the RocketM's radio with the airMAX Sector Antenna's reach to create a powerful basestation. This versatile combination gives network architects unparalleled flexibility and convenience.

On the right is one example of how the airMAX Sector Antenna can be deployed:

PtMP (Point to Multi-Point) Link Example

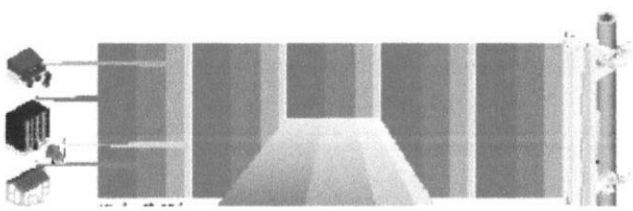


airMAX Sector Antennas provide sector-wide coverage and utilize airMAX technology to produce carrier-class performance and power.

Utilize airMAX Technology*

Unlike standard Wi-Fi protocol, Ubiquiti's Time Division Multiple Access (TDMA) airMAX protocol allows each client to send and receive data using pre-designated time slots scheduled by an intelligent AP controller.

This "time slot" method eliminates hidden node collisions and maximizes



Cap. Anexos Figura#14 Datasheet Ubiquiti

PERMISO DE FUNCIONAMIENTO OTORGADO POR SENATEL

	FORMULARIO PARA SISTEMAS DE MODULACIÓN DIGITAL DE BANDA ANCHA (ENLACES PUNTO-PUNTO)	RC– 9A Elab.: DGGER Versión: 02
ATEL		1) No. Registro:

2) **CLASE DE SISTEMA**

PRIVADO EXPLOTACION (P)	**NOTA:** En el caso de que su empresa cuente con el Permiso de Operación de Red Privada, adjuntar una copia.

3) **CARACTERISTICAS TECNICAS Y DE OPERACION DEL SISTEMA FIJO PUNTO - PUNTO**

No. ENLACE	BANDA DE FRECUENCIAS (MHz)	TIPO DE OPERACION SECUENCIA DIRECTA : TDMA; FHSS ; HIBRIDO ; OFDM; OTRAS	DISTANCIA DEL ENLACE (Km)
L2	5470 – 5725	(O)	0.072

4) **CARACTERISTICAS DE LAS ESTACIONES FIJAS**

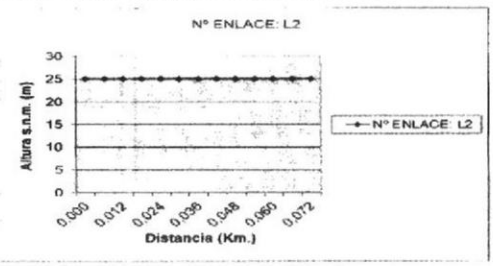
INDICATIVO	AC. (A,M,I,E)	ESTRUCTURA ASOCIADA	ANTENA(S) ASOCIADA(S)	POTENCIA DE OPERACION (mW)	EQUIPO UTILIZADO
F3	I	S3	A3	25	E3
F4	I	S4	A4	25	E4

5) **PERFIL TOPOGRAFICO**

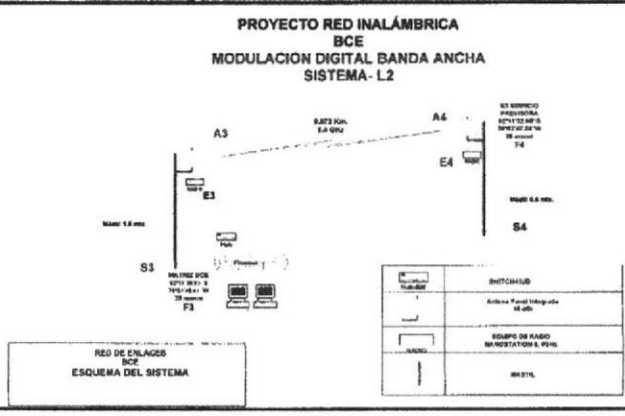
DISTANCIA (Km)	0	D/12	D/6	D/4	D/3	5D/12	D/2	7D/12	2D/3	3D/4	5D/6	11D/12	D
ALTURA s.n.m. (m)	25	25	25	25	25	25	25	25	25	25	25	25	25

Donde D = Distancia entre las estaciones del enlace.
NOTA: Adjuntar las gráficas del perfil de cada enlace.

