UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADEMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIERIA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

TEMA:

"Implementación de una VPN con seguridades de la red inalámbrica y red externa para la empresa exportadora de flores GP FLOWERS ubicada en el cantón Latacunga"

Tesis de Grado Previo a la Obtención del Título de Ingeniero en Informática y Sistemas Computacionales.

Postulantes:

Almachi Oñate Paúl Noé

Chiluisa Quimbita Carlos Orlando

Director de Tesis:

Ing. Patricio Navas

Latacunga – Ecuador

2010

AUTORÍA

Nosotros, Almachi Oñate Paúl Noé y Chiluisa Quimbita Carlos Orlando, declaramos que el contenido de la presente Tesis de Grado, es la responsabilidad, investigación y esfuerzo constante que asumimos al momento de iniciar con este anhelado proyecto, que nos llevara a cumplir un objetivo propuesto con éxito.

……	…….
Chiluisa Quimbita Carlos Orlando	Almachi Oñate Paúl Noé
C.I. 050266482-4	C.I. 050267725-5

CERTIFICACIÓN

HONORABLE CONSEJO ACADÉMICO DE LA UNIDAD ACADEMICA DE CIENCIAS DE LA INGENIERIA Y APLICADAS DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI.

De mi consideración.

Cumpliendo con lo estipulado en el capítulo IV, (art. 9 literal f), del reglamento del curso profesional de la Universidad Técnica de Cotopaxi, informo que los postulantes: Chiluisa Quimbita Carlos Orlando y Almachi Oñate Paul Noé, han desarrollado su tesis de grado de acuerdo al planteamiento formulado en el plan de tesis con el tema: "Implementación de una VPN con Seguridades de la Red Inalámbrica Y red Externa para la Empresa Exportadora de Flores GP FLOWERS SA ubicada en el Cantón Latacunga", cumpliendo con los objetivos planteados.

En virtud de lo antes expuesto, considero que la presente tesis se encuentra habilitada para presentarse al acto de la defensa de tesis.

Latacunga, 22 de Julio del 2010

Atentamente,

Ing. Patricio Navas.
DIRECTOR DE TESIS

GP FLOWERS

Latacunga, Julio del 2010

De: Ing. Patricia Marín

GERENTE DE LA EMPRESA GP FLOWERS.

Para: Ing. Diana Marín

DIRECTOR DE LA UNIDAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS.

CERTIFICA

Que los Srs. **Chiluisa Quimbita Carlos Orlando con C.I. 050266482-4 y Almachi Oñate Paul Noé, C.I. 050267725-5**, Han implementado de manera satisfactoria el sistema de tesis con el tema: **"Implementación de una VPN con Seguridades de la Red Inalámbrica y Red Externa para la Empresa Exportadora de Flores GP FLOWER ubicada en el Cantón Latacunga"**, el sistema ha sido entregado de conformidad con lo solicitado para la aplicación de cada una de las actividades realizadas en nuestra Empresa Exportadora de Flores.

Es todo cuanto puedo certificar en honor a la verdad, los interesados pueden hacer uso del presente certificado para los fines que consideren necesarios.

Cordialmente

ING. Patricia Marín

GERENTE DE GP FLOWERS

AGRADECIMIENTO

Mi profundo agradecimiento a Dios quien nos concedió la vida y nos a permitido alcanzar mi anhelo profesional.

De manera muy especial a mi director de tesis Ing. Patricio Navas quien con su nobleza y paciencia supo compartir sus conocimientos y su invalorable tiempo para apoyarnos en el desarrollo del proyecto.

Quiero dejar constancia de nuestro profundo agradecimiento a la Universidad Técnica de Cotopaxi; quien nos acogió durante varios años para llenarnos de conocimientos, cumplir mis metas e ideales; y ser un profesional independiente en la sociedad.

Carlos

AGRADECIMIENTO

Agradezco a la Universidad y al personal docente quienes fueron la parte esencial en mi formación profesional y humana, ya que ellos supieron ser docentes y amigos a la vez.

Deseo expresar mi agradecimiento al Director de Tesis, Ing. Patricio Navas, por su apoyo incondicional, sugerencias y confianza que he recibido de el.

Y agradezco de manera especial a mis Padres quienes supieron dar todo de sí para que yo como hijo pudiera obtener un título profesional, además me siento en la necesidad de agradecer a todas las personas que de una u otra manera se preocuparon por mi durante el desarrollo de mi carrera estudiantil.

A todos mi mayor reconocimiento y gratitud.

Paúl

DEDICATORIA

Este trabajo dedico con todo mi amor a Dios quien me dio la vida y valor para seguir adelante, a la Virgen de las Mercedes, del Quinche y mi Niño Divino acompañándome siempre durante todo este trayecto.

¡Porque el estudio es la herencia más preciada que mis padres me han podido regalar!

Es por eso que quiero dedicar mi esfuerzo y sacrificio a mis padres, CARLOS, y BEATRIZ quienes me inculcaron valores, esfuerzo y ganas para ser una persona de éxito.

Ellos fueron que día tras día me motivaron para seguir adelante y culminar mi gran sueño. A mi hermana por la fuerza y el apoyo que me brindo en aquellos momentos que me sentía desvanecer.

Y sin dejar atrás a mis sobrina Dayana por todo el cariñó que me ha sabido brindar y ese sublime amor que solo ella me puede dar.

En la vida el amor es la parte fundamental para complementar el éxito de un ser. Por eso mi deseo de dedicar a una persona en especial. C/R por siempre.

Carlos

DEDICATORIA

Dedico este logro alcanzado a Dios por darme valor y sabiduría para enfrentar un reto más en mi vida.

A toda mi familia por brindarme todo su apoyo incondicional y desinteresado durante el transcurso de mi carrera estudiantil; de manera especial a MIS PADRES CESÁR Y MARIANA que nunca desmayaron en el trayecto de alcanzar mi triunfo ya que siempre me brindaron todo su confianza y su comprensión y me supieron guiar por el camino del bien.

Además dedico mi triunfo A MIS HERMANOS quienes fueron una parte esencial en mi vida estudiantil, por sus consejos, por todo lo vivido junto a ellos entre alegrías y tristezas, A MIS SOBRINOS por su cariño que me han brindado.

Paul

ÍNDICE GENERAL

CAPITULO II

CAPITULO III

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

RESUMEN

En los últimos años las redes privadas virtuales (VPN) están ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas. Las VPN permiten a sus usuarios acceder a información y recursos en tiempo real sin necesidad de estar físicamente conectados a un determinado lugar.

El presente proyecto investigativo nace a partir de la necesidad de contar con las debidas y necesarias seguridades que debe brindar una red inalámbrica interna y externa por donde va a circular la información de la empresa, puesto que el mundo globalizado actual exige tomar en cuenta todas las seguridades para el correcto funcionamiento de la red.

La implementación de la VPN es el resultado de una ardua labor la cual está compuesta de un análisis profundo de las seguridades con las que contaba el sistema, así como también de las necesidades y sugerencias de los funcionarios empleados(as) de la empresa GP Flowers.

Esta tesis presenta la implementación de una red inalámbrica para la empresa GP Flowers Ubicada en el Cantón Latacunga, cuyo objetivo es tener acceso confiable a la red y a los servicios que presta la empresa y sobre todo establecer los parámetros de seguridad requeridos para obtener una conexión segura.

Para su desarrollo se utilizó un sistema operativo basado en Linux el cual es robusto, estable, multiusuario, multitarea, multiplataforma y con gran capacidad para gestión de redes como es el CentOS 4.5, Red inalámbrica interna y externa, Internet.

SUMMARY

In the last years the private virtual (VPN) nets are winning a lot of recognition that is increased as their benefits increase and they are discovered new applications for them. VPN allows their users to accede to information and resources in real-time without necessity of being physically connected to a certain place.

The present investigative project is born starting from the necessity of having the due and necessary securities that it should offer a wireless internal and external net for where the information of the company will circulate, since the globalized world current demands to take into account all the securities for the correct operation of the net.

The implementation of VPN is the result of an arduous work which is made up of a deep analysis of the securities that the system counted, as well as of the necessities and suggestions of the workers from GP Flowers Company.

This thesis presents the execution of a wireless net for the GP Flowers Company, located in Latacunga whose objective is to have reliable access to the net and the services that lend the company and mainly to establish the parameters of security required to obtain a sure connection.

For its development an operating system was used based on Linux which is robust, stable, multiuser, multitasking, and multiplatform with a great capacity for nets management like CentOS 4.5 internal wireless net and external Internet.

CERTIFICACION DE TRADUCCION

Yo, Myrian Verónica Chiluisa Taipe, portadora de la cedula de identidad 0502655061, en calidad de Licenciada en ingles, tengo el bien de CERTIFICAR, que los egresados de la Universidad Técnica de Cotopaxi, Sr. Carlos Orlando Chiluisa Quimbita y Paul Noé Almachi Oñate, han realizado la debida corrección con mi persona del Summary de la Tesis de Grado con el Tema "IMPLEMENTACION DE UNA VPN CON SEGURIDADES DE LA RED INALAMBRICA Y RED EXTERNA PARA LA EMPRESA EXPORTADORA DE FLORES GP FLOWER UBICADA EN EL CANTON LATACUNGA" .

El cual se encuentra bien estructurado, por lo que doy fe del presente trabajo.

Por tal motivo faculto a los peticionarios hacer uso del presente certificado como a bien lo tuvieren.

English Teacher.
Myrian Chiluisa
C.I. 050265506-1

Latacunga, Julio del 2010

INTRODUCCIÓN

La evolución de la sociedad nos ha demostrado que los avances tecnológicos son la diferencia entre el desarrollo y el retraso por tanto la tecnología ha ido creciendo constantemente. Desde la llegada de la computadora todo el mundo ha hecho lo posible por tratar de mantenerse en el progreso tecnológico, dicho progreso dio a la luz al Internet lo cual fue muy importante para la administración de la información en muchas empresas.

Todas las empresas se han visto en la necesidad de estar a la par de la tecnología. Por esta misma razón las personas están obligadas a incluir en sus vidas cotidianas aparatos tecnológicos como dispositivos móviles, agendas electrónicas y computadoras portátiles.

En la actualidad el mercado tecnológico e informático es muy fuerte, cada mes o incluso hasta en menos tiempo aparecen nuevos avances tecnológicos lo que nos obliga a las personas a actualizarnos constantemente para no desentonar con los avances tecnológicos. Ahora bien, imagínese la maravilla de poder acceder al Internet en el trabajo, en la casa, en el café, en el aeropuerto sin tener que preocuparnos por conexiones telefónicas y aun mejor sin tener que preocuparnos por los molestos cables.

Al mismo tiempo que el Internet es muy útil y necesario se ha convertido en un arma de doble filo a causa de su mala utilización, en algunas ocasiones hasta con fines dolosos ya que la información hoy en día es pública y casi todas las transacciones personales y comerciales se las hace o se la puede realizar por internet.

Es por eso que una VPN de seguridades de la red inalámbrica y red externa es muy importante en la actualidad ya que nos ayudaría a mantener segura nuestra información. VPN es una abreviatura de Redes Privadas Virtuales

Como se puede observar es una gran ventaja el tener acceso a la información por medio de la VPN, pero con esto tendremos mayor seguridades con la información que va a circular.

La seguridad se han desarrollado a lo largo de los años pero no ayudado mucho ya que ha existido alteración de información es por ello que las VPN nos ayudara de mucho para poder proteger la información.

Por todo lo anteriormente anotado la importancia de implementar una VPN con seguridades de la red inalámbrica y red externa para la empresa exportadora de flores Gp Flowers ubicada en el cantón Latacunga para la optimización de recursos, tratamiento de información confiable, logrando así tener un sistema de comunicación desde cualquier punto , accediendo a todas las bondades de la red y una interconexión con la red cableada tanto en: datos, textos, imágenes, voz, vídeo, multimedia, etc, que beneficiará a todo el personal de la empresa.

Para la obtención de este proyecto, se realizaron algunos pasos como:

- Recopilar de toda la información de campo necesaria para conocer el estado actual del tema planteado.

- Analizar los fundamentos teóricos de las fuentes consultadas para fundamentar la investigación relacionada con la implementación de seguridades.

Cabe mencionar que se utilizó la Investigación descriptiva debido a que nos facilitó tener un contacto directo con la realidad de las seguridades de la red, y se utilizo el Método Inductivo ya que partimos de un hecho particular para llegar a un hecho general, y con la Encuesta como técnica.

Este trabajo investigativo consta de tres capítulos que son los siguientes:

El presente capítulo donde se hace una introducción que incluye, una exposición de los principales motivos que llevaron al desarrollo de la presente tesis. También en este capítulo se identifican algunos conceptos necesarios para la implantación de seguridades con una VPN.

Además, se plantean los objetivos que se pretenden conseguir en la tesis.

El segundo capítulo tenemos los Antecedentes Históricos de la Empresa GP Flowers la tabulación, análisis e interpretación de las encuestas realizadas en la empresa Gp Flowers del Cantón Latacunga, realizada tanto a funcionarios como empleados (as). .

El tercer capítulo se presenta la implantación propuesta en la tesis. Este constituye la principal aportación teórica donde se explica la configuración del servidor bajo Linux CentOS como también los servicios y las seguridades que prestará la VPN.

Por último, se presentan las conclusiones y recomendaciones en las que se detallan las principales aportaciones del trabajo desarrollado.

CAPITULO I

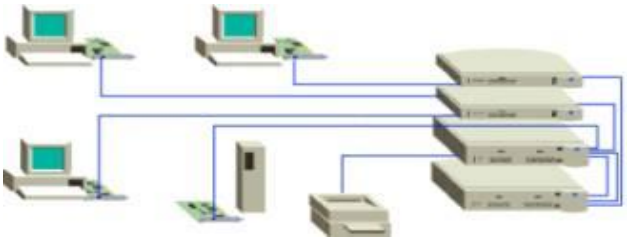
1. ESTUDIO DE LAS VPN Y SEGURIDAD INALÁMBRICA

1.1. Redes

1.1.1. Concepto de red

En http://es.wikipedia.org/wiki/Concepto_Red, establece que "Las redes están formadas por conexiones entre grupos de computadoras y dispositivos asociados que permiten a los usuarios la transferencia electrónica de información.

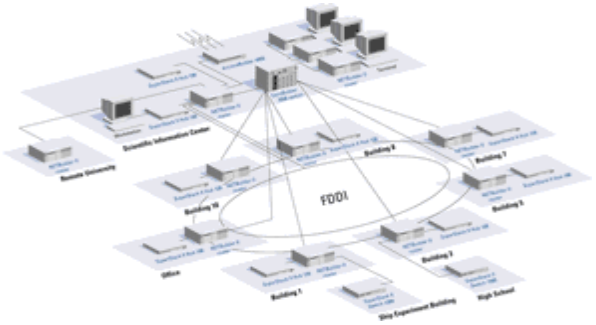
GRÁFICO 1.1: REDES INALÁMBRICAS



Fuente: http://www.redes.com

Los dispositivos que constituyen una red funcionan transmitiendo información de uno a otro, en grupos de impulsos eléctricos pequeños (conocidos como paquetes). Cada paquete contiene la dirección del dispositivo transmisor (la dirección fuente) y la del dispositivo receptor (dirección de destino). Parte del equipo que forma la red utiliza esta información de la dirección para ayudar al paquete a llegar a su destino."

GRÁFICO 1.2: REDES INALÁMBRICAS

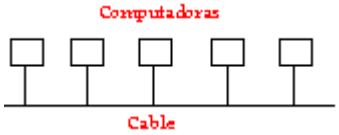


Fuente: http://www.redes.com

1.1.2 Tipos de red

En http://es.wikipedia.org/wiki/Tipos de Red, establece que "LAN**:** Iníciales de red de área local (Local Área Network), grupo de computadoras y otros dispositivos en un área limitada, como un edificio, conectadas por un enlace de comunicaciones que permite interactuar a los dispositivos de la red.

GRÁFICO 1.3: TIPOS DE RED

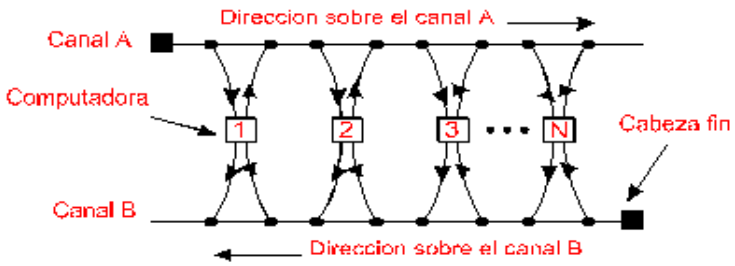


Fuente: http://www.monografias.com

MAN: Redes de área metropolitana (Metropolitan Area Network) con dos buses unidireccionales, cada uno de ellos es independiente del otro en cuanto a la transferencia de datos. Es básicamente una gran versión de LAN y usa una tecnología similar. Puede cubrir un grupo de oficinas de una misma corporación o ciudad, esta puede ser pública o privada. El mecanismo para la resolución de conflictos en la transmisión de datos que usan las MANs, es DQDB.

DQDB consiste en dos buses unidireccionales, en los cuales todas las estaciones están conectadas, cada bus tiene una cabecera y un fin. Cuando una computadora quiere transmitir a otra, si esta está ubicada a la izquierda usa el bus de arriba, caso contrario el de abajo.

GRÁFICO 1.4: TIPOS DE RED



Fuente: http://www.monografias.com

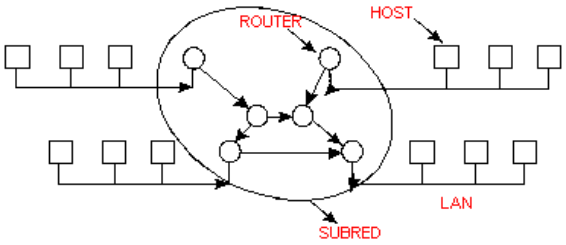
WAN**:** Red de área amplia (Wide Area Network). El alcance es una gran área geográfica, como por ejemplo: una ciudad o un continente. Está formada por una vasta cantidad de computadoras interconectadas (llamadas hosts), por medio de subredes de comunicación o subredes pequeñas, con el fin de ejecutar aplicaciones, programas, etc.

