Enlazar dos edificios inalámbricamente para habilitar oficina pública del Banco Central en la ciudad de Guayaquil

David Mendoza Jaéns [(1)] Washington Medina [(2)]
Facultad de Ingeniería en Electricidad y Computación [(1) (2)]
Escuela Superior Politécnica del Litoral (ESPOL) [(1) (2)]
Campus Gustavo Galindo, Km 30.5 vía Perimetral [(1) (2)]
Apartado 09-01-5863. Guayaquil-Ecuador [(1) (2)]
@espol.edu.ec [(1)] wmedina@espol.edu.ec [(2)]

Resumen

Debido a cambios propuestos por el Gobierno actual, el Gerente General del Banco Central del Ecuador, reubicó personal que laboraba en las oficinas ubicadas en el edificio principal ubicado en 9 de Octubre 200 y Pichincha, donde el departamento de Recuperación y Liquidación de la Banca Cerrada Guayaquil cumplía sus funciones. Ante este requerimiento, se le solicitó al personal de Ingeniería de Sistemas y Comunicaciones dar la solución técnica que mantenga el nivel de servicio de los funcionarios que fueron reubicados.

Se descartó las opciones de realizar un enlace físico con fibra óptica, por las dificultades que existían en el sector bancario donde se encuentran los edificios; la opción viable fue la de implementar un enlace inalámbrico considerando que existía línea de vista y frecuencia disponible no saturada en el sector.

Luego de definir el dispositivo que se ajustaba al requerimiento, en el que se consideró: la cantidad de usuarios reubicados, los sistemas transaccionales, el acceso a internet y correo institucional, a los que los usuarios debían seguir teniendo acceso; tiempo de respuesta requerido, seguridad del enlace inalámbrico, seguridad de la información trasmitida, se procedió a realizar las pruebas de campo y penetración que confirmaron la calidad de servicio recibido por los usuarios con tiempo de respuesta aceptable.

El sistema se implementó para enlazar piso cuarto del edificio principal del Banco Central (Centro de Datos) con el piso undécimo del edificio Ex Previsora, para luego realizar un segundo enlace entre el Centro de Datos, ubicado en el edificio principal del Banco Central con el piso decimosexto del edificio Ex Previsora, justificado por el incremento de personal. Configurando los enlaces como contingencia cruzada, en caso de falla de alguno de los dispositivos de comunicación.

Palabras Claves:

Abstract

Due to changes proposed by the actual government, Central Bank of Ecuador's CEO relocated staff of the Recovery and Liquidation of Closed Banks department that worked in the main building of the institution, which is located in the intersection of 9 de Octubre Ave. and Pichincha St. With this requirement, System Engineering and Communications staff was asked to give the proper technic solution in the way that it maintains the same level of quality of service that the relocated staff needs.

Physical optical fiber link was discarded because of the existent difficulties of the banking zone, where both buildings are located. The best option was to implement a wireless link, considering that a line of view and unsaturated available frequency was existent in this zone.

After defining the device that best adjust to the requirement, which considered: quantity of users, transactional systems, internet access, institutional email, which the staff must keep using; required answer time, wireless link security and transmitted information security; the staff proceeded to make the field tests and penetration tests that confirmed the quality of the service that the staff were experiencing with an acceptable answer time.

The system was implemented to link the 4^{th} floor of the Central Bank main building (Data Center,) with the 11^{th} floor of the Ex Previsora building, for later implement a second ling between Data Center with the 16^{th} floor of the Ex Previsora building, this justified by the staff increment. Both links were configured as crossed backup in case of failure of either of the communication devices.

Keywords*:*

1. Introducción

Los funcionarios del Banco Central laborabamos 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 y solamente quedaron tres pisos habilitados para el Banco Central; la oficina de Recuperación y Liquidación cuya labor era la de regularizar deudas y acreencias de los deudores de la Banca Cerrada fueron reubicados en

los pisos 11, 16 y 17 del edificio Ex Previsora, ubicado en Malecón y 9 de Octubre, por orden de la Gerencia General.

Para seguir desarrollando sus actividades los funcionarios trasladados debían mantener operativos sus sistemas informáticos, aplicativos, correo electrónico y navegación a través de Internet. Los usuarios debían mantener las políticas internas y normas de control interno, descritas en los manuales de procedimientos del Subproceso de Seguridad Informática, conservando los mismos perfiles definidos en los servidores.

El Proyecto se inició con el levantamiento de información, análisis técnico, cotizaciones de equipos y elaboración de cronogramas de implementación del enlace, considerando que la reubicación tenía carácter de urgente.

Durante el análisis técnico se presentaron tres propuestas:

La primera opción, fue extender la LAN del BCE utilizando cable UTP blindado, a través de los postes del sector; esta situación no fue factible, 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.

En la segunda opción, se propuso implementar el enlace usando fibra óptica subterránea, a través de ductos existentes; pero tampoco fue factible, 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.

