ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERIA

USO DE VPNS PARA LA RED CORPORATIVA DE UNA EMPRESA FLORICOLA

PROYECTO PREVIO A LA OBTENCIÒN DEL TITULO DE INGENIERO INFORMÁTICO MENCION EN REDES

WASHINGTON EDUARDO SINCHIGUANO PANCHI
EDWIN VINICIO USIÑA TOCAIN

DIRECTOR: ING. CARLOS BADILLO

Quito, marzo 2006

DECLARACIÒN

Nosotros Washington Eduardo Sinchiguano Panchi, Edwin Vinicio Usiña Tocain declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de esta declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

----------	**----------**
WASHINGTON EDUARDO	**EDWIN VINICIO**
SINCHIGUANO PANCHI	**USIÑA TOCAIN**

CERTIFICACION

Certifico que el presente trabajo fue desarrollado por Washington Eduardo Sinchiguano Panchi y Edwin Vinicio Usiña Tocain, bajo mi supervisión.

ING. CARLOS BADILLO
DIRECTOR DEL PROYECTO

Deseo dejar constancia de mi mas profundo y sincero a agradecimiento a Dios, que con su infinita divinidad supo guiarme en todo el trayecto para al elaboración de este proyecto.

Además resulto invaluable la ayuda brindada por el Ing. Carlos Badillo, quien con su experiencia y conocimientos supo guiarme de manera acertada en el desarrollo y finalización de este presente proyecto.

De corazón un profundo respeto y agradecimiento a mis Padres quienes con su ejemplo, hicieron de mi un hombre de bien y a mi esposa por su comprensión y apoyo incondicional.

Washington Sinchiguano

Agradezco a Dios por la oportunidad que he tenido de aprender, mejorar y de crecer junto a personas tan valiosas para mí.

Agradecimiento especial para mi tutor, Ing. Carlos Badillo, por su amistad, paciencia y su constante apoyo durante el desarrollo de esta tesis. De igual forma deseo expresar mi agradecimiento al Tribunal Calificador de este proyecto: Ing. Maritzol Tenemaza e Ing. Cesar Gallardo.

Mis más sinceros agradecimientos, cariño y respeto a mis Madres Gladys Tocaín y Magda Guevara quien con su ayuda, apoyo y ejemplo han hecho de mi un hombre de bien. Gracias también a Kruskaya Alberca, quien fue la inspiración y fortaleza en los momentos más difíciles de todo el proceso estudiantil y profesional de mi vida. Sin importar donde este, un millón de gracias.

Edwin Usiña

CONTENIDO

INDICE DE FIGURAS

CAPITULO 1

CAPITULO 2

CAPITULO 3

CAPITULO 4

INDICES DE TABLAS

CAPITULO 1

CAPITULO 2

CAPITULO 3

CAPITULO 4

RESUMEN

El presente proyecto esta conformado por cinco capítulos distribuidos de la siguiente forma: El capitulo 1, describe la parte teórica de Redes Privadas Virtuales, sus características, tipos de arquitectura, criptografía y tecnologías más utilizadas. En el capitulo 2 se describe las situación actual de la empresa, la distribución de las fincas y matriz, equipos que posee y la problemática de no contar con un sistema de producción en línea, por la falta de comunicación entre las fincas y la oficina central. En el capitulo 3 se analiza la factibilidad de implantar la interconexión que permita la transferencia de datos con un estándar se seguridad elevado, como también, se analiza diferentes alternativas de enlaces dedicados, VPN's con hardware y software, además se presente un análisis de costos que debe incurrir la empresa con cada una de estas alternativas. En el capitulo 4 se analiza las diferentes propuestas de interconexión y se toma en cuenta los aspectos técnicos para analizar estas opciones, con la implantación de un prototipo de VPN con hardware y software se pretende mostrar la factibilidad, finalmente en el capitulo 5 se saca conclusiones y recomendaciones del proyecto.

XIX

PRESENTACION

El presente trabajo comprende el análisis y la implementación de un prototipo para la interconexión de las fincas con la oficina matriz de una empresa florícola a través de una VPN (Virtual Private Network). Se analizan las necesidades que la empresa requiere para una comunicación segura y confiable, presentando propuestas de enlaces dedicados y VPN a través del Internet con una infraestructura de hardware y software. Se realiza un análisis costo-beneficio para cada una de las alternativas, determinando que la opción VPN con Internet es la más aceptable por su bajo costo y facilidad de configuración. Se implementa un prototipo con las arquitecturas de hardware (Router VPN DLINK) y software (Linux ipsec-tools), simulando la interconexión de una finca con la oficina matriz. Se levanta el servicio de replicación de datos en MSSQLServer para la comprobación del funcionamiento del túnel virtual, se garantiza un nivel de seguridad aceptable con la utilización de certificados digitales X509.

CAPITULO 1

1. REDES PRIVADAS VIRTUALES (VPNs)

1.1 INTRODUCCIÓN Y CONCEPTOS BASICOS DE UNA VPN

Las Redes Privadas Virtuales (VPN – Virtual Private Network) deben su creciente popularidad al hecho que, las grandes y pequeñas empresas han buscado la forma de utilizar el Internet público para aumentar la movilidad, mejorar la productividad de los empleados y contribuir al desarrollo.

Las VPNs permiten a los usuarios remotos que trabajen en la calle, en el hogar o en otras oficinas tener acceso a la red privada LAN de la compañía desde cualquier parte del mundo, utilizando su computadora portátil o computadora del hogar a través del Internet.

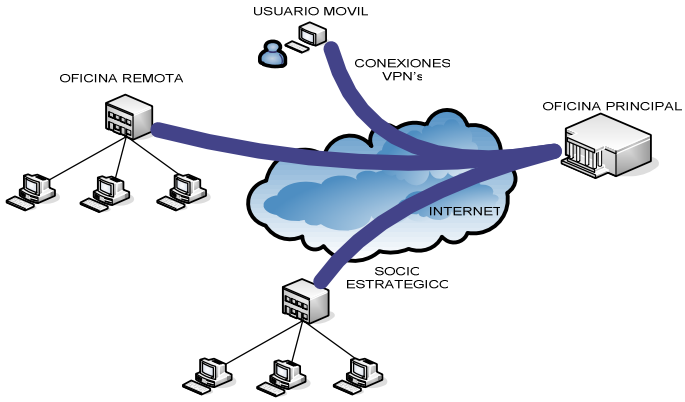

Figura 1.1: Ejemplos de VPN.

1.1.1 DEFINICIÓN DE UNA VPN.

Red Privada Virtual (VPN – RFC 4026): Una red privada virtual (Virtual Private Network) es una red privada que se extiende mediante un proceso de encapsulación y de encriptación de los paquetes de datos a distintos puntos remotos, mediante el uso de infraestructuras públicas de transporte, más conocida como Internet. Los paquetes de datos de la red privada viajan por medio

de un "túnel" definido en la red pública. La Red Privada Virtual, tiene su definición de acuerdo a su nombre, tal como se indica a continuación:

Virtual: Virtual porque al momento del establecimiento de una conexión VPN el cliente virtualmente extiende la red de la empresa hasta donde él esté, esto lo hace trabajar lógicamente dentro de la misma empresa, pero dentro de un concepto "virtual".

Private (Privada): Privada porque el concepto de privacidad se mantiene una vez implementada la VPN. La privacidad en las comunicaciones de la empresa es parte esencial en las políticas de seguridad. Las comunicaciones a través de VPN mantiene su privacidad sobre medios públicos ya que van encapsuladas dentro de un túnel encriptado y autentificado.

Network (Red): La VPN trabaja a nivel de red (NETWORK), de allí la capacidad que tiene de interconectar, extender y comunicar redes o segmentos de redes. Las VPNS también pueden crear túneles de comunicación internos entre una máquina y un servidor dentro de la red de la misma empresa. Hay empresas que tienen VPNS dentro de sus propias redes, para asegurar comunicaciones con servidores críticos**.**

En el caso de acceso remoto, la VPN permite al usuario acceder a su red corporativa, asignándole a su servidor remoto las direcciones y privilegios de la misma, aunque la conexión la haya realizado por medio de un acceso a Internet público.

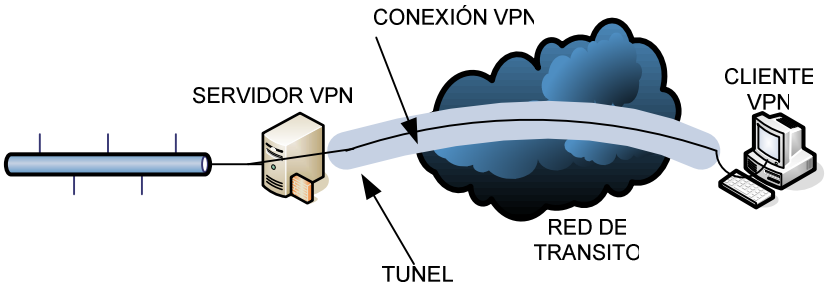

Figura 1.2: Acceso remoto a la red privada

Túneles: Un túnel es el que permite conectar un protocolo a través de otro, estableciendo una comunicación directa entre los dos extremos, a continuación se listan algunos ejemplos:

- Túnel SNA (System Network Architecture): para enviar paquetes IP
- MBone: túneles multicast sobre redes unicast.
- 6Bone: túneles IPv6 sobre redes IPv4.
- Túneles IPv4: para hacer enrutamiento desde el origen.

1.1.2 CONCEPTOS BASICOS MÁS UTILIZADOS

***a) Escalabilidad*:** Los elementos deben ser escalables dentro de las plataformas VPN, se debe tener en cuenta la habilidad de adaptar la VPN a diferentes ambientes y plataformas, en el cual se tiene un ancho de banda cambiante y las necesidades de la conectividad.

b) Seguridad (Tunneling): La encriptación y autenticación del paquete son necesarios para seguridad de transporte en redes públicas, razón por la cual la VPN, usa el túnel (*tunneling*) como mecanismo de seguridad

c) Servicios de la VPN: Deben ser tomados en cuenta de acuerdo al ancho de banda y QoS a ser usados, así como también se debe considerar la congestión de red, tráfico generado y clasificación del paquete. Esto va a depender del protocolo que se va a utilizar para la comunicación y transmisión de datos. Los principales servicios que se pueden tener a través de una VPN son los siguientes:

- ***Interconexión ATM / FR[1] y NNI (Interfaces Network to Network):*** Implica un mayor alcance en la implementación de los diversos servicios a ser utilizados.

[1] **ATM** (Asynchronous Transfer Mode), **FR** (Frame Relay), son tecnologías para transmisión de datos.

- ***Servicio de acceso remoto (RAS):*** Este servicio puede admitir dos modelos de RAS para proporcionar acceso general de Internet a través de la VPN: reservas de túnel y reservas de pasarela (Gateway).
- ***Acceso seguro a Internet*****:** Seguridad en el acceso a Internet a través de los Firewalls, que permiten aislar red LAN de una empresa del mundo.
- ***Acceso dedicado a Internet:*** Permite tener un acceso seguro a la VPN y un acceso directo a Internet
- ***Acceso a fracciones de la velocidad básica:*** Se pueden tener facilidades de fraccionamiento de las velocidades de acceso a Internet así, por ejemplo: 64K, 128K e incrementos de 128K.
- ***Control de Ancho de Banda:*** Se puede repartir el ancho de banda de acuerdo a las aplicaciones que van a ser transmitidas por la VPN, de forma que se puedan controlar los costos.
- ***Compartición de carga:*** Compartición de carga IP para cada paquete entre múltiples conexiones a través de un mismo servidor.

Todos estos servicios encierran varias ventajas en una solución VPN, tal como son: Confiabilidad, Calidad de Servicio, Performance, Conectividad Universal, Seguridad, Reducción de costos, Simplicidad.

1.1.3 ELEMENTOS DE UNA VPN

Para la correcta implementación de una VPN, es necesario conocer una serie de elementos y conceptos entre los que se destacan los siguientes:

a) Acceso a Internet: Existen muchas maneras de conectarse a Internet: a través de un módem, cable de banda ancha, DSL (Digital Subscriber Line), satélite de banda ancha, ISDN (Integrated Services Digital Network) y Líneas T[2]. No todos los tipos de conexiones están disponibles en cada área geográfica. Así

[2] **Línea T:** El sistema T cargador es un enlace directo a Internet. Las líneas T son muy costosas y las usan los ISPs para proporcionar a los suscriptores con acceso a Internet o a los negocios con lo necesario para colocar redes privadas de punto a punto.

que su selección está limitada a lo que los proveedores locales pueden ofrecerle y cuyas características son:

- **Módem/Conexión telefónica:** Este es el método más común de conectarse a Internet. Debido a que los módems de conexión telefónica funcionan en una línea telefónica normal.

- ***Cable de Banda ancha:*** Los módems de cable lo conectan a Internet a través de la línea de TV por cable. Muchas compañías de cable ofrecen ahora acceso a Internet, así como a TV.

- ***DSL (Digital Subscriber Line):*** *Hay* varias formas de suscribirse a una línea digital que trabaja a varias velocidades y distancias desde la subestación telefónica más cercana. DSL puede incrementar su velocidad de conexión hasta 10 veces comparado con un módem de acceso telefónico estándar.

- ***Banda ancha satelital:*** El servicio de banda ancha satelital de dos vías transmite datos vía satélite a una antena de disco en la casa. Su principal ventaja es llegar a sitios inaccesibles donde los sistemas de comunicaciones tradicionales no pueden llegar (radio, telefonía, wireless, etc.). Su principal desventaja son los tiempos de retardo debido al doble salto satelital.

- ***ISDN (*Integrated Services Digital Network*):*** ISDN son las siglas en inglés de Integrated Services Digital Network (Red de servicios digitales integrales). Las conexiones digitales ofrecen menos errores en la transmisión, lo cual significa que pueden obtener gráficas, páginas Web, sonido y multimedia hasta cuatro veces más rápido que con módems tradicionales.

  Conexiones Inalámbricas

  - **Wi-Fi:** Una vez que los estándares IEEE 802.11b para comunicaciones inalámbricas, permiten tener acceso a Internet sin cableado, en radios de

corto alcance para computadoras estacionarias, laptops, y asistentes personales (PDAs).

- **Bluetooth:** Es una tecnología con un rango de sólo 9 metros y una conexión más lenta de 720-1,000 Kbps. Permite conectarse a Internet a través de teléfonos celulares y PDAs.

b) Servidor VPN: Puede ser una PC (o un equipo especial, en hardware y software) conectada a Internet esperando por conexiones de usuarios VPN y si estos cumplen con el proceso de autenticación, el servidor aceptará la conexión y dará acceso a los recursos de la red interna. Existen equipos especiales que pueden ser servidores de VPNs, entre los más utilizados se tienen: *Routers* (Ruteadores), *Bridges* (Puentes), *Gateways* (Traductores de protocolos) y F*irewalls* (Cortafuegos) cuyas características son:

- ***Router:*** Un *router (enrutador o encaminador*) es un dispositivo hardware o software de interconexión de redes de ordenadores/computadoras que opera en la capa 3 (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hacen pasar paquetes de datos entre redes, tomando como base la información de la capa de red.

  Los routers, toman decisiones basándose en diversos parámetros. El más importante es la dirección de la red hacía la que va destinado el paquete (En el caso del protocolo *IP* esta sería la dirección IP). Es importante recalcar que los routers a más del direccionamiento IP, vienen con opciones adicionales de servicios de red tal como; autenticación, cifrado y con soporte para establecer conexiones WAN con VPNs.

- ***Puentes o Bridges:*** Estos equipos se utilizan así mismo, para interconectar segmentos de red, (amplía una red que ha llegado a su máximo, ya sea por distancia o por el número de equipos) y se utilizan cuando el tráfico no es excesivamente alto en las redes, pero interesa aislar las colisiones que se

produzcan en los segmentos interconectados entre sí. Estos equipos también soportan conexiones WAN, a través de VPNs.

- ***Gateways:*** También llamados *traductores de protocolos*, son equipos que se encargan >como su nombre indica<, de servir como intermediarios entre los distintos protocolos de comunicaciones, para facilitar la interconexión de equipos distintos entre sí. Su forma de funcionar es que tienen duplicada la pila OSI, es decir, la correspondiente a un protocolo y paralelamente, la del otro protocolo. Reciben los datos encapsulados de un protocolo, los van desencapsulando hasta el nivel más alto, para posteriormente ir encapsulando los datos en el otro protocolo desde el nivel más alto al nivel más bajo, y vuelven a dejar la información en la red, pero ya traducida. Estos también pueden venir con soporte de VPNs.

- ***Firewall (Cortafuegos):*** Un firewall es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

  Un firewall, es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean, permite o deniega su paso.

  Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el Web, el correo, chat, etc. Dependiendo del servicio el firewall decide si permite o no el tráfico. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o denegarla. Estos equipos son los más idóneos para establecer la comunicación a través de VPNs, ya que viene con políticas se seguridad para el tráfico e la red.

c) Cliente VPN: Es básicamente una PC (o un equipo especial de los descritos en el literal b.), la cual puede ser un usuario remoto de otra LAN. El cliente puede estar en la misma red (misma empresa) o en una red distinta (cualquier parte del mundo – Acceso remoto). El cliente VPN necesita autentificarse al momento de establecer la conexión con el servidor, y esto lo puede realizar a través de un nombre de usuario y password, y si se desea aumentar el nivel de seguridad, se puede hacer uso de certificados y firmas digitales.

***d) El túnel VPN*:** Esta compuesto por dos máquinas o equipos (routers, firewalls) que permiten establecer la comunicación en los dos extremos, a través de protocolos de autentificación y de encriptación de la información, con lo cual se establece un canal seguro para la transferencia de la información.

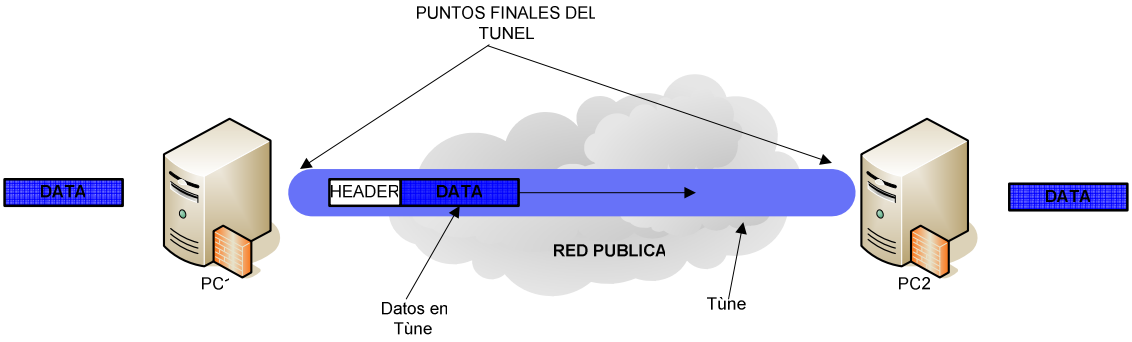

Figura 1.3: Esquema del Túnel VPN.

e) Protocolos de la VPN: Son los que permiten establecer las reglas de comunicación entre los extremos que van a formar parte de la VPN, permitiendo crear un "túnel" confiable entre ambas máquinas, sabiendo quien está en cada extremo y validando que el otro sea realmente la persona en la que se confía cada vez que se reciben datos. En los literales: 1.1.5.2, 1.1.5.3 y 1.1.6 del presente capítulo, se describen con mayor detalle los protocolos más usados por las VPNs.

f) Red Pública: Consiste en el acceso a los servicios proporcionados a través de redes públicas de telecomunicaciones.

Las redes públicas de datos tienen como objetivo poner a disposición de los usuarios medios de comunicación entre ubicaciones distintas, para permitir la transmisión de información digital.

De forma simplificada, este tipo de redes puede entenderse como el equivalente de la red telefónica de voz para los ordenadores y cualquier tipo de equipo que procese información digital.

***g) Tarjetas de interfaz de red*:** Las tarjetas de interfaz de red (*NICs - Network Interface Cards*) son adaptadores instalados en un dispositivo, conectándolo de esta forma en red. Es el pilar en el que sustenta toda red local, y el único elemento imprescindible para enlazar dos ordenadores a buena velocidad (excepción hecha del cable y el software).

La tarjeta de interfaz obtiene la información de la PC, la convierte al formato adecuado y la envía a través del cable a otra tarjeta de interfaz de la red local. Esta tarjeta recibe la información, la traduce y la envía a la PC para que ésta la pueda entender.

1.1.4 USOS Y CONEXIONES DE UNA VPN

Hay varias posibilidades de conexiones VPN, esto será definido según los requerimientos de cada organización. Se recomienda hacer un buen relevamiento, a fin de obtener datos para enlazar dos o más redes, o si solo se conectarán usuarios remotos. Las posibilidades de conexiones que se pueden tener son:

a) **Cliente a Servidor (Client to Server):** Un usuario remoto que solo necesita servicios o aplicaciones que corren en el mismo servidor VPN.

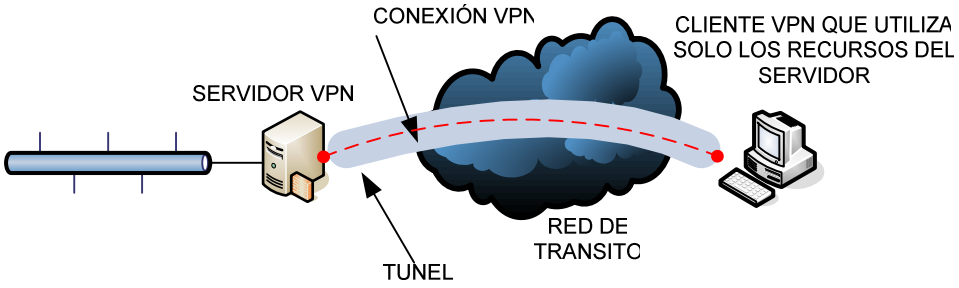

Figura 1.4: Conexión VPN Cliente a Servidor

b) Cliente a Red Interna (Client to LAN): Un usuario remoto que utilizará servicios o aplicaciones que se encuentran en uno o más equipos dentro de la red interna.

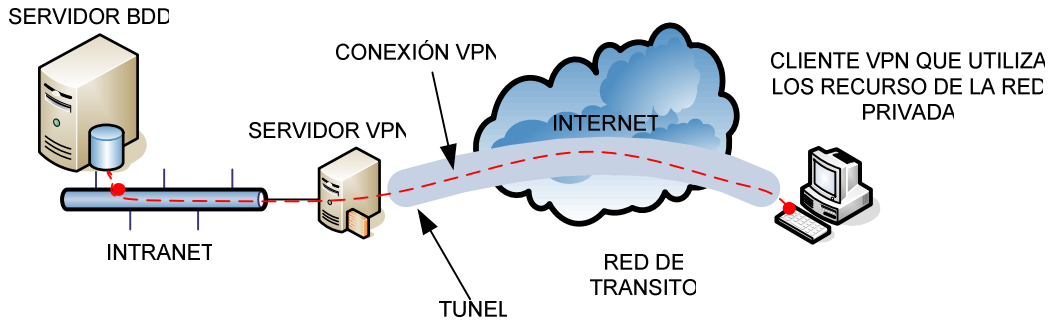

Figura 1.5: Conexión VPN Cliente a Red Interna

c) Red Interna a Red Interna (LAN to LAN): Esta forma supone la posibilidad de unir dos intranets, a través de dos enrutadores. El servidor VPN en una de las intranets y el cliente VPN en la otra. Aquí entran en juego el mantenimiento de tablas de ruteo y enmascaramiento.

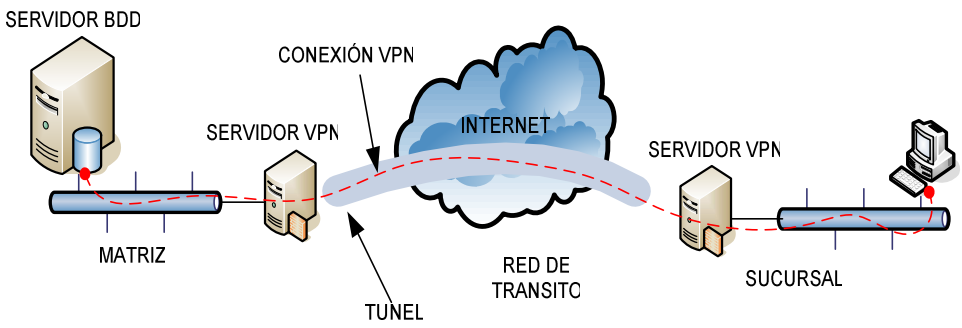

Figura 1.6: Conexión VPN LAN a LAN

1.1.5 CRIPTOGRAFÍA

Criptografía está definida como la "*técnica de escribir con clave secreta",* o más bien, es un conjunto de técnicas que tratan sobre la protección y ocultamiento de la información frente a observadores no autorizados dentro de una red.

La criptografía es una alternativa que permite tener redes seguras, y esto se lo consigue con la ayuda de protocolos y algoritmos de encriptación, logrando de esta manera, proteger información crítica que debe viajar por canales de transmisión inseguros, como lo es el Internet.

1.1.5.1 Algoritmos Criptográficos

En la actualidad, prácticamente todas las aplicaciones criptográficas emplean computadoras para realizar sus cálculos, y por tanto las computadoras convencionales están diseñadas para ejecutar complejos algoritmos.

Se define a los algoritmos como una secuencia finita y ordenada de instrucciones elementales que, dados los valores de entrada de un problema, en algún momento finaliza y devuelve la solución. Estos algoritmos son utilizados para proteger la información y evitar así, ser leída por personas no autorizadas.

En términos generales hay tres tipos de algoritmos criptográficos: *a) de clave secreta o privada (simétricos), b) de clave pública (asimétricos) y c) de hashing.*

1.1.5.1.1 Algoritmos de Clave Privada (Simétricos)

Los algoritmos de clave privada son simétricos en el sentido de que ambos usuarios en la comunicación comparten una única clave. Dentro de este tipo de

algoritmos los más comunes son: ***DES*** (*Data Encryption Standard*) e ***IDEA*** (*International Data Encryption Algorithm*).

Data Encryption Standard (DES): DES encripta un bloque de 64 bits de texto usando una clave de 64 bits. De hecho, la llave sólo tiene 56 bits útiles, el último bit de cada uno de los 8 Bytes de la llave es un bit de paridad para ese Byte. DES tiene tres fases distintas:

- Los 64 bits en el bloque son permutados (cambiados de orden dentro del bloque).
- A los datos resultantes más la clave se les aplica 16 veces una misma operación.
- El inverso de la permutación original es aplicado al resultado.

No hay ninguna prueba matemática de que DES sea un algoritmo seguro. Aunque la única manera conocida de romper DES es probando todas las posibles claves de 56 bits (de hecho, en media, sólo habría que probar la mitad), Este tiempo es considerado marginalmente seguro en diversos ámbitos, y por esta razón se utiliza Triple-DES (3DES), que es encriptar los datos tres veces, utilizando tres claves distintas, o bien utilizando dos claves, repitiendo la primera en la tercera aplicación de DES.

***IDEA (International Data Encryption Algorithm)*:** Al ser DES un algoritmo inseguro, dos prestigiosos criptógrafos (Xuejia Lai y James Massey), desarrollaron a finales de la década de los ochenta el algoritmo compatible con DES (para aprovechar el gran número de equipos que utilizan este algoritmo), y con una robustez garantizada por la clave de 128 bits que utiliza este cifrador de bloques y las complejas operaciones utilizadas para evitar el éxito de un posible atacante.

El algoritmo IDEA está siendo ampliamente aceptado en diversas aplicaciones informáticas orientadas a la seguridad de los datos. Numerosos programas

destinados a trabajar en red, utilizan ya este algoritmo como el principal decifrador.

1.1.5.1.2 Algoritmos de Clave Pública (Asimétricos)

En contraste con un par de usuarios compartiendo una única clave, la criptografía de clave pública implica que cada usuario posea una *clave privada* no compartida con nadie y una *clave pública* que es distribuida de manera que todos los usuarios la conozcan. Para enviar un mensaje seguro a un usuario de este tipo de algoritmo, se encripta el mensaje utilizando la conocida clave pública del destinatario. El usuario desencripta el mensaje utilizando su propia clave privada. El RSA (Rivest, Shamir, Adleman) es el más conocido de los algoritmos de clave pública.

***RSA (Rivest, Shamir, Adleman)*:** RSA es un algoritmo muy diferente a DES, no solo porque requiere el uso de claves diferentes para el encriptado (clave pública) y desencriptado (clave privada), sino también porque está basado en la teoría de números. El hecho de encriptar o desencriptar un mensaje es descrito como una función simple, pero esta función requiere un enorme poder de computación. RSA usa claves de 512 bits, siendo más costoso de calcular que DES.

1.1.5.1.3 Algoritmos del Tipo Hashing

El tercer tipo de algoritmo criptográfico es conocido como función *hash* (troceado) o de *message digest* (la función *hash* genera un resumen de mensaje o huella digital). A diferencia de los anteriores algoritmos, este tipo no requiere el uso de claves. De hecho, la idea es transformar un mensaje potencialmente largo, en un número pequeño de tamaño fijo.

La mejor manera de ver este algoritmo es como un calculador de un *checksum*[3] *criptográfico* sobre el mensaje. Este checksum criptográfico protege al receptor de posibles cambios (maliciosos) en el mensaje. Esto es posible dado que estos algoritmos criptográficos de hash, son cuidadosamente seleccionados para ser funciones de un solo sentido: dado un determinado checksum criptográfico para un mensaje, es virtualmente imposible de adivinar qué mensaje produjo ese checksum. Dicho de otra manera, no es posible hallar mediante cómputos dos mensajes que generen el mismo checksum criptográfico. Uno de los algoritmos de hash más utilizados es el Message Digest v5 (MD5). Además de las propiedades anteriormente citadas, MD5 es mucho más rápido de calcular que DES o RSA.

MD5 (Boletín de Mensajes 5): MD5 es un algoritmo hash utilizado para autenticar los datos de un paquete, la mayoría de equipos (routers y firewalls), utilizan MD5, Una función tipo hash, es una algoritmo de cifrado unidireccional que toma como entrada un mensaje de longitud abierta y produce un mensaje de salida de longitud fija (huella digital).

1.1.5.2 Protocolos para asegurar la integridad de los mensajes

La integridad de un mensaje esta determinada por la imposibilidad de ser modificado cuando dos personas establecen una comunicación a través de una red pública. A continuación se describen tres alternativas para asegurar la integridad de los mensajes. El primero usa RSA, pero como es bastante lento de calcular, los dos siguientes usan MD5 en combinación de RSA para aumentar la eficiencia del proceso.

[3] Checksum: Función que permite realizar una verificación de errores en un mensaje enviado.

1.1.5.2.1 Firma Digital usando RSA

Una *firma digital,* es un caso especial de código de integridad de mensaje, donde el código sólo puede ser generado por uno de los usuarios. El algoritmo de firma digital más fácil de entender es una firma RSA: como un usuario es el único que conoce su clave privada, este participante usa esta clave para generar la firma. El otro usuario puede verificar la firma utilizando la correspondiente clave pública. Para firmar un mensaje, se encripta con la clave privada, y para verificar una firma, se desencripta utilizando la clave pública del supuesto emisor.

1.1.5.2.2 MD5 con clave

Dos usuarios se ponen de acuerdo para compartir una clave secreta k. El emisor entonces aplica MD5 a la concatenación del mensaje (m) con esta llave. La clave k es borrada del mensaje una vez MD5 ha finalizado. Lo que el emisor envía es: $m + MD5(m + k)$. El receptor del mensaje aplica MD5 a la concatenación del mensaje con la clave secreta k. Si el resultado coincide con el checksum enviado con el mensaje, entonces el mensaje debe haber sido enviado por el usuario que tiene la clave.

1.1.5.2.3 MD5 con firma RSA

El emisor aplica MD5 sobre el mensaje original que quiere proteger, generando un checksum. Entonces firma (encripta) el checksum con su clave privada RSA. Es decir, el emisor no firma el mensaje entero, tan solo el checksum.

El receptor verifica el mensaje:

- Aplicando MD5 sobre el mensaje recibido.
- Desencriptando el checksum con la clave pública del emisor.

- Comparando los dos checksums.

Si coinciden significa que el mensaje no fue modificado desde que el emisor calculó el checksum y lo firmó.

1.1.5.3 Protocolos para Asegurar la Autenticación de los Mensajes

1.1.5.3.1 E AP (Extensible Authentication Protocol – RFC 2284)

El Protocolo de autenticación extensible (EAP) es una extensión del Protocolo punto a punto (PPP). EAP se desarrolló como respuesta al aumento de la demanda de autenticación de usuarios de acceso remoto que utilice otros dispositivos de seguridad. EAP proporciona un mecanismo estándar para aceptar métodos de autenticación adicionales junto con PPP. Al utilizar EAP, se pueden agregar varios esquemas de autenticación, entre los que se incluyen tarjetas de identificación, contraseñas de un solo uso, autenticación por clave pública mediante tarjetas inteligentes, certificados y otros. EAP, junto con los métodos de autenticación EAP de alto nivel, es un componente tecnológico crítico para las conexiones seguras a través de una red privada virtual (VPN), puesto que ofrece mayor seguridad frente a ataques físicos o de diccionario y de investigación de contraseñas, que otros métodos de autenticación, como CHAP.

1.1.5.3.2 MS-CHAP (RFC 2433)

Protocolo de autenticación por desafío mutuo de Microsoft (MS-CHAP)

Microsoft ha creado MS-CHAP para autenticar estaciones de trabajo Windows remotas, y proporciona la funcionalidad a la que los usuarios de LAN están habituados, al mismo tiempo que integra los algoritmos de cifrado y de hash (El objetivo de una función hash segura es producir una “huella dactilar” en el mensaje).

Siempre que es posible, MS-CHAP es coherente con el estándar CHAP. Su paquete de respuesta tiene un formato diseñado específicamente para los productos de red de Windows NT y Windows 2000, y Windows 95 y posteriores. Además, MS-CHAP no requiere el uso de contraseñas de texto simple o con formato reversible.

1.1.5.3.3 MS-CHAP V2 (RFC 2759)

Protocolo de Autenticación por Desafío Mutuo de Microsoft versión 2 (MS-CHAP V2)

Hay disponible una nueva versión del Protocolo de autenticación por desafío mutuo de Microsoft (MS-CHAP v2). Este nuevo protocolo proporciona una autenticación mutua, claves iniciales de cifrado de datos más seguras y claves de cifrado diferentes para envío y recepción. Para minimizar el riesgo de comprometer las contraseñas durante los intercambios de MS-CHAP, MS-CHAP v2, no acepta el cambio de contraseña de MS-CHAP y no transmite la contraseña codificada.

Para las conexiones de red privada virtual (VPN), Windows 2000 Server ofrece MS-CHAP v2 antes de ofrecer el protocolo MS-CHAP heredado. Los clientes de Windows actualizados aceptan MS-CHAP v2 cuando se les ofrece. Las conexiones de acceso telefónico a redes no se ven afectadas.

1.1.5.3.4 PAP (RFC 1334)

Protocolo de autenticación de contraseña (PAP)

El Protocolo de autenticación de contraseña (PAP) utiliza contraseñas en texto simple (no cifradas) y es el protocolo de autenticación menos sofisticado.

PAP se suele utilizar, si la conexión y el servidor no pueden negociar una forma de validación más segura. Puede que necesite utilizar este protocolo si va a llamar a un servidor que ejecute un sistema operativo distinto de Windows.

1.1.5.4 Certificados Digitales

Un certificado es un tipo especial de documento firmado digitalmente. Viene a decir: *Certifico que la clave pública de este documento pertenece a la entidad mencionada en el mismo, firmado X*. Usualmente X será una *autoridad de certificación* (CA), una entidad administrativa que está en el negocio de expender certificados. Este certificado sólo es útil para un usuario que ya tenga la clave pública de X, porque esta clave es necesaria para verificar la firma.

Uno de los mayores estándares para certificados es conocido como X.509. Este estándar deja muchos detalles abiertos, pero especifica una estructura básica. Los componentes de un certificado deben incluir claramente:

- El nombre de la entidad que está siendo certificada.
- La clave pública de dicha entidad.
- El nombre de la autoridad de certificación.
- Una firma digital.

1.1.5.4.1 Distribución de la Clave Pública (Certificados X.509)

Suponer que un usuario A quiere dar a conocer su clave pública a un usuario B. No puede usar un simple e-mail para enviarla a B, porque sin la clave pública de A, B no tiene manera de autentificar que la clave realmente vino de A. Alguien podría enviar una clave pública a B y decir que quien la envía es A. Si A y B son personas que se conocen, pueden reunirse en una habitación y A puede entregar a B la clave pública directamente, ya sea en un disket o mediante una tarjeta. Esta solución, sin embargo, pasa por el hecho de que A y B puedan coincidir en una habitación, cosa que no siempre es posible. La solución básica a este problema reside en el uso de *certificados digitales*.

Los certificados X.509 pueden usar diferentes algoritmos para el firmado digital, de manera que el certificado debe especificar que algoritmo usa. Otro posible componente del certificado es la fecha de expiración, cuya utilidad se verá a continuación.

1.1.5.4.2 Revocación de Certificados

Cuando un usuario sospecha que alguien ha descubierto su clave privada. Puede haber un número indeterminado de certificados que afirman que es el propietario de la clave pública correspondiente con esa clave privada. La persona que ha descubierto su clave privada tiene todo lo necesario para suplantarle: certificados válidos y su clave privada. Debe de haber alguna manera de revocar o deshacer dichos certificados.

La solución al problema es bastante simple. Una autoridad de certificación puede expender una *lista de revocación de certificados* (CRL), que es una lista firmada digitalmente de certificados que han sido revocados. Esta lista se actualiza periódicamente y se hace pública.

Cuando A recibe un certificado de B que quiere verificar, A consultará primero la última CRL expendida por la autoridad de certificación. Mientras el certificado no haya sido revocado, es válido. Nótese que si los certificados tuvieran una validez ilimitada, la CRL se volvería cada vez más grande, dado que no se podría borrar un certificado por miedo a que alguna copia de dicho certificado revocado pudiera ser utilizada. Sin embargo, añadiendo una fecha de expiración al certificado cuando es expendido, se limita el tiempo para que un certificado revocado necesite estar en la CRL.

1.1.6 PROTOCOLOS USADOS PARA LAS VPNS

Cada tipo de implementación utiliza diversas combinaciones de protocolos para garantizar las tres características fundamentales mencionadas anteriormente, como son: autenticación, integridad y confidencialidad.

El protocolo estándar de hecho es el IPSEC, pero también existen PPTP, L2TP, SSL/TLS, SSH, etc. Cada uno con sus ventajas y desventajas en cuanto a seguridad, facilidad, mantenimiento y tipos de clientes soportados.

1.1.6.1 PPTP (Point to Point Tunneling Protocol - RFC 2631)

Este es uno de los protocolos más populares y fue originalmente diseñado para permitir el transporte (de modo encapsulado) de protocolos diferentes al TCP/IP a través de Internet. Fue desarrollado por el foro PPTP, el cual está formado por las siguientes empresas: Ascend Communications, Microsoft Corporations, 3Com, E.C.I. Telematics y U.S. Robotics (ahora 3Com).

Básicamente, PPTP lo que hace es encapsular los paquetes del protocolo punto a punto **PPP** (*Point to Point Protocol*) que a su vez ya vienen encriptados en un paso previo para poder enviarlos a través de la red. El proceso de encriptación es gestionado por PPP y luego es recibido por PPTP, este ultimo utiliza una conexión TCP llamada conexión de control para crear el túnel y una versión modificada de la Encapsulación de Enrutamiento Genérico (**GRE**, *Generic Routing Encapsulation*) para enviar los datos en formato de datagramas IP, que serían paquetes PPP encapsulados, desde el cliente hasta el servidor y viceversa.

El proceso de autenticación de PPTP utiliza los mismos métodos que usa PPP al momento de establecer una conexión, como por ejemplo **PAP** (Password Authenticaction Protocol) y CHAP (Challenge-Handshake Authentication Protocol). El método de encriptación que usa PPTP es el *Microsoft Point to Point*

Encryption, **MPPE**, y solo es posible su utilización cuando se emplea CHAP (o MS-CHAP en los NT) como medio de autenticación.

1.1.6.2 L2TP (Layer To Tunneling Protocol - RFC 2661)

L2TP utiliza paquetes UDP para la creación y mantenimiento del túnel. En Windows 2000 y posteriores se utiliza la puerta UDP 1701. Para la creación de un túnel virtual el cliente manda un paquete UDP al servidor VPN. Si, un paquete UDP. Como L2TP puede mantener la integridad de los datos si utiliza UDP, utiliza message sequencing (esto es similar a los ACK en TCP).

La autentificación en L2TP sobre IPsec (L2TP/IPSec) es a nivel de usuario y máquina. La autentificación entre las máquinas (que es la que hace segura la creación del túnel y a los end-points) se hace intercambiando los certificados de las máquinas. Esto es: el cliente le entrega una caja y una llave al servidor para que le envíe los datos en esa caja cerrada (llave pública del cliente). El servidor le manda también una caja con una llave al cliente para que le envíe los datos en esa caja cerrada (llave privada del servidor). Como estas cajas están cerradas nadie las puedes abrir, excepto los dueños de las cajas, ya que ellos tienen la copia de la llave que puede abrirlas. (la llave que se intercambian entre ellos solo sirve para cerrar la caja no para abrirla). Esto asegura la confidencialidad de los datos sobre un medio público.

Una vez que se han intercambiado los certificados y con sus correspondientes llaves toda la información que sea transmitida entre las dos máquinas será transportada en esas cajitas cerradas, las cuales son a prueba de curiosos o intrusos. Entre los algoritmos de encriptación que pueden ser manejados con IPSec se destacan DES a 56 bits y 3DES que usa 3 llaves de 56 bits cada una.

1.1.6.3 IPSEC (Security Architecture for the Internet Protocol - RFC 1825)

IPsec es una extensión al protocolo IP que proporciona seguridad a IP y a los protocolos de capas superiores. Fue desarrollado para el nuevo estándar IPv6 y después fue portado a IPv4. La arquitectura IPsec se describe en el RFC2401.

IPsec emplea dos protocolos diferentes; ***AH*** (Cabecera de Autenticación) y ***ESP*** (Sobrecarga de Seguridad del Encapsulado) - para asegurarla autenticación, integridad y confidencialidad de la comunicación. Puede proteger el datagrama IP completo o solo los protocolos de capas superiores. Estos modos se denominan respectivamente, modo túnel y modo transporte. En modo túnel el datagrama IP se encapsula completamente dentro de un nuevo datagrama IP que emplea el protocolo IPsec. En modo transporte IPsec solo maneja la carga del datagrama IP, insertándose la cabecera IPsec entre la cabecera IP y la cabecera del protocolo de capas superiores.

IPSec también utiliza otros estándares de cifrado existentes, para formar una suite de protocolos, de los cuales algunos ya han sido nombrados, en el literal de 1.1.5 de Criptografía, y estos son:

- Protocolos de seguridad IP.
  -- ***AH*** *(Cabecera de Autenticación)*, Proporciona autenticación e integridad a los datagramas pasados entre dos sistemas.
  -- ***ESP*** *(Sobrecarga de Seguridad del Encapsulado)*, Proporciona confidencialidad realizando un cifrado en la capa del paquete IP
- ***DES*** *(Estándar de Cifrado de Datos)*, Algoritmo de clave pública que utiliza una clave de 56 bits.
- ***3DES*** *(Triple DES)*. Similar a DES, sino que procesa cada tres veces cada bloque.
- ***D-H*** *(Diffie Hellman)*, Protocolo de cifrado de clave pública, usa 768 bits y 1024 bits.
- ***MD5*** *(Boletín de Mensajes 5)*, Algoritmo hash utilizado para autenticar los datos de un paquete.

- ***SHA-1*** (*Algoritmo Hash Seguro – 1)*, Algoritmo hash utilizado para autenticar los datos de un paquete, es similar al MD5
- ***RSA*** *(Firmas Rivest, Shamir y Alderman)*, Algoritmo criptográfico de clave pública, usado para la autenticación.
- ***IKE*** *(Intercambio de Clave de Internet)*, Protocolo híbrido que proporciona servicios de utilidad para IPSec.
- ***CA*** *(Autoridades de Certificados)*, Autoridad certificadora que permite acreditar certificados digitales.

1.2 ARQUITECTURAS DE LA VPN

Las formas en que pueden implementar las VPNs pueden ser basadas en HARDWARE o a través de SOFTWARE, pero lo más importante es el protocolo que se utilice para la implementación, los cuales fueron ya descritos en los apartados anteriores. La forma de implementación de una VPN por SW y HW es la siguiente:

VPN por software (SW) requiere:

- Servidor (Ordenador con altos requisitos de hardware).
- Sistema operativo servidor que permita configurar VPN (Ejemplo : Windows 2000 Server o Windows 2003 Server)
- Pago de licencias.
- Es vulnerable ante : cuelgues, virus, bugs, etc.
- Pago extra por la integración aparte de un firewall.

VPN por hardware (HW) requiere:

- Todas las funcionalidades integradas en el dispositivo.
- Independiente del sistema operativo instalado en los servidores y clientes (Windows 9.X/ME, NT, 2000, XP, Linux, etc.)

- No es vulnerable ante, cuelgues, virus, bugs, etc.
- Integra firewall.

Las VPNs basadas en HARDWARE utilizan básicamente equipos dedicados como por ejemplo los switches, routers, firewalls, entre los más importantes, estos equipos, son seguros y fáciles de usar, ofreciendo gran rendimiento ya que todos los procesos están dedicados al funcionamiento de la red a diferencia de un sistema operativo, el cual utiliza muchos recursos del procesador para brindar otros servicios, en síntesis, los equipos dedicados son de fácil implementación y buen rendimiento, solo que las desventajas que tienen son su alto costo y que poseen sistemas operativos propios y a veces también protocolos que son *propietarios.*

Actualmente hay una línea de productos en crecimiento relacionada con el protocolo SSL/TLS, que intenta hacer más amigable la configuración y operación de estas soluciones.