Una subred está formada por dos componentes:

Líneas de transmisión: quienes son las encargadas de llevar los bits entre los hosts.

Elementos interruptores (routers): son computadoras especializadas usadas por dos o más líneas de transmisión. Para que un paquete llegue de un router a otro, generalmente debe pasar por routers intermedios, cada uno de estos lo recibe por una línea de entrada, lo almacena y cuando una línea de salida está libre, lo retransmite.”

GRÁFICO 1.5: ROUTER



Fuente: http://www.monografias.com

1.2. Red privada virtual

1.2.1. Concepto de la VPN

En http://www.monografias.com/trabajos1/reqpri/repri.html, establece que VPN "es una unión de redes dispersas en Internet con una relación de confianza (configurable) entre las mismas, y niveles de autenticación y cifrado. Como indica su nombre, es una red privada, puesto que brinda autenticación y cifrado (privacidad en definitiva) y virtual porque se implementa sobre las redes públicas existentes y que no tienen los niveles de seguridad adecuados. La comunicación en una VPN viaja a través de Internet, pero está encapsulada y encriptada por lo que su contenido es secreto. Sólo el emisor y el receptor legítimo del mensaje pueden verla en su estado normal."

1.2.2. Importancia de la VPN

La importancia de las VPNs radica fundamentalmente en el hecho de lograr disminuir el costo del enlace entre dos sitios remotos.

Cuando se desea conectar las oficinas centrales de una empresa con alguna de sus sucursales u oficinas remotas, o los usuarios remotos conectarse con la misma, se tienen tres opciones de conexión fundamentales:

- **CONEXIÓN POR MODEM TELEFONICO:** Las desventajas en que incurre ese tipo de conexión están dadas principalmente por el costo de la llamada, que para el usuario seria una llamada telefónica convencional, por lo que se pagaría según el tiempo de conexión, esto empeoraría si la llamada es de larga distancia; por otra parte no se cuenta con la calidad y velocidad adecuadas que estarían poco más allá de los 40Kbps en orden descendente utilizando módems V90.

- **CONEXIÓN POR LINEA PRIVADA O ARRENDADA:** En este caso la conexión entre las dos entidades generalmente es por cables de pares de cobre o por fibra óptica de un punto a otro. Aquí el costo del enlace entre la oficina central y una sucursal es elevado, ya que esta dado por una tarifa mensual por kilometro de distancia sin importar el trafico cursado por enlace.

- **CONEXIÓN A TRAVES DE UNA RED PRIVADA VIRTUAL:** En el caso de una conexión por VPN, una empresa se ahorra en inversión de infraestructura tecnológica, administración y mantenimiento, además puede integrar varios servicios en un solo enlace. Como ejemplo se eliminan las llamadas de larga distancia las cuales son sustituidas por llamadas locales al proveedor local, o podría usarse un enlace dedicado a Internet ya establecido por lo que desaparecen los pagos por concepto de enlaces dedicados para la interconexión de oficinas remotas.

1.2.3. Ventajas y desventajas de la VPN

Ventajas

- Integridad, confidencialidad y seguridad de datos.
- Las VPN reducen los costes y son sencillas de usar.
- Facilita la comunicación entre dos usuarios en lugares distantes.
- Extensión de conectividad a nivel geográfico.
- Mejoras de seguridad.
- Mejora la productividad.

- Simplifica la topología de red.
- Proporciona oportunidades de comunicaciones adicionales.

Desventajas

- No se garantiza disponibilidad (NO Internet --> NO VPN).
- No se garantiza el caudal.
- Gestión de claves de acceso y autenticación delicada y laboriosa.
- La fiabilidad es menor que en una línea dedicada
- Mayor carga en el cliente VPN (encapsulación y encriptación)
- Mayor complejidad en la configuración del cliente (proxy, servidor de correo),
- Una VPN se considera segura pero no hay que olvidar que viajamos por Internet (no seguro y expuestos a ataques).

1.2.4. Tipos de vpn según el modo de conexión

VPN de acceso remoto

Es quizás el modelo más usado actualmente y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autentificados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

VPN punto a punto

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de

banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales, sobre todo en las comunicaciones internacionales.

1.3. Redes privadas virtuales basadas en internet

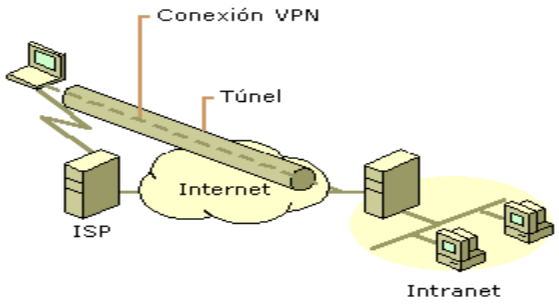
En http://www.monografias.org/wiki/RedesPrivadasVirtuales_Red, establece que "Mediante una conexión de red privada virtual (VPN) basada en Internet, puede ahorrar los gastos de llamadas telefónicas a larga distancia y aprovechar la disponibilidad de Internet."

Acceso remoto a través de Internet

En lugar de realizar una llamada de larga distancia para conectar con un servidor de acceso a la red (NAS, Network Access Server) de la compañía o externo, los clientes de acceso remoto pueden llamar a un ISP local. Mediante la conexión física establecida con el ISP local, el cliente de acceso remoto inicia una conexión VPN a través de Internet con el servidor VPN de la organización. Una vez creada la conexión VPN, el cliente de acceso remoto puede tener acceso a los recursos de la intranet privada.

La ilustración siguiente muestra el acceso remoto a través de Internet.

GRÁFICO 1.6: VPN



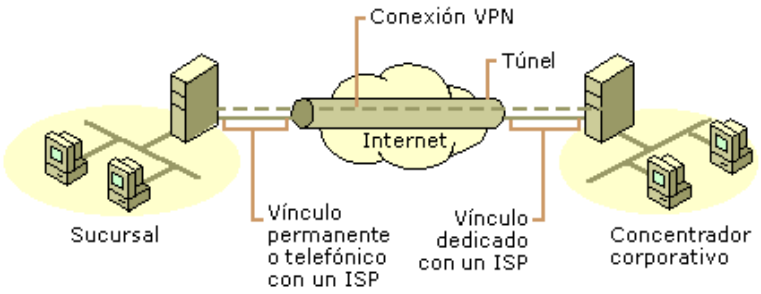
Fuente: http://www.wikipedia.com

Conectar redes a través de Internet

Cuando las redes están conectadas a través de Internet, un enrutador reenvía paquetes a otro enrutador a través de una conexión VPN. Para los enrutadores, la red privada virtual funciona como un vínculo de la capa de vínculo de datos.

La ilustración siguiente muestra la conexión de redes a través de Internet.

GRÁFICO 1.7: TIPOS DE RED VPN



Fuente: http://www.wikipedia.com

Usar vínculos WAN dedicados

En lugar de utilizar un vínculo WAN dedicado de larga distancia y caro entre las distintas oficinas de la compañía, los enrutadores de las oficinas se conectan a Internet mediante vínculos WAN dedicados locales con un ISP local. Así, cualquiera de los enrutadores inicia una conexión VPN de enrutador a enrutador a través de Internet. Una vez conectados, los enrutadores pueden reenviarse entre sí transmisiones de protocolos enrutadas o directas mediante la conexión VPN.

Usar vínculos WAN de acceso telefónico

En lugar de realizar una llamada de larga distancia para conectar con un NAS de la compañía o externo, el enrutador de una oficina puede llamar a un ISP local.

Mediante la conexión establecida con el ISP local, el enrutador de la sucursal inicia una conexión VPN de enrutador a enrutador con el enrutador de la oficina central a través de Internet. El enrutador de la oficina central actúa como un servidor VPN y debe estar conectado a un ISP local mediante un vínculo WAN dedicado.

Es posible mantener conectadas ambas oficinas a Internet mediante un vínculo WAN de acceso telefónico. Sin embargo, esto sólo es posible si el ISP admite el enrutamiento a clientes mediante marcado a petición; es decir, el ISP llama al enrutador del cliente cuando hay que entregar un datagrama IP al cliente. Muchos ISP no admiten el enrutamiento de marcado a petición para clientes.

1.4. Tuneles ip-ip

En http://es.wikipedia.org/wiki/Tuneles_IP-IP, establece que "En las redes que no utilizan ATM como protocolo de transporte, se pueden realizar túneles IP. En este caso los datos viajan a través de la red como si hubiese un enlace virtual entre cada nodo origen y cada nodo destino.

Los túneles IP aportan pocas ventajas sobre los PVC ATM salvo la independencia del medio. Los PVC solo valen para ATM, y los túneles al ser IP están por encima del nivel físico y de enlace, siendo en teoría independiente al medio de transmisión.

El túnel más común es GRE el cual fue desarrollado por Cisco originalmente, y constituyen túneles IP sobre IP cifrados. Este puede hacer unas cuantas cosas más que los túneles IP-sobre-IP cifrados. Este puede hacer unas cuantas coas más que los túneles IP-sobre-IP. Por ejemplo, se puede transportar tráfico multicast e IPv6 sobre un túnel GRE.

Una arquitectura típica cuando se usan túneles es hacer pasar estos por un "Concentrador de Túneles". Este equipo suele ser de gran potencia y bastante costoso.

Además del trafico tipo "túnel" no suele ser observado por los routers, con lo que se pierde la información de la cabecera IP como los bits de precedencia, impidiendo las políticas tradicionales de QoS."

1.5. Tuneles ip-sec

En http://es.wikipedia.org/wiki/Tuneles_IP-Sec, establece que "Este protocolo está siendo desarrollando por el grupo de trabajo de seguridad del IETF (Internet Engineering Task Force, Grupo de Trabajo de Ingeniería Internet).
El protocolo IPSec surgió a partir del desarrollo de Ipv6. Empezó siendo una extensión de la cabecera en Ipv6, pero debido a que cubría las necesidades de un gran número de clientes, se decidió implementar en parte para Ipv4.

IPSec tiene como característica más importante la posibilidad de encriptar los datos transmitidos. Esta cualidad es hoy en día el gran valor que tiene este protocolo y es lo que está permitiendo su rápida difusión en el mundo empresarial.
Entre las ventajas que puede presentar se destacan las siguientes:

- Es un protocolo complejo.
- Su configuración es complicada.
- Requiere configuración en el cliente.
- Tiene una provisión lenta y complicada.

A pesar de estos inconvenientes IPSec está teniendo una gran difusión en las redes actuales debido a la seguridad que proporciona tener los datos encriptados."

1.6. Mpls

En http://www.dspace.espol.edu.ec/bitstream/pdf/mpls, establece que "MPLS (Multiprotocol Label Switching Conmutación Multi-Protocolo mediante Etiquetas) es un mecanismo de transporte de datos estándar opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico,

incluyendo tráfico de voz y de paquetes IP. Es una nueva tecnología de conmutación creada para proporcionar circuitos virtuales en las redes IP, sobre las que introduce una serie de mejoras:

- Redes privadas virtuales.
- Ingeniería de tráfico.
- Mecanismos de protección frente a fallos."

1.7. Técnicas de seguridad

En http://www.dric.com.mx/seguridad/tecnicas_Red, establece que "Proveen seguridad en comunicaciones de voz, datos y video a través de redes públicas de datos como Internet, al emplear túneles de IPsec, servicios de encriptación y autentificación, que logran mantener la integridad de las comunicaciones.

Cuentan con servicios de Firewall que crean una barrera segura contra ataques provenientes de Internet.

Además de solventar servicios de conectividad WAN, proveen servicios de Firewall que protegen la red de la organización de ataques por Internet.
Cuentan con dispositivos que gestionan un acceso confiable a los usuarios de la red interna, a través de servicios seguros de autentificación de ataques."

1.8. Aplicación de la encriptación en las vpn

En http://www.dspace.espol.edu.ec/bitstream/encript_VPN, establece que "Existen dos tipos de técnicas de encriptación que se usan en las VPN: Encriptación de clave secreta, o privada, y Encriptación de clave pública.

En la encriptación con clave secreta se utiliza una contraseña secreta conocida por todos los participantes que van a hacer uso de la información encriptada. La contraseña se utiliza tanto para encriptar como para desencriptar la información.

Este tipo de sistema tiene el problema que, al ser compartida por todos los participantes y debe mantenerse secreta, al ser revelada, tiene que ser cambiada y distribuida a los participantes, lo que puede crear problemas de seguridad.

La **encriptación de clave pública** implica la utilización de dos claves, una pública y una secreta. La primera es enviada a los demás participantes. Al encriptar, se usa la clave privada propia y la clave pública del otro participante de la conversación.

Al recibir la información, ésta es desencriptada usando su propia clave privada y la pública del generador de la información. La gran desventaja de este tipo de encriptación es que resulta ser más lenta que la de clave secreta. “

1.9. Redes inalámbricas

1.9.1. Conceptos

En http://www.cisco.com/warp/concepto_Red, establece que “Las redes inalámbricas (wireless network) son aquellas que se comunican por un medio de transmisión no guiado (sin cables) mediante ondas electromagnéticas. La transmisión y la recepción se realizan a través de antenas. Tienen ventajas como la rápida instalación de la red sin la necesidad de usar cableado, permiten la movilidad y tienen menos costos de mantenimiento que una red convencional.”

1.9.2. Orígenes

El origen de las LAN inalámbricas se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, que consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados en el volumen 67 de los Proceeding del IEEE(Institute of Electrical and Electronics Engineers), puede considerarse como el punto de partida en la línea evolutiva de esta tecnología.

Las investigaciones siguieron adelante tanto con infrarrojos como con microondas, donde se utilizaba el esquema del "spread-spectrum"(frecuencias altas), siempre a nivel de laboratorio. En mayo de 1985, y tras cuatro años de estudios, el FCC (Federal Communications Comission), la agencia federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas IMS (Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz a las redes inalámbricas basadas en "spread-spectrum". IMS es una banda para uso comercial sin licencia: es decir, el FCC simplemente asigna la banda y establece las directrices de utilización, pero no se involucra ni decide sobre quién debe transmitir en esa banda.

1.9.3. Ámbito de aplicación

Las bandas más importantes con aplicaciones inalámbricas, del rango de frecuencias que abarcan las ondas de radio, son la VLF (comunicaciones en navegación y submarinos), LF (radio AM de onda larga), MF (radio AM de onda media), HF (radio AM de onda corta), VHF (radio FM y TV), UHF (TV).

Mediante las microondas terrestres, existen diferentes aplicaciones basadas en protocolos como Bluetooth o ZigBee para interconectar ordenadores portátiles, PDAs, teléfonos u otros aparatos. También se utilizan las microondas para comunicaciones con radares (detección de velocidad o otras características de objetos remotos) y para la televisión digital terrestre.

Las microondas por satélite se usan para la difusión de televisión por satélite, transmisión telefónica a larga distancia y en redes privadas.

1.10. Orígenes de las redes de área local inalámbricas

En http://es.wikipedia.org/wiki/Red_inal%cC3%mbrica, establece que “Las redes locales inalámbricas no han sabido o podido conquistar el mercado. Aunque con un gran nivel de aplicabilidad a distintos escenarios donde el cable resulta

inadecuado o imposible, la falta de estándares y sus reducidas prestaciones en cuanto a velocidad han limitado tanto el interés de la industria como de los usuarios. La aparición, sin embargo, de la norma IEEE 802.11 podría suponer una reactivación del mercado, al introducir un necesario factor de estabilidad e inter-operatividad imprescindible para su desarrollo. Y ya se trabaja para conseguir LAN inalámbricas a 10 Mbps.

GRÁFICO 1.8: ORIGEN DE RED LOCAL

Fuente: http://www.rincondelbago.com

Una red de área local por radio frecuencia o WLAN (Wireless LAN) puede definirse como una red local que utiliza tecnología de radiofrecuencia para enlazar los equipos conectados a la red, en lugar de los cables coaxiales o de fibra óptica que se utilizan en las LAN convencionales cableadas, o se puede definir de la siguiente manera: cuando los medios de unión entre sus terminales no son los cables antes mencionados, sino un medio inalámbrico, como por ejemplo la radio, los infrarrojos o el láser.

GRÁFICO 1.9: ORÍGENES DE RED ÁREA LOCAL

Fuente: http://www.rincondelbago.com

La tecnología basada en microondas se puede considerar como la más madura, dado que es donde se han conseguido los resultados más claros. La basada en infrarrojos, por el contrario, se encuentra de momento menos desarrollada, las distancias que se cubren son sensiblemente más cortas y existen aún una importante serie de problemas técnicos por resolver. Pese a ello, presenta la ventaja frente a las microondas de que no existe el problema de la saturación del espectro de frecuencias, lo que la hace tremendamente atractiva ya que se basa en un "espacio libre" de actuación.

Para ser considerada como WLAN, la red tiene que tener una velocidad de transmisión de tipo medio (el mínimo establecido por el IEEE 802.11 es de 1 Mbps, aunque las actuales tienen una velocidad del orden de 2 Mbps), y además deben trabajar en el entorno de frecuencias de 2,45 GHz.

GRÁFICO 1.10: ORÍGENES DE RED ÁREA LOCAL

Fuente: http://www.rincondelbago.com

La aparición en el mercado de los laptops y los PDA (Personal Digital Assistant), y en general de sistemas y equipos de informática portátiles es lo que ha generado realmente la necesidad de una red que los pueda acoger, o sea, de la WLAN. De esta manera, la WLAN hace posible que los usuarios de ordenadores portátiles puedan estar en continuo movimiento, al mismo tiempo que están en contacto con los servidores y con los otros ordenadores de la red, es decir, la WLAN permite movilidad y acceso simultáneo a la red.”

