CAPITULO III

3. PROPUESTA DE IMPLEMENTACION DE SEGURIDADES EN LA EMPRESA MISHAN SERVICES

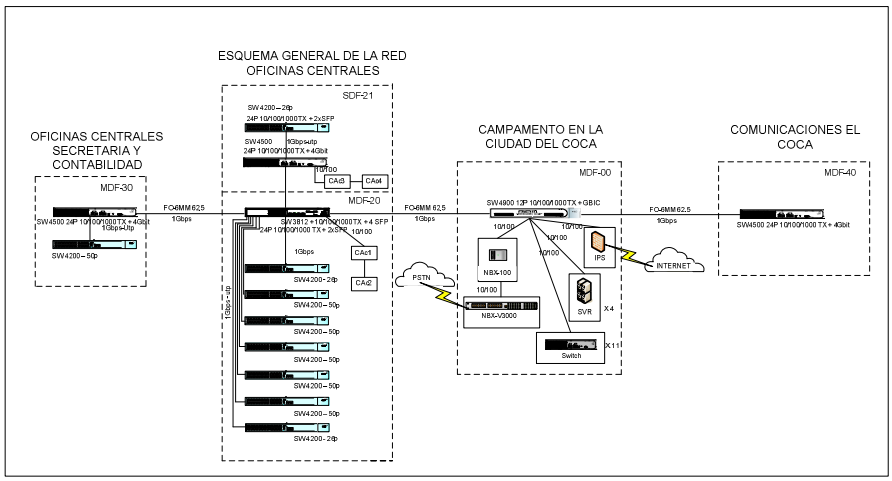
La empresa Mishan Services como prestadora de servicios profesionales de distinta índole en el sector minero y de hidrocarburos del país se encuentra en franco proceso de automatización y actualización de procesos principalmente del área Informática y de sistemas los cuales son considerados como parte fundamental en todas las actividades que desarrolla está empresa.

Es importante notar que la investigación está relacionada con las seguridades que se pueden brindar a los equipos y a las redes de computadores de la empresa dentro de los campamentos a los cuales se prestan los servicios profesionales y estos a su vez tienen una comunicación con las oficinas centrales en la ciudad de Quito, es importante hacer notar que redes de área local se las realiza mediante cableado estructurado mientras que las comunicaciones con las oficinas centrales se las realiza mediante contratación directa con una empresa de prestación de servicios de internet, el cual a su vez nos proporciona una VPN o canal dedicado para el envió - recepción de información de Quito al Coca.

3.1 Diseño de las seguridades a nivel de redes

El proceso de implementación de seguridades debe ser dado de acuerdo a las necesidades que se generan en las empresas, y todo debe guardar un orden partiendo de un correcto ordenamiento de los equipos en cada uno de los RAC y de los MDF para que se pueda guardar una buena relación entre departamentos dentro de una misma oficina, dentro de una misma ciudad, pero también es importante detallar como se encuentra ordenado de forma general la empresa en su infraestructura tecnológica ya que es desde donde se puede partir para las comunicaciones de la empresa, en base a lo que se dispone es donde se puede optar por brindar las respetivas seguridades.

Grafica 3.1. : Esquema General de la red de datos
Fuente: Mario Araque B.



La infraestructura tecnológica de la empresa como se pudo observar en el grafico 3.1 es de última generación incluso el cableado estructurado se

elaboro bajo las normas de la EIA/TIA 568B la misma que fue certificada por empresas certificadoras del país. Para poder ser proveedor de servicios profesionales en empresas del ramo de los hidrocarburos se necesita de que todo este amparado en estándares internacionales ya que estas trabajan en conjunto para obtener las certificaciones ISO en todos los procesos.

La distribución de los equipos de concentración como routers y switch se encuentran con una nomenclatura que corresponde a los estándares de la IEEE 802. X los mismos que están dados para lo que es cableado y comunicaciones en redes LAN.