Las soluciones de hardware casi siempre ofrecen mayor rendimiento y facilidad de configuración, aunque no tienen la flexibilidad de las versiones por software. Dentro de esta familia tenemos a los productos de Cisco, Linksys, Netscreen, Symantec, Nokia, US Robotics, etc.

En el caso basado en firewalls, se obtiene un nivel de seguridad alto por la protección que brinda el firewall, pero se pierde en rendimiento. Muchas veces se ofrece hardware adicional para procesar la carga VPN. Ejemplo Checkpoint NG, Cisco Pix.

1.2.1 ARQUITECTURA VPN BASADA EN CORTAFUEGOS (FIREWALLS)

Consiste en un dispositivo formado por uno o varios equipos que se sitúan entre la red de la empresa y la red exterior (*normalmente la Internet*), que analiza todos

los paquetes que transitan entre ambas redes y filtra los que no deben ser reenviados, de acuerdo con un *criterio establecido de antemano*, de forma simple.

Para que no se convierta en *cuello de botella* en la red, deben procesar los paquetes a una ***velocidad*** igual o superior al router. Crea un ***perímetro*** de seguridad y defensa de la organización que protege. Su diseño debe ser acorde con los *servicios que se necesitan tanto privados como públicos* (*WWW, FTP, Telnet)* así como conexiones por remotas.
Al definir un perímetro, el cortafuego opera también como **NAT**[4] (*Network Address Traslation*) y **Proxy** (*servidor multipasarela*).

Tipo de filtrado:

- *A nivel de red*, con direcciones IP y la interfaz por la que llega el paquete, generalmente a través de ***listas de acceso*** (en los *routers*).

- A nivel de **transporte**, con los puertos y tipo de conexión, a través de ***listas de acceso*** (en los *routers*).

- A nivel de *aplicación*, con los datos, a través de *pasarelas* para las aplicaciones permitidas analizando el contenido de los paquetes y los protocolos de aplicación (ejemplo: *servidor proxy o pasarela multiaplicación).*

- ***Un router separando la red Intranet de Internet***, también conocido como *Screened Host Firewall*, que puede enviar el tráfico de entrada sólo al *host bastión.*

[4] **NAT** (*Network Address Traslation*): Traducción de la dirección de red, es una aplicación no técnica y sencilla que determinado dispositivo o aplicación software es capaz de cambiar la dirección IP de origen o destino por otra dirección definida previamente.

- ***Un host bastión o pasarela para las aplicaciones permitidas separando la red Intranet de Internet****,* también conocido como *Dual Homed Gateway.* Permite filtrado hasta la capa de aplicación

- ***Con dos routers separando la red Intranet e Internet y con el host bastión dentro de la red formada por ambos routers****,* también conocida como *Screened Subnet*, esta red interna es conocida como zona neutra de seguridad o zona desmilitarizada (*DMZ*[5] *Demilitarized Zone).*

1.2.2 ARQUITECTURA VPN BASADA EN CAJA NEGRA

Muchas empresas no disponen entre su personal de expertos informáticos. Entonces las cajas negras son una buena opción para implementar VPN's.

Estas cajas negras son sistemas cerrados, con necesidad de mantenimiento cero, actualizables en remoto, totalmente seguros y con software de encriptación y autenticación propios.

Este tipo de arquitectura, simplifica la implementación y gestión de las VPNs, aprovecha las ventajas de los estándares y las aplicaciones Web emergentes y maximiza el rendimiento de la seguridad en Internet, incluye una amplia variedad de tecnologías articuladas en torno a los conceptos de conectar, proteger y gestionar. De esta forma, quienes adopten este tipo de arquitectura podrán gozar de inmediato de todas las ventajas que aportan los últimos avances tecnológicos y de seguridad en redes. Y todo esto, encapsulado en módulos cuyo funcionamiento es transparente para el usuario.

Esta arquitectura es modular, solución de la industria que permite a las empresas escalar, implementar y gestionar fácilmente redes VPN seguras con más de un millar de emplazamientos remotos. Utiliza un enfoque de perfil unificado para

[5] **DMZ**: Zona desmilitarizada donde se encuentran los servidores que dan la cara al Internet, como son los Servidores WEB.

definir una política de seguridad central y asociarla a miles de VPNs. Esta es una solución que simplifica y escala la gestión de redes distribuidas ampliamente y reduce drásticamente el costo total de propiedad gracias a: "perfiles" rápidos y sencillos basados en plantillas, el aprovechamiento de la infraestructura de esta arquitectura que proporciona políticas automatizadas.

1.2.3 ARQUITECTURA VPN BASADA EN ENRUTADORES (ROUTERS)

Aplicaciones del Router: El Router es un equipo que combina su funcionalidad de enrutamiento con la flexibilidad de establecer un túnel de comunicación punto a punto en dos extremos distantes, se puede establecer una Red Virtual Privada (VPN), solo con dos routers configurados para este fin. En combinación con el firewall, protección antivirus para correo electrónico y filtración de contenido. Es una solución económica, fácil de manejar, que es ideal para negocios pequeños y medianos que busquen agregar una o todas las diversas aplicaciones a la red.

1.2.4 ARQUITECTURA VPN BASADA EN ACCESO REMOTO

VPN para Usuarios Remotos: La aplicación cliente-a-LAN VPN reemplaza el tradicional acceso remoto permitiendo a un usuario remoto conectarse a la LAN corporativa mediante un túnel de seguridad sobre la Internet. La ventaja es que el usuario remoto puede hacer una llamada local a un Proveedor de Servicio Internet, sin sacrificar la seguridad de la compañía, contrariamente a lo que haría si realiza una llamada de larga distancia para conectarse al servidor de acceso remoto de la empresa.

Puede configurar un servidor que permita a los usuarios remotos tener acceso a los recursos de una red privada mediante conexiones de acceso telefónico o de red privada virtual (VPN). Este tipo de servidor se denomina servidor VPN de acceso remoto. Los servidores VPN de acceso remoto también pueden

proporcionar traducción de direcciones de red (NAT). Con NAT, los equipos de la red privada pueden compartir una única conexión a Internet. Con VPN y NAT, los clientes VPN pueden determinar las direcciones IP de los equipos de la red privada, mientras que los demás equipos en Internet no tendrán acceso a esta información.

1.2.5 ARQUITECTURA VPN BASADA EN SOFTWARE

Todas las distintas opciones disponibles en la actualidad caen en tres categorías básicas: soluciones de hardware, soluciones basadas en firewall y aplicaciones VPN por software.
Cada tipo de implementación utiliza diversas combinaciones de protocolos para garantizar las tres características fundamentales como son: Autenticación, Integridad y Confidencialidad.

El protocolo estándar para la implementación de una VPN basada en software, de hecho es el IPSEC, pero también tenemos PPTP, L2TP, SSL/TLS, SSH, etc. Cada uno con sus ventajas y desventajas en cuanto a seguridad, facilidad, mantenimiento y tipos de clientes soportados.

***Las aplicaciones VPN por software*:** son las más configurables y son ideales cuando surgen problemas de interoperatividad en los modelos anteriores. Obviamente el rendimiento es menor y la configuración más delicada, porque se suma el sistema operativo y la seguridad del equipo en general. Aquí tenemos por ejemplo a las soluciones nativas de Windows, Linux y los Unix en general. Por ejemplo productos de código abierto (Open Source) como OpenSSH, OpenVPN y FreeS/Wan.

Estos sistemas son ideales para las situaciones donde los dos puntos de conexión de la VPN no están controlados en la misma organización, o cuando los diferentes cortafuegos o routers no son implementados por la misma

organización. Este tipo de VPN's ofrecen el método mas flexible en cuanto a el manejo de tráfico. Con este tipo, el tráfico puede ser enviado a través de un túnel, en función de las direcciones o protocolos, en cambio en los VPN por hardware, todo el tráfico será enrutado por el túnel. Podemos hacer un enrutamiento inteligente de una manera mucho más fácil.

1.3 BENEFICIOS DE UNA VPN DESDE UN PUNTO DE VISTA TECNICO

Los innegables beneficios en infraestructura y costos que ofrece la implantación de Redes Privadas Virtuales (VPNs), como soporte de las comunicaciones corporativas necesitan de una fuerte garantía de seguridad que haga factible su empleo máximo, cuando el medio sobre el que se montan es totalmente abierto y, para determinados propósitos incluso hostil. El factor crítico en la operación de las VPN no está en el túnel de conexión, sino en los mecanismos de seguridad que preservan la confidencialidad e integridad de la comunicación. Dentro de los principales beneficios de las VPNs se tienen:

- *Seguridad*: provee encriptación y encapsulación de datos de manera que hace que estos viajen codificados y a través de un túnel.

- *Costos*: ahorran grandes sumas de dinero en líneas dedicadas o enlaces físicos.

- *Mejor administración*: cada usuario que se conecta puede tener un número de IP fijo asignado por el administrador, lo que facilita algunas tareas como por ejemplo mandar impresiones remotamente, aunque también es posible asignar las direcciones IP dinámicamente si así se requiere.

- ***Facilidad*:** para los usuarios con poca experiencia para conectarse a grandes redes corporativas transfiriendo sus datos.

1.3.1 AHORRO EN COSTOS

Una forma de reducir costo con las VPNs, es eliminando la necesidad del uso de enlaces dedicados, que tiene valores elevados. Con las VPNs, una organización sólo necesita una conexión a Internet, la cual puede ser suministrada por un Proveedor de Servicio de Internet local (ISP).

Otra forma de reducir costos es disminuir la carga de teléfono para accesos remotos. Los ahorros de costos suelen ser cuantitativos y cualitativos, para las redes internas punto a punto, y mucho mayores cuando se trata de redes internacionales para el acceso de teleoperadores y trabajadores móviles.

Además de ahorrar costos en la conexión telefónica, usando otras alternativas de conexión, como por ejemplo; aprovechar la infraestructura existente de TV Cable, banda ancha inalámbrica, conexiones de alta velocidad de tipo ADSL o ISDN, lo que implica un alto grado de flexibilidad y reducción de costos al momento de configurar la red. Incluso, es posible compatibilizar aplicaciones de telefonía sobre IP usando la misma VPN, con un significativo ahorro de costos en telefonía de larga distancia.

La implantación de VPNs, permite unificar redes empresariales con las de sus proveedores y clientes para hacer más eficientes procesos como pedidos, seguimientos de entrega, información sobre productos, etc. Esto involucra una reducción de costos al eliminar procesos tardados y poco eficientes como el fax y teléfono. La eficiencia en procesos de pagos, cobros y facturación también pueden verse beneficiados con ésta integración.

1.3.2 FLEXIBILIDAD

La flexibilidad ha ganado posiciones en el orden de prioridades, gracias al aumento de las reubicaciones de usuarios y al desarrollo de nuevas aplicaciones.

La flexibilidad también es esencial para lograr los objetivos del entorno e-business: conectar los sistemas internos con los clientes, socios y proveedores de una empresa pequeña o una corporativa.

Las redes corporativas tradicionales basadas en circuitos fijos, ya sean líneas alquiladas o PVC (Circuitos Virtuales Permanentes) dentro de una red Frame Relay o ATM (Modo de Transferencia Asíncrona), no son las más adecuadas para este nuevo entorno e-business. Se requiere una red que soporte todo tipo de conexiones y se pueda reconfigurar con facilidad para introducir nuevos usuarios o añadir servicios adicionales (*Como son las VPNs*). Esta red también debe permitir la variación de las calidades de servicio para poder hacer frente, tanto a sencillas transferencias de archivos sin limitación de tiempo, como a aplicaciones multimedia en tiempo real, y el flujo de vídeo y voz.

Regularmente son los proveedores de servicios de telefonía o de Internet los que de manera más rápida las adoptan. En el último año se ha observado un movimiento interesante, debido a que diversos sectores han adoptado ya este tipo de tecnología.

1.3.3 FACILIDAD DE INSTALACION

Con las VPNs, las redes son de conectividad más sencilla porque todos los servicios los obtienen de estas, esto ayuda a las empresas a que tengan menos complejidad en sus instalaciones y el mismo servicio con tecnología de punta, a la que además, es mucho más fácil de agregarles aplicaciones. Esto se lo consigue con el mejoramiento de equipos que cada vez vienen integrados con funcionalidades más sofisticadas y de fácil instalación. Los cuales brindan características tales como:

- Encriptación de los datos
- Detección de intrusos (incorporación de *firewalls*)

- Incrementación de la seguridad del cliente VPN (bloqueo seguro anti-hacker)
- Creación de túneles VPN
- Administración remota de múltiples unidades
- Extrema flexibilidad de instalación: IPSec a través de NAT.

Todas estas funcionalidades y características, se manejan de manera transparente para el usuario y son de fácil instalación para el proveedor del servicio de la VPN (ISP).

La instalación de circuitos VPN es mucho más fácil y económica que el coste de instalación de varios circuitos dedicados privados. Así, cada sede (lugar remoto) tan sólo necesita conectarse al nodo de interconexión (Servidor), y establecer la conexión segura de la VPN a través del Internet.

1.3.4 TRANSPARENCIA

El uso de la VPN permite a los usuarios de una red empresarial, sin importar en qué sucursal se encuentren, acceder a los mismos archivos como si estuvieran en el mismo lugar físico. Estos accesos y transmisión de información son transparentes para el usuario, teniendo como factor principal para estas conexiones, el ancho de banda del Proveedor del Servicio de Internet (ISP).

La Red Privada Virtual (VPN) se puede implantar utilizando tanto accesos analógicos, RDSI *(*Integrated Services Digital Network*)*, ADSL (Asymmetric Digital Subscriber Line), LMDS[6] (Conexiones vía radio), como a través de cualquier otro tipo de conexión a Internet no filtrado. La

[6] **LMDS**: Son conexiones vía radio enlaces, esta tecnología aprovecha los despliegues las nuevas operadoras telefónicas (celulares) en sus redes fijas de voz para que llegue Internet a los hogares y oficinas de forma permanente y rápida

diferencia entre una y otra es la velocidad de transmisión (transferencia) de acuerdo al ancho de banda utilizado y al número de clientes conectados (Tráfico de la Red). La velocidad de transferencia puede considerarse óptima cuando esta por encima del 75% de la velocidad máxima teórica.

Ancho de Banda Teórico Kbits / seg	Tasa de Velocidad Óptima Kbits / seg	Tasa de Velocidad Óptima KBytes / seg
56	> 42	> 5,25
128	> 96	> 12
256	> 192	> 24
512	> 384	> 48
1.024	> 768	> 96
2.048	> 1.500	

Tabla 1.1 Tasas de velocidad de transferencia de datos.

El ***ancho de banda***, parece el tema crítico, especialmente a la hora de seleccionar un buen proveedor de acceso a Internet. Se supone que cuanto más ancho de banda, es mayor la rapidez de acceso.

El ***ancho de banda*** se suele asimilar al diámetro de una tubería que sirviese para canalizar el flujo de datos. Pero esa simplificación es excesiva.

De entrada, el ***ancho de banda*** es la capacidad de una línea para transmitir información. Pero hay que tener en cuenta que la línea está compartida frecuentemente por muchos usuarios. Por tanto nos sirve de muy poco saber el ancho de banda que tiene un proveedor, si no sabemos cuantos usuarios comparten esa línea en un momento determinado. Hay pequeños proveedores con pocos clientes que utilizan una línea "estrecha"; sin embargo pueden ofrecer mejores tiempos de acceso que otros proveedores con canales más potentes, porque éstos tienen demasiados usuarios compartiendo la línea. La proporción es lo que cuenta, no el ancho en sí mismo a al hora de escoger un ISP.

CAPITULO 2

2. ANALISIS TECNOLÓGICO DE LA SITUACIÓN ACTUAL DE LA EMPRESA.

2.1 SERVICIOS DISPONIBLES EN LA RED

En este capítulo se analizarán los servicios de red que la empresa tiene, como también los que la empresa florícola vaya a requerir y la problemática de la empresa en el área de las comunicaciones. Buscando alternativas que conlleven a la solución de los problemas de comunicación entre los diferentes sitios que la empresa posee.

2.1.1 DESCRIPCIÓN GENERAL DE LA EMPRESA

La empresa a la que se va hacer referencia en el desarrollo del presente proyecto, se dedica a la producción, comercialización y exportación de flores.

La experiencia en la producción, exportación de rosas frescas inicia en 1990. Desde entonces, la marca se ha convertido en pionera en cuanto a la calidad y al liderazgo en el mercado de las rosas ecuatorianas y a nivel internacional.

El clima y ubicación geográfica del Ecuador, proporcionan las condiciones adecuadas para cultivar las mejores rosas del mundo. Estas condiciones ideales combinadas con el conocimiento, investigación constante y personal calificado, permite ofrecer un producto que sobrepasa las expectativas de los mercados más exigentes.

Para satisfacer las demandas de los mercados de América del Norte, parte de Europa y Asia, se busca mantener un alto nivel de calidad y ser los primeros en introducir cada vez nuevas variedades con gran potencial de comercialización.
Todo el trabajo que a diario se realiza, permite garantizar un producto exclusivo, que acompañado con la imagen y la experiencia adquirida en todos estos años, les permiten seguir introduciendo los productos a más mercados, ampliando así, su comercialización.

La ***Misión*** de la empresa es velar por el mejoramiento de cada uno de sus procesos, con los cuales se logra obtener día a día una mejor aceptación de los productos, que se generan con mano de obra calificada y tecnología florícola de punta.

La empresa tiene como ***Visión*** lograr introducir en forma masiva sus productos en nuevos mercados, en donde la alta competitividad de productos similares, hacen que no se descuiden los mínimos detalles de calidad en los procesos de producción.

Actualmente la empresa esta formada por dos fincas; la primera ubicada en la ciudad de Tabacundo (Al norte de la provincia de Pichincha) y la segunda en Mulaló (Al norte de la provincia de Cotopaxi), además consta de una Oficina Matriz, ubicada en la parte norte de la ciudad de Quito, que es el centro de operaciones y control de toda la empresa.

Para una mejor comprensión, a lo largo de este trabajo, se identificará a la finca ubicada en Tabacundo como “FINCA1”, y a la finca ubicada en la parte sur, Mulaló (Cotopaxi) como “FINCA2” y a las oficinas ubicadas en Quito como “CENTRALUIO”. La red general de la Empresa, se ilustra mediante el siguiente esquema:

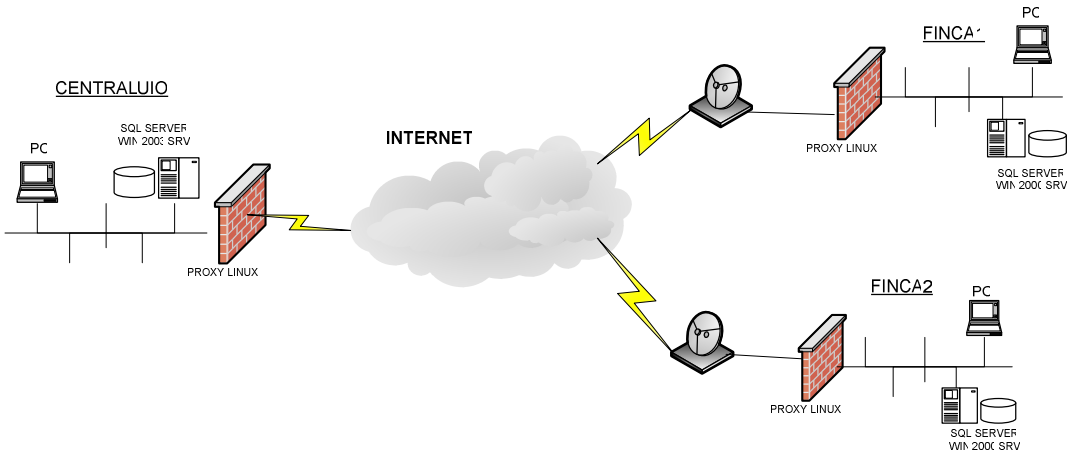

Figura 2.1: Diagrama general de la red empresarial

2.1.2 PROBLEMÁTICA ACTUAL DE LA EMPRESA.

Durante los últimos años las empresas agro-exportadoras han descubierto las ventajas de un adecuado sistema de comunicaciones nacional e internacional.

Estas ventajas comprenden mayor eficiencia, reducción de costos, ahorro de tiempo y esfuerzo, pero quizá una de las mayores ventajas es el mejoramiento de la imagen frente al cliente al momento de ofrecer sus productos.

Se debe tener muy en cuenta, que el aumento de la demanda de servicios de telecomunicaciones en el área empresarial va en aumento. Pero la limitante de algunas empresas, es no tener cobertura suficiente de última milla en las áreas rurales.

Por ejemplo, para una finca agro-exportadora que está ubicada fuera del perímetro urbano, la obtención de una línea telefónica es muy difícil, no se diga si se desea que además tenga una buena calidad de comunicación. La situación es peor aún cuando se requiere opciones para acceso a Internet o comunicación de datos para los programas de administración, cada vez más frecuentes en estas empresas.

Por otro lado las alternativas satelitales existentes y nuevas tecnologías de intercomunicación, tienen el inconveniente de un alto costo mensual, haciéndolas accesibles solamente a empresas de gran volumen de facturación y ventas. Pero surge un problema con aquellas empresas medianas y pequeñas, cuyas

necesidades son igualmente urgentes, pero que no pueden costear un servicio tan caro. Es por eso que la interconexión entre las Fincas y la Matriz para este proyecto, es la parte más crítica a ser analizada.
Otro de los problemas que la empresa tiene, es el control y manejo de información de todas las actividades que se realizan en cada una de las fincas en el área de producción, éstas son almacenadas en bases de datos locales; razón por la cual, se lleva dicha información en medios magnéticos cada fin de semana (sábados por la tarde), a la Oficina Matriz para realizar la actualización de la base de datos general, con los cuales se realizan los diferentes informes, análisis de costos y proyecciones de la producción semanal.

Las actualizaciones semanales de la información, generan molestias y retrasos para la toma de decisiones, planificación diaria y exportación de las flores. A más de que se debe tener en cuenta que los medios magnéticos están sujetos a daños y extravíos, retrasando aún más la actualización de la base de datos general.

Al momento la comunicación entra las fincas y la oficina central, se realiza por correo, el cual sale por el Internet a través del enlace satelital que le provee el ISP. Esta transferencia de información se la realiza sin ningún tipo de nivel de seguridad, es decir, puede ser presa fácil de piratas informáticos.

2.1.3 SERVICIOS DISPONIBLES EN LA EMPRESA

La disponibilidad de la Información, provee a las Empresas acceso sin interrupciones a sus recursos y a toda su información crítica del negocio, utilizando tecnología, infraestructura y la experiencia técnica. Es por esto que en este capítulo se va a realizar un análisis detallado de todos los servicios disponibles en la red, que la empresa posee en la actualidad, y con estos datos poder enfrentar de mejor manera la problemática actual de la misma.

A continuación se describen detalladamente los servicios de red disponibles en cada finca y la central de Quito. En vista que los servicios de red disponibles en las dos fincas son parecidos, estos se agrupan en una sola la descripción.

2.1.3.1 Servidor Controlador de Dominio (Windows 2000 Server SP4 y Windows 2003 small Bussines Server)

***Windows 2000 Server* y Windows 2003 small Bussines Server:** Son sistemas operativos de la familia Windows Server de Microsoft, orientados a ser, principalmente, servidores de archivos, impresión y aplicaciones. También ofrecen la posibilidad de servidores de servicios Web.

Principales Características:

1- Disminución de costos respecto a sistemas anteriores: Esto se debe a que la organización y administración de la red es mucho más sencilla y rápida porque permite la instalación y actualización de aplicaciones en los clientes de manera automática.

2- Seguridad: Identifican a cada usuario que quiere acceder a datos o aplicaciones para verificar que tiene permiso para realizar dicha acción. Proporcionan seguridad local y a nivel de red, revisando archivos y carpetas. Soportan el protocolo de seguridad Kerberos.

3- Servicios de directorio: Esta es una de las características más útiles de Windows Server. Mediante el Active Directory (directorio activo) se puede agrupar usuarios según los criterios que más útiles sean, aunque estén a miles de kilómetros de distancia unos de otros. Así, los administradores pueden gestionar recursos y cuentas de usuario para que estos últimos accedan a cualquier recurso de la red empresarial que necesiten en cada momento, siempre y cuando tengan permiso previo para ello.

4- Rendimiento: Soportan multitarea para procesos de programas y sistemas. Soportan hasta cuatro microprocesadores.

5- Servicios de red y comunicación: Incorporan soporte para los protocolos de red más utilizados, como TCP/IP e IPX/SPX. Ofrecen conectividad con Novell Netware, UNIX y Apple Talk. Proporcionan acceso telefónico a redes, así un usuario móvil puede acceder a la red desde cualquier lugar.

6- Internet: Incluye una plataforma segura de servidor Web: el IIS (Internet Information Server). Los escritorios de los usuarios están integrados con Internet para que éstos, puedan explorar de manera segura los recursos de la red (tanto Intranet como Internet).

7- Herramientas de administración integradas: Ofrecen la posibilidad de crear herramientas personalizadas para gestionar CPUs mediante una única interfaz estándar.

8- Soporte de hardware: Soportan plug and play (no es necesario reiniciar tras instalar un nuevo componente de hardware). Soporta USB

Los sistemas operativos que usan cada una de las FINCAS y Oficina CENTRALUIO, para el Controlador de Dominio son:

FINCA 1 y FINCA 2

Controlador de Dominio: Para este servicio, en las fincas se trabaja con Windows 2000 Server SP4, el nombre asignado a cada dominio en cada una de las fincas será: *“domfinca1.local”* y *“domfinca2.local”* respectivamente. En este mismo servidor corren los servicios de DNS y Active Directory.

OFICINA CENTRALUIO

Controlador del Dominio: En la CentralUIO, se trabaja con Windows 2003 small Bussines Server. A este dominio se le identifica como *"domcentraluio.local".*

Al momento se trabaja con 36 usuarios, los que se rigen a políticas de seguridad configurados en este servidor. En este mismo servidor corren los servicios de DNS y Active Directory.

2.1.3.2 Servidores de Archivos

El servicio de información centralizada, básicamente es un servidor de archivos en una red de computadores cuya función es permitir el acceso remoto a archivos almacenados en él o directamente accesibles por este. En principio, cualquier computador conectado a una red con un software apropiado, puede funcionar como servidor de archivos. Desde el punto de vista del cliente de un servidor de archivos, la localización de los archivos compartidos es transparente. Normalmente no hay diferencias perceptibles si un archivo está almacenado en un servidor remoto o en el disco de la propia máquina.

El manejo de la información en las FINCAS Y la Oficina CENTRALUIO es:

FINCA 1 y FINCA 2

Información Centralizada.- Esta Información es conocida por todos los usuarios a través de un directorio compartido, ubicado en el servidor principal, el mismo que es mapeado por los clientes a través de una unidad virtual. Los permisos de acceso a este directorio son administrados de acuerdo a la necesidad que tenga cada cliente (lectura, escritura, ejecución).

OFICINA CENTRALUIO

Información Centralizada: Al igual que en las fincas, la información se maneja con carpetas compartidas y mapeadas como unidades virtuales en los clientes.

2.1.3.3 Servidor de Correo (Send Mail / M. Exchange Server 5.0)

Un servidor de correo es una aplicación que permite enviar mensajes (correos) de unos usuarios a otros, con independencia de la red que éstos estén utilizando. Para lograrlo se definen una serie de protocolos, cada uno con una finalidad concreta:

SMTP *(Simple Mail Transport Protocol)*: Es el protocolo que se utiliza para que dos servidores de correo intercambien mensajes.

POP *(Post Office Protocol)*: Se utiliza para obtener los mensajes guardados en el servidor y pasárselos al usuario.

IMAP *(Internet Message Access Protocol)*: Su finalidad es la misma que la de POP, pero el funcionamiento es diferente. Así pues, un servidor de correo consta en realidad de dos servidores: un servidor SMTP que será el encargado de enviar y recibir mensajes, y un servidor POP/IMAP que será el que permita a los usuarios obtener sus mensajes.

Sendmail: Este servidor es un popular *agente de transporte de correo* (MTA - Mail Transport Agent) en Internet, cuya tarea consiste en encaminar los mensajes de correos de forma que estos lleguen a su destino. Este servidor es el más popular MTA, corriendo sobre sistemas Unix, aunque se le critica su alto número de alertas de seguridad (la mayoría de ellas parchadas a las pocas horas), además de no ser sencillo de configurar.

Microsoft Exchange Server 5.0: Las principales características del cliente de Exchange es que combina una interfaz única de usuario para correo electrónico, compartición de información, acceso a Internet, proceso de textos, fax, etc. y éste se lo realiza de forma personalizada y extensible.

Exchange define dos tipos de carpetas de información: Personal Folders y Public Folders.

***Personal Folders o carpetas personales*:** se usan para almacenar mensajes y documentos que el usuario no desea compartir con los demás miembros de la organización. Las carpetas personales pueden residir tanto en el servidor de Exchange como en el disco duro local de la máquina del usuario o en cualquier otro servidor de ficheros de la red.

***Public Folders o carpetas públicas*:** son almacenados en el servidor de Exchange y proporcionan la capacidad de que todos o determinados miembros de la organización puedan compartir todo tipo de información: mensajes, documentos o aplicaciones. Una carpeta pública es una aplicación del tipo de una BBS (Bulletin Board Service) a la cual, varios usuarios pueden acceder e interactuar con la información.

Cuando instala Microsoft Exchange Server 5.0, el soporte de POP3 (Post Office Protocol 3) esta activado de forma predeterminada, permitiendo a los clientes POP3 recuperar su correo electrónico tan pronto como se configura el servidor.

FINCA 1 y FINCA 2

Servicio de Correo (Clientes): En las fincas solo se trabaja con los clientes, que acceden a un servidor remoto SMTP y POP3 (SENDMAIL-LINUX) ubicado en oficina CENTRALUIO. En cada estación de trabajo los usuarios tienen cuentas creadas en Microsoft Outlook u Outlook Express. Este servicio corre sobre Internet, sin ningún nivel de seguridad.

OFICINA CENTRALUIO

Servidor de correo: Aquí se tiene el servidor principal, este servicio está integrado con el Controlador del Dominio y Active Directory con lo que es más versátil el manejo de cuentas de usuario, como los de correo. Se utiliza Microsoft Exchange, y también corre sobre Internet sin seguridades.

2.1.3.4 Servidor de Antivirus (Trend Microsystem)

Trend Microsystem: proporciona detección antivirus integral a lo largo y ancho de la red para los servidores de archivos con los sistemas operativos: Microsoft Windows 2000, Microsoft WindowsNT y Novell NetWare. Administrados a través de una consola portátil.

Server Protect, administra la protección contra las epidemias de virus (virus outbreak), mediante la detección centralizada de códigos maliciosos, actualizaciones de patrones de virus, reportes de eventos y configuración antivirus. Protege al servidor en tiempo real contra virus, gusanos y ataques de caballos de Troya. Ayuda a la confiabilidad y estabilidad del servidor mediante la certificación Windows 2000 Server.

FINCA 1 y FINCA 2

Servidor de Antivirus: Se trabaja con Trend Microsystem. Corre sobre un sistema operativo Windows XP Profesional SP2. En cada estación se instala el cliente apuntando al servidor antes mencionado. La actualización del servidor lo realiza en forma automática y la administración y visor de logs se realiza vía Web.

OFICINA CENTRALUIO

Servidor de Antivirus: Al igual que en las fincas, se trabaja con Trend Microsystem instalado en una máquina con Windows XP Professional SP2. Los clientes acceden a este servidor para obtener actualizaciones y últimas definiciones de virus.

2.1.3.5 Servidor de Respaldos (Veritas Backup).

VERITAS Backup Exec. Es una solución que permite realizar backups y recuperación de datos, a través del soporte y las ayudas que este sistema tiene. Se pueden realizar los backup´s de bases de datos que se encuentran trabajando en la red. El agente remoto de VERITAS Backup Exec está instalado en los sistemas que deben ser respaldados. Esta aplicación utiliza el puerto 10000 del TCP.

El manejo del servicio de respaldos (backups) en cada una de las FINCAS y Oficina CENTRALUIO esta dado por:

FINCA 1 y FINCA 2

Servidor de Respaldos: Este servicio se tiene instalado en el controlador del dominio, se trabaja con Veritas backup Exec 8.0 en el que están configuradas varias tareas que se ejecutan en un horario específico, respaldando las bases del SQL Server. Estas son almacenadas en cintas magnéticas de 4 mm data, las que son enviadas cada fin de semana a la oficina central para restaurar y replicar la información en las bases de datos de la Oficina CENTRALUIO, cada sábado por la tarde.

OFICINA CENTRALUIO

Servidor de Respaldos: Al igual que en las fincas, este servicio se tiene instalado en el controlador del dominio. Se trabaja con Veritas backup Exec 8.0,

Adicionalmente se respaldan los archivos y carpetas compartidas del servidor principal.

2.1.3.6 Servidor de Base de Datos (SQL Server 6.5 SP6)

Dos características dominantes de una base de datos del servidor llegan a ser importantes debido al acceso del cliente a los datos. La primera característica proporciona un solo punto del acceso a los datos en la base. La segunda divide el proceso y la manipulación entre el cliente y los sistemas del servidor.

Aunque las organizaciones utilizan rutinariamente el servidor SQL para manipular millones de expedientes, el servidor SQL proporciona varias herramientas que ayudan a manejar el sistema y sus bases de datos y tablas.

Las herramientas de Windows y funciones que vienen con el servidor SQL permiten trabajar y ejecutar muchas de las funcionalidades que el Servidor SQL tiene. Entre las más importantes se mencionan las siguientes:

- Realiza la administración de las bases de datos.
- Controla el acceso a los datos en las bases.
- Controla la manipulación de datos en las bases.

Las bases de datos con las que se trabajan en las FINCAS y en la Oficina CENTRALUIO, se describen de la siguiente forma:

FINCA 1 y FINCA 2

Base de Datos: Se trabaja con SQL Server 6.5 SP6 que esta instalado en el mismo equipo que corre el controlador de dominio. La información generada diariamente en estas bases, son llevadas en cintas magnéticas a Oficina CENTRALUIO cada fin de semana.

OFICINA CENTRALUIO

Base de Datos: Al igual que en las Fincas se utiliza el SQL Server 6.5, el cual esta instalado sobre Windows NT Server.

2.1.3.7 Servidor Proxy / Firewall

El termino ***Proxy*** significa ***"hacer algo en nombre de otro"***. El *proxy* es un Programa de Software que se instala en un único PC de una red local, y que permite que varios computadores conectados a una misma red local puedan compartir un mismo acceso a Internet o conexión a Internet de manera simultánea.

En términos de redes, un servidor proxy aísla las computadoras de la red exterior, envía solicitudes en representación de ellas a otros servidores, es decir un proxy http, es una máquina que recibe peticiones de páginas Web de otra Máquina (Máquina A), el proxy obtiene la página solicitada y retorna el resultado a la Máquina A. El proxy puede tener un caché con las páginas solicitadas; así, si otra Máquina solicita la misma página le será enviada la copia que reside en el caché. Eso permite un uso eficiente del ancho de banda y un menor tiempo de respuesta. Como efecto colateral; las Máquinas cliente no están directamente conectadas al exterior, esta es una forma de incrementar la seguridad de la red interna. Un proxy bien configurado puede ser tan efectivo como un buen firewall.
El trabajo del servidor Proxy en las FINCAS y Oficina CENTRALUIO, se resume de la siguiente manera:

FINCA 1 y FINCA 2

Servidor Proxy: Este servicio corre sobre un sistema operativo Linux White Box Edition 4.0, dispone de dos tarjetas de red, una conectada a la red interna y la segunda al INTERNET. Se trabaja con Squid nativo del sistema Linux.

OFICINA CENTRALUIO

Firewall / Proxy: Este servicio corre sobre Linux White Box Edition 4.0, se utiliza Interscan Virus Wall SMB for Unix 5.0 de Trend Microsystem. Este servidor dispone de dos tarjetas de red, una da la cara al Internet y la otra está conectada a la red interna. Este servidor hace de Proxy, para los usuarios internos y enrutador SMTP para el servidor Exchange. Todo el tráfico pasa y se filtra por este servidor, aquí se restringe acceso a sitios prohibidos y se escanea las páginas visitadas. El correo entrante y saliente pasa por el filtro SMTP que dispone este producto.

2.2 INFRAESTRUCTURA DE COMUNICACIONES

Dentro de la infraestructura de comunicaciones, la empresa florícola dispone de los siguientes equipos, que serán detallados de forma separada para las FINCAS y la Oficina CENTRALUIO.

2.2.1 TOPOLOGÍA DE LA RED DE DATOS

La topología de la red de datos de las FINCAS y de la Oficina CENTRALUIO es la siguiente:

FINCA 1 Y FINCA 2

Red: El cableado está hecho con categoría 5. La topología de la red es estrella, para lo cual se utilizan Switches 3COM de 24 Puertos de 10/100/1GB de velocidad de acceso a la red, los cuales están acordes con la categoría del cableado.

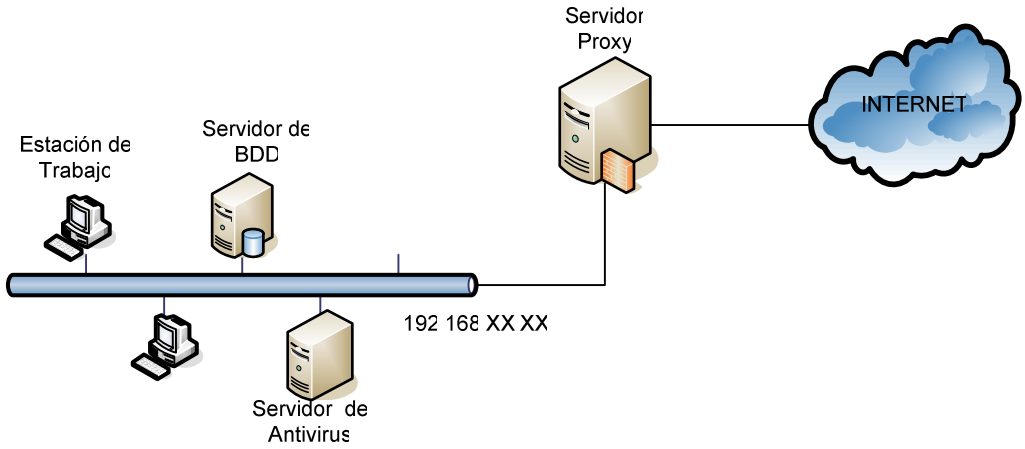

Figura 2.2: Diagrama de Red de las FINCAS.

OFICINA CENTRALUIO

Red: Semejante a las fincas se tiene un cableado con categoría 5, con topología de red tipo estrella, los Switches son 3COM de 24 Puertos de 10/100/1GB de velocidad.

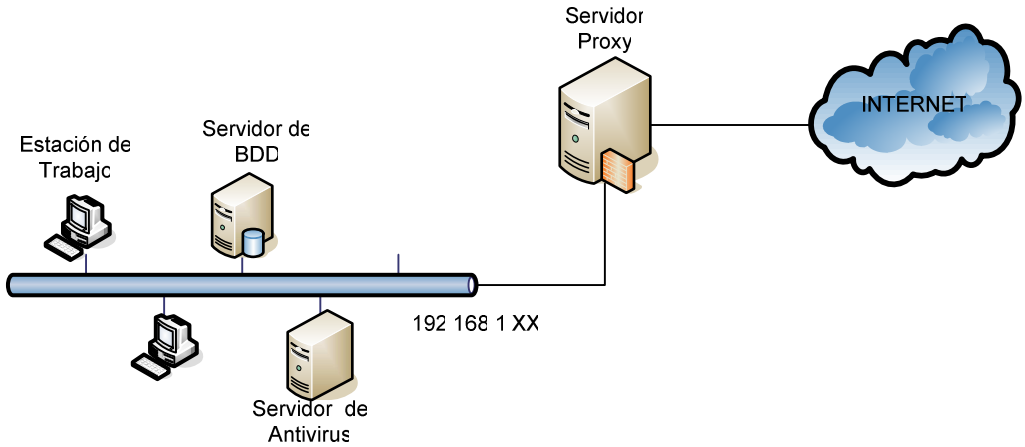

Figura 2.3: Diagrama de Red de la CENTRALUIO

2.2.2 SISTEMA TELEFÓNICO

El sistema telefónico de las FINCAS y de la Oficina CENTRALUIO, responde a las siguientes características:

FINCA 1 Y FINCA 2

Sistema telefónico: Cuenta con una central telefónica marca Nitsuko, con capacidad para 28 extensiones y 8 troncales. Para la comunicación entre FINCAS y oficina CENTRALUIO se lo realiza a través de la red de Andinatel.

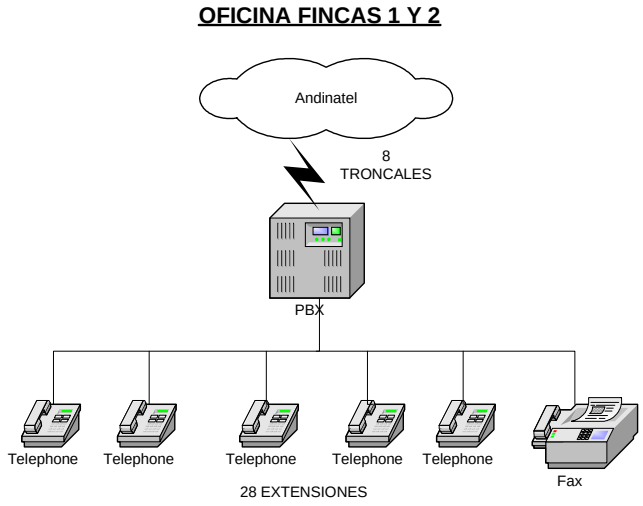

Figura 2.4: Diagrama del sistema telefónico de las FINCAS

OFICINA CENTRALUIO

Sistema Telefónico: Cuenta con una central telefónica marca Nitsuko de idénticas características que las usadas en las fincas, con la variante que ésta es de mayor capacidad en cuanto a sus extensiones (32), utilizando el mismo número de troncales (8).

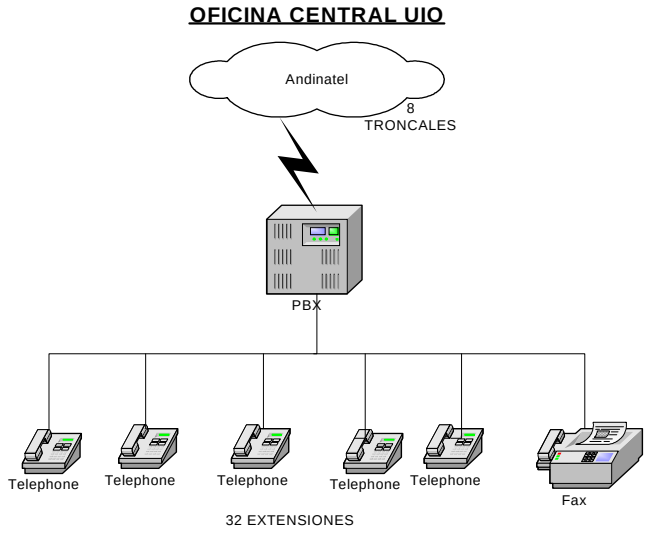

Figura 2.5: Diagrama del sistema telefónico de la CENTRALUIO

2.2.3 ENLACES DE COMUNICACIONES

Los enlaces de comunicaciones que se tienen actualmente el las FINCAS y en la Oficina CENTRALUIO son:

FINCA 1 Y FINCA 2

Los fincas tienen enlaces satelitales, los cuales constan en su infraestructura física de una antena parabólica de 1.2 m de diámetro, la misma que está apuntada al este, hacia un satélite Geoestacionario ubicado a 30 000 Km. de altura (INTELSAT 805) en la banda C (3625-6425 MHz) con polaridad vertical paralela, tiene un LNB (Low Noise Block), Feed (pantalla) y una Unidad de Radio Frecuencia (RF). En la parte interna consta de un MODEM Satelital, en la que está integrada la parte de Frecuencia Intermedia (IF) y la tarjeta de red.

El cable de interconexión que une el LNB, la Unidad de RF con el MODEM satelital es el RG6 y conectores tipo F. A continuación se ilustra un gráfico que muestra estos componentes.

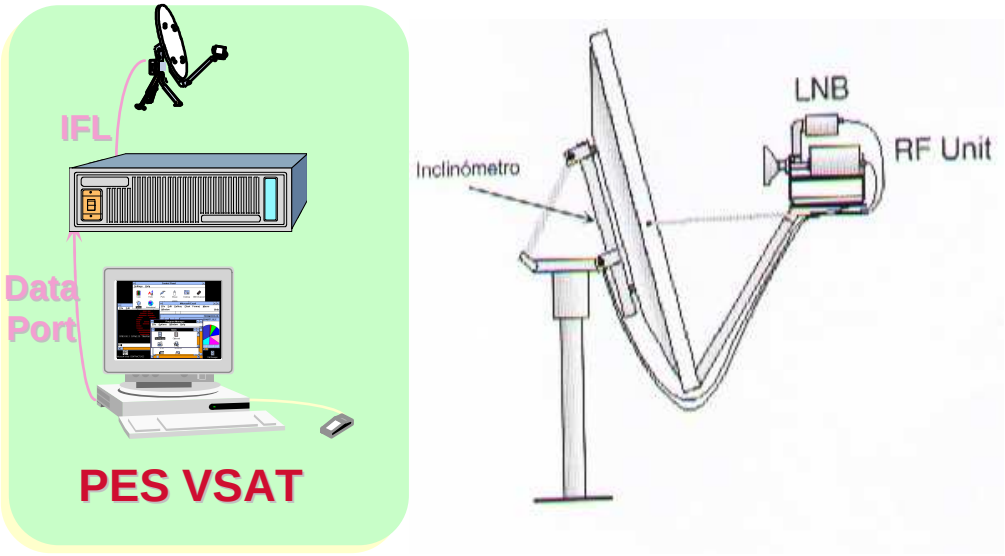

Figura 2.6: Diagrama del enlace de comunicaciones para las FINCAS.