GRÁFICO 1.11: ORÍGENES DE RED ÁREA LOCAL

Fuente: http://www.rincondelbago.com

1.10.1. Tipos de redes inalámbricas

1.10.1.1. Redes de área local (LAN)

Las LAN constan de los siguientes componentes:

- Computadores
- Tarjetas de interfaz de red
- Dispositivos periféricos
- Medios de networking
- Dispositivos de networking

Las LAN permiten a las empresas aplicar tecnología informática para compartir localmente archivos e impresoras de manera eficiente, y posibilitar las comunicaciones internas. Un buen ejemplo de esta tecnología es el correo electrónico. Los que hacen es conectar los datos, las comunicaciones locales y los equipos informáticos.

1.10.1.2. Redes de área amplia (WAN)

Las WAN están diseñadas para realizar lo siguiente:

- Operar entre áreas geográficas extensas y distantes
- Posibilitar capacidades de comunicación en tiempo real entre usuarios

- Brindar recursos remotos de tiempo completo, conectados a los servicios locales
- Brindar servicios de correo electrónico, World Wide Web, transferencia de archivos y comercio electrónico.

1.10.1.3 Redes de área metropolitana (MAN)

La MAN es una red que abarca un área metropolitana, como, por ejemplo, una ciudad o una zona suburbana. Una MAN generalmente consta de una o más LAN dentro de un área geográfica común. Por ejemplo, un banco con varias sucursales puede utilizar una MAN.

Normalmente, se utiliza un proveedor de servicios para conectar dos o más sitios LAN utilizando líneas privadas de comunicación o servicios ópticos. También se puede crear una MAN usando tecnologías de puente inalámbrico enviando haces de luz a través de áreas públicas.

1.10.2. Ventajas de las redes inalámbricas

Accesibilidad: Todos los equipos portátiles y la mayoría de los teléfonos móviles de hoy día vienen equipados con la tecnología Wi-Fi necesaria para conectarse directamente a una LAN inalámbrica. Los usuarios pueden acceder de forma segura a sus recursos de red desde cualquier ubicación dentro de su área de cobertura. Generalmente, el área de cobertura es su instalación, aunque se puede ampliar para incluir más de un edificio.

Movilidad: Los empleados pueden permanecer conectados a la red incluso cuando no se encuentren en sus mesas. Los asistentes de una reunión pueden acceder a documentos y aplicaciones. Los vendedores pueden consultar la red para obtener información importante desde cualquier ubicación.

Productividad: El acceso a la información y a las aplicaciones clave de su empresa ayuda a su personal a realizar su trabajo y fomentar la colaboración. Los visitantes

(como clientes, contratistas o proveedores) pueden tener acceso de invitado seguro a Internet y a sus datos de empresa.

Fácil configuración: Al no tener que colocar cables físicos en una ubicación, la instalación puede ser más rápida y rentable. Las redes LAN inalámbricas también facilitan la conectividad de red en ubicaciones de difícil acceso, como en un almacén o en una fábrica.

Escalabilidad: Conforme crecen sus operaciones comerciales, puede que necesite ampliar su red rápidamente. Generalmente, las redes inalámbricas se pueden ampliar con el equipo existente, mientras que una red cableada puede necesitar cableado adicional.

Seguridad: Controlar y gestionar el acceso a su red inalámbrica es importante para su éxito. Los avances en tecnología Wi-Fi proporcionan protecciones de seguridad sólidas para que sus datos sólo estén disponibles para las personas a las que le permita el acceso.

Costes: Con una red inalámbrica puede reducir los costes, ya que se eliminan o se reducen los costes de cableado durante los traslados de oficina, nuevas configuraciones o expansiones.

1.10.3. Estándares inalámbricos

1.10.3.1 IEE 802.11(A), IEE 802.11(B), IEE 802.11(G)

IEEE802.11a.
Una mejora de las anteriores. Operará ya en la banda de 5 GHz y brindará velocidades de datos que oscilarán entre 6 y 54 Mbps.

IEEE802.11b.
Aunque trabaja en la frecuencia 2,4 GHz, ofrece una velocidad de 11 Mbps. La interoperabilidad entre los distintos dispositivos ha quedado resuelta gracias a la

marca Wi-Fi, amparada por la Alianza para la Compatibilidad de Ethernet Inalámbrica (WECA), que fue creada en 1999.

IEEE802.11g.
Todavía pendiente de ratificación por parte del IEEE permitirá conseguir transmisiones inalámbricas de alta velocidad a 20 Mbps. En cuanto a la banda de frecuencia utiliza los 2,5 GHz.

1.11. Topologías y protocolos inalámbricos

1.11.1. Redes ad-Hoc

En http://www.dspace.espol.edu.ec/bitstream/topologias_protoc, establece que "Una red ad hoc es una red inalámbrica descentralizada. La red es ad hoc porque cada nodo está preparado para reenviar datos a los demás y la decisión sobre qué nodos reenvían los datos se toma de forma dinámica en función de la conectividad de la red. Esto contrasta con las redes tradicionales en las que los router llevan a cabo esa función. También difiere de las redes inalámbricas convencionales en las que un nodo especial, llamado punto de acceso, gestiona las comunicaciones con el resto de nodos.

La naturaleza descentralizada de las redes ad hoc, hace de ellas las más adecuadas en aquellas situaciones en las que no puede confiarse en un nodo central y mejora su escalabilidad comparada con las redes inalámbricas tradicionales, desde el punto de vista teórico y práctico

Las redes ah hoc son también útiles en situaciones de emergencia, como desastres naturales o conflictos bélicos, al requerir muy poca configuración y permitir un despliegue rápido. El protocolo de encaminamiento dinámico permite que entren en funcionamiento en un tiempo muy reducido."

1.11.2. Redes de infraestructura

Contrario al modo ad hoc donde no hay un elemento central, en el modo de infraestructura hay un elemento de "coordinación": un punto de acceso o estación base. Si el punto de acceso se conecta a una red Ethernet cableada, los clientes inalámbricos pueden acceder a la red fija a través del punto de acceso. Para interconectar muchos puntos de acceso y clientes inalámbricos, todos deben configurarse con el mismo SSID.

Para asegurar que se maximice la capacidad total de la red, no configure el mismo canal en todos los puntos de acceso que se encuentran en la misma área física. Los clientes descubrirán (a través del escaneo de la red) cuál canal está usando el punto de acceso de manera que no se requiere que ellos conozcan de antemano el número de canal.

En redes IEEE 802.11 el modo de infraestructura es conocido como Conjunto de Servicios Básicos (BSS – Basic Service Set). También se conoce como Maestro y Cliente.

1.12. Instalación y configuración de access point

1.12.1 Modo de operación

En http://es.wikipedia.org/wiki/Wi-Fi_Instalacion_Access_Point, establece que "El modo del punto de acceso no debe ser confundido con los dos modos básicos "de radio" de cualquier tarjeta inalámbrica, que son infraestructura y ad hoc.

El modo de un punto de acceso se refiere al tipo de tareas que éste realiza. La denotación de "modo" puede ser confusa en muchos casos ya que los fabricantes usan diferentes nombres para describir el modo de operación de un producto.

Todo punto de acceso funciona como puente entre la red cableada y la inalámbrica, y cuando se limita a esta tarea se dice que funciona como puente. Si,

además, realiza funciones adicionales como enrutamiento y enmascaramiento (NAT), entonces estamos hablando de un enrutador inalámbrico. Los modos se diferencian principalmente en cuándo el punto de acceso actúa como puente o enrutador/NAT."

En la siguiente sección se describe el conjunto típico de "modos" que usted encontrará en los puntos de acceso (o enrutadores inalámbricos). Note que el nombre del modo puede diferir de vendedor en vendedor.

Punto de acceso (Access Point Bridging / Access Point Mode)
El punto de acceso trabaja como un puente transparente entre el enrutador y los clientes inalámbricos.

El punto de acceso no realiza labores de enrutamiento o NAT. Este es el modo de configuración más simple de un punto de acceso inalámbrico.

Pasarela (Gateway)
El punto de acceso actúa como un enrutador inalámbrico entre una LAN y un grupo de clientes inalámbricos llevando a cabo el enrutamiento o el enmascaramiento (NAT) para esos clientes. El punto de acceso puede obtener del proveedor de acceso a la Red una dirección IP a través de DHCP (Dynamic Host Configuration Protocol). El punto de acceso puede entregar direcciones IP a sus clientes usando DHCP.

Puente punto a punto (Point-to-Point bridge / Repeater mode)
Se usan dos puntos de acceso para tender un puente entre DOS redes cableadas. No se realiza NAT en los puntos de acceso ya que el enmascaramiento simplemente pasa sobre los paquetes de datos.

Enrutamiento punto a punto (Point-to-Point routing / Wireless Bridge Link)
El punto de acceso es usado como un enrutador inalámbrico entre dos LAN separadas.

Adaptador inalámbrico Ethernet (Wireless Ethernet adapter / Wireless Client mode)

Este modo se usa para conectar un computador que no soporta adaptadores inalámbricos. Conectando un punto de acceso como un dispositivo a través de los puertos Ethernet o USB, el punto de acceso se puede usar "como un adaptador inalámbrico".

1.12.2. Punto de Acceso

Es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos. Muchos WAPs pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar "roaming". Por otro lado, una red donde los dispositivos cliente se administran a sí mismos -sin la necesidad de un punto de acceso- se convierten en una red ad-hoc. Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados.

Son los encargados de crear la red, están siempre a la espera de nuevos clientes a los que dar servicios. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) y la LAN cableada.

Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos. Este o su antena son normalmente colocados en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, mediante una antena inalámbrica.

GRÁFICO 1.12: ADAPTADORES

Fuente: http://www.rincondelbago.com

1.12.3. Cliente inalámbrico

Un cliente inalámbrico es cualquier estación inalámbrica que se conecta a una red de área local (LAN–Local Área Network) inalámbrica para compartir sus recursos. Una estación inalámbrica se define como cualquier computador con una tarjeta adaptadora de red inalámbrica instalada que transmite y recibe señales de Radio Frecuencia (RF).

Algunos de los clientes inalámbricos más comunes son las computadoras portátiles, PDAs, equipos de vigilancia y teléfonos inalámbricos de VoIP.

1.12.4. Puente inalámbrico

Los puentes inalámbricos, son un uso especializado de la misma tecnología diseñada para conectar dos o más redes juntas.

Un puente inalámbrico no puede servir como un punto de acceso y un punto de acceso no puede servir como puente. La confusión es que un puente inalámbrico y un punto de acceso inalámbrico pueden ser ambos contenidos en el mismo aparato físico. Hay solamente dos tipos de puentes inalámbricos, el punto-a-punto y el punto-a-de múltiples puntos. El diseño del puente inalámbrico atravesará la distancia necesaria.

1.12.5. Puente multi-punto

El puente multipunto utilizado actualmente en la ENIC es analógico. Se compone de cuatro códecs. Se ha elaborado un soporte lógico específico de control de este puente. Este soporte lógico está adaptado a las "director de conferencia", "voto" o "tiempo compartido". Este modo de gestión informatizado racionaliza el desarrollo de la reunión con la ayuda de elementos objetivos como la duración de la intervención de cada participante.

1.12.6. Repetidor

Un repetidor es un dispositivo electrónico que recibe una señal débil o de bajo nivel y la retransmite a una potencia o nivel más alto, de tal modo que se puedan cubrir distancias más largas sin degradación o con una degradación tolerable.

1.12.7. Antenas direccionales

Orientan la señal en una dirección muy determinada con un haz estrecho pero de largo alcance. Una antena direccional actúa de forma parecida a un foco que emite un haz concreto y estrecho pero de forma intensa (más alcance).

Las antenas Direccionales "envían" la información a una cierta zona de cobertura, a un ángulo determinado, por lo cual su alcance es mayor, sin embargo fuera de la zona de cobertura no se "escucha" nada, no se puede establecer comunicación entre los interlocutores.

1.13. Interconexión wlan

En http://es.wikipedia.org/wiki/Wi-Fi_Interconexion_Wlan, establece que "LA WLAN al ser redes físicas independientes, pueden coexistir con otras redes físicas e interconectarse a las mismas por medio de las denominadas pasarelas.
A su vez, los modos de trabajo en WLAN pueden ser de dos tipos:

Distribuido (peer to peer) es una red anárquica de igual a igual en la q todos los dispositivos tienen un adaptador WLAN.

Centralizada (infraestructura) estructura jerárquica, en la que un punto de acceso controla el tráfico entre los diferentes equipos o estaciones de la red, de forma que todos los equipos deben acceder a dicho punto de acceso.

Además este punto de acceso permite el acceso a redes LAN cableadas de forma que también hacen el papel de pasarelas".

1.13.1. Ventajas y desventajas wlan.

Ventajas

Movilidad: Las redes inalámbricas pueden proveer a los usuarios de una LAN acceso a la información en tiempo real en cualquier lugar dentro de la organización. Esta movilidad incluye oportunidades de productividad y servicio que no es posible con una red inalámbrica.

Simplicidad y rapidez en la instalación: La instalación de una red inalámbrica puede ser tan rápida y fácil y además que puede eliminar la posibilidad de tirar cable a través de paredes y techos.

Flexibilidad en la instalación: La tecnología inalámbrica permite a la red ir donde la inalámbrica no puede ir.

Costo de propiedad reducido: Mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en hardware de una LAN inalámbrica, la inversión de toda la instalación y el costo del ciclo de vida puede ser significativamente inferior. Los beneficios y costos a largo plazo son superiores en ambientes dinámicos que requieren acciones y movimientos frecuentes.

Escalabilidad: Los sistemas de WLANs pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son muy fáciles de cambiar y además es muy fácil la incorporación de nuevos usuarios a la red.

Desventajas

Calidad de Servicio: Las redes inalámbricas ofrecen una peor calidad de servicio que las redes cableadas. Estamos hablando de velocidades que no superan habitualmente los 10 Mbps, frente a los 100 que puede alcanzar una red normal y corriente. Por otra parte hay que tener en cuenta también la tasa de error debida a las interferencias. Esta se puede situar alrededor de10-4 frente a las 10-10 de las redes cableadas. Esto significa que has 6órdenes de magnitud de diferencia y eso es mucho.

Restricciones: Estas redes operan en un trozo del espectro radioeléctrico. Éste está muy saturado hoy día y las redes deben amoldarse a las reglas que existan dentro de cada país.

1.14. Introducción a la seguridad

1.14.1 Seguridad en Wlan

En http://www.dspace.espol.edu.ec/bitstream/seguridad_wlan, establece que "La seguridad WLAN abarca dos elementos: el acceso a la red y la protección de los datos (autenticación y encriptación, respectivamente). Las violaciones a la seguridad de la red inalámbrica, generalmente, vienen de los puntos de acceso no autorizados, aquéllos instalados sin el conocimiento de los administradores de la red, o que operan con las funcionalidades de protección deshabilitadas (que es la configuración por omisión en los dispositivos inalámbricos).

Estos "hoyos" en la seguridad, pueden ser aprovechados por personal no autorizado (hackers), que en caso de que logren asociarse con el punto de acceso,

ponen en riesgo no únicamente la infraestructura inalámbrica, sino también la red inalámbrica a la cual se conecta. La tabla siguiente contiene los mecanismos de seguridad usados en redes WLAN, así como las ventajas y desventajas de cada uno de ellos."

1.14.2 Mecanismo de seguridad

En los inicios de la tecnología inalámbrica, los procedimientos y mecanismos de seguridad eran tan débiles que podía ganarse acceso con relativa facilidad hacia redes WLAN de compañías desde la calle.

Existe el término "wardriving", que se refiere a la acción de recorrer una ciudad para buscar la existencia de redes inalámbricas y ganar acceso a ellas. En la actualidad, existen técnicas más sofisticadas y complejas, las cuales fortalecen los inconvenientes de los mecanismos WLAN y ayudan a mantener la confidencialidad y resistencia ante los ataques dirigidos hacia este tipo de redes.

El estándar inalámbrico 802.11 original incorpora encriptación y autenticación WEP (Privacidad Equivalente a Cable). Sin embargo, en el 2001 se publicaron artículos que comunicaban las deficiencias que enfrentaba dicho mecanismo. Al interceptar y decodificar los datos transmitidos en el aire, y en cuestión de horas en una red WLAN con tráfico intenso, la clave WEP puede ser deducida y se puede ganar acceso no autorizado. Esta situación desencadenó una serie de acciones por parte del IEEE y de la industria para mejorar la seguridad en las redes de tecnología inalámbrica.

1.15. Amenazas

1.15.1 Spoofing

En http://www.cisco.com/warp/public/amenazas, establece que "Spoofing se conoce a la creación de tramas TCP/IP utilizando una dirección IP falseada; la idea de este ataque al menos la idea es muy sencilla: desde su equipo, un pirata

simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del host suplantado. Y como los anillos de confianza basados en estas características tan fácilmente falsificables son aún demasiado abundantes (no tenemos más que pensar en los comandos r-, los accesos NFS, o la protección de servicios de red mediante TCP Wrapper), el spoofing sigue siendo en la actualidad un ataque no trivial, pero factible contra cualquier tipo de organización.

En el spoofing entran en juego tres máquinas: un atacante, un atacado, y un sistema suplantado que tiene cierta relación con el atacado; para que el pirata pueda conseguir su objetivo necesita por un lado establecer una comunicación falseada con su objetivo, y por otro evitar que el equipo suplantado interfiera en el ataque”

1.15.2. Suplantación

Consiste básicamente en sustituir la dirección IP origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar. Esto se consigue generalmente gracias a programas destinados a ello y puede ser usado para cualquier protocolo dentro de TCP/IP como ICMP, UDP o TCP. Hay que tener en cuenta que las respuestas del host que reciba los paquetes irán dirigidas a la IP falsificada. Por ejemplo si enviamos un ping (paquete icmp "echo request") spoofeado, la respuesta será recibida por el host al que pertenece la IP legalmente.