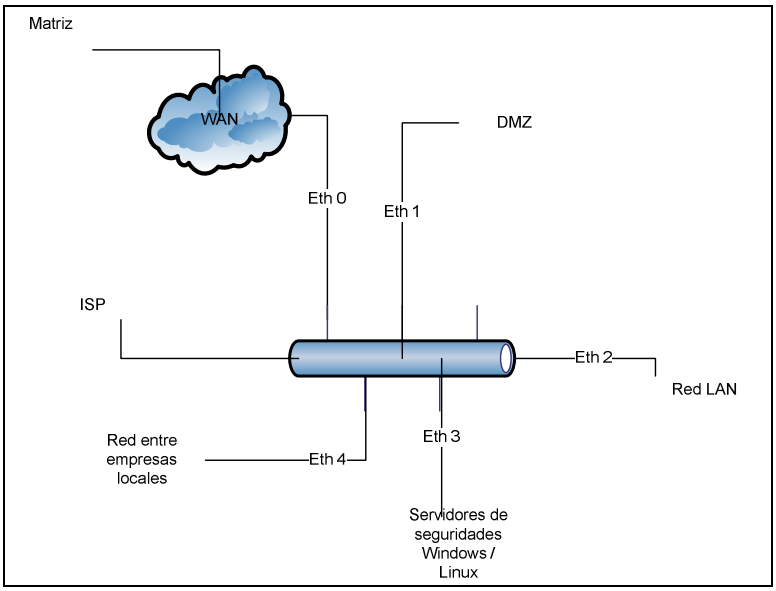
Es importante notar que toda la infraestructura guarda el estándar del MDF es decir del RAC según la dependencia donde se encuentre operando los concentradores, la empresa cuenta ya con un servidor que puede ser empotrado en el RAC con la finalidad de cada día optimizar de mejor manera el espacio físico de la empresa y cada una de las dependencias. Este es el primer paso para poder poner a punto la centralización de recursos.

3.1.1. Análisis de requisitos

Como toda empresa que está implicada en brindar servicios de calidad a empresas de calidad, MISHAN SERVICES ha creído conveniente tomar

en cuenta la distribución del espacio tanto en Quito como en el campamento del Coca, para un mejor servicio de la empresa en la propuesta de esta investigación se plantea la creación de los DMZ para la administración de la pagina web, la intranet los servicios mediante descargas de archivos mediante ftp, comunicaciones remotas mediante ssh que es un protocolo remoto de acceso a datos y para poder explotar al máximo los recursos del Linux de igual manera se plantea

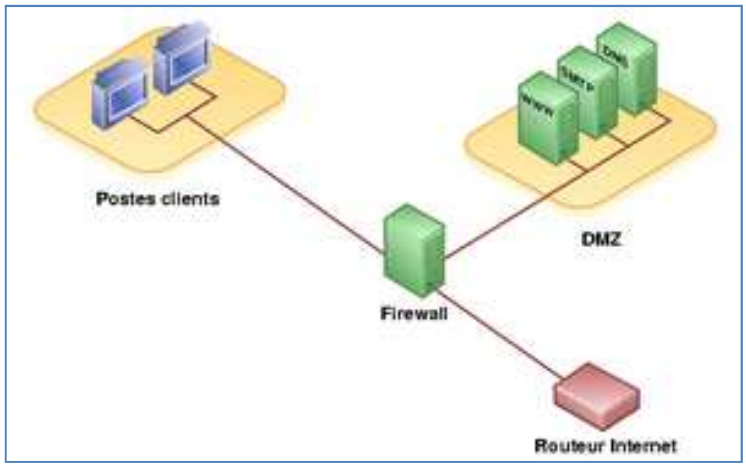
Grafica 3.2. : Esquema Planteado del servidor principal de la red de datos
Fuente: Mario Araque B.



Según se puede observar en la configuración planteada por el investigador se contempla u servidor principal el mismo que este equipado cuando menos con 4 tarjetas de red y que va a ser el nexo entre el servidor de Windows 2003 Server y el Linux y la salida a través de los DMZ al exterior según se puede observar el dmz que no es otra cosa que una zona

llamada desmilitarizada la misma que nos ayudara a prevenir de posibles ataques a la red a través del internet por servicios o puertos que se encuentren abiertos como el DNS, e mail o la misma zona de la navegación web.

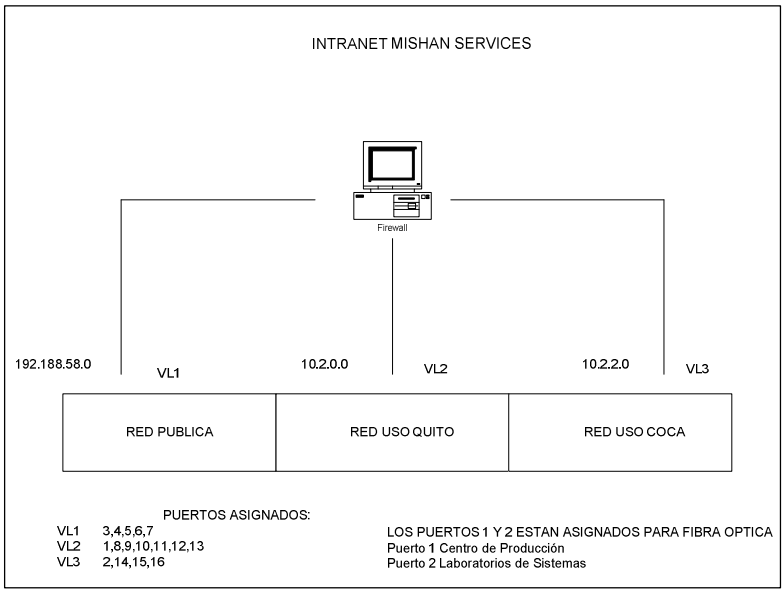
Grafica 3.3. : Esquema de un DMZ
Fuente: Mario Araque B.