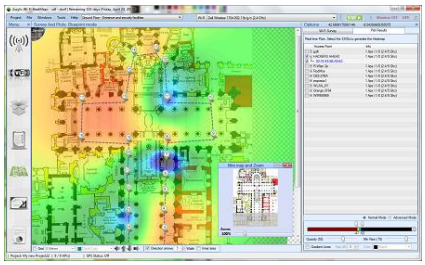
La tercera opción propuesta, consistió en implementar un enlace inalámbrico entre los edificios, la misma que resultó ser la más idónea.

Considerando experiencias similares de enlaces establecidos con espacios culturales que administraba la Institución, iniciamos la investigación de antenas que se adapten a la situación geográfica y al requerimiento de los usuarios reubicados.

La decisión fue la de utilizar equipos ubiquitti, cuya fortaleza es el ancho de banda, la potencia configurable vía software, el monitoreo en línea de la calidad de señal, la protección contra el hacking malicioso y la facilidad de configuración via browser.

ANALISIS TECNICO

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 utilizada en el sector era 2346, y dicha frecuencia se configuró 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” y será la nueva oficina para los usuarios re-ubicados.

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

En el cuarto piso del edificio CFN, está ubicado el Centro de Datos y se encuentra la totalidad de la infraestructura informática del Banco Central.

El edificio Ex Previsora tiene tres pisos que pertenecen al Banco Central, las oficinas están disponibles para los funcionarios del área de Recuperación y Liquidación.

Información de usuarios y aplicativos utilizados.-

En promedio la información que cada usuario maneja es 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 en su nueva ubicación la comunicación de los usuarios no se transforme en un problema para la trasmisión de datos.

Las condiciones mínimas de funcionamiento del enlace son:

- 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 para los equipos de comunicación.

La Institución implementó enlaces entre oficinas remotas ubicadas dentro del perímetro urbano, pero alejadas del casco comercial, esta situación se tomó como punto de partida para realizar el presente análisis técnico; aunque la cantidad de usuarios, el volumen de información y la transaccionalidad de los enlaces era diferente.

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 (troughput) y que cumpla con lo que determinan las mejores prácticas de comunicación inalámbrica Itil, Iso 27000.

Para escoger la antena también se consideró la ubicación física en los edificios, pues los edificios de la referencia están ubicados en medio de otros edificios de gran altura.

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

Luego del estudio y análisis correspondiente de los parámetros mínimos requeridos, decidimos utilizar las antenas Nano M5, fabricadas por Netware Ubiquiti, mostradas en la fig. 1.2 equipo que de acuerdo a las referencias técnicas, había sido probado en situaciones ambientales y físicas similares al caso presentado y se obtuvo resultados altamente eficientes.

Las antenas Nano, tienen las siguientes ventajas de funcionamiento:

Fuente: DataShet del Fabricante

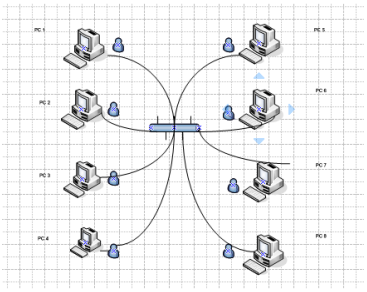
Figura 1.2: Modelos Antenas

- 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 cual se configuró el Nano/m5 no estaba saturada de acuerdo al site survey practicado, por lo que no provocarían interferencias otros dispositivos inalámbricos instalados en la zona.
- Son configurables, tal como los Router
- 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 del WAP2-PSK para dar seguridad a la trasmisión de datos.
- Deshabilitación del SSID para evitar que el enlace sea público.
- 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.
- 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 navegación por 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.

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

Primero se instaló una antena en la ventana del piso 4to del edificio CFN enlazada con una antena ubicada en el piso 11 del edificio Ex Previsora.

Como se incrementó la cantidad de usuarios y se los ubicó en el piso 16 del edificio Ex Previsora, inicialmente se utilizó el mismo enlace, pero la eficiencia de trasmisión decayó y se incrementó el tiempo de respuesta, por lo que se implementó otro enlace de igual característica que el anterior entre el piso 4to del edificio CFN y 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 parámetros configurables para proteger la antena y la información que se transmitirá, estos parámetros los configura el administrador para precautelar los datos a trasmitir.

Seguridades de la conexión de red.-

El SSID (Service Set IDentifier) 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.

Uno de los métodos más básicos de proteger una red inalámbrica es desactivar la difusión (broadcast) del SSID, lo cual se hará en nuestro caso para que el enlace no esté a la vista del público. Se deben utilizar también otros sistemas de cifrado y autentificación.