Este tipo de spooofing unido al uso de peticiones broadcast a diferentes redes es usado en un tipo de ataque de flood conocido como ataque Smurf. Para poder realizar IP SPOOFING en sesiones TCP, se debe tener en cuenta el comportamiento de dicho protocolo con el envío de paquetes SYN y ACK con su ISN específico y teniendo en cuenta que el propietario real de la IP podría (si no se le impide de alguna manera) cortar la conexión en cualquier momento al recibir paquetes sin haberlos solicitado. También hay que tener en cuenta que los routers

actuales no admiten el envío de paquetes con IP origen no perteneciente a una de las redes que administra (los paquetes spoofeados no sobrepasarán el router).

1.15.3 Soluciones y practicas seguras

El desarrollo, instalación y configuración de sistemas que garanticen la seguridad de su red. Los mismos se pueden dividir en seguridad de acceso y seguridad de datos.

La seguridad de acceso consiste en impedir el acceso de personas no deseadas a determinada información.

Entre estos sistemas se incluyen los Firewalls (filtrado de paquetes que circulan a través de su red) o IDS (Intrussion Detection System, sistemas que monitorean su red constantemente en busca de intrusos), pero también en muchos casos se hace necesario el desarrollo y configuración de sistemas a medida.

La seguridad de datos consiste en correr procedimientos sobre los datos que circulan a través de su red y hacia el exterior, para que se ajusten a determinadas normas de seguridad.

1.15.4. Filtrado MAC

El filtrado por MAC es un nivel de seguridad que nos permite aplicar los routers wifi, como medida de seguridad es válida para un tanto por ciento de la gente que desconoce realmente lo que es una dirección MAC o lo fácil que es vulnerar esa medida de seguridad.

La mayoría de 802,11 (Wi-Fi), los puntos de acceso permiten al administrador de la red para entrar en una lista de MAC (Media Access Control) se ocupa de que se les permite comunicarse en la red.

Esta funcionalidad, conocida como dirección MAC Filtrados permite al administrador de red para denegar el acceso a cualquier dirección MAC que no esté específicamente permitido en la red.

Esto exige que cada nuevo dispositivo de la red tiene su dirección MAC, entró en la base de datos como un dispositivo autorizado.

Por otro lado, la mayoría de 802,11 (Wi-Fi), tarjetas le permiten configurar la dirección MAC de la tarjeta en el software.

Por lo tanto, si usted puede oler la dirección MAC de un nodo de red, es posible unirse a la red usando la dirección MAC de ese nodo.

1.15.5. Activación WEP

WEP son las siglas de Wired Equivalency Protocol. WEP es un un intento de crear redes inalámbricas al menos tan seguras como las redes cableadas o al menos de seguridad equivalente a dichas redes. Por desgracia el sistema WEP es débil y resulta bastante sencillo de romper. Esto significa que cuando se transmite información de carácter crítico no se debe confiar únicamente en este sistema de cifrado.

La activación del cifrado WEP de 128 bits evitará que el pirata informático ocasional acceda a sus archivos o emplee su conexión a Internet de alta velocidad. Sin embargo, si la clave de seguridad es estática o no cambia, es posible que un intruso motivado irrumpa en su red mediante el empleo de tiempo y esfuerzo.

Por lo tanto, se recomienda cambiar la clave WEP frecuentemente. A pesar de esta limitación, WEP es mejor que no disponer de ningún tipo de seguridad y debería estar activado como nivel de seguridad mínimo.

1.15.6. Broadcast SSID

Una forma de proteger su red contra accesos no autorizados es ocultar el hecho de que haya una red inalámbrica en todos. De forma predeterminada, los equipos de red inalámbrica normalmente emite una señal de baliza, anunciando su presencia en el mundo y proporcionar información clave necesaria para los dispositivos se conecten a ella, incluido el SSID.

El SSID (Service Set Identifier) o nombre de la red, de la red inalámbrica es necesario para los dispositivos se conecten a ella. Si usted no desea azar dispositivos inalámbricos para conectarse a su red, entonces ciertamente no quieren anunciar su presencia y son una de las piezas clave de la información que necesitan para hacerlo.

1.15.7. Radius

Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1813 UDP para establecer sus conexiones.

Cuando se realiza la conexión con un ISP mediante módem, DSL, cablemódem, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo NAS (Servidor de Acceso a la Red o Network Access Server (NAS)) sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc.

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.

CAPITULO II

2. PRESENTACIÓN, INTERPRETACIÓN Y ANÁLISIS DE RESULTADOS.

2.1. Antecedentes Históricos de la Empresa GP Flowers SA

Apasionada por el aroma, el perfume y la belleza de las flores Patricia Eugenia Marín Chacón compra dos hectáreas de terreno el 15 de julio del 2007; En el barrio Zaragozín ubicado al occidente y aproximadamente a 20 minutos de la ciudad de Latacunga, provincia de Cotopaxi país Ecuador. Con el objetivo de sembrar una variedad de plantas ornamentales, para luego cultivarlas y comercializarlas entre sus vecinos, familiares y amigos.

Convirtiéndose así en una pequeña empresaria. Así lo hizo, al poco tiempo de la compra del terreno, construyo varios invernaderos divididos estos a la vez en bloques y le asignó el nombre de "GP FLOWERS" sembrando varios tipos de plantas ornamentales como menciona anteriormente. En pocos meses dándoles el tratamiento adecuado, debido cuidado y con la ayuda y apoyo de sus padres, hermanos y con el respaldo de un buen técnico, los bloques comenzaron a florecer, transformándose esta plantación en la admiración de todo el sector, seguidamente llegó la etapa del cultivo al cual se acercaron muchas personas a requerir de esa belleza natural como son las flores, las cuales fueron utilizadas para adornar salas, comedores, y recepciones.

Encantada por haber realizado un exitoso trabajo, y motivado por las felicitaciones y los halagos de propios y extraños Patricia realiza varias visitas a distintas y muy importantes fincas del país con el fin de conocer más sobre la producción y el cultivo de plantas. Fue ahí cuando empezó a darse cuenta que ella

también podía comercializar sus flores de una forma más abierta a todo el público quien deseara disponer de este producto.

En el 2008 luego de capacitarse y de haber adquirido muchos conocimientos acerca del tema y una vez de haber conseguido varios clientes fijos, creo una oficina dentro de la ciudad de Latacunga (calle Juan Abel Echeverría y Av. Oriente). La constituye legalmente y empezó su apertura a los mercados externos a distintos países del mundo como CHILE, E.E.U.U., ESPAÑA Y RUSIA. Hoy con 10 hectáreas de cultivos surte de variedad de flores a países como Estados Unidos, México y La Unión Europea, teniendo como prioridad al clavel en todas sus diversidades.

Con la comercialización de muchas multiplicidades de semillas, plantas y flores exóticas, conseguidas durante todo este tiempo y que hoy su diversidad llega a muchos países del mundo, los técnicos profesionales en la materia quienes trabajan en esta reconocida empresa se dedican a investigar, para hacer de estas semillas día a día más resistente al clima y a las plagas.

Tres generaciones han pasado y hoy Patricia y "GP FLOWERS". Están preparadas para afrontar los retos este mundo global, con la producción y una gran oferta de flores y semillas, con una logística que garantiza el recibido de las flores a tiempo y en buen estado por sus consumidores a lo largo y ancho de todo el mundo. Convirtiendo a "GP FLOWER" En una empresa de renombre y a Patricia en una gran y excelente empresaria.

2.1.1. Enfoque general de la Empresa

2.1.1.2. Cobertura de la Empresa

- Cantón Latacunga Provincia de Cotopaxi

2.1.1.3. Objetivo General

Consolidar la producción y las exportaciones, en los mercados internacionales, aplicando técnicas y métodos acordes a la realidad de nuestra empresa, ofertando productos innovadores y de calidad.

2.1.1.4 . Objetivos Específicos

- Crear fuentes de empleo.
- Equipar a la empresa.
- Cumplir y hacer cumplir las metas propuestas por la empresa y el cliente final.
- Mejorar la atención al cliente mediante capacitación a nuestros empleados.
- Fortalecer el nivel confiabilidad de nuestros.
- Dotación de infraestructura deportiva, de producción y social
- Crear condiciones y acciones para fortalecer la comunicación entre la empresa y los clientes.

2.1.1.5 . Misión

A partir de las necesidades del cliente, ser una empresa de éxito, generadora de fuentes de trabajo, fortaleciendo el comercio exterior y contribuir a elevar la competitividad de nuestras flores mediante el cultivo y producción de calidad que garanticen la orientación hacia los mercados internacionales.

2.1.1.6. Visión

Ser la Florícola líder a nivel mundial en Producción, Calidad, Confiabilidad y altamente Exportadora, capaz de satisfacer los requerimientos de entrega a través de innovación, con gente comprometida y guiada por valores compartidos.

2.2. Metodología de Desarrollo

Para el desarrollo de este proyecto se utilizó la investigación descriptiva debido a que nos facilitó tener un contacto directo con la realidad de las seguridades de la red con la que cuenta la empresa por donde circula la información; esta investigación nos fue útil para obtener nuestras propias conclusiones, las cuales nos ayudaron a ver de otra manera el problema. Además utilizamos el método inductivo ya que partimos de un hecho particular para llegar a un hecho general, es decir que seguimos una secuencia de procesos que se realizaron en nuestro proyecto investigativo, partiendo de hechos particulares como son la observación, el planteamiento de hipótesis para posteriormente realizar la implementación de una VPN con todas sus seguridades, siguiendo una serie de pasos lógicos, tales como: Observación**,** Experimentación, Comparación, Abstracción, Generalización. El método Científico también fue aplicado ya que se basa en una serie de pasos sistemáticos e instrumentos que nos lleva a un conocimiento científico.

Este método se basa en la recopilación de datos, su ordenamiento y para posteriormente realizar un análisis, ya que este método busca siempre obtener más información hasta darle sentido a las cosas, hasta llegar a la verdad del fenómeno estudiado. Los pasos del método científico son: Observación, Planteo de un Problema, Recopilación de Datos, Formulación de Hipótesis, Experimentación, Conclusión, Teoría o Ley.

En cuanto se refiere a las técnicas se aplicó la Observación ya que permitió al grupo investigador observar de forma directa y minuciosa el hecho que se realiza en la transmisión de información, generando una idea de los procesos que se ejecutan. Otra técnica utilizada fue la encuesta porque nos permitió obtener datos de varias personas, para nuestro proyecto, se aplicó a los funcionarios empleados(as) de la empresa GP Flowers, cuyas opiniones permitieron solucionar el problema que suscitaba en dicha empresa, una ventaja de esta técnica es que nos permitió tener una estadística mas real ya que pudimos graficarlos y tabularlos, es decir nos permitió obtener datos o información fácil y legible, para

ello se elaboró un listado de preguntas de una manera escrita. Y por último aplicamos la técnica Bibliográfica puesto que nos permitió recopilar información bibliográfica para la realización de la parte teórica de la investigación.

2.2.1. Aplicación De Técnicas de Investigación

Para conocer la realidad de la Empresa, es necesario utilizar técnicas de recopilación de datos e información, para de esta manera optimizar recursos económicos y de tiempo empleado en esta actividad.

De esta manera se decidió utilizar las siguientes técnicas de investigación.

2.2.2. Observaciones

Mediante esta técnica se logro verificar las necesidades que acoge a la Empresa Exportadora de flores "GP Flowers" ubicada en el Cantón Latacunga, con referencia a las seguridades de la información generada por esta.

2.2.3. Población

La investigación propuesta se realizará en la Empresa GP Flowers, las encuestas estarán enfocadas a los funcionarios empleados (as).

INVOLUCRADOS	POBLACIÓN
FUNCIONARIOS EMPLEADOS (AS)	28
TOTAL	28

2.2.4. Muestra

Debido a que la población es muy pequeña dentro de la investigación se concluye que se trabajará con la totalidad de los funcionarios empleados (as)

2.3. Presentación, Análisis e Interpretación de Información y Metodología de Desarrollo

En el siguiente capítulo se realizara el análisis de todas las encuestas aplicadas hacia los funcionarios y empleados (as) de la Empresa GP Flowers, ya que gracias a cada una de las respuestas proporcionadas por los mismos nos permitirán analizar los datos de una manera cuantitativa y cualitativa, estos resultados han facilitado desarrollar cada una de las operaciones o actividades que se deben realizar en el sistema por lo que los aportes realizados por los mismos son de mucha ayuda para el grupo investigador.

Así como también de acuerdo a los resultados se podrá verificar la hipótesis que nos hemos planteado al inicio de la investigación.

2.3.1. Análisis de los resultados de la encuesta realizada a los funcionarios y empleados (as) de la Empresa GP Flowers.

Conforme a las encuestas realizadas a los Funcionarios y empleados (as) de la Empresa GP Flowers, se obtuvo la siguiente información puntualizando las siguientes preguntas:

PREGUNTA 1

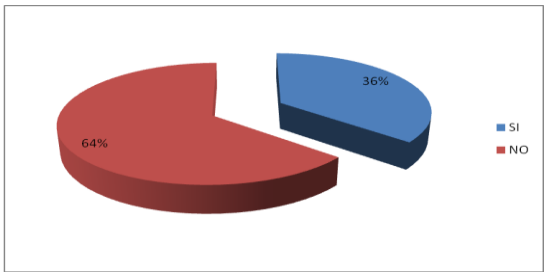
¿Conoce Ud. Sobre las Redes Inalámbricas?

TABLA No. 2.1: CONOCIMIENTO SOBRE REDES INALÁMBRICAS

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	10	36%
NO	18	64%
TOTAL	**2**	**100%**

Fuente: Funcionarios Empleados
Realizado por: Grupo Investigador

GRAFICO No. 2.1: CONOCIMIENTO SOBRE REDES INALÁMBRICAS



Fuente: Funcionarios Empleados
Realizado por: Grupo Investigador

ANÁLISIS E INTERPRETACIÓN

De los 28 Funcionarios empleados (as) de la Empresa GP Flowers, 10 de los funcionarios empleados(as) encuestados que corresponde al 36% conocen acerca de las redes inalámbricas, mientras que 18 funcionarios empleados(as) que corresponden al 56% no tiene ningún conocimiento sobre redes inalámbricas.

PREGUNTA 2

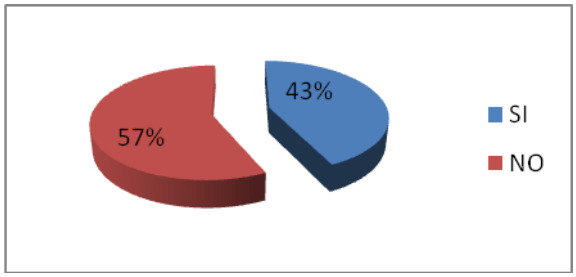
¿La Empresa ha prestado seguridades en servicios como el internet eficientes para el departamento financiero?

TABLA No. 2.2: LA EMPRESA PRESTA SEGURIDADES EN SUS SERVICIOS

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	12	43%
NO	16	57%
TOTAL	**28**	**100%**

Fuente: Funcionarios Empleados
Realizado por: Grupo Investigador

GRAFICO No. 2.2: LA EMPRESA PRESTA SEGURIDADES EN SUS SERVICIOS



Fuente: Funcionarios Empleados
Realizado por: Grupo Investigador

ANÁLISIS E INTERPRETACIÓN

De las encuestas realizadas a 28 Funcionarios empleados (as) de la Empresa GP Flowers, 12 funcionarios empleados(as) que corresponden al 43% manifestaron que la empresa si presta seguridades en sus servicios los mismos que son eficientes para el departamento administrativo, en cuanto a la segunda opción 16 funcionarios empleados(as) que corresponden al 57% opinaron que la empresa no ha aportado en nada en cuanto se refiere a las seguridades de sus servicios

PREGUNTA 3

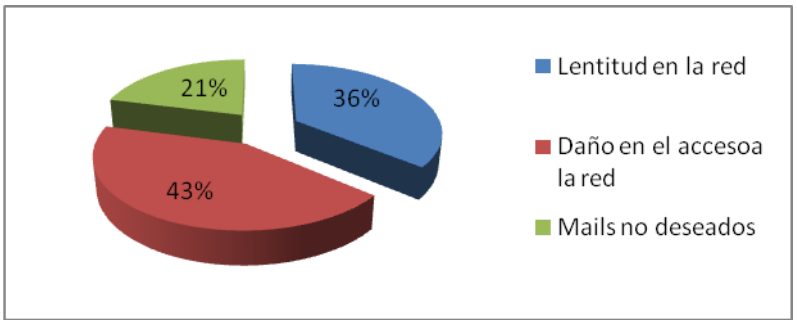
¿Cuáles son los problemas más importantes que se han presentado al usar el Internet en la Empresa GP Flowers?

TABLA No. 2.3: PROBLEMAS AL USAR EL INTERNET EN LA EMPRESA

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Lentitud de la red	10	36%
Daño en el acceso a la red	12	43%
Mails no deseados	6	21%
TOTAL	**28**	**100%**

Fuente: Funcionarios Empleados
Realizado por: Grupo Investigador

GRAFICO No. 2.3: PROBLEMAS AL USAR EL INTERNET EN LA EMPRESA



Fuente: Funcionarios Empleados
Realizado por: Grupo Investigador

ANÁLISIS E INTERPRETACIÓN

De las encuestas realizadas a 28 Funcionarios empleados (as) de la Empresa GP Flowers, 10 funcionarios empleados(as) que corresponden al 36% manifestaron que uno de los problemas que se presenta en la Empresa al utilizar el Internet es la lentitud en la red, mientras que 12 funcionarios empleados(as) que corresponden al 43% piensan que mediante el uso del Internet uno de los problemas que enfrenta la Empresa es el daño en el acceso a la red y 6 funcionarios empleados(as) que corresponden al 21% consideran que el uso del Internet provoca mails no deseados.