OFICINA CENTRALUIO

En la oficina CENTRAIUIO, se tiene una DTU (Data Terminal Unit) 36.00 Marca Newbridge, la misma que a través de cobre se conecta a un concentrador de DTU´s, ubicado en uno de los nodos del proveedor.

Se tiene un router cisco de la serie 1700, cuyo puerto serial está conectado a la DTU y el puerto Ethernet a una tarjeta de Firewall con cable cruzado.

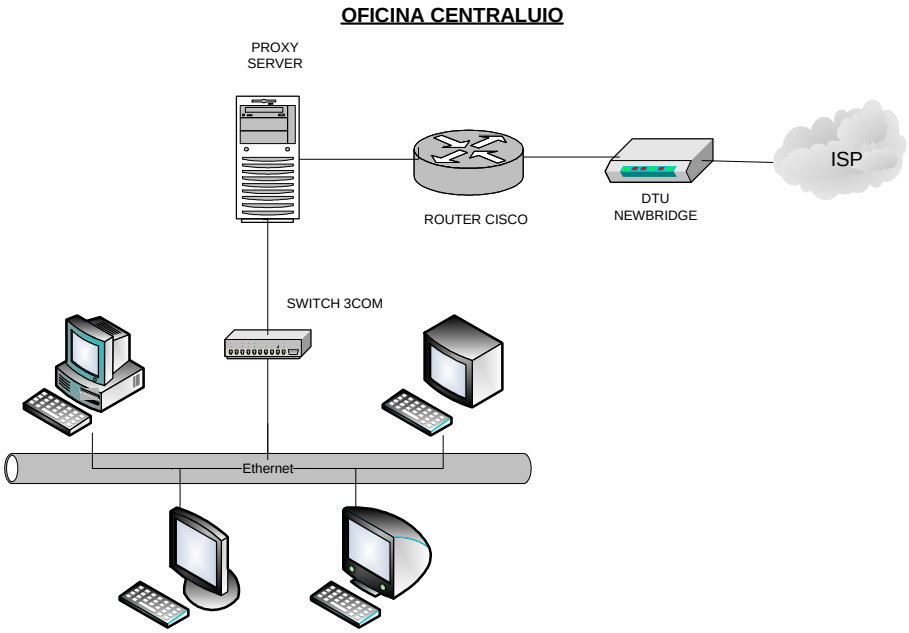

Figura 2.7 Diagrama del sistemas de comunicación de la CENTRALUIO.

2.2.4 ACCESO A INTERNET

Internet es una red de redes a escala mundial de millones de computadoras interconectadas con el conjunto de protocolos TCP/IP. También se usa este nombre como sustantivo común y por tanto en minúsculas para designar a cualquier red de redes que use las mismas tecnologías que la Internet, independientemente de su extensión o de que sea pública o privada.
Al contrario de lo que se piensa comúnmente, "Internet" no es sinónimo de World Wide Web. Esta es parte de aquella, siendo la World Wide Web uno de los muchos servicios ofertados en la red Internet. La Web es un sistema de información mucho más reciente (1995) que emplea la red Internet como medio de transmisión.

Algunos de los servicios disponibles en Internet aparte de la Web son el acceso remoto a otras máquinas (SSH - Secure Shell y Telnet), transferencia de archivos (FTP), correo electrónico (e-mail), boletines electrónicos (news o grupos de noticias), conversaciones en línea (chats), mensajería instantánea

Los accesos a Internet que se tiene actualmente el las FINCAS y la Oficina CENTRALUIO son:

FINCA 1 Y FINCA 2

Acceso a Internet: Las fincas cuentan con un acceso a Internet dedicado, el cual trabaja a 64 Kbps de Subida (Upload) y 128 Kbps de Bajada (Download) vía satélite. Utiliza tecnología VSAT, ya descrita anteriormente en capítulo 1, literal 1.1.3.

Un análisis detallado del tráfico y consumo del ancho de banda del acceso a Internet de las fincas, se muestra en el literal 3.2.1.2.1 apartados (b) y (c).

OFICINA CENTRALUIO

Acceso a Internet: La oficina cuenta con un acceso a Internet dedicado vía cobre, que trabaja a 512 Kbps con tecnología Frame-Relay (FR), teniendo como ISP, un proveedor local (Impsat).

Un análisis detallado del tráfico y consumo del ancho de banda del acceso a Internet de la Matriz, se muestra en el literal 3.2.1.2.1 apartados (a).

2.2 INFRAESTRUCTURA DE HARDWARE Y SOFTWARE

La infraestructura de Hardware y Software que se tiene en cada una de las FINCAS y en la Oficina CENTRALUIO es la siguiente:

2.3.1 SERVIDORES

FINCA 1

SERVIDORES

EQUIPO	SOFTWARE
HP Proliant ML330 Pentium ® 3 CPU 800 Mhz Disco SCSI 40 GB RAM 512 MB Tape Backup Segate IBM 4 mm.	Microsoft Windows 2000 Server SP4 SQL SERVER 6,5 Veritas Backup Exec
HP Compaq d530 SFF Pentium ® 4 CPU 2,8 Ghz RAM 248 MB Disco Duro Maxtor 40 GB Broadcom Netxtreme Gigabit Ethernet	Microsoft Windows XP Profesional SP2 Trend Microsystem Antivirus
Compaq Deskpro EP Pentium ® III Procesor 256 MB RAM Disco 40 GB NIC Compaq NC3120 Fast Ethernet NIC 3com Fast Ethernet XL 10/100 Mb	Linux White Box Edition 4.0 SQUID

Tabla 2.1: Servidores de la Finca1

FINCA 2

SERVIDORES

EQUIPO	SOFTWARE
HP Proliant ML330 Pentium ® 3 CPU 800 Mhz Disco SCSI 40 GB RAM 512 MB Tape Backup Segate IBM 4 mm.	Microsoft Windows 2000 Server SP4 SQL SERVER 6,5 Veritas Backup Exec
HP Compaq d530 SFF Pentium ® 4 CPU 2,8 Ghz RAM 248 MB Disco Duro Maxtor 40 GB Broadcom Netxtreme Gigabit Ethernet	Microsoft Windows XP Profesional SP2 Trend Microsystem Antivirus
Compaq Deskpro EP Pentium ® III Procesor 256 MB RAM Disco 40 GB NIC Compaq NC3120 Fast Ethernet NIC 3com Fast Ethernet XL 10/100 Mb	Linux White Box Edition 4.0 SQUID

Tabla 2.2: Servidores de la Finca 2

OFICINA CENTRALUIO

SERVIDORES

EQUIPO	SOFTWARE
HP Proliant ML370 Procesador Xenón ™ 3,2 Ghz Disco Ultra SCSI 36,4 GB RAM 1 GB HP C5683A SCSI Sequential Device HP NC7781 Gigabit Server Adapter	Microsoft Windows 2003 Server para Small Business Server Microsoft Exchange 5,0 Veritas Backup Exec
Compaq Prosignia X86 Family 5 Model 2 Stepping 12 Disco SCSI 20 GB RAM 64 MB Net Intelligent 10T PCI UTP Bus 0	Microsoft Windows NT SQL SERVER 6,5
HP Compaq d530 SFF Pentium ® 4 CPU 2,8 Ghz RAM 248 MB Disco Duro Maxtor 40 GB Broadcom Netxtreme Gigabit Ethernet	Microsoft Windows XP Profesional SP2 Trend Microsystem Antivirus
HP Compaq d530 SFF Pentium ® 4 CPU 2,8 Ghz RAM 248 MB Disco Duro Maxtor 40 GB Broadcom Netxtreme Gigabit Ethernet	Linux White Box Edition 4.0 Interscan Virus Wall 5,0 (Trend Microsystem)

Tabla 2.3: Servidores de la CENTRALUIO

2.3.2 ESTACIONES DE TRABAJO

FINCA 1

ESTACIONES DE TRABAJO

EQUIPO	No. ESTAC.	SOFTWARE
Compaq Deskpro ECD Geniune Intel x86 Family 6 Model Stepping 1 256 MB RAM Disco 40 GB NIC Compaq NC3120 Fast Ethernet	9	win 98 2DA Edición Offices 2000 Estándar
Compaq Deskpro EP Pentium ® III Procesor 64 MB RAM Disco 40 GB NIC 3com Fast Ethernet XL 10/100 Mb	10	win 98 2DA Edición Offices 2000 Estándar
HP Compaq d530 SFF Pentium ® 4 CPU 2,8 Ghz RAM 248 MB Disco Duro Maxtor 40 GB Broadcom Netxtreme Gigabit Ethernet	4	WIN XP Pro. SP2 Offices 2000 Estándar

Tabla 2.4: Estaciones de Trabajo de la Finca 1

FINCA 2

ESTACIONES DE TRABAJO

EQUIPO	No. ESTAC.	SOFTWARE
Compaq Deskpro ECD Geniune Intel x86 Family 6 Model Stepping 1 256 MB RAM Disco 40 GB NIC Compaq NC3120 Fast Ethernet	9	win 98 2DA Edición Offices 2000 Standar
Compaq Deskpro EP Pentium ® III Procesor 64 MB RAM Disco 40 GB NIC 3com Fast Ethernet XL 10/100 Mb	10	win 98 2DA Edición Offices 2000 Standar
HP Compaq d530 SFF Pentium ® 4 CPU 2,8 Ghz RAM 248 MB Disco Duro Maxtor 40 GB Broadcom Netxtreme Gigabit Ethernet	4	WIN XP Pro. SP2 Offices 2000 Standar

Tabla 2.5: Estaciones de Trabajo de la Finca 2

OFICINA CENTRALUIO

ESTACIONES DE TRABAJO

EQUIPO	No. ESTAC.	SOFTWARE
Compaq Deskpro ECD Geniune Intel x86 Family 6 Model Stepping 1 256 MB RAM Disco 40 GB NIC Compaq NC3120 Fast Ethernet	14	win 98 2DA Edición Offices 2000 Estándar
Compaq Deskpro EP Pentium ® III Procesor 64 MB RAM Disco 40 GB NIC 3com Fast Ethernet XL 10/100 Mb	12	win 98 2DA Edición Offices 2000 Estándar
HP Compaq d530 SFF Pentium ® 4 CPU 2,8 Ghz RAM 248 MB Disco Duro Maxtor 40 GB Broadcom Netxtreme Gigabit Ethernet	10	WIN XP Pro. SP2 Offices 2000 Estándar

Tabla 2.6: Estaciones de Trabajo de la Centraluio.

2.3.3 EQUIPOS DE COMUNICACIONES

FINCA 1

EQUIPOS DE COMUNICACIONES

EQUIPO
Switch 3com Baseline 10/100 Super Stack 24 Puertos
Central Telefónica Nitsuko TX Series

Tabla 2.7 Equipos de comunicaciones de la Finca 1

FINCA 2

EQUIPOS DE COMUNICACIONES

EQUIPO
Switch 3com Baseline 10/100 Super Stack 24 Puertos
Central Telefónica Nitsuko TX Series

Tabla 2.8 Equipos de comunicaciones de la Finca 2

OFICINA CENTRALUIO

EQUIPOS DE COMUNICACIONES

EQUIPO
Switch 3com Baseline 10/100 Super Stack 24 Puertos
Central Telefónica Nitsuko TX Series

Tabla 2.9 Equipos de comunicaciones e la Centraluio.

2.3.4 EQUIPOS DE ALIMENTACION ELECTRICA

FINCA 1 Y FINCA 2

EQUIPOS DE ALIMENTACION ELECTRICA

EQUIPO
UPS Power Prestige Firmesa 6KVA 2 Módulos de Baterías

Tabla 2.10: Equipos alimentación eléctrica de las Fincas

OFICINA CENTRALUIO

EQUIPOS DE ALIMENTACION ELECTRICA

EQUIPO
UPS
Power Prestige Firmesa
6KVA
Un Generador Caterpillar de 1000 W
2 Módulos de Baterías

Tabla 2.11: Equipos alimentación eléctrica de la Centraluio

CAPITULO 3

3. ANÁLISIS DE FACTIBILIDAD

El propósito de este capítulo, es el análisis y búsqueda de soluciones al problema descrito en el literal 2.1.2 del capítulo anterior, las mismas que permitirán tener una transferencia segura, confiable y en tiempo real (en línea) de la información desde las Fincas, hacia la Oficina Central (CENTRALUIO) en Quito.

Para llevar a cabo este cometido, se analizará la replicación de la información como una alternativa para mantener la información actualizada desde las fincas hacia la base de datos general ubicada en la oficina CENTRALUIO en Quito.

Luego se analizará la interconexión entre las fincas con los medios disponibles en la empresa y con medios alternativos. Cabe destacar que en este capitulo, únicamente se analizarán la opciones de interconexión con sus costos, mas no se elegirá una determinada alternativa. Esto se detalla en el capitulo 4 del presente proyecto.

Finalmente se detallará el costo/beneficio que acarrea mantener interconectada la red empresarial y disponer de la información actualizada.

3.1 SERVICIOS A SER IMPLEMENTADOS

3.1.1 DESCRIPCIÓN DEL SERVICIO

La transmisión y la actualización de la información de las bases de datos de las Fincas hacia la Oficina CENTRALUIO en Quito, es el principal problema a ser resuelto en este proyecto. Para esto es conveniente realizar un análisis detallado

del problema para encontrar los mecanismos idóneos que conlleven a la solución del mismo.

En las fincas, los usuarios del área de cosecha y poscosecha son los que ingresan la información en la base de datos local, por medio de un sistema desarrollado en visual Basic 6.0, conectado hacia el servidor por un ODBC (conector a base de datos). Las modificaciones hechas a la base de datos local, deben actualizarse en la base de datos general (CENTRALUIO), con esto se cumple uno de los objetivos de este proyecto que es mantener la información actualizada y en línea.

La replicación en bases de datos es una alternativa viable, por lo que se analizará esta opción en el siguiente apartado.

3.1.1.1 Replicación de Información (Base de datos)

En esta parte del proyecto se analizan los métodos de replicación de bases de datos que están incluidos en la versión Enterprise del SQL Server 2000 de Microsoft.

3.1.1.1.1 Conceptos Básicos de Replicación en SQL Server 2000

La replicación de datos entre servidores es la capacidad para difundir una fuente de datos de manera fiable entre diferentes servidores. Esto permite distribuir datos entre servidores que pueden estar muy alejados físicamente y conectados a través de líneas de comunicación de poca capacidad o disponibles solo en ciertos momentos. De esta manera los datos estarán físicamente más cercanos en el lugar en donde van a ser usados, en sus diversas aplicaciones.

La replicación consiste en intercambiar entre servidores remotos copias de los datos que residen en ellos, manteniéndolas actualizadas con cierta periodicidad

los cambios que en cada fuente de datos se produzcan. Ese proceso de actualización se denomina *sincronización*.

Para llevar a cabo el proceso de replicación se ha definido un modelo basado en ***publicador-suscriptor*** (*Publisher-subscrib*er). En este modelo el servidor que pone a disposición los datos a replicar se denomina *publicador*, mientras que el servidor que recibe los datos implicados se denomina *suscriptor*. Para completar este modelo se necesita de un *tercer servidor* denominado *distribuidor*, quien es el que transmite los datos desde el publicador a los suscriptores. Contiene una base de datos denominada distribución. En muchas ocasiones el publicador y distribuidor están integrados en un mismo equipo.

Dentro de un publicador existirán artículos que pondrán a disposición de los suscriptores, estos artículos pueden ser tablas, procedimientos almacenados y vistas.

3.1.1.1.2 Tipos de Replicación.

a) Replicación Transaccional: La replicación transaccional se basa en el *"Transaction Log",* tras la sincronización inicial, la replicación se realiza propagando las transacciones que están marcadas y sujetas a replicación a los suscriptores.

b) Replicación de Fusión: La replicación de fusión o mezcla de datos, permite que cada suscriptor pueda actualizar su copia mientras está conectado o desconectado, para después fusionar o mezclar sus modificaciones con las que pueden haberse producido en el publicador u otros suscriptores.

c) Replicación de Instantáneas: Este método de replicación copia a los suscriptores el estado de la replicación en un cierto instante de tiempo. En este modo y a intervalos de tiempos prefijados. La tabla publicada se actualiza y dicha

imagen instantánea del estado de la tabla es la entidad que se distribuye hasta la próxima actualización.

3.1.1.1.3 Replicación Transaccional (Transactional Replication)

Replicación y Trans action Log

Cuando una transacción que se haya aplicado a la base de datos fuente del proceso se marca como susceptible de replicación, ésta se almacena en el *transaction log.* En el momento de la actualización del sistema, leerá el log y los cambios a los que se haya visto sometida la fuente de datos y se reflejarán en los servidores que reciban la copia. Esta replicación recibe el nombre de "*replicación transacional".*

Cada cambio que se llave a cabo sobre registros almacenados en datos que conformen un artículo en una replicación, son registros en el transaction log de la base de datos que se publica. El proceso de replicación transfiere esas modificaciones anotadas en el log a la base de datos de distribución. Cuando los suscriptores son sincronizados, las operaciones replicadas se aplican a aquellos, en el mismo orden que se produjeron en el replicador. De este modo, y a intervalos prefijados por el modo de sincronización, los datos fluyen desde el duplicador, a los suscriptores de manera incremental. Se debe recalcar que, este modo de replicación de datos solo puede ser actualizado en el duplicador.

3.1.1.1.4 Escenarios de la Replicación Transaccional

Publicador Único: Consiste en un único servidor, el cual proporciona los datos a todos los suscriptores.

Publicador Único – Distribuidor: Consiste en un único servidor que asigna los datos a un distribuidor que los hace accesibles a todos los suscriptores.

Publicadores y suscriptores múltiples: Consta de múltiples servidores que provee los datos a múltiples suscriptores.

3.1.1.1.5 Proceso de Sincronización

Cada vez que se crea una publicación debe llevarse a cabo un proceso de sincronización inicial antes de que puedan comenzar a replicarse los datos.

Este proceso garantiza al suscriptor o suscriptores tengan preparadas las estructuras de datos de almacenamiento para la recepción de los datos. Esto toma el nombre de *sincronización inicial.* La sincronización inicial permite al suscriptor y publicador poner cada uno de los objetos que forman parte de la replicación en el mismo estado.

Este estado comprende tanto la estructura de las tablas que hay detrás de los artículos publicados, como los propios datos que albergan. La sincronización es imprescindible y si no se la lleva a cabo, no podrá ejecutarse la replicación.

Realizar una publicación, significa poner a disposición de los suscriptores la copia de una o varias tablas. El proceso de sincronización inicial construye, para cada artículo de cada publicación, una copia de los datos de la tabla a publicar y la almacena en un fichero. Este fichero, junto con el que se crea en el momento de la definición de la publicación y que contiene la estructura de la tabla que da lugar al artículo, constituye la información necesaria para proceder a la sincronización.

La sincronización inicial puede configurarse para ser realizada de manera automática o manual.

a) Sincronización automática: Es el modo que viene configurado por defecto. SQL Server llevará a cabo el proceso de sincronización a intervalos fijos. Todo el proceso se ejecuta a través de tareas automáticas (jobs) que radican en la base de datos de distribución, sin que sea preciso ningún tipo de operación manual.

La sincronización automática, es adecuada para entornos en los que las conexiones sean buenas entre los servidores y permite que los suscriptores tengan copias de los datos prácticamente en tiempo real, con intervalos de actualización de minutos.

b) Sincronización manual: Este modo de sincronización requiere que un usuario sincronice las bases de datos y que notifique a SQL Server que dicho proceso se ha completado. El proceso en si, es decir, la creación de las copias del esquema y los datos en ficheros, es llevado a cabo por el duplicador.

En la sincronización manual, el usuario es quien debe proceder a la transferencia de la información almacenada en los ficheros hacia los suscriptores. Este modo es útil cuando han de manejarse grandes tablas o líneas de comunicación lentas.

3.1.1.1.6 Proceso de Replicación Transaccional

De lo visto anteriormente, el proceso de replicación se basa en el transaction log, y se lleva a cabo con la ayuda de una base da datos de distribución. Las transacciones a ser replicadas están marcadas en el transaction log de la base de datos publicada. El proceso lector del transaction log busca estas transacciones, crea las sentencias SQL necesarias y las envía a la base de datos de distribución.

El proceso de replicación envía al suscriptor las transacciones encontradas en la base de datos de distribución. Luego, estas transacciones son eliminadas, y para reducir el tráfico necesario en la transferencia de las modificaciones en lugar de enviar datos reales, se utilizan sentencias SQL.

- **Servidor y base de datos de distribución:** El servidor de distribución y la base de datos del mismo nombre sirven de puente entre el publicador y los suscriptores. Existen básicamente dos maneras de habilitar el servidor de distribución, como servidor remoto o en el propio servidor local de publicación.

Si se realiza la opción de servidor remoto se minimiza la carga de trabajo y transacciones del servidor de publicación. Debe tenerse en cuenta que el proceso de replicación conlleva la ejecución de un buen número de procedimientos almacenados y de transacciones que suponen un esfuerzo para el servidor que lo lleve a cabo. Es posible, sin embargo, ubicar en el mismo servidor el publicador y el distribuidor, hecho que facilitará la administración pero disminuirá el rendimiento.

La base de datos de distribución almacena las transacciones que deben ser duplicadas. Dichas transacciones permanecerán en ellas hasta que todos los suscriptores hayan actualizado la información. Se puede decir que SQL Server utilizará esta base de datos como un mecanismo para tener controlado el proceso de transferencia de información entre el publicador y el suscriptor.

- **Agentes del proceso de replicación transaccional:** El proceso de replicación transaccional se realiza mediante la actuación de un conjunto de procesos que se describen a continuación.
  El Agente lector del trasaction log (Log reader Agent) se ejecuta en el distribuidor y se detectan aquellas transacciones que afectan a datos publicados y las ubica en la base de datos de distribución. Su ejecución puede ser continua o programada, de manera que esta detección se lleve a cabo a intervalos especificados en el momento de crear la publicación:

  1. El Agente Lector lee inicialmente el transaction log de la base de datos en la que se basa la publicación y detecta las operaciones que han sido marcadas como susceptibles de ser replicadas.

  2. El Agente copia solo las transacciones conformadas a la base de datos de distribución.

  3. A medida que va transcurriendo el tiempo, el Agente ejecuta el comando *sp_replcmds* para determinar que transacciones deben

transferirse a la base de datos de distribución y procede a esta transferencia.

4. Cuando ha culminado la transferencia de transacciones el Agente llama a *sp_repldone* para marcar el punto final de la replicación de las transacciones.

5. El Agente de distribución transfiere los datos desde la base de datos de distribución hacia los suscriptores, bien a petición de estos, o bajo la iniciativa del distribuidor. El Agente de distribución se encuentra en el suscriptor o en el distribuidor, en función de sí, la sincronización se lleva a cabo a petición del suscriptor (*pull suscriptions*) o del publicador (*push suscriptions*).

6. El Agente lleva a cabo la copia de los datos replicados.

3.1.1.1.7 Replicación Transaccional de Procedimientos Almacenados

Se pueden publicar como artículos, procedimientos almacenados en sitios de la base de publicación. En la replicación transaccional, la replicación supone la transmisión de las ejecuciones de los procedimientos almacenados que se produzcan en el publicador. Esto reduce enormemente el tráfico de red.

3.1.1.1.8 Tipos de Replicación de Procedimientos

Existen tres métodos diferentes de replicación de procedimientos.

- **Replicación incondicional de la ejecución:** Transmite la ejecución del procedimiento a todos los suscriptores y no importa si la ejecución de todas las sentencias SQL que contiene se han completado con éxito o no. Este proceso conlleva que sea imposible conocer si los datos de todos los servidores contienen los mismos datos. Se pierde, la coherencia transaccional.

- **Replicación de la ejecución en un contexto transaccional *(serializable procedure execution)*:** Solo se replica la ejecución del procedimiento si ésta se desarrolla en el publicador en el ámbito de una transacción serializable. En caso contrario no se replicará la ejecución del procedimiento sino sus operaciones individuales, una a una.

- **Replicación de datos actualizables:** En SQL Server 6.5 la replicación era esencialmente un proceso en el que se transmitían copias de solo lectura de los datos desde el publicador a los suscriptores. Es decir, estos no podían en ningún momento actualizar los datos publicados.

  En SQL Server 7 se añadió la posibilidad de que los suscriptores pueden realizar modificaciones sobre los datos publicados. Esta posibilidad, que se mantiene en SQL Server 2000 es denominada Actualización Inmediata de Suscriptores (*Inmediate Updating Subscribers*).

  En SQL Server 2000 se añade la actualización asíncrona o en cola (*queued updating subscribers*). Las dos modalidades de actualizaciones del SQL Server 2000 son:

3.1.1.1.9 Actualización Inmediata o Síncrona (Inmediate Updating Subscribers)

Esta funcionalidad permite que los suscriptores actualicen los datos del publicador. La transmisión de información entre ambos servidores se lleva a cabo siguiendo el protocolo de confirmación en dos fases (Two-Phase commit). Posteriormente, el publicador enviará los datos modificados al resto de suscriptores.

El método es muy sencillo. El suscriptor inicia un proceso de actualización gobernado por el protocolo Two-Phase commit. Las modificaciones que el citado suscriptor ha realizado en su base de datos local (copia transferida por el publicador en la anterior sincronización), se transfieren al publicador. Cuando se produzca el siguiente proceso de sincronización todos los suscriptores recibirán estas modificaciones. El principal problema que se plantea es que el servidor de publicación debe estar conectado con el suscriptor en el momento de realizar la actualización, requisito indispensable para que el protocolo de confirmación de dos fases pueda llevarse a cabo, con lo que la autonomía, evidentemente es afectada.

El proceso de replicación se ocupa de los aspectos del protocolo de confirmación en dos fases, sin que las aplicaciones sean concientes de ello. La aplicación realiza siempre las actualizaciones localmente, el proceso de replicación es quien se encarga de programar las copias en el suscriptor. Cuando la replicación falle, (el proceso de replicación con protocolo Two-Phase commit) la aplicación recibirá una notificación de error en la transacción.

La principal ventaja que se obtiene frente a un proceso estándar de transacciones distribuidas que utilicen un mismo protocolo, es que no es necesario que todos los servidores involucrados estén conectados en todo momento sino que al contrario, solo se requiere esta presencia real por parejas de servidores, entre publicador y el suscriptor que quiere realizar la actualización.

3.1.1.1.10 Actualización Asíncrona o en Cola (Queued Updating Subscribers)

La actualización en cola permite que los suscriptores actualicen los datos publicados aunque en el momento de la actualización no exista una conexión activa entre el publicador y suscriptor. Esta nueva funcionalidad aumenta la autonomía, pero es un serio atentado a la consistencia transaccional. Cuando el suscriptor modifica los datos mediante *INSERT, UPDATE, DELETE,* los cambios se almacenan en la cola.

La cola se implementa como una tabla en el propio SQL Server, pero si el servidor está instalado en Windows 2000, se puede integrar utilizando el servicio del sistema operativo Message Queue Server. Si se utilizan colas de SQL Server, las actualizaciones se almacenan en la tabla MSreplication_queue. Si se utiliza Message Queue Server, las actualizaciones se almacenarán en una cola de mensajes en el distribuidor.

Las transacciones en cola se aplican al publicador cuando se restaura la conexión de red. Esta asincronía es una potencial fuente de errores, que no existía en la versión 7, en la que cualquier modificación debía ser síncrona utilizando el mecanismo Two-Phase commit, ya que los mismos datos pueden haber sido actualizados por el publicador o por otro suscriptor y por lo tanto, se pueden producir conflictos. No obstante, existen mecanismos para resolver automática y manualmente los conflictos. El proceso a seguir durante la replicación de la actualización asíncrona es el siguiente:

1. Un conjunto de *triggers (Código para actuaizaciones de una cola)* que se crean en la base de datos de suscripción (en el momento de crear la publicación) en las tablas que sustentan los artículos, se disparan como respuesta a las actualizaciones realizadas en el suscriptor. Estos *triggers* contiene código para almacenar las actualizaciones en una cola.

2. El Agente Lectura de cola (un nuevo Agente en SQL Server 2000) aplica las transacciones en la cola a la publicación apropiada, cuando se dispone de conexión con el duplicador.

3. Se detectan y resuelven los conflictos existentes según la directiva de resolución de conflictos definida.

4. Los cambios realizados en el publicador se propagan a los demás suscriptores.

3.1.1.2 Esquema de Replicación Aplicada al Proyecto.

La información generada en las fincas, se almacena en una base de datos local. Cada uno de estos servidores se configuran como publicador y distribuidor de la base de datos de producción. Los artículos a publicarse, serán determinadas tablas, en donde se almacenarán los datos de la producción diaria.

El servidor de la Matriz (CENTRALUIO) será configurado como suscriptor. En éste se almacenará toda la información proveniente de las Fincas, las actualizaciones se las realizarán de forma automática, logrando con esto mantener la información en línea en la Matriz, tal como se ilustra en la siguiente gráfica.

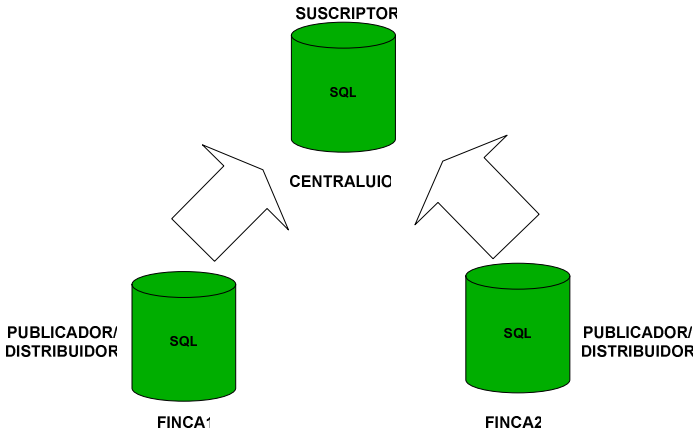

Figura 3.1: Diagrama de Replicas.

3.2 ANÁLISIS TÉCNICO

3.2.1 ALTERNATIVAS DE INTERCONEXIÓN PARA LA RED EMPRESARIAL

El objetivo de la Interconexión de Redes (Internetworking), es dar un servicio de comunicación de datos que involucre diversas redes con diferentes tecnologías de forma transparente para el usuario.
Algunas de las ventajas que plantea la interconexión de redes, son:

- Compartición de recursos dispersos.
- Coordinación de tareas de diversos grupos de trabajo.
- Reducción de costos, al utilizar recursos de otras redes.
- Aumento de la cobertura geográfica.

Existen varios tipos de interconexión de redes, pero la forma como está distribuida la red corporativa (geográficamente distantes), hace que se analice la interconexión con enlaces dedicados y VPN con Internet.

3.2.1.1 Enlaces Dedicados

Hoy, la necesidad de mantener comunicadas las sucursales con la oficina matriz de un empresa a hecho que varias compañías se dediquen a ofrecer el servicio de interconexión de redes mediante enlaces dedicados denominados carriers o portadores de datos. En el país existen varias empresas dedicadas a este propósito como: Impsat, Telconet, Andinadatos, Grupo TV-Cable, etc. Cada una de éstas con sus ventajas, precios y productos, accesibles a las empresas que necesitan soluciones en telecomunicaciones.

En general, los mecanismos de envío de información desde un punto a otro puede clasificarse de las siguientes formas:

Frame Relay: A cada acceso que el cliente necesite enlazar, se definen previamente los Circuitos Virtuales Permanentes (PVC) asignándole a cada PVC una velocidad de transferencia de información mínima (CIR) garantizada por la red. Si el cliente lo requiere, puede utilizar una mayor velocidad hasta un máximo determinado por la capacidad física de acceso.

Clear Channel: Es una conexión dedicada y exclusiva que permite enlazar en forma permanente dos puntos predeterminados. Clear Channel es ideal para aquellas aplicaciones que necesitan mantener un flujo de información constante, o comunicaciones de gran caudal y calidad por períodos de tiempo prolongados.

Por sus características especiales Clear Channel, sirve de hecho como backbone de alta velocidad para clientes.

V-SAT (Very Small Aperture Terminals): Es una solución satelital integrada de conectividad y equipamiento para redes, destinada a interconexiones entre oficinas centrales y dependencias corporativas, que ofrece un gran número de puntos remotos, mediante vínculos digitales bidireccionales.

Dataplus: Es una solución integral de conectividad vía satélite que permite establecer enlaces digitales bidireccionales de alto tráfico y transparentes al protocolo.

3.2.1.1.1 Determinación del Ancho de Banda para el Enlace Dedicado

Para determinar la capacidad de ancho de banda del canal dedicado se tomará como referencia el tráfico generado por el servicio a implementarse (replicación en base de datos), como una necesidad urgente de la empresa.

a) Cálculo del ancho de banda producido por la replicación en base de datos

Para realizar el cálculo del ancho de banda producido por la replicación transaccional, se llevo a cabo un muestreo de la cantidad de ***insert, update*** *y* ***delete*** que se realiza en las tablas donde se guarda la información de la producción diaria de las fincas durante una semana, esto debido a que únicamente las sentencias descritas anteriormente son sujetas de replicación en el modelo transaccional de SQL Server.

Con esta información se procederá a calcular un promedio de transacciones por hora que en el servidor de las fincas se llevan a cabo, luego se simulará en el prototipo, en el lado del publicador, la ejecución de un número de transacciones igual al promedio calculado, esto causara la distribución de los cambios realizados en el publicador al suscriptor produciendo trafico en la red, el mismo que será capturado con ayuda de la herramienta MRTG. Con esto se tiene los siguientes pasos a realizar:

- Muestreo de transacciones en los servidores de las fincas.
- Cálculo del promedio de transacciones por minuto.
- Simulación de la ejecución del promedio de transacciones por hora en el publicador y toma de muestras de tráfico con MRTG.

Muestreo de transacciones en los servidores de las fincas.

Primero se buscará donde almacenar la información del número de transacciones hechas en las tablas que son sujetas de replicación, para esto se creara un tabla denominada AUDIT, en los servidores de las dos fincas, con los siguientes campos: tipo_evento, fecha, descripción, usuario y terminal.

Luego cada tabla que se desea muestrear tendrá un disparador (*trigger*) que cada ves que detecte una modificación en la tabla (insert, update o delete), inserte un registro en la tabla AUDIT con el tipo de evento, fecha, descripción, usuario,

terminal y aplicación[7]. Con esto se obtendrá un registro del número de transacciones realizadas durante una semana laboral, de lunes a viernes desde las ocho hasta las cinco de la tarde. En las siguientes tablas se muestran los resultados obtenidos:

FECHA	INSTRUCCIÓN	NUMERO DE TRANSACCIONES
07/11/2005	INSERT	431678
	UPDATE	132392
	DELETE	952
08/11/2005	INSERT	428943
	UPDATE	130778
	DELETE	1928
09/11/2005	INSERT	429724
	UPDATE	131283
	DELETE	1892
10/11/2005	INSERT	427182
	UPDATE	129482
	DELETE	1348
11/11/2005	INSERT	435127
	UPDATE	130593
	DELETE	1492
TOTAL		**2814794**

Tabla 3.1: Número de transacciones por día de la FINCA1.

FECHA	INSTRUCCIÓN	NUMERO DE TRANSACCIONES
07/11/2005	INSERT	358142
	UPDATE	101997
	DELETE	932
08/11/2005	INSERT	362281
	UPDATE	99895
	DELETE	1528
09/11/2005	INSERT	360034
	UPDATE	107987
	DELETE	1892
10/11/2005	INSERT	357327
	UPDATE	103556
	DELETE	1348
11/11/2005	INSERT	362098
	UPDATE	104785
	DELETE	1492
TOTAL		**2325294**

Tabla 3.2: Número de transacciones por día de la FINCA2

[7] La configuración del trigger se muestra en el Anexo ***A***

En las siguientes tablas se muestran el número total de transacciones por semana de las fincas.

INSTRUCCIÓN	TRANSC/SEMANA
INSERT	2152654
UPDATE	654528
DELETE	7612

Tabla 3.3 Número total de transacciones de una semana de la FINCA1

INSTRUCCIÓN	TRANSC/SEMANA
INSERT	1799882
UPDATE	518220
DELETE	7192

Tabla 3.4: Número total de transacciones de una semana de la FINCA2

Cálculo del promedio de transacciones por hora.

Para calcular el promedio de transacciones por hora se tomara en cuenta la siguiente consideración.

El número de horas laborables en las fincas son 8, por lo que únicamente en este periodo de tiempo se tendrá tráfico producido por la replicación de base de datos, entonces se tomará este lapso de tiempo para calcular el promedio de transacciones por hora.

INSTRUCCIÓN	TOTAL	H. LABORABLES SEMANALES	TRANSAC/HORA	TRANSAC/MINUTO
INSERT	2152654	40	53816,35	897
UPDATE	654528	40	16363,2	272
DELETE	7612	40	190,3	3

Tabla 3.5: Promedio de transacciones por hora y por minuto de la FINCA1

INSTRUCCIÓN	TOTAL	H. LABORABLES SEMANALES	TRANASAC/HORA	TRANSAC/MINUTO
INSERT	1799882	40	44997,05	750
UPDATE	518220	40	12955,5	216
DELETE	7192	40	179,8	3

Tabla 3.6: Promedio de transacciones por hora de la FINCA2

Simulación del promedio de transacciones por minuto

Para la simulación del tráfico que produce la replicación transaccional de SQLServer 2000 se tomó como referencia los promedios de transacciones por minuto de cada una de las fincas, con estos valores se configuraron tres tareas en cada uno de los publicadores de prueba, para simular los insert, update y delete, las tareas están calendarizadas para ejecutarse en un numero igual al promedio por minuto detallado en las tablas 3.5 y 3.6[8].

El tráfico producido por la replicación de base de datos fue capturado con la herramienta MRTG durante 8 horas. Los siguientes gráficos muestran el ancho de banda utilizado por el publicador para realizar la replica de datos.

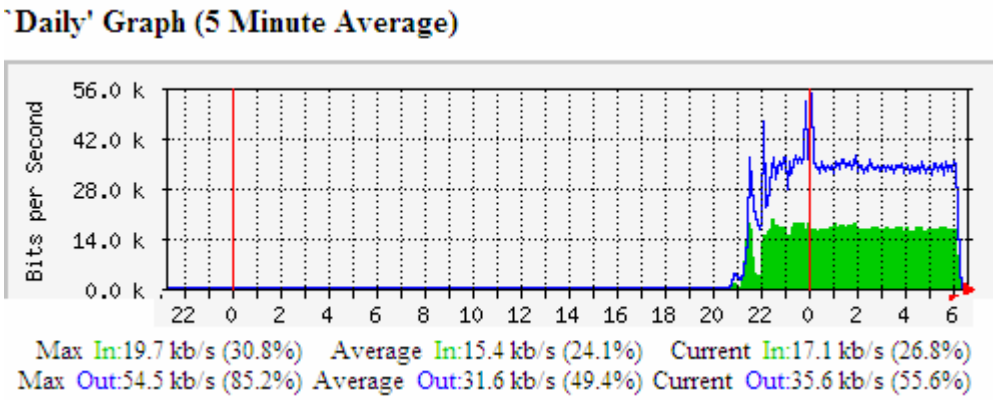

Figura 3.2: Tráfico de la replicación simulado para la FINCA1.

[8] El strip de las tareas se muestran en el Anexo ***B***

Horas	Tráf. Entrante [Kbps]	Tráf. Saliente [Kbps]
22:00	16	45
23:00	18	35
0:00	18	55
1:00	19	36
2:00	19	37
3:00	18	35
4:00	18	35
5:00	18	35
6:00	18	35
Promedio	**18**	**38.67**

Tabla 3.7: Promedio tráfico simulado para la FINCA1.

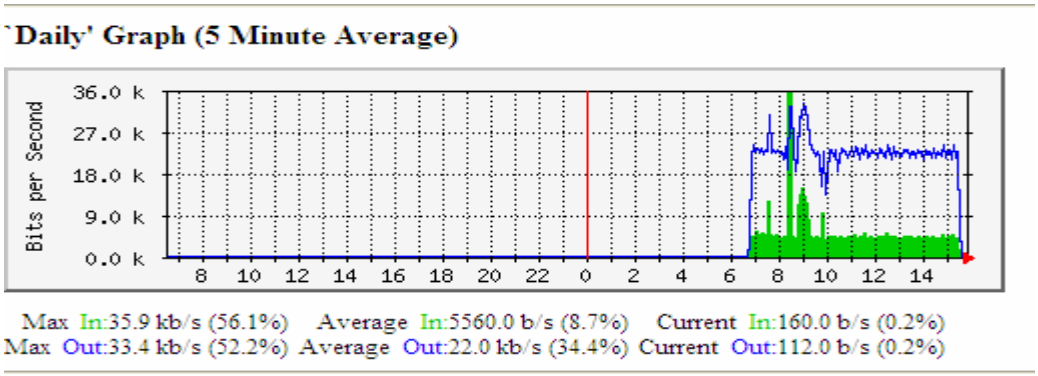

Figura 3.3: Tráfico de la replicación simulado para la FINCA2

Horas	Tráf. Entrante [Kbps]	Tráf. Saliente [Kbps]
7:00	5	26
8:00	25	33
9:00	17	34
10:00	10	21
11:00	4	25
12:00	4	25
13:00	4	25
14:00	4	25
15:00	4	26
Promedio	**8,56**	**26,67**

Tabla 3.8: Promedio tráfico simulado para la FINCA2

El valor del ancho de banda para las fincas son los promedios obtenidos del tráfico generado en la simulación de replicación en base de datos. Detallados en las tablas 3.7 y 3.8.

Para determinar el ancho de banda de la matriz se toma en consideración que en este sitio convergen los tráficos de las fincas, de esta forma se tiene:

TMATRIZ = TFINCA1 + TFINCA2

TMATRIZ = 38.67Kbps + 26.67Kbps

TMATRIZ = 65.34Kbps.

En la siguiente tabla se muestra la capacidad de ancho de banda requerida por la empresa y la ofrecida en el mercado.

Sitio	Capacidad Requerida (Kbps)	Capacidad Ofrecida en el Mercado (Kbps)
CENTRALUIO	65.34	128
FINCA1	38.67	64
FINCA2	26.67	64

Tabla 3.9: Capacidad de ancho de banda total requerida en un enlace dedicado

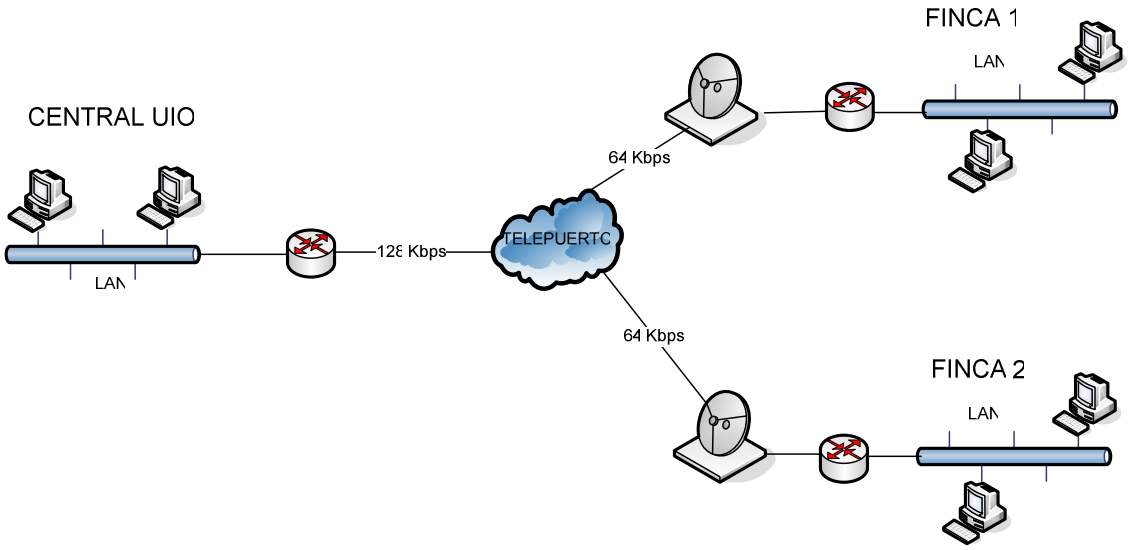

Figura 3.4: Diagrama del enlace dedicado

3.2.1.2 VPNs con Internet

Las Redes Privadas Virtuales (VPNs) sobre Internet ofrecen una buena alternativa de interconexión fiable e íntegra entre dos sitios ubicados geográficamente distantes, siendo ésta la principal razón para la que la mayoría de empresas estén optando por el uso de esta tecnología.

Para el análisis de factibilidad se basará en la tecnología disponible en el mercado para implementar VPN's; que son con hardware y software:

a) Con Hardware

Para este análisis se han tomado las marcas más conocidas y los modelos más económicos que cumplen con los requerimientos básicos, en cuanto a la implementación de las VPNs.