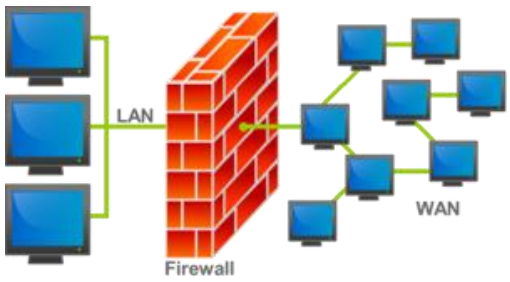
WPA2 (Wi-Fi Protected Access 2 - Acceso Protegido Wi-Fi 2) es una versión mejorada, creada para corregir las vulnerabilidades detectadas en WPA.

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

Escogimos encriptación WPA2-PSK por ser más robusta y presentar un nivel superior de protección. 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

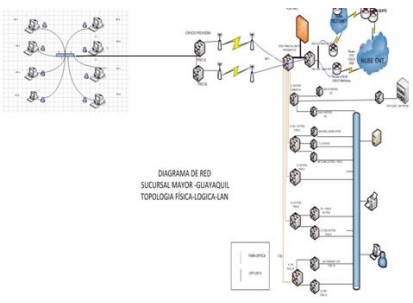
Figura 1.4 Red Firewall

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 al firewall 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 Metodología

SERVICIOS DE TI INCORPORADOS.

En la actualidad, existen 200 usuarios conectados en las oficinas del edificio ExPrevisora y la comunicación mantiene la eficiencia, 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.

Se cumplió el requerimiento, 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.

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 más 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 Ubiquitti

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:

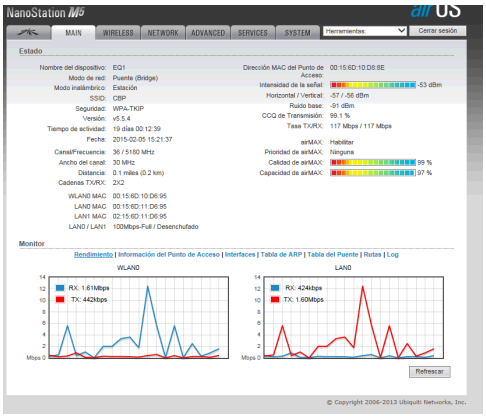
- Umbral RTS
- Datos Multicast
- Control EIRP
- Umbral de sensibilidad
- Velocidad de LAN
- Modo de Red
- Elegir modo de operación del equipo: Router o AP.
- Reportes de rendimiento de las antenas

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.

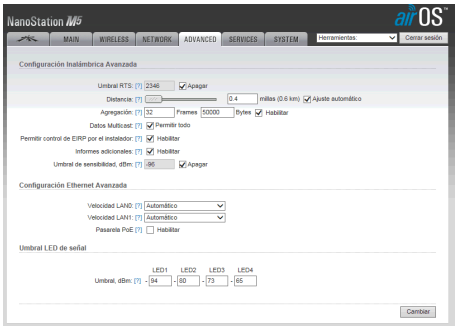
El software de la Antena, permite monitorear la calidad de la señal, para si es necesario se puede cambiar los parámetros de potencia, umbrales de frecuencia, rendimiento y uso de canales de comunicación, de esta manera mejoramos los servicios de trasmisión de datos y evitamos la saturación de los mismos.

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.



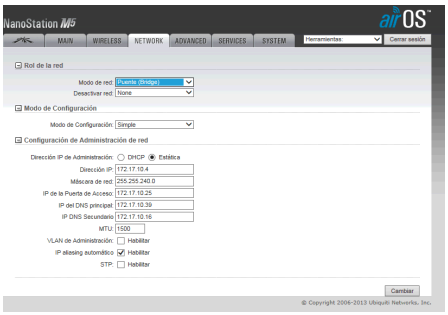
Fuente: Pantalla de Monitoreo del Software

Fig. 3.1 Configuración de Antenas



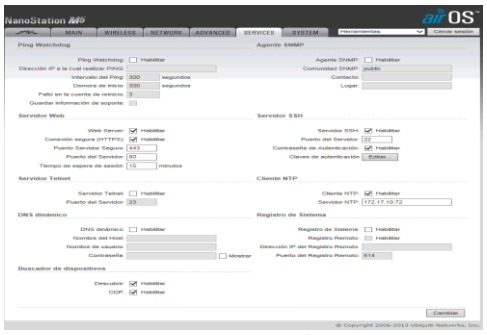
Fuente: Pantalla de Configuración del Software

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 por confidencialidad no debe ser divulgada, en cumplimiento de un compromiso 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:

Equipos comunicación inalámbrica/accesorios	$ 15.000
100 puntos voz / datos (incluye materiales)	$ 15.000
50 puntos eléctricos, polarizados, aterrizados	$ 5.000
UPS 10 KVA	$ 7.000

RECOMENDACIONES

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.

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.

Para prevenir el ataque de hackers, cada vez que se realice un proyecto, donde se maneja información reservada y sensible, el equipo multidiciplinario al que se encarga la elaboración del diseño y la implementación de 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