PREGUNTA 4

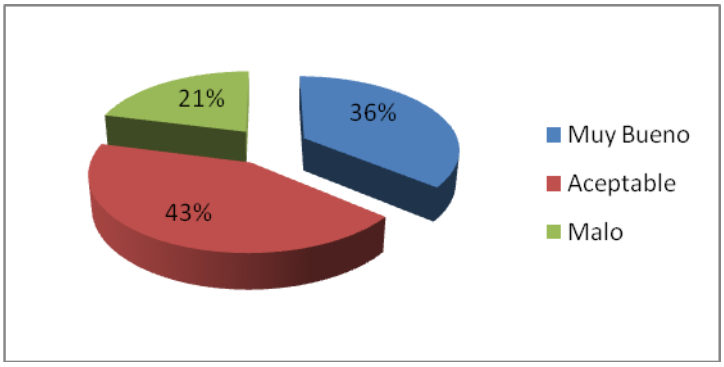
¿El servicio de Internet en la Empresa GP Flowers para realizar sus actividades cotidianas es?

TABLA No. 2.4: DESCRIPCION DEL SERVICIO DE INTERNET EN LAS ACTIVIDADES COTIDIANAS

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Muy bueno	10	36%
Aceptable	12	43%
Malo	6	21%
TOTAL	**28**	**100%**

Fuente: Funcionarios Empleados
Realizado por: Grupo Investigador

GRAFICO No. 2.4: DESCRIPCION DEL SERVICIO DE INTERNET EN LAS ACTIVIDADES COTIDIANAS



Fuente: Funcionarios Empleados
Realizado por: Grupo Investigador

ANÁLISIS E INTERPRETACIÓN

De las encuestas realizadas a 28 Funcionarios empleados (as) de la Empresa GP Flowers, 10 funcionarios empleados(as) que representan al 36% consideran que el servicio de Internet que posee la Empresa es muy bueno, por otro lado 12 funcionarios empleados(as) que representan al 43% opinan que el Internet de la Empresa es aceptable y 6 funcionarios empleados(as) que representan al 21% piensan que el Internet es malo.

PREGUNTA 5

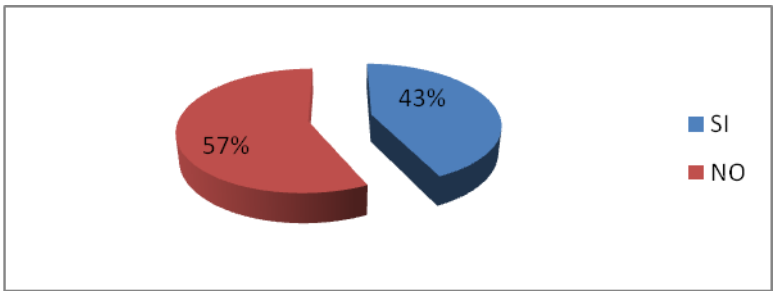
¿Considera que la información que circula en la red de la empresa está garantizada?

TABLA No. 2.5: LA INFORMACIÓN QUE CIRCULA EN LA RED DE LA EMPRESA ESTÁ GARANTIZADA

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	12	43%
NO	16	57%
TOTAL	**28**	**100%**

Fuente: Funcionarios Empleados
Realizado por: Grupo Investigador

GRAFICO No. 2.5: LA INFORMACION QUE CIRCULA EN LA RED DE LA EMPRESA ESTA GARANTIZADA



Fuente: Funcionarios Empleados
Realizado por: Grupo Investigador

ANÁLISIS E INTERPRETACIÓN

De las encuestas realizadas a 28 Funcionarios empleados (as) de la Empresa GP Flowers, 12 funcionarios empleados(as) que corresponden al 43% consideran que la información que circula en la red de la Empresa está garantizada, sin embargo 16 funcionarios empleados(as) que corresponden al 57% consideran todo lo contrario es decir piensan que la información que circula en la red de la Empresa no está garantizada

PREGUNTA 6

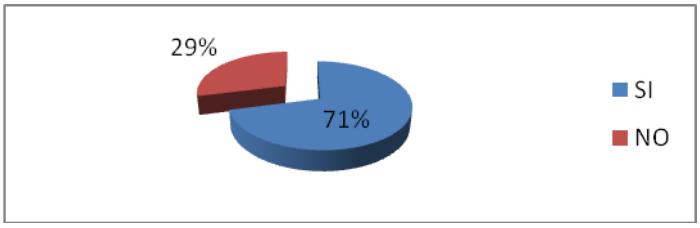
¿Considera que el uso de las TICS (Tecnología de la Información y de las Telecomunicaciones) permitirá solucionar las dificultades de seguridad en la conexión y prestación de servicios?

TABLA No. 2.6: EL USO DE LAS TICS (TECNOLOGÍA DE LA INFORMACIÓN Y DE LAS TELECOMUNICACIONES) PERMITIRÁ SOLUCIONAR LAS DIFICULTADES DE SEGURIDAD EN LA CONEXIÓN Y PRESTACIÓN DE SERVICIOS

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	20	71%
NO	8	29%
TOTAL	**28**	**100%**

Fuente: Funcionarios Empleados
Realizado por: Grupo Investigador

GRAFICO No. 2.6: EL USO DE LAS TICS (TECNOLOGÍA DE LA INFORMACIÓN Y DE LAS TELECOMUNICACIONES) PERMITIRÁ SOLUCIONAR LAS DIFICULTADES DE SEGURIDAD EN LA CONEXIÓN Y PRESTACIÓN DE SERVICIOS



Fuente: Funcionarios Empleados
Realizado por: Grupo Investigador

ANÁLISIS E INTERPRETACIÓN

De las encuestas realizadas a 28 Funcionarios empleados (as) de la Empresa GP Flowers, 20 funcionarios empleados(as) que corresponden al 71% consideran que el uso de las TICS (Tecnología de la Información y de las Telecomunicaciones) permitirá solucionar las dificultades de seguridad en la conexión y prestación de servicios, en cuanto a la segunda opción 8 funcionarios empleados(as) que corresponden al 29% consideran que el uso de las TICS (Tecnología de la Información y de las Telecomunicaciones) no es la solución para las dificultades de seguridad en la conexión y prestación de servicios.

PREGUNTA 7

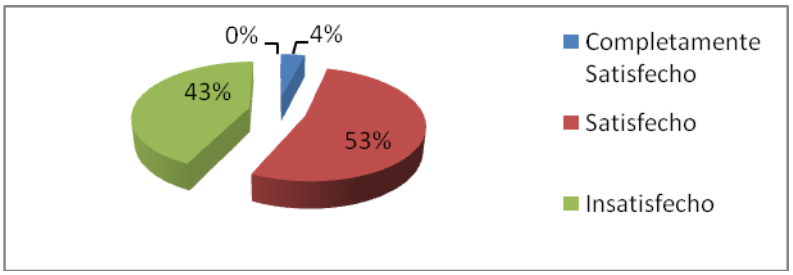
¿Cuál es su grado de satisfacción general con el uso de Internet en la Empresa GP Flowers?

TABLA No. 2.7: GRADO DE SATISFACCIÓN GENERAL CON EL USO DE INTERNET EN LA EMPRESA GP FLOWERS

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Completamente satisfecho	1	4%
Satisfecho	15	53%
Insatisfecho	12	43%
Completamente insatisfecho	0	0%
TOTAL	**28**	**100%**

Fuente: Funcionarios Empleados
Realizado por: Grupo Investigador

GRAFICO No. 2.7: GRADO DE SATISFACCION GENERAL CON EL USO DE INTERNET EN LA EMPRESA GP FLOWERS.



Fuente: Funcionarios Empleados
Realizado por: Grupo Investigador

ANÁLISIS E INTERPRETACIÓN

De las encuestas realizadas a 28 Funcionarios empleados (as) de la Empresa GP Flowers, 1 funcionario empleado(a) que representan al 4% se siente completamente satisfecho con el uso del internet de la empresa, por otro lado 15 funcionarios empleados(as) que representan al 53% consideran que su grado de satisfacción en cuanto al uso del internet que posee la empresa es satisfecho, mientras que 12 funcionarios empleados(as) que representan al 43% opinan que su grado de satisfacción mediante el uso del internet es insatisfecho y ningún encuestado opto por la última alternativa que era completamente insatisfecho..

PREGUNTA 8

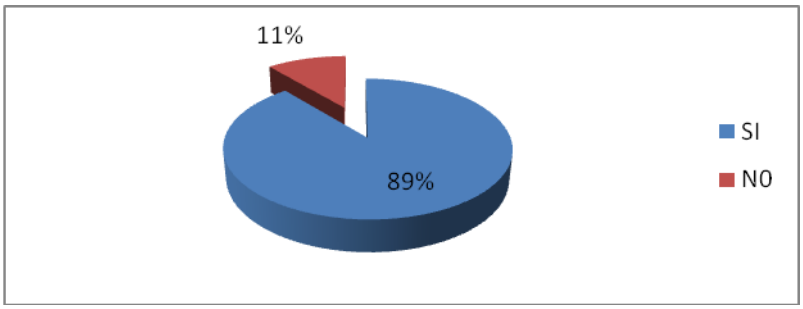
¿Considera usted que la transmisión de datos debe ser optimizada?

TABLA No. 2.8: LA TRANSMISIÓN DE DATOS DEBE SER OPTIMIZADA

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	25	89%
NO	3	11%
TOTAL	**28**	**100%**

Fuente: Funcionarios Empleados
Realizado por: Grupo Investigador

GRAFICO No. 2.8: LA TRANSMISIÓN DE DATOS DEBE SER OPTIMIZADA



Fuente: Funcionarios Empleados
Realizado por: Grupo Investigador

ANÁLISIS E INTERPRETACIÓN

De las encuestas realizadas a 28 Funcionarios empleados (as) de la Empresa GP Flowers, 25 funcionarios empleados(as) que corresponden al 89% consideran que la información que circula en la red de la Empresa de ser optimizada, sin embargo 3 funcionarios empleados(as) que corresponden al 11% consideran todo lo contrario es decir piensan que la información que circula en la red de la Empresa no debe ser optimizada.

PREGUNTA 9

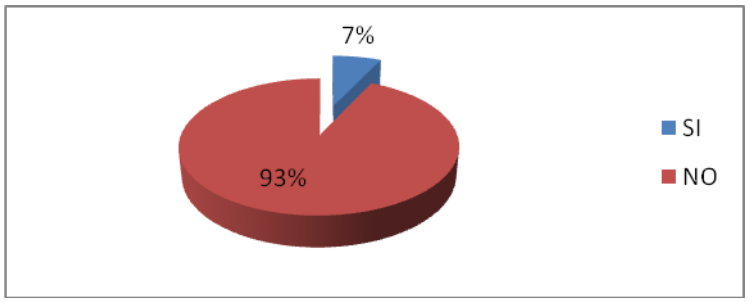
¿Conoce algo usted sobre VPN (Red Privada Virtual)?

TABLA No. 2.9: CONOCIMIENTO SOBRE VPN (Red Privada Virtual)

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Si	2	7%
No	26	93%
TOTAL	**28**	**100%**

Fuente: Funcionarios Empleados
Realizado por: Grupo Investigador

GRAFICO No. 2.9: CONOCIMIENTO SOBRE VPN (Red Privada Virtual)



Fuente: Funcionarios Empleados
Realizado por: Grupo Investigador

ANÁLISIS E INTERPRETACIÓN

De los 28 Funcionarios empleados (as) de la Empresa GP Flowers, 26 de los funcionarios empleados(as) encuestados que corresponde al 93% tienen conocimiento sobre VPN (redes privadas virtuales), mientras que 2 funcionarios empleados(as) que corresponden al 7% no tiene ningún conocimiento sobre VPN (redes privadas virtuales).

PREGUNTA 10

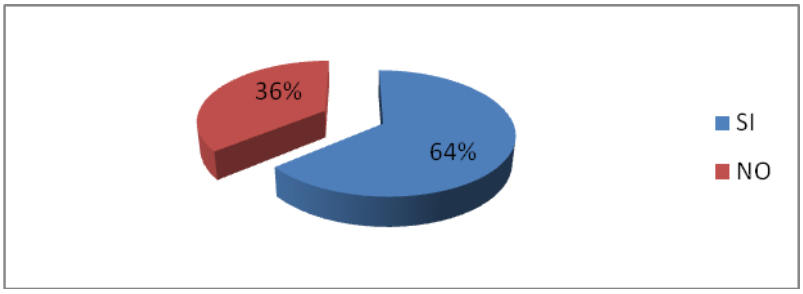
¿Considera usted que una VPN (Red Privada Virtual) va a garantizar el flujo de información?

TABLA No. 2.10: LA VPN (RED PRIVADA VIRTUAL) VA A GARANTIZAR EL FLUJO DE INFORMACIÓN

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Si	18	64%
No	10	36%
TOTAL	**28**	**100%**

Fuente: Funcionarios Empleados
Realizado por: Grupo Investigador

GRAFICO No. 2.10: LA VPN (RED PRIVADA VIRTUAL) VA A GARANTIZAR EL FLUJO DE INFORMACIÓN



Fuente: Funcionarios Empleados
Realizado por: Grupo Investigador

ANÁLISIS E INTERPRETACIÓN

De las encuestas realizadas a 28 Funcionarios empleados (as) de la Empresa GP Flowers, 18 funcionarios empleados(as) que corresponden al 84% consideran que la Red Privada Virtual (VPN) va a garantizar la información que circula en la red de la Empresa, sin embargo 10 funcionarios empleados(as) que corresponden al 36% consideran todo lo contrario es decir piensan que la Red Privada Virtual (VPN) no va a garantizar la información que circula en la red de la Empresa.

2.3.2. Verificación de Hipótesis

Una vez realizado la investigación de campo, los resultados son analizados e interpretados con mucho cuidado, llegando a lo previsto para determinar la hipótesis que es la **"Implementación de una vpn con seguridades de la red inalámbrica y red externa para la empresa exportadora de flores gp flowers ubicada en el cantón Latacunga."** evitando molestos contratiempos en el congestionamiento de la comunicación e información.

Una vez verificada podemos prescribir las siguientes valorizaciones de las encuestas realizadas.

- El 64 %de los encuestados manifiestan que no saben a que es una red inalámbrica.
- El 57% manifiestan que La Empresa ha prestado seguridades en servicios como el internet eficientes para el departamento financiero
- El 57 % de los investigados manifiestan considera que la información que circula en la red de la empresa está garantizada
- El 71 % de encuestados manifiestan que considera que el uso de las TICS (Tecnología de la Información y de las Telecomunicaciones) permitirá solucionar las dificultades de seguridad en la conexión y prestación de servicios
- El 89 % de los encuestados Consideran que la transmisión de datos debe ser optimizada

2.4. Conclusiones y recomendaciones

2.4.1. Conclusión

- Es importante implementar un vpn.
- Afecta de manera directa a las seguridades de la empresa

- Es notable que al momento del envío de información de la empresa se expone a toda la red de internet.

2.4.2. Recomendación

- Implementar dentro de la empresa una vpn.
- Garantizar la seguridad al momento del envío.
- Es importante dar paso a la tecnología que va marcando la diferencia con respecto a seguridades.

TABLA No. 2.11:

VERIFICACIÓN DE HIPOTESIS

No.	PREGUNTAS					
1	¿Conoce Ud. Sobre las Redes Inalámbricas?	**SI**	**NO**			
		36%	64 %			
2	¿La Empresa ha prestado seguridades en servicios como el internet eficientes para el departamento financiero?	**SI**	**NO**			
		43%	57 %			
3	¿Cuáles son los problemas más importantes que se han presentado al usar el Internet en la Empresa GP Flowers?	**Lentitud de la red**	**Daño en el acceso a la red**	**Mails no deseados**		
		36%	43 %	21%		
4	¿El servicio de internet en la empresa GP Flowers para realizar sus actividades cotidianas es?	**Muy bueno**	**Aceptable**	**Malo**		
		36 %	43 %	21 %		
5	¿Considera que la información que circula en la red de la empresa está garantizada?	**SI**	**NO**			
		43 %	57 %			

6	¿Considera que el uso de las TICS (Tecnología de la Información y de las Telecomunicaciones) permitirá solucionar las dificultades de seguridad en la conexión y prestación de servicios?	**SI**	**NO**			
		71 %	29 %			
7	¿Cuál es el grado de satisfacción general con el uso del internet en la empresa GP Flowers?	**Completamente Satisfecho**	**Satisfecho**	**Insatisfecho**	**Completamente insatisfecho**	
		4%	53 %	43%	0%	
8	¿Considera usted que la transmisión de datos debe ser optimizada?	**Si**	**No**			
		89 %	11 %			
9	¿Conoce algo usted sobre VPN (Red Privada Virtual)?	**SI**	**NO**			
		7 %	93%			
10	¿Considera usted que una VPN (Red Privada Virtual) va a garantizar el flujo de información?	**SI** 64%	**NO** 36%			

2.5. Análisis Global de los Resultados

Con los porcentajes conseguidos por la aplicación de varias preguntas realizadas a los funcionarios empleados(as) de la empresa GP Flowers, se puede observar claramente que existe un pequeño porcentaje que conoce algo sobre redes inalámbricas, del mismo modo la mayoría de la población opina que la empresa no ha brindado seguridades en servicios como el internet eficientes para el departamento administrativo, mientras que un porcentaje mayoritario considera que al utilizar el internet existe problemas pero el más importante es el daño en el acceso a la red, así como se puede observar que un porcentaje alto considera que la información que circula en la red de la empresa no está garantizada, casi en su totalidad los encuestados no conocen algo sobre lo que es una VPN (Red Privada Virtual) además en la siguiente inquietud planteada en la encuesta que se los hizo nos podemos dar cuenta que un porcentaje mayor piensa que la transmisión de datos debe ser optimizada.

Por otra parte la mayoría de funcionarios empleados(as) han señalado que una VPN (Red Privada Virtual) va a garantizar el flujo de información.

Las opciones y sugerencias manifestadas por los funcionarios empleados(as) fueron realmente importantes, ya que están nos sirvieron de mucho para la implementación de una VPN para que realice cada uno de los procesos de una manera rápida y eficiente y por supuesto que cuente con todas las seguridades necesarias para el correcto funcionamiento.

Ante los resultados se observa claramente la gran acogida a la propuesta de Implementar una VPN con seguridades de la red inalámbrica y red externa para la empresa exportadora de flores Gp Flowers ubicada en el Cantón Latacunga.