EQUIPO	VERSION	CARACTERISTICAS
Routers: **Cisco 1601** **Cisco 1750** **3COM 3015**	Version 3.0.0. Version 3.5.0.	• SRP features-IPS with less than 50-ms restoration time • IP routing protocols including IS-IS, OSPF, and BGP • Multicast support including protocol-independent multicase. • L2VPN-L2TPv3 for Ethernet based Layer 2 VPN services • L3VPN provider and provider edge functionality • QoS features-Modular QoS CLI, CAR, WRED, and ACLs • Ethernet HDX-FDX (TDR) for 10/100BASE-TX. • Security: authentication, authorization and accounting (AAA)
D-link **(DI-804 HV)**	NA	• Soporte VPN Site-to-Site o Client-to-Site • Soporte VPN pass-through para IPSec, PPTP y L**2**PT • Funcionalidades Firewall, Domain y URL Filtering • Soporte de una DMZ-Host • Soporte Ruteo IP, RIP-**1**/RIP-**2** • Puerto serial para Dial Backup vía ISDN o módem análogo • Administración Web y DHCP Server • Diseño innovador
firewall: **Cisco PIX 520**	Firewall 6.3(5) Device Manager 3.0(4)	• Licensed Features: • Failover: Enabled • VPN-DES: Enabled • VPN-3DES-AES: Enabled • Maximum Physical Interfaces: 6 • Maximum Interfaces: 12 • URL-filtering: Enabled • Inside Hosts: Unlimited • Throughput: Unlimited • IKE peers: Unlimited

Tabla 3.10: Cuadro comparativo de varios equipos que soportan VPNs.

b) Con Software

Para este análisis se han tomado los tipos de software más conocidos y que cumplan con los requerimientos básicos, en cuanto a la implementación de las VPNs.

Producto	Version	Caracteristicas	Cliente Remoto
Check Point	VPN-1/Firewall-1 SamallOffice	Site-to-site client-to-site Ipsec PPPoE PPTP plataformas windows, linux y mac Licencia	VPN-1 SecureClient
ISA Server	(ISA) Server 2004	Site-to-site client-to-site Ipsec PPTP Plataforma windows Integración con el Directorio Activo Licencia	Cliente Propio de Windows
Ipsec-Tools	ipsec-tools-0.3.3-6	Site-to-site client-to-site Ipsec plataforma LINUX kernel 2.6 Licencia GNU-GPL	Cliente Propio de Windows
Poptop The PPTP Server for Linux	pptpd-1.2.3-1	client-to-site protocolos ppp, pptp, GRE plataforma LINUX kernel 2.6 Licencia GNU-GPL	Cliente Propio de Windows

Tabla 3.11: Cuadro comparativo de varios productos Software que soportan VPN.

La VPN, permitirá disponer de una base de datos actualizada de toda la producción diaria de cada una de las Fincas con la Matriz. Esto se realizará a través de un *Proceso de Replicación Transaccional de Datos (descrito en el literal* 3.1.1.1*),* sin necesidad de un enlace adicional, con lo que se asegura, que la información a trasmitir cumpla con los requerimientos de seguridad como: autenticación, confidencialidad, integridad y disponibilidad.

Para la Interconexión de la red empresarial, se utilizará los accesos a Internet que la empresa posee actualmente, tanto en las Fincas como en la Oficina CENTRALUIO (descrito en el capítulo 2). Por lo que se realizará un análisis de

tráfico para determinar el ancho de banda consumido en cada uno de los accesos.

3.2.1.2.1 Análisis del Tráfico Actual de la Empresa.

La determinación del tráfico actual de la empresa, se realizará con los datos entregados por el programa MRTG (Multi Router Traffic Grapher). Para esto se ha recopilado información durante una semana laboral (de lunes a viernes), para cada Finca y la Matriz.

La interpretación de los gráficos obtenidos con las lecturas del MRTG son: las línea de color negro representa el tráfico saliente, mientras que el área en gris, representa el tráfico entrante, el eje x corresponde al tiempo en horas y el eje y, la tasa de transferencia en bps (bits por segundo).

a) Matriz (OFICINA CENTALUIO)

La determinación del tráfico en la Matriz, se realizó a través de un muestreo durante una semana de trabajo de lunes a viernes, dentro de una jornada laboral (8H00 a 18H00), debido a que en este lapso de tiempo, se tiene mayor intercambio de información de datos desde la red interna hacia el Internet y viceversa. Los resultados de las gráficas obtenidas en estos muestreos se presentan en las figuras y tablas siguientes:

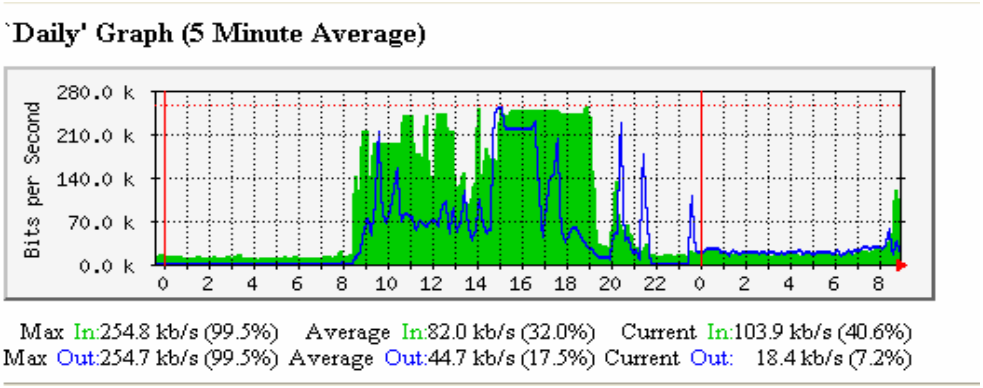

Figura 3m.1: Tráfico del LUNES 07/nov/2005

Horas	Tráf. Entrante (Kbps)	Tráf. Saliente (Kbps)
8:00	10	5
9:00	220	70
10:00	200	70
11:00	245	80
12:00	140	70
13:00	130	90
14:00	250	105
15:00	240	256
16:00	250	220
17:00	250	50
18:00	240	50
Promedio	**197.73**	**96.91**

Tabla 3m.1: Tráfico del LUNES 07/nov/2005

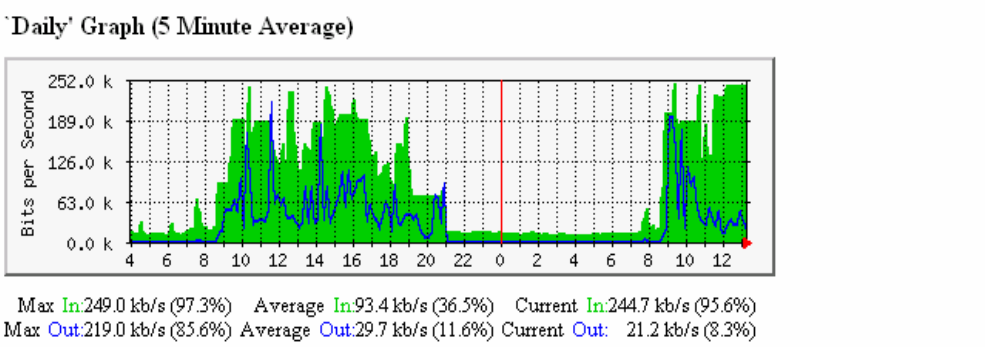

Figura 3m.2: Tráfico del MARTES 08/nov/2005

Horas	Tráf. Entrante (Kbps)	Tráf. Saliente (Kbps)
8:00	25	5
9:00	93	55
10:00	190	175
11:00	190	40
12:00	140	150
13:00	230	30
14:00	190	190
15:00	240	60
16:00	220	70
17:00	138	60
18:00	126	90
Promedio	**162**	**84.09**

Tabla 3m.2: Tráfico del MARTES 08/nov/2005

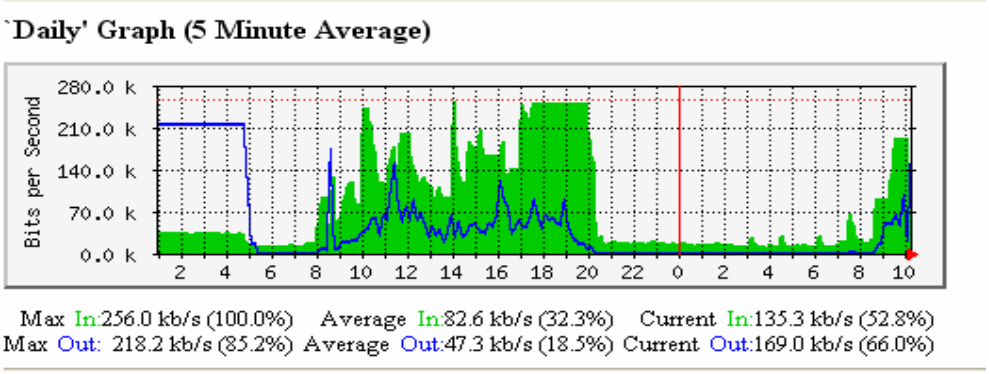

Figura 3m.3: Tráfico del MIERCOLES 09/nov/2005

Horas	Tráf. Entrante (Kbps)	Tráf. Saliente (Kbps)
8:00	100	8
9:00	65	90
10:00	260	40
11:00	170	110
12:00	200	80
13:00	125	50
14:00	256	70
15:00	210	60
16:00	190	130
17:00	256	60
18:00	256	80
Promedio	**189.82**	**70.73**

Tabla 3m.3: Tráfico del MIERCOLES 09/nov/2005

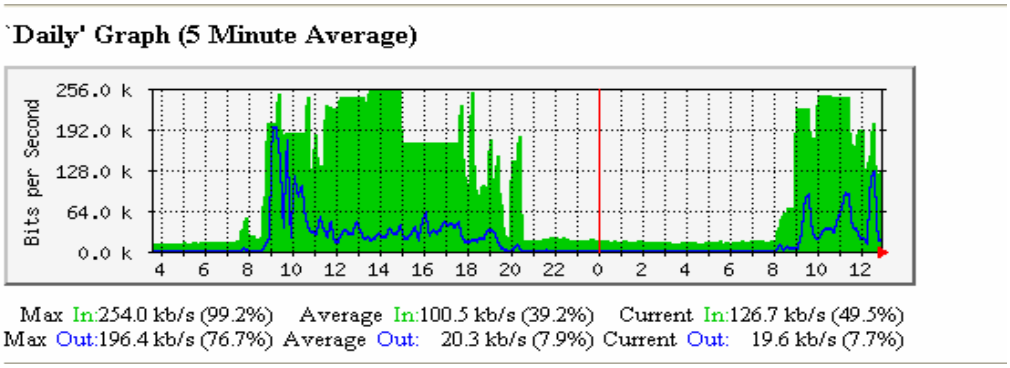

Figura 3m.4: Tráfico del JUEVES 10/nov/2005

Horas	Tráf. Entrante (Kbps)	Tráf. Saliente (Kbps)
8:00	50	5
9:00	220	200
10:00	190	150
11:00	210	45
12:00	240	30
13:00	250	45
14:00	256	40
15:00	256	50
16:00	180	64
17:00	180	50
18:00	250	30
Promedio	**207.45**	**64.45**

Tabla 3m.4: Tráfico del JUEVES 10/nov/2005

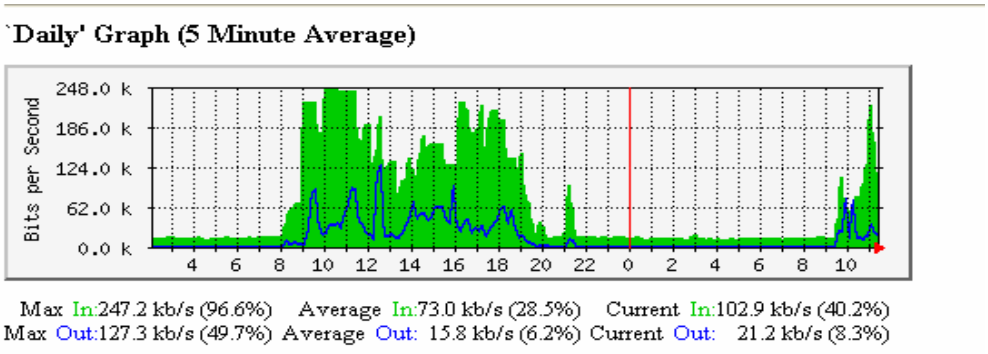

Figura 3m.5: Tráfico del VIERNES 11/nov/2005

Horas	Tráf. Entrante (Kbps)	Tráf. Saliente (Kbps)
8:00	10	5
9:00	230	5
10:00	248	60
11:00	245	95
12:00	190	25
13:00	150	70
14:00	140	65
15:00	160	62
16:00	235	95
17:00	230	30
18:00	225	62
Promedio	**187.55**	**52.18**

Tabla 3m.5: Tráfico del VIERNES 11/nov/2005.

La siguiente tabla muestra el promedio total para la Matriz (CentralUIO)

Dia	Tráf. Entrante (Kbps)	Tráf. Saliente (Kbps)
LUNES 07/11/05	197.73	96.91
MARTES 08/11/05	162.00	84.09
MIERCOLES 09/11/05	189.82	70.73
JUEVES 10/11/05	207.45	64.45
VIERNES 11/11/05	187.55	52.18
Promedio	**188.91**	**73.67**

Tabla 3m.6: Tráfico promedio semanal (Matriz)

b) Finca 1

La determinación del tráfico en la FINCA1, se ha realizado a través de un muestreo durante una semana de trabajo de lunes a viernes, dentro de una jornada laboral (8H00 a 18H00), debido a que en este lapso de tiempo, se tiene mayor intercambio de información de datos desde la red interna hacia el Internet

y viceversa. Los resultados de las gráficas obtenidas en estos muestreos se presentan en las figuras y tablas siguientes:

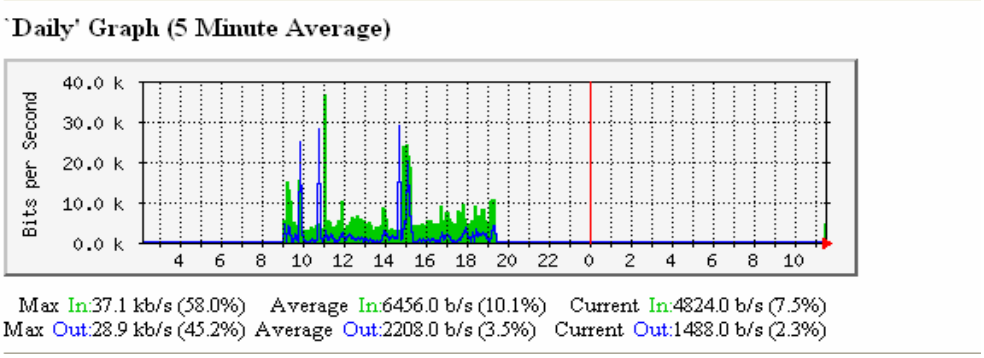

Figura 3f1.1: Tráfico del LUNES 07/nov/2005.

Horas	Tráf. Entrante (Kbps)	Tráf. Saliente (Kbps)
8:00	2	2
9:00	15	4
10:00	15	26
11:00	38	28
12:00	10	11
13:00	5	5
14:00	8	8
15:00	24	25
16:00	5	3
17:00	8	8
18:00	10	4
Promedio	**12.73**	**1.27**

Tabla 3f1.1: Tráfico del Lunes 07/nov/2005

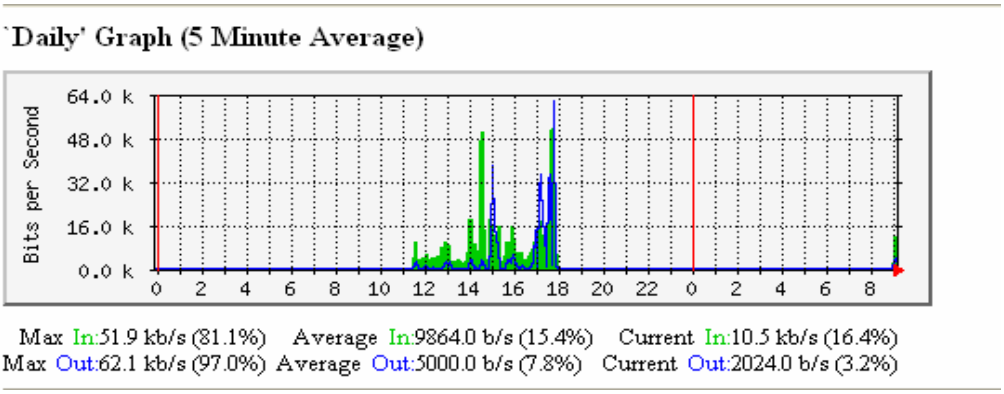

Figura 3f1.2: Tráfico del MARTES 08/nov/2005

Horas	Tráf. Entrante (Kbps)	Tráf. Saliente (Kbps)
8:00	2	2
9:00	2	2
10:00	2	2
11:00	2	2
12:00	7	3
13:00	9	4
14:00	18	4
15:00	33	40
16:00	16	5
17:00	16	36
18:00	50	62
Promedio	**14.27**	**14.73**

Tabla 3f1.2: Tráfico del MARTES 08/nov/2005

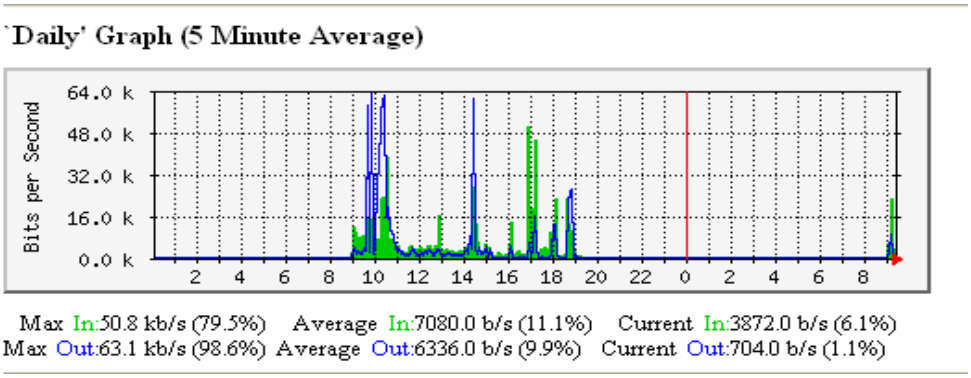

Figura 3f1.3: Tráfico del MIERCOLES 09/nov/2005

Horas	Tráf. Entrante (Kbps)	Tráf. Saliente (Kbps)
8:00	2	2
9:00	14	6
10:00	26	64
11:00	21	8
12:00	4	6
13:00	16	6
14:00	15	62
15:00	4	6
16:00	14	6
17:00	50	17
18:00	25	15
Promedio	**17.36**	**18.00**

Tabla 3f1.3: Tráfico del MIERCOLES 09/nov/2005

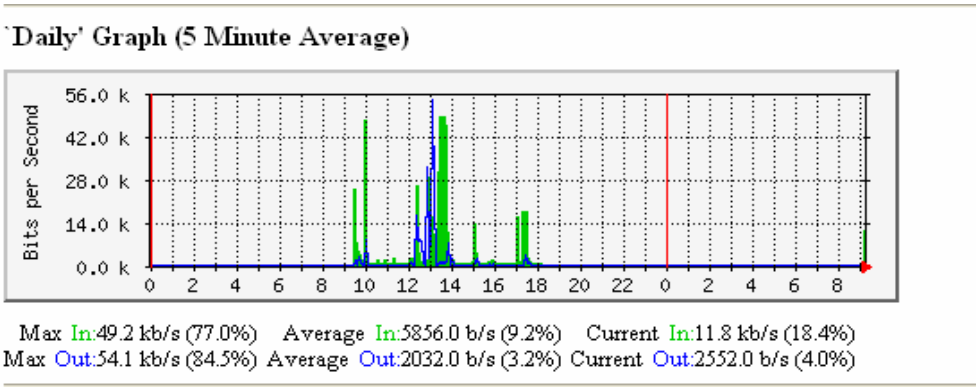

Figura 3f1.4: Tráfico del JUEVES 10/nov/2005.

Horas	Tráf. Entrante (Kbps)	Tráf. Saliente (Kbps)
8:00	2	2
9:00	2	2
10:00	48	10
11:00	3	3
12:00	15	16
13:00	30	55
14:00	50	7
15:00	15	5
16:00	3	3
17:00	17	3
18:00	2	3
Promedio	**17.00**	**9.91**

Tabla 3f1.4: Tráfico del JUEVES 10/nov/2005

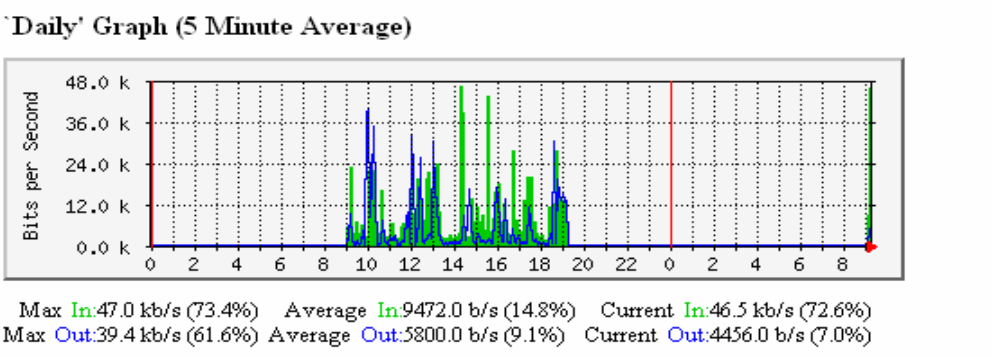

Figura 3f1.5: Tráfico del VIERNES 11/nov/2005

Horas	Tráf. Entrante (Kbps)	Tráf. Saliente (Kbps)
8:00	2	2
9:00	24	10
10:00	24	40
11:00	7	5
12:00	24	30
13:00	24	28
14:00	48	5
15:00	13	18
16:00	28	19
17:00	30	5
18:00	5	13
Promedio	**20.82**	**15.91**

Tabla 3f1.5: Tráfico del VIERNES 11/nov/2005

En la siguiente tabla se muestra el promedio semanal de Tráfico para la FINCA1.

DIA	Tráf. Entrante (Kbps)	Tráf. Saliente (Kbps)
LUNES 07/11/05	12.73	11.27
MARTES 08/11/05	14.27	14.73
MIERCOLES 09/11/05	17.36	18.00
JUEVES 10/11/05	17.00	9.91
VIERNES 11/11/05	20.82	15.91
Promedio	**16.44**	**13.96**

Tabla 3f1.6: Tráfico promedio semanal (Finca 1).

c) Finca 2

La determinación del tráfico en la FINCA2, se ha realizado a través de un muestreo durante una semana de trabajo de lunes a viernes, dentro de una jornada laboral (8H00 a 18H00), debido a que en este lapso de tiempo, se tiene mayor intercambio de información de datos desde la red interna hacia el Internet

y viceversa. Los resultados de las gráficas obtenidas en estos muestreos se presentan en las figuras y tablas:

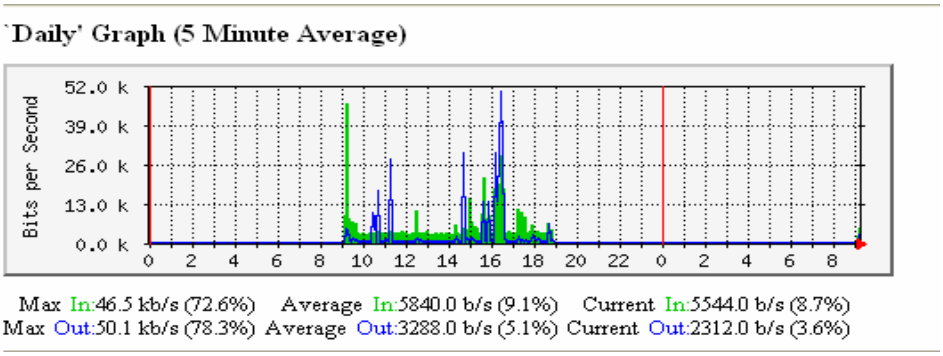

Figura 3f2.1: Tráfico del LUNES 07/nov/2005.

Horas	Tráf. Entrante (Kbps)	Tráf. Saliente (Kbps)
8:00	2	2
9:00	48	5
10:00	5	3
11:00	5	28
12:00	5	3
13:00	6	3
14:00	6	3
15:00	16	30
16:00	23	48
17:00	10	5
18:00	6	5
Promedio	**12.00**	**12.27**

Tabla 3f2.1: Tráfico del LUNES 07/nov/2005

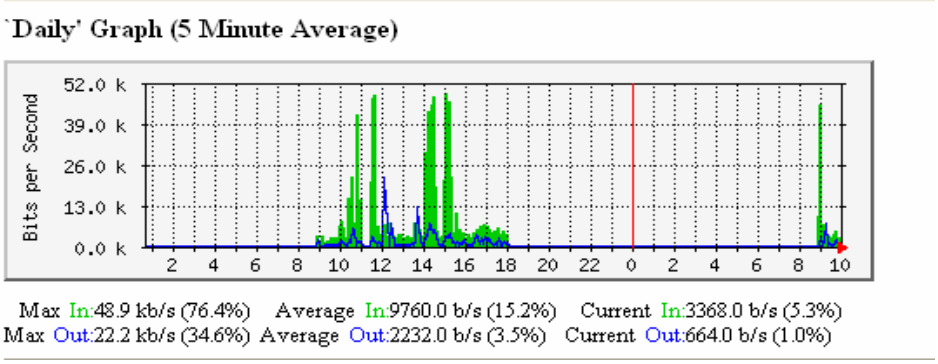

Figura 3f2.2: Tráfico del MARTES 08/nov/2005

Horas	Tráf. Entrante (Kbps)	Tráf. Saliente (Kbps)
8:00	2	2
9:00	4	4
10:00	10	5
11:00	44	8
12:00	50	24
13:00	6	3
14:00	43	6
15:00	50	5
16:00	6	3
17:00	9	5
18:00	6	3
Promedio	**20.91**	**6.18**

Tabla 3f2.2: Tráfico del MARTES 08/nov/2005

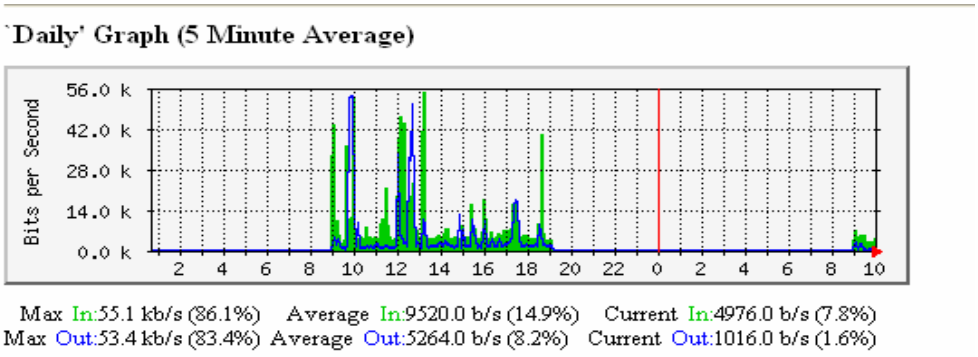

Figura 3f2.3: Tráfico del MIERCOLES 09/nov/2005

Horas	Tráf. Entrante (Kbps)	Tráf. Saliente (Kbps)
8:00	2	2
9:00	45	6
10:00	36	54
11:00	11	5
12:00	48	38
13:00	56	12
14:00	8	5
15:00	13	14
16:00	18	12
17:00	8	14
18:00	8	5
Promedio	**23.00**	**15.18**

Tabla 3f2.3: Tráfico del MIERCOLES 09/nov/2005

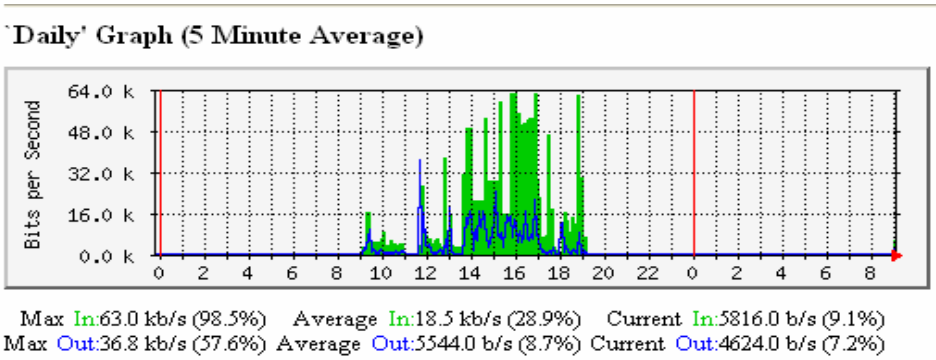

Figura 3f2.4: Tráfico del JUEVES 10/nov/2005

Horas	Tráf. Entrante (Kbps)	Tráf. Saliente (Kbps)
8:00	2	2
9:00	16	8
10:00	8	5
11:00	5	3
12:00	30	38
13:00	40	19
14:00	50	19
15:00	35	26
16:00	64	16
17:00	64	18
18:00	16	14
Promedio	**30.00**	**15.27**

Tabla 3f2.4: Tráfico del JUEVES 10/nov/2005

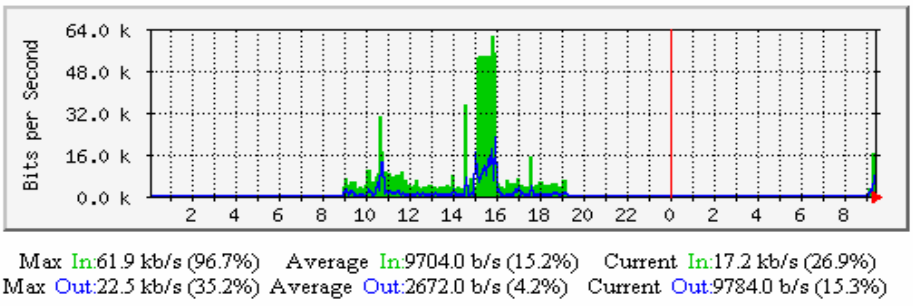

Figura 3f2.5: Tráfico del VIERNES 11/nov/2005

Horas	Tráf. Entrante (Kbps)	Tráf. Saliente (Kbps)
8:00	2	2
9:00	7	5
10:00	9	5
11:00	21	10
12:00	7	3
13:00	4	3
14:00	6	3
15:00	56	18
16:00	61	26
17:00	5	5
18:00	8	5
Promedio	**16,91**	**7,73**

Tabla 3f2.5: Tráfico del VIERNES 11/nov/2005

En la siguiente tabla se muestra el promedio total semanal para la FINCA 2.

DIA	Tráf. Entrante (Kbps)	Tráf. Saliente (Kbps)
LUNES 07/11/05	12.00	12.27
MARTES 08/11/05	20.91	6.18
MIERCOLES 09/11/05	23.00	15.18
JUEVES 10/11/05	30.00	15.27
VIERNES 11/11/05	16.91	7.73
Promedio	**20.56**	**11.33**

Tabla 3f2.6: Tráfico promedio semanal.

Promedio global de la empresa.

SITIO	Tráf. Entrante (Kbps)	Tráf. Saliente (Kbps)
CENTRALUIO	188.91	73.67
FINCA 1	16.44	13.96
FINCA 2	20,56	11,33

Tabla 3.12: Tráfico promedio global

3.2.1.2.2 Determinación del Ancho de Banda para la VPN

Para este apartado se tomará en consideración lo analizado en la parte 3.2.1.1.1 literal (*a)* del presente proyecto. Así se tiene:

a) Cálculo de la capacidad requerida para FINCA1

Se toma un margen de tolerancia del 15% debido al overhead producido por el encapsulamiento que sufren los datos al momento de ingresar al túnel VPN.

T FINCA1 = 38.67Kbps + 15% (overhead[9] VPN)
T FINCA1 = 44.47Kbps.

Este resultado se suma con el promedio obtenido del tráfico saliente de la finca debido a que el sentido de la replicación es de las fincas a la matriz.

T FINCA1 = 44.47Kbps + 13.96Kbps
T FINCA1 = 58.43Kbps.

[9] **Overhead:** Información que se agregan a los datos que se van a transmitir, permitiendo el control de: errores, direccionamiento, etc.

b) Cálculo de la capacidad requerida FINCA2

Para el cálculo del ancho de banda de la FINCA2 se procede de forma similar que la descrita en la FINCA1, resumida a continuación:
T FINCA2 = 26.67Kbps + 15% (overhead VPN)
T FINCA2 = 30.67Kbps.

Este resultado se suma con el promedio obtenido del tráfico saliente de la finca debido a que el sentido de la replicación es de las fincas a la matriz.

T FINCA2 = 30.67Kbps + 11.33Kbps
T FINCA2 = 42.00Kbps.

c) Cálculo de la capacidad requerida CENTRALUIO

Como hacia la matriz convergen los tráficos de las fincas, se debe tomar en cuenta el tráfico entrante a la misma, para realizar el cálculo total del ancho requerido.
TCENTRALUIO = TFINCA1 + TFINCA2 + TEntrante Matriz.
TCENTRALUIO = 58.43Kbps + 42.00Kbps + 188.91Kbps.
TCENTRALUIO = 289.34Kbps.

En la siguiente tabla se muestra la capacidad de ancho de banda en Internet requerida para la interconexión VPN. Se debe recalcar que la conexión a Internet de las fincas, es asimétrica, por lo que el ancho de banda utilizado por la replicación, será el de 64 Kbps, que es canal de salida.

Sitio	Capacidad Requerida (Kbps)	Capacidad Actual (Kbps)
CENTRALUIO	289.34	512
FINCA1	58.43	128 ↓ / 64 ↑
FINCA2	42.00	128 ↓ / 64 ↑

Tabla 3.13: Capacidad requerida para la VPN

Como se muestra en la tabla 3.13, la capacidad requerida es menor a la que se tiene actualmente disponible, pero es recomendable aumentar 32 Kbps en las fincas, debido a que no se ha considerado para el cálculo, el crecimiento de la empresa para los siguientes años, con lo que aumentaría el tráfico en los accesos a Internet. No así, en la matriz, que posee un acceso a Internet con un margen aceptable.

3.3 ANALISIS COSTO / BENEFICIO

3.3.1 COSTOS

El propósito de este análisis es detallar los costos que la empresa tiene actualmente en los sistemas de comunicaciones (Acceso a Internet) y los costos que debería invertir para interconectar las fincas con la oficina central.

3.3.1.1 Costos Actuales

Se detallan en la siguiente tabla los costos de los enlaces a Internet que actualmente la empresa posee.

SITIO	Velocidad de Transmisión	Tipo de Enlace	Costo Mensual del Servicio de Internet (USD)
CENTRALUIO	512	Local	**1400**
FINCA1	128/64	Satelital	**700**
FINCA2	128/64	Satelital	**700**

Tabla 3.14: Costos actuales de Internet.

3.3.1.2 Costos Utilizando Enlaces Dedicados

Se han cotizado dos posibles formas de enlazar la matriz CENTRALUIO con las FINCAS; la primera, con un enlace satelital Dataplus (Proforma proporcionada por Impsatel del Ecuador) y la segunda un radio enlace (Spread Spectrum) con repetidoras, el mismo que pertenecerá y será administrado por la empresa florícola (Equipos proporcionado por High-Telecom). Estas cotizaciones se muestran al final de este documento, en el Anexo C.

El valor que debería pagar la empresa por los enlaces será:

SITIO	Velocidad de Tx [Kbps]	Tipo de Enlace	Costo Mensual del Enlace [USD]	Costo Instalación y Configuración [USD]
Telepuerto - Centraluio	128	local	235	350
Telepuerto - Finca1	64	Satelital	1795	1200
Telepuerto - Finca2	64	Satelital	1795	1200
TOTAL			**3825**	**2750**

Tabla 3.15: Costos enlace dedicado (Satelital)

SITIO	Velocidad de Tx [GHz]	Tipo de Enlace	Costo del Enlace [USD]	Costo Instalación y Configuración [USD]
Centraluio - Finca1	5.8	Spread Spectrum	11466.13	2880
Centraluio - Finca2	5.8	Spread Spectrum	25727.35	
TOTAL			**37193.48**	**2880**

Tabla 3.16: Costos del radio enlace (Spread Spectrum).

3.3.1.3 Costos Utilizando la VPN a Través de Internet

a) Con Hardware

Los costos por hardware, están directamente enfocados a la implementación de las VPNs con routers. En el Anexo C, se adjuntan cotizaciones de routers. Se debe indicar que todos estos costos no incluyen el IVA.

PRODUCTO	PRECIO (USD)		COSTO IMPLEMENTACION		TOTAL
Routers (HW)	P. UNITARIO	P. TOTAL	COSTO POR SITIO (USD)	COSTO TOTAL (USD)	
Cisco 1601/1750	1365	4095	200	600	**4695**
3COM 3015	1010	3030	200	600	**3630**
D-link (DI-804 HV)	100	300	200	600	**900**
SonicWall	500	1500	200	600	**2100**

Tabla 3.17: Precios de VPN con hardware.

b) Con software

Para el análisis de costos de la implementación de la VPN con software (SW) se toma en cuenta, el tipo de software a implementar, el valor de las licencias y el costo por los servicios técnicos de la implementación. Tal como se ilustra en la siguiente tabla.

PRODUCTO	PRECIO	COSTO IMPLEMENTACION		TOTAL
(SW)	(USD)	COSTO POR SITIO (USD)	COSTO TOTAL (USD)	
Check Point	2500	200	600	**3100**
ISA Server	3500	200	600	**4100**
Ipsec-Tools	0	200	600	**600**

Tabla 3.18: Precios de VPN con software.

3.3.2 COSTO/BENEFICIOS

Para este análisis no se tomarán los costos por acceso a Internet ya que es un gasto que la empresa ya tiene, mas bien se analizarán los costos en los que debería incurrir la empresa para mantener interconectadas las fincas por medio de un enlace dedicado o enlace VPN (hardware y software) sobre Internet, se analizarán cada una de estas alternativas con los ventajas, desventajas y costos que estos implican desde un punto de vista económico y funcional, de esta forma se podrá estimar el impacto financiero del proyecto.

Para esto es importante considerar que muchos beneficios no se pueden cuantificar pero son resultado de la implementación del proyecto; como: la moral de los empleados, la seguridad, la satisfacción del cliente, fluidez en los procesos de producción, etc.

En la siguiente tabla se muestra un resumen de costos para las alternativas analizadas anteriormente.

ALTERNATIVAS	INSTALACION	MENSUALIDAD
Enlace Dedicado		
IMPSAT	2750	3825
HIGH TELECOM	40073,48	Arriendo repetidor
VPN-HARDWARE		
Cisco 1601 / 1750	4695	0
3COM 3015	3630	0
D-link (DI-804 HV)	900	0
SonicWall	2100	0
VPN-SOFTWARE		
Check Point	3100	0
ISA Server	4100	0
Ipsec-Tools	600	0

Tabla 3.19: Resumen de costos de las alternativas.

De la tabla anterior se desprende las siguientes observaciones:

- En los enlaces dedicados se tomaron en cuenta dos opciones; la primera, es el arrendamiento de un canal satelital dedicado a una empresa proveedora de servicios (IMPSAT), cuyo costo inicial es $6575, en el cual se incluyen la instalación y la primera mensualidad. Los beneficios que se pueden obtener con este tipo de interconexión es ahorros en infraestructura de comunicaciones, tiempo de instalación cortos y fácil acceso a sitios remotos.

  La segunda es la implantación de un sistema de comunicaciones propio para la empresa, por un valor de $40073,48 aquí se incluye los radios, antenas y demás accesorios necesarios para el enlace, este equipamiento será provistos por la empresa HIGH-TELECOM, mientras que la infraestructura civil (torres, tomas reguladas y polarizadas, canaletas, pararrayos, arriendo de repetidora) será provista por la florícola. Un beneficio importante en este tipo de enlaces es que la empresa administrará sus enlaces y el ancho de banda de acuerdo a sus necesidades. Mientras que si algún equipo se daña o por alguna razón el enlace no funciona la empresa corre con todos los gastos para repararlo.

- En la alternativa de interconexión mediante enlaces VPN con hardware y software se tiene una gran variedad de productos para elegir en el mercado, los más utilizados y funcionales se listan en esta propuesta (Cisco, 3COM, D-Link, SonicWall), sin embargo se puede aprovechar la infraestructura existente en la empresa, es así; que se pueden utilizar los servidores Linux para levantar el túnel VPN. La empresa invertirá únicamente en la mano de obra que son $600 obteniendo con esto, un enlace seguro y confiable, siendo ésta la mejor alternativa a analizar.

  En la siguiente tabla se muestra una comparación entre las diferentes alternativas:

ALTERNATIVAS	Costo total	Características Básicas
Enlace Dedicado *Imsat*	Mediano	Fácil acceso remoto, poca infraestructura, tiempos de implementación bajos, pago mensual por el servicio, tiempos de retardo en TX medianos
High-Telecom	Muy Alto	Difícil acceso remoto, compleja infraestructura, tiempos de implementación altos, arriendo repetidor, no hay arriendo mensual (equipos comprados),
VPN-HARDWARE ***Cisco 1601 / 1750***	Mediano alto	Arquitectura robusta y estable, compleja implementación altos niveles de seguridad,
3COM 3015	Mediano	Arquitectura robusta y estable, compleja implementación altos niveles de seguridad,
D-link (DI-804 HV)	Bajo	Arquitectura no robusta, fácil implementación bajos niveles de seguridad,
SonicWall	Mediano bajo	Arquitectura no robusta, fácil implementación medianos niveles de seguridad,
VPN-SOFTWARE ***Check Point***	Mediano	Software robusto y estable, compleja implementación altos niveles de seguridad y fiabilidad, independencia de plataforma
ISA Server	Mediano	Software robusto y estable, compleja implementación altos niveles de seguridad y fiabilidad, Solo Plataforma Microsoft
Ipsec-Tools	Bajo	Software robusto y estable, mediana complejidad de implementación altos niveles de seguridad, independencia de plataforma

Tabla 3.20: Resumen de los beneficios de las alternativas.

CAPITULO 4

4. ANALISIS E IMPLEMENTACION DE UNA VPN.

Las redes privadas virtuales VPNs, ofrecen una buena alternativa de interconexión a los usuarios remotos de cada una de las Fincas, los cuales podrán acceder a los recursos que ofrece la red de la Oficina CENTRALUIO y viceversa, tal como si estuvieran conectados directamente a la red LAN de estas oficinas, mediante el uso de infraestructura pública como lo es el Internet.

El propósito de este capitulo es el análisis de VPNs, para la red corporativa de una empresa Florícola, base de estudio del presente proyecto, para lo cual se presentan dos escenarios de uso de una VPN: a) La conexión de un usuario remoto a la red corporativa y b) La conexión de una red remota a la red corporativa. Tal como muestra la siguiente figura.

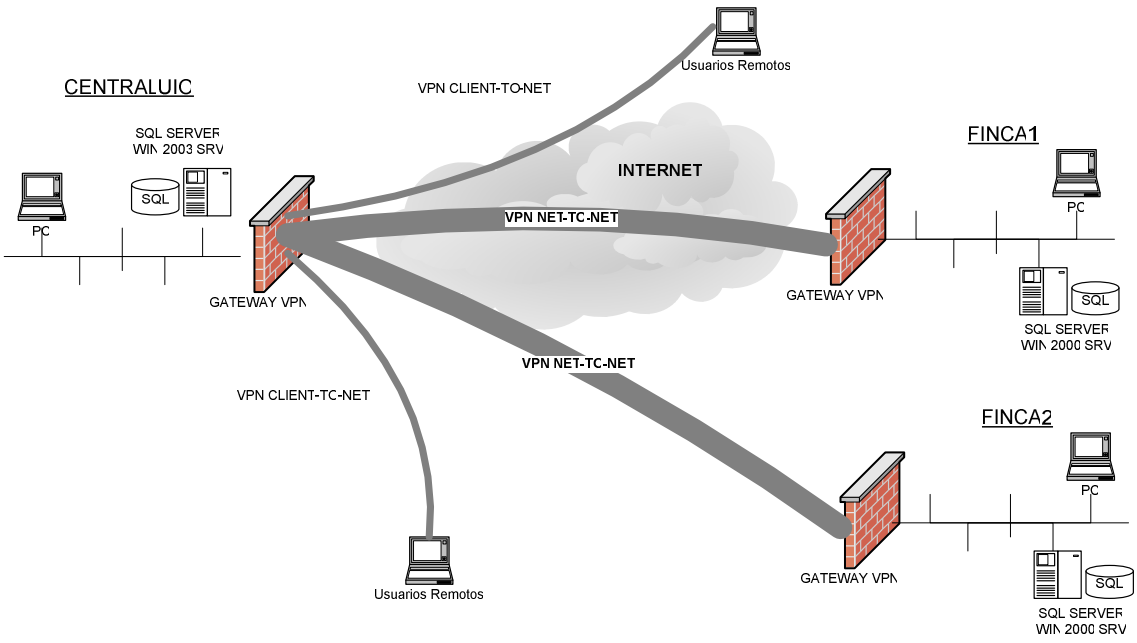

Figura 4.1: Conjunto de redes y conexiones de la VPN

Los protocolos y métodos de acceso, así como la tecnología utilizada se analizarán en los siguientes párrafos. Con esta información, se dará inicio al

diseño de la VPN y la implementación de un prototipo, luego se pondrá en funcionamiento un aplicativo útil para la empresa, que permitirá tener la información de sus fincas actualizadas y en línea, a través de la replicación de base de datos, tal como se analizó en el capítulo 3, demostrando con esto los beneficios y ventajas de las conexiones VPNs.

Finalmente se analizarán las metodologías de seguridad en VPNs y se implementarán en el prototipo, una de estas, para garantizar la integridad, autenticidad y confidencialidad en la transmisión de la información a través de la VPN.

4.1 DESCRIPCION Y SELECCION DE LA ARQUITECTURA

Para proceder con la selección de la arquitectura se analizaron las tecnologías disponibles en el mercado informático, tomando en consideración las tablas 3.10 y 3.11 del capítulo 3, en las que muestran la comparación de diferentes tecnologías de hardware y software respectivamente, llegando a las siguientes conclusiones:

- A pesar que la marca CISCO, con sus productos más usados; routers, firewallpix, ofrece una buena alternativa de gateway para VPN, su costo hace que no sea factible la implementación para el prototipo.

- Existen otras marcas de Routers (D-Link, SonicWall) que tiene las mismas funcionalidades básicas de los routers CISCO, y sus precios son relativamente bajos, es por esto que se usará el router D-Link DI 804-HV, cuyas propiedades se describirán más adelante.