3.1.2. Diseño de la red de área local

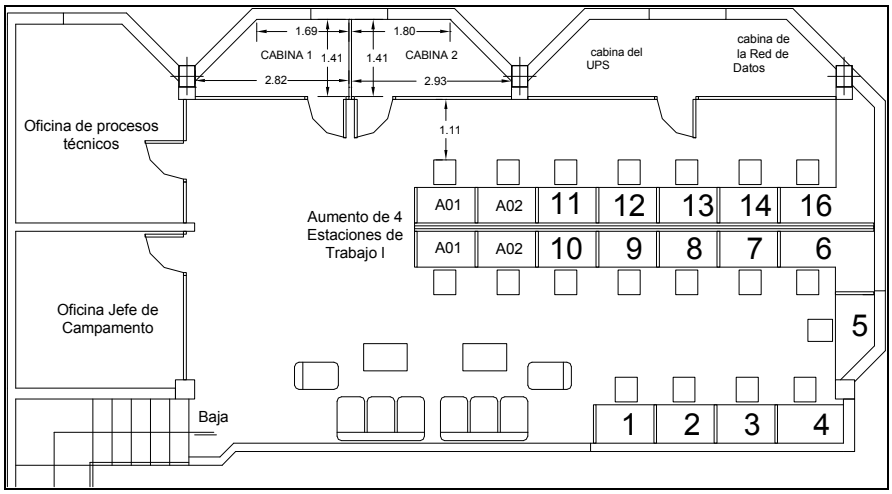
En lo que tiene que ver con el diseño de la red de forma general nos hemos visto en la necesidad de centralizar la administración de los equipos es decir solo un ´proveedor de internet de lo que se contaba con dos ya que el segundo solamente lo utilizaríamos como una conexión VPN para garantizar el flujo de la información a través de las comunicaciones de los proveedores de internet de un punto hacia otro o entre ciudades.

Grafica 3.4. : Diseño propuesto de la Intranet
Fuente: Mario Araque B.



Como se puede observar el diseño contempla la implementación de una red centralizada mediante un switch de core el mismo que repartirá información a través de switch de enlace a los tres puntos que se encuentran detallados más abajo, es importante notar que se repartirá la información a los switch de enlace mediante VLAN´s, las mismas que no podrán verse entre si es decir la comunicación o los datos que se envíen dentro de cada una de ellas es responsabilidad independiente, solamente el servidor como regulador será quien pueda ver la información que circule a través de la red sea la VLAN que sea.

Grafica 3.5. : Diseño de la Red LAN actual en la ciudad del Coca
Fuente: Mario Araque B.



En el campamento de la empresa en la ciudad del Coca se dispone de más o menos 20 personas las mismas que se pueden distribuir en un reducido espacio físico, por lo que las seguridades no pueden pasarse por alto ya que se puede perder información por contagio de virus, o por desconocimiento de configuraciones se puede borrar involuntariamente datos importantes para el normal desempeño de las funciones.

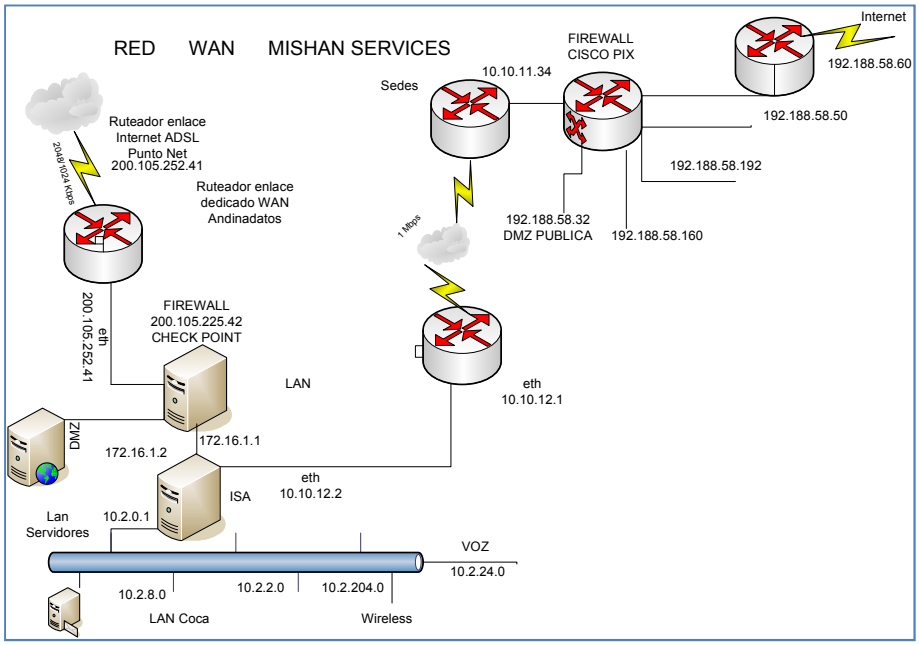
La información que generan cada uno de los usuarios se almacenara en el servidor de archivos y respaldos que cuenta cada uno de las sedes, los sistemas se encuentran en la ciudad de Quito al igual que las bases de datos por lo que la administración de los sistemas se los hace mediante conexiones Cliente/servidor y el back end de las aplicaciones son alimentadas mediante comunicaciones dedicadas en VPN. Los front end de las aplicaciones que están en Visual C están en cada una de las

