



Escuela Superior Politécnica del Litoral

Facultad de Ingeniería en Electricidad y Computación (FIEC)

“Plan de Negocio para la creación de ROCA TECNOLOGIES S.A. microempresa que comercializara servicios de Auditoría de Sistemas y la implementación de un sistema detector de intrusos”

TESIS DE GRADO

**Presentado por:
Previo a la obtención del Título de:**

**Christian Mario Carranza Hidalgo
INGENIERO EN ELECTRICIDAD ESPECIALIZACION
ELECTRONICA**

**Soni Enrique Rojas Quintero
INGENIERO EN ELECTRONICA Y
TELECOMUNICACIONES**

Guayaquil – Ecuador

AÑO 2009

AGRADECIMIENTO

Principalmente a Dios, por ser el responsable de la realización de este emprendimiento, luego a mis padres, por su apoyo incondicional y por último a mi mujer y mi hijo que fueron la motivación para salir adelante.

Christian Carranza Hidalgo

Agradezco a Dios por darme fuerzas para siempre luchar en la vida. Agradezco a mi madre por su apoyo incondicional

Soni Rojas Quintero

DEDICATORIA

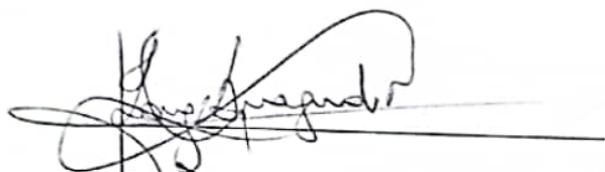
Se la dedico especialmente a mis padres que nunca dejaron de creer en mí, y siempre estuvieron en los buenos y malos momentos, también a mi hijo que fue mi principal motivación para este logro.

Christian Carranza Hidalgo

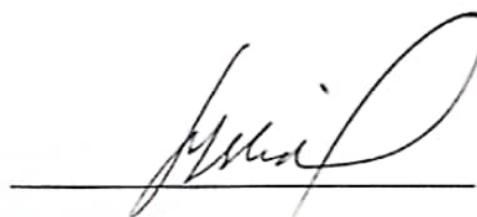
Dedico este trabajo a mi hijo, a mi esposa, a mi padre que en paz descansa y sobre todo a mi sacrificada madre.

Soni Rojas Quintero

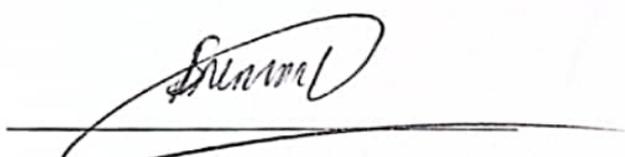
TRIBUNAL DE GRADUACION



Ing. Jorge Aragundi R.
SUBDECANO DE LA FIEC



Ing. Victor Bastidas J.
DIRECTOR DEL TOPICO



Ing. Carlos Salazar
MIEMBRO PRINCIPAL



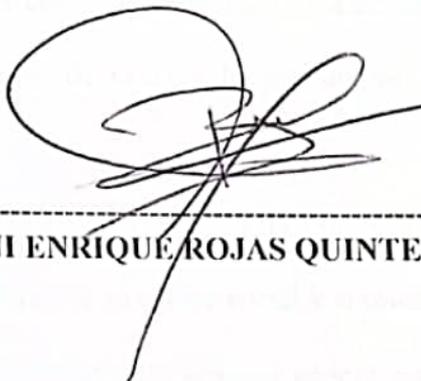
Ing. Cesar Martin M.
MIEMBRO PRINCIPAL

DECLARACION EXPRESA

La responsabilidad del contenido de esta tesis de grado nos corresponde exclusivamente, y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITECNICA DEL LITORAL.



CHRISTIAN MARIO CARRANZA HIDALGO



SONI ENRIQUE ROJAS QUINTERO

RESUMEN

El presente trabajo se refiere a un plan de negocios para la creación de “ROCA TECHNOLOGIES S.A.” microempresa que comercializará servicios de Auditoria de Sistemas y un sistema de detección de intrusos. En el mismo se implementa un “prototipo” aplicado en la red de la empresa ECUAESTIBAS S.A. para encontrar y eliminar problemas de seguridad informática.

En el primer capítulo se describe la oportunidad y necesidad encontrada las cuales dan origen a nuestro emprendimiento y se procede a detallar nuestro producto y servicio.

En el segundo capítulo se detalla el diseño, construcción y funcionamiento de nuestro producto, así mismo se incluye conceptos y teoría utilizados en el desarrollo del proyecto.

En el tercer capítulo se explica cómo se seleccionó el mercado a ser atendido por nuestra empresa, cómo se eligió el precio de venta y las estrategias de mercadeo utilizadas en la operación del negocio.

En el cuarto capítulo se detalla como constituir la empresa, se explica cómo va a estar estructurada la empresa y cuál va a ser su aporte social y ambiental.

En los capítulos quinto y sexto se hace un análisis económico y financiero de la inversión necesaria para iniciar la empresa y de los movimientos económicos realizados en la operación durante los primeros 3 años. También se justifica la rentabilidad del negocio.

En el último capítulo se realiza un análisis de los diferentes riesgos que corre nuestro emprendimiento y las variables que lo pueden afectar en forma directa o indirecta.

Para finalizar se presentan las conclusiones y recomendaciones que surgieron a lo largo de la investigación y desarrollo de este proyecto.

INDICE GENERAL

RESUMEN.....	VI
INDICE DE FIGURAS.....	XI
INDICE DE TABLAS.....	XII
LISTA DE ANEXOS.....	XII
INTRODUCCION.....	XIV

CAPITULO 1

DEFINICIÓN Y JUSTIFICACIÓN DEL EMPRENDIMIENTO

1.1.- Oportunidad que es satisfecha con nuestro emprendimiento.....	1
1.2.- Descripción general del emprendimiento.....	1
1.3.- Misión.....	2
1.4.- Visión.....	2
1.5.- Objetivos generales de la empresa.....	3
1.6.- Propuesta de valor / factores clave.....	3
1.7.- Análisis FODA.....	3

CAPITULO 2

ANALISIS TECNICO Y DESA3ROLLO DEL PRODUCTO/SERVICIO

“PROTOTIPO”

2.1.- Oportunidad/Necesidad que es satisfecha con nuestro primer prototipo.....	6
2.2.- Descripción del Producto/Servicio.....	6
2.3.- Diseño y construcción de un prototipo.....	7
2.3.1.- Conceptos y principios generales.....	7
2.3.1.2.- Protocolo TCP/IP.....	8
2.3.1.3.- Clasificación de ataques.....	13

2.3.1.4.- Firewall.....	21
2.3.1.5.-IDS-Sistemas de detección de intrusos.....	25
2.3.2.- Diseño del Producto.....	28
2.3.2.1.- Software de Monitoreo WhatsUp.....	30
2.3.3.- Construcción del Producto/Servicio.....	33
2.3.4.- Operación/funcionamiento del Producto/Servicio	34
2.3.4.1.- Mapeo de la red.....	34
2.3.4.2.- Monitoreo de la red.....	42
2.3.4.3.- Ejecutando WhatsUp como servicio NT.....	50
2.3.4.4.- Configurando en la consola de Windows.....	51
2.3.4.5.- Emisión de reportes.....	53
2.3.5.- Costos de fabricación del prototipo.....	68
2.4.- Instalación y espacio físico de la microempresa.....	70
2.4.1.- Equipos y maquinaria.....	70
2.4.2.- Distribución de la planta.....	71
2.4.3.- Plan de producción.....	72

CAPITULO 3

ANALISIS DEL MERCADO

3.1.- Contexto y análisis del sector.....	73
3.2.- Análisis del mercado propiamente dicho.....	75
3.2.1.- Clientes.....	75
3.2.2.- Competencia.....	76
3.2.3.- Tamaño del mercado global.....	78
3.3.- Plan de Mercadeo.....	79
3.3.1.- Estrategia de precio.....	79

3.3.2.- Estrategia y tácticas de venta.....	81
3.3.3.- Estrategia Promocional.....	81
3.3.4.- Políticas de Servicio.....	82

CAPITULO 4

ANÁLISIS LEGAL, ADMINISTRATIVO Y SOCIAL

4.1.- Análisis Legal.....	83
4.1.1.- Búsqueda y reserva del nombre de la empresa en los Registros Públicos.....	83
4.1.2.- Elaboración de la minuta	85
4.1.3.- Elevar la minuta a escritura pública	86
4.1.4.- Elevar la escritura pública en los Registros Público.....	86
4.1.5.- Obtención del número de RUC.....	87
4.1.6.- Elegir régimen tributario.....	87
4.1.7.- Comprar y legalizar libros contables.....	87
4.1.8.- Legalizar el Libro de Planillas en el Ministerio de Trabajo (Si fuera el caso).....	88
4.1.9.- Inscribir a los trabajadores en el I.E.S.S.....	88
4.1.10.- Solicitud de licencia municipal.....	88
4.2.- Equipo emprendedor.....	89
4.3.- Análisis administrativo.....	90
4.4.- Análisis Social.....	91

CAPITULO 5

ANÁLISIS ECONOMICO

5.1.- Estructura accionarial y propuesta de inversión.....	94
5.2.- Inversión de activos fijos.....	95

5.3.- Inversión de capital de trabajo.....	95
5.4.- Presupuesto de ingresos.....	95
5.5.- Presupuesto de materias primas, servicios e insumos.....	96
5.6.- Presupuesto de personal.....	96
5.7.- Análisis de costos.....	97
CAPITULO 6	
ANÁLISIS FINANCIERO	
6.1.- Flujo de caja.....	98
6.2.- Estado de resultados.....	99
6.3.- Balance general.....	99
CAPITULO 7	
RIESGOS Y EVALUACION DEL EMPRENDIMIENTO.....	101
CONCLUSIONES Y RECOMENDACIONES.....	103
GLOSARIO.....	104
LISTA DE ANEXOS.....	XII
BIBLIOGRAFÍA.....	107

INDICE DE FIGURAS

CAPITULO 2

Figura 2.1: Diagrama de bloques del prototipo.....	28
Figura 2.2: Funcionamiento del sistema.....	30
Figura 2.3: Presentación del software versión Gold.....	31
Figura 2.4.1: Red de Ecuastibas S.A.	32
Figura 2.4.2: Mapa de una red.....	35
Figura 2.6: Configurando la consola de WhatsUp.....	51
Figura 2.7.- Configurando el acceso de usuarios al servidor web.....	52
Figura 2.8: Configurando opciones de gráficos.....	56
Figura 2.9: Ventana de configuración de Notificaciones.....	59
Figura 2.10: Configurando una notificación vía Beeper	63
Figura 2.11.- Configurando una notificación vía e-mail.....	65
Figura 2.12: Configurando una notificación de voz.....	68
Figura 2.13: plano de la oficina.....	71

CAPITULO 3.

Figura 3.1: Anuario del año 2007 de la Superintendencia de compañías.....	79
---	----

CAPITULO 4.

Figura 4.1: Pantalla de búsqueda de nombres de compañías existentes.....	84
Figura 4.2: Pantalla no encuentra resultados para la búsqueda realizada.....	84
Figura 4.3: Organigrama de ROCA TECNOLOGIES S.A.....	91

INDICE DE TABLAS

CAPITULO 2.

Tabla 2.1: Variables usadas en las notificaciones.....	61
Tabla 2.2: Costos de fabricación del prototipo.....	69

CAPITULO 3.

Tabla 3.1: Lista de la competencia.....	77
Tabla 3.2.- Nuestros proveedores.....	77
Tabla 3.3.- Anuario 2007 de la Superintendencia de Compañías.....	77
Tabla 3.4.- Segmento 1 del mercado.....	79
Tabla 3.5.- Segmento 2 del mercado.....	79
Tabla 3.6.- Precios del Producto.....	81
Tabla 3.7.- Precios del Servicio de Auditoría.....	81
Tabla 3.8.- Precios del mantenimiento del producto.....	81

LISTA DE ANEXOS

Anexo A: Indice de Tablas del Análisis Económico.....	78
Anexo B: Indice de Tablas del Análisis Financiero.....	78
Anexo D: Glosario.....	

ANEXO A

INDICE DE TABLAS DEL ANALISIS ECONOMICO

Tabla # 0: Mercado Objetivo

Tabla # 1: Proyección de Clientes en el primer año

Tabla # 2: Precios del Producto y Servicio

Tabla # 3: Proyección de Ventas

Tabla # 4: Presupuesto de Inversión en Activos Fijos

Tabla # 5: Presupuesto de Ingresos

Tabla # 6: Gastos de Depreciación y Amortización

Tabla # 8: Costo Adicional para ofrecer el Producto y los Servicios

Tabla # 9: Presupuesto de Gastos de Personal

Tabla # 11: Presupuesto de Gastos de Operación

Tabla # 12: Presupuesto de Gastos de Administración y Ventas

Tabla # 13: Análisis de Costos

ANEXO B

INDICE DE TABLAS DEL ANALISIS FINANCIERO

Tabla # 14: Flujo de Caja

Tabla # 15: Estado de Resultados

Tabla # 16: Balance General

Tabla # 17: Flujo de Caja Neto

INTRODUCCIÓN

Entorno económico para emprender: el mundo, el país, Guayaquil

Las tendencias actuales de gestión empresarial ponen en un lugar muy importante a las tecnologías de la información y las telecomunicaciones, adoptando además nuevas propuestas de modelos que se basan en la gestión de los activos intangibles y el capital intelectual, lo que globalmente se conoce como la gestión del conocimiento. Consideramos que en la práctica, para conseguir una buena gestión de la información y el conocimiento, las empresas deben organizar y conseguir un buen sistema de gestión documental.

Al realizar una investigación del entorno encontramos que actualmente, en el país, hay muy pocas compañías brindando el servicio de auditoría informática pero en compensación se encontró un gran número de Instituciones de Educación Superior que están abriendo carreras y dictando materias o cursos orientados a este tema, incluso están entregando certificaciones como por ejemplo ISACA capítulo Quito-Ecuador, que entrega los certificados CISA (Certified Information System Auditor) y CISM (Certified Information Security Manager).

Haciendo un análisis del entorno económico del país, para el año 2007 se encontró que la tasa de crecimiento del país fue una de las más débiles de la región, apenas del 2.6 %, según las propias autoridades monetarias. Comparado con Colombia (6%) o Perú (4%), nos coloca en una situación de desventaja. Además, una economía con una inflación del 3% nos sitúa ante precios ante precios de crecimiento galopante. También se dio una reducción del empleo real y esa tasa ha venido de la mano de la desinversión de la obra pública, que fue la promesa del gobierno. Esto junto a la inseguridad política y jurídica provocará que pocos inversionistas coloquen su capital en pro de un crecimiento

sostenido, todo esto es muy desmotivador para quien ve su futuro como empleado, por lo que la única forma de ver más cercana nuestra independencia económica es arrancando con este emprendimiento, que aparte de generar ingresos para los socios fundadores, servirán para que en un principio sea una fuente de trabajo para siete familias, esto es, en un principio, y a futuro con la ayuda de Dios, creceremos y tendremos más trabajo, razón por la cual necesitaremos de más inversión, más personal, esto a su vez generará muchos más ingresos, las ganancias serán mucho más mayores.

Con nuestro emprendimiento, estaremos cubriendo una necesidad, que tenemos en nuestra ciudad porque como lo dijimos anteriormente, las empresas que se dedicaban a esta actividad eran extranjeras, o se encontraban en Quito. Con la creación de ROCA TECHNOLOGIES no será necesario acudir a estas, y consecuentemente los precios y costos serán muchos más bajos, para las empresas que requieran de nuestro servicio.

Por estar en el mercado local, nuestro producto va a ser mucho accesible para cualquier empresa, ya que con las empresas extranjeras, sólo para hacer un estudio cobran transporte, alimentación y estadía, nosotros haremos un análisis preciso y conciso y con un costo bajo ajustado a la realidad de nuestro país.

¿Por qué escogimos esta alternativa de graduación?

Una de las razones importantes de nuestro emprendimiento, es que una vez trabajando en la red de mi empresa, se nos colgó el sistema, cuando ya superamos el problema y quisimos volver a trabajar en la red, nos dimos cuenta que cierta persona, que nunca supimos en realidad quien fue, había extraído información que era muy valiosa para la empresa, al hacer esto, se produjo una falla en el sistema, ocasionando pérdidas muy grandes tanto a nivel de información, como a nivel económico.