- IPSec actúa en la capa de red, protegiendo los paquetes IP entre los gateways VPNs. Además posibilita las siguientes características:

- ***Confidencialidad de datos***. El emisor IPSec puede cifrar paquetes antes de transmitirlos por la red.

- ***Integridad de datos.*** El receptor IPSec puede autenticar paquetes enviados por el emisor IPSec, para garantizar que los datos no han sido alterados durante la transmisión.

- ***Autenticación de origen de datos.*** El receptor IPSec puede autenticar el origen de los paquetes IPSec enviados. Este servicio depende del servicio de integridad de datos.

- ***Antireproducción.*** El receptor puede detectar y rechazar paquetes reproducidos.

A pesar que otras tecnologías de autenticación y cifrado para enlaces VPNs también disponen de estas características, IPSec es un protocolo que viene por defecto en IPV6 y además es nativo del kernel 2.6.9-11.EL de Linux White Box 4.0 instalado en los proxys de las fincas y oficina central, esto hace que sea el protocolo elegido para el diseño de la VPN corporativa y la implementación del prototipo.

- Linux proporciona una serie de ventajas imbatibles, frente a otros sistemas operativos que tienen una política de licenciamiento enormemente restrictiva como lo es Microsoft (licencia por cantidad de conexiones, por cantidad de usuarios, por tipo de servicio o aplicativo, etc.). La implementación de un servidor Linux no tiene límite en cuanto a número de clientes conectados, ni cantidad de usuarios, así como también en el número de servidores en los que se puede instalar.
- *Ipsec con Linux*, ofrece una buena alternativa de interconexión puesto que se pueden utilizar los dispositivos disponibles en la red empresarial, como los proxys. La implementación de VPNs representa una alternativa rentable para conectar todas las redes remotas de una manera segura y económica.

- En cuanto al medio de transmisión, el Internet es la mejor opción debido a que las fincas y la oficina central ya cuentan con un acceso, en contraposición con un enlace dedicado, que demandaría de obras civiles para su instalación como lozas superficiales, mástiles, tomas eléctricas, puntos de red adicionales, costo de instalación y pago mensual del servicio.

- A más de utilizar el servidor Linux como gateway Ipsec, se pueden implementar varios servicios como filtro de páginas indeseables (pornográficas, violentas, y aquellas que no tengan nada que ver con el trabajo de cada usuario), scan de virus en páginas web visitadas, firewall, DNS, Proxy, etc.

- El router DLINK DI 804-HV, es un equipo diseñado para soportar hasta 40 túneles VPN, soporta IPSec. La seguridad del canal está implementada a través de claves compartidas. Para el presente proyecto se hará uso de dos túneles VPN, y para el prototipo solo se utilizará uno, por lo que este equipo se ajusta a las necesidades de esta implementación.

Debido a que no se quiere dar preferencia a un determinado producto para diseñar e implementar la VPN, se considera necesario presentar dos opciones, la primera con software IPSec-Linux y las segunda con hardware (router VPN DLINK DI 804-HV) cada una de estas opciones con sus respectivas ventajas mencionadas anteriormente.

4.2 ANALISIS E IMPLEMENTACIÓN DE LA RED PRIVADA VIRTUAL (VPN).

4.2.1 ANÁLISIS DE LA RED PRIVADA VIRTUAL (VPN)

Los requerimientos de la empresa son conectar, a través de Internet el servidor de base de datos de la Matriz, con los servidores de las Fincas y replicar la

información desde cada uno de estos sitios hacia oficina central, lo que permitirá disponer de una base de datos actualizada con la producción diaria de la empresa. De esta manera, las características del nuevo esquema de red quedarían como se detalla a continuación:

- El tráfico generado por la replicación de base de datos desde las fincas debe protegerse.

- El soporte IPSec únicamente llegará hasta los limites de la red interna, es decir hasta los gateway Linux o routers VPN DLINK.

- Las direcciones IP para el uso en las redes internas o privadas de la empresa florícola serán tomadas de un espacio de direcciones privado. Solo las interfaces de los gateways que se unen al backbone de la red pública requerirán de direcciones IP públicas.

- Para el dimensionamiento de la velocidad de transmisión, (Ancho de Banda-BW) se tomarán como base las tablas 3.12 y 3.13 del capitulo 3.

4.2.1.1 Plan de Direccionamiento IP

Para el direccionamiento de la parte pública, es el ISP quien asigna las IPs, es por esta razón que se tienen tres direcciones públicas, en este proyecto se usará para la Matriz (CENTRALUIO) la IP 200.92.23.25/255.255.255.248, siendo ésta de clase C.

El espacio de direccionamiento para la Matriz CENTRALUIO y de las FINCAS va a ser del tipo clase C, y con máscara de 255.255.255.0, dando una capacidad total de 254 máquinas, que para el caso de la Matriz, es más que suficiente, ya que tiene 36 estaciones de trabajo. De igual manera se hace una consideración para las Fincas, ya que éstas tienen 23 estaciones de trabajo al momento y esto

permite tener una reserva suficiente para un crecimiento futuro de toda la Florícola.

El espacio de direccionamiento para los tres sitios se resume en la siguiente tabla:

RED	LUGAR	SITIO	RED
WAN	Tabacundo (Norte Pichincha)	FINCA1	192.45.18.10 /24
	Mulaló (Cotopaxi)	FINCA2	192.45.18.12/24
	Matriz Quito	CENTRALUO	200.92.23.25/24
LAN	Tabacundo (Norte Pichincha)	FINCA1	192.168.1.0/24
	Mulaló (Cotopaxi)	FINCA2	192.168.2.0/24
	Matriz Quito	CENTRALUO	192.168.0.0/24

Tabla 4.1: Direcciones IP asignadas a la Red de Florícola

La configuración del direccionamiento de la red a ser implementada en la florícola, se representa en el siguiente esquema.

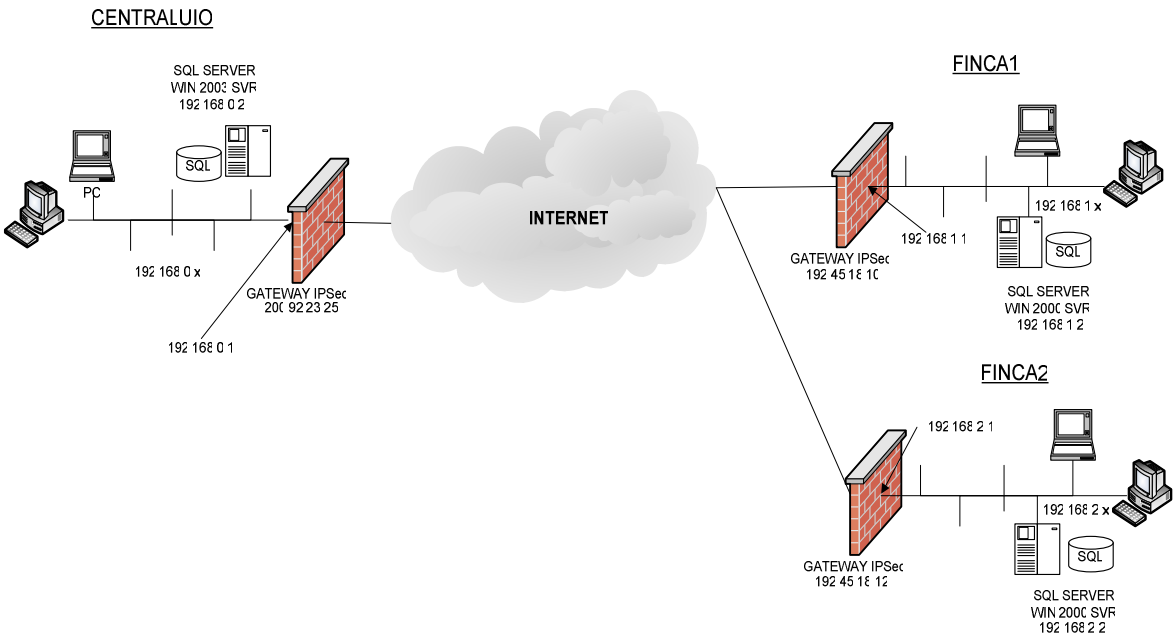

Figura 4.2: Esquema de configuración de red.

4.2.1.2 Alternativas para la Implementación de la VPN

En este proyecto se presentan dos alternativas para al implementación de la VPN. a) La primera de ellas consiste en una solución basada en software, utilizando tres computadoras de mediana capacidad corriendo bajo el sistema operativo Linux White Box 4.0 con kernel 2.6.9-11.EL, b) La segunda en cambio, utiliza tres routers D-LINK DI 804-HV. Las configuraciones de estas dos alternativas, que serán esquematizadas con detalle en el prototipo. Las características básicas de los equipos utilizados para la implementación de cada una de las alternativas son:

a) VPN con Software (Gateway IPSec bajo Linux)

El sistema operativo Linux fue creado en el inicio de la década de los 90's por el finlandés Linux Torvalds, como una implementación complementaria y con independencia del kernel Unix, adoptando las características de multitarea, multiusuario, multiplataforma, capacidad de gestión de redes y soporte para distintos sistemas de archivos de dicho sistema operativo.

Desde su creación, Linux ha sido perfeccionado continuamente, lo que le ha permitido ganar un importante espacio dentro del campo de las telecomunicaciones e Internet, debido principalmente a su gran estabilidad y a su distribución gratuita.

Viene incorporada una gran cantidad de funciones que generalmente no vienen incluidas con otros sistemas operativos. Por ejemplo: e-mail, firewall, NAT, Proxy, VPN's, entre otras; mientras que en sistemas propietarios, para implementar los servicios mencionadas anteriormente, se necesita adquirir paquetes adicionales como: Exchange Server (e-mail), ISA Server, Check Point, etc; los cuales tienen un valor por licencias, por tanto Linux a demás de tener ventajas técnicas, también tiene ventajas económicas.

La función principal de un gateway IPSec es la interconexión de una red pública no confiable con una red privada confiable, por lo tanto el gateway IPSec tendrá dos interfaces de red, una hacia el Internet y la segunda hacia la red privada.

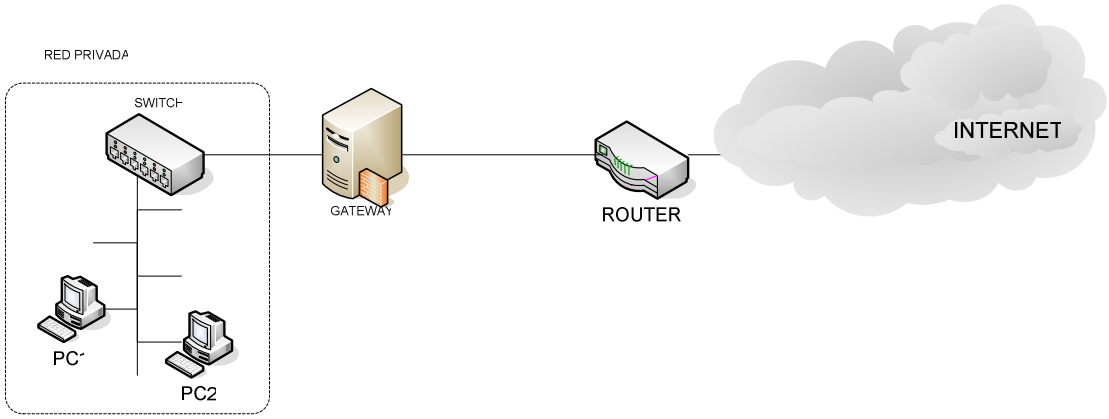

Figura 4.3: Diagrama de interconexión con un gateway

La asignación de direcciones IP para las redes de las fincas y oficina central, se basa en el RFC 1918, es decir son IP's privadas, entonces si alguna máquina necesita acceder a Internet, deberá utilizar una dirección publica, que le permita sin conflictos, comunicarse. Esto se logra por medio del enmascaramiento IP, lo que permite que las máquinas de la red interna que no tienen direcciones públicas, puedan tener acceso al Internet mediante la interfaz pública del gateway.

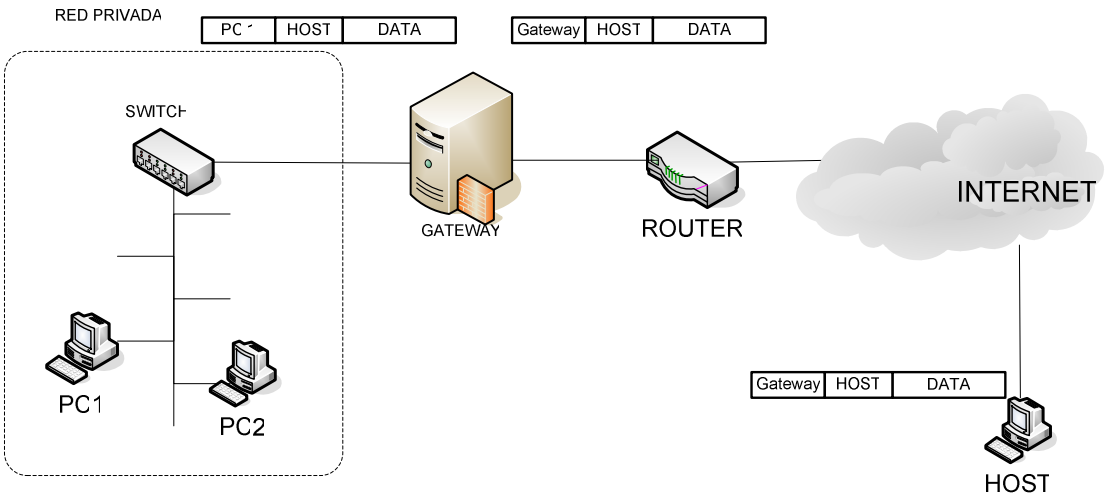

Figura 4.4: Diagrama de Enmascaramiento IP.

La combinación del enmascaramiento IP con un sistema de firewall permite generar un entorno de red seguro y confiable, de manera que sea posible disminuir los riesgos de potenciales ataques a la red interna y a la vez administrar y auditar el tráfico entrante y saliente de la red privada. Mediante la utilización del servidor Linux, se puede implementar un firewall de filtrado de paquetes, el cual se configura mediante la herramienta *"iptables".*

El software necesario para el enmascaramiento VPN se puede encontrar en las versiones del kernel de Linux 2.6 o superiores.

Ipsec-tools: Permite implementar el conjunto de protocolos IPSec. Puede trabajar en modo túnel o transporte. Soporta varios tipos de encriptación y autenticación. El intercambio de llaves puede ser de tipo manual o automático. Para este ultimo, se utiliza la función ***racoon***. Con este servidor se pueden establecer conexiones IPSec, con difusión automática de claves. *Racoon* permite emplear autenticación basada en claves compartidas con anterioridad, certificados X.509 y Kerberos. El servidor puede usarse en modo principal, modo agresivo y modo base, en fase uno de IKE.

La configuración de *racoon* se encuentra en el directorio /etc/racoon. Aquí encontramos archivos como racoon.conf, psk.txt, el directorio certs, en donde se guardan las llaves públicas, privadas y certificados X509. A continuación un diagrama de red con esta alternativa.

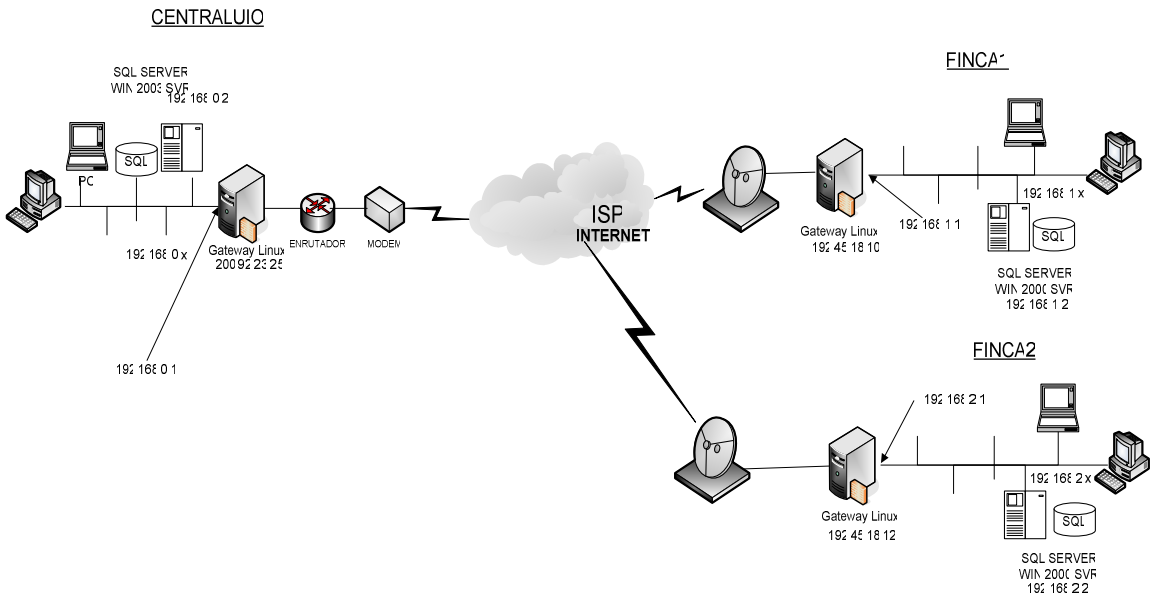

Figura 4.5: Diagrama de red con Gateway Linux.

b) VPN con hardware (DLINK DI 804-HV)

El DLINK DI 804-HV es un router con capacidad de manejar hasta 40 conexiones VPN, debido a que la encriptación y autenticación se la maneja a nivel de circuitos integrados. El procesamiento es más rápido y el rendimiento mejora con respecto a las VPN's implementadas con software.

Las principales características del equipo son:

- IPSec (40 IPSec Tunnels).
- IP Authentication Header (AH).
- IP Encapsulating Security Payload (ESP).
- Internet Key Exchange (IKE).
- Autentication (MD5 / SHA-1).
- NULL/DES/3DES Algoritmos de encriptación utilizados con IPSec.
- Main and Aggressive mode.

Figura 4.6: Equipo DLINK DI 804-HV

La forma en que establece el uso del equipo mencionado anteriormente y su enlace con los otros elementos del sistema se detallan en el diagrama siguiente:

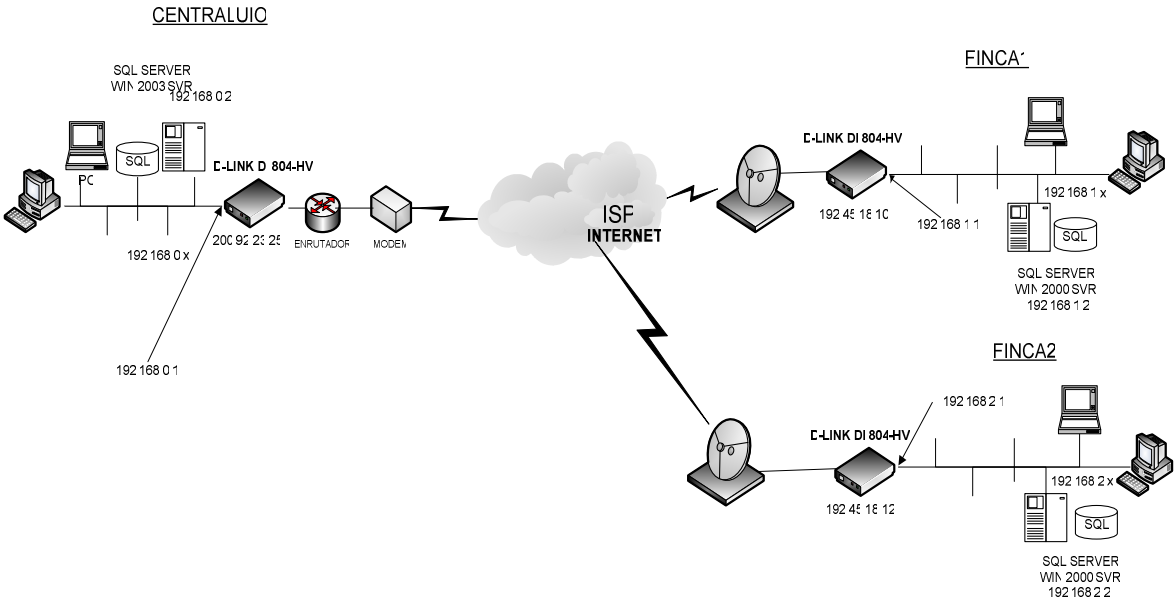

Figura 4.7: Diagrama de red con Equipo DLINK DI 804-HV.

4.2.2 IMPLEMENTACION DEL PROTOTIPO DE LA RED PRIVADA VIRTUAL (VPN)

Para la implementación del prototipo, se tomó como referencia el diseño propuesto en el literal 4.2.1.2, con lo que se demostrará la factibilidad de estas propuestas.

El servicio a ser implementado a través de las VPN será la replicación de base de datos.

4.2.2.1 Propuesta con Software (IPSec Bajo Linux)

Para este caso, se utilizaran dos máquinas configuradas como gateways (server1 y server2), instalados en el sistema operativo Linux White Box 4.0 Kernel 2.6.9-11.EL.

Las máquinas que van a utilizarse como gateways tienen las siguientes características que van detalladas en la tabla que se adjunta a continuación:

EQUIPO	DESCRIPCION	
SERVER1	Procesador	Pentium III
	Velocidad del procesador	1Ghz
	Memoria RAM	256 MB
	Disco Duro	80 GB
	Tarjeta red 1	Sis 900
	Tarjeta red 2	VIA VT 61015
SERVER2	Procesador	Celeron
	Velocidad del procesador	2Ghz
	Memoria RAM	256 MB
	Disco Duro	80 GB
	Tarjeta red 1	CNET
	Tarjeta red 2	Sis 900

Tabla 4.2: Características de los equipos utilizados como gateways

Los equipos a ser utilizados como gateways y las relaciones que tienen con el resto de elementos que integran la red de comunicación del prototipo, se encuentran detallados en el siguiente diagrama:

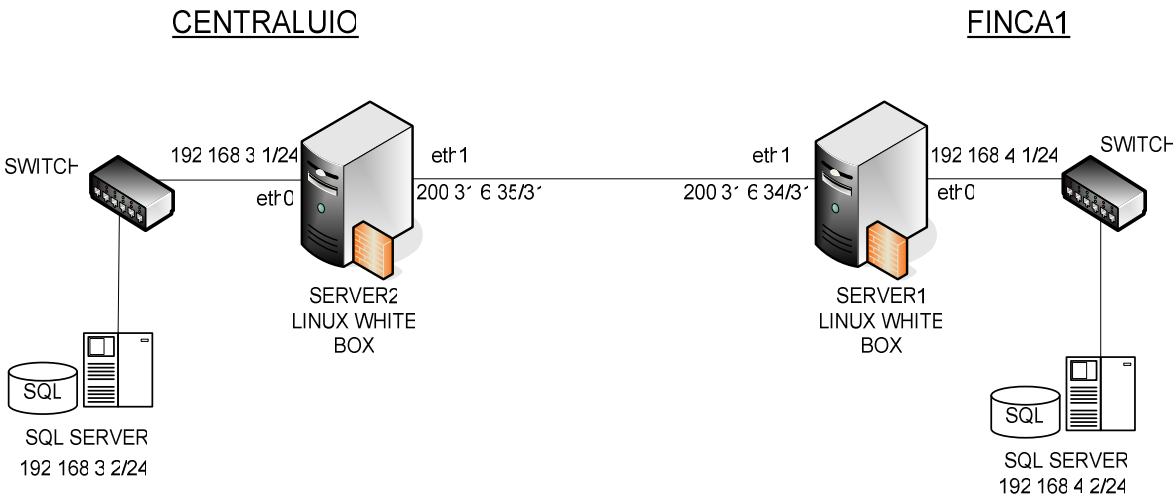

Figura 4.8: Diagrama de red del prototipo

4.2.2.1.1 Configuraciones para los Equipos con Linux

En los gateways se instaló el sistema operativo Linux White Box 4.0, en la opción por defecto de servidor. La configuración de las direcciones IP se basó en el diagrama de red presentado en la figura 4.6. Para esto se ingreso al directorio */etc/sysconfig/network-scrip,* en donde se encuentran los archivos de configuración *ifcfg-eth0* y *ifcfg-eth1* correspondientes a las tarjetas de red del gateway. Para centralizar el control de los servidores se utilizará la herramienta Putty Telnet (Cliente SSH) para acceder de forma remota y segura a los gateways.

a) Configuración del Equipo SERVER1

A continuación se muestran los archivos de configuración de las tarjetas de red para los equipos utilizados en el prototipo, SERVER1 Y SERVER2.

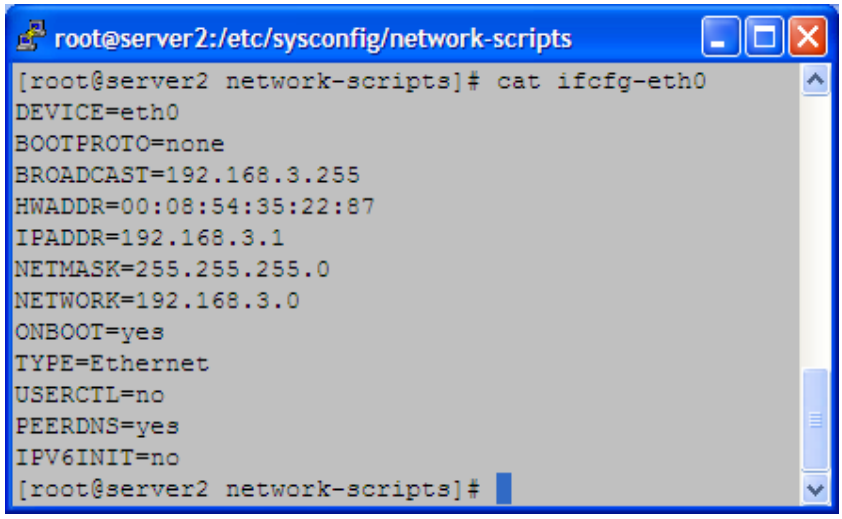

Figura 4.9: Archivo ifcfg-eth0 en SERVER2

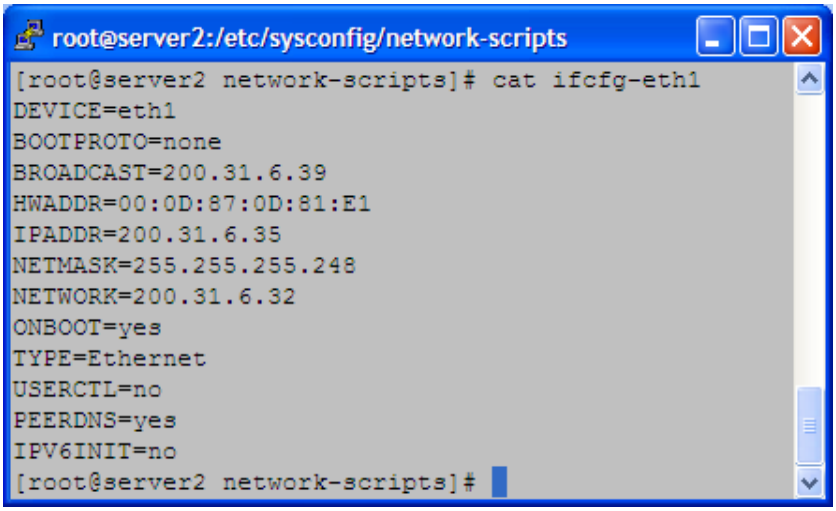

Figura 4.10: Archivo ifcfg-eth1 en SERVER2

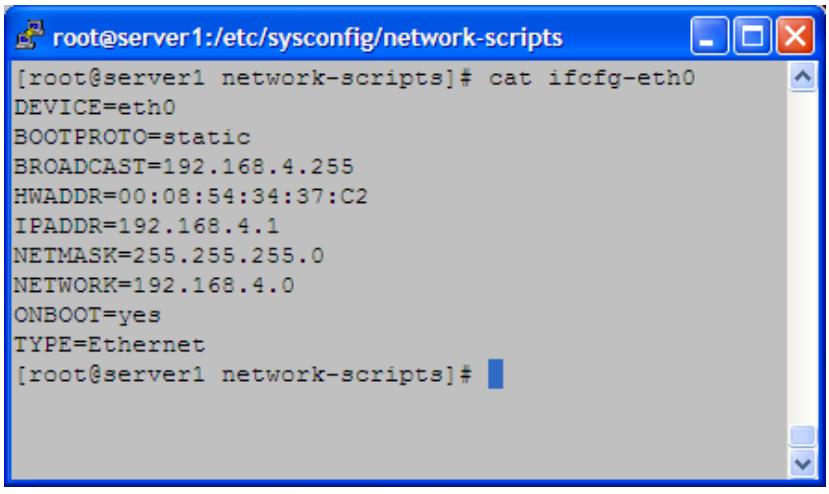

Figura 4.11: Archivo ifcfg-eth0 en SERVER1

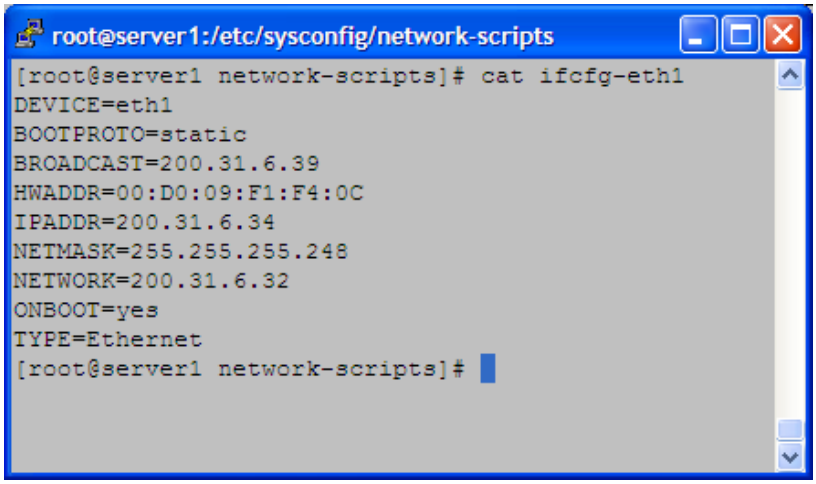

Figura 4.12: Archivo ifcfg-eth1 en SERVER1

Debido a que la opción de soporte IPSec no se activa al momento de la instalación, es necesario recompilar el Kernel para tener esta opción activa. Entonces se seguirán los siguientes pasos:

1. Se arranca Linux.
2. Se accesa de forma remota a los equipos con Putty Telnet con el user y password de cada servidor.
3. Se comprueba la versión del núcleo: uname –sr

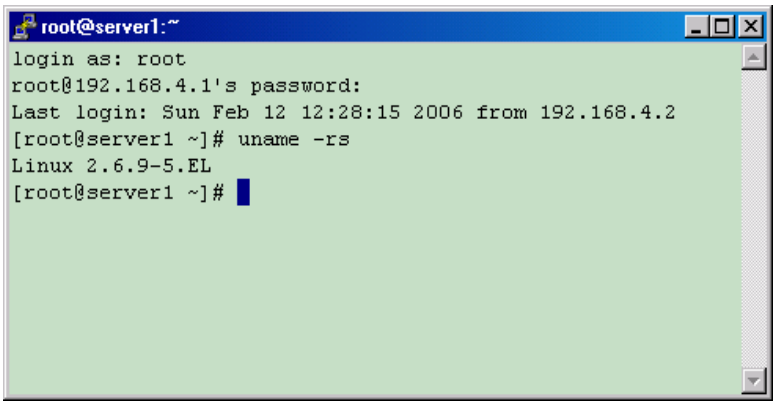

Figura 4.13: Versión del kernel instalado (2.6.9-5.EL)

4. En www.kernel.org aparece la versión estable más reciente (Es la que aparece en la línea que pone: The latest stable version of the Linux kernel is).
5. Se descarga la version 2.6.9-11.EL-i686.tar y se copia en /usr/src/kernels/, *con el comando: tar –xvf* 2.6.9-11.EL-i686.tar se desempaqueta el archivo.

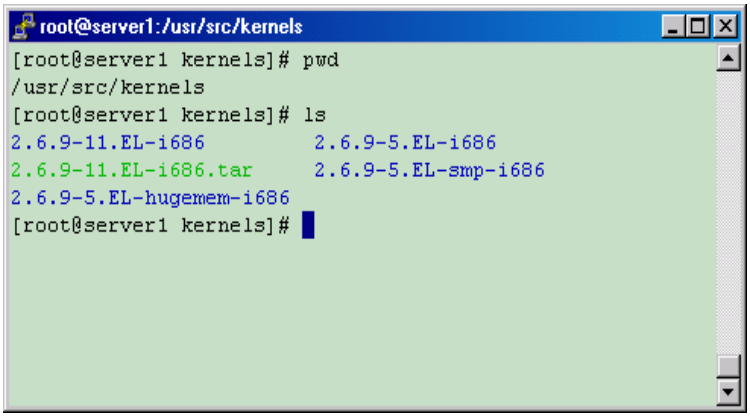

Figura 4.14: Archivo comprimido del kernel

6. Se posiciona en el directorio /usr/src/kernels/2.6.9-11.EL-i686

cd /usr/src/kernels/2.6.9-11.EL-i686.

7. Se comprueba el contenido del directorio:

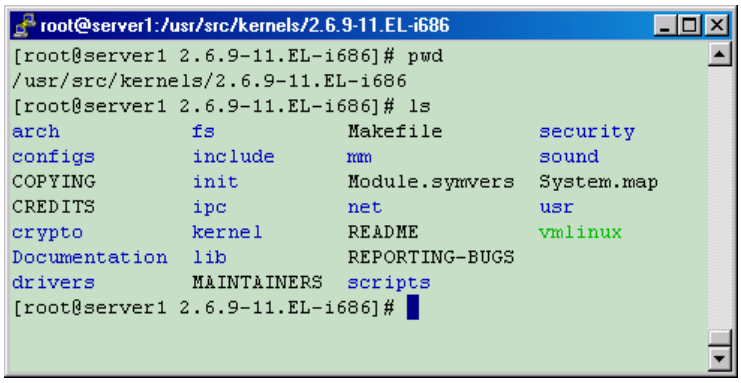

Figura 4.15: Lista de archivos del kernel

8. Si ya hubo una compilación anterior del núcleo, se ejecuta:

make mrproper

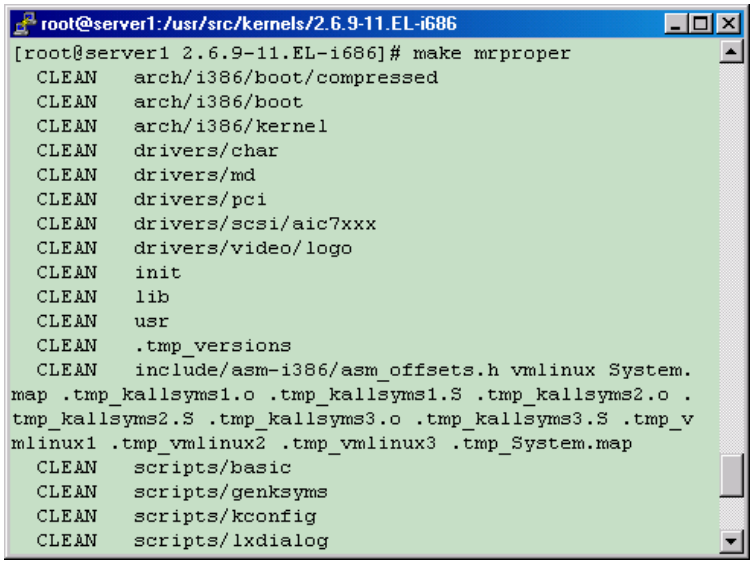

Figura 4.16: resultado de make mrproper

9. En caso de que exista en ese directorio el archivo de configuración para la compilación del núcleo actual (será un archivo que contenga la palabra config), se copia al directorio /usr/src/kernels/2.6.9-11.EL-i686 con el nombre .config

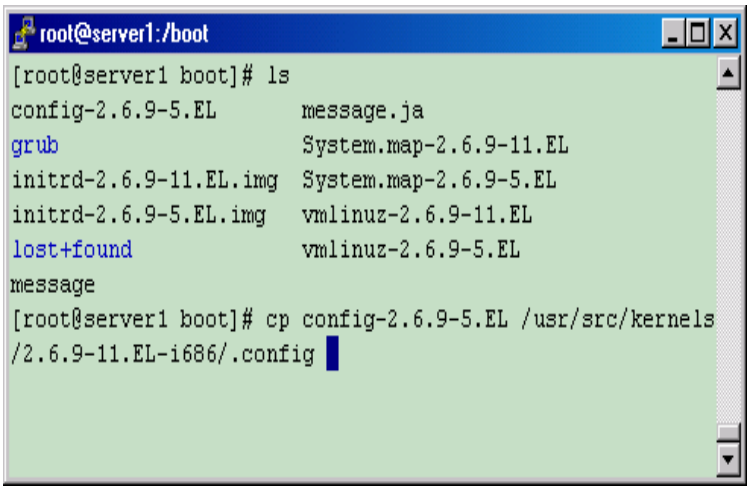

Figura 4.17: Copia del archivo de configuración del kernel

Luego se ejecuta make oldconfig. Con esto se actualiza el archivo .config con las opciones del nuevo núcleo. Si en este proceso hace alguna pregunta, simplemente se pulsa INTRO para seleccionar la opción por defecto.

10. Ahora se configura el kernel: mediante el modo gráfico de consola:

make menuconfig

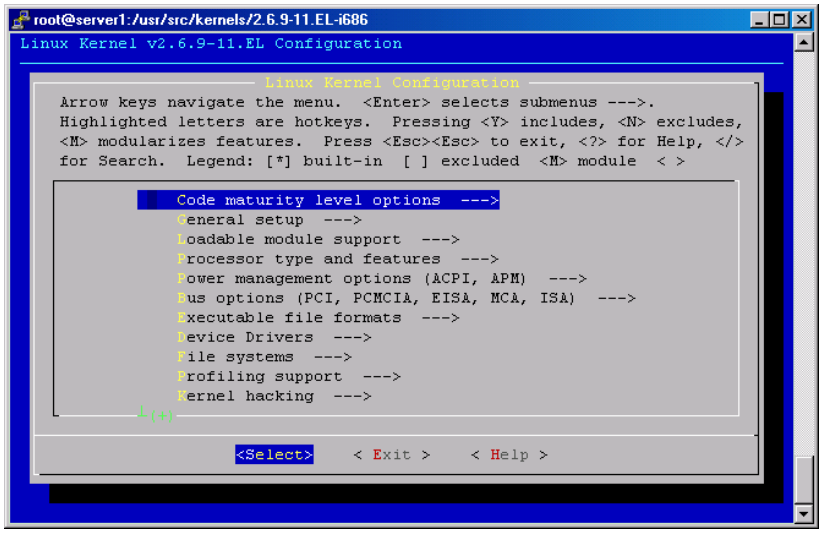

Figura 4.18: Pantalla de inicio de menú config

11. Se configura las opciones en el Kernel que necesita IPSec. Del menú anterior se escoge: “ Device Drivers”
12. Luego se hace clic en la opción: “Networking support. Se escoge la opción: “Networking options” y finalmente se habilita “PF_KEY sockets”, IP: AH transformation (INET_AH), IP: ESP transformation (INET_ESP), IP: IPsec user configuration interface (XFRM_USER)

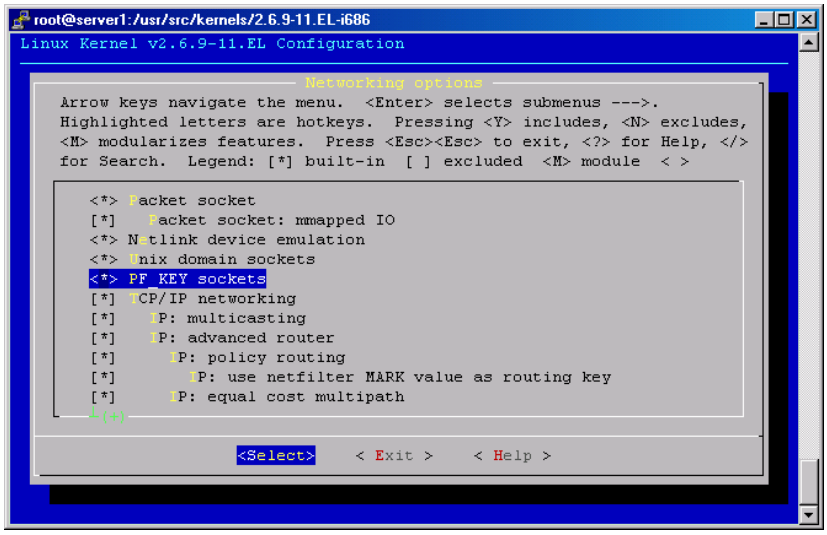

Figura 4.19: Habilitación de IPSec

13. Dentro de “Cryptographic options” se habilita: HMAC support (CRYPTO_HMAC), Null algorithms (CRYPTO_NULL), MD5 digest algorithm (CRYPTO_MD5), SHA1 digest algorithm (CRYPTO_SHA1), DES and Triple DES EDE cipher algorithms (CRYPTO_DES), AES cipher algorithms (CRYPTO_AES).

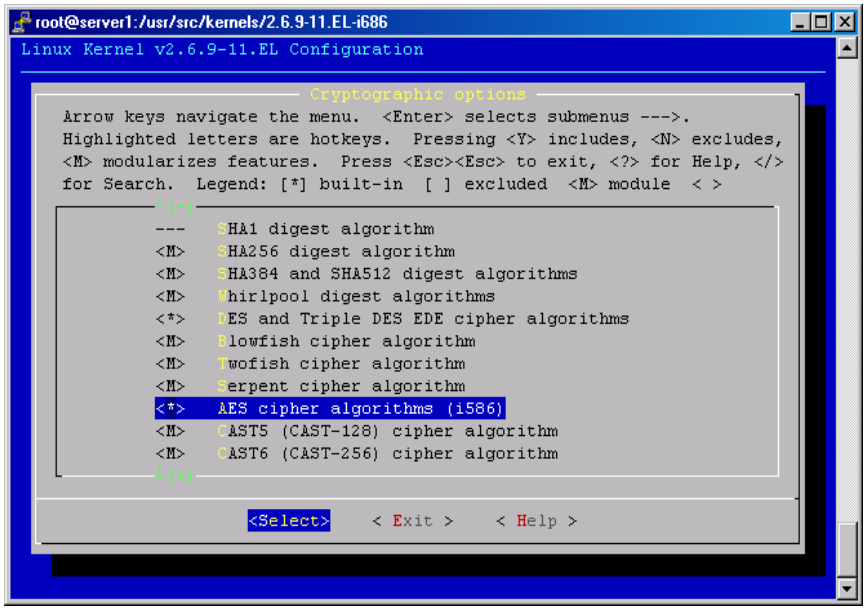

Figura 4.20: Habilitación algoritmos de encriptación y cifrado

14. Ahora llega el momento de compilar, para ello se ejecuta: make dep

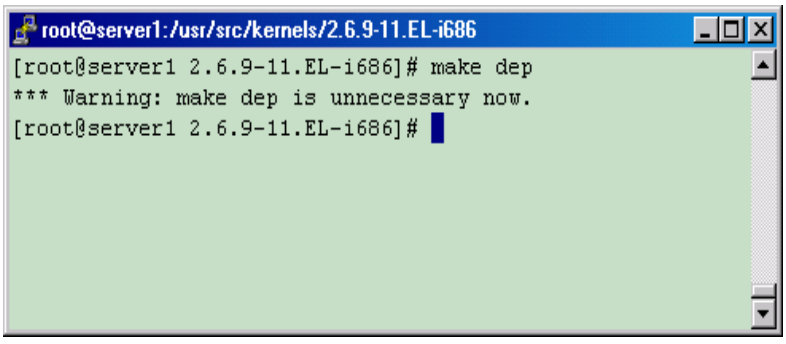

Figura 4.21: Resultado de make dep

make clean

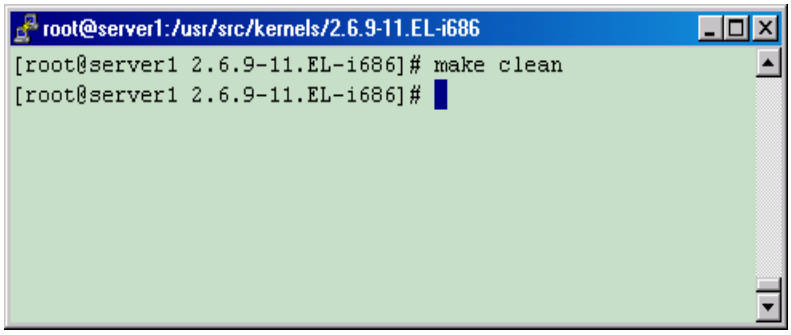

Figura 4.22: Resultados de make clean

make bzImage

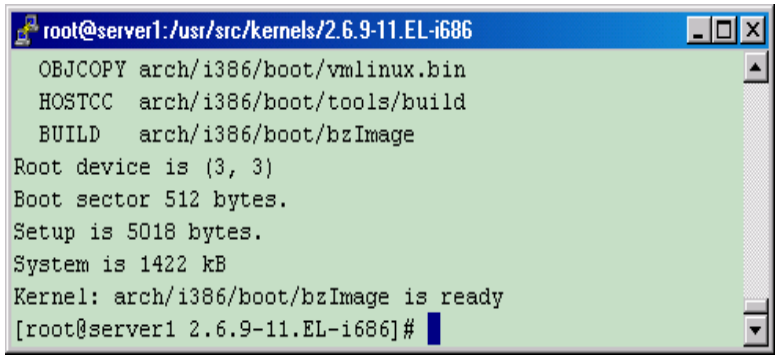

Figura 4.23: Resultados de make bzImage

Según la potencia de máquina utilizada, el proceso puede tardar un buen rato.