estaciones de trabajo, todo lo que aquí se genera se respalda en la ciudad de Quito ya que se debe precautelar toda la información.

3.2. Diseño de la red de área extensa

El diseño de la red de área extensa o extendida como se lo había mencionada en los gráficos anteriores se lo hace mediante comunicaciones VPN las mismas que lo realizan los proveedores del internet que en la actualidad todavía se mantiene bajo contratación directa con CNT y puntonet pero como es de conocimiento general la ultima milla de puntonet se la realiza la misma empresa estatal CNT por lo que se ha decidió rescindir contrato con esta empresa y que la generación de la señal de comunicaciones la administre la empresa CNT.

Grafica 3.6. : Diseño de la Red WAN
Fuente: Mario Araque B.

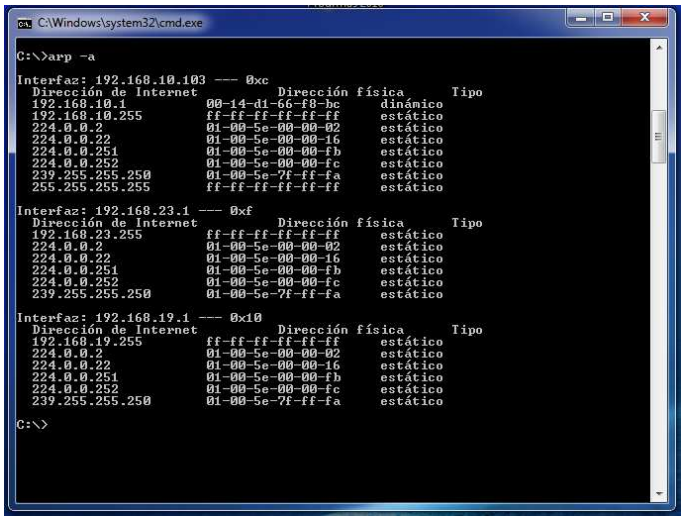


El diseño de la red de área extensa se lo realiza mediante los equipos CISCO ya que son los mejores del mercado y estos a su vez garantizan que toda la información que se genera va a ser administrada de forma correcta por los switch de enlace previo a las comunicaciones remotas de los routers, por lo general las comunicaciones entre routers están dadas por empresas que se dedican a la administración de este tipo de comunicaciones ya que se los realiza mediante protocolos públicos y estos a su vez se encargan de aterrizar la señal a los usuarios de la red de área local.

3.3. Pruebas de la red

Las Pruebas de la red se las realizaron en los servidores de la empresa que se encuentran en la ciudad del Coca ya que la administración ahí es lo que se desea precautelar, con esta investigación.

Grafica 3.7. : Diseño de la Red WAN
Fuente: Mario Araque B.



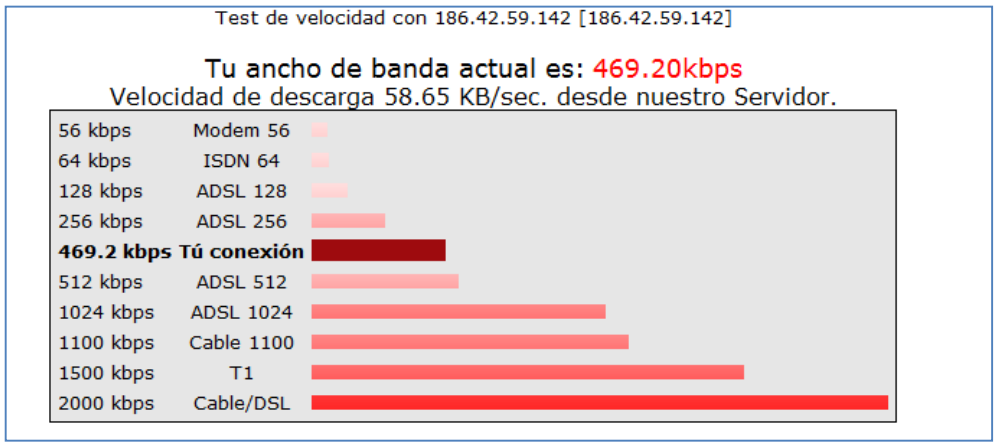
En las pruebas que se realizaron en los equipos de la empresa sobre los puertos abiertos y sobre todo lo que se requiere para poder llegar con las señales a las oficinas centrales en la ciudad de Quito mediante el mapeo de la red, se hizo necesario el abrir puertos tanto en Windows 2003 como en el Linux que es el que se encarga del cortafuegos y de la administración del internet.