Luego de este inconveniente, el Gerente General me encomendó la tarea de darle solución al problema, y tratar de que no se produzca de nuevo un incidente como este, contactando con empresas dedicadas a esta actividad, pude ver, que en Guayaquil no había empresas dedicadas a la seguridad informática, que habían empresas extranjeras que se dedicaban a este tipo de seguridad, por otro lado me pasaron información de que solo existían en Quito y que apenas habían unas cuantas, esto me dio la pauta para la creación de una empresa que se dedicara a la Seguridad Informática y que además prestara el servicio de Auditoría de Sistemas, pero por sobretodo y lo más importante, que se localice en la ciudad de Guayaquil.

Por la situación económica de nuestro país, es necesario emprender, encontrar nuevas oportunidades de trabajo, en otros campos que la gente no ha explotado todavía, con la creación de nuestra microempresa, esperamos dar oportunidades a personas que tienen las ganas y los deseos de salir adelante, mediante lo cual, puedan ser el sostén de sus respectivas familias.

Porque debemos dejar que nuestros recursos sean para empresas extranjeras, cuando esos recursos pueden quedar para nosotros mismos, es lo que me pregunté, y es esta la razón principal de nuestro emprendimiento.

CAPITULO 1

DEFINICIÓN Y JUSTIFICACIÓN DEL NEGOCIO

1.1.- Oportunidad/Necesidad que es satisfecha con nuestro emprendimiento

Las pocas empresas que se preocupan por el problema de seguridad informática contratan en gran mayoría de veces, empresas extranjeras para que se aplique una auditoria de sistemas, es aquí donde identificamos la oportunidad de negocio ya que como empresa local podemos dar el mismo servicio a precios relativamente bajos y de excelente calidad.

Tenemos datos de empresas que contratan personal con sueldo mensual para que se dediquen a la función de monitorear los enlaces de comunicación, los cuales son esenciales para que la empresa funcione. Con nuestro sistema podemos reemplazar este recurso o permitir que se dedique a otras actividades, ya que al caerse un enlace o un elemento determinado de la red el sistema automáticamente alertará de forma remota al personal indicado, esto se dará ya sea se encuentre dentro o fuera de la empresa

1.2.- Descripción general del emprendimiento

Factores más relevantes:

Ü **Descripción detallada del Producto y Servicio.**

Nuestra microempresa ofrecerá los servicios de auditoría de sistemas que consiste en:

- § Análisis e identificación de vulnerabilidad de seguridad en la red de voz y datos.
- § Monitoreo en sitio y remoto de la eficiencia de la red.
- § Levantamiento de información de la topología de la red de voz y datos.
- § Análisis del crecimiento no proyectado de las redes.

§ Realizar un reporte de los diferentes huecos de seguridad encontrados.

§ Implantación de un sistema de detección de intrusos.

Ü **Aplicación del Producto y Servicio.**

Las redes de muchas empresas de mediano y gran tamaño en Guayaquil se encuentran sin herramientas eficientes que permitan a los administradores o personal de sistemas velar por el buen funcionamiento de los dispositivos de la red, aplicaciones y servicios. Así como también se ven constantemente amenazados por intrusos intentando violar las seguridades de la red de voz y datos, siendo objeto de ataques y muchas veces hasta del uso inadecuado de la red.

Ü **Elementos especiales del Producto y Servicio.**

El sistema de detección de intrusos escaneará la red periódica y constantemente en busca de computadores ajenos a la red, se realizará constante monitoreo de todos los equipos o algunos específicos como servidores o ruteadores, en caso de falla alertará en forma remota al personal encargado de sistemas o gerencia, dichos avisos pueden ser pantallas emergentes en su computador, emails, mensajes SMS al celular, mensajes al beeper o mensajes grabados por vía telefónica.

1.3.- Misión

Asistir a las empresas para hacer más seguras sus redes de voz y datos, crear una cultura de seguridad informática, contribuir a su crecimiento, seguridad de la información y actualización de sistemas.

1.4.- Visión

Ser líder y referente de recursos y herramientas para Auditoria de Sistemas y seguridad informática a nivel nacional, para que a un plazo no muy lejano tratar de ser un referente para las empresas locales que brinden o tengan semejanza a la actividad que estamos realizando.

1.5.- Objetivos generales de la empresa

- En un año posicionarnos en el mercado con 5 clientes fijos, ya que la implementación del sistema es un proceso de medio/largo plazo dependiendo del cliente.
- Lograr que el Periodo de Recuperación de la Inversión sea de un año.
- Cada cuatro meses incorporar algo nuevo a nuestra cartera de productos a ofrecer.

1.6.- Propuesta de valor / factores clave

- Las compañías que usan este servicio casi siempre contratan empresas extranjeras, esto pone en ventaja a Roca Technologies S.A. por ser de Ecuador sus gastos y por ende sus precios serán muy inferiores y con la misma calidad.
- El conocimiento del mercado local y de los casos más comunes a nivel del Ecuador.
- El equipo de trabajo está formado por especialistas en Networking y seguridad informática.
- Contar con una cartera de productos variada nos permite satisfacer las necesidades de nuestros clientes.
- Participar en las operaciones permite velar que se cumplan los objetivos de la empresa.

1.7.- Análisis FODA

Fortalezas

- Personal técnico CISCO.
- El equipo de trabajo serán socios de la compañía por lo que se sentirán comprometidos a hacer todo lo posible por que el proyecto avance.
- Experiencia en el mercado. Tenemos 6 años trabajando en el área de sistemas en varias empresas, en dos o tres de ellas hemos aportado a las auditorías realizadas

(por extranjeros). En todas las empresas donde hemos trabajado siempre hemos encontrado potenciales huecos de seguridad.

- La facilidad para socializar con los clientes y facilidad de palabra nos permite prescindir de personal asignado como agente de ventas.

Oportunidades

- No hay competencia local, el 95 % de las empresas que dan este servicio son extranjeras.
- Normas que regularicen estas actividades en el país no hay por lo que nos permite ser bastantes flexibles.
- El contar con asesores de las incubadoras de negocios nos permite cubrir nuestras falencias en cuanto a conocimientos legales, financieros y por qué no alguno que otro técnico.
- La experiencia laboral que tenemos nos permite contar con una gran cartera de clientes.

Debilidades

- Poco capital, varios clientes solicitan una garantía en caso incumplimiento de contrato o de entrega tardía de resultados.
- El no hablar inglés es un gran problema, ya que hay clientes extranjeros para los cuales la auditoria de sistemas es una norma en sus actividades, el negociar con ellos o realizar las distintas entrevistas de investigación será una tarea muy difícil y frustrante.
- Poco personal, la empresa se iniciará con dos empleados lo que será un problema al trabajar en dos proyectos simultáneamente.

- El no tener una oficina en las áreas comerciales o empresariales quita credibilidad a la empresa.
- El tener funciones gerenciales y al mismo tiempo de técnico de la empresa puede afectar el logro de los objetivos de la empresa, razón por la cual, tendríamos

Amenazas

- En Internet se ha encontrado información de que ciertas empresas extranjeras piensan abrir oficinas en el país, un ejemplo es TATA, la competencia sería muy fuerte, ya que es una empresa multinacional, y se encuentra posicionada hace muchos años, razón por la cual, nos lleva una gran ventaja con respecto a nosotros que recién estamos empezando.
- Otra amenaza es que se están creando empresas en el país, que están brindando un servicio parecido al que nosotros ofreceremos, principalmente se están posicionando en Quito, razón por la cual tendremos que apurarnos, con este emprendimiento, ya que nuestro objetivo principal, es posicionarnos a nivel local, es decir en nuestro país.

CAPITULO 2

ANÁLISIS TÉCNICO

2.1. Oportunidad/ Necesidad que es satisfecha con nuestro primer prototipo

Las redes de muchas empresas de mediano y gran tamaño en Guayaquil, se encuentran sin una herramienta eficiente que les permita a los operadores y administradores de red velar por el buen funcionamiento de los equipos, aplicaciones y servicios. Los sistemas y redes se ven constantemente amenazadas por intrusos intentando violar las seguridades, siendo objeto de ataques y uso inadecuado de la red.

El aumento y la gravedad de los ataques hoy en día causan que los sistemas de detección de intrusos sean una parte indispensable de la seguridad. Cualquier empresa que no esté buscando ser objeto de un intento de ataque, no tienen idea acerca de cuáles son las amenazas que están allí. Una vez implementado, el sistema de detección de intrusos reportará las amenazas que pueden respaldar las sospechas de que la red de la compañía está siendo atacada. Además, entender la frecuencia y los tipos de ataques le permite a la organización determinar los controles de seguridad que se deben adoptar.

Las pocas empresas que se preocupan por este problema contratan siempre empresas extranjeras para que se aplique una auditoria de sistemas, es aquí donde identificamos la oportunidad de negocio ya que como empresa local podemos dar el mismo servicio a precios relativamente bajos y de excelente calidad.

2.2. Descripción del Producto/Servicio

Los servicios de auditoría de sistemas que ofreceremos consisten en:

- Análisis e identificación de vulnerabilidad de seguridad en la red de voz y datos.

- Monitoreo en sitio y remoto de la eficiencia de la red.
- Levantamiento de información de la topología de la red de voz y datos.
- Análisis del crecimiento no proyectado de las redes.
- Realizar un reporte de los diferentes huecos de seguridad encontrados.
- Implantación de un sistema de detección de intrusos.

El sistema de detección de intrusos escaneará la red periódica y constantemente en busca de computadores ajenos a la red, se realizará constante monitoreo de todos los equipos o algunos específicos como servidores o ruteadores, en caso de falla alertará en forma remota al personal encargado de sistemas o gerencia, dichos avisos pueden ser pantallas emergentes en su computador, emails, mensajes SMS al celular, mensajes al beeper o mensajes grabados por vía telefónica.

El software utilizado en nuestro sistema será WhatsUp 8,0

2.3. Diseño y construcción de un prototipo

2.3.1. Conceptos y principios generales

Presentaremos algunas nociones de seguridad y otros conceptos necesarios para una buena comprensión del análisis de seguridad que llevaremos a cabo sobre la infraestructura de la red de Ecuastibas.

El sector de la seguridad informática es muy amplio y abarca muchos y diversos campos por lo que nos centraremos en la seguridad en redes LAN/WAN, servidores (Web, aplicaciones, bases de datos, correos, etc.) y otros puntos que tienen que ver con el cliente.

2.3.1.2. Protocolo TCP/IP

Se han desarrollado diferentes familias de protocolos para comunicación por red de datos para los sistemas UNIX. El más ampliamente utilizado es el Internet Protocol Suite, comúnmente conocido como TCP / IP (1).

Es un protocolo DARPA que proporciona transmisión fiable de paquetes de datos sobre redes. El nombre TCP / IP proviene de dos protocolos importantes de la familia, el Transmission Control Protocol (TCP) y el Internet Protocol (IP). Todos juntos llegan a ser más de 100 protocolos diferentes definidos en este conjunto.

El TCP / IP es la base del Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local y área extensa. TCP / IP fue desarrollado y demostrado por primera vez en 1972 por el departamento de defensa de los EE.UU, ejecutándolo en el ARPANET una red de área extensa del departamento de defensa.

Internet es una red de computadoras que utiliza convenciones comunes a la hora de nombrar y direccionar sistemas. Es una colección de redes independientes interconectadas; no hay nadie que sea dueño o active Internet al completo.

Las computadoras que componen Internet trabajan en UNIX, el sistema operativo Macintosh, Windows 9x/2000/XP y muchos otros. Utilizando TCP/IP y los protocolos veremos dos servicios de red:

- Servicios de Internet a nivel de aplicación
- Servicios de Internet a nivel de red

Servicios de internet a nivel de aplicación:

Desde el punto de vista de un usuario, una red de redes TCP/IP aparece como un grupo de programas de aplicación que utilizan la red para llevar a cabo tareas útiles de comunicación. Utilizamos el término interoperabilidad para referirnos a la habilidad que tienen diversos sistemas de cómputo para cooperar en la resolución de problemas computacionales. Los programas de aplicación de Internet muestran un alto grado de interoperabilidad. La mayoría de usuarios que accesan a Internet lo hacen al correr programas de aplicación sin entender la tecnología TCP/IP, la estructura de la red de redes subyacente o incluso sin entender el camino que siguen los datos hacia su destino. Sólo los programadores que crean los programas de aplicación de red necesitan ver a la red de redes como una red, así como entender parte de la tecnología. Los servicios de aplicación de Internet más populares y difundidos incluyen:

- Correo electrónico. El correo electrónico permite que un usuario componga memorandos y los envíe a individuos o grupos. Otra parte de la aplicación de correo permite que un usuario lea los memorandos que ha recibido. El correo electrónico ha sido tan exitoso que muchos usuarios de Internet depende de él para su correspondencia normal de negocios. Aunque existen muchos sistemas de correo electrónico, al utilizar TCP/IP se logra que la entrega sea más confiable debido a que no se basa en compradoras

intermedias para distribuir los mensajes de correo. Un sistema de entrega de correo TCP/IP opera al hacer que la máquina del transmisor contacte directamente la máquina del receptor. Por lo tanto, el transmisor sabe que, una vez que el mensaje salga de su máquina local, se habrá recibido de manera exitosa en el sitio de destino.

- Transferencia de archivos. Aunque los usuarios algunas veces transfieren archivos por medio del correo electrónico, el correo está diseñado principalmente para mensajes cortos de texto. Los protocolos TCP/IP incluyen un programa de aplicación para transferencia de archivos, el cual permite que los usuarios envíen o reciban archivos arbitrariamente grandes de programas o de datos. Por ejemplo, al utilizar el programa de transferencia de archivos, se puede copiar de una máquina a otra una gran base de datos que contenga imágenes de satélite, un programa escrito en Pascal o C++, o un diccionario del idioma inglés. El sistema proporciona una manera de verificar que los usuarios cuenten con autorización o, incluso, de impedir el acceso. Como el correo, la transferencia de archivos a través de una red de redes TCP/IP es confiable debido a que las dos máquinas comprendidas se comunican de manera directa, sin tener que confiar en máquinas intermedias para hacer copias del archivo a lo largo del camino.
- Acceso remoto. El acceso remoto permite que un usuario que esté frente a una computadora se conecte a una máquina remota y establezca una sesión interactiva. El acceso remoto hace aparecer una ventana en la pantalla del usuario, la cual se conecta directamente con la máquina remota al enviar

cada golpe de tecla desde el teclado del usuario a una máquina remota y muestra en la ventana del usuario cada carácter que la computadora remota lo genere. Cuando termina la sesión de acceso remoto, la aplicación regresa al usuario a su sistema local.

Servicios de internet a nivel de red

Un programador que crea programas de aplicación que utilizan protocolos TCP/IP tiene una visión totalmente diferente de una red de redes, con respecto a la visión que tiene un usuario que únicamente ejecuta aplicaciones como el correo electrónico. En el nivel de red, una red de redes proporciona dos grandes tipos de servicios que todos los programas de aplicación utilizan. Aunque no es importante en este momento entender los detalles de estos servicios, no se deben omitir del panorama general del TCP/IP:

- Servicio sin conexión de entrega de paquetes. La entrega sin conexión es una abstracción del servicio que la mayoría de las redes de conmutación de paquetes ofrece. Simplemente significa que una red de redes TCP/IP rutea mensajes pequeños de una máquina a otra, basándose en la información de dirección que contiene cada mensaje. Debido a que el servicio sin conexión rutea cada paquete por separado, no garantiza una entrega confiable y en orden. Como por lo general se introduce directamente en el hardware subyacente, el servicio sin conexión es muy eficiente.
- Servicio de transporte de flujo confiable. La mayor parte de las aplicaciones necesitan mucho más que sólo la entrega de paquetes, debido a que requieren que el software de comunicaciones se recupere de manera

automática de los errores de transmisión, paquetes perdidos o fallas de conmutadores intermedios a lo largo del camino entre el transmisor y el receptor. El servicio de transporte confiable resuelve dichos problemas. Permite que una aplicación en una computadora establezca una "conexión" con una aplicación en otra computadora, para después enviar un gran volumen de datos a través de la conexión como si fuera perramente y directa del hardware.