15. Una vez compilado el núcleo, les toca el turno a los módulos:

make modules && make modules_install

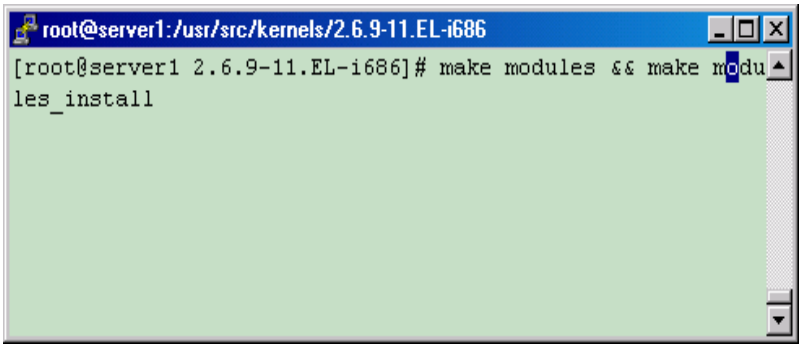

Figura 4.24: Resultados de make modules && make modules_install.

Esto también tardará otro algunos minutos (probablemente más que la compilación del núcleo).

16. Se copia el fichero **System.map** y el núcleo obtenido (que se encuentra en **/usr/src/kernels/2.6.9-11.EL-i686/arch/i386/boot/bzImage**, si la arquitectura es i386) al directorio /boot , con los nombres ***System.map-2.6.9-11.EL*** y **vmlinuz-2.6.9-11.EL:**

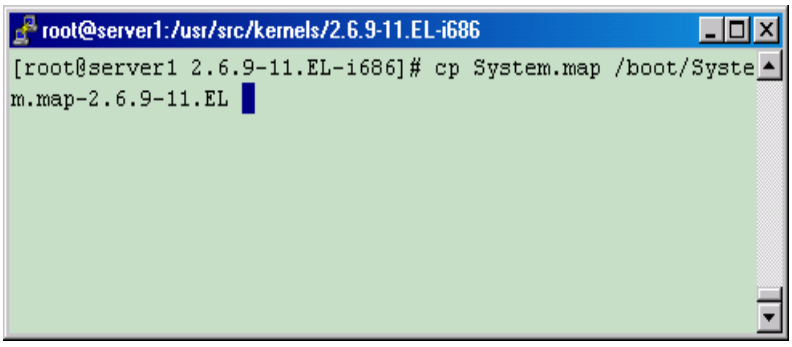

Figura 4.25: Copia de los archivo generados en la compilación

Se genera el archivo initrd-2.6.9-11.EL.img en el directorio /boot

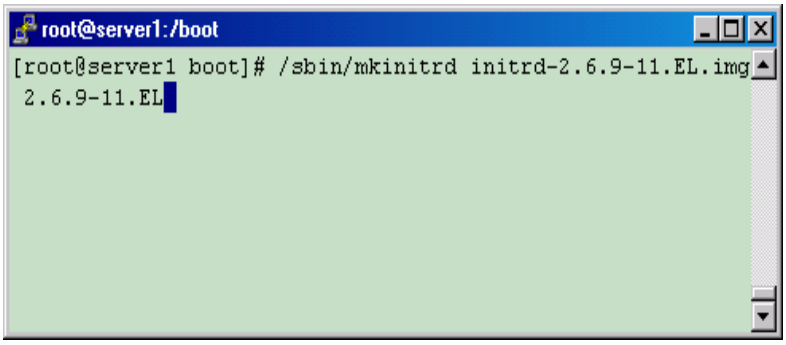

Figura 4.26: Generación del initrd

17. Se edita el archivo de configuración ***menu.list*** del gestor de arranque GRUB y se agrega una entrada para la nueva versión del kernel compilado.

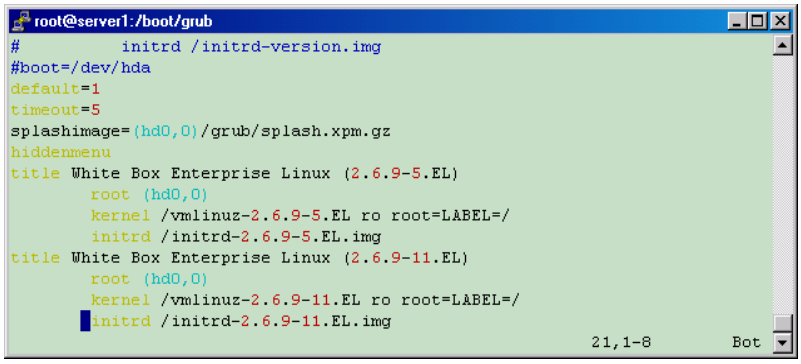

Figura 4.27: Entrada en menu.list de GRUB

18. Luego se reinicia la máquina, que arrancará con el nuevo núcleo, como comprobaremos con: uname –sr.

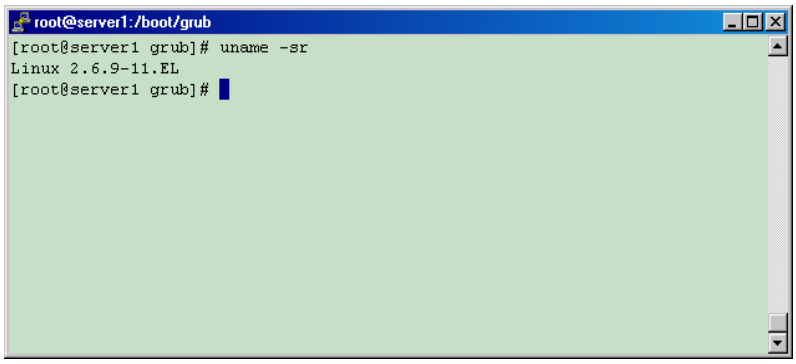

Figura 4.28: Verificación del núcleo

b) Configuración del Equipo SERVER2

Cabe destacar que este procedimiento también se ejecuta en el SERVER2. Con esto ya se tiene habilitado el soporte IPSec en los gateways. El próximo paso, será configurar el túnel virtual entre los dos servidores. Para esto se siguen los pasos ejecutados en el SERVER2:

1. Se ubica en el directorio */etc/sysconfig/network-scripts,* donde se encuentran los archivos de configuración de las interfaces de red del sistema operativo.

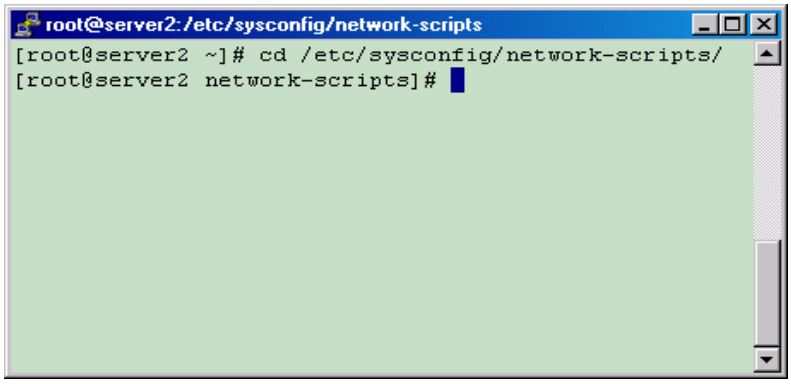

Figura 4.29: Ubicación en el directorio de configuración

2. Se crea un archivo *"ifcfg-ipsec0"* en donde se edita la configuración de la interfase ipsec, para levantar la conexión VPN, tal como se indica a continuación:

ONBOOT=yes Activa la interfaz al momento de iniciar el servicio de red.

IKE_METHOD=PSK	Método de autenticación (claves compartidas).
DSTGW=192.168.4.1	Dirección IP privada del gateway de destino.
SRCGW=192.168.3.1	Dirección IP privada del gateway de origen.
DSTNET=192.168.4.0/24	Dirección de red privada destino.
SRCNET=192.168.3.0/24	Dirección de red privada origen.
DST=200.31.6.34	IP pública del servidor remoto.
TYPE=IPSEC	Protocolo de seguridad IP.

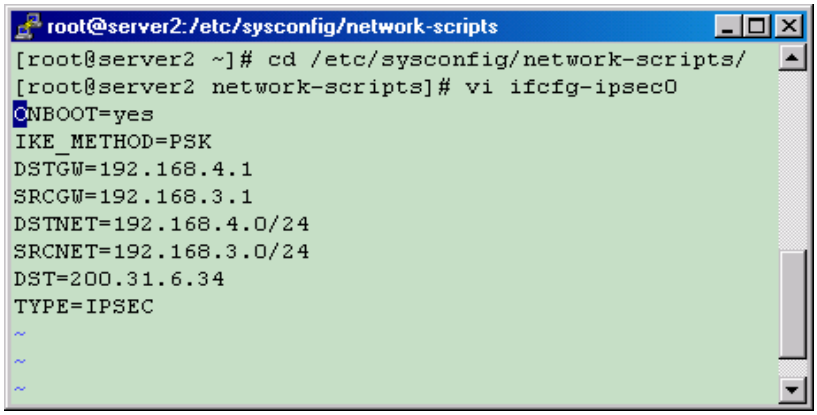

Figura 4.30: Archivo de configuración de la internas IPSec.

3. Se emplea el dispositivo **/dev/random** para asegurar las claves aleatorias de 192 bits, con la que los servidores se autenticarán al momento de establecer la conexión VPN.

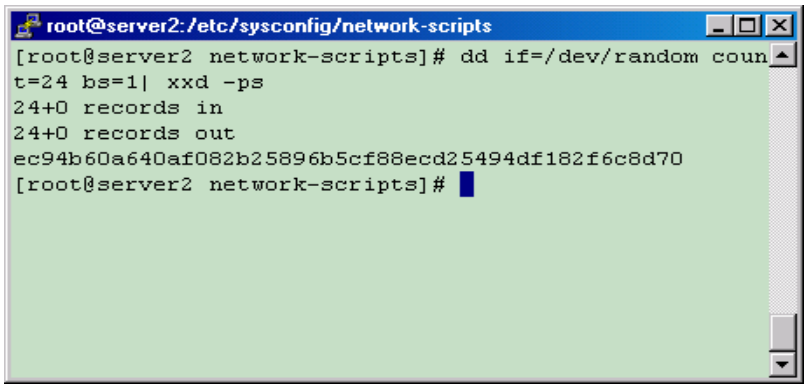

Figura 4.31: Generación de la clave compartida

4. Se crea el archivo “keys-ipsec0”, en el cual se edita la clave generada en el paso anterior.

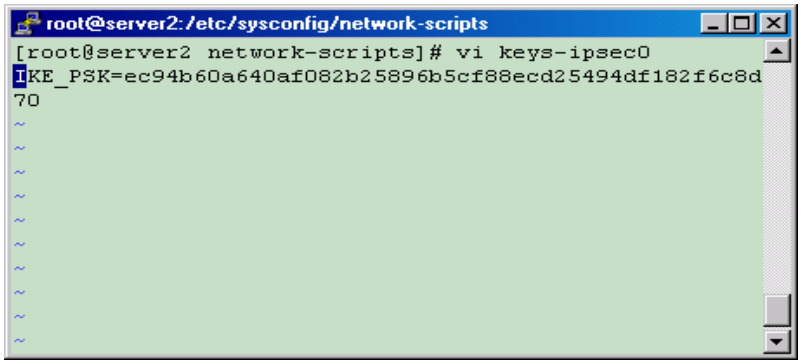

Figura 4.32: Archivo de configuración keys-ipsec0

5. Para establecer la conexión VPN, es necesario habilitar los puertos y protocolos que utiliza ipsec en el firewall local de servidor, por defecto Linux White Box 4.0 viene solo con el puerto ssh (22) habilitado. Para esto editamos el archivo de configuración *iptables*, ubicado en *“/etc/sysconfig”* e ingresamos las siguientes directivas:

-A RH-Firewall-1-INPUT -p 50 -j ACCEPT (Protocolo ESP).

-A RH-Firewall-1-INPUT -p 51 -j ACCEPT (Protocolo AH).

-A RH-Firewall-1-INPUT -p udp -m udp --dport 500 --sport 500 -j ACCEPT.

-A RH-Firewall-1-INPUT -d 192.168.4.2 -i eth0 -j ACCEPT.

-A RH-Firewall-1-INPUT -s 192.168.4.2.0 -i eth0 -j ACCEPT.

6. Se reinicia el servicio iptables, para que tomen efecto los cambios realizados.

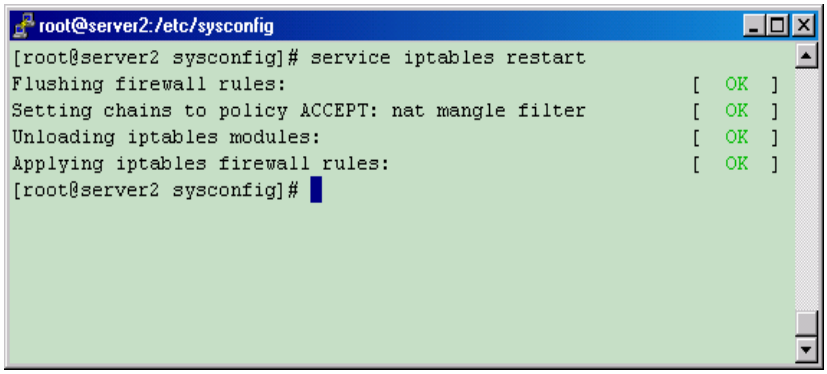

Figura 4.33: Restart del servicio iptables

7. Se habilita el ipforward para reenvío de paquetes entre las interfaces, a través del siguiente comando *"echo 1 > /proc/sys/net/ipv4/ip_forward".*

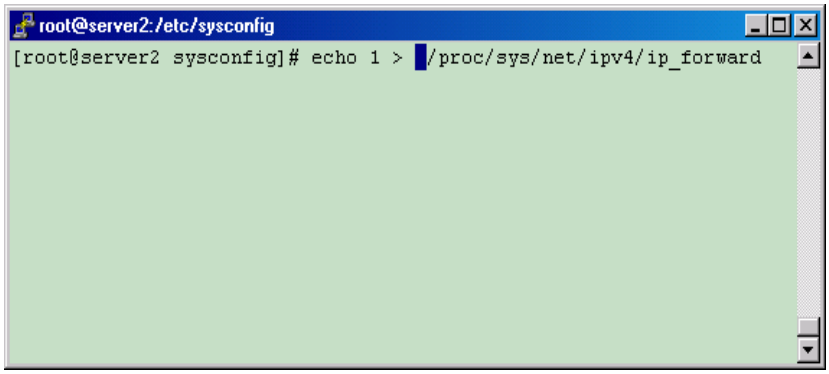

Figura 4.34: Habilitación del ip_forward

8. De la misma forma se configura en el SERVER1, solo se deben intercambiar las direcciones fuente y destino.

9. Finalmente levantamos el servicio para la conexión vpn a través del siguiente comando *"ifup ipsec0".* En los dos equipos, en este momento no se establece la conexión VPN, la negociación inicia cuando existe algún

paquete dirigido hacia la red remota. Esto se puede lograr ejecutando el comando ping con destino al gateway remoto.

Como se puede apreciar en la gráfica se pierde un paquete del comando ping, debido a que en ese momento está en proceso de negociación. Con la ayuda del comando *tail –f /var/log/messages,* se puede observar el proceso de negociación del enlace VPN.

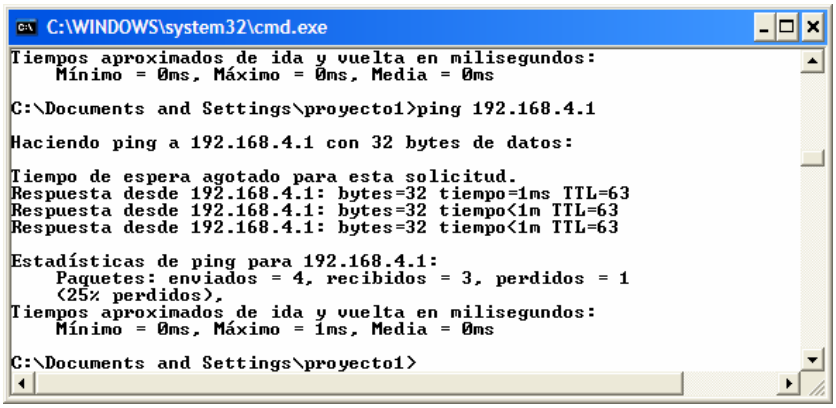

Figura 4.35: Ping hacia el gateway remoto.

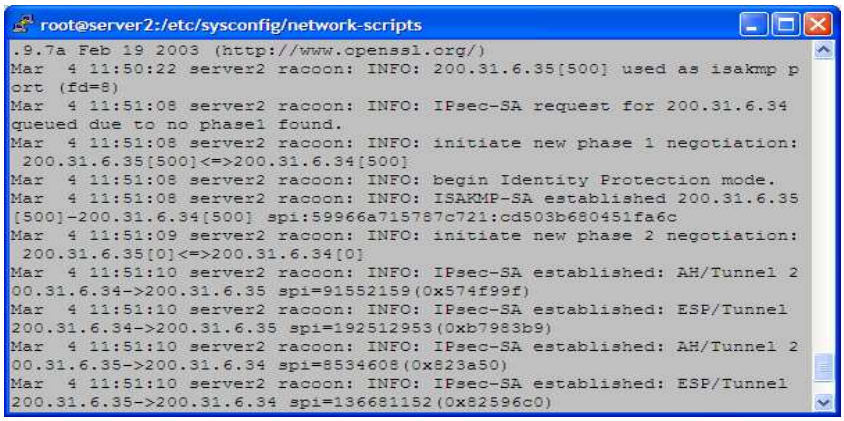

Figura 4.36: Logs del establecimiento de la conexión VPN

4.2.2.2 Propuesta con Hardware (DLINK DI 804-HV)

Los equipos D-LINK traen por defecto, dos interfaces de red: una WAN y otra LAN. Esta última, viene con cuatro entradas configuradas en modo de switch.

Para el prototipo se utilizan dos equipos D-LINK cuyas direcciones IP y configuraciones se detallan en el siguiente diagrama:

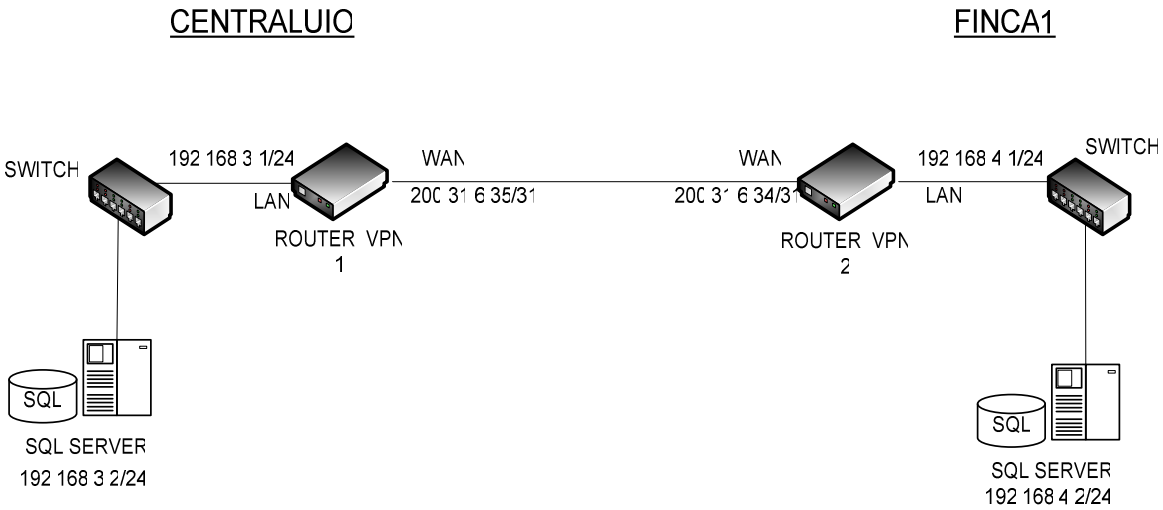

Figura 4.37: Diagrama de red con Routers VPN D-Link

4.2.2.2.1 Configuraciones para los Equipos D-LINK

Los siguientes gráficos corresponden a la configuración del ROUTER VPN 1. Esta configuración se extiende al segundo ROUTER, teniendo en cuenta que es necesario cambiar las direcciones de destino y origen:

a) Configuración del Equipo ROUTER VPN1

1. Se ingresa a la configuración a través del explorador web a la URL http://192.168.3.1. El usuario de configuración viene por defecto “admin” y el password en blanco, la URL por defecto es http://192.168.0.1

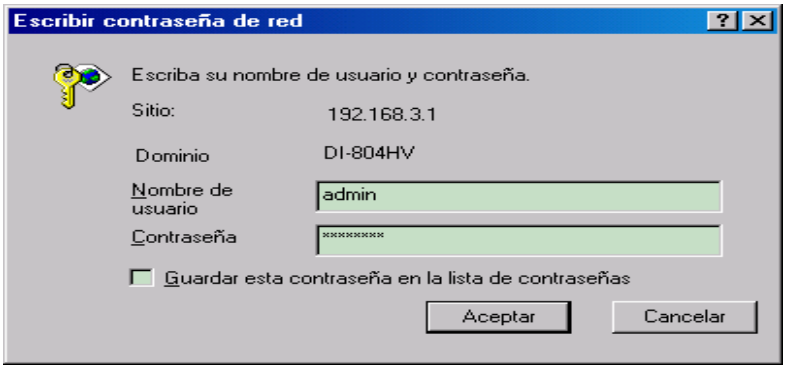

Figura 4.38: Pantalla de autenticación.

2. Se muestra la página de configuración, en la cual se ingresan los datos de las diferentes opciones que se van a configurar tal como: WAN, LAN y VPN.

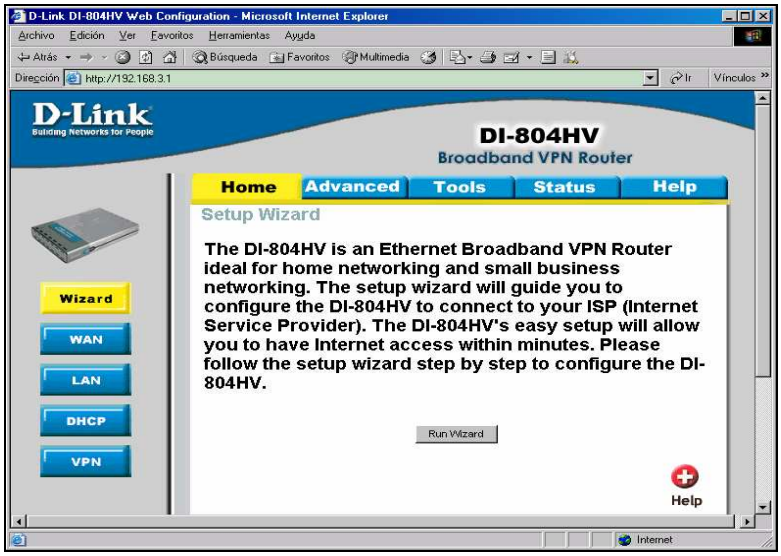

Figura 4.39: Pantalla de inicio para la configuración del ROUTER VPN1

3. Para la configuración de la parte WAN, se ingresan los datos que se muestran a continuación:

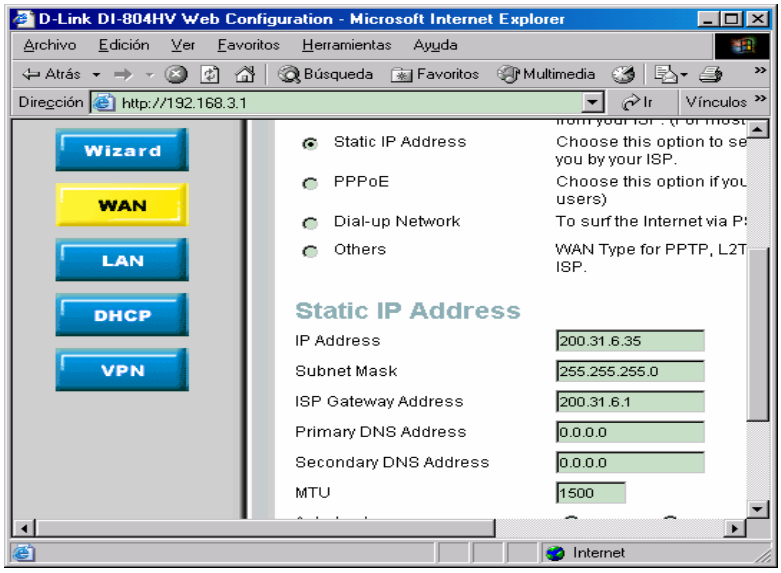

Figura 4.40: Configuración WAN

4. Para la configuración de la LAN, se ingresan los siguientes datos; IP Address 192.168.3.1, Subset Mask: 255.255.255.0, Domain Name: tesis.com

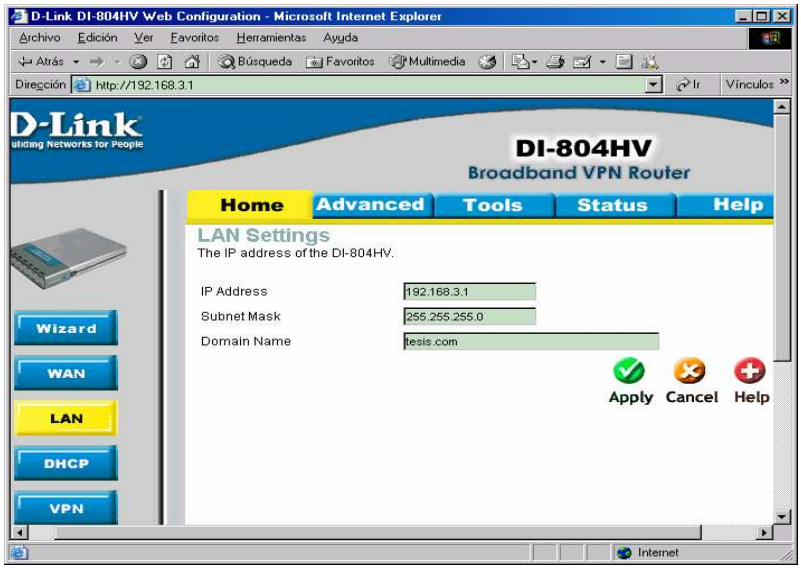

Figura 4.41: Configuración LAN

5. Luego de configurar, la parte WAN y LAN, se habilitan las opciones para la VPN. Se ingresa el nombre del túnel vpn: ipsec0 y el método es IKE (Internet Key Exchange, que es la forma automática de intercambio de claves).

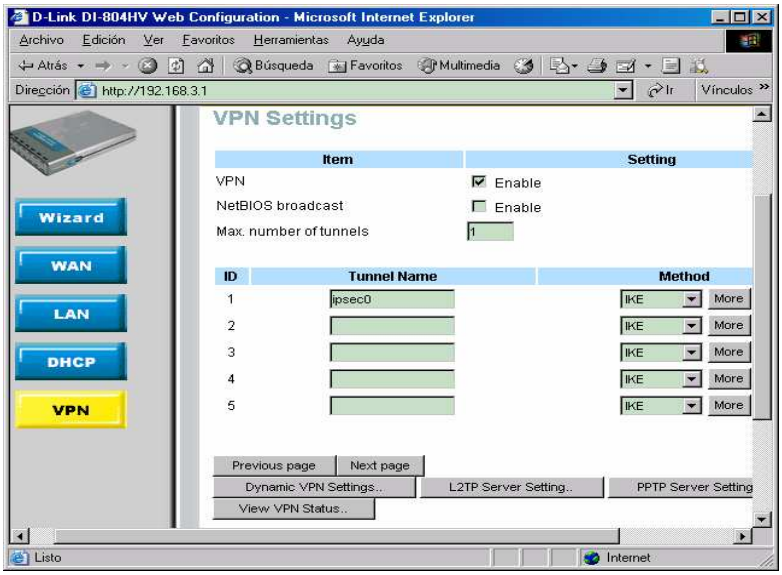

Figura 4.42: Configuración VPN

6. Del paso anterior se hace clic en “More”, y se tiene la siguiente pantalla. En ésta, se configuran los datos de LAN (Subnet y Mask) de los dos Routers (local y remoto), como también el Gateway remoto, y la clave precompartida “edwin123”, con la cual se van autenticar.

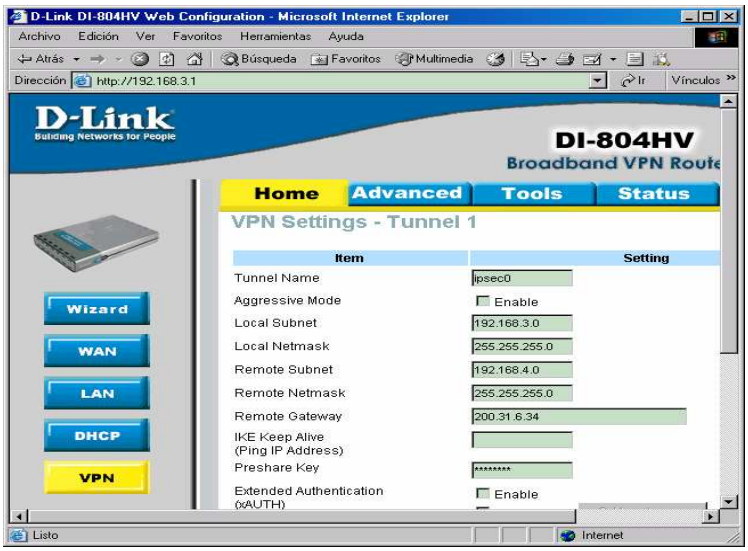

Figura 4.43: Configuración de red local y remota en el túnel VPN

7. Una vez ingresados los datos que van a establecer el túnel, se hace clic en la opción “Select IKE Prosposal”, en donde se configura la encriptación y autenticación de la información. Para este prototipo, se escogieron las

siguientes opciones: ID Prosposal Name: “test” y 1 (parte inferior). Se hace clic en agregar, DH Group (Diffie Hellman): “Group2” (1024 bits), Encrypt Algorithm: “3DES” (Data Encription Standar), Auth Algorithm: “MD5” , Life Time: “300” (tiempo de vida de renegociación de claves), Life Time Unit: “sec”.

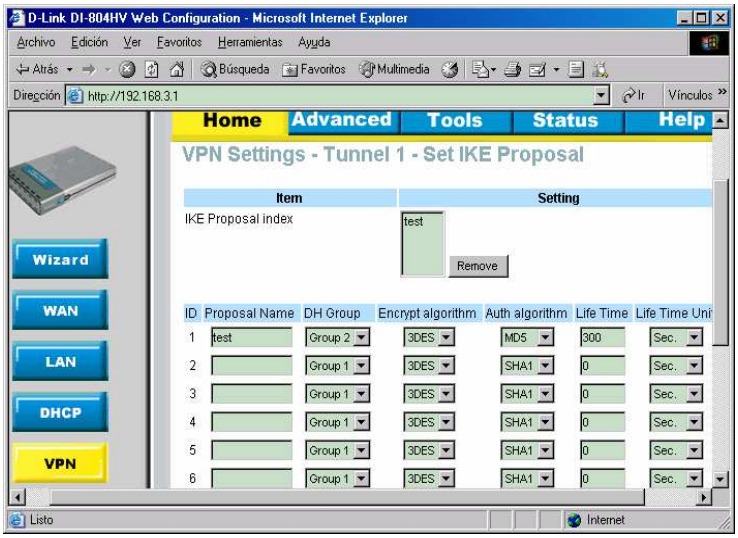

Figura 4.44: Configuración IKE proposal.

8. Se hace clic en back, y se escoge la opción; “Select IPSec Prosposal”, que permite seleccionar la forma en que IPSec negociará la conexión. Se procede de la misma manera que para el apartado anterior, con la única diferencia del protocolo de encapsulamiento; Encap protocol: “ESP” (Encapsulation Security Paiload).

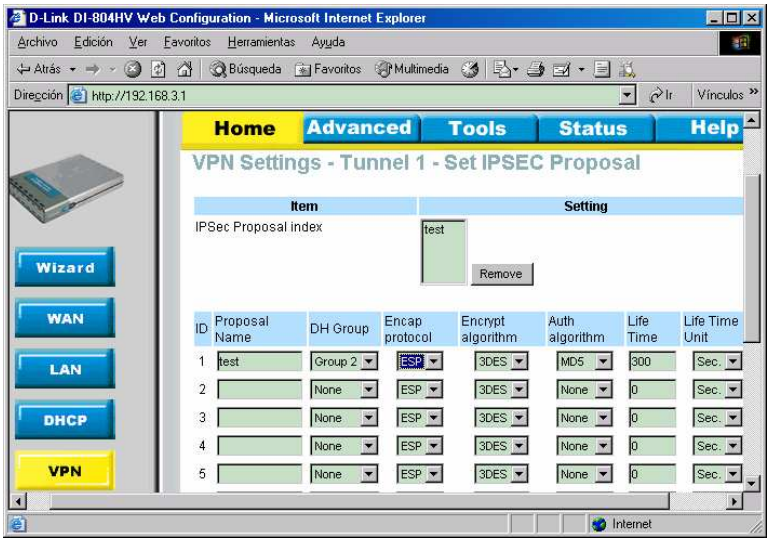

Figura 4.45: Configuración IPSec proposal.

9. A continuación se muestra el estatus de la configuración total de las direcciones IP, del Router VPN 1:

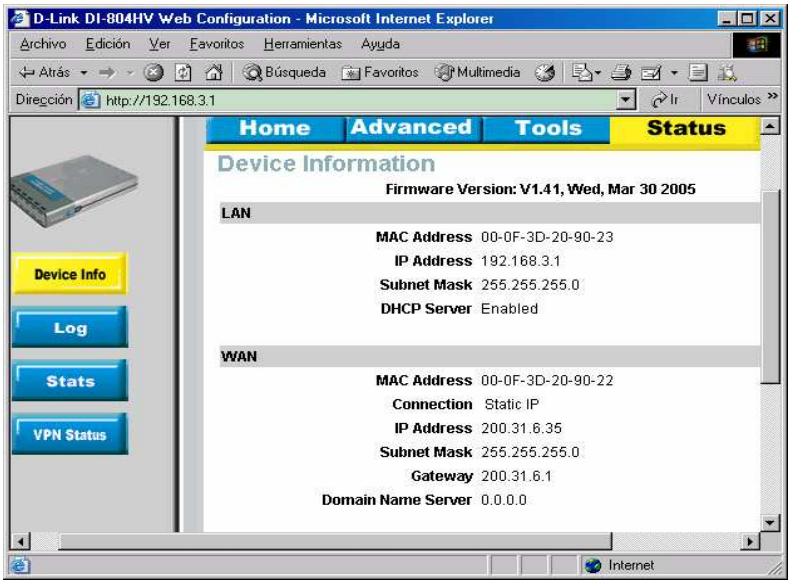

Figura 4.46: Configuración total ROUTER VPN1.

10. Se muestra la configuración de la conexión y los datos de la las subred del router A, ya esta establecida la conexión.

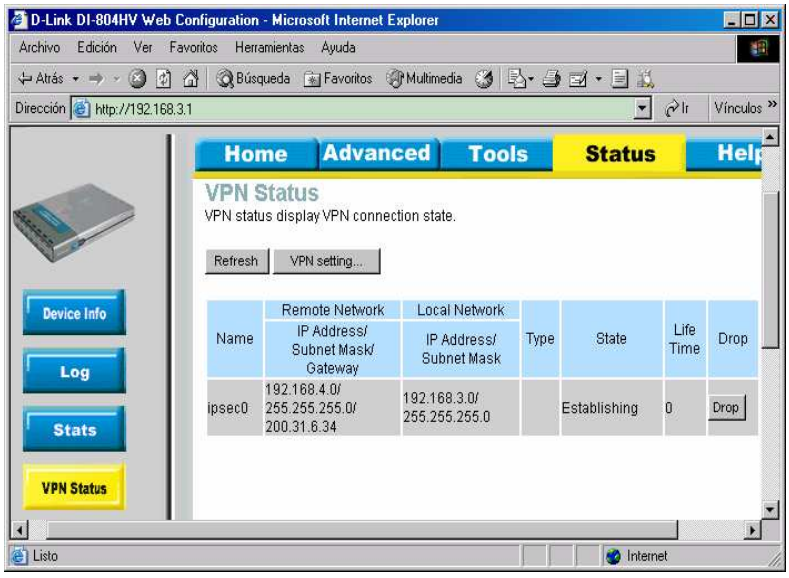

Figura 4.47: Status del ROUTER VPN1.

b) Configuración del Equipo ROUTER VPN2

11. La configuración del ROUTER VPN2, se la realiza de manera similar a la del ROUTER VPN 1, por esta razón; solo se va describir los las pantallas de la configuración total, tal como se muestra a continuación. La pantalla siguiente indica la configuración de las direcciones IP de las Conexiones LAN y WAN. El acceso a este router se realiza a través de la URL: http://192.168.4.1, con el mismo usuario y password del ROUTER VPN1.

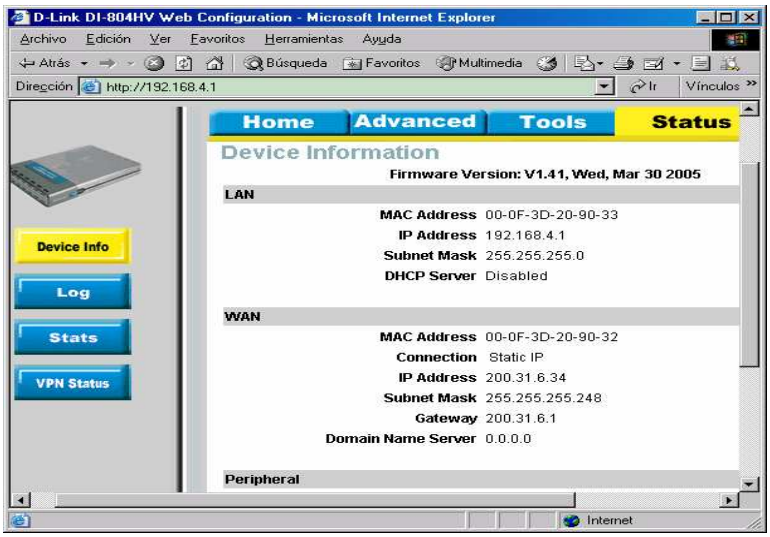

Figura 4.48: Configuración total ROUTER VPN2.

12. En la siguiente pantalla, muestra el status de la conexión establecida.

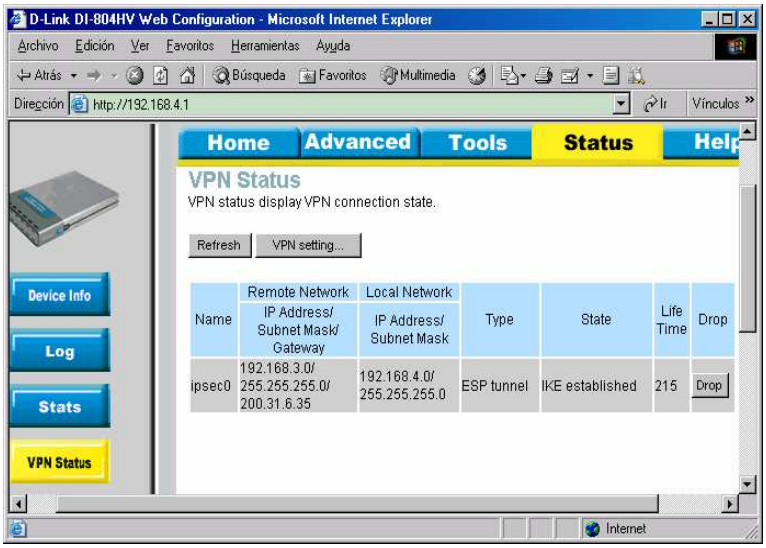

Figura 4.49: Status de la conexión VPN2.

13. Para la verificación del enlace se ejecuta el comando ping desde la LAN (Router VPN1) IP 192.168.3.2 hacia la WAN del Router VPN2 IP 200.31.6.35. Como se puede observar, se tiene la conexión de la VPN levantada, entre estos puntos.

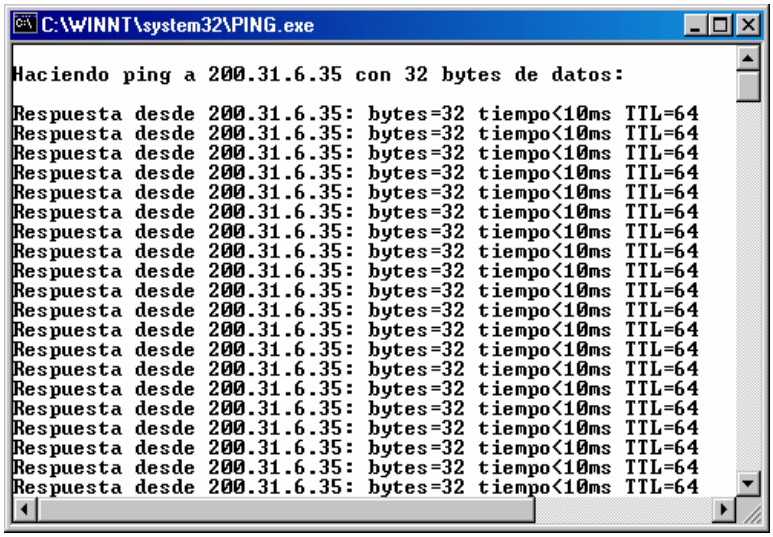

Figura 4.50: Resultado del PING hacia la WAN del ROUTER VPN2.

14. Ping desde la LAN (Router 1) IP 192.168.3.2 hacia la LAN del Router 2, IP 192.168.4.1. Como se puede observar, se tiene la conexión de la VPN levantada, entre estos puntos.

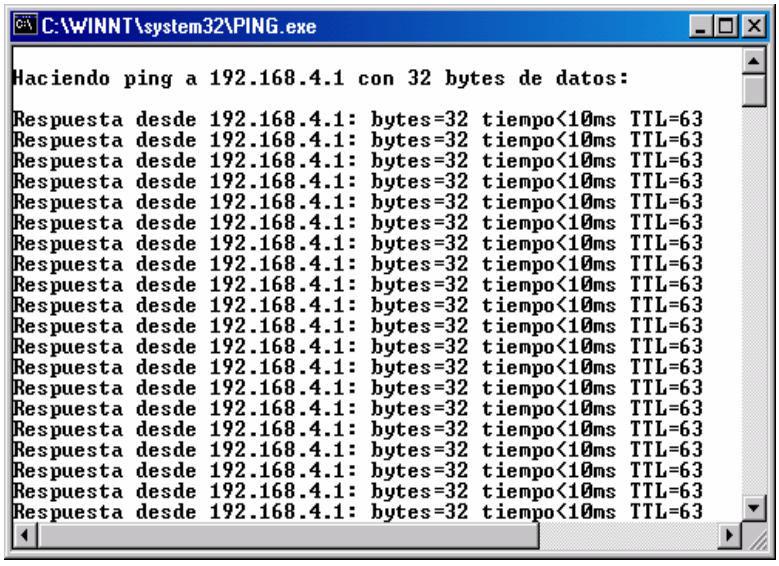

Figura 4.51: Resultado del PING hacia al LAN del ROUTER 2.

15. Ping desde la LAN (Router 2) IP 192.168.4.2 hacia la WAN del Router 2, IP 200.31.6.34. Como se puede observar, se tiene la conexión de la VPN levantada, entre estos puntos.

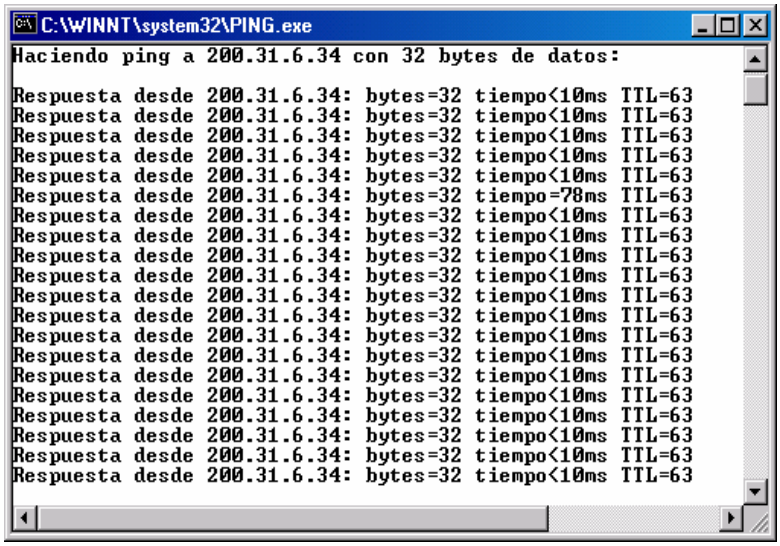

Figura 4.52: Resultado del PING hacia al WAN del ROUTER 1

16. Ping desde la LAN (Router 2) IP 192.168.4.2 hacia la LAN del Router 1, IP 192.168.3.1. Como se puede observar, se tiene la conexión de la VPN levantada, entre estos puntos

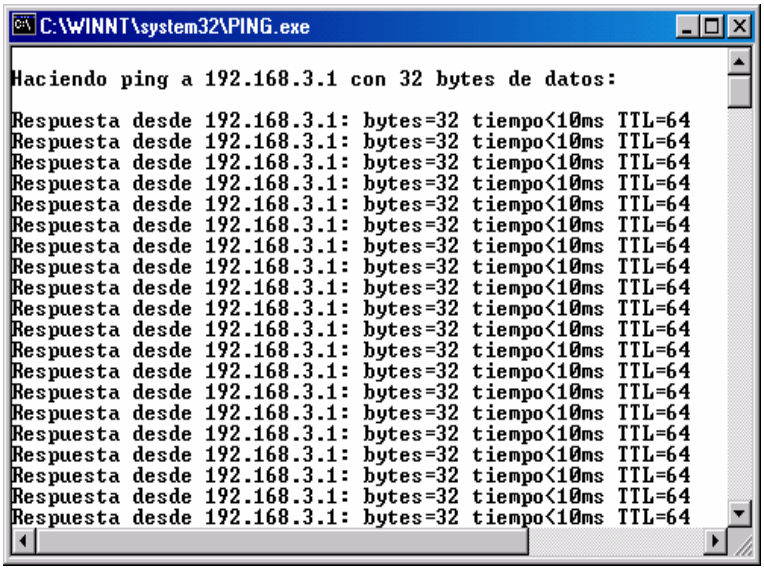

Figura 4.53: Resultado del PING hacia al LAN del ROUTER 1.