CAPITULO III

3. IMPLEMENTACIÓN DE LA VPN CON SEGURIDADES DE LA RED INALAMBRICA Y LA RED EXTERNA PARA LA EMPRESA EXPORTADORA DE FLORES GP FLOWER UBICADA EN EL CANTON LATACUNGA

3.1. Presentación

Una red privada virtual o VPN (virtual prívate network, Red Privada Virtual), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

La posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel en otro país. Todo ello utilizando la infraestructura de Internet.

Caso palpable ha sido la presente investigación la misma que se ha planteado para comunicar las oficinas centrales de la empresa florícola Gp Flowers de la ciudad de Latacunga que se encuentra ubicada en pleno centro económico de la ciudad y las instalaciones de la finca ubicada en el sector de Zaragozín, la empresa y los personeros de gp flowers por motivos de negocios en muchas ocasiones viajan al

extranjero y en ocasiones requieren de información pero en ocasiones resulta delicado llamar a solicitar la misma a personas que no forman parte de la empresa. En vista de esta realidad el grupo investigador ha creído conveniente que se desarrolle una vpn para resolver todos estos inconvenientes ya que de igual manera la atención en las oficinas se las hace medio día y el otro medio día el personal se traslada a la finca por lo que en algunas ocasiones se ha hecho necesario que el personal de contabilidad o secretaria tenga regresarse por uno o más archivos a las oficinas causando de esta manera perdidas a nivel de recurso económico y de tiempo.

3.2. Justificación

Hoy en día las aplicaciones transcendentales del hombre son confiadas en las computadoras ya sean en el ámbito social, económico y cultural por esta razón la informática viene a ser la ciencia al tratamiento racional y automático de la información por parte de las computadoras por lo que el desarrollo de una VPN que otorgue seguridades en la red inalámbrica y en la red externa permitirá una adecuada comunicación desde cualquier lugar logrando el progreso de la empresa.

La necesidad e importancia de desarrollar este tema es porque, se propone dar solución a los problemas como detectar mal servicio, congestionamiento, invasión, daños en la red, interferencias, deficiencia en el servicio de Internet y acceso a los recursos compartidos en forma ilegal, debido a que ésta por ser de carácter tecnológico debe estar en constante actualización; y al no contar con una VPN ocasionara el incumplimiento de los objetivos y metas propuestas por la entidad; además porque cada área debe contar con seguridades en la red inalámbrica y en la red externa para un mejor desenvolvimiento de toda la compañía.

El interés por investigar este tema es: Conocer los fenómenos, las causas y los efectos que están ocasionando la inexistencia de una VPN de seguridades en la red inalámbrica, perjudicando de esta manera a los usuarios que utilizan el Internet para realizar las actividades diarias de empleados y trabajadores.

Esta implementación de seguridades se realizará basándose en la realidad en que se encuentra la red inalámbrica de la empresa; y servirá como guía no solo para la empresa GP Flowers sino para las diversas empresas que requieran actualizar su red a través de una adecuada planificación que permitirá brindar al usuario servicios de calidad, estableciendo una mejor comunicación en cada una de las áreas y así como garantizar el verdadero flujo de la información, un eficiente ancho de banda, proporcionar los medios para controlar el acceso a las aplicaciones críticas de red inalámbrica, a los datos y a los servicios, con el objetivo que sólo los usuarios, administradores e información legitimada puedan utilizar la red de datos y evitar el ingreso de intrusos que podrían mermar los recursos de red con que cuenta la empresa.

Los resultados obtenidos dentro de la investigación tendrán una significación práctica ya que a través de la implementación de una VPN para seguridades tanto en la red inalámbrica como en la red externa, permitirá que la información fluya con mayor agilidad y a la vez determinara que no sean penetrados por acciones de intrusos que vulneren el normal desarrollo de la red que pueden causar averías dentro de la red.

Por estos aspectos los investigadores se han basado en instrumentos y teorías que nos permitirán la elaboración de la propuesta en donde tomamos en cuenta parámetros de seguridad reconocidos Internacionalmente; pero que tendrán que ser adaptados al equipo y a las necesidades que tienen la empresa para prevenir los problemas y las acciones de los Hackers que quieren vulnerar la información.

En la novedad científica al no contar la empresa GP Flowers con una VPN que permita a los trabajadores de dicha empresa conectarse a la red empresarial a pesar de encontrarse fuera de su lugar de trabajo, además que evite ingresar indebidamente a información clasificada que puede ser utilizada para perjudicar a la empresa por lo que se hace necesario implementar seguridades en la red inalámbrica y en la red externa basada en la tecnología de punta, al implementar estándares Internacionales y conjugar con las necesidades de la empresa.

La necesidad de manejar información segura en función de comercializar la flor en distintos puntos de la provincia que se encuentran a grandes distancias a repercutir en pérdida de la eficiencia de las transacciones. Lo que requiere una instalación de una red privada virtual que mejorar la actividad comercial.

3.3. Objetivos

3.3.1. Objetivo General

- Implementar una VPN con seguridades de la red inalámbrica y red externa para la empresa exportadora de flores GP Flowers ubicada en el cantón Latacunga.

3.3.2. Objetivo Especifico

- Determinar las necesidades de seguridad que existe en toda la red inalámbrica y en la red externa de la empresa Gp Flowers.

- Realizar un estudio de calidad y servicio de la VPN para detectar problemas y por ende dar soluciones**.**

- Implementar una Red Privada Virtual que mantenga la seguridad necesaria en el estándar que garantice la comercialización efectiva y la seguridad en los datos.

3.4. Servidores de Seguridad

Los diferentes tipos de servidores de seguridad utilizan distintas técnicas.

La mayor parte de los servidores de seguridad utilizan dos o más de las técnicas siguientes:

- Filtros de paquetes: un filtro de paquetes examina cada paquete que entra o sale de la red y acepta o rechaza el paquete según las reglas definidas por el usuario. El filtrado de paquetes es bastante eficaz y transparente, pero resulta difícil de configurar. Además, es vulnerable a la suplantación IP.

- Puerta de enlace a aplicaciones: una puerta de enlace a aplicaciones aplica mecanismos de seguridad a determinados programas, como FTP y Telnet. Esta técnica es muy eficaz, pero puede reducir el rendimiento.

- Puerta de enlace a capas de circuitos: esta técnica aplica mecanismos de seguridad cuando se establece una conexión de Protocolo de control de transporte (TCP) o de Protocolo de datagramas de usuario (UDP). Una vez establecida la conexión, los paquetes pueden fluir entre los hosts sin que se realice ninguna otra comprobación.

- Servidor proxy: un servidor proxy intercepta todos los mensajes que entran y salen de la red. El servidor proxy oculta de manera eficaz las direcciones de red verdaderas.

- Servidores proxy de la aplicación: los servidores proxy de la aplicación tienen acceso a toda la información en la pila de red. De esta manera, los servidores proxy pueden tomar decisiones basándose en la autorización básica (el origen, el destino y el protocolo) y filtrar comandos ofensivos o no permitidos en la secuencia de datos. Los servidores proxy de aplicaciones mantienen el "estado" de las conexiones de manera inherente. La característica Servidor de seguridad de conexión a Internet incluida en Windows XP es un servidor de seguridad que mantiene el estado

3.4.1. Mecanismo de acceso

Como hemos indicado en un apartado anterior, desde el punto de vista del usuario que se conecta a ella, el funcionamiento de una VPN es similar al de cualquier red

normal, aunque realmente para que el comportamiento se perciba como el mismo hay un gran número de elementos y factores que hacen esto posible.

La comunicación entre los dos extremos de la red privada a través de la red pública se hace estableciendo túneles virtuales entre esos dos puntos y usando sistemas de encriptación y autentificación que aseguren la confidencialidad e integridad de los datos transmitidos a través de esa red pública. Debido al uso de estas redes públicas, generalmente Internet, es necesario prestar especial atención a las cuestiones de seguridad para evitar accesos no deseados.

La tecnología de túneles (Tunneling) es un modo de envío de datos en el que se encapsula un tipo de paquetes de datos dentro del paquete de datos propio de algún protocolo de comunicaciones, y al llegar a su destino, el paquete original es desempaquetado volviendo así a su estado original.

En el traslado a través de Internet, los paquetes viajan encriptados, por este motivo, las técnicas de autenticación son esenciales para el correcto funcionamiento de las VPNs, ya que se aseguran a emisor y receptor que están intercambiando información con el usuario o dispositivo correcto.

La autenticación en redes virtuales es similar al sistema de inicio de sesión a través de usuario y contraseña, pero tienes unas necesidades mayores de aseguramiento de validación de identidades.

La mayoría de los sistemas de autenticación usados en VPN están basados en sistema de claves compartidas.

La autenticación se realiza normalmente al inicio de una sesión, y luego, aleatoriamente, durante el transcurso de la sesión, para asegurar que no haya algún tercer participante que se haya podido entrometer en la conversación.

Todas las VPNs usan algún tipo de tecnología de encriptación, que empaqueta los datos en un paquete seguro para su envío por la red pública.

La encriptación hay que considerarla tan esencial como la autenticación, ya que permite proteger los datos transportados de poder ser vistos y entendidos en el viaje de un extremo a otro de la conexión.

Existen dos tipos de técnicas de encriptación que se usan en las VPN: **Encriptación de clave secreta**, o privada, y **Encriptación de clave pública**.

En la **encriptación con clave secreta** se utiliza una contraseña secreta conocida por todos los participantes que van a hacer uso de la información encriptada. La contraseña se utiliza tanto para encriptar como para desencriptar la información. Este tipo de sistema tiene el problema que, al ser compartida por todos los participantes y debe mantenerse secreta, al ser revelada, tiene que ser cambiada y distribuida a los participantes, lo que puede crear problemas de seguridad.

La **encriptación de clave pública** implica la utilización de dos claves, una pública y una secreta. La primera es enviada a los demás participantes. Al encriptar, se usa la clave privada propia y la clave pública del otro participante de la conversación. Al recibir la información, ésta es desencriptada usando su propia clave privada y la pública del generador de la información. La gran desventaja de este tipo de encriptación es que resulta ser más lenta que la de clave secreta.

En las redes virtuales, la encriptación debe ser realizada en tiempo real, de esta manera, los flujos de información encriptada a través de una red lo son utilizando encriptación de clave secreta con claves que son válidas únicamente para la sesión usada en ese momento.

3.4.2. Seguridad

Conectarse a Internet sin un servidor de seguridad es como dejar las llaves en el automóvil con el motor en marcha y las puertas abiertas mientras entra en la tienda. Aunque es posible que pueda entrar y salir sin que suceda nada, alguien podría aprovechar esta oportunidad. En Internet, los piratas informáticos utilizan

código malintencionado (como virus, gusanos y troyanos) para intentar encontrar equipos desprotegidos.

Un servidor de seguridad puede proteger su equipo de este ataque de seguridad y de otro tipo.

Mientras que algunos ataques son simples molestias que gastan bromas pesadas, otros se crean con intención maliciosa. Estos ataques más graves pueden intentar eliminar información del equipo, bloquearlo o incluso robar información personal, como contraseñas o números de tarjeta de crédito. A algunos piratas simplemente les gusta acceder a equipos vulnerables. Los virus, gusanos y troyanos son de temer. Afortunadamente, puede reducir el riesgo de infección mediante un servidor de seguridad

3.5. Configuraciones del VPN

3.5.1. LOG ME IN

Logmein es un software que se encuentra gratuito en internet y que está en la capacidad de realizar vpn utilizando todos los recursos que cuentan las redes LAN de una o más empresas.

Este software utiliza los puertos que están abiertos en el correo electrónico sea este de hotmail, yahoo. gmail, etc.

Para el caso de la empresa gp flowers cuenta con una licencia de logmein ya que esta necesita de conexión permanente con las oficinas centrales desde las fincas cuando se requiere de información sin necesidad de mover al contingente humano para llevar o traer la información en medios magnéticos o enviar y recibir información a través de correo electrónico arriesgando de esta manera todos los recursos empresariales, la ventaja que tiene este software que se ha probado en la empresa antes mencionado es que puede ser utilizado desde cualquier parte del

mundo solamente con que se cuente con una cuenta de correo electrónico en las principales paginas dedicadas a prestar servicios.

Dentro de las características importantes que hemos podido observar en este software están:
Hay tres tipos de redes que puede configurar con Hamachi; **Meshed**, **Hub y Spoke**, y **Gateway**.

Meshed: Este tipo de red es la norma cuando se refiere a conexiones entre pares. En este tipo de red, todos los usuarios tendrán una conexión directa con todos los demás usuarios.

Hub-y-Spoke: Este es un tipo de red donde una o más computadoras funcionará como el centro de la red, y todos los otros equipos enviar su tráfico a los ordenadores, que luego se enviaron a la computadora de destino. Muy parecido al de una rueda si uno o más equipos están en el centro, y todos los demás equipos están en los radios. Este tipo de red es lo que se suele utilizar en una red de área local (LAN).

Gateway: Este tipo de red que se utiliza en la situación para conectar dos o más LANs a través de la VPN mediante el establecimiento de un servidor como un nodo de puerta de enlace, lo que permite el tráfico hacia y desde la red que controla el acceso a viajar en la VPN. Esta red requiere un sistema operativo que puede establecer un puente de red. Windows 2000 (Server y Workstation) y Small Business Server 2003 no puede crear la Red Puentes, y por lo tanto no puede ser utilizado como puerta de enlace de los nodos.

GRÁFICO 3.1. LogMeIn

Fuente: http://www.wikipedia.com

El logo que demuestra las empresas que aportan a la investigación de nuevas soluciones informáticas que aportan a una mejor administración de los recursos empresariales, logmein a parte de un software de vpn permite agilitar la comunicación con dispositivos móviles los mismos que son limitados en memoria y almacenamiento utilizan los recursos de los computadores a los que están accediendo.

GRÁFICO 3.2. LogMeIn

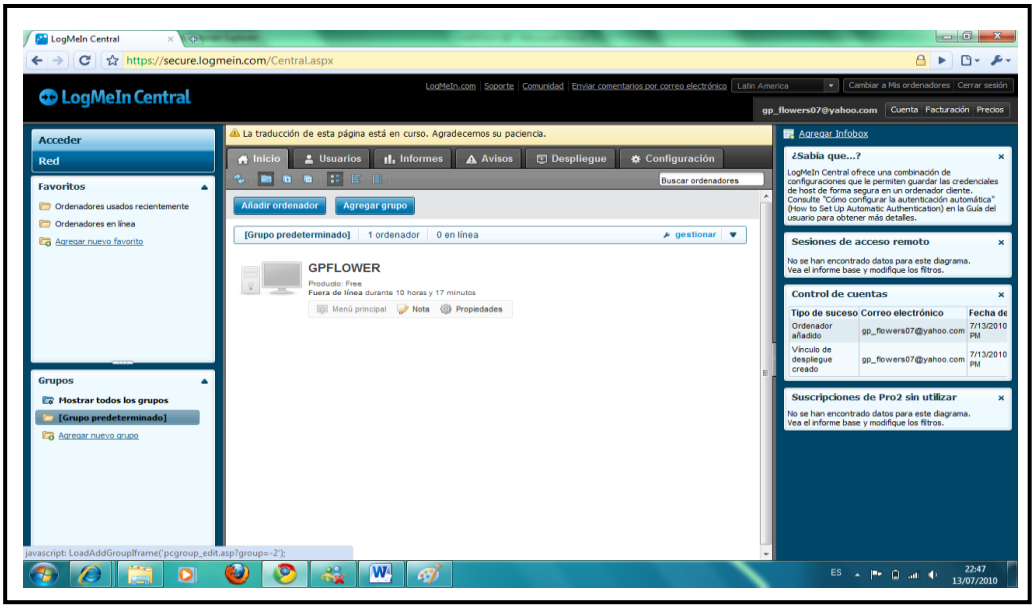
Fuente: http://www.logmein.com

Para poder administrar de forma remota las computadores o los servidores que se encuentren dentro de la familia Microsoft, es necesario hacer notar que el software a nivel de cliente puede trabajar dentro de Linux, Solaris o desde el mismo MAC, pero a nivel de host solamente puede ser instalado en Windows NT Service Pack

4, Windows 2000 Server Advanced Server y Profesional, Windows 2003 Server, Windows 2008, para los servidores y para clientes desde Windows Me en adelante.

El acceso a las redes de Área local de cualquier empresa se hace a través de los puertos de navegación de internet es decir del puerto de http y del htpps.

GRÁFICO 3.3. LogMeIn Central 1



Fuente: http://www.logmein.com

El software para la administración del servidor de host se debe de instalar el msi que está disponible en la pagina web: www.logmein.com, aquí se puede tener todas las opciones de configuraciones para la administración de los equipos.

GRÁFICO 3.4. LogMeIn Central 2

Fuente: http://www.logmein.com

Esta herramienta es tan poderosa que permite de igual manera iniciar la sesión en un equipo así este se encuentre apagado, siempre y cuando esta mantenga una conexión a una red con conexión física de cable ya que las tarjetas de red no se pueden apagar cuando el equipo de cómputo cambia de estado, la administración se lo puedo hacer de forma remota con todos los privilegios que esto puede brindar.

Todas las actividades que se realizan en el cliente lo ejecuta el equipo host o denominado en la mayoría de casos como servidores.

La ventaja se la puede observar de mejor manera cuando se puede trabajar en equipos que cuenten con sistemas operativos que sean SERVER ya que estos privilegios son los que ayudan al software a desplegar todas sus fortalezas.

3.5.2. OPEN VPN

OpenVPN es una solución de conectividad basada en software: SSL (Secure Sockets Layer) VPN Virtual Private Network (red virtual privada), OpenVPN ofrece conectividad punto-a-punto con validación jerárquica de usuarios y host conectados remotamente, resulta una muy buena opción en tecnologías Wi-

Fi (redes inalámbricas EEI 802.11) y soporta una amplia configuración, entre ellas balanceo de cargas.