Muchas redes proporcionan servicios básicos similares a los servicios TCP/IP, pero existen unas características principales que los distingue de los otros servicios:

- Independencia de la tecnología de red. Ya que el TCP/IP está basado en una tecnología convencional de conmutación de paquetes, es independiente de cualquier marca de hardware en particular. La Internet global incluye una variedad de tecnologías de red que van de redes diseñadas para operar dentro de un solo edificio a las diseñadas para abarcar grandes distancias. Los protocolos TCP/IP definen la unidad de transmisión de datos, llamada datagrama, y especifican cómo transmitir los datagramas en una red en particular.
- Interconexión universal. Una red de redes TCP/IP permite que se comunique cualquier par de computadoras conectadas a ella. Cada computadora tiene asignada una dirección reconocida de manera universal dentro de la red de redes. Cada datagrama lleva en su interior las direcciones de destino para tomar decisiones de ruteo.

- Acuses de recibo punto-a-punto. Los protocolos TCP/IP de una red de redes proporcionan acuses de recibo entre la fuente y el último destino en vez de proporcionarlos entre máquinas sucesivas a lo largo del camino, aún cuando las dos máquinas no estén conectadas a la misma red física.
- Estándares de protocolo de aplicación. Además de los servicios básicos de nivel de transporte (como las conexiones de flujo confiable), los protocolos TCP/IP incluyen estándares para muchas aplicaciones comunes, incluyendo correo electrónico, transferencia de archivos y acceso remoto. Por lo tanto, cuando se diseñan programas de aplicación que utilizan el TCP/IP, los programadores a menudo se encuentran con que el software ya existente proporciona los servicios de comunicación que necesitan

2.3.1.3. Clasificación de ataques

Los métodos de ataque descritos a continuación están divididos en categorías generales que pueden estar relacionadas entre sí, ya que el uso de un método en una categoría permite el uso de otros métodos en otras (2). Por ejemplo: después de crackear una password, un intruso realiza un login como usuario legítimo para navegar entre los archivos y explotar vulnerabilidades del sistema. Eventualmente también, el atacante puede adquirir derechos a lugares que le permitan dejar un virus u otras bombas lógicas para paralizar todo un sistema antes de huir.

EAVESDROPPING Y PACKET SNIFFING

Muchas redes son vulnerables al eavesdropping, o la pasiva interceptación (sin modificación) del tráfico de red. En Internet esto es realizado por packet sniffers, que son programas que monitorean los paquetes de red que están direccionados a la computadora donde están instalados. El sniffer puede ser colocado tanto en una estación de trabajo conectada a la red, como a un equipo router o a un gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías. Existen kits disponibles para facilitar su instalación.

Este método es muy utilizado para capturar loginIDs y passwords de usuarios, que generalmente viajan claros (sin encriptar) al ingresar a sistemas de acceso remoto (RAS). También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mails entrantes y salientes. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos.

SNOOPING Y DOWNLOADING

Los ataques de esta categoría tienen el mismo objetivo que el sniffing, obtener la información sin modificarla. Sin embargo los métodos son diferentes. Además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de e-mail y otra información guardada, realizando en la mayoría de los casos un downloading de esa información a su propia computadora.

El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software. Los casos más resonantes de este tipo de ataques fueron: el robo de un archivo con mas de 1700 números de tarjetas de crédito desde una compañía de música

mundialmente famosa, y la difusión ilegal de reportes oficiales reservados de las Naciones Unidas, acerca de la violación de derechos humanos en algunos países europeos en estado de guerra.

TAMPERING O DATA DIDDLE

Esta categoría se refiere a la modificación desautorizada a los datos, o al software instalado en un sistema, incluyendo borrado de archivos. Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliberada. O aún si no hubo intenciones de ello, el administrador posiblemente necesite dar de baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada.

Como siempre, esto puede ser realizado por insiders u outsiders, generalmente con el propósito de fraude o dejar fuera de servicio un competidor.

Son innumerables los casos de este tipo como empleados (o externos) bancarios que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes, o contribuyentes que pagan para que se les anule la deuda por impuestos en el sistema municipal.

Múltiples web sites han sido víctimas del cambio de sus home page por imágenes terroristas o humorísticas, o el reemplazo de versiones de software para download por otros con el mismo nombre pero que incorporan código malicioso (virus, troyanos).

La utilización de programas troyanos esta dentro de esta categoría, y refiere a falsas versiones de un software con el objetivo de averiguar información, borrar archivos y hasta tomar control remoto de una computadora a través de Internet como el caso de Back Orifice y NetBus, de reciente aparición.

SPOOFING

Esta técnica es utilizada para actuar en nombre de otros usuarios, usualmente para realizar tareas de snoofing o tampering. Una forma común de spoofing, es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él, como puede ser el envío de falsos e-mails.

El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y en otro. Este proceso, llamado Looping, tiene la finalidad de evaporar la identificación y la ubicación del atacante. El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país. Otra consecuencia del looping es que una compañía o gobierno pueden suponer que están siendo atacados por un competidor o una agencia de gobierno extranjera, cuando en realidad están seguramente siendo atacado por un insider, o por un estudiante a miles de km de distancia, pero que ha tomado la identidad de otros. El looping hace su investigación casi imposible, ya que el investigador debe contar con la colaboración de cada administrador de cada red utilizada en la ruta, que pueden ser de distintas jurisdicciones.

Los protocolos de red también son vulnerables al spoofing. Con el IP spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo From, pero que es aceptada por el destinatario del paquete.

El envío de falsos e-mails es otra forma de spoofing permitida por las redes. Aquí el atacante envía a nombre de otra persona e-mails con otros objetivos. Tal fue el caso de una universidad en USA que en 1998 debió reprogramar una fecha completa de exámenes ya que alguien en nombre de la secretaría había cancelado la fecha verdadera y enviado el mensaje a toda la nómina (163 estudiantes).

Muchos ataques de este tipo comienzan con ingeniería social, y la falta de cultura por parte de los usuarios para facilitar a extraños sus identificaciones dentro del sistema. Esta primera información es usualmente conseguida a través de una simple llamada telefónica.

JAMMING o FLOODING

Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más puede utilizarla.

Muchos ISPs (proveedores de Internet) han sufrido bajas temporales del servicio por ataques que explotan el protocolo TCP. Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP (o sea que este ataque involucra también spoofing). El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas.

Muchos host de Internet han sido dados de baja por el "ping de la muerte", una versión-trampa del comando ping. Mientras que el ping normal simplemente verifica si un sistema esta enlazado a la red, el ping de la muerte causa el reboot o el apagado instantáneo del equipo.

Otra acción común es la de enviar millares de e-mails sin sentido a todos los usuarios posibles en forma continua, saturando los distintos servers destino.

Caballos de Troya

Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones, por supuesto no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto (P.ej. Formatear el disco duro, modificar un fichero, sacar un mensaje, etc.).

Bombas logicas

Este suele ser el procedimiento de sabotaje más comúnmente utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada destruirá, modificara la información o provocara el cuelgue del sistema.

Ingeniería social

Básicamente convencer a la gente de que haga lo que en realidad no debería. Por ejemplo llamar a un usuario haciéndose pasar por administrador del sistema

y requerirle la password con alguna excusa convincente. Esto es común cuando en el Centro de Cómputo los administradores son amigos o conocidos.

Difusión de virus

Si bien es un ataque de tipo tampering, difiere de este porque puede ser ingresado al sistema por un dispositivo externo (diskettes) o través de la red (e-mails u otros protocolos) sin intervención directa del atacante. Dado que el virus tiene como característica propia su autoreproducción, no necesita de mucha ayuda para propagarse a través de una LAN o WAN rápidamente, si es que no está instalada una protección antivirus en los servidores, estaciones de trabajo, y los servidores de e-mail. Existen distintos tipos de virus, como aquellos que infectan archivos ejecutables (.exe, .com, .bat, etc.) y los sectores de boot-partición de discos y diskettes, pero aquellos que causan en estos tiempos mas problemas son los macro-virus, que están ocultos en simples documentos o planilla de cálculo, aplicaciones que utiliza cualquier usuario de PC, y cuya difusión se potencia con la posibilidad de su transmisión de un continente a otro a través de cualquier red o Internet. Y además son multiplataforma, es decir, no están atados a un sistema operativo en particular, ya que un documento de MS-Word puede ser procesado tanto en un equipo Windows 3.x/95/98, como en una Macintosh u otras. Cientos de virus son descubiertos mes a mes, y técnicas más complejas se desarrollan a una velocidad muy importante a medida que el avance tecnológico permite la creación de nuevas puertas de entrada. Por eso es indispensable contar con una herramienta antivirus actualizada y que pueda responder rápidamente ante cada nueva amenaza.

El ataque de virus es el más común para la mayoría de las empresas, que en un gran porcentaje responden afirmativamente cuando se les pregunta si han sido víctimas de algún virus en los últimos 5 años.

Obtención de passwords, códigos y claves

Este método (usualmente denominado cracking), comprende la obtención "por fuerza bruta" de aquellas claves que permiten ingresar a servidores, aplicaciones, cuentas, etc (5). Muchas passwords de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario, que además nunca la cambia. En este caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves hasta encontrar la password correcta.

Es muy frecuente crackear una password explotando agujeros en los algoritmos de encriptación utilizados, o en la administración de las claves por parte la empresa.

Por ser el uso de passwords la herramienta de seguridad más cercana a los usuarios, es aquí donde hay que poner énfasis en la parte "humana" con políticas claras (como se define una password?, a quien se está autorizado a revelarla?) y una administración eficiente (cada cuanto se están cambiando?). No muchas organizaciones están exentas de mostrar passwords escritas y pegadas en la base del monitor de sus usuarios, u obtenerlas simplemente preguntando al responsable de cualquier PC, cual es su password?

Eliminar el blanco

Ping mortal. Algunos ataques eliminan el blanco en lugar de inundarlo con trabajo. Un ejemplo de este tipo es el ping mortal, un paquete ping ilícitamente enorme, que hace que el equipo de destino se cuelgue. Muchas implementaciones de routers, la mayoría de los Unix y todas las versiones de Windows se mostraron vulnerables a este ataque cuando se lo descubrió por primera vez hace un par de años. A pesar de que los vendedores lanzaron parches de inmediato, hay todavía cantidades significativas de hosts "no corregidos" en las redes de producción (en especial, las que corren bajo el Windows 9x).

TCP/IP permite un tamaño máximo de paquete de 64 kilobytes (KB, este máximo está dividido en piezas mucho más pequeñas a través de protocolos de capas más bajas, como Ethernet o token ring, pero dentro de una computadora, paquetes mucho más grandes son posibles). Para lidiar con un paquete de 64 KB, la cola TCP/IP asigna un buffer en memoria de 64 KB. Al recibir una cantidad ilícitamente grande de información, como un ping mortal, el buffer del equipo de destino se desborda y el sistema se puede colgar. Todos los IDS que se probaron detectaron paquetes de ping mortal en nuestro test.

2.3.1.4. Firewall

Un firewall es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra (3). Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Un firewall es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el Web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

De este modo un firewall puede permitir desde una red local hacia Internet servicios de web, correo y ftp, pero no a IRC que puede ser innecesario para nuestro trabajo. También podemos configurar los accesos que se hagan desde Internet hacia la red local y podemos denegarlos todos o permitir algunos servicios como el de la web, (si es que poseemos un servidor web y queremos que sea accesible desde Internet). Dependiendo del firewall que tengamos también podremos permitir algunos accesos a la red local desde Internet si el usuario se ha autenticado como usuario de la red local.

Un firewall puede ser un dispositivo software o hardware, es decir, un aparatito que se conecta entre la red y el cable de la conexión a Internet, o bien un programa que se instala en la máquina que tiene el modem que conecta con Internet. Incluso podemos encontrar ordenadores computadores muy potentes y con softwares específicos que lo único que hacen es monitorizar las comunicaciones entre redes.

En la era de la información, las ideas, datos y archivos en su red son probablemente lo más valioso que su empresa posee. Piense acerca de sus listas de clientes y registros de accionistas, transacciones comerciales y

material de marketing, estrategias de comercialización y diseño de productos.

Cuánto valen ellos para su organización?

Cuán importante es esta información para el éxito de su empresa?

En su estado actual, la información que esta almacenada en su red no es utilizada con comodidad si la misma no es de fácil acceso e intercambio. Esto significa, que usted debe elegir entre accesibilidad sobre seguridad. Muchas compañías piensan que ellos deben dejar que la información fluya libremente en su red, pero no piensan lo mismo sobre su dinero cuando lo depositan en el banco.

El Firewall logra el balance optimo entre seguridad y accesibilidad, de esta manera su empresa puede obtener todas las ventajas que ofrece el libre manejo de su información sabiendo que esta se encuentra completamente protegida.

Si su empresa tiene una red interna conectada a Internet o a una Intranet corporativa usted necesita un firewall para mantenerlas normas de seguridad entre ellas. El firewall mantiene separada su red interna (de la cual usted tiene control) de diferentes tipos de redes externas (de las cual usted NO tiene control). El firewall controla la entrada y salida de trafico protegiendo su red de intromisiones indeseadas.

La función del firewall es ser una sólida barrera entre su red y el mundo exterior. Este permite habilitar el acceso a usuarios y servicios aprobados.

Algunas de las prestaciones que le brindan son:

- Previene que usuarios no autorizados obtengan acceso a su red.
- Provee acceso transparente hacia Internet a los usuarios habilitados.
- Asegura que los datos privados sean transferidos en forma segura por la red pública.
- Ayuda a sus administradores a buscar y reparar problemas de seguridad.
- Provee un amplio sistema de alarmas advirtiendo intentos de intromisión a su red.

Estas son algunas de sus características técnicas:

- Dos tipos de configuración, local y remota.
- Configuración remota por medio de una interfase grafica que corre sobre sistema operativo Windows 9X/NT.
- Configuración local por medio de una interfase "ncurses" la cual se utiliza desde la consola del firewall.
- Permite el uso de aplicaciones basados en servicios tales como RADIUS y TACACS+ los cuales se utilizan en tasación de tiempos de conexión y uso de servicios.
- Soporta el uso de proxy-server para la configuración de su red interna.
- Conexiones de todos los servicios comunes de TCP/IP a través del firewall de manera totalmente transparente.
- Soporta servicios multimedia, incluyendo Real Audio, CuSeeMe, Internet Relay Chat, etc.
- Amplio sistema de logeo de conexiones entrantes/salientes totalmente configurable.

- Auto configuración de servidores que proveen servicios hacia el exterior de la red interna por medio de normas de seguridad.
- Múltiples alarmas de intentos de ingreso fallidos hacia la red.
- Sistema de alarmas configurable que permite el envío de avisos por medio de FAX, Pager, Mail, Voice Mail y advertencia visuales.
- Filtro de acceso de conexiones permitidas por interfaces no permitidas, este filtro es importante para contrarrestar técnicas IP-SPOOFING.
- La configuración del firewall se puede hacer mediante el mismo server o desde un servidor remoto corriendo un sistema de administración específico que utiliza para esta tarea una interfase dedicada o TUNNELING (comunicación encriptada).
- Soporte de comunicaciones encriptadas entre dos FIREWALL (tunneling) en forma totalmente transparente usando algoritmo IDEA/3DES, no es necesario que entre las dos puntas de la comunicación se encuentren dos FIREWALL también se puede efectuar la conexión con cualquier servidor corriendo sistema operativo de tipo BSD, SunOS, Solaris, etc por medio de un daemon que el Firewall provee para cada sistema operativo.
- Los módulos de alarmas corren tanto dentro del FIREWALL (centralizador de alarmas) como también en los servidores de su red para poder brindar detalles más específicos.

2.3.1.5. IDS-Sistemas de detección de intrusos

Un sistema de detección de intrusos (o IDS de sus siglas en inglés *Intrusion Detection System*) es un programa usado para detectar accesos no-

autorizados a un computador o a una red (4). Estos accesos pueden ser ataques de habilidosos hackers que usan herramientas automáticas (6).

El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red). El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas.

El funcionamiento de estas herramientas se basa en el análisis pormenorizado del tráfico de red, el cual al entrar al analizador es comparado con firmas de ataques conocidos, o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes malformados, etc. El IDS no sólo analiza qué tipo de tráfico es, sino que también revisa el contenido y su comportamiento.