4.2.2.3 Configuración de la Replicación Transaccional

De acuerdo a las necesidades y requerimientos de la empresa, analizadas en el capítulo 3; para tener la información actualizada de la producción diaria de las fincas, se utilizará la replicación de las bases de datos, para poder sustentar los requerimientos de informes, estadísticas y reportes que tiene la Gerencia, el Departamento Financiero y demás áreas, que demandan de esta información importante al momento de toma de decisiones; sobre el incremento de la producción de una u otra variedad de flores, dependiendo de la demanda del mercado nacional e internacional.

Con este antecedente la información que se almacenará en la base de datos de oficina central, no sufrirá ningún cambio en sus tablas, sino que más bien se utilizará como una base de consultas, mientras que en la base de las fincas se almacena la información diaria de la producción, aquí existirán cambios en la base, con las sentencias SQL *insert, update y delete.* Estos cambios deben pasar a la base de la oficina central. De esta forma, el diagrama de replicación será en un solo sentido; de las fincas hacia la matriz, tal como se muestra en la siguiente figura.

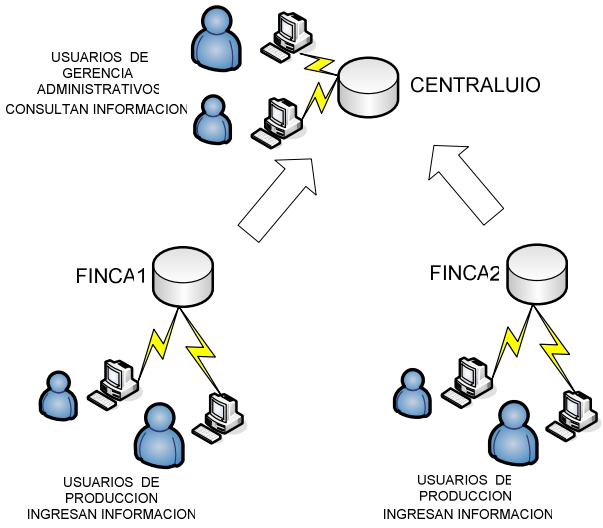

Figura 4.54: Diagrama de replicación para una empresa florícola

Para efectos del prototipo y con el objeto de mostrar el funcionamiento de la VPN, se implementará un esquema de replicación del tipo transaccional. Para esto se utilizarán dos equipos denominados:

- PROYECTO-TESIS, que simula un servidor remoto ubicado en las fincas (FINCA1 y FINCA2), y
- EQUIPO1, que es el servidor ubicado en oficinas de Quito (CENTRALUIO).

En el equipo correspondiente a las fincas está instalado el sistema operativo Windows 2000 Server con service pack 4 y Sql Server Enterprise Edition. Esto debido a que la replicación del tipo transaccional corre únicamente en este ambiente. Este servidor tendrá el rol de *publicador-distribuidor* mientras que el servidor EQUIPO1 tendrá el rol de *suscriptor.* Para que el servidor cumpla con este rol, no es necesario de requisitos como los que exige el publicador. Es por esta razón, que se decidió instalar el sistema operativo Windows XP Professional service pack 2 con SQL Server Personal Edition y con el afán de mostrar la interoperabilidad entre los diferentes productos de Microsoft. La base de datos que se hará público es ***"PUBS"***, con los siguientes artículos: *jobs*, *authors y employee.*

En el suscriptor se creará una nueva base de datos denominada ***"TESIS",*** en la que se recibirán los datos replicados desde la base de datos pública. Al final se observará que en la base TESIS se tendrá nuevas tablas, idénticas a los de la base "*PUBS"*, si modificamos estas tablas sus cambios se reflejaran en la base TESIS del servidor de suscripción. Con esta información se presenta el diagrama de replicación de las bases de datos del prototipo.

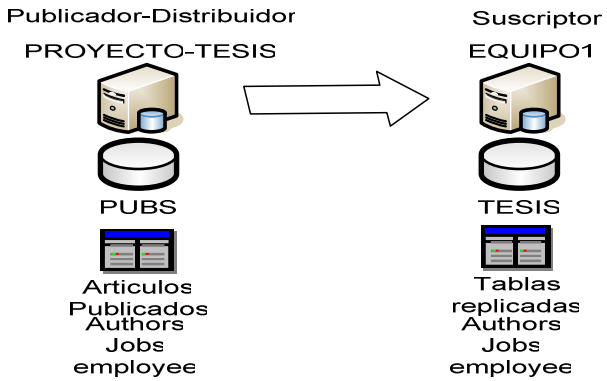

Figura 4.55: Diagrama de replicación para el prototipo

Las características de los equipos utilizados, constan en la siguiente tabla:

EQUIPO	**DESCRIPCION**	
Proyecto-Tesis	Procesador	Pentium IV
(Clon)	Velocidad del procesador	1.8 GHz
	Memoria RAM	512 MB
	Disco Duro	80 GB
	Tarjeta red 1	CNet
EQUIPO1	Procesador	Centrino
(Laptop HP)	Velocidad del procesador	1.86 Ghz
	Memoria RAM	1GB
	Disco Duro	80 GB
	Tarjeta red 1	Broadcom

Tabla 4.3: Características de los equipos utilizados como Servidores de BDD.

4.2.2.3.1 Configuración del Publicador-Distribuidor y Suscriptor

1. En inicio/Programas/Microsoft SQL Server, se escoge Administrador Corporativo, para iniciar la consola de administración del SQL y configurar la replicación.

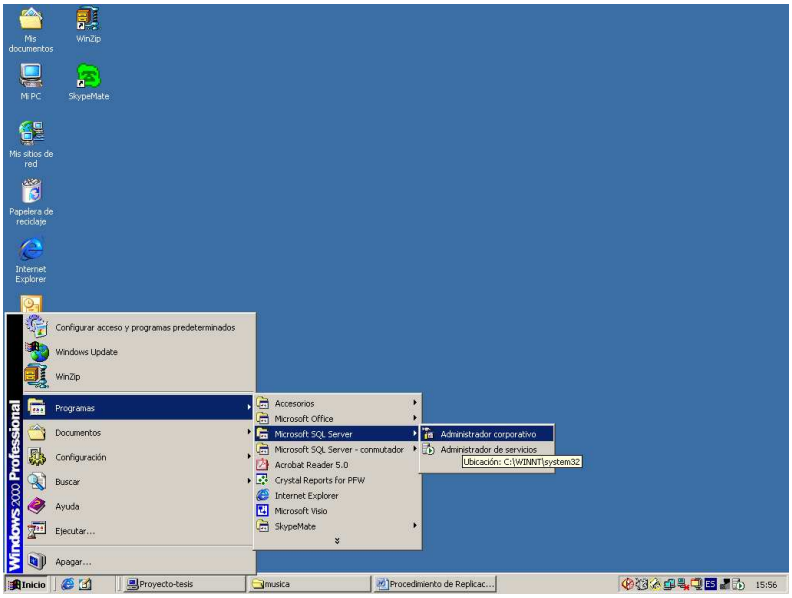

Figura 4.56: Ubicación del administrador corporativo del SQL Server.

2. Seleccionar el servidor que va ser de publicador y suscriptor.

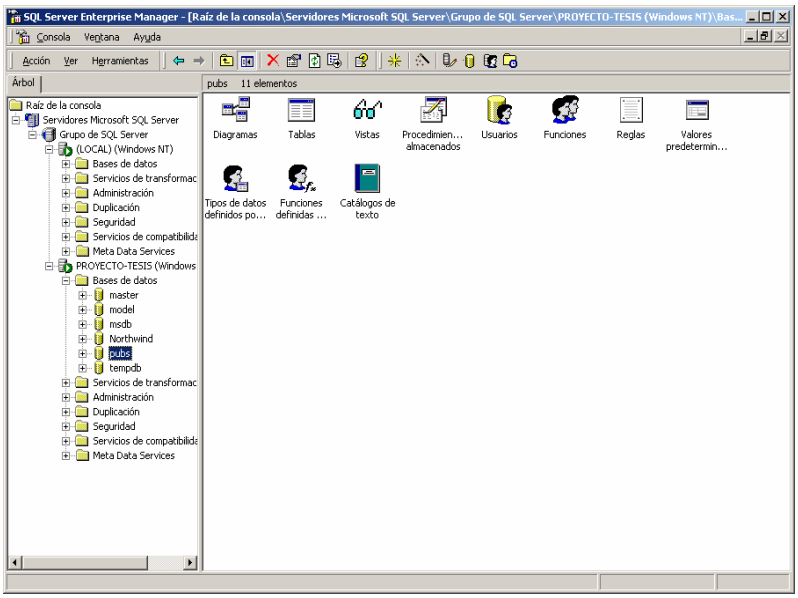

Figura 4.57: Selección del servidor como publicador

3. Hacer clic en herramientas/replicación/crear y administrar publicaciones.
4. Clic en crear publicación.

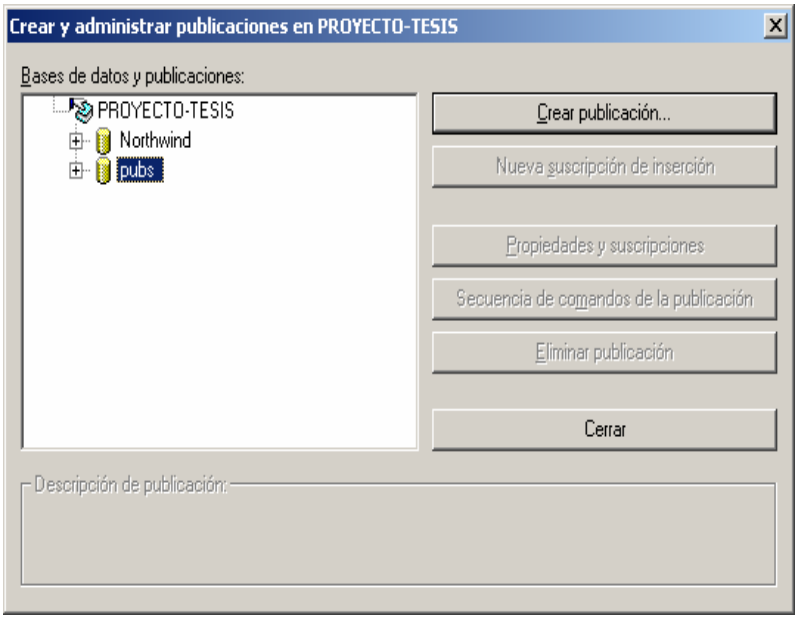

Figura 4.58: Pantalla donde se inicia la configuración de la publicación

5. La siguiente pantalla muestra el asistente para empezar a configurar la replicación. Clic en siguiente.

Figura 4.59: Asistente para configurar la publicación

6. En esta pantalla se escoge el servidor que será distribuidor, para este caso es “PROYECTO-TESIS”.

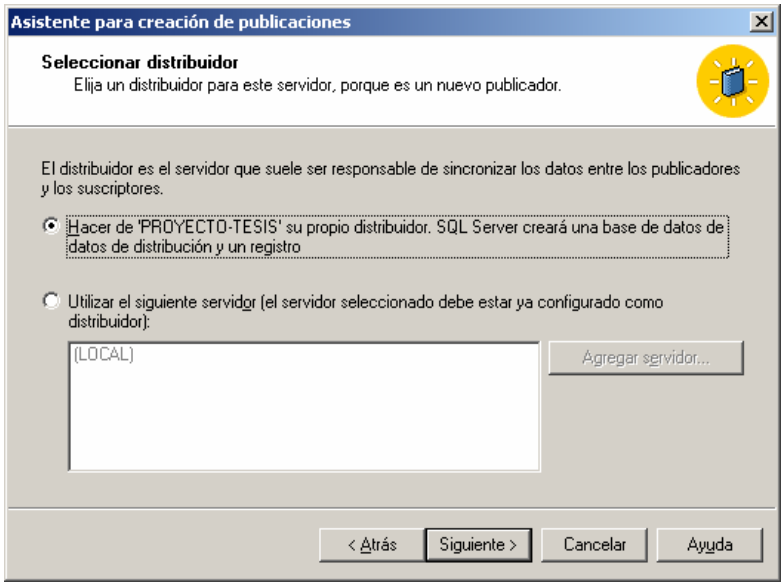

Figura 4.60: Selección de servidor como distribuidor.

7. El asistente permitirá elegir la ubicación de la carpeta en la que se almacenarán las instantáneas (copia de los artículos publicados). Clic en siguiente.

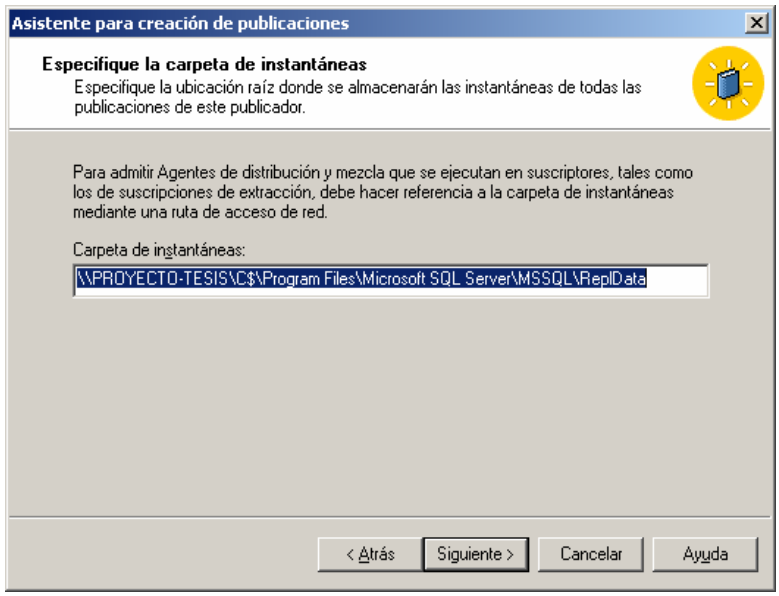

Figura 4.61: Ubicación de las carpetas de instantáneas.

8. Se elige la base de datos que va a ser publicada

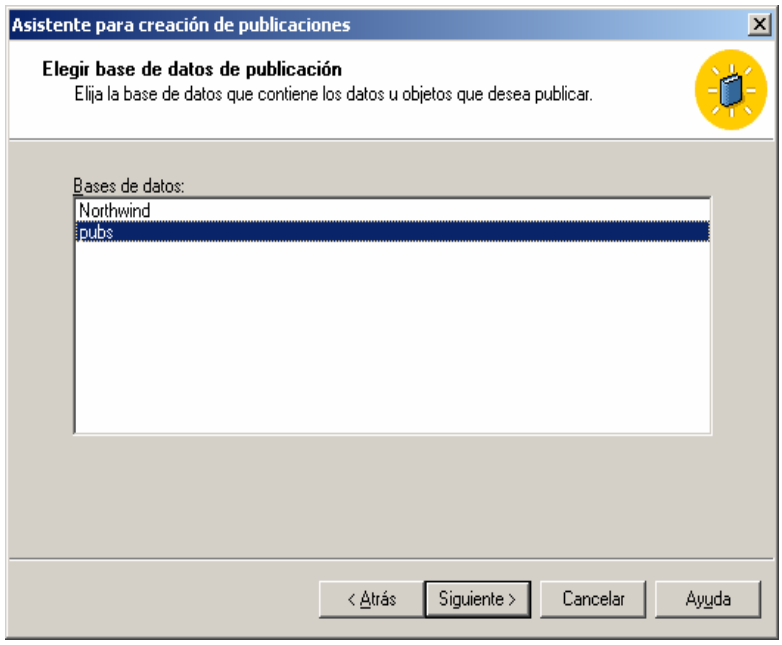

Figura 4.62: Selección de la base de datos a publicar.

9. Se elige el tipo de publicación (Publicación Transaccional)

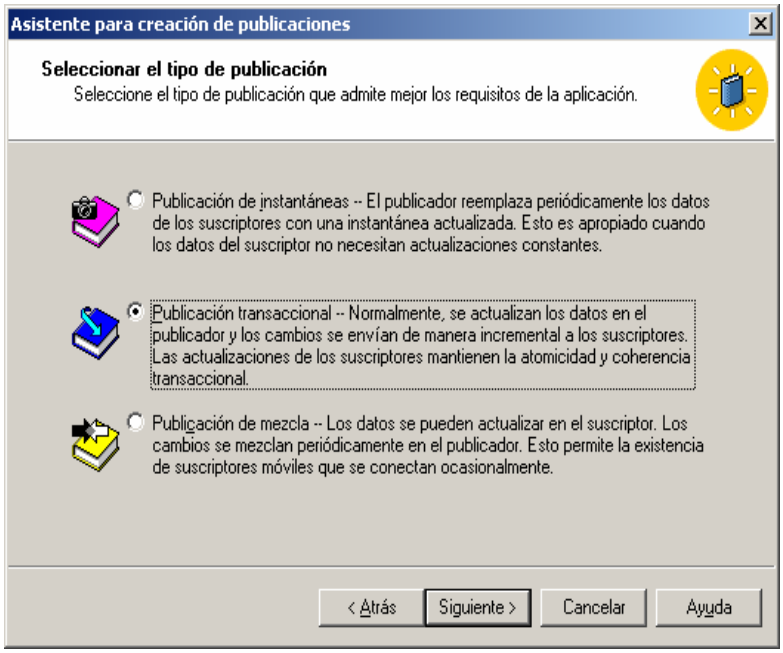

Figura 4.63: Tipo de replicación

10. Se configura la replicación en doble sentido, es decir desde el publicador al suscriptor y viceversa. Para el presente proyecto, se usará la replicación en una sola vía (del publicador al suscriptor) por lo que no se escoge ninguna de estas opciones. Clic en siguiente.

11. No se necesita de transformación de datos, el suscriptor recibe los datos directamente. Clic en siguiente.

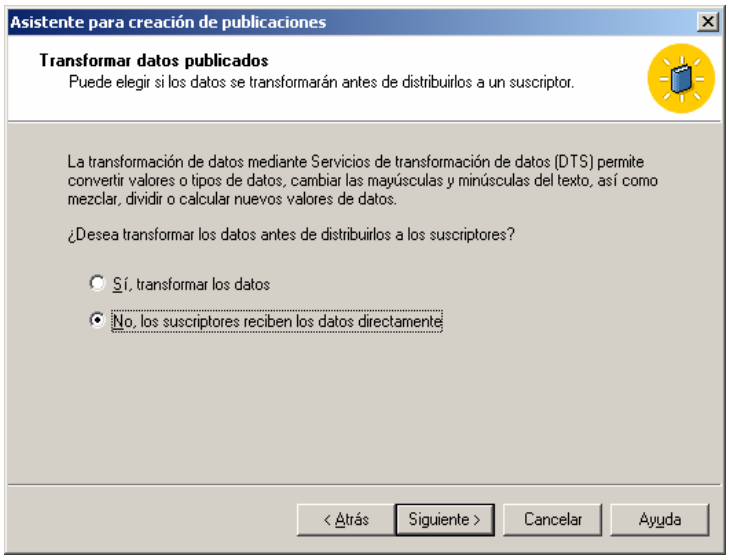

Figura 4.64: Configuración de transformación de datos.

12. Se escoge el tipo de suscriptor. Para este caso, solo se trabajará con SQL Server 2000. Clic en siguiente.

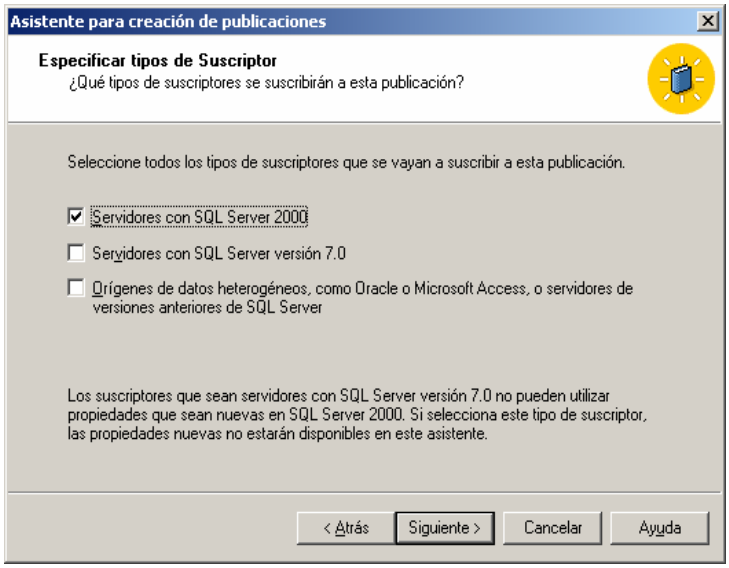

Figura 4.65: Selección de tipo de suscriptores.

13. Se especifican los artículos a publicar, pudiendo ser tablas, procedimientos almacenados o vistas. Para este caso, se utilizarán solo tablas. Clic en siguiente.

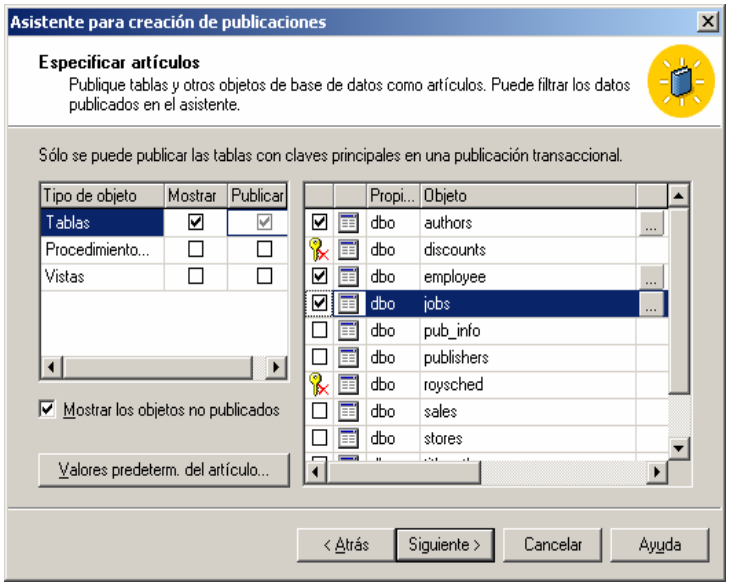

Figura 4.66: Selección de artículos a publicar.

14. Se da un nombre y descripción a la publicación. Clic en siguiente.

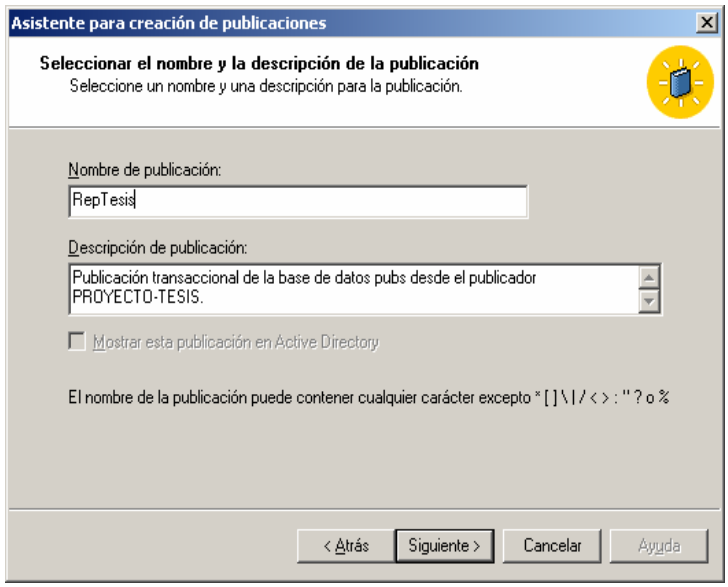

Figura 4.67: Nombre de la publicación.

15. Se escoge la opción *"No, crear la publicación como se especifica"*, ya para este proyecto no se va hacer uso de filtros. Clic en siguiente.

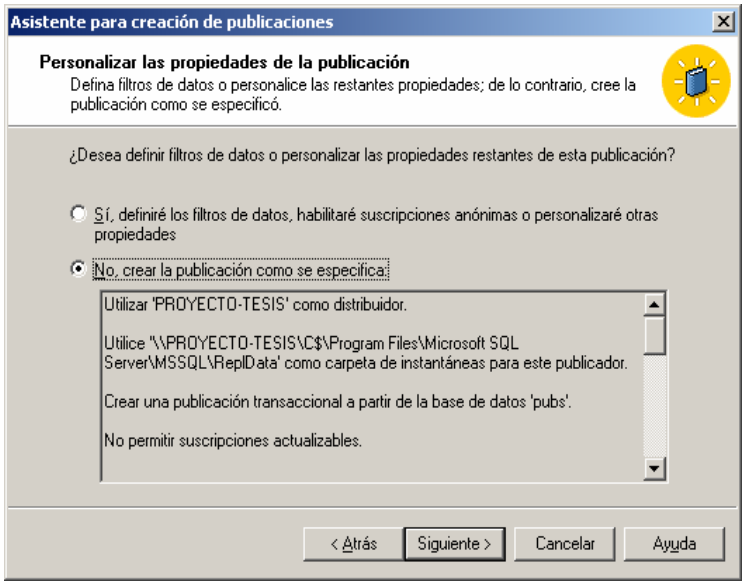

Figura 4.68: Crear la publicación como se especifica.

16. Hacer clic en finalizar. Luego de esto, el asistente muestra el proceso y la culminación exitosa de la creación del publicador. Tal como se indica en las siguientes pantallas.

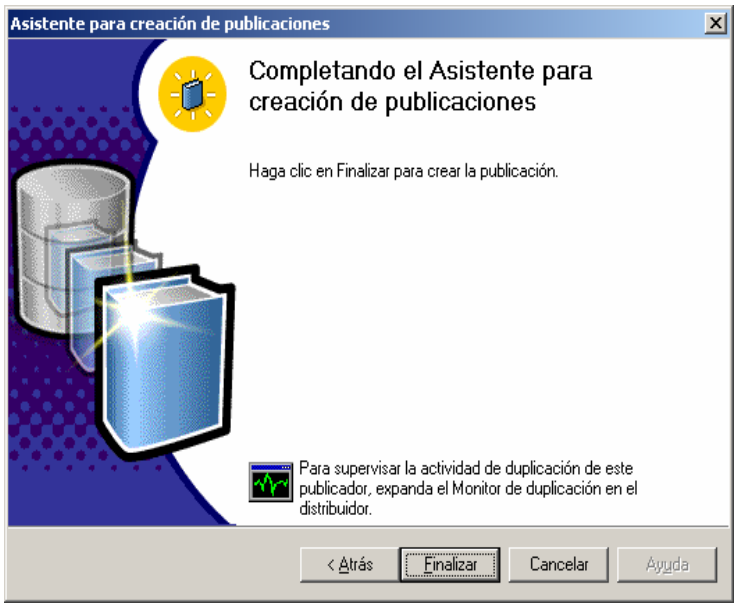

Figura 4.69: Finalización del asistente.

17. En la siguiente pantalla se observa que el publicador está listo para empezar a recibir suscriptores. Clic en Nueva suscripción de inserción.

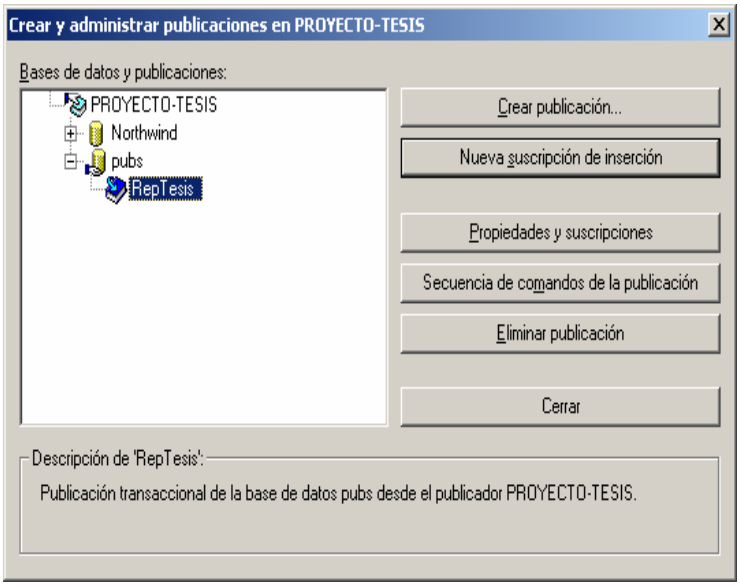

Figura 4.70: Creación de suscriptores.

Para la configuración de suscriptor se creo una base de datos llamada “tesis”, en donde se guardarán las duplicaciones.

18. La siguiente pantalla se la obtiene de la opción indicada en el paso 17 y muestra el asistente para iniciar la configuración del suscriptor. Clic en siguiente.

Figura 4.71: Asistente de suscripción.

19. Se elige el equipo que va hacer de suscriptor, para este caso “EQUIPO1”. Clic en siguiente.

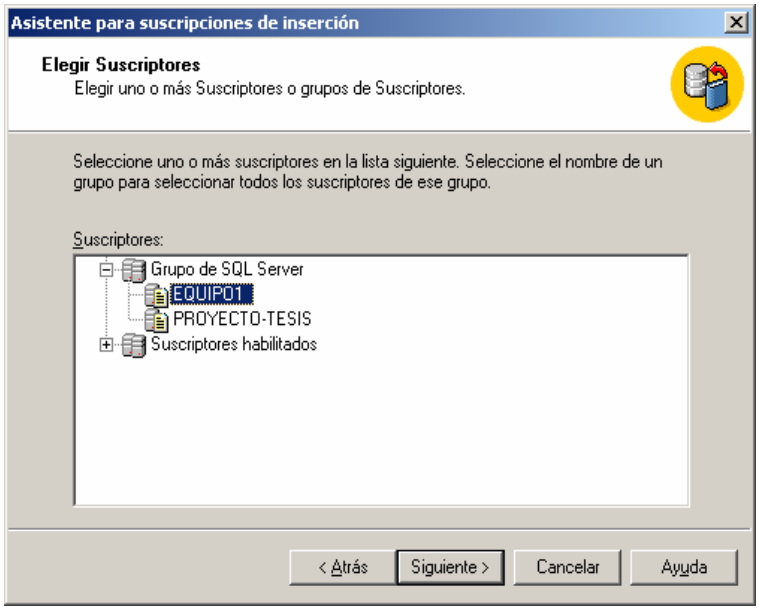

Figura 4.72: Selección de equipo como suscriptor.

20. Se elige la base de datos en donde se va a guardar la información replicada en el suscriptor. Para este caso es “tesis”. Tal como se muestra en la siguiente gráfica.

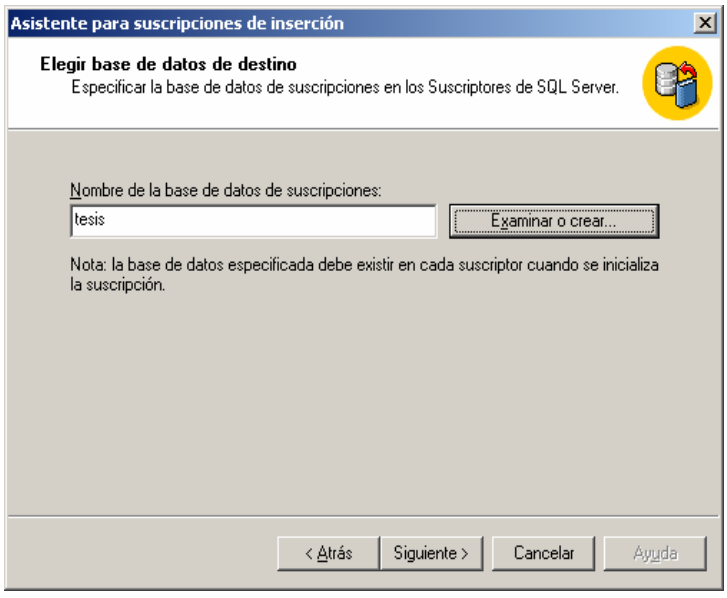

Figura 4.73: Selección de base datos de destino.

21. En la siguiente pantalla, se configura la frecuencia con la que se van a actualizar las replicas en los suscriptores. En este caso se elige actualizaciones continuas. Clic en siguiente.

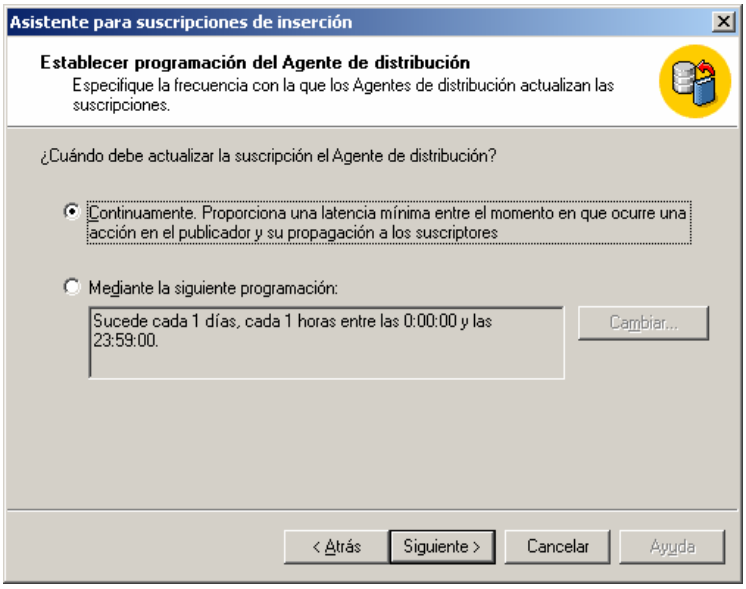

Figura 4.74: Selección la frecuencia de actualización.

22. En la siguiente pantalla se escoge la opción "*Si, inicializar el esquema y los datos",* debido a que la base "tesis" en el suscriptor no tiene ningún esquema, ni datos.

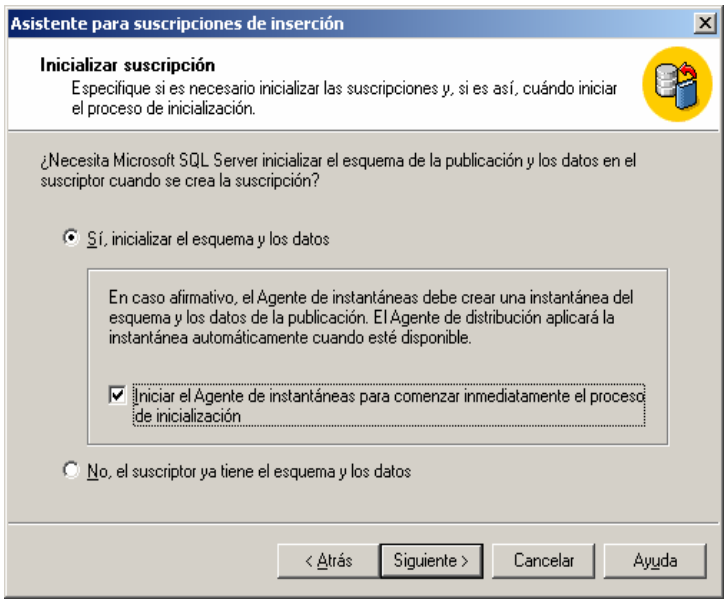

Figura 4.75: Inicializar el esquema de datos.

23. El asistente, pide inicializar los servicios requeridos para inicializar la replicación. Clic en siguiente.

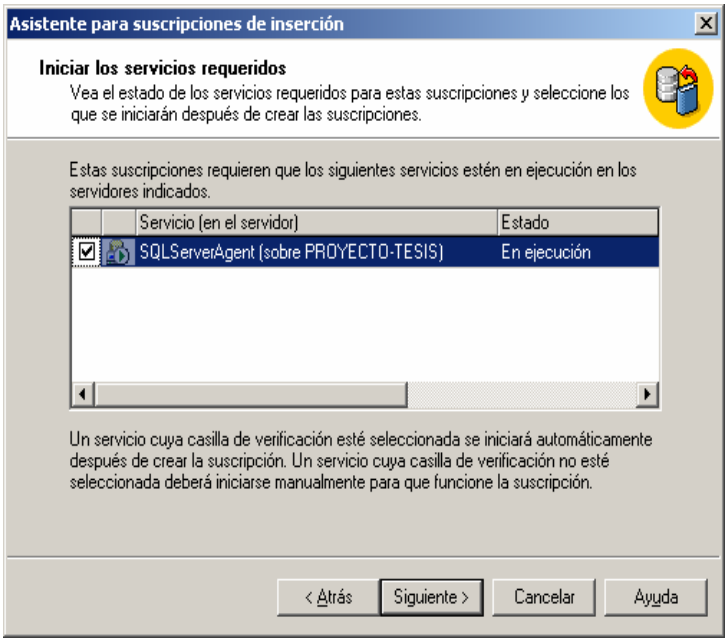

Figura 4.76: Inicializar servicios requeridos.

24. Clic en finalizar.

Figura 4.77: Finalización de la configuración

4.2.2.4 Análisis de Resultados

4.2.2.4.1 Resultados obtenidos en la replicación de datos

El propósito de los túneles VPN, configurados en el prototipo, independientemente de la tecnología que se utilizo para su implementación, es la interconexión de las bases de datos de las fincas con la matriz, de tal forma que si en las fincas realizan alguna modificación a los artículos publicados, estos cambios se reflejarán inmediatamente en la base del servidor configurado como suscriptor.

Como se muestra en el figura 4.78 del presente capítulo, en el prototipo se implementó un publicador y un suscriptor para simular la solución al problema de la empresa, que es la actualización de la información en la Matriz, se inserto varias filas en la tabla *authors (con esto se simula la modificación de la información en las fincas)* de la base de datos PUBS en el publicador, estos cambios se reflejan en la base de datos del suscriptor *(Con esto se simula la actualización de la información en la matriz)* en la tabla ***authors*** de la base de datos denominada TESIS, para esto se ejecuto las siguientes sentencias, que insertan los registros en la tabla. Para verificar la replicación se inserto cinco registros tal como se indica en las siguientes instrucciones SQL:

```
INSERT authors (au_id, au_lname, au_fname,
                phone, address, city, state, zip, contract)
VALUES ('445-45-9865', 'Tesis', 'Informatica',
        '360 379-3011', '214 la Florida', 'Quito', 'EC', '98688', 1 )

INSERT authors (au_id, au_lname, au_fname,
                phone, address, city, state, zip, contract)
VALUES ('445-45-9864', 'Washington', 'Sinchiguano',
        '360 379-3071', '211 la Florida', 'Manta', 'EC', '98689', 1 )

INSERT authors (au_id, au_lname, au_fname,
                phone, address, city, state, zip, contract)
```

```
VALUES ('445-45-9866', 'Edwin', 'Usiña',
        '360 379-3071', '211 la Florida', 'Cuenca', 'EC', '98690', 1 )

INSERT authors (au_id, au_lname, au_fname,
                phone, address, city, state, zip, contract)
VALUES ('445-45-9867', 'Eduardo', 'Panchi',
        '360 379-3071', '211 la Florida', 'Latacunga', 'EC', '98691', 1 )

INSERT authors (au_id, au_lname, au_fname,
                phone, address, city, state, zip, contract)
VALUES ('445-45-9868', 'Vinicio', 'Tocain',
        '360 379-3071', '211 la Florida', 'Ibarra', 'EC', '98692', 1 )

INSERT authors (au_id, au_lname, au_fname,
                phone, address, city, state, zip, contract)
VALUES ('445-45-9869', 'Manuelito', 'Andrade',
        '360 379-3071', '211 la Florida', 'Ambatp', 'EC', '98693', 1 )
```

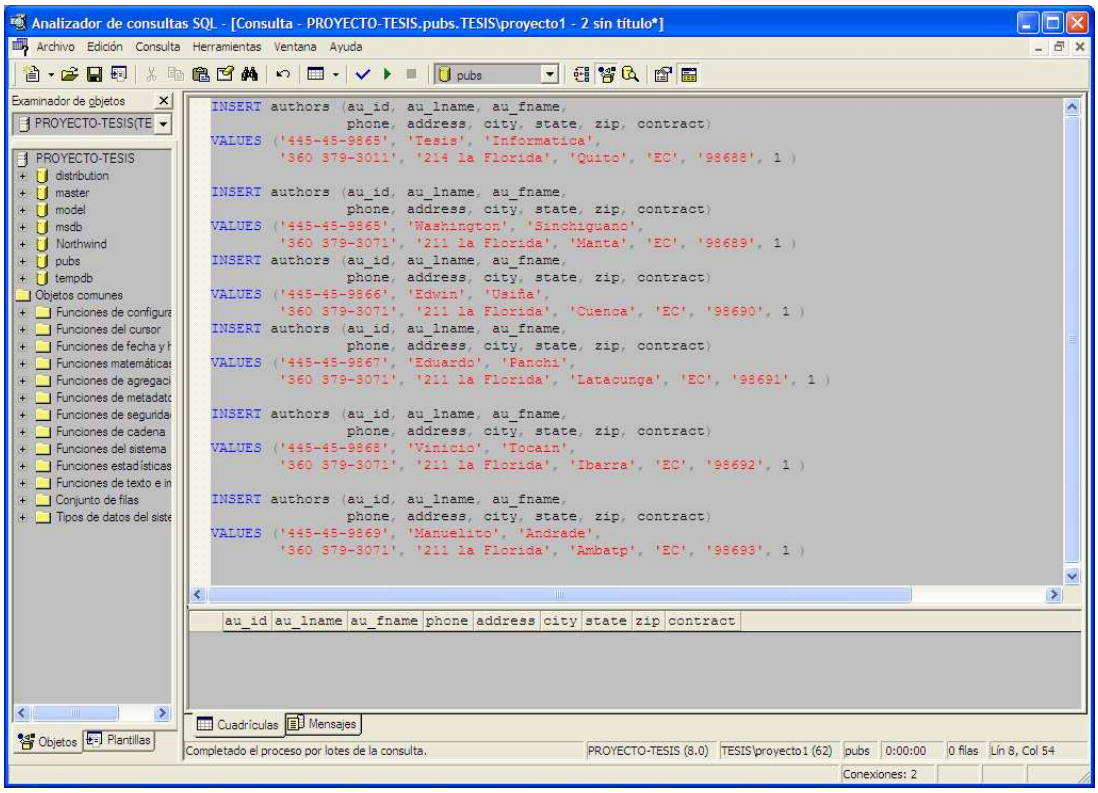

Figura 4.78: Datos insertados en la base del publicador.

Resultados de la sentencia ***select*** en el suscriptor, con esto se comprueba que los cambios hechos en la base de datos del publicador se reflejan al suscriptor a través del túnel VPN.

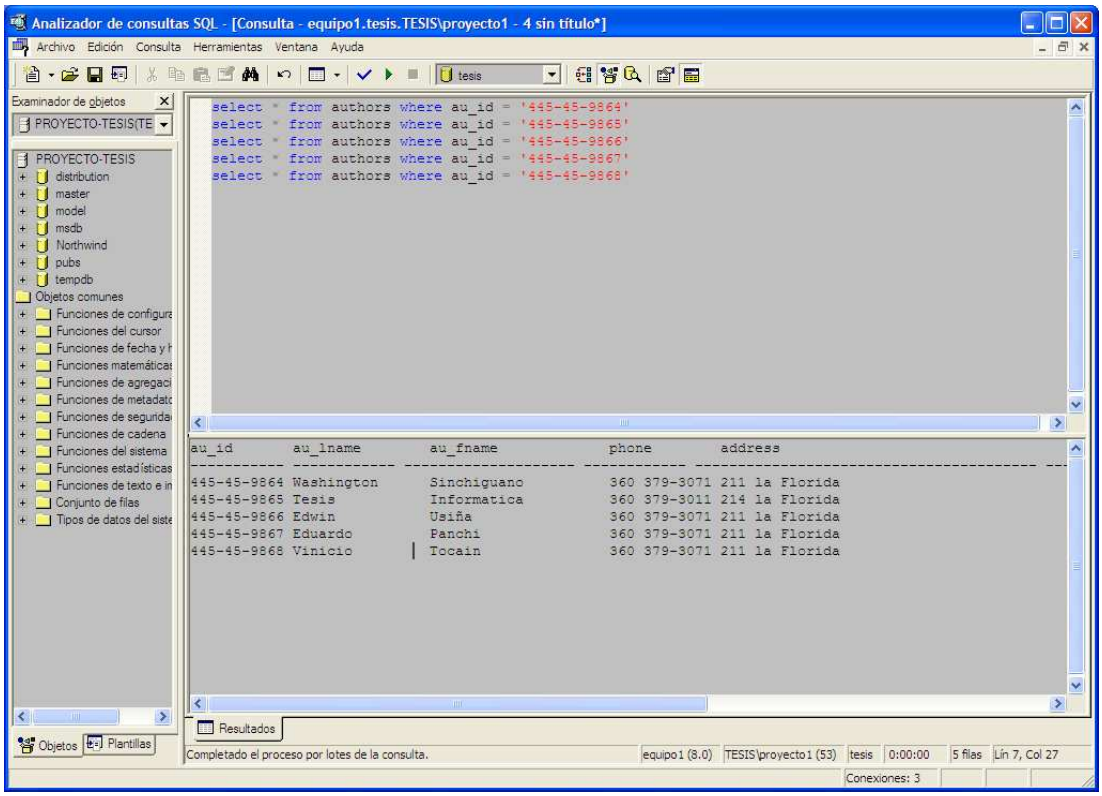

Figura 4.79: Datos replicados en la base del suscriptor.