3.3.1. Implementación

Una vez implementada la red podemos realizar las pruebas a las comunicaciones mediante medidores de recursos los mismos que son proveídos por las empresas de internet.

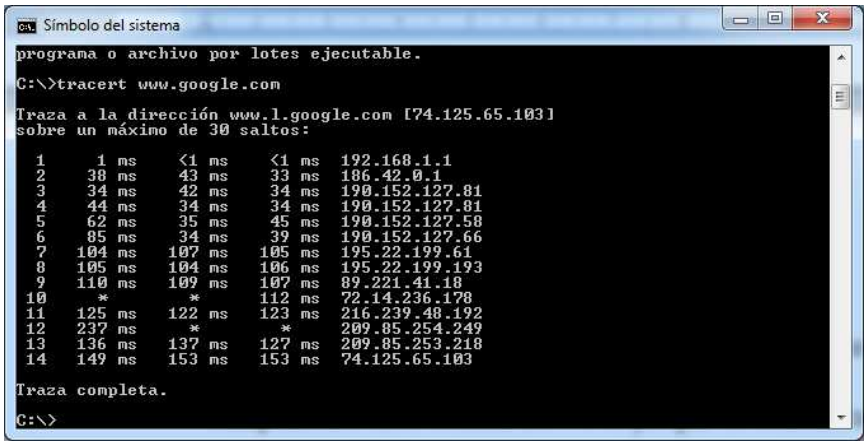
Cuando medimos la traza de las direcciones en la red podemos tener todas las direcciones de los protocolos

Grafica 3.8. : Medición del recurso del internet desde un usuario del servicio
Fuente: Mario Araque B.



El ancho de banda que puede llegar a un usuario es de 500Kbps al campamento en la ciudad del Coca ya que la comunicación total para toda la empresa es de un T1 por lo que es ideal se tiene el 33% en las estaciones.

Grafica 3.9. : Traza de la red hacia la dirección www.google.com
Fuente: Mario Araque B.



La traza muestra todas las configuraciones que tiene que pasar un paquete para poder llegar a una dirección en internet que para nuestro caso fue www.google.com, con esto también podemos confirmar que el firewall de la empresa se encuentra trabajando de forma optima ya que se puede ver que la dirección se encuentra encriptado con un * todas las direcciones de la empresa sean estas públicas o privadas se están dado de acuerdo a lo que se planifico en la presente investigación.

Con el ancho de banda que se pudo comprobar con el software de medición de recurso se hizo muy importante conocer cuál sería la

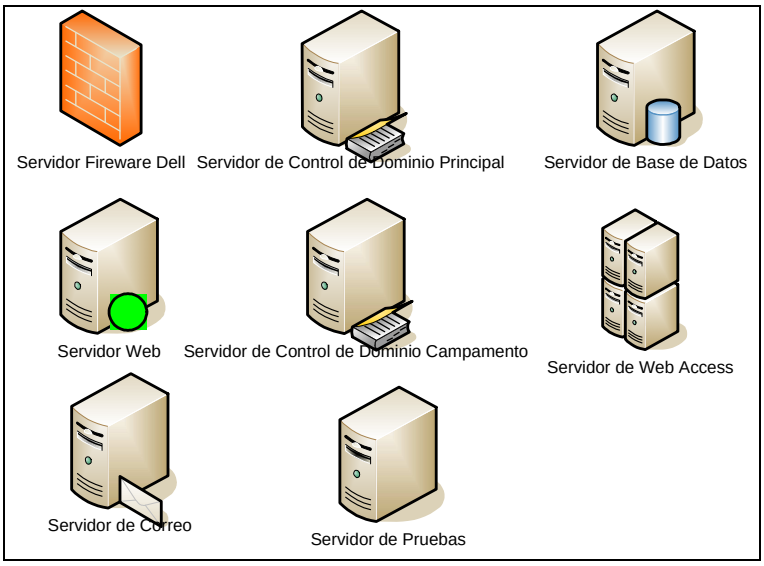
velocidad de la información al momento de enviar los paquetes hacia la ciudad de Quito desde el campamento.

Todos los trazos que se pueden observar están centralizados en los servidores tanto del campalmente como de las oficinas centrales, es necesario hacer notar como parte de la investigación que nuestra empresa cuenta con 3 direcciones publicas mismas que están correctamente utilizadas para cada una de las actividades planificadas.