Normalmente esta herramienta se integra con un firewall. El detector de intrusos es incapaz de detener los ataques por sí solo, excepto los que trabajan conjuntamente en un dispositivo de puerta de enlace con funcionalidad de firewall, convirtiéndose en una herramienta muy poderosa ya que se une la inteligencia del IDS y el poder de bloqueo del firewall, al ser el punto donde forzosamente deben pasar los paquetes y pueden ser bloqueados antes de penetrar en la red.

Los IDS suelen disponer de una base de datos de “firmas” de ataques conocidos.

Dichas firmas permiten al IDS distinguir entre el uso normal del PC y el uso fraudulento, y/o entre el tráfico normal de la red y el tráfico que puede ser resultado de un ataque o intento del mismo.

Tipos de IDS

Existen tres tipos de sistemas de detección de intrusos:

1. **HIDS** (*HostIDS*): un IDS vigilando un único ordenador y por tanto su interfaz corre en modo no promiscuo. La ventaja es que la carga de procesado es mucho menor.
2. **NIDS** (*NetworkIDS*): un IDS basado en red, detectando ataques a todo el segmento de la red. Su interfaz debe funcionar en modo promiscuo capturando así todo el tráfico de la red.
3. **DIDS** (*DistributedIDS*): sistema basado en la arquitectura cliente-servidor compuesto por una serie de NIDS (IDS de redes) que actúan como sensores centralizando la información de posibles ataques en una unidad central que puede almacenar o recuperar los datos de una base de datos centralizada. La ventaja es que en cada NIDS se puede fijar unas reglas de control especializándose para cada segmento de red. Es la estructura habitual en redes privadas virtuales (VPN).

Sistemas pasivos y sistemas reactivos

En un sistema pasivo, el sensor detecta una posible intrusión, almacena la información y manda una señal de alerta que se almacena en una base de datos.

En un sistema reactivo, el IDS responde a la actividad sospechosa

reprogramando el cortafuego para que bloquee tráfico que proviene de la red del atacante.

Implementación

Para poner en funcionamiento un sistema de detección de intrusos se debe tener en cuenta que es posible optar por una solución hardware, software o incluso una combinación de estos dos (7). La posibilidad de introducir un elemento hardware es debido al alto requerimiento de procesador en redes con mucho tráfico. A su vez los registros de firmas y las bases de datos con los posibles ataques necesitan gran cantidad de memoria, aspecto a tener en cuenta.

En redes es necesario considerar el lugar de colocación del IDS. Si la red está segmentada con hub (capa 1 del modelo OSI) no hay problema en analizar todo el tráfico de la red realizando una conexión a cualquier puerto. En cambio, si se utiliza un switch (capa 2 del modelo OSI), es necesario conectar el IDS a un puerto SPAN (Switch Port Analiser) para poder analizar todo el tráfico de esta red.

2.3.2. Diseño del Producto

Analizando la necesidad que aprovecharemos para nuestro inicio en los negocios necesitamos un sistema que se conecte a la red de voz y datos de la empresa a usar como parte de nuestro prototipo, este sistema monitoreara de forma permanente todos o varios equipos determinados de la red, y cuando detecte una anomalía en dichos equipos o cuando detecte un equipo ajeno a la red se comunicará con un tercer bloque que viene a ser un proveedor externo de servicios de comunicaciones

móviles, este proveedor comunicara la novedad al personal encargado de la red, en la figura 2.1 se puede apreciar lo mencionado anteriormente.

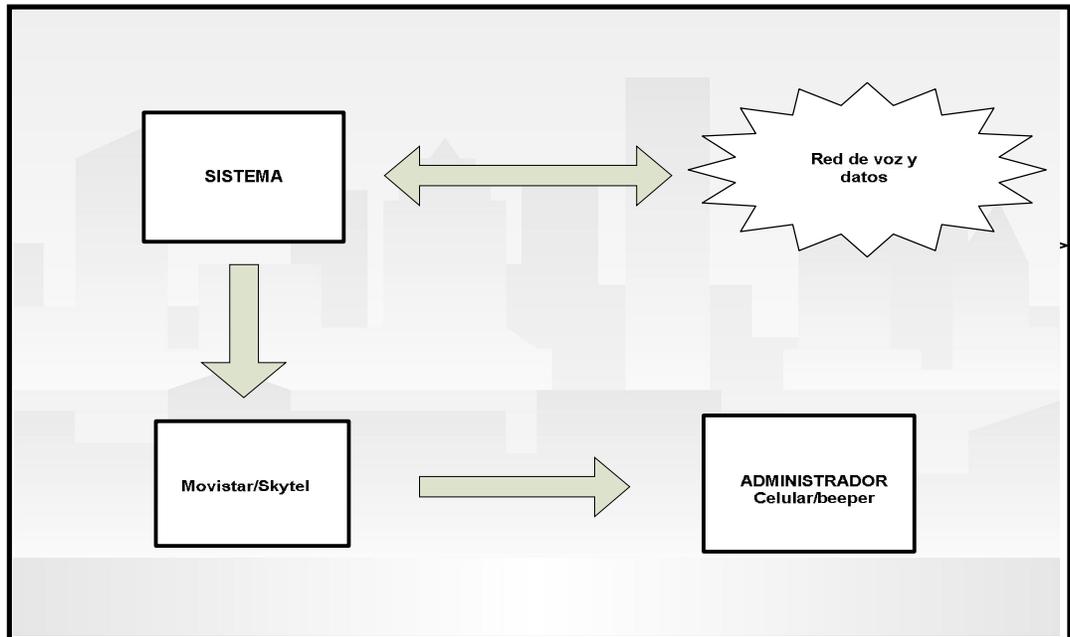


Figura 2.1.- Diagrama de bloque del prototipo

Nuestro sistema estará conformado básicamente por un PC que monitoreará periódicamente y de manera permanente la red de voz y datos de la empresa, al detectar alguna anomalía el sistema inmediatamente enviará una o varias alertas a los administradores de la red. Para enviar estas alertas usaremos los recursos de proveedores externos, en este caso Movistar y Skytel. Por todos es conocido que hoy en día el principal medio de ubicación más inmediato es el celular, por ello enviaremos mensajes SMS previamente grabados en nuestro sistema. Aunque el beeper es un equipo que ya está pasando a la historia, de igual forma podemos enviar mensajes pregrabados como lo muestra el diagrama de bloques abajo mostrado.

El equipo encargado de monitorear la red puede ser un PC con requerimientos básicos:

Windows 98/XP, espacio libre de disco 1 Gb, memoria RAM 128, dispositivo lector de CD ROM, tarjeta ethernet 10/100 y tarjeta Fax Modem 56 K.

En este equipo se instalará software de monitoreo de la red y detección de intrusos, para este caso hemos elegido por muchas ventajas explicadas más adelante a WhatsUp de Ipswitch.

Como medio de comunicación externa necesitaremos una base celular o una línea telefónica con salida celular.

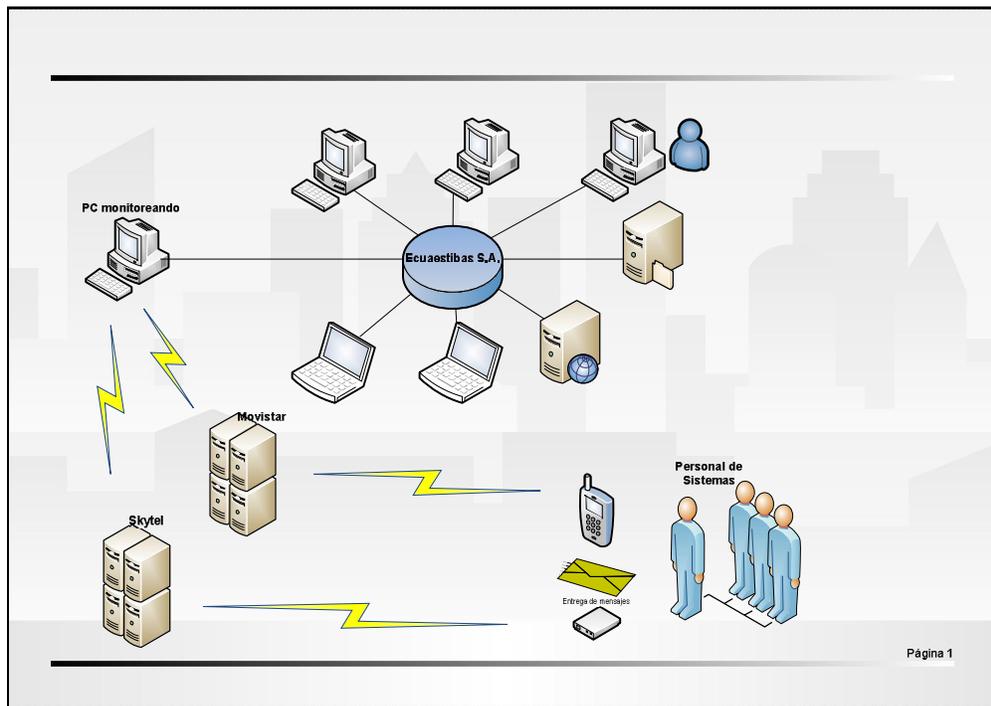


Figura 2.2.- Funcionamiento del sistema.

2.3.2.1 Software de Monitoreo WhatsUp

WhatsUp fue desarrollado por Ipswitch, es una herramienta de fácil uso para monitoreo de redes TCP/IP, IPX y NETBEUI, la versión que se utilizará es la

versión Gold, que posee alarmas audibles y visibles. Es decir WhatsUp Gold inicia alarmas visibles y de sonido cuando elementos de la red no responden a las herramientas de sondeo. WhatsUp siempre notificará vía beeper digital, mensajes alfanuméricos, alarmas de sonido, ventanas emergentes, e-mails o mensajes de voz.



Figura 2.3.- Presentación del software versión Gold.

Fue diseñado para PCs con sistema operativo Windows 95 o Windows NT, WhatsUp Gold puede ser instalado en cualquier PC y no requiere de hardware costoso y dedicado, el software se ejecuta en segundo plano en el PC por lo que se puede trabajar normalmente en las aplicaciones usadas en el trabajo diario, puede ejecutarse en cualquier host TCP/IP de 32 bits tales como Windows 95 y Windows NT y puede ser configurado para que inicie el monitoreo automático de la red sin ningún entrenamiento especial.

WhatsUp Gold monitorea elementos vitales de la red y servicios de sistema, genera una alarma cuando en uno de ellos surge un problema. Esto también

facilita el soporte remoto y diagnóstico permitiendo fácilmente monitorear el estatus de uno, varios o todos los elementos de la red. Permite rápidamente escanear la red y realizar una representación gráfica y envía notificaciones si un elemento de la red o un servicio se cae o levanta.

Características de WhatsUp Gold Versión 7.02

Esta versión del software ofrece muchas herramientas útiles para el administrador de red entre ellas las siguientes:

- **Monitoreo IPX.** WhatsUp puede monitorear un elemento de la red que use el protocolo IPX de Novel Netware, además las herramientas Auto Load y WinNet pueden detectar un elemento de red que ejecute IPX, crea un icono para este en el mapa de la red y automáticamente comienza a monitorear el elemento.
- **Total administración Web.** El acceso remoto vía Web al sistema WhatsUp ofrece casi todas las características del WhatsUp, los usuarios pueden logonearse al servidor Web y dependiendo de sus privilegios de acceso asignado pueden ver mapas, estado de un elemento, logs y configurar mapas, hosts, reportes y usuarios.
- **Ejecutar WhatsUp como un servicio NT.** Se puede ejecutar el software como un servicio NT y usar la interface Web para ver mapas y monitorear la red.
- **Nueva utilidad gráfica SNMP.** Se puede graficar en tiempo real datos SNMP, tales como la entrada y salida de paquetes de un router monitoreado, para proveer monitoreo adicional y análisis del funcionamiento de la red.

- Notificación de Mensajes SNMP. Además de los reportes de mensajes SNMP en los logs, WhatsUp puede enviar un mensaje de notificación vía pager, vía beeper, e-mail o mensajes de voz cuando una alerta es recibida por un elemento de red.
- Mejoras en el escaneo de red. WhatsUp aceleró inmensamente el proceso de escaneo y detección de red, puede escanear todos los puertos de un dispositivo de red identificando los servicios en ejecución en cada puerto. Los administradores de red ahora fácilmente pueden determinar cuales puertos están activos y estar seguros de que los puertos correctos están siendo usados por cada servicio.
- Captura y reporte de estadísticas de red, tales como tiempo de respuesta, número total de sondeos, total de paquetes perdidos, tiempo de respuesta mínimo y máximo.

2.3.3. Construcción del Producto/Servicio

Para la implementación de nuestro prototipo usamos el computador de uno de los emprendedores con las siguientes características:

- Procesador Intel Celeron 530 – 1.73 GHz, 1 MB L2 cache
- RAM 512 MB DDR2
- 80 GB HDD
- 802.11 b/g WLAN
- Sistema Operativo Windows XP SP2
- Tarjeta Ethernet 10/100 Mbps

Se descargo de internet una versión de prueba del Software What's Up Gold de IPswitch.

Para conectarnos a la red de Ecuastibas se usó un Switch 3COM de 8 puertos 10/100 Mbps. Se escaneo la red y se determino la arquitectura de la red. Se determino que hay cuatro edificios conectados por medio de un enlace de radio proporcionados por la compañía Ecutel, los cuales usan 4 Routers Cisco 5500. Se determino como prueba que se monitoreara 3 PCs las cuales simularan ser servidores de Datos, Internet y Correo. Se utilizará una base celular de movistar de propiedad de Ecuastibas por medio de la cual se establece contacto directo con Movistar y Skytel. Hay que indicar que Ecuastibas tiene 74 PCs en red.

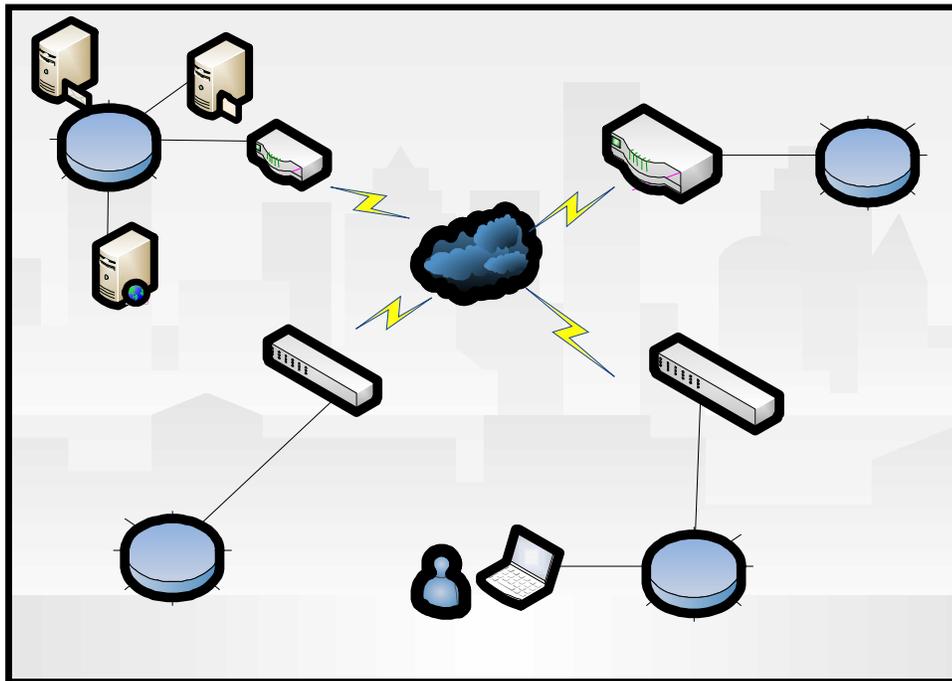


Figura 2.4.1.- Red de Ecuastibas S.A.

2.3.4. Operación - funcionamiento del Producto/Servicio

2.3.4.1 Mapeo de la red

Antes de poder monitorear los sistemas en la red se necesita configurar un mapa de la red, se puede usar uno de los métodos automáticos para mapear la

red o crearlo manualmente, configurar propiedades para los elementos de la red tales como servidores, hosts, ruteadores, etc. Esas propiedades especifican cómo usualmente ese elemento de la red será sondeado y algunas acciones a tomar tales como emitir alguna alarma o enviar una notificación cuando el elemento no responda al sondeo. Se puede iniciar el monitoreo sin realizar cambio alguno a las propiedades si se desea usar las configuraciones por defecto. Configurar el mapa para determinar como WhatsUp monitoreará los elementos de red y finalmente gravar el mapa.