4.2.2.4.2 Resultados Obtenidos con Software (IPSec bajo Linux).

- El proceso de configuración e implementación de la VPN mediante Software, requiere conocimientos de Linux, ya que se necesita compilar el Kernel y editar los archivos de configuración.

- Al momento de empezar la transmisión se establece el intercambio de claves y es por eso que existen pérdidas de paquetes en ese instante, luego de terminado este proceso, la comunicación y transmisión de los paquetes son normales.

- Para replicación de las bases de datos y más servicios que se envíen través del Internet, se debe tener muy en cuenta que la velocidad de transmisión a través del túnel VPN, va a depender del nivel de congestión que exista en la red (Internet).

- El túnel VPN con IPSec bajo Linux, permite un mejor control de tráfico y visualización de los paquetes que viajan encriptados a través la VPN. Con lo que se pede monitorear si el tráfico que se tiene, cumple con los niveles de seguridad preestablecidos.

- La opción con software, permite un control y administración con lo referente al tamaño de las claves; privada y pública.

- La VPN con software, es mucho más robusta en lo que respecta a los niveles de seguridad que se pueden implementar, como son los protocolos de autenticación e integridad. Pudiéndose usar certificados digitales como un nivel de seguridad extra.

- La VPN con IPSec bajo Linux, es una solución y una alternativa que permite establecer túneles seguros y a bajo costo, pues este sistema operativo es de libre distribución y vienen incorporadas en el kernel muchas funcionalidades que otros sistemas operativos necesitan licencias para su correcto funcionamiento.

4.2.2.4.3 Resultados Obtenidos con Hardware (Routers D-Link DI 804-HV)

- El proceso de configuración de los routers D-Link, es muy fácil y sencillo, debido a la poca complejidad de estos equipos.

- Para la replicación de las bases de datos con estos equipos no generó ningún inconveniente, se tuvo un idéntico resultado a la opción con

software y como utilizan el mismo protocolo de encriptación, poseen las mismas funcionalidades básicas.

- Se debe recalcar que se escogió este equipo (router D-Link) para la implementación del prototipo por su bajo costo y para demostrar que cualquiera de las dos alternativas (software y hardware) son válidas para la implementación de un túnel VPN.

- La VPN levantada con los equipos D-Link, es muy fácil y sencilla, con lo cual se demostró que con dispositivos hardware también se puede elaborar sistemas de comunicación estables y seguros. El equipo utilizado va a depender del nivel de seguridad que se vaya a implementar.

- La velocidad de transmisión de los datos replicados a través del túnel VPN con estos equipos, van a depender exclusivamente del nivel de tráfico que se tenga en la red LAN, WAM y del Internet.

4.3 SEGURIDAD EN VPNs

En esta parte proyecto se mostrarán algunos consejos para mejorar la seguridad en una red privada virtual, tomando en consideración el esquema adoptado en el diseño y prototipo.

- ***Aggressive Mode***.- Este modo de IKE, no debe ser utilizado en conjunto con claves compartidas (PSK), ya que permitirá ataques que podrán ver y modificar de manera inadvertida el tráfico cifrado.

- ***PFS***.- Esta propiedad puede ser utilizada tanto en la etapa de IKE, como en la de transmisión de datos, y nos asegurará que cualquier clave que se pueda haber filtrado por error u obtenido por algún otro método (por ejemplo fuerza bruta), no sirva para descifrar el resto del contenido de una conexión.

- ***PSK (Pre Shared Key)***.- Las claves compartidas son un método válido de autenticación cuando sólo dos extremos la conocen, y además se utilizan claves suficientemente “fuertes”.

  Las principales desventajas que posee son: que no son seguras, por un problema de diseño, cuando se utilizan junto al “aggressive mode”, y que en el caso de ser compartidas por más de un extremo (por ejemplo, si las queremos utilizar para “usuarios remotos”), no podemos identificar cual de los “usuarios” es el que se conecta, y peor aún, si no se utiliza PFS, se corre el riesgo de que un usuario malicioso utilice la clave para ver o modificar conexiones ajenas.

- ***Firewalls***.- En la mayoría de los casos, un firewall instalado entre dos extremos que intenten comunicarse por los medios descritos en esta guía, no permitirá la conexión. Para que ésta pueda realizarse, habrá que configurarlo para que permita el paso del protocolo 50(ESP), y del puerto 500/UDP (IKE).

- Una alternativa valida y muy extendida para la autenticación especialmente en comercio electrónico, es la utilización de certificados X509. La idea de los certificados es tener una CA (Certificate Authority – Autoridad Certificadora) que actúa de “validadora” de certificados. Si un certificado (que provenga desde cualquier parte del Internet) está firmado por la CA en la que se confía, entonces se asume que este cerificado es un certificado válido.

Para ilustrar mejor la parte de certificados digitales (X509), se implementará en el prototipo con software (Linux) la autenticación mediante este método. Uno de los equipos, debe tomar el rol de CA. En este ejemplo, el gateway SERVER2 tomará esta función, y SERVER1 como un nodo remoto. De esta forma, los pasos para llevar a cabo este cometido son:

- Armar una CA (Certificate Authority).

- Generar un certificado para cada gateway.
- Firmar los certificados con la CA creada en el paso 1.

4.3.1 ARMAR UNA CA (SERVER2)

Para armar una CA es necesario utilizar el comando **openssl** para generar un certificado firmado por uno mismo (en inglés: self-signed). Este comando hace justamente esto, generando por un lado una clave privada cakey.pem y por el otro el certificado público firmado cacert.pem.

 # openssl req -x509 -newkey rsa:2048 –keyout private/cakey.pem -out cacerts/cacert.pem

El comando pregunta una serie de cosas. El único campo importante, es el “Organization Name” o “Compañía”. El mismo dato que se ingresa aquí, hay que ingresarlo a la hora de crear un requerimiento de certificado (esto es para hacer más fácil el procedimiento).

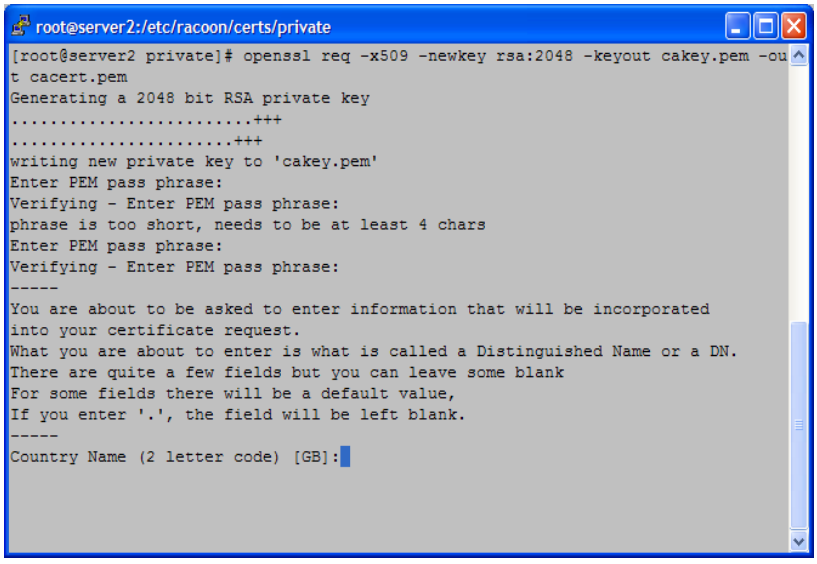

Figura 4.80: Generación de la CA.

4.3.2 GENERAR UN CERTIFICADO POR NODO

Una vez que está armado el certificado de la CA, se pueden empezar a armar los certificados de los nodos. En realidad lo que se hace, es generar un "requerimiento de certificado". Esto tiene una validez por defecto de 30 días.

Este requerimiento de certificado, es lo que se hace firmar por la CA y en el proceso de creación del requerimiento se crea la parte privada del certificado.
Este comando crea el requerimiento de certificado y su clave privada correspondiente.

 # openssl req -newkey rsa:1024 -keyout private/KeySrv2.pem -out Srv2Req.pem

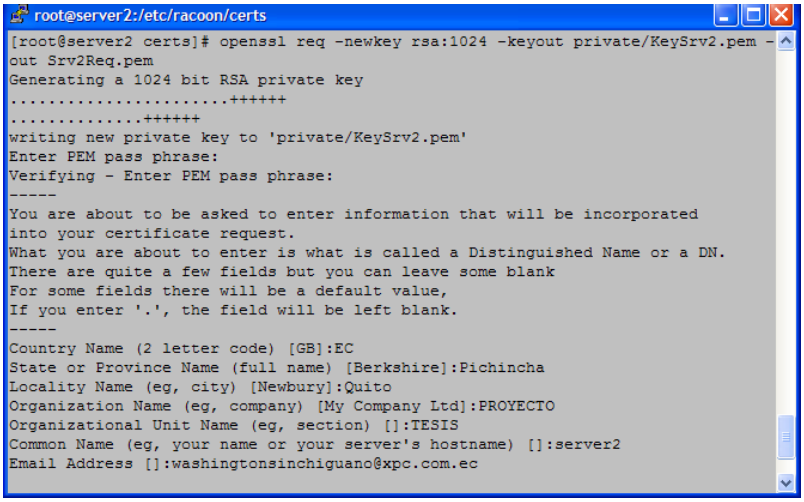

Figura 4.81: Generación del requerimiento del certificado

Este comando formula una serie de preguntas. La más importante para mantener las cosas simples, es la pregunta de "Organization Name" (Nombre de la Organización). En el prototipo, es importante ponerle lo mismo que se ha puesto al armar el certificado de la CA.

4.3.3 FIRMAR LOS CERTIFICADOS

Antes de firmar los requerimientos de certificado con la CA se deben hacer algunos ajustes.

Se copia el archivo /usr/share/ssl/openssl.cnf al directorio /etc/racoon. Hay que editar este archivo y cambiar la variable “dir” bajo la sección “[CA_default]”. Se debe reemplazar la cadena “./demoCA” por “./” únicamente; y también hay que cambiar la variable “certificate” y ponerle el valor “$dir/cacerts/cacert.pem”. Por último se deberá crear un archivo vacío llamado index.txt en el directorio /etc/racoon y crear otro archivo, llamado serial con el número 01 en su interior.

Con estos ajustes se está listo para firmar los requerimientos de certificados. El siguiente, es el comando que se utiliza.

 # openssl ca -in Srv2Req.pem -out CertSrv2Signed.pem -notext -config ./openssl.cnf

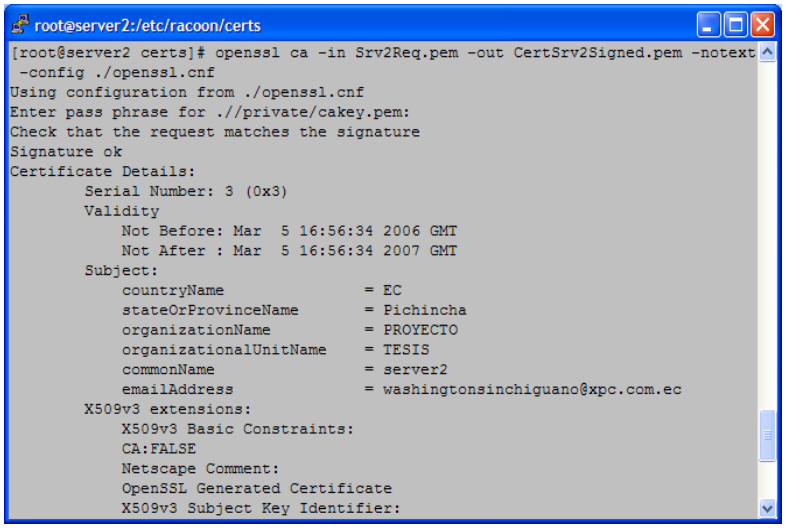

Figura 4.82: Firma del requerimiento de certificado

Una vez que los requerimientos de certificados están firmados (por lo tanto ya se los considera “un certificado”), se establece la comunicación.

Para generar el requerimiento de certificado para el nodo (SERVER1), se ejecuta el requerimiento de cerificado en el concentrador o en el nodo. En este caso, se genera el requerimiento en el nodo y se copia al concentrador. Aquí, se firma el certificado y se regresa al nodo un certificado firmado.

 # openssl req -newkey rsa:1024 -keyout private/KeySrv1.pem -out Srv1Req.pem

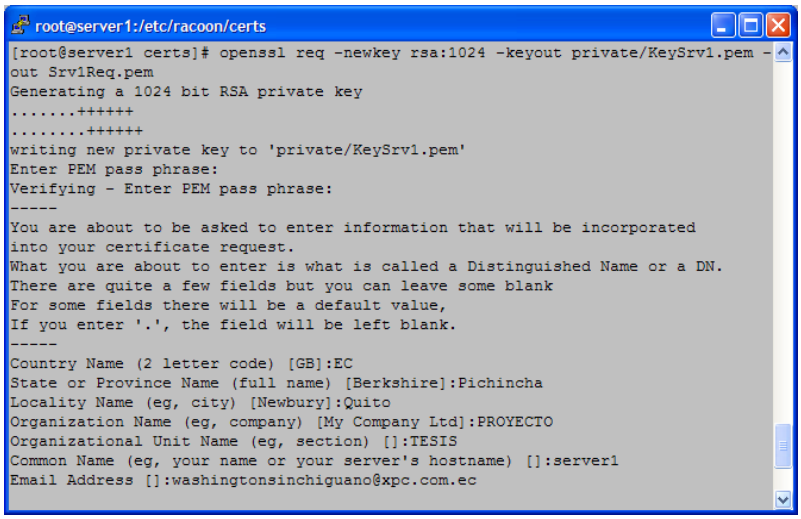

Figura 4.83: Requerimiento de certificado del nodo

en el concentrador :

 # openssl ca -in Srv1Req.pem -out CertSrv1Signed.pem -notext -config ./openssl.cnf

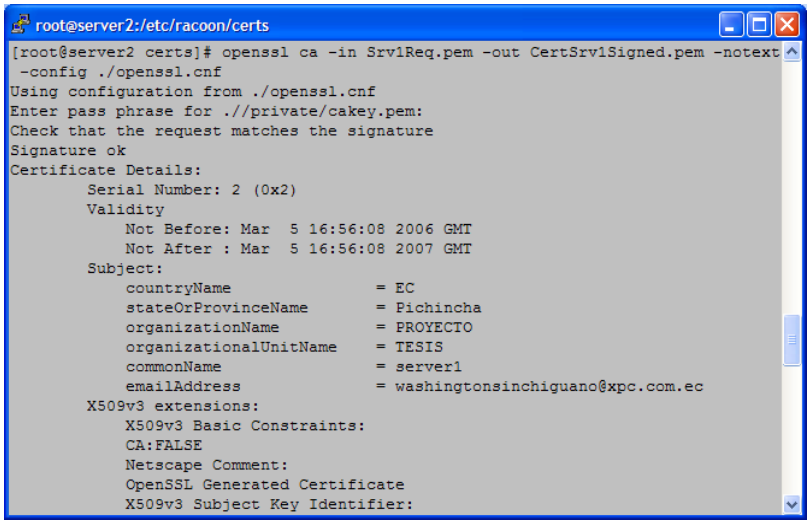

Figura 4.84: Firma del requerimiento de certificado del nodo.

Finalmente, se edita el archivo de configuración de racoon para que maneje la autenticación con este método. El archivo de configuración queda de la siguiente forma:

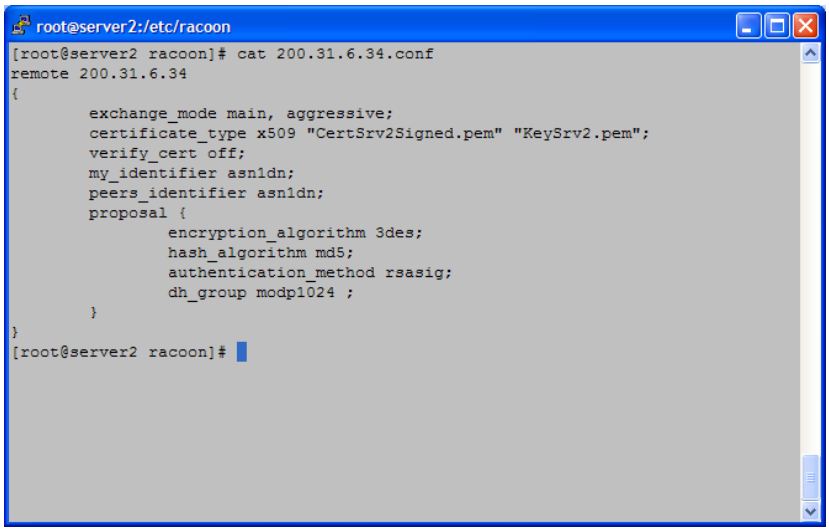

Figura 4.85: Archivo de configuración de SERVER2

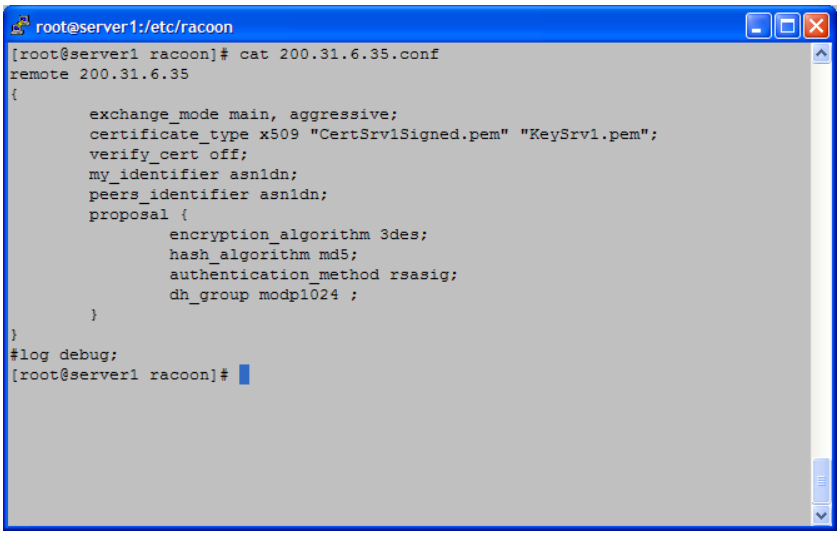

Figura 4.86: Archivo de configuración de SERVER1

CAPITULO 5

5. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Las redes privadas virtuales (VPNs), ofrecen una alternativa económica y viable en empresas que necesitan mantener interconectadas las sucursales con la matriz a través de infraestructura pública como lo es el Internet.

- Debido a que la información viaja a través de un medio público, la criptografía juega un papel importante en la tecnología de las VPNs, es por esta razón que se debe analizar los algoritmos criptográficos que se utilizarán para implementar la VPN, especialmente para garantizar la integridad y confidencialidad de los datos.

- Muchas empresas tienen accesos a Internet en todas las sucursales y por desconocimiento o falta de información sobre VPNs, no aprovechan este recurso accesible, económico y fácil de implementar.

- El protocolo IPSec esta incluido de facto en IPv6 y es el estándar en las tecnologías VPN tanto en hardware como en software, siendo éste el principal protocolo para la implementación de túneles VPN.

- La gran ventaja de IPSec es la opción de poder combinar dos protocolos, AH y ESP, para proteger el paquete IP, el primero es utilizado en modo transporte con lo que se protege únicamente la cabecera IP y el segundo en modo túnel que protege íntegramente el paquete IP.

- Actualmente la replicación de la base de datos se realiza manualmente, esto toma de 3 a 4 horas y mucho tiempo más si existen inconsistencias en las tablas sujetas de replicación. Con las VPN se pretende que este tiempo se aproveche en otras actividades productivas para la empresa como mejoras en los sistemas, implementación de seguridades en la red, implementación de políticas de acceso a Internet, inventarios de hardware y software, etc.

- En varias ocasiones, la empresa ha sufrido retardos en la actualización de la información debido a la perdida o daños producidos en las cintas magnéticas. Con la VPNs se pretende eliminar estos inconvenientes adicionando un nivel de seguridad más alto que una cinta.

- La utilización de equipos en los cuales esta instalado el sistema operativo Linux, para la implementación de una VPN, es una alternativa viable por su bajo costo y por ser un software muy difundido y de libre acceso.

- El MRTG es una herramienta eficaz al momento de tomar muestras de tráfico de red, se sabe que con las configuraciones adecuadas, a mas de censar el tráfico, se puede medir la carga de una CPU, tiempo de acceso a disco, paginas visitadas en servidor Web, etc.

- Por cuestiones de seguridad, en los Gateways IPSec se debe habilitar únicamente los puertos necesarios indicando la dirección IP o red de destino, dirección IP o red de origen, protocolo (TCP, UDP), interfaz (eth0, eth1).

- Existen en el mercado equipos diseñados para interconectar sitios mediante túneles VPN, económicos y accesibles.

5.2 RECOMENDACIONES

- Si a futuro se desea implementar VoIP y Video Conferencia, se recomienda realizar pruebas del consumo de ancho de banda previo a la implementación de estos servicios, para poder determinar la necesidad de mantener o aumentar el ancho de banda actual.

- Luego de implementar la VPN en al empresa florícola, se recomienda instalar el servicio de MRTG para medir el tráfico producido por los enlaces VPN, de esta forma se puede determinar si es necesario aumentar, disminuir o mantener el ancho de banda de los enlaces a Internet.

- En el proceso de replicación de la base de datos se recomienda mantener un historial de las transacciones, con lo cual se puede establecer un mejor control en el número de transacciones diarias que se tienen en las bases de datos.

- La versión de Linux que se utiliza en la empresa florícola es freeware (libre distribución), razón por la cual las actualizaciones no pueden ser obtenidas de forma inmediata, generando un agujero de seguridad. Se recomienda adquirir un versión de Linux con licencia, como Red Hat Entrerprise 4.0 o superiores.

- Se recomienda realizar un upgrade a todos los servidores y estaciones de trabajo en cuanto al Hardware (Tamaño de Discos duros) y Software (Aplicaciones y Sistemas Operativos). El tamaño de los discos duros son muy pequeños y tarde o temprano colapsarán.

6. REFERENCIAS BIBLIOGRAFICAS

- Murhammer, Martín W; Bourne, Tim A.; GAIDOSH, Tamas; A guide to virtual private networks. Primera ediciòn. 1998.

- Andrew G. Mason, CCIE 7144; Redes Privadas Virtuales de Cisco Secure.

- Ivan Pepelnjak, CCIE; Jim Guichard, CCIE Arquitecturas MPLS y VPN.

- Albert Delgado ; Edición Especial SQL Server 2000: Pearson Educación. S.A Madrid 2001.

- Thomas Lee; Joseph Davies; Windows 2000 TCP/IP Protocolos Y Servicios; Referencia Técnica.

INTERNET:

- Virtual Private Networks (VPN) – Monografías.com http://www.monografías.com/trabajos12/monvpn/monvpn.shtml.

- VPN Technologies: Definitions and Requirements http://www.vpnc.org/vpn-technologies.html último acceso 31/03/2005

- IPsec, Security for the Internet Protocol http://www.freeswan.org/freeswan_trees/freeswan-2.06/doc/intro.html último acceso 31/03/2005

- IP Security Protocol (ipsec) http://www.ietf.org/html.charters/ipsec-charter.html último acceso 31/03/2005

- RFC 2411 IP Security Document Roadmap November 1998

- RFC 2401 Security Architecture for IP November 1998
- http://www.entarasys.com/la
- http://www.cisco.com/warp/public/44/solutions/network/vpn.shtml.
- Certificados de la Autoridad Certificadora. http://www.acepta.com/ServiciosOnLine/CertificadoPersona/Buscar/BuscarCertificadosWeb.html

ANEXO A

Configuración de Triggers en SQL Server 2000

ANEXO A

CONFIGURACIÓN DE TRIGGER'S EN SQLSERVER

El script para la creación de la tabla es:

```
CREATE TABLE [dbo].[AUDIT] (
        [id_evento] [int] IDENTITY (1, 1) NOT NULL ,
        [tipo_evento] [char] (10) NOT NULL ,
        [fecha] [datetime] NOT NULL ,
        [descripcion] [char] (50)  NULL ,
        [usuario] [char] (30)  NULL ,
        [terminal] [char] (30)  NULL ,
        [aplicacion] [char] (30)  NULL
) ON [PRIMARY]
GO

ALTER TABLE [dbo].[AUDIT] WITH NOCHECK ADD
        CONSTRAINT [PK_AUDIT] PRIMARY KEY  NONCLUSTERED
        (
                [id_evento]
        )  ON [PRIMARY]
GO
```

El script para la creación del trigger es:

```
CREATE TRIGGER AUDITdel ON PRODUCCION FOR DELETE
AS
Insert into AUDIT
select "Delete", getdate(), "Eliminacion de un registro", SYSTEM_USER,
host_name(),APP_NAME()

CREATE TRIGGER AUDITins ON PRODUCCION FOR INSERT
AS
insert into AUDIT
select "Insert", getdate(), "Insercion de un registro", SYSTEM_USER,
host_name(),APP_NAME()

CREATE TRIGGER AUDITdel ON PRODUCCION FOR UPDATE
AS
insert into AUDIT
select "Update", getdate(), "Modificacion de un registro", SYSTEM_USER,
host_name(),APP_NAME()
```

ANEXO B

Configuración de tareas en SQL Server 2000

ANEXO B

CONFIGURACIÓN DE TAREAS EN SQLSERVER

FINCA1

INSERT

```
--script q inserta filas a la tabla sujeta de replicación
--en el servidor de las fincas
declare @rand float
declare @str varchar (15)
declare @uno varchar (3)
declare @dos varchar (2)
declare @tres varchar (4)
declare @id varchar (11)
declare @bandera int
declare @numeroInsert int

set @bandera = 1
set @numeroInsert = 1

while @numeroInsert < 898
begin
set @bandera = 1
        while @bandera  = 1
        begin
                set @rand = rand()
                set @str = rtrim(ltrim(cast(@rand as varchar(15))))
                set @uno = right(@str, 3)

                set @rand = rand()
                set @str = rtrim(ltrim(cast(@rand as varchar(15))))
                set @dos = right(@str, 2)

                set @rand = rand()
                set @str = rtrim(ltrim(cast(@rand as varchar(15))))
                set @tres = right(@str, 4)
                set @id = @uno + '-' + @dos + '-' + @tres

                if not exists (select au_id from authors where  au_id = @id)
                begin
                        INSERT authors (au_id, au_lname, au_fname, phone, address, city,
state, zip, contract)
                        VALUES (@id, 'Eduardo', 'edwin', '360 379-3071', '211 la Florida',
'Quito', 'EC', '98688', 1 )
                        --select @id
                         WAITFOR DELAY '00:00:00.05'
                        set @bandera = 0
                end
        end
```

```
        set @numeroInsert = @numeroInsert + 1
end
--select count (*) from authors
```

UPDATE

```
--script q borra filas a la tabla sujeta de replicación
--en el servidor de las fincas

declare @id varchar(15)
declare @rand varchar(15)
declare @NumAl varchar(15)
declare @str varchar(15)
declare @i int
set @i = 1

while @i < 272
begin
        set @rand = rand()
        set @str = rtrim(ltrim(cast(@rand as varchar(15))))
        set @NumAl = right(@str, 2)
        set @NumAl = '%' + @NumAl  + '%'
        set @id = rtrim(ltrim((select top 1 au_id from authors where au_id like @NumAl)))
        update authors set  au_lname = 'Washington', au_fname = 'Vinicio', phone = '120
222-3072', address = '315 La Colmena', city = 'Ambato', state = 'EC', zip = '12345',
contract = 1 where au_id = @id
        set @i = 1 + @i
         WAITFOR DELAY '00:00:00.15'
        --select * from authors where au_id = @id
End
```

DELETE

```
--script q borra filas a la tabla sujeta de replicación
--en el servidor de las fincas

declare @id varchar(11)
declare @i int
set @i = 1

while @i < 4
begin
        set @id = rtrim(ltrim((select max(au_id) from authors)))
        delete authors where au_id = @id
        set @i = 1 + @i
        WAITFOR DELAY '00:00:00.2'
--      select @id
end
```

FINCA2

INSERT

```
--script q inserta filas a la tabla sujeta de replicación
--en el servidor de las fincas
declare @rand float
declare @str varchar (15)
declare @uno varchar (3)
declare @dos varchar (2)
declare @tres varchar (4)
declare @id varchar (11)
declare @bandera int
declare @numeroInsert int

set @bandera = 1
set @numeroInsert = 1

while @numeroInsert < 751
begin
set @bandera = 1
        while @bandera  = 1
        begin
                set @rand = rand()
                set @str = rtrim(ltrim(cast(@rand as varchar(15))))
                set @uno = right(@str, 3)

                set @rand = rand()
                set @str = rtrim(ltrim(cast(@rand as varchar(15))))
                set @dos = right(@str, 2)

                set @rand = rand()
                set @str = rtrim(ltrim(cast(@rand as varchar(15))))
                set @tres = right(@str, 4)
                set @id = @uno + '-' + @dos + '-' + @tres

                if not exists (select au_id from authors where  au_id = @id)
                begin
                        INSERT authors (au_id, au_lname, au_fname, phone, address, city,
state, zip, contract)
                        VALUES (@id, 'Eduardo', 'edwin', '360 379-3071', '211 la Florida',
'Quito', 'EC', '98688', 1 )
                        --select @id
                         WAITFOR DELAY '00:00:00.05'
                        set @bandera = 0
                end
        end
        set @numeroInsert = @numeroInsert + 1
end
--select count (*) from authors
```

UPDATE

```
--script q borra filas a la tabla sujeta de replicación
--en el servidor de las fincas

declare @id varchar(15)
declare @rand varchar(15)
declare @NumAl varchar(15)
declare @str varchar(15)
declare @i int
set @i = 1

while @i < 217
begin
        set @rand = rand()
        set @str = rtrim(ltrim(cast(@rand as varchar(15))))
        set @NumAl = right(@str, 2)
        set @NumAl = '%' + @NumAl  + '%'
        set @id = rtrim(ltrim((select top 1 au_id from authors where au_id like @NumAl)))
        update authors set  au_lname = 'Washington', au_fname = 'Vinicio', phone = '120
222-3072', address = '315 La Colmena', city = 'Ambato', state = 'EC', zip = '12345',
contract = 1 where au_id = @id
        set @i = 1 + @i
         WAITFOR DELAY '00:00:00.15'
        --select * from authors where au_id = @id
End
```

DELETE

```
--script q borra filas a la tabla sujeta de replicación
--en el servidor de las fincas

declare @id varchar(11)
declare @i int
set @i = 1

while @i < 3
begin
        set @id = rtrim(ltrim((select max(au_id) from authors)))
        delete authors where au_id = @id
        set @i = 1 + @i
        WAITFOR DELAY '00:00:00.2'
--      select @id
end
```

ANEXO C

Proformas de cotizaciones de los enlaces dedicados y routers

3] Propuesta Comercial

La siguiente es nuestra propuesta económica para la implementación de la solución integral de Telecomunicaciones de la ROAD TRACK, de acuerdo con las configuraciones descritas anteriormente:

PROPUESTA DE SERVICIOS PORTADORES DE TELECOMUNICACIONES PARA ROAD TRACK

SERVICIOS PORTADORES					
DESCRIPCIÓN	**ANCHO DE BANDA**	**DESDE**	**HASTA**	**ABONO MENSUAL**	**CARGO ÚNICO DE INSTALACIÓN**
Servicio portador de telecomunicaciones para datos	2048 Kbps	Quito - Matriz Road Track (6 de Diciembre y Granados)	Carretas	$ 1500,00	$ 300,00
Servicio portador de telecomunicaciones para Internet - ADI	64 Kbps	Quito - Matriz Road Track (6 de Diciembre y Granados)	Telepuerto Impsat Quito	$ 333,00	$ 450,00
Servicio portador de telecomunicaciones para Internet - ADI	256 Kbps	Quito - Matriz Road Track (6 de Diciembre y Granados)	Telepuerto Impsat Quito	$ 800,00	$ 450,00
TOTAL				$ 2633,00	$ 1200,00

NOTAS:

- **SE DEBERÁ REALIZAR UNA INSPECCIÓN PREVIA SIN COSTO.**
- **LOS ENLACES DE INTERNET SERÁN FRAME RELAY.**
- **COMO SEGUNDA OPCIÓN, SE PODRÍA CONSIDERAR ENTREGAR SOLO UN ACCESO A 320K PARA INTERNET Y SEPARAR EL TRÁFICO DE LAS DOS APLICACIONES CON DOS PVCS INDEPENDIENTES.**

ANEXO D

Proformas y costos de la implementación de una VPN adquiriendo todos los equipos

En la siguiente tabla se muestra el costo total de la implementación con software incluido el costo del hardware necesario.

PRODUCTO (SW)	PRECIO (USD)	COSTO IMPLEMENTACION		COSTO HARDWARE (3 PC)	TOTAL
		COSTO POR SITIO (USD)	COSTO TOTAL (USD)		
Check Point	2500	200	600	1336.27	**4436**
ISA Server	3500	200	600	1336.27	**5436**
Ipsec-Tools	0	200	600	1336.27	**1936**

Glosario

Acceso - Servicio entre un punto "A" y un punto "B" que utiliza medios de comunicación tales como radio, par metálico, fibra óptica o satélite.

Acceso dedicado - Servicio entre dos puntos utilizado por un único cliente.

ADSL (Línea Asimétrica de Abonado Digital) - Línea telefónica con tasas de transmisión diferentes en ambos sentidos.

ASP (Active Server Pages) - Lenguaje para el desarrollo dinámico de contenido Web, que permite la consulta a bases de datos y el tratamiento de formularios en la Web.

ATM - Una tecnología de conmutación de células capaz de procesar datos, voz y vídeo en tiempo real. El ATM está definido en el estándar ISDN Broadband (RDSI de banda ancha) y proporciona ancho de banda bajo demanda, tarifando a los usuarios por la cantidad de datos enviados. Se puede utilizar tanto en redes de larga distancia (WANs), como en redes locales (LANs), pasando por las redes intermediarias (MANs).

BroadBand (Banda Ancha) - Conexión para transmisión de datos, voz e imágenes a alta velocidad.

Browser - Programa para buscar y recibir informaciones de la World Wide Web (Internet). Los más utilizados son el Internet Explorer y el Netscape.

Cable módem - Módem usado para conectar una computadora a un sistema de TV a cable que ofrece servicios de red.

Chat - Tipo de interacción de red, común en Internet, en muchos BBSs y otros servicios de red, en los cuales dos o más personas escriben y envían mensajes los unos para los otros, conversando en tiempo real.

Cobertura - Área atendida por el Backbone de una red de telecomunicaciones.

Data Center - Local con infraestructura para albergar servidores.

Dial Up - Tipo de conexión a un servidor ISP por línea discada o convencional.

Dominio - Nombre de una red en Internet. Este nombre es la forma más humana de direccionar a las computadoras. El dominio es traducido en direcciones IP por las computadoras y enrutadores e Internet.

E1 - Estándar para transmisión digital a alta velocidad a 2048 Kbps adoptado en Brasil y en Europa, con 32 canales de 64 Kbps disponibles para tránsito. También denominado 2 Mega.

E-3 - Estándar que representa 34 Mbps (megabits) por segundo en la transferencia de datos.

E-Commerce (Comercio Electrónico) - Automatización de las interacciones comerciales entre empresas (Business-to-Business, o B2B) o entre empresas y personas (Business-to-Consumer, o B2C) a través de la comunicación entre computadoras, usando la infraestructura de redes públicas o privadas.

E-mail (Electronic Mail ó Correo Electrónico) - Mensaje de texto enviado electrónicamente a otro usuario de la red que puede contener o no archivos anexados. Para estar operación se necesita un servidor de mensajes (Mail Server).

Encryption (Encriptar o Codificar) - Forma de transmitir datos codificados para fines de seguridad. Utilizar llaves públicas y privadas de seguridad para dificultar la acción de invasores de redes.

Extranet - Red que también utiliza el protocolo de comunicación TCP/IP, sin embargo solamente entre redes de empresas diferentes. Es típicamente el modelo de comunicación utilizado entre empresas y sus asociados de negocios.

Ethernet - Red local desarrollada por Xerox, Digital Equipment Corp. e Intel. La red Ethernet conecta hasta 1024 puntos en 10 Mbps en cable de par trenzado, coaxial y de fibras ópticas. Es un protocolo de enlace de datos.

Fibra Óptica - Compuesta básicamente por material dieléctrico (en general sílice), con una larga estructura cilíndrica, transparente y flexible, de dimensiones microscópicas, comparables a las de un cabello humano. Permite altísimas tasas de transmisión, del orden de los 1 Gbps (mil millones de bits por segundo), que dependen, sin embargo, de las limitaciones de los equipos utilizados. Es inmune a interferencias electromagnéticas externas y presenta alto grado de seguridad para la información transportada.

File and Print Sharing (Compartir Archivos e Impresoras) - Componente de red que permite a un usuario compartir archivos o impresoras de su computadora con otros integrantes de la red.

First Mile (Primera Milla) - Acceso inicial de la "puerta" del cliente a un Backbone.

Frame Relay - Red de conmutación de paquetes análogo a los estandarizados por la ITU, pero sin verificación de errores y con altas velocidades de transmisión.

FTP (File Transfer Protocol) - Conjunto de mandos usados para acceder a directorios y copiar archivos en redes Unix e Internet.

Home Page - Consiste en un conjunto de páginas, que se pueden visualizar por medio de la utilización de browsers.

Hosting (Hosting) - Arrendamiento de un servidor dedicado o de un espacio en un servidor (compartido).

HTML (Hyper Text Markup Language) - Estándar para la definición de documentos con vínculos de hipertexto. Lenguaje utilizado para crear y exhibir documentos en la Web.

HTTP (Hyper Text Transfer Protocol) - Estándar para el intercambio de archivos (texto, gráficos y multimedia) a través de Internet. Protocolo cliente-servidor.

HTTPS (Hyper Text Transfer Protocol Secure) - Ampliación del HTTP desarrollado por Netscape para ofrecer seguridad en sitios Web.

Hub Nodes (Hubs) - Más conocidos como "hubs", tienen la función de servir como punto de concentración y de conmutación para redes de banda ancha fija por cable e inalámbricas.

IIS (Internet Information Server) - Sistema Servidor Web y FTP de alto desempeño nativo en el ambiente Windows NT, desarrollado por Microsoft.

IMAP (Internet Mail Access Protocol) - Protocolo avanzado para consulta de sistemas de correo electrónico en Internet.

Internet - Red mundial de computadoras interconectadas entre sí a través del protocolo TCP/IP.

Intranet - Es una red que utiliza el protocolo de comunicación TCP/IP en ambientes internos, o sea, solamente puede ser accedido dentro de la empresa o externamente por personas autorizadas.

IP (Internet Protocol) - Protocolo de conexión utilizado en Internet. El IP enruta mensajes a través de las redes.

IP Address (Dirección del Protocolo Internet) - Número que identifica a una computadora en Internet. Ese número es exclusivo.

IP Config - Utilidad de prompt de comando del Windows NT que exhibe la configuración de TCP/IP de la computadora.

IP Network - Red basada en una familia de protocolos que rastrean la dirección de Internet de los nudos, hacen el enrutamiento de mensajes de salida y reconocen mensajes de entrada.

ISP (Internet Service Provider) - Proveedor de servicios para Internet, que sirve tanto a usuarios domésticos como corporativos.

LAN (Local Area Network) - Red formada por computadoras localizadas en el mismo espacio físico, como una sala o un edificio.

Last Mile (Última Milla) - Acceso del backbone al punto final del circuito.

Link - Circuito de comunicación o vía de transmisión que conecta a dos puntos.

LP - Línea privada de datos. Punto a punto o punto a multipunto.

MAN (Metropolitan Area Network) - Interconecta varias redes dentro de una misma área metropolitana.

Módem - Dispositivo de hardware que conecta una computadora con un servicio de comunicación, generalmente un teléfono o cable. El módem adapta las señales digitales de la computadora para señales de áudio de la línea Telefónica y viceversa.

NetBEUI (NetBIOS Extended User Interface o Interfaz de Usuario Ampliada NetBIOS) - Versión perfeccionada del NetBIOS, protocolo de red utilizado para la comunicación entre computadoras conectadas a una red LAN.

NIC (Network Interface Card o Placa de Interfaz de Red) - Placa de interfaz que conecta la computadora a los cables de una red.

Nube de Internet - Forma simbólica de demostrar la Internet.

OS (Operating System o Sistema Operativo) - Software que administra el hardware y los recursos en una computadora.

OSI (Open Systems Interconnection) - Modelo de arquitectura de red desarrollado por ISO (International Standards Organization) para el proyecto de sistemas abiertos de red. Todas las funciones de comunicación se dividen en siete capas estandarizadas (física, enlace de datos, red, transporte, sesión, presentación y aplicación).

PCI (Peripheral Component Interconnect o Interconexión de Componentes Periféricos) - Bus local de alto desempeño con un canal de datos entre la CPU y los periféricos de alta velocidad independientes del procesador.

Ping (Packet Internet Groper) - Recurso usado para determinar cuales dispositivos están activos en una red o sitio de Internet.

POP (Point of Presence) - Región o punto de presencia donde se encuentran instalados los equipos de una empresa.

POP3 (Post Office Protocol 3) - Versión corriente del protocolo más utilizado para recibir e-mail en una red TCP/IP.

Portal - Sitio Web concebido con la finalidad de suministrar un amplio conjunto de informaciones y servicios a los usuarios de Internet, constituyendo un punto de acceso a Internet.

Profile (Perfil) - Registro almacenado en una computadora que contiene los ajustes y las preferencias de cada uno de los usuarios que comparten esta computadora.

Protocol (Protocolo) - Reglas que gobiernan la transmisión de datos, incluyendo inicialización, verificación, direccionamiento, recolección de datos y corrección de errores.

Proveedor - Empresa responsable por suministrar acceso para personas físicas o jurídicas a la Internet.

RF (Radio Frequency o Frecuencia de Radio) - Banda del espectro de señales electromagnéticas utilizada para transportar señales de radio (que puede consistir en AM, FM, microondas y otros).

SDH (Synchronous Digital Hierarchy) - Arquitectura de multiplexación y de transmisión de señales digitales entre elementos de redes cuyas señales de reloj de muestreo son sincronizadas con exactitud. La velocidad de transmisión es de 155 Mbps.

Server (Servidor) - Computadora y/o software que suministra y controla los recursos para Clientes en una red. Estos recursos pueden incluir dispositivos de hardware, tales como impresoras y sistemas de almacenaje o archivos, como en el caso de un servidor Web.

Servidor de Correo Electrónico (Mail Server) - Sistema que almacena, recibe y envía mensajes de correo electrónico, permitiendo su integración entre empresas y con Internet.

SMTP (Simple Mail Transfer Protocol o Protocolo Simple para la Transferencia de Correo) - Protocolo de TCP/IP utilizado para transmitir e-mail en una red o para direccionar e-mail en Internet.

SOHO (Small Office Home Office) - Segmento del mercado compuesto por empresas de pequeña envergadura (Small Office) y toda la gama de profesionales liberales (Home Office).

SSL (Secure Sockets Layer) - Protocolo de Internet desarrollado para transferencia y acceso de datos con seguridad a partir de browsers. Es muy utilizado para transacciones comerciales vía Internet.

STM-1 - Estándar que representa 155 Mbps (Megabits) por segundo en la transferencia de datos.

TCP/IP (Transmission Control Protocol / Internet Protocol) - Conjunto de protocolos en capas que permite el uso de aplicaciones compartidas entre PC´s, host´s o estaciones de trabajo en ambientes de comunicación de alta velocidad.

Telnet - Protocolo de emulación de terminal normalmente usado en aplicaciones que usan línea de comando, en Internet.

Transporte - Conducir o llevar informaciones de un lugar a otro utilizando medios de telecomunicaciones suministrados por los Proveedores.

UPS/Geradores/PDU – (Uninterrupted Power Supply) En caso de falta de energía, la UPS proporciona inmediatamente energía de reserva. Después de haber sido encendidos y "calentados", los generadores se adelantan y pasan a suministrar la energía a los equipos.

URL (Uniform Resource Locator o Localizador Uniforme de Recursos) - Dirección de un sitio en Internet que contiene el protocolo utilizado para el sitio, el nombre del dominio o dirección IP del mismo y, opcionalmente, la carpeta o página en el sitio donde están almacenadas determinadas informaciones.

USB (Universal Serial Bus) - Estándar "plug-and-play" para conectar varios dispositivos de entrada/salida a un único puerto de gran ancho de banda.

VPN (Virtual Private Network) - Garantiza el uso seguro de una red pública, tal como Internet. A través de VPN, los accesos a los datos entre redes de la empresa y entre usuarios y la empresa son codificados, ofreciendo total seguridad a los usuarios y a la red de acceso.

WAN (Wide Area Network) - Red de larga distancia que interconecta a computadoras distribuidas en áreas separadas geográficamente, es decir, un conjunto de redes locales interconectadas por medios de comunicación remotos (radios, líneas dedicadas, módems etc.).

WAP (Wireless Access Protocol) - Es una especificación abierta y global que permite al usuario de dispositivos wireless, tales como celulares, pagers o palm tops, tener acceso fácil e interaccionar instantáneamente con informaciones y servicios.

Web Hosting - Consiste en hospedar, mantener y servir archivos para los sitios. Además de espacio para el servidor, una rápida conexión a Internet también puede formar parte del contrato.

Wireless (Inalámbrico) - Tecnologías que utilizan el aire como medio de transmisión (satélite, microondas y spread spectrum).