3.3.2. Diseño de las seguridades a nivel de servidores

Las seguridades están dadas en cada uno de los servidores que a continuación se detallan pero aunque en algunos casos no son todos físicos se puede notar que cada uno guarda relación con la investigación planteada.

Grafica 3.10. : Ilustración de los servidores plateados en la investigación
Fuente: Mario Araque B.



- **Servidor de archivos**: Este servidor en la empresa se encarga de almacenar varios tipos de archivo y los distribuye a otros clientes en la red.

- **Servidor de impresiones**: controla una o más impresoras y acepta trabajos de impresión de otros clientes de la red, poniendo en cola los trabajos de impresión (aunque también puede cambiar la prioridad de las diferentes impresiones), y realizando la mayoría o todas las otras funciones que en un sitio de trabajo se realizaría para lograr una tarea de impresión si la impresora fuera conectada directamente con el puerto de impresora del sitio de trabajo.

- **Servidor de correo**: almacena, envía, recibe, enruta y realiza otras operaciones relacionadas con e-mail para los clientes de la red.

- **Servidor proxy**: realiza un cierto tipo de funciones a nombre de otros clientes en la red para aumentar el funcionamiento de ciertas operaciones (p. ej., prefetching y depositar documentos u otros datos que se soliciten muy frecuentemente). También sirve seguridad; esto es, tiene un Firewall(cortafuegos). Permite administrar el acceso a internet en una red de computadoras permitiendo o negando el acceso a diferentes sitios web.

- **Servidor del acceso remoto (RAS)**: controla las líneas de módem de los monitores u otros canales de comunicación de la red para que las peticiones conecten con la red de una posición remota, responden llamadas telefónicas entrantes o reconocen la petición de la red y realizan los chequeos necesarios de seguridad y otros procedimientos necesarios para registrar a un usuario en la red.

- **Servidor de uso**: realiza la parte lógica de la informática o del negocio de un uso del cliente, aceptando las instrucciones para que se realicen las operaciones de un sitio de trabajo y sirviendo los resultados a su vez al sitio de trabajo, mientras que el sitio de trabajo realiza el interfaz operador o la porción del GUI del proceso (es decir, la lógica de la presentación) que se requiere para trabajar correctamente.

- **Servidor web**: almacena documentos HTML, imágenes, archivos de texto, escrituras, y demás material Web compuesto por datos (conocidos colectivamente como contenido), y distribuye este contenido a clientes que la piden en la red.

- **Servidor de reserva**: tiene el software de reserva de la red instalado y tiene cantidades grandes de almacenamiento de la red en discos duros u otras formas del almacenamiento (cinta, etc.) disponibles para que se utilice con el fin de asegurarse de que la pérdida de un servidor principal no afecte a la red. Esta técnica también es denominada clustering.

3.3.3. Análisis de requisitos

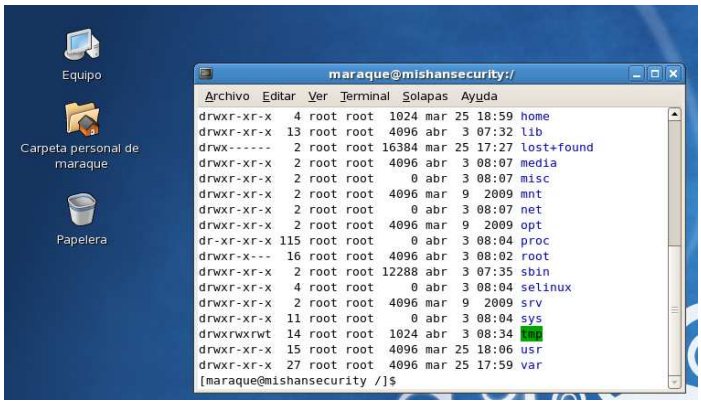
En base a lo expuesto hemos planteado la implementación de dos servidores el de Linux CentOS 5 y el de Windows 2003 Enterprise Server, en el Windows 2003 se configuro un servidor ldap es decir una base de datos para poder asignar privilegios de acuerdo a los perfiles de los usuarios de la empresa pero que labora únicamente en la ciudad del Coca.

Por otro lado el servidor Linux se encarga de toda la configuración de las seguridades y de la administración remota, como también de la administración de los servicios del internet.

3.3.4. Instalación y Configuración de un servidor Linux

El servidor Linux de la empresa tiene las configuraciones centradas en el IPTABLES del rc.d dentro de las configuraciones del etc, las mismas que están dadas de acuerdo a las necesidades de la empresa y como las reglas son las que se les da de acuerdo a las necesidades de comunicación, se tiene que al tratarse de una empresa de prestación de servicios de 24 horas al día, 7 días a la semana es decir permanente no se puede suspender el servicio, en vista de esta realidad hemos optado por que se tenga privilegios completos permanentemente.