Crear un mapa de red.

El mapa de red es una representación gráfica de los elementos en la red que se desea monitorear, los elementos pueden ser PCs, servidores, ruteadores, switches, hubs, enlaces, impresoras o subredes, la figura 2.4 muestra un mapa de red típico.

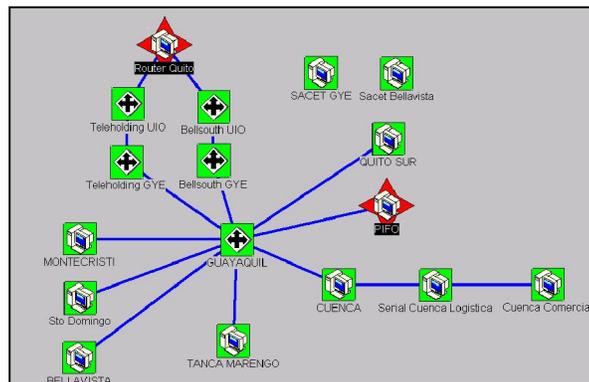


Figura 2.4.2.- Mapa de una red

Hay varias opciones para crear un mapa de red y agregar un elemento a un mapa existente:

Use la herramienta *Auto Load Wizard* para hacer que WhatsUp cree un mapa desde información contenida en su computadora o en la red a la cual su

computadora está conectada; whatsup crea un mapa leyendo los archivos de red en tu equipo local e identificando sistemas listados en los archivos.

Cargue un archivo de Hosts y WhatsUp creará un icono por cada host encontrado en el archivo.

Use *Scan IP* para automáticamente detectar y listar los elementos dentro de un rango específico de direcciones IP. Scan IP puede también escanear para cada elemento de red servicios tales como FTP o HTTP.

Use *Scan WinNet* para hacer que WhatsUp escanee una red Windows a la cual su computadora está conectada y cree un mapa de los sistemas que este encuentre.

Mapée la ruta desde su computadora local a un host remoto usando la herramienta *Traceroute*.

Manualmente creé un icono para cada elemento de red e ingrese información sobre el elemento.

En cualquiera de los casos, después de crear los elementos de red, usted puede organizar estos de manera que representen de la mejor manera su red usando el *Map Editor*. El editor de mapa permite dibujar líneas continuas entre los elementos de red y agregar rectángulos, elipses y texto. Usted puede usar estos objetos de dibujo para agrupar elementos de red en el mapa y proveer señales visuales para identificar diferentes segmentos de la red.

Auto Load Wizard

La herramienta Auto Load Wizard permite seleccionar parámetros los cuales automáticamente serán usados para determinar sistemas en la red y crear un icono por cada elemento. Dependiendo de los parámetros seleccionados

WhatsUp creará un mapa leyendo los archivos de red en tu PC local y identificando sistemas listados en los archivos. Estos archivos podrían o no podrían estar presentes en el sistema y pueden incluir un archivo host, el registro de windows, entradas en el registro de Internet Explorer e información de red.

Para usar Auto Load Wizard:

- a) Desde el menú *File*, seleccione *New* o presione un click en el botón *New* en la barra de herramientas y la caja de dialogo aparecerá.
- b) Seleccione la opción *Auto Load Map*, entonces hacer click en el botón *Next*. La pantalla *Auto Load Parameters* aparecerá.
- c) Seleccione los parámetros que se desee usar para crear el mapa.

Cargando un archivo de Hosts.

WhatsUp puede cargar un archivo Hosts, el cual lista nombres de hosts y sus direcciones IP asociadas, WhatsUp creará un icono por cada sistema listado en el archivo.

- a) Seleccione un mapa existente o cree un mapa nuevo. Para seleccionar un mapa existente, elegir *Open* en el menú *File* y buscar el nombre del archivo mapa. Para crear un nuevo mapa, seleccionar *New* en el menú *File*, o hacer click sobre el botón *New* en la barra de herramientas. Seleccione la opción *Create empty map* y entonces presionar el botón *Finish*.
- b) Desde el menú *Tools*, seleccione la opción *Import*, luego seleccionar *Hosts File*. Entonces la caja de diálogo *Browse* aparecerá.

- c) Localice el archivo host y presionar un click en el botón *OK*. WhatsUp lee el archivo host y crea un icono por cada elemento de red que este encuentre en el archivo hosts.
- d) Use el editor de mapa para organizar los elementos de red, cambiar tipos de icono, y agregar líneas de conexión y objetos de dibujo. Para cambiar un icono de elemento de red, doble click sobre este para mostrar la caja de diálogo Propiedades, seleccione la viñeta *Main*, entonces seleccionar *New Tipe*.
- e) Modifique las propiedades de los elementos de red.

Herramienta Scan IP.

Si se desea mapear un rango de sistemas en una red, usted puede usar la herramienta Scan IP. En esta herramienta se especifica un rango de direcciones IP a ser escaneadas y WhatUp sondeará cada dirección en ese rango. Si WhatsUp encuentra un dispositivo activo en esa dirección, se creará un icono de Workstation para el host.

Un escaneo puede también identificar los servicios de red que son válidos en cada sistema así que usted puede también monitorear los servicios tales como FTP, HTTP y SMTP.

Para iniciar Scan IP:

- a) Seleccione un mapa existente o cree un nuevo mapa de Windows.
- b) Desde el menú *Tools* seleccione *Net Tools*, elegir *Scan*, la caja de dialogo Scan aparecerá.
- c) Ingrese un rango de direcciones de red para escanear. Por ejemplo si su rango de direcciones de red es desde 156.21.50.1 hasta 156.21.50.254,

usted debería ingresar el rango como lo muestra la figura 2.5. Note que el escaneo trabaja consecutivamente desde el número de dirección de inicio hasta el último número en la dirección final en cada red, por ejemplo si se ingreso 245.245.1.50 como la dirección de inicio y 10.60 como la dirección final, este solo escaneará desde la IP 50 a la 60 en cada una de las redes desde 245.245.1 hasta 245.245.10.

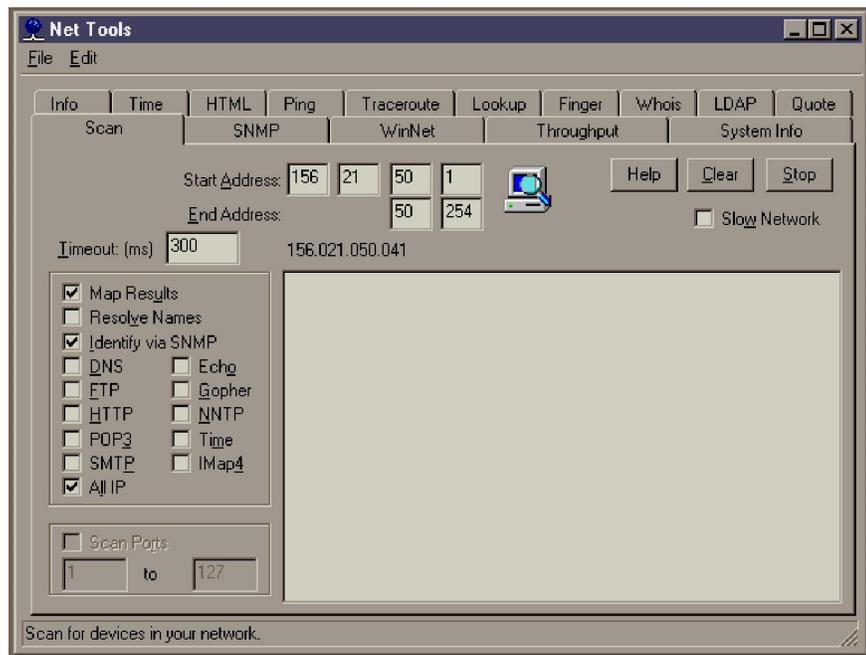


Figura 2.5. Herramienta Scan detectando dispositivos Hosts

- d) Seleccionar cualquiera de las opciones que se desee usar.
- *Map Results*, cuando esta opción es seleccionada, WhatsUp creará un icono por cada host que este encuentre, esta opción es marcada por defecto.
 - *Resolve Names*, cuando esta opción es seleccionada WhatsUp resuelve el nombre de host para cada dirección IP activa y muestra el

nombre en la caja de dialogo Scan y en el mapa (sí Map Results es marcada).

- *Time*, ingrese el tiempo fuera en milisegundos, si un elemento de red no responde al escaneo dentro de este tiempo, el Scan Ip continua en la próxima dirección IP; el timeout debe ser fijado en 300 ms o superior. Para máxima velocidad de escaneo fije el timeout en 300 y deshabilite la opción Resolve Names.
 - *Server Options*, (DNS, FTP, POP3, SMTP, IMAP4, HTTP, NNTP, SNMP, Echo, Gopher, Telnet) marque cualquiera de los tipos de servicios para los cuales se desee escanear, WhatsUp escaneará cada host activo que este encuentre para los servicios seleccionados. Esto permite monitorear los mencionados servicios en un host si están arriba o abajo.
 - *All IP*, cuando esta opción es seleccionada el Scan IP encontrara todos los dispositivos en el rango de direcciones IP especificado. Si la opción no es marcada el Scan IP encontrará solo los dispositivos que estén ejecutando los servicios seleccionados.
 - *Scan Ports*, puede usar la opción Scan Ports para escanear los puertos IP en cada elemento y listar cuales puertos están activos.
- e) Presionar el botón *Start*, WhatsUp escaneará el rango de direcciones IP, para cada dirección IP activa que este encuentre listará la dirección IP y también el hostname si la opción Resolve Names es seleccionada. La caja de dialogo Scan muestra las direcciones IP encontradas y presenta el mensaje “The scan is completed” después de escanear la dirección IP

final. Si la opción Maps results es seleccionada WhatsUp crea un icono en el mapa para sistema que este encuentre.

- f) Presionar *Close* para cerrar la caja de dialogo Scan IP.
- g) Use el editor de mapa para organizar los elementos de red, cambiar tipos de iconos y agregar líneas de conexión.
- h) Modifique las propiedades de los elementos de red.
- i) En el menú *File*, seleccione *Save* o *Save As* para guardar el mapa.

Scan WinNet

La herramienta Scan WinNet crea un mapa escaneando la red Windows a la cual la computadora está conectada y encuentra otros sistemas en la red. Este crea un icono por cada host que este encuentre en la red.

Para iniciar el Scan WinNet:

- a) Seleccione un mapa existente o cree un nuevo mapa.
- b) Desde *Tools* menú selecciones *Import*, luego *Scan WinNet*. WhatsUp escaneará la red Windows y creará un icono en el mapa por cada sistema que este encuentre. Note que el scaneo puede tomar unos pocos minutos para completarse dependiendo del tamaño de la red.
- c) Use el editor de mapa para organizar los elementos de red, cambiar el tipo de iconos, agregar líneas de conexión y objetos de dibujo.
- d) Modifique las propiedades de los elementos de red.
- e) Desde el menú File seleccione Save or Save As para guardar el mapa.

Herramienta Traceroute

La herramienta Traceroute es una herramienta de diagnóstico que permite ver y trazar la ruta actual de un paquete IP que sigue a un host internet. Se puede usar la herramienta Traceroute para mapear los elementos de red (usualmente ruteadores) que comprendan la ruta desde un host en nuestra red a un host remoto. WhatsUp mostrará un icono por cada ruteador y mostrará las conexiones de ruteador a ruteador hasta que encuentre el host remoto.

2.3.4.2 Monitoreo de la red

Después de crear el mapa de red se puede definir cada elemento de red y configurar como se desea monitorear un elemento y cómo seremos notificados si el estado cambia. Cada elemento de red tiene un conjunto de propiedades a través de las cuales se puede:

- Especificar el nombre y dirección del elemento y seleccionar el protocolo a usar para el sondeo.
- Configurar cada cuanto se desea sondear el elemento.
- Especificar cómo se desea que WhatsUp notifique cuando el estado de un elemento de red cambie. Podemos recibir notificación por medio de una alarma de sonido o un mensaje de beeper, pager, e-mail o voz.
- Especificar cualquier servicio (tal como Web, Mail, News Services) a ser monitoreado.
- Crear notas de texto para asociar con el elemento.
- Personalizar un menú de ventanas emergentes.

Monitoreo de servicios, recursos y aplicaciones.

WhatsUp puede ser configurado para monitorear los servicios encontrados en un elemento de red, servicios tales como DNS, FTP, POP3, SMTP, HTTP, IMAP4, NNTP, SNMP, Echo, Gopher y Telnet y notificará si uno de estos servicios está abajo.

Se puede también definir un servicio específico y ejecutar el monitoreo para este servicio definido por el usuario, esto es útil si un servicio no aparece en la lista de servicios o si este usa un número de puerto no estándar.

En Opciones de Servidor marcar alguno de los tipos de servicios que se desea escanear, WhatsUp escaneará cada host activo que encuentre para los servicios seleccionados. Esto permitirá monitorear cuales de los servicios están arriba o abajo.

Note que escanear hosts por esos servicios puede significativamente incrementar el tiempo que le tomaría a WhatsUp completar el escaneo.

Monitoreo de un servicio estandar.

Se puede seleccionar el servicio a ser monitoreado desde la lista de servicios estandar.

- 1) Selecciona un elemento de red. Hacer click derecho y seleccione la opción *Properties*.
- 2) En la caja de dialogo *propiedades* hacer click sobre la opción servicios y las opciones de servicios aparecerá. Por defecto WhatsUp monitorea servicios usando el protocolo de red ICMP. Si se está monitoreando un servicio fuera de un firewall y este firewall no permite paquetes ICMP, se necesita configurar el tipo de red a TCP/IP.

- 3) Seleccionar los servicios que se desea monitorear, WhatsUp escaneará todos los servicios que sean seleccionados. Si se usó la herramienta *Scan* para crear el mapa de red podríamos haber ya escaneado cada elemento de red por servicio válido. En este caso, cuando se seleccione la casilla servicios en propiedades de un elemento de red, la lista de servicios presentará los servicios que son válidos en ese elemento de red. Así mismo se puede eliminar los servicios que no se desee monitorear. Puede hacer click sobre la opción *Scan* en la caja de dialogo Servicios para escanear el elemento de red y determinar si alguno de los servicios estandar está corriendo en ese host.
- 4) Hacer click en la opción *Apply* para grabar los cambios.

Monitorear un servicio definido por el usuario.

Se puede monitorear un servicio específico que no aparece en la lista de servicios estándar. Se puede definir hasta tres servicios a monitorear definidos por usuario para un elemento de red. Por ejemplo, se puede desear monitorear un servicio IRC (Internet Relay Chat) o un servidor RADIUS (Remote Authentication and Dial-In User Service).

Para configurar el monitoreo de un servicio específico en un elemento de red:

- 1) Seleccione un elemento de red y hacer click en el icono *Monitor* y habilitar la opción *Monitor This*.
- 2) En la caja de dialogo Propiedades, hacer click en la opción Servicios. Las propiedades de servicios aparecerán.
- 3) En la caja de texto Name, ingrese un nombre único para el servicio. Este nombre será mostrado en la ventana de servicios.

- 4) En la caja de texto Port, ingresar el puerto TCP/UDP que se desea monitorear.
- 5) Seleccione el tipo de red TCP o UDP.
- 6) Opcionalmente en la caja de texto Timeout Seconds cambiar el tiempo fuera por defecto (5 segundos) para el estado de servicio.
- 7) Opcionalmente en la caja de texto Expect on Connect, ingresar un mensaje que el servicio remoto enviará de vuelta al conectar. La longitud de este mensaje está limitado a 19 caracteres.
- 8) Opcionalmente en la caja Send Command on Connect, ingresar el comando a enviar al puerto del servicio. En la caja Expected command response ingresar el mensaje de respuesta esperado para el comando send.
- 9) Opcionalmente en la caja de texto Send to disconnect ingresar el comando a enviar al desconectarse del servicio inapropiadamente. Si un comando no es especificado la conexión es serrada enviando un paquete FIN y entonces un paquete RST.
- 10) Hacer click en el botón Apply para grabar los cambios.