OpenVPN, es un producto de software creado por James Yonan en el año 2001 y que ha estado siendo mejorado desde entonces.

Ninguna otra solución ofrece una mezcla semejante de seguridad a nivel empresarial, seguridad, facilidad de uso y riqueza de características.

Es una solución multiplataforma que ha simplificado mucho la configuración de VPN's dejando atrás los tiempos de otras soluciones difíciles de configurar como IPsec y haciéndola más accesible para gente inexperta en este tipo de tecnología.
Supongamos que necesitamos comunicar diferentes sucursales de una organización. A continuación veremos algunas soluciones que se han ofrecido como respuesta a este tipo de necesidades.

En el pasado las comunicaciones se realizaban por correo, teléfono o fax. Hoy en día hay factores que hacen necesaria la implementación de soluciones más sofisticadas de conectividad entre las oficinas de las organizaciones a lo largo del mundo.

Dichos factores son:

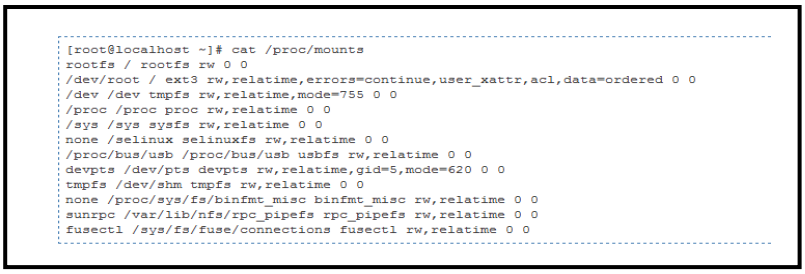
- La aceleración de los procesos de negocios y su consecuente aumento en la necesidad de intercambio flexible y rápido de información.

- Muchas organizaciones tienen varias sucursales en diferentes ubicaciones así como también tele trabajadores remotos desde sus casas, quienes necesitan intercambiar información sin ninguna demora, como si estuvieran físicamente juntos.

- La necesidad de las redes de computación de cumplir altos estándares de seguridad que aseguren la autenticidad, integridad y disponibilidad.

Procedemos a descargar el paquete de vpn en cualquier página de Linux sea Centos, Fedora o Red had, se procede a instalar mediante el comando yum $ yum –y installopenvpn*

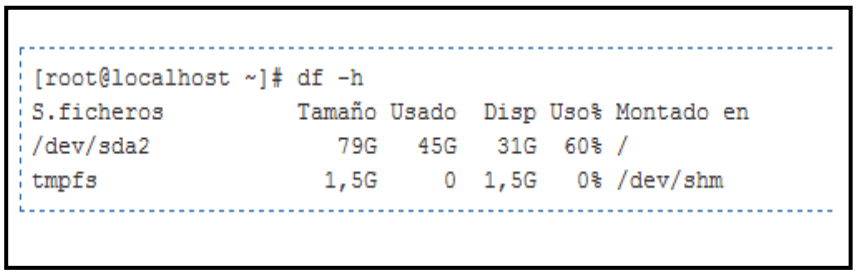
GRÁFICO 3.5. Comando yum $ yum –y installopenvpn*



Fuente: http://www.logmein.com

Una vez desempaquetado el software de encriptación de envió/recepción de archivos mediante el internet podemos observar esta pantalla la misma que nos muestra todos los archivos de configuración que se encuentran arriba.

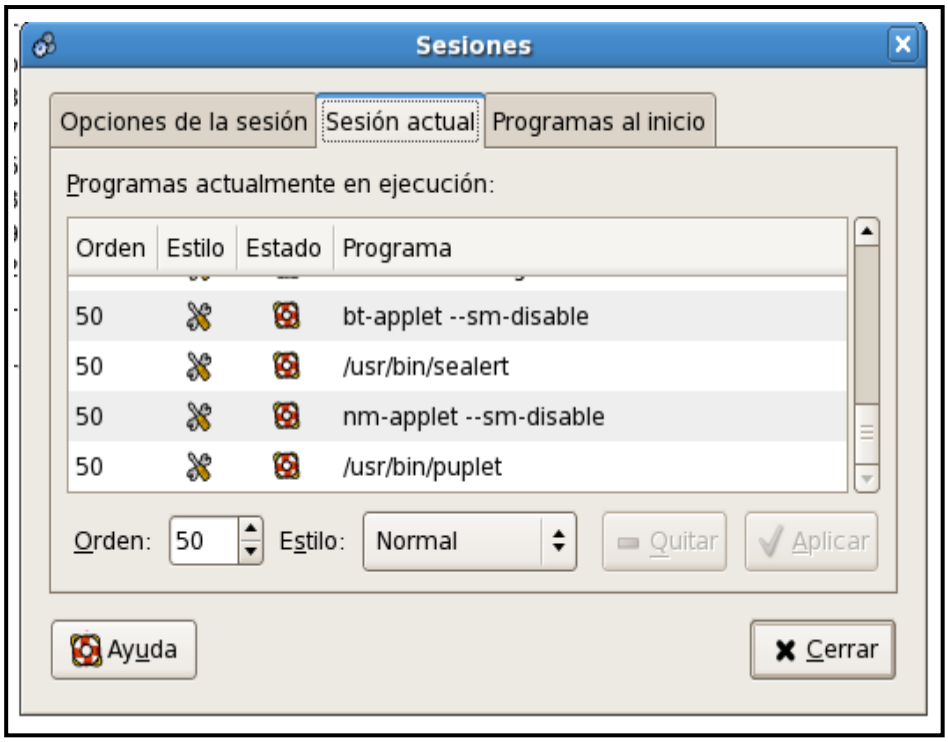
GRÁFICO 3.6. Archivo de Configuración



Fuente: http://www.logmein.com

Nos muestra toda la información que dispone los dispositivos de almacenamiento para la transmisión de la información

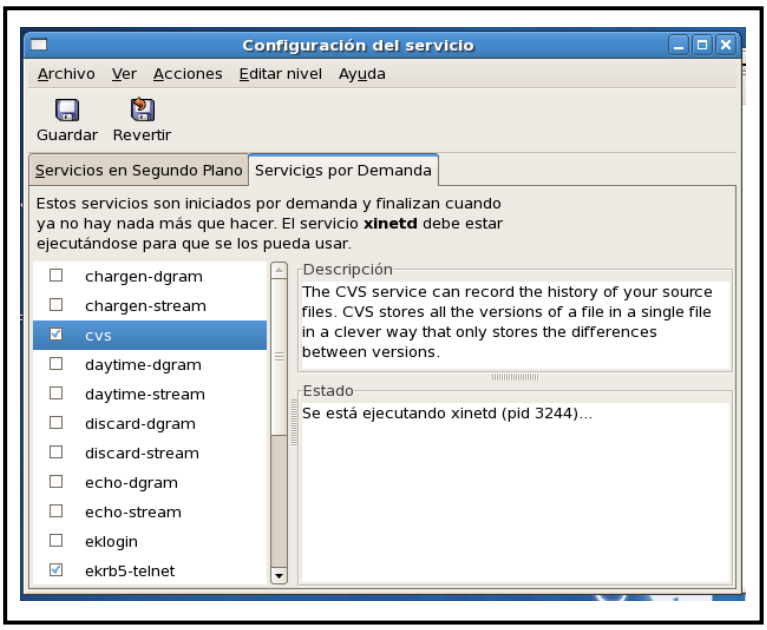
GRÁFICO 3.7. Almacenamiento para la Transmisión de la Información



Fuente: http://www.logmein.com

Una vez instalada la versión de openvpn se creara una carpeta dentro del directorio etc. que es donde se almacena todas las configuraciones que tiene Linux.

GRÁFICO 3.8. Configuración del Servicio

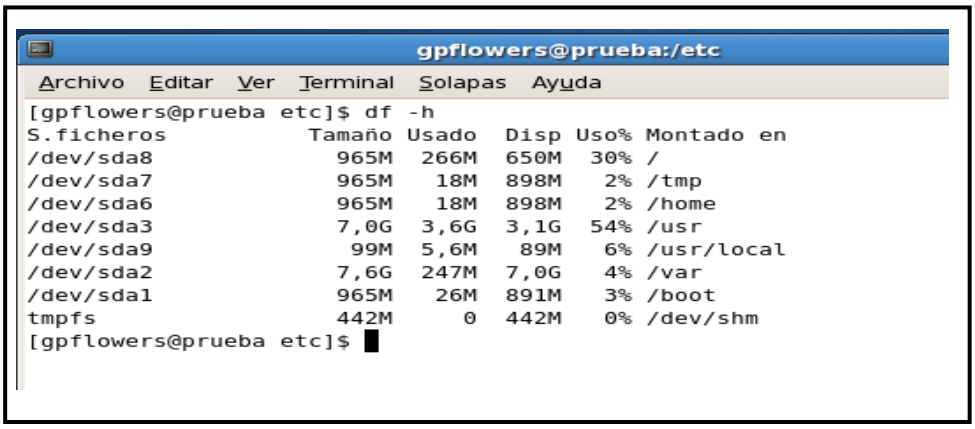


Fuente: http://www.logmein.com

En el directorio del vpn se creara algunos archivos y subcarpetas las mismas que contienen información de las configuraciones que tienen todos los servicios.

$ ls –la o la alternativa $ ll

GRÁFICO 3.9. Directorio



Fuente: http://www.logmein.com

Dentro de las configuraciones que cuentan el openvpn podemos detallar en el siguiente cuadro el cual muestra un completo análisis de cada una de las funciones.

TABLA 3.1. Funciones

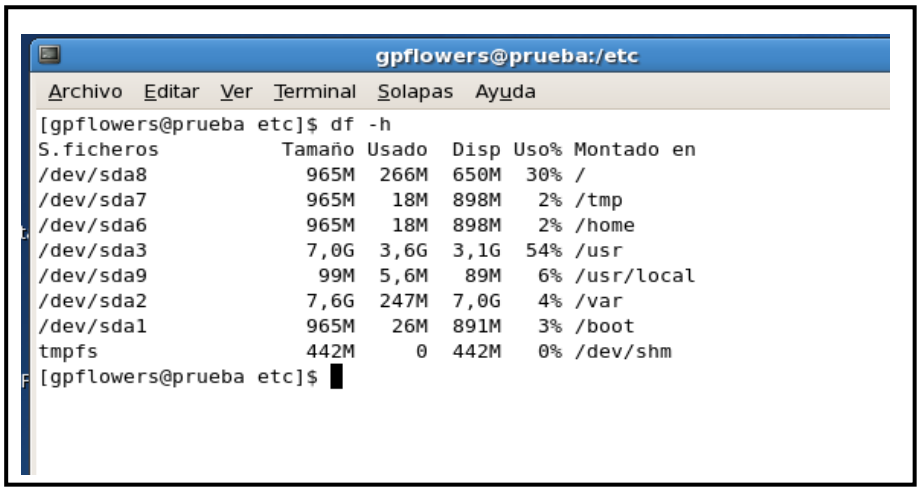
Port:	Especifica el puerto que será utilizado para que los clientes vpn puedan conectarse al servidor.
Proto:	tipo de protocolo que se empleará en la conexión a través de VPN
dev:	Tipo de interfaz de conexión virtual que se utilizará el servidor openvpn.
Ca	Especifica la ubicación exacta del fichero de Autoridad Certificadora [.ca].
cert:	Especifica la ubicación del fichero [.crt] creado para el servidor.
key:	Especifica la ubicación de la llave [.key] creada para el servidor openvpn.
dh:	Ruta exacta del fichero [.pem] el cual contiene el formato de DiffieHellman (requirerido para **--tls-server**solamente).
server:	Se asigna el rango IP virtual que se utilizará en la red del túnel VPN.
Ifconfig-pool-persist:	Fichero en donde quedarán registrado las direcciones IP de los clientes que se encuentran conectados al servidor OpenVPN.
Keepalive 10 120 :	Envía los paquetes que se manejan por la red una vez cada 10 segundos; y asuma que el acoplamiento es abajo si ninguna respuesta ocurre por 120 segundos.
comp-lzo:	Especifica los datos que recorren el túnel vpnserá compactados durante la trasferencia de estos paquetes.
persist-key:	Esta opción soluciona el problema por llaves que persisten a través de los reajustes SIGUSR1, así que no necesitan ser releídos.
persist-tun:	Permite que no se cierre y re-abre los dispositivos TAP/TUN al correr los guiones up/down

status	fichero donde se almacenará los eventos y datos sobre la conexión del servidor [.log]
verb 3:	Nivel de información (default=1). Cada nivel demuestra todo el Info de los niveles anteriores. Se recomienda el nivel 3 si usted desea un buen resumen de qué está sucediendo.

Fuente: LOS INVESTIGADORES

El vpn nos ayudó a poder compartir información entre dos segmentos de las redes que no podían comunicarse y también para poder controlar desde grandes distancias el trabajo que se tiene pendiente en las oficinas centrales dentro de la empresa florícola

GRÁFICO 3.10. Compartimiento de Información



Fuente: http://www.logmein.com

Verificación de Objetivos

Para el desarrollo de la presente investigación se había planteado como objetivo general el implementar una VPN con seguridades de la red inalámbrica y red externa para la empresa exportadora de flores GP Flowers ubicada en el cantón Latacunga, debido a que se consume grandes cantidades de recursos tanto económicos como de personal por la distante que se encuentran las instalaciones

desde las oficinas principales en el parque Vicente león hacia la finca que se encuentra ubicada en Zaragozín, en una distancia de más de 10 Km.

Dentro de los grandes inconvenientes que se podía encontrar al empezar la investigación era que no se disponía de una comunicación permanente entre computadores es decir no existía una red de datos que pudiera ayudar a enviar y recibir información entre las oficinas principales y la finca.

Debido a esto nosotros como grupo investigador planteamos la implementación de una vpn que ayude al envió/recepción de la información entre las oficinas principales y la finca donde se desarrolla toda la actividad de la empresa florícola, es necesario mencionar que la industria cuenta con el capital humano y tecnológico para poder desarrollar toda la investigación ya que disponen de la gerencia, contabilidad y un asesor tecnológico en el área de sistemas.

El problema se suscita con él envió de información que se lo hace desde las oficinas por correo electrónico el mismo que no es suministrado por ningún software de intranet corporativo sino desde las cuentas de Hotmail, yahoo y gmail las mismas que son seguras pero solo para uso de forma general y más no especifica en información confidencial.

En razón a esto con la implementación de un servidor en openvpn y con la ayuda de la herramienta gratuita de internet como es el logmein se pudo enviar y recibir información en tiempo real desde las oficinas a cualquier parte en donde se encuentre las personas que administren la información que se genere en la oficinas matrices de la empresa.

Por otro lado para cumplir con el objetivo general se tenía en consideración tres objetivos específicos los mismos que sumando podrían ayudar a cumplir este objetivo general:

Determinar las necesidades de seguridad que existe en toda la red inalámbrica y en la red externa de la empresa Gp Flowers, como se mencionó anteriormente no cuenta con seguridad alguna la red ya que solamente cuenta con un router que

provee el servicio de internet el mismo que fue contratado por la empresa telconet de la ciudad de Quito el cual cuenta con una muy buena señal hacia las oficinas lo que resulta difícil es la comunicación interna ya que no cuenta con un servidor centralizado para la administración de recursos tecnológicos.

Realizar un estudio de calidad y servicio de la VPN para detectar problemas y por ende dar soluciones, al probar y demostrar que los servicios del VPN se desarrollan con toda normalidad damos por cumplido este objetivo que era de medir el desempeño del envió/recepción de la información mediante la cuantificación del desempeño de la aplicación que se desarrolló para este fin**.**

Implementar una Red Privada Virtual que mantenga la seguridad necesaria en el estándar que garantice la comercialización efectiva y la seguridad en los datos, finalmente se cumplió con la implementación de la VPN como se manifestó en las páginas de desarrollo de este proyecto ya que se cuenta con el software necesario para la administración remota para poder copiar la información necesaria para optimizar recursos tanto de hardware, redes como de software que se genera en las oficinas centrales y que con tranquilidad se lo puede enviar a cualquier sitio donde se encuentre el personal que labora en la empresa gp flowers.

Comprobación de Hipótesis

Al iniciar la investigación nos habíamos planteado como hipótesis

La implementación de una VPN para seguridades en la red inalámbrica y en la red externa mejorará la calidad de servicio para los empleados y clientes de la empresa GP Flowers evitando molestos contratiempos en el congestionamiento de la comunicación e información.

Se logró conseguir que la información que se genera dentro de la empresa sea ésta en las oficinas o en finca se encuentre a buen recaudo ya que una vpn hoy en día es la solución tecnológica a la encriptación de cuentas de correo a nivel mundial y son

las más utilizadas por los estándares de la IEEE en lo que tiene que ver al manejo de seguridades en redes inalámbricas.

En empresas como gp flowers el tiempo significa mucho dinero es por eso que con la vpn los costos son bajos porque solo realizo llamadas a través del internet mediante un modem inalámbrico hacia las oficinas principales para poder tomar la información que se requiera para poder ejecutar los procesos en la finca o en las propias oficinas, otra de las ventajas fue el tener la posibilidad de que los datos viajen encriptados y seguros, con una buena calidad y velocidad.

3.6. CONCLUSIONES

1. Las redes inalámbricas están tomando mucha importancia en las actividades empresariales de hoy en día. Para lograr ser competitivos se requiere tener un acceso a la información de la empresa florícola gp flowers que se encuentra ubicadas en la ciudad de Latacunga provincia de Cotopaxi de una manera rápida y sin restricciones en cualquier momento y lugar.

2. La velocidad de las redes inalámbricas es satisfactoria cuando se trata de transmisión y acceso a archivos de datos. Esto no sucede cuando se trata de transferencia de imágenes o videos según las pruebas realizadas por parte del grupo investigador con el técnico de sistemas de la empresa gp flowers mediante las herramientas utilizadas como el logmein.

3. Las seguridades dentro de las redes inalámbricas, al igual que una red cableada, tiene sus desventajas, pero actualmente se están estudiando mejoras para efectivizarlas y dar confianza a los usuarios de la misma.