Grafica 3.11. : Configuraciones de Seguridades en CentOS por usuario
Fuente: Mario Araque B.



Cuando ingresamos con un usuario no se tiene la administración ni en un 50% de lo que es el servidor Linux ya que los privilegios de cada usuario por más administrador (root) que sea se complica sobre todo cuando se ha

hecho necesario asignar nuevos privilegios a todos los que acceden a los servicios de las redes sean estas locales o remotas como en las oficinas centrales en la ciudad de Quito.

Grafica 3.12. : Configuración servidor samba(smb)
Fuente: Mario Araque B.

El servidor samba es el que nos permite copiar archivos desde un cliente hacia los servidores o viceversa además en el caso de la empresa este servicio se encuentra arriba con la finalidad de que los usuarios de Quito puedan copiar documentos que se envían por correo pero entre eventualidades se puede tomar como alternativa el copiar mediante la compartición de los recursos propios que los da el servidor smb.

Todos los usuarios creados en Linux tienen los privilegios de utilizar este servicio muy importante para optimizar recursos dentro de la intranet empresarial.

Grafica 3.13. : Configuración Grafica del Firewall de Mishan Services
Fuente: Mario Araque B.

Las opciones están dadas de acuerdo a los DMZ es decir de la zona desmilitarizada, con la finalidad de que las seguridades sean administradas por las personas que laboran en el departamento de sistemas se ha hecho necesario que el nivel de seguridad del firewall de linux en los iptables estén dados con el perfil de obedientes ya que siempre se estará en contacto con las personas que administran los servidores de comunicaciones desde la ciudad de Quito.

El cortafuegos no está dado para que las páginas web tengan restricciones al contrario se las define de acuerdo a la necesidad de la empresa ya que lo que se requería era optimizar los recursos y está es una manera de hacerlo.

El proxy de igual manera se encuentra distribuyendo de acuerdo a la necesidad mediante un dhcp (Servidor de direcciones IP automáticas) y estas son dadas desde el .2.100 hasta el .2.240. Siempre de acuerdo a las necesidades de los usuarios que requieran el servicio.

Grafica 3.14. : Ilustración de los servidores plateados en la investigación
Fuente: Mario Araque B.

Aquí se puede notar de mejor manera como se está asignando los privilegios de forma grafica pero sin que intervenga directamente la configuración por consola que es lo ideal para precautelar posibles cambios de configuraciones.

3.3.5. Instalación y Configuración de un servidor Windows 2003

Windows Server 2003 es un sistema operativo de la familia Windows de la marca Microsoft para servidores que salió al mercado en el año 2003. Está basada en tecnología NT y su versión del núcleo NT es la 5.2.

En términos generales, Windows Server 2003 se podría considerar como un Windows XP modificado, no con menos funciones, sino que estas están deshabilitadas por defecto para obtener un mejor rendimiento y para centrar el uso de procesador en las características de servidor, por ejemplo, la interfaz gráfica denominada Luna de Windows XP viene desactivada y viene con la interfaz clásica de Windows. Sin embargo, es posible volver a activar las características mediante comandos services.msc. En internet existen varios trucos para hacerlo semejante a Windows XP.

De las características más importantes que pueden ser consideradas como alcances son:

- Sistema de archivos NTFS:

    1. cuotas
    2. cifrado y compresión de archivos, carpetas y no unidades completas.
    3. permite montar dispositivos de almacenamiento sobre sistemas de archivos de otros dispositivos al estilo Unix

- Gestión de almacenamiento, backups... incluye gestión jerárquica del almacenamiento, consiste en utilizar un algoritmo de caché para pasar los datos menos usados de discos duros a medios ópticos o similares más lentos, y volverlos a leer a disco duro cuando se necesitan.

- Windows Driver Model: Implementación básica de los dispositivos más utilizados, de esa manera los fabricantes de dispositivos sólo han de programar ciertas especificaciones de su hardware.

- Active Directory Directorio de organización basado en LDAP (“LIGHTWEIGHT DIRECTORY ACCES PROTOCOL”), permite gestionar de forma centralizada la seguridad de una red corporativa a nivel local.
    - Autentificación Kerberos5
    - DNS con registro de IP's dinámicamente
    - Políticas de seguridad

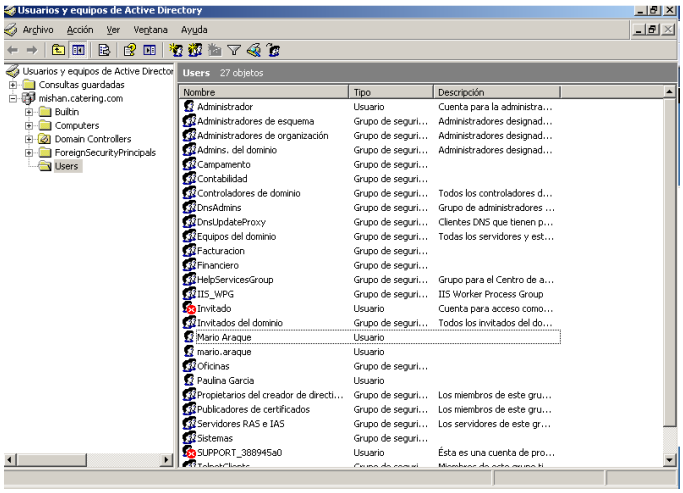
Grafica 3.15. : Ingreso al servidor de Windows con dominios
Fuente: Mario Araque B.