Monitoreo desde la Web

Esta sección describe como configurar WhatsUp Web Server y usar un Web Browser para acceder a las funciones de mapeo, monitoreo y notificación desde un computador remoto. WhatsUp provee un servidor Web que permite ver el estado de la red y realizar cambios en la configuración del whatsapp desde cualquier Browser. Se puede habilitar y deshabilitar el web server y fijar accesos a este servidor a través de las propiedades web.

Para configurar el web server:

- 1) Desde el menú *Configure*, seleccione *Web server*. La caja de texto *Web Server Properties* aparecerá.
- 2) Seleccionar la opción General para mostrar las opciones por configurar.
- 3) Estar seguro de que la opción *Enable Web Server* sea marcada.
- 4) Si se desea que los usuarios web estén habilitados a realizar cambios en las opciones del whatsapp, estar seguros que la opción *Enable Web Configuration* sea marcada. Se puede fijar accesos a funciones para cada cuenta de usuario web. Si la opción Enable Web Configuration no es chequeada, los usuarios web no podrán realizar cambios en ninguna de las configuraciones del whatsapp, ellos solo tendrán capacidad de ver el estado de la red.
- 5) Ingrese o cambie alguna de la información de configuración.

Main Title. El título mostrado en la página web principal para el sitio web de whatsapp. Se puede ingresar cualquier texto para el título. Refresh frequency. El número de segundos entre actualizaciones a la pantalla de whatsapp en el sitio web. Se puede fijar el tiempo de actualización en un rango desde 10 hasta 99999 segundos. TCP port. Por defecto es el puerto 80, el cual es el puerto estándar TCP/IP para un servidor web. Si ya se tiene un servidor web corriendo en el sistema, fijar el número de puerto en este campo a otro número de puerto (por ejemplo 8000).
- 6) Hacer click en OK para aplicar los cambios. Estos cambios toman efecto inmediatamente.

Personalizando el Sitio Web de WhatsUp

Se puede personalizar el sitio web de whatsapp agregando una propia página web al sitio o agregando información a la mostrada en los botones de la página principal la cual es mostrada después de entrar a el sitio web.

Desde el menú *View* seleccionar *Program Options*. La caja de texto Options aparecerá.

Seleccione la viñeta Web para mostrar las propiedades de configuración.

Use las siguientes opciones para agregar información al sitio web.

HTML Files Directory.

Si se desea que el servidor web de whatsapp contenga sus propias páginas, se puede agregar cualquier archivo HTML a este directorio. Por defecto es el subdirectorio Web en donde se instala el whatsapp. Si se usa un directorio diferente, se necesita especificar la ruta total a el directorio en esta caja de texto. Para abrir las páginas web en este directorio, en el campo para direcciones del browser ingresar el nombre de equipo del whatsapp host y el nombre de archivo para la página web.

Main Page Prefix.

Ingresa un mensaje a ser mostrado en la parte superior de la página web. Se puede ingresar hasta 100 caracteres de texto plano y/o código HTML en esta caja de edición. Las etiquetas HTML de comienzo y fin son automáticamente agregadas a cualquier código HTML que se ingrese. Un click del botón derecho del mouse en la ventana de edición dará acceso a las funciones copiar, pegar y eliminar de windows.

Un click en el campo OK aplicará los cambios. Los cambios tomarán efecto inmediatamente. La figura siguiente muestra la página web principal con información detallada.

Mapas disponibles para presentación web

Cualquier mapa de red que este abierto en whatsapp puede ser visto desde un browser. Además, los usuarios web con acceso a *Configure program* pueden cargar cualquier mapa localizado en el directorio map o en el sistema whatsapp. A continuación dos métodos de configurar el directorio map:

- En whatsapp seleccionar *Program Options* desde el menú *View*; un click en al viñeta Startup mostrará las opciones Startup. En la caja de texto *Directory* ingresar la ruta total para el directorio que contiene los mapas de red.
- Desde un Browser web, ingresar al servidor web de whatsapp. La pagina principal del whatsapp aparecerá. Seleccione *Settings* para mostrar las configuraciones del programa. En la caja de texto *Startup Map Directory* ingresar la ruta para el directorio que contiene los mapas de red.

Se debe reiniciar el whatsapp para que los cambios tomen efecto.

Configurando accesos al servidor web

Whatsup tiene dos modos en que se puede configurar el acceso al servidor web.

Se puede usar uno de ellos o ambos juntos.

- Se requiere un Id de usuario y password para ver datos en el sitio web del whatsapp. Esto incluye configurar la presentación y funciones que el usuario pueda acceder.

- Especificar una dirección IP o grupo de direcciones IP que garanticen el acceso al sitio web o sea denegado el acceso..

Cuentas de usuario por defecto para el servidor web

WhatsUp provee dos Id de usuarios por defecto para acceder al servidor web:

- El Id de usuario admin tiene acceso total a las funciones y presentaciones del whatsapp, con la excepción que ellos no pueden configurar o cambiar cuentas de usuario web.
- El Id de usuario guest sin password tiene acceso a todas las presentaciones del whatsapp pero no puede cambiar ninguna configuración del whatsapp. Si un usuario ingresa un Id de usuario sin password, el será logoneado dentro de una cuenta invitado. Si no se desea que los usuarios accedan al servidor web en este modo, entonces se debe deshabilitar los privilegios para cuentas invitado.

Configurando cuentas de usuario para el servidor web.

Se puede agregar hasta 20 cuentas de usuario para acceso web al whatsapp y se puede asignar diferentes niveles de acceso para cada usuario.

- 1) Desde el menú *Configure*, seleccione *Web Server*. La caja de texto *Web Server Properties* aparecerá.
- 2) Seleccione la viñeta *Users* para presentar las propiedades de acceso de usuario
- 3) Seleccione la opción *Enable Web Security* (estar seguro que esta opción esté marcada). Si esta opción no es marcada los usuarios web estarán habilitados a ingresar o logonearse sin ingresar un password.

- 4) Un click en Add User e ingrese el nombre de usuario y el password .
- 5) Seleccione la página web de whatsapp y las funciones web que se desee proveer al usuario.
- 6) Si se desea realizar cambios desde la interface web en la aplicación whatsapp, seleccione la opción *Automaically save changes from web site*. Si esta opción no es seleccionada cualquier cambio realizado desde la interface web se perderá al cerrar la sesión web.
- 7) Un click en la opción OK aplicará los cambios.
Cuando un usuario abre la página web de whatsapp deberá ingresar un useríd y password para que pueda ver la página.

2.3.4.3.- Ejecutando WhatsUp como servicio NT

WhatsUp puede ejecutarse como un servicio de sistema en Windows NT o posterior. Cuando se ejecuta como un servicio se debe usar la interface web para ver los mapas y cambiar configuraciones, así se usa menos memoria.

Algunos beneficios de ejecutar Whatsup como un servicio NT son:

- El servicio puede correr completamente oculto, así se provee un nivel extra de seguridad.
 - Como con cualquier servicio NT, se puede configurar WhatsUp para que inicie automáticamente siempre que el Windows sea reiniciado.
- 1) Primero cree el mapa y configure el monitoreo desde la consola del WhatsUp.
 - 2) Cuando este satisfecho con la configuración del mapa, fijar las opciones que afectan como se trabajará con el servicio NT.
 - 3) Inicie el servicio NT.

2.3.4.4.- Configurando en la consola de Windows.

Se recomienda que se cree el mapa de red usando whatsapp en modo de operación normal en la consola de windows. Una vez que el mapa sea creado seleccione cualquier opción de programa deseado. Esas opciones tomarán efecto durante la operación como un servicio NT.

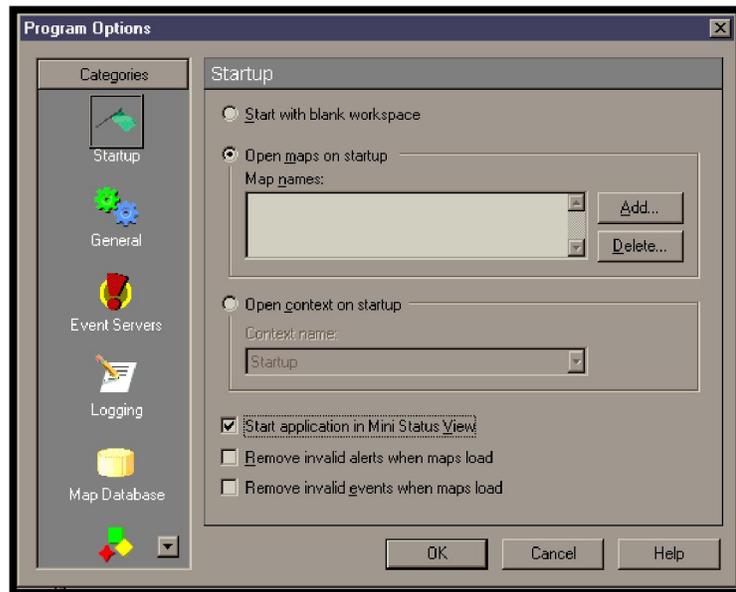


Fig 2.6.- Configurando la consola de WhatsUp

En el cuadro de dialogo *Startup*, en las opciones de programa (Configure -> Program Options -> Startup), se puede especificar múltiples mapas a cargar en Startup en la caja de texto *Map Names*. Asegurarse que la opción Open maps on startup sea marcada y los mapas listados en la caja de texto Map Names carguen al inicio. Hacer click en *Add* y seleccione cualquier mapa adicional que se desea que cargue al inicio. Mapas adicionales pueden ser subsecuentemente cargados y descargados usando la interface web.

Fijar cualquiera de las opciones de servidor web (Configure -> Web Server -> User). Seleccione Enable Web Security. Si se fija algún permiso o cualquier otro parámetro de configuración web mientras se ejecuta WhatsUp en modo de operación normal en la consola Windows, se necesita parar y reiniciar el modo de servicio NT.

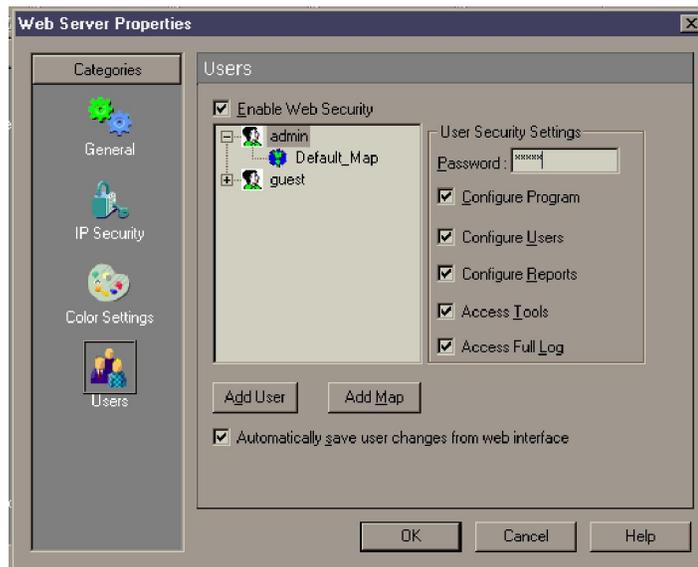


Figura 2.7.- Configurando el acceso de usuarios al servidor web

En la caja de diálogo *Users*, si se selecciona *Automatically save user changes from web interface* se estará habilitado para cambiar opciones de usuario desde la interface web.

Iniciando y preparando el servicio NT

La instalación de WhatsUp incluye un archivo ejecutable llamado *wugsvc.exe* para el propósito de instalar, remover, iniciar y parar el servicio WhatsUp NT.

Para instalar e iniciar whatsapp como servicio NT:

- Ir al prompt DOS.
- Navegue hasta el directorio del programa whatsapp.
- Ingrese el siguiente comando: *wuagsvc*–install.

Para remover whatsapp como un servicio NT:

- Ir al prompt DOS y cambiarse al directorio de whatsapp.
- Ingrese el siguiente comando *wuagsvc*–remove.

Note que esos dos comandos no remueven el whatsapp, ellos solo remueven la capacidad de servicio NT.

2.3.4.5.- Emisión de reportes

Informes con historiales

Whatsup provee cuatro tipos de logs (reportes):

- Syslog – Logs (*SL-yyyy-mm-dd.tab*) mensajes UDP estándar enviados desde routers, switches, hosts UNIX, etc.
- Activities – son cambios al estado de red, tal como un dispositivo dado de baja o un dispositivo volviendo a levantar. Activities son guardadas en el Activity Log, el cual provee una historia de que ha ocurrido en la red. En adición la ventana Debug Log provee una vista de actividades y como ellas ocurrieron.
- Polling Statics – son los tiempos de ciclos acumulados de sondeos enviados a un dispositivo. Las estadísticas de sondeo son guardadas en el Statics Log (*ST-yyyy-mm-dd.tab*).
- SNMP traps – el log Trap SNMP (*SP-yyyy-mm-dd.tab*) muestra todas capturas SNMP que han sido recibidas. Cuando se usa este visor, todas las

capturas pueden ser observadas. Para habilitar SNMP traps, ir a Configure -> Program Options -> Event Servers -> SNMP Traps, un click en *Configure* y seleccione *Listen for messages on Port*.

Desde estos datos en el Log, Whatsup puede crear varios reportes y gráficos que muestra el estado de la red en diferentes formas. Desde el menú *Reports* se puede crear lo siguiente:

Performance Graphs. Muestra dispositivos por mejor o peor funcionamiento basado en estadísticas de sondeo, y muestra gráficas por cada dispositivo.

Outage Reports. Muestra cambios en el estado de dispositivos, servicios y actividades del Whatsup como abrir y cerrar mapas. Se puede imprimir este reporte o crear un archivo de formato definido.

Statics Report. Muestra el tiempo de viaje y regreso y porcentajes de sondeos perdidos basados en las estadísticas de sondeo acumuladas para cada dispositivo. Se puede imprimir o crear un archivo de formato definido.

Informes gráficos de los niveles de servicio

Se puede graficar las estadísticas de sondeo que Whatsup acumula para un dispositivo de la red. Los gráficos muestran el funcionamiento de un dispositivo trazando el tiempo promedio que le tomó a un dispositivo responder a un sondeo. Además, las gráficas pueden mostrar datos adicionales, como el dispositivo con la mejor o peor disponibilidad, o el dispositivo con el más alto o más bajo promedio de sondeos perdidos, o el mejor o peor día de la semana para el funcionamiento de la red.

Altos valores de tiempo (RTT) de respuesta indican un pobre funcionamiento, bajos valores indican un muy buen funcionamiento, y bajos valores para sondeos perdidos indican alta disponibilidad.

Opciones de gráfico

Cuando se desea crear un gráfico de funcionamiento, se puede escoger:

- El intervalo de tiempo para el cual se desea ver las estadísticas: diariamente, semanal, mensual o todas las observaciones en el log.
- En algunos casos el formato de gráfico puede ser bar chart o área chart.
- Como se desea ordenar los datos, por nombre de dispositivo, en orden ascendente o descendente.
- Que mapas y que dispositivos se incluyen en un gráfico.
- El formato de archivo, se puede exportar un gráfico a la mayoría de los formatos conocidos.

Creando un gráfico

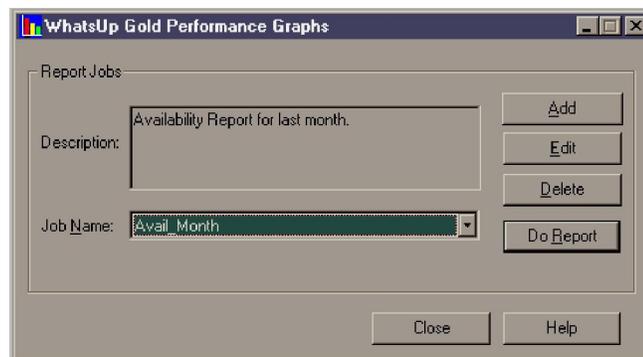


Figura 2.8.- Configurando opciones de gráficos.

Para crear un gráfico:

- 1 Inicie la herramienta *Performance Graphs* haciendo la siguiente:

- Desde el menú *Reports*, seleccione *Performance Graphs*.
- Desde el menú Start, seleccione Whatsup -> Whatsup Gold -> Whatsup Gold Performance Graphs.
 - En la pantalla mapa, seleccione el dispositivo, haciendo click derecho seleccione Performance Graphs.