4. Una red inalámbrica bien configurada, es tan eficiente como una red cableada. Pues podemos tener una comunicación de datos en tiempo real y seguro.

5. Si el diseño no es correcto al configurar e implantar una red inalámbrica, se puede interferir en otra red inalámbrica cercana ya que la empresa y sus empresas se encuentran en pleno centro comercial de la ciudad.

6. Los costos de mantenimiento en una red inalámbrica, son menores que los costos de una red cableada; ya que en una red cableada cualquier remodelamiento de un espacio físico contribuye al incremento de gastos.

7. La investigación siempre es de gran aporte a la realidad de nuestra comunidad ya que con precios bajos se pueden obtener grandes aportes a empresas que recurren a la Universidad como alternativa para mejorar sus servicios

8. Se debe tomar siempre en cuenta los estándares y normas internacionales para la configuración y administración de ciertos servicios con que cuentan las configuraciones de una VPN sea esta pública o privada de la institución

9. El continuo avance de las tecnologías ha influenciado notablemente en la reestructuración de los estándares de la IEEE y de las normas ISO y dentro de estos se ha implementado el Código de Práctica para la Administración de la Seguridad de la Información.

10. La capacitación de nuevas tecnologías en el personal que labora en gp flowers se lo debe hacer de inmediato ya que esto mejorara en el desempeño de las funciones de todos los que laboran en esta importante empresa.

3.7. RECOMENDACIONES

1. Se recomienda realizar mayores aportes de parte del personal técnico con que cuenta la empresa para que de esta manera mejorar los servicios en las redes inalámbricas y en las configuraciones de los VPN que están en funcionamiento pero que requieren de soporte técnico especializado.

2. Al utilizar redes inalámbricas, se recomienda que estas sean utilizadas para transferencias y acceso a archivos de datos, pues por el momento, es en este punto donde denota su mayor utilidad.

3. Se recomienda utilizar redes inalámbricas en medios en los que continuamente se realizan cambios de infraestructura dentro de un edificio, pues su costo a la larga es mucho más conveniente.

4. Se debe realizar un análisis de diseño antes de implementar una red inalámbrica, pues de su buen diseño y configuración depende de que no interfiera en otras redes cercanas.

5. La adquisición de equipos sean estos servidores o equipos personales se lo debe realizar buscando cumplir con las expectativas de la empresa o institución donde se vaya a implementar la red inalámbrica.

6. Los servidores establecidos en la empresa gp flowers de Latacunga son los necesarios en la actualidad pero para un futuro con el crecimiento se debería pensar en incrementar muchos más recursos sobre todo para fomentar la investigación.

7. Los estándares aplicados en este proyecto de tesis están siempre en actualización por lo cual no se debe dejar de revisar dichas actualizaciones y aplicar a la empresa donde se lo implemente para poder dar un mejor servicio a los usuarios y para mantener un mejor control sobre estos.

8. Se recomienda la capacitación en el manejo responsable de las redes inalámbricas que en la actualidad se encuentra implementadas en la empresa.

3.8. GLOSARIO DE TÉRMINOS Y SIGLAS

Acceso Físico

Es el medio utilizado para obtener información de las oficinas, salas de cómputo, escritorios y archivos.

Acceso Lógico

Es el medio utilizado para obtener información de las bases de datos y sistemas de información de la organización.

Activos

Son los recursos de la organización. Existen varios tipos de activos como son: Los recursos de información (bases de datos, los documentos de sistemas), los recursos de software (software de sistemas operativos, herramientas de desarrollo), activos físicos (equipamiento informático, equipos de comunicaciones, otros) y servicios (iluminación, energía eléctrica, etc.)

Amplitud de banda

La amplitud de banda especifica la cantidad de datos que pueden transmitirse en una cantidad de tiempo fija. En el caso de los dispositivos digitales, la amplitud de banda se define en bits por segundo (bps) o bytes por segundo.

ASIC

Circuito integrado específico de una aplicación. Chip personalizado diseñado para una aplicación específica.
Asignaciones de amplitud de banda
La cantidad de amplitud de banda asignada a una aplicación, usuario o interfaz específicos.

Anomalía

Irregularidad en el funcionamiento de un sistema, de un software, de un control, etc.

Camino Forzado

Ruta limitada entre una Terminal de usuario y los servicios del computador. Evita que los usuarios seleccionen rutas fuera de la trazada entre su Terminal y los servicios a los cuales está autorizado a acceder.

Canal Oculto

Es un cauce de comunicación que permite a un proceso receptor y aun emisor intercambiar información de forma que viole la política de seguridad del sistema; esencialmente se trata de un método de comunicación que no es parte del diseño original del sistema pero que puede utilizarse para transferir información a un proceso o usuario que a priori no estaría autorizado a acceder a dicha información.

Clave Pública

Clave que puede ser revelada a cualquier persona.

Clave Secreta

Clave que debe mantenerse en secreto.

Código Troyano

Es un programa que llega al ordenador de manera encubierta, aparentando ser inofensivo, se instala y realiza determinadas acciones que afectan a la confidencialidad del usuario afectado.

Comercio Electrónico

Consiste en la compra, venta, marketing y suministro de información complementaria para productos o servicios a través de redes informáticas.

Computación Móvil

Se define como la serie de artefactos y equipos portátiles, hardware, que hacen uso de la computación para lograr su funcionamiento, así, se tiene a las computadoras portátiles, los teléfonos celulares, los cuadernos de notas computarizados, las calculadoras de bolsillo, etc.

Criptografía

Dícese de la ciencia que estudia la forma de codificar y descodificar documentos, de forma que sólo puedan ser leídos por la persona que posee la clave de descodificación.

Capa 2

Capa de vínculo de datos o capa MAC. Contiene la dirección física de un cliente o estación de servidor. El proceso de la capa 2 es más rápido que el de la capa 3 porque hay menos información que deba procesarse.

Capa 4

Establece una conexión y garantiza que todos los datos lleguen a su destino. Los paquetes inspeccionados en el nivel de la capa 4 se analizan y las decisiones se reenvían en función de sus aplicaciones.

Capa MAC

Subcapa de la capa de control de vínculo de datos (DTL).

Class of Service (Clase de servicio)

La clase de servicio es el esquema de prioridad 802.1p. La CoS proporciona un método para asignar etiquetas a los paquetes con información sobre la prioridad. Un valor de CoS situado entre 0 y 7 se agrega al encabezado de la capa 2 de los paquetes, donde cero es la prioridad más baja y siete es la más alta.
Transmisión de superposición de dos o más paquetes que colisionan. Los datos transmitidos no pueden utilizarse, y la sesión se reinicia.

Dirección IP

Dirección del protocolo de Internet. Dirección exclusiva asignada a un dispositivo de red con dos o más LAN o WAN interconectadas.

Dirección MAC

Dirección Media Access Control. La dirección MAC es una dirección específica del hardware que identifica cada nodo de red.

DSCP

DiffServe Code Point (DSCP). DSCP proporciona un método de asignación de etiquetas de paquetes IP con información de prioridad QoS.

Evaluación de Riesgos

Es un proceso dirigido a estimar la magnitud de aquellos riesgos que no hayan podido evitarse, obteniendo la información necesaria para que el empresario esté en condiciones de tomar una decisión apropiada sobre la necesidad de adoptar medidas preventivas y, en tal caso, sobre el tipo de medidas que deben adoptarse.

La evaluación de riesgos consta de una fase llamada de análisis de riesgos (identificación de peligros y estimación de los riesgos) y una fase posterior de valoración de riesgos y de control de riesgos si fuese posible.

Evidencia

Datos, registros, declaraciones de hecho o cualquier otra información que respaldan la existencia o veracidad de algo.

HONEYPOTS (Tarro de Miel)

Recurso de red destinado ha ser atacado o comprometido. Los Honeypots son los encargados de proporcionar información valiosa sobre los posibles atacantes en potencia a nuestra red antes de que comprometan sistemas reales. Es decir el objetivo de los Honeypots es recibir los ataques, no recoger información para demandar a los atacantes del Honeypot.

HONEYNETS (Tarro de Miel)

Es un tipo de Honeypot. Específicamente es un Honeypot altamente interactivo diseñado para la investigación y la obtención de información sobre atacantes. Un Honeynet es una arquitectura, no un producto concreto o un software determinado. Y consiste no en falsear datos o engañar a un posible atacante (como suelen hacer algunos Honeypot), sino que el objetivo principales recoger información real de cómo actúan los atacantes en un entorno de verdad.

Incidente

Dícese del fallo que sucede en un equipo o sistema de manera temporal o aleatoria, sin que existan unos motivos claros para ello.

Procesamiento de Información

Es la capacidad del Sistema de Información para efectuar cálculos de acuerdo con una secuencia de operaciones preestablecida.

Estos cálculos pueden efectuarse con datos introducidos recientemente en el sistema o bien con datos que están almacenados.

Seguridad Informática

Conjunto de técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionales. Estos daños incluyen el acceso a bases de datos de personas no autorizadas, el mal funcionamiento del hardware y la pérdida física de datos.

Seguridad de la Información

La seguridad de la información consiste en proteger uno de los principales activos de cualquier empresa: la información. La seguridad de la información es requisito previo para la existencia a largo plazo de cualquier negocio o entidad. La información es usada en cada uno de los ámbitos empresariales, los cuales dependen de su almacenamiento, procesado y presentación.

Servicio de Información

Un servicio para los sistemas que proporciona un sistema de base de datos para los archivos de configuración comunes.

Servicio de Red

Es un servicio para que cualquier máquina de la red puede comunicarse con otra distinta y esta conectividad permite enlazar redes físicamente independientes.

Sistema de Información

Conjunto de elementos, ordenadamente relacionados entre sí que aporta al sistema objeto, es decir, a la organización a la cual sirve y le marca directrices de

funcionamiento, la información necesaria para el cumplimiento de sus fines, para lo cual tendrá que recoger, procesar y almacenar la información, facilitando la recuperación de la misma.

Sistema Informático

Es aquel sistema que se encarga del manejo de información en la computadora, a través de la cual el usuario controla las operaciones que realiza el procesador.

Sistema Operativo

Termino que se utiliza para referirse al conjunto de programas interrelacionados, que se dedican a controlar las funciones básicas del sistema, las operaciones de bajo nivel y el manejo de archivos sin necesidad de que intervenga un operador.

Software Malicioso

Software que ha sido deliberadamente diseñado para producir un resultado defectuoso o dañoso para el usuario. Incluye tanto la categoría genérica de los virus informáticos, como la del llamado spyware.

Trabajo Remoto

Se refiere al trabajo que una persona realiza por fuera de supuesto de trabajo normal.

Utilitarios del Sistema

Reconstruir índices, compactar y validar bases de datos, validar consistencia de datos, cambiar fecha de operación y del sistema, importar y exportar datos entre empresas, transferir productos, precios, existencias de almacén y acceso al generador de reportes.

TFTP

Protocolo trivial de transferencia de archivos. Utiliza el protocolo de datos de usuario (UDP) sin características de seguridad para transferir archivos.

Trama

Los paquetes que contienen el encabezado y la información de cola que requiere el medio físico.

Tramas gigantes

Permiten transportar datos idénticos en menos tramas. Las tramas gigantes reducen el coste, necesitan un tiempo de procesamiento inferior y garantizan menos interrupciones.

Velocidad de puerto

Indica la velocidad del puerto. La velocidad de los puertos incluye:
Ethernet 10 Mbps
Fast Ethernet 100 Mbps
Gigabit Ethernet 1000 Mbps

3.9. BIBLIOGRAFÍA

- **Andrew Tanenbaum,** Redes de Computadores, Cuarta Edición 2004
- **Tyson Creer,** Así son las Intranets, Segunda Edición. 2002
- BuildingCisco Multilayer Switched Networks; Cisco System, Cisco Press, 2000.
- Cisco CCNA Exam #640-607; Cisco System, Cisco Press, 2002.
- Implementing Cisco Quality of Service v 2.0; Cisco System, Cisco Press, 2003.
- **VLADIMIROV Andrew A. (2005)**, Seguridad de redes Inalámbricas, EDICIONES AMAYA MULTIMEDIA, Madrid, España.
- **ANSI/IEEE STD 802.11, 1999** Edition. [1]"Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications"
- **Hills. "Large-Scale Wireless LAN Design**". IEEE Communications Magazine, vol. 39, nº 11, noviembre 2001.

3.9.1. WEB BIBLIOGRAFÍA

- http://www.linuxparatodos.com/openvpn.htm
- http://www.linuxparatodos.com/vpn.htm
- http://www.linuxparatodos.com/mrtg.htm
- http://www.linuxparatodos.com/ips.htm
- http://lauca.usach.cl/~lsanchez/Vlan/
- http://www.eduangi.com/documentos/3_CCNA2.pdf
- http://www.avantel.net/~rcruz/Cap3qosrba.pdf
- http://www.lavioleta.net/Capitulo1.htm
- http://www.commlogik.com.ar/cisco.html
- http://informatica.uv.es/doctorado/SST/docto-2-qos.ppt#389,2,Sumario
- http://www.3com.es/news/reportajes/pdfs/switching_comunicaciones_world.pdf
- http://dmi.uib.es/~loren/docencia/webxtel/bibliografia/tutorial%20VLAN.pdf

- http://net21.ucdavis.edu/newvlan.htm
- http://www.itlp.edu.mx/publica/revistas/revista_isc/anteriores/jun99/vlan.html
- http://iie.fing.edu.uy/~rgaglian/Docs/VPLS.pdf
- http://www.emagister.com/frame.cfm?id_user=889302005026967485067487070455 5&id_centro=57953030052957564866666952674548&id_curso=654250400501675554576855506745 55&url_frame=http://www.emagister.com/public/pdf/comunidad_emagister/01793120043168694849677065484567-config-ciscos.pdf
- http://www.it.iitb.ac.in/~it605/resources/Local/Docs/VLAN/VLANIntro.pdf
- http://www.isa.uniovi.es/docencia/redes/tema4.pdf
- http://www.mythdragon.com/QoS/documents/QoS%20routing%20for%20support%20MM%20apps.pdf
- http://www.alcatel.ch/com/en/appcontent/apl/A0506-Broadband_QoS-ES_tcm172-287901635.pdf
- http://www.adictosaltrabajo.com/linux/proxy.htm
- http://www.adictosaltrabajo.com/linux/proxyinverso.htm
- http://www.adictosaltrabajo.com/linux/firewall.htm
- http://www.adictosaltrabajo.com/linux/vpn.htm
- http://www.monografias.com/vpn.htm
- http://www.monografias.com/firewall.htm
- http://www.cudi.edu.mx/primavera_2005/presentaciones/felipe_alvarez.pdf
- http://www.si.uji.es/bin/ponencies/ipp.pdf
- http://www.idg.es/comunicaciones/especial-avether160/Pag08.pdf
- http://www.iec.uia.mx/proy/titulacion/proy14/vpnprin.htm

ANEXOS

ENCUESTA DIRIGIDA A EMPLEADOS Y FUNCIONARIOS DE LA EMPRESA GP FLOWERS S.A

ESTIMADO FUNCIONARIO EMPLEADO (A)

LA PRESENTE ENCUESTA CONSTITUYE UN ACERCAMIENTO DE LA EMPRESA HACIA USTED CON LA INTENCIÓN DE MEJORAR EL FUNCIONAMIENTO DE LAS SEGURIDADES PARA PROTEGER LA INFORMACIÓN DE LA EMPRESA DE LA RED PUBLICA COMO EL INTERNET.

1. **¿Conoce Ud. Sobre las Redes Inalámbricas?**

   SI ( ) NO ( )

2. **¿La Empresa ha prestado seguridades en servicios como el internet eficientes para el departamento administrativo?**

   SI ( ) NO ( )

3. **¿Cuáles son los problemas más importantes que se han presentado al usar el Internet en la Empresa GP Flowers?**

   Lentitud de la red ◯

   Daño en el acceso a la red ◯

   Mails no deseados ◯

4. **¿El servicio de Internet en la Empresa Gp Flowers para realizar sus actividades cotidianas es?**

   Muy bueno ◯

   Aceptable ◯

   Malo ◯

5. **¿Considera que la información que circula en la red de la empresa esta garantizada?**

   SI ( ) NO ( )

6. **¿Considera usted que el uso de las TICS (Tecnología de la Información y las Comunicaciones) permitirá solucionar las dificultades de seguridad en la conexión y prestación de servicios?**

   SI ( ) NO ( )

7. **¿Cuál es su grado de satisfacción general con el uso de el Internet en la Empresa Gp Flowers?**

   Completamente satisfecho ◯

   Satisfecho ◯

   Insatisfecho ◯

   Completamente insatisfecho ◯

8. **¿Considera usted que la transmisión de datos debe ser optimizada?**

   SI ( ) NO ( )

9. **¿Conoce usted algo sobre VPN (Red Privada Virtual)?**

   SI ( ) NO ( )

10. **¿Considera usted que una VPN (Red Privada Virtual) va a garantizar el flujo de información?**

    SI ( ) NO ( )

FORMULARIO DE ENTREVISTA

1. ¿Conoce usted el sistema de la Red Privada Virtual?
2. ¿Considera que puede ser favorable para la empresa Exportadora de Flores GP Flowers contar con este sistema de seguridad?
3. ¿Con que frecuencia utiliza en la empresa el internet y qué tipo de información se transfiere?
4. ¿Al ser una información confidencial es necesario contar con claves para acceder a las mismas?
5. ¿Se ha empleado algún sistema de seguridad en la red de internet por parte del proveedor?
6. ¿Considera que los empleados y funcionarios de la empresa exportadora de flores GP Flowers requiere contar con seguridades en la red?
7. ¿Los empleados y funcionarios requerirán de una capacitación previa para el manejo del Sistema de Seguridad?
8. ¿Cree conveniente dejar constancia escrita de nuestro trabajo mediante un manual o documento?
9. ¿Qué problemas se presentan en el servicio de Internet?