6) **GRAFICA DEL PERFIL TOPOGRAFICO**



7) **ESQUEMA DEL SISTEMA**



Cap. Anexos Figura#15 Esquema del Sistema

REGISTRO PARA LA AMPLIACIÓN Y MODIFICACIÓN DE LA INFRAESTRUCTURA
DEL PERMISO DE OPERACIÓN DE RED PRIVADA

1. DESCRIPCIÓN TÉCNICA DE LA AMPLIACIÓN Y MODIFICACIÓN DE LA INFRAESTRUCTURA

En el permiso de Operación de Red Privada, se ampliará y modificará el contenido de la infraestructura de transmisión de acuerdo al siguiente detalle:

1.1 UBICACIÓN GEOGRÁFICA DE LAS INSTALACIONES A CONECTAR

No.	Tipo de instalación (Estación o Repetidora)	Provincia	Cantón	Nombre	Dirección	Latitud	Longitud	Observación
1	ESTACIÓN	Guayas	Guayaquil		9 de Octubre 200 entre Pichincha y Pedro Carbo	2°11'30.95"S	79°52'49.47"W	
2	ESTACIÓN	Guayas	Guayaquil		9 de Octubre y Malecón Ed. Ex Banco Previsora	2°11'32.06"S	79°52'47.38"W	
3	ESTACIÓN	Guayas	Guayaquil		9 de Octubre 200 entre Pichincha y Pedro Carbo	2°11'31.57"S	79°52'49.59" W	
4	ESTACIÓN	Guayas	Guayaquil		Av. 25 de Julio Km. 4 Vía a Puerto Marítimo.	2°15'34.28"S	79°53'43.67"W	

	FORMULARIO PARA INFORMACION DE ANTENAS	RC – 3A Elab.: DGGER Versión: 02
		1) Cod. Cont:

2)
CARACTERISTICAS TECNICAS DE LAS ANTENAS

CARACTERISTICAS TECNICAS	ANTENA 1	ANTENA 2
CODIGO DE ANTENA:	A3	A4
MARCA:	UBIQUITI	UBIQUITI
MODELO:	15-211	15-211
RANGO DE FRECUENCIAS (MHz):	5470-5825	5470-5825
TIPO:	PANEL	PANEL
IMPEDANCIA (ohmios):	50	50
POLARIZACION:	VERTICAL	VERTICAL
GANANCIA (dBd):	12.85	12.85
DIÁMETRO (m):		
AZIMUT DE RADIACION MAXIMA (°):	117.78	297.78
ANGULO DE ELEVACION (°):	16.08	-16.08
ALTURA BASE-ANTENA (m):	15	36

2)

Cap. Anexos Figura#17 – Características Técnica

	FORMULARIO PARA ESTUDIO TECNICO DE EMISIONES DE RNI (CALCULO DE LA DISTANCIA DE SEGURIDAD)	RC-15A RNI-T1
		Fecha.:

1) *USUARIO :*

NOMBRE DE LA EMPRESA:	BANCO CENTRAL DEL ECUADOR
DIRECCIÓN	9 de Octubre 200 entre Pichincha y Pedro Carbo

2) *UBICACIÓN DEL SITIO :*

PROVINCIA :	CIUDAD / CANTON :	LOCALIDAD :	LATITUD (°) () (')	LONGITUD (°) () (')
GUAYAS	GUAYAQUIL	9 de Octubre y Malecón, Ex Edificio La Previsora	2° 11' 32.06"S	79°52'47.38" W

3) *S_{pm} A CONSIDERAR (VER ARTICULO 5 DEL REGLAMENTO) :*

FRECUENCIAS (MHz)	S_{pm} OCUPACIONAL (W/m^2)	S_{pm} POBLACIONAL (W/m^2)
5470 – 5725	50	10

4) *CALCULO DE R^2 :*

Altura h (m) :	36	$R = \sqrt{(X^2 + (h - d)^2)}$
DISTANCIA X		VALOR CALCULADO PARA R (m)
2 m		34.55
5 m		34.86
10 m		35.92
20 m		39.87
50 m		60.74

5) *CALCULO DEL PIRE :*

POTENCIA MAXIMA DEL EQUIPO (W)	GANACIA MAXIMA DE LA ANTENA	VALOR DE PIRE (W)
0.5	31.62	15.81

6) *CALCULO DEL S_{pm} TEORICO :*

$S_{pm} = PIRE / (\pi * R^2)$

DISTANCIA	VALOR DE $(\pi * R^2)$	VALOR DE S_{pm} (W/m^2)
2 m	3750.12	0.004
5 m	3817.72	0.0041
10 m	4053.42	0.0039
20 m	4993.92	0.0031
50 m	11590.42	0.0013

Cap. Anexos Figura#18 – Calculo de Distancia