Todos los trabajos de reporte están disponibles en la caja de lista *Job Name*. Cuando un nombre es seleccionado una descripción de este es mostrada en el campo descripción.

Para crear un reporte solicitado, seleccione este y hacer click en *Do Repor*.

Se puede también agregar, editar o eliminar trabajos de reporte.

Si se edita un *Job Name* o se agrega uno nuevo, la caja de dialogo *Report Job Properties* aparecerá.

- 2 Seleccione *Report Type* para fijar que datos de funcionamiento se verán y el formato del gráfico.
- 3 Seleccione el Date Range para el reporte. Cuando se seleccione una opción el *Start Date* y *End Date* son presentados. Seleccione *Custom* si se desea ingresar un Start y un End Date para el reporte. Las fechas se deben ingresar en el formato *yyyymmdd*.
- 4 El cuadro *Data Source* muestra *wugstatdata.tab* como el valor por defecto. Estadísticas normales son siempre logeadas en *ST-yyyy-mm-dd.tab*. Para archivar estadísticas, se puede copiar la estadística normal a un nombre

de archivo diferente tan largo como el archivo lo es en la parte superior del whatsapp.

5 El *Sort Order* es sorteado por el nombre de dispositivo en orden alfabético. Se puede ordenar en orden ascendente o descendente para todos los reportes.

6 Use *Zoom Factor* para cambiar el tamaño de presentación del reporte.

7 *Export Options*. Si se desea exportar el reporte fijar las siguientes opciones:

- *Export Format*. Selecciona el formato de exportación deseado.
- *Destination*. Selecciona cualquier archivo de disco o Microsoft Mail.

8 Ingrese el *Query Options* para determinar que mapas y que dispositivos incluir en el mapa.

9 Hacer un click en *Do Report*. Se puede tener que esperar unos pocos segundos para que el reporte aparezca, dependiendo del número de dispositivos incluidos en el reporte. Como los datos se acumulan para el reporte la caja de diálogo *Exporting Reports* aparecerá. Dentro de esta caja de diálogo se puede cancelar el reporte haciendo click en cerrar.

Notificación de eventos

Cuando una actividad ocurre en la red (cambia un dispositivo o servicio, ocurre un evento, etc.), whatsapp puede ejecutar muchas diferentes acciones:

- Guarda la actividad en un Activity Log.
- Actualiza las propiedades de estado de dispositivo y cajas de diálogo Log.
- Cambia la apariencia del icono de dispositivo en el mapa.
- Opcionalmente envía una notificación.

Whatsup puede enviar una notificación en muchos modos, este puede:

- Enviar una alarma de sonido.
- Activar un beeper.
- Ejecutar un programa.
- Parar o reiniciar un servicio.
- Enviar un mensaje a un pager.
- Enviar un mensaje E-mail SMTP.
- Enviar un mensaje pregrabado a un teléfono, solo si se tiene instalado un modem.
- Mostrar una pantalla emergente en un sistema Windows.
- Enviar un grupo de notificaciones que incluyen cualquiera de los tipos ya mencionados.

Configurar una notificación envuelve dos pasos:

- Primero se necesita definir la notificación que se desea usar tal como activar el beeper de un administrador de red o enviar un e-mail.
- Entonces se asigna la notificación a un dispositivo en particular, dispositivos seleccionados o todos los dispositivos.

Para realizar estos pasos se usa el *Notifications Library*, el cual muestra las notificaciones que se pueden asignar a uno o múltiples dispositivos. En esta ventana es en donde se crea una nueva notificación, se prueba, se edita, o se remueve desde la librería.

Desde el menú *Configure*, seleccione *Notifications Library*.

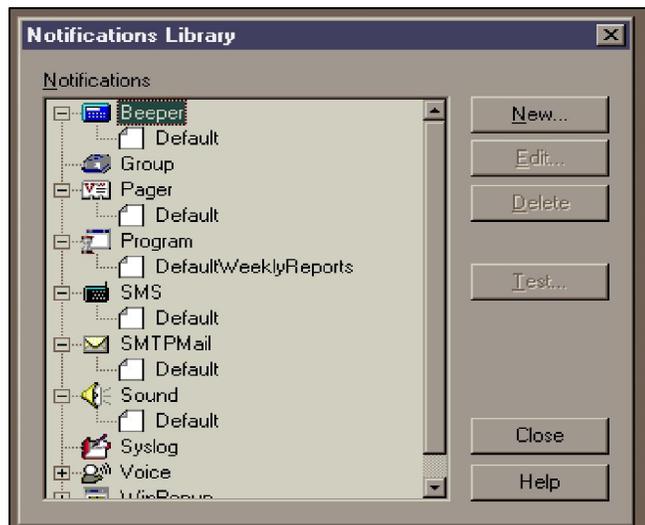


Figura 2.9.- Ventana de configuración de Notificaciones

Alarmas de escritorio

Notificaciones WinPopup

Una notificación WinPopus muestra un mensaje de ventana emergente en un sistema Windows. Se puede definir una notificación para cada dispositivo windows por el cual se deseé mostrar un mensaje.

Para definir una notificación WinPopup:

- 1) Desde el menú *Configure*, seleccione *Notifications Library*, entonces seleccione *WinPopup*.
- 2) Un click en *New*, e ingrese un nombre único para la notificación en el campo *Display Name*.
- 3) En el campo *Destination*, especifique el dispositivo o dominio donde se desee recibir la notificación. Note que un dominio es marcado con un asterisco (*).
- 4) En el campo de texto *Message*, ingrese un mensaje de texto más cualquiera de las variables de notificación.
- 5) Click en *OK*.

Device Variable	Returns
%1	Info line 1 (from General of device properties)
%2	Info line 2 (from General of device properties)
%a	IP Address (from General of device properties)
%C	Device Identifier (set in the Alert setup 1px; BORDER-LEFT: #000000 0.5pt solid; WIDTH: 322px; PADDING-TOP: 1px; BORDER-BOTTOM: #000000 0.5pt solid" width=322>
%c	Same as %T. returns the device type. Use %T, %c was used in previous versions.
%h	Host Name (from General of device properties)
%M	SNMP Community
%m	Detailed Event description. (SNMP traps - Returns the full SNMP trap text.) (Windows Log Entries - Returns information contained in the Windows Event Log entries.) (Syslog Entries - Returns the text contained in the Syslog message.)
%N	Notes. (Notes are from the device properties Notes).
%n	Display Name (from General of device properties)
%O	SNMP Object identifier. This is the word "unknown" if SNMP Object box is blank.
%R	SNMP Read Community (from the SNMP of device properties)
%S	Device status (such as "timed out" or "did not respond")
%s	Winsock error code
%T	Device Type (from General of device properties)
%u	Can result in the word "UP", "DOWN", "SVCUP", "SVCDOWN", or "Event
%V	Names of down services or monitors, followed by the word "Services"
%v	Names of down services or monitors
%W	SNMP Write Community (from SNMP of device properties)
%Y	Full service names of all UP monitored services on a device
%y	Abbreviated names of all UP monitored services on a device
%Z	List of down services using the abbreviated name if available
%(services::up)	Abbreviated names of all services that are up
%(services::down)	Abbreviated names of all services that are down
%(services::justup)	Abbreviated names of all services that just came back up with the last poll
%(services::justdown)	Abbreviated names of all services that just went down with the last poll
%(*)	Displays all of the contents of the

	Event Payload
System Variable	Returns
%A	Names of devices with down services
%D	# of Down Devices
%d	Date format is (mm/dd/yyyy)
%e	Display Names of Down Devices
%L	The last 100 lines of the Activity Log file, EV-yyyy-mm-dd.tab (or %Lnn where nn = last nn lines of the log file)
%Lnn	Last nn lines of the log file (n can go up to 99)
%o	# of devices with Down Services
%P	Display Names of Up Devices
%t	Current time (hh:mm:ss)
%U	# of Up Devices

Tabla 2.1. Variables usadas en las notificaciones

Busca personas

Se puede definir notificaciones de beeper para activar un dispositivo busca personas cuando un dispositivo de red no responda al sondeo.

- 1) Desde el menú *Configure* seleccione Notifications Library, y entonces seleccione *beeper*.
- 2) Un click en *New* y luego ingrese un nombre único en el campo *Display Name* para identificar la notificación de beeper, por ejemplo, “ Beep Alberto”.
- 3) En el campo Beeper Number ingrese el número de teléfono a marcar.
- 4) En el campo Dial String, el valor por defecto es ATDT%s,,,%s#; whatsapp reemplaza el primer %s con el número de teléfono y el segundo %s con el código de beeper. La mayoría de los módems y beepers soportan el uso de # para terminar el mensaje. Se puede encontrar la necesidad de incrementar el número de comas en el campo Dial String, el dial string puede ser editado desde la caja de diálogo *Port Settings*.

- 5) En la caja de lista *Modem Setup*, seleccione el modem primario o uno alternativo. Modem Setup es usado específicamente para soportar diferentes proveedores de servicios en caso de que se use más de un proveedor para el envío de las notificaciones de beeper. Note que cambiar los valores de *Port Settings* para el modem seleccionado afecta todos los usos de esa configuración.
- 6) En la sección *Signal Codes*, el *Up Code* especifica los caracteres a enviar al beeper para indicar que ha levantado después de estar un tiempo determinado abajo (el valor por defecto es 0*). El campo *Down Code* especifica el código a enviar para especificar que el dispositivo está abajo (el valor por defecto es 9*). El campo *On Event Code* especifica el código a enviar para indicar que un evento ha sido recibido por el dispositivo, se puede usar el carácter asterisco (*) para separar códigos desde el mensaje subsecuente.
- 7) Realice un click en *OK* para grabar la nueva notificación.



Figura 2.10. - Configurando una notificación vía Beeper.

Para probar una notificación, seleccione esta y realice un click en el botón *Test*, whatsapp ejecutará y responderá con un mensaje Satisfactorio o Falla de mensaje.

Para editar una notificación, seleccione *esta* en la caja de lista y hacer click en *Edit*, y entonces ingrese los cambios en las propiedades. Click en *Ok* para grabar los cambios.

Para eliminar una notificación, selecciónela en la caja *Lista* y hacer un click en *Delete*.

Emails

WhatsUp puede enviar un mensaje a una dirección e-mail cuando un dispositivo no responda al sondeo. Por ejemplo crear una notificación que será

asignada a un servidor web, cuando este dispositivo emita una alerta esta notificación será enviada al administrador web.

- 1) Desde el menú *Configure*, seleccione *Notifications Library*, y entonces seleccione *SMTP Mail*.
- 2) Realice un click en *New* e ingrese un nombre único en *Display Name* para identificar la notificación e-mail, por ejemplo “Mail Web Master”.
- 3) En el campo *Mail Server*, ingrese la dirección IP del servidor e-mail (servidor SMTP).
- 4) En el campo *To*, ingrese una o más direcciones e-mail aceptadas por el servidor SMTP. Separe cada dirección con una coma.
- 5) La dirección *From* define el remitente de una notificación e-mail como `whatsup@%1`, donde %1 es convertido por Whatsup al nombre de equipo local. Si se cambia la dirección por defecto asegurarse de mantener los corchetes (<>) en su lugar. El servidor e-mail puede requerir estos para ser un usuario e-mail válido.
- 6) En el campo *Subject*, ingrese un mensaje de texto o cualquiera de las variables de notificación.
- 7) En el campo *Message*, ingrese un mensaje texto más cualquiera de las variables de notificación.

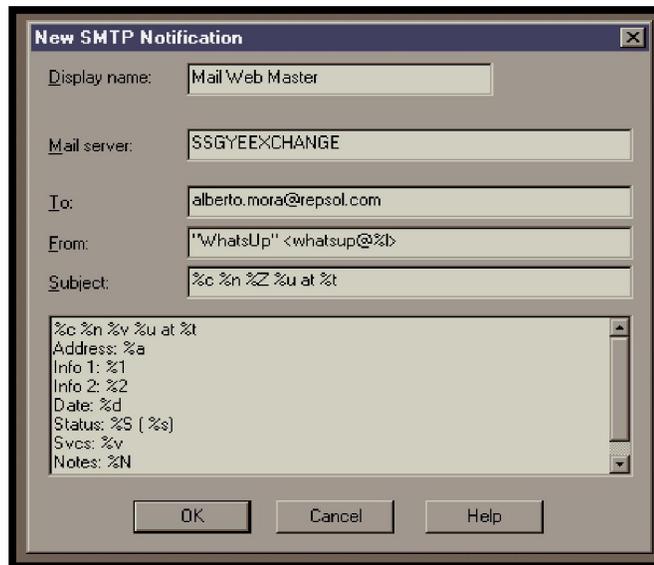


Figura 2.11.- Configurando una notificación vía e-mail.

8) Un click en *OK* para grabar la nueva notificación.

Para probar la notificación, seleccione *esta* en la ventana Notification Library y hacer un click en el botón Test. Whatsup ejecutará una prueba y responderá con un mensaje satisfactorio o Falla de mensaje.

Mensajes SMS

Si se tiene instalado el plug-in SMS de Whatsup, se estará habilitado para enviar notificaciones SMS (Short Message Service). SMS es similar a paging. Sin embargo, mensajes SMS no requiere que un teléfono móvil esté activo y esté dentro de un rango y será sostenido por un número de días hasta que el teléfono esté activo y dentro del rango de cobertura. Los mensajes SMS son transmitidos dentro de la misma celda o a cualquiera con servicio roaming habilitado. Note que whatsapp transmite los mensajes SMS al proveedor y el

proveedor realiza un forward de este al teléfono móvil. Whatsup no hace broadcast de mensajes SMS directamente.

Llamadas al teléfono

Se puede definir una notificación de voz para enviar un mensaje de voz a un teléfono cuando un dispositivo o servicio llega a caer o levantar. Se pueden utilizar los archivos .wav por defecto incluidos en el whatsapp o se puede grabar sus propios archivos .wav.

Cuando una notificación de voz es disparada (sea por un dispositivo o servicio caído) whatsapp llama al número de teléfono especificado y ejecuta un mensaje inicial. El mensaje por defecto es “*whatsapp tiene un mensaje para ti. Presione 1 para escuchar el mensaje*”, cuando se presione el 1 en el teléfono, uno de los mensajes para dispositivo caído o levantado será escuchado. Tal como “un host está caído”, si se desea incluir el nombre del dispositivo en el mensaje se debe grabar un archivo .wav para el dispositivo en particular en ingresar el nombre del archivo en la caja de diálogo *Add Notifications* cuando se agregue una notificación de voz a algún dispositivo. Note que el campo Voice en el sistema de notificaciones solo será mostrado por whatsapp si el sistema dispone de un modem y su respectivo controlador instalado.

- 1) Desde el menú *Configure, seleccione Notifications Library*, y entonces seleccione *Voice*.
- 2) Realice un click en *New* ingrese un nombre único en *Display Name* para identificar la notificación de voz, por ejemplo “Llamada al administrador”.
- 3) En el campo *Phone number*, ingrese el número a marcar.

- 4) En el campo *Repeat mesg*, ingrese o seleccione el archivo de sonido .wav que será ejecutado como mensaje de voz inicial que le dirá al administrador que se ha recibido un mensaje desde whatsapp.
- 5) En el campo *Count*, ingrese el número de veces a enviar el mensaje inicial.
- 6) En el campo *Button*, ingrese el número a presionar en el teléfono por el administrador para conocer el mensaje de estado. El mensaje por defecto le dice al receptor presionar 1 para recibir el mensaje de estado, pero se puede fijar este número en 99 para que este acepte cualquier número presionado en el teléfono. Note que si una máquina contestadora contesta el teléfono, la notificación de voz no llegará más allá del mensaje inicial.

Opcionalmente, ingrese el archivo de sonido que será ejecutado para cualquiera de los mensajes de estado o whatsapp usará los mensajes por defecto.

- Item Down. Busca el archivo .wav elegido que se desea ejecutar cuando el dispositivo en el mapa está caído
- Item Up. Busca el archivo .wav elegido que se ejecutará cuando el dispositivo levanta.
- Service Down. Busca el archivo elegido que se desea ejecutar cuando el servicio monitoreado en un dispositivo está caído.
- Service Up. Busca el archivo a ejecutar cuando el servicio monitoreado en un dispositivo llega a levantar.