El acceso al servidor de dominios es muy simple siempre y cuando se encuentre registrado en el servidor de Windows 2003 el cual guarda relación con el servidor de Linux para evitar potenciales ataques a la red de información empresarial y por lo tanto evitamos la perdida de la información.

En la empresa se tienen dos grupos de dominios los mismos que precautelan la información pero sobre todo clasifica de forma ordenada las actividades que realiza los usuarios de los computadores-

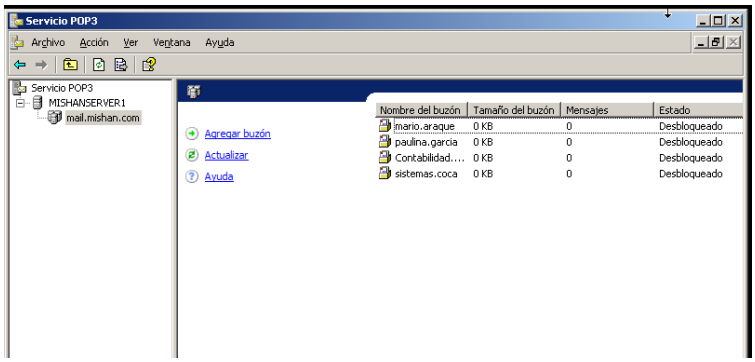
Es importante hacer notar que MISHAN es un dominio de un bosque que se encuentra configurado localmente en el Coca pero q también se tiene en Quito y que mediante replicas de señal estos pueden fusionarse aunque no ha sido el caso todavía pero la opción existe con la finalidad de optimizar recursos de comunicaciones.

Grafica 3.16. : Ilustración de los usuarios que deben logearse para ingresar
Fuente: Mario Araque B.



Esta es la forma clásica de creación y administración de usuarios que tiene el dominio de Windows 2003 server con la particularidad de que en la empresa para la creación de usuarios se maneja lo que son grupos de trabajo los mismos que abarcan a los usuarios de acuerdo a la función que se desempeña en la empresa.

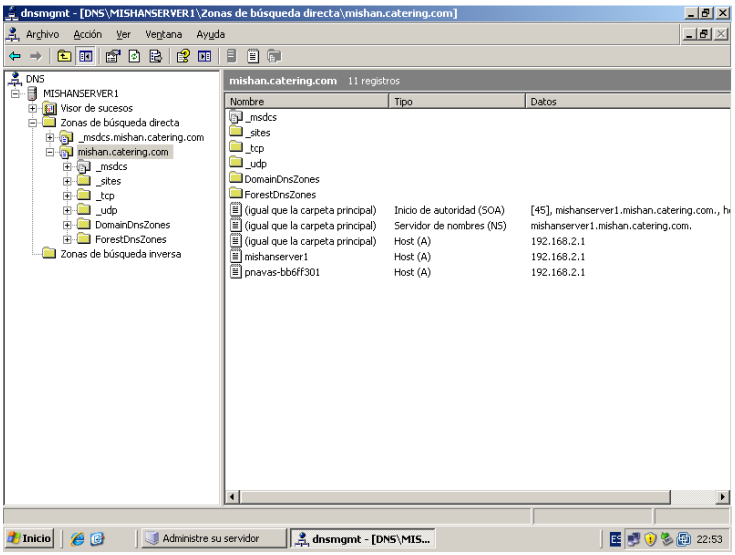
Grafica 3.17. : Usuarios del e mail corporativo con Outlook
Fuente: Mario Araque B.



En la empresa se tiene configurado una intranet de Microsoft la misma que permite la configuración del correo electrónico interno pero se lo realiza con un mínimo grupo de usuarios ya que las comunicaciones todavía no

abastece como para que todos los usuarios de computadores pueda acceder a este servicio por lo que la alternativa planteada era la configuración del servidor de smb en Linux para copiar y enviar archivos desde El coca a Quito y viceversa.

Grafica 3.18. : Configuración del servidor de dhcp
Fuente: Mario Araque B.



El servidor de dhcp es el que se encarga de proveer las direcciones ip dinámicas a todos los usuarios de las redes en la empresa se lo hace de esta manera ya que estamos precautelando de que siempre tengan red para que accedan a él internet o imprimir.