Figura 2.12.- Configurando una notificación de voz

2.3.5. Costos de fabricación del prototipo

Para implementar nuestro sistema necesitaremos un computador con características bastantes muy básicas, la empresa cuenta con personal calificado en ensamblaje de PCs, por lo que el valor final de este equipo sería en promedio \$500. Cabe indicar que el cliente puede proporcionar el equipo a la hora de ofrecer el producto/servicio.

Se necesita de un punto de red con conexión a la red de voz y datos de la compañía, tenemos personal capacitado para la instalación de este ítem. Puede darse el caso que el cliente ya tenga un punto sin usar o personal que realice esta tarea.

La licencia del software What's Up tiene un valor de \$ 50 para 4 PC's y de \$ 84 para un número ilimitado de equipos, según el estudio de mercado realizado para este emprendimiento se encontró que estas dos licencias son las preferidas en nuestro entorno.

Se necesitará una base celular o una línea de teléfono con salida a celulares activada, hemos elegido Movistar para nuestro emprendimiento ya que la empresa

elegida para nuestro prototipo cuenta con estos planes corporativos. Hay que indicar que hay clientes que proporcionarían este equipo.

El único proveedor en el mercado local actualmente es Skytel, hoy en día muy pocas empresas usan este medio para localizar a sus empleados pero se lo presenta de forma opcional.

Items	Observación	Valor
Computador	Opcional	\$ 500,00
Punto de red	Opcional	\$ 45,00
Softward	What´s Up	\$ 84,00
Base Celular	Opcional	\$ 100,00
Movistar	valor mensual a pagar	\$ 10,00
Skytel	Valor mensual a pagar	\$ 4,40
TOTAL		\$ 743,40
Items	Observación	Valor
Computador	Opcional	\$ 0,00
Punto de red	Opcional	\$ 0,00
Softward	What´s Up	\$ 84,00
Base Celular	Opcional	\$ 0,00
Movistar	valor mensual a pagar	\$ 10,00
Skytel	Valor mensual a pagar	\$ 4,40
TOTAL		\$ 89,40

Tabla 2.2.- Costos de fabricación del prototipo.

Como se detalla en la tabla 2.2 el costo de fabricación de nuestro prototipo puede variar según lo desee el cliente desde \$ 89,40 hasta \$ 743,40. Esto se debe a que hay clientes que ya tienen ciertos ítems necesarios.

2.4. Instalación y espacio físico de la microempresa

2.4.1. Equipos y maquinaria

Los equipos que necesitaremos para nuestra empresa son los siguientes:

Área de trabajo común:

- 3 PCs para el área de trabajo
- 3 UPS
- 3 escritorios esquineros para el área de trabajo común
- 1 copiadora multifunción para el área de trabajo
- 4 sillas
- 1 Teléfono

Área de recepción:

- 1 PC para el área de recepción
- 1 escritorio para la recepción
- 1 juego de muebles para la sala de espera en la recepción
- 1 silla
- 1 Teléfono

Área de Gerencia de Proyectos:

- 1 portátil para el área de gerencia
- 1 mesa de reunión para juntas de trabajo y juntas con clientes
- 1 escritorio para la gerencia
- 9 sillas
- 1 sillón gerencial
- 1 Teléfono

Área de Gerencia de Proyectos:

- 1 portátil para el área de gerencia
- 1 Escritorio
- 1 silla y 1 sillón gerencial
- 1 Teléfono

2.4.2. - Distribución de la planta

Nuestra empresa estará ubicada en la planta baja de la casa de uno de los emprendedores la cual está ubicada en la ciudadela COVIEM Mz.-47 S-6, cuyas dimensiones son de 15m de largo por 10m de ancho, nuestra empresa contará con una sala de recepción la cual tendrá una pequeña salita de estar, una oficina tipo laboratorio que será nuestra área de trabajo común, contará también con una oficina para la gerencia, además tendremos una cafetería y un baño general como se muestra en la fig. 2.13

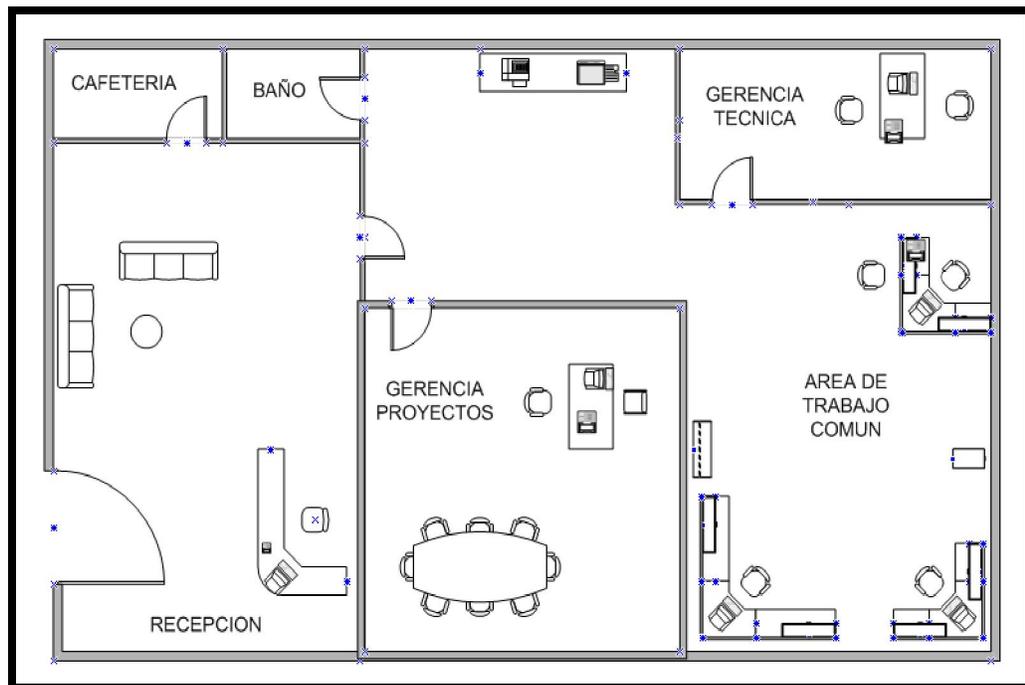


Figura 2.13.- plano de la oficina

2.4.3. Plan de producción

Considerando el número de clientes potenciales y que la implementación del producto es a mediano/largo plazo creemos que podemos colocar en el mercado un número respetable de soluciones para PYMES. Nuestro contacto en el exterior nos hace llegar las licencias en 15 días, realizaríamos una compra inicial de 5 licencias para 5 equipos y 5 ilimitadas, con lo cual creemos tener stock para dos meses.

Una vez que el cliente solicite el servicio se realiza la compra de las partes para ensamblar un computador, al cual ya se le instala el software, esto tomara 24 horas. Instalar el punto de red y configurar el PC ya conectado a la red del cliente tomaría alrededor de 3 días. Se le dará una capacitación de 1 día y se le entregará un manual detallado. Al cliente se le da un periodo de prueba de 2 semanas durante lo cual se realizaran varios simulacros programados junto con el cliente. Detallando todo lo anterior podemos poner en producción un promedio de 5 productos en el mercado.

CAPITULO 3

ANALISIS DEL MERCADO

3.1.- Contexto y análisis del sector

Aspectos a estudiar:

Ü **Diagnostico de la estructura actual y perspectivas del sector en el cual se va a entrar. Posibilidades de crecimiento.**

En el mercado actual toda empresa necesita proteger su red de datos y la mayoría de las empresas con lo único que cuentan es con un antivirus, tienen poca o ninguna noción de los beneficios de un IDS, firewall, y otros muy importantes sistemas de protección.

Ü **Estado del sector, en términos de: productos, mercados, clientes, empresas nuevas, tecnología, administración, desarrollo, etc.**

Actualmente se está difundiendo una cultura de auditoría de sistemas por ejemplo se han dictado un par de seminarios o charlas de estos temas en el CRIEL (Colegio Regional de Ingenieros Eléctricos y Electrónicos), si se revisa catálogos de productos de Networking se encuentran variados dispositivos para brindar seguridad a las redes pero son pocas las empresas que se deciden a invertir en implementar estos sistemas ya sea por desconocimiento, lo consideran un gasto en vano, o piensan que nunca serian objeto de ataque por un hacker.

Ü **Tendencias económicas, sociales o culturales que afectan al sector.**

La gerencia siempre por minimizar gastos rechazan los proyectos presentados por su personal de sistemas.

Hay una gran creencia que los ataques de hackers se dan solo en las películas de ciencia ficción.

La tercerización más conocida como Outsourcing afecta mucho ya que es muy conocido que personal de sistemas por no sentirse de la empresa tienden a: robar software/equipos, conectar a la red equipos ajenos a la empresa, y por qué no boicotear las operaciones diarias.

La globalización es un aspecto positivo ya que obligan a realizar auditoria de sistemas, algo que aquí en el país es algo no practicado.

Barreras de ingreso o salida.

- Darle a entender a los potenciales clientes que este producto es la mejor forma de cuidar algunos de sus principales recursos (información, equipos)
- Gerentes priorizando la reducción de gastos dan poca importancia a una auditoria.
- Empresas locales absorbidas por multinacionales donde la auditoria es una regla.
- Clientes que temen al cambio.

Ü Rivalidades entre los competidores.

Es un mercado nuevo no hay competencia local, a nivel nacional se ha encontrado información en Internet de empresas en Quito que podrían extenderse hasta Guayaquil.

Ü Poder de negociación de clientes y proveedores.

Nuestra experiencia en el mercado nos permite decir que estamos preparados para manejar clientes especiales y proveedores que en este caso se mantendrá el contacto por medio de internet.

Ü **Amenaza de ingreso de nuevos productos o de sustitutos.**

Uno de los principales problemas al trabajar con tecnología es que esta cambia con una velocidad asombrosa, por lo que se puede decir que siempre nos veremos amenazados por el ingreso de nuevos productos o sustitutos.

Ü **Amenaza de ingreso de nuevos negocios.**

Esta probabilidad es grande pero consideramos que tenemos una ventaja al ser pioneros en el mercado local

3.2.- Análisis del mercado propiamente dicho

3.2.1- Clientes

Debe analizarse:

- Ü Tipos de compradores potenciales, segmentados por actividad, edad, sector, nivel, ubicación, ingresos, etc.
- Ü Características básicas de esos clientes (mayoristas, minoristas, productores, consumidores directos).
- Ü Localización geográfica de los clientes.
- Ü Base de decisión de compra de los clientes (precio, calidad, servicio, amistad, política, religión, forma de pago, etc.).
- Ü Opiniones de clientes que han mostrado interés en su P/S.
- Ü Formas posibles de evitar la falta de interés.

3.2.2- Competencia

Nuestra investigación dio como resultado que un gran número de la competencia se encuentra localizada en Quito y un pequeño número de compañías existe actualmente en Guayaquil, a continuación un cuadro detallado de algunos competidores:

Institución	Información	Comentario
ISACA-QUITO-ECUADOR	w_ww.isaca .org	Ofrece auditoria de sistemas y otorga certificados a profesionales CISA y CISM. Empresa de Quito
Acevedo y Asociados	Auditoria, asesoría, asesoría financiera, administración financiera de negocios, asesoría de sistemas, asesoría de RR.HH., asesores tributarios.	Competidores entrantes Empresa de Quito
AudiSecurit	Auditoria informática integral, Evaluación de centros de cómputo, Evaluación de la gestión IT, auditoría interna de sistemas. Análisis de riesgo.	Empresa de Quito
Kruger Corporation S.A.	Auditora de sistemas de información, Diagnostico y planificación estratégica, consultoría en business, consultoría de negocios	Empresa extranjera radicada en Quito
IngelSystem	Auditoría de sistemas	No se encontró localidad
NEXIA INTERNATIONAL MONTES & ASOCIADOS S.A	http://nexamya.com.co Auditoria de sistemas, Asesoría tributaria, gestión de calidad, Outsourcing administrativo.	Empresa colombiana entrando al país la sede principal queda en Londres
LeadSolutions	Soluciones informáticas empresariales	Guayaquil, aliándose con IMPSAT.

Tabla 3.1.- lista de la competencia

El poder de los proveedores

Necesitaremos proveedores de productos, servicios e información. Nuestros productos y servicios dependerán del precio, calidad y la buena relación que tengamos con nuestros proveedores. A continuación algunos proveedores:

Proveedor	P/S o Información	Comentario
Empresa privada	Página web y Equipos de computación	Necesitamos formalizar nuestra oficina
Empresa privada y pública	Propaganda en nuestra página web	Se pueden lograr clientes
Empresa Extranjeras	Software, Información	Necesitaremos actualizarnos continuamente
Empresa Privada extranjera	Software, Información, Certificaciones	Necesitaremos alianzas en el marco de beneficios mutuos.

Tabla 3.2.- Nuestros proveedores

Competidores entrantes

Siempre existirá la amenaza de nuevos competidores que ingresan al mercado y traen consigo nuevas tecnologías, ideas innovadoras y gran capital, un ejemplo es la empresa TATA la cual ya está radicada aquí y tiene un contrato millonario con el banco del Pichincha y sabemos que tienen tecnología como para ser un fuerte competidor. Como se mencionó anteriormente las compañías auditoras contables actualmente tienden a brindar el servicio de auditoría de sistemas.

PROVINCIA	TOTAL CIU REV.3	Agricultura ,Ganadería ,Caza y Silvicultur	Pesca	Explotación de Minas y Canteras	Industrias Manufacturer as	Suministros de Electricidad, Gas y Agua	Construcción
COSTA	20.485	1.296	638	130	1.640	46	1.337
EL ORO	814	83	85	39	54	1	55
ESMERALDAS	155	11	1	5	11	2	13
GUAYAS	18.092	1.106	439	81	1.428	37	1.127
LOS RIOS	156	45	0	0	17	0	10
MANABI	1.065	42	94	3	111	5	119
SANTA ELENA	203	9	19	2	19	1	13
SIERRA	16.310	674	15	252	1.764	82	774
AZUAY	1.543	54	2	10	183	6	54
BOLIVAR	15	0	0	0	0	0	1
CAÑAR	121	6	1	0	5	2	4
CARCHI	62	5	0	0	1	1	0
COTOPAXI	209	41	0	1	22	1	3
CHIMBORAZO	166	8	0	0	15	1	15
IMBABURA	252	19	0	1	16	2	7
LOJA	285	9	0	10	24	7	62
PICHINCHA	12.895	487	11	229	1.388	55	595
TUNGURAHUA	480	14	0	0	81	5	13
SANTO DOMINGO DE LOS TSACHILAS	282	31	1	1	29	2	20
ORIENTE	256	5	0	7	7	3	42
MORONA SANTIAGO	41	0	0	0	0	1	2
NAPO	22	1	0	0	1	0	2
PASTAZA	40	0	0	0	0	0	16
ZAMORA CHINCHIPE	32	1	0	1	2	1	4
SUCUMBIOS	56	3	0	2	1	1	10
ORELLANA	65	0	0	4	3	0	8
INSULAR O	84	0	0	1	2	1	1
GALAPAGOS	84	0	0	1	2	1	1
Total Provincia	37.135	1.975	653	390	3.413	132	2.154

Tabla 3.3.- Anuario del año 2007 de la Superintendencia de compañías

CLIENTES	%	Mercado
Total de compañías en Guayas		19.946
4 o más PCs	80	15.957
Interesados en seguridad inform	40	6,383
interesados sin servicio	70	4.468
Potenciales anuales	5	223

Tabla 3.4.- Segmento 1 del mercado

CLIENTES	%	Mercado
Total de compañías en Guayas		19.946
3 o menos PCs	20	3.989
Interesados en seguridad inform	25	997
interesados sin servicio	50	499
Potenciales anuales	5	25

Tabla 3.5.- Segmento 2 del mercado

Del mercado global hay un 20% de compañías que cuentan con menos de 4 PCs las cuales serían el segmento 2 del mercado como lo indica la tabla 3.4. Este segmento del mercado es menos interesado en seguridad informática (25%) resultando 997 compañías de las cuales un 50% estarían interesadas en nuestros servicios pero nuestro objetivo es atender al 5% de ellas, lo que indica que en el primer año planeamos tener como clientes a 25 compañías de este sector del mercado.

Recalcaremos que un gran porcentaje de nuestros ingresos serán generados a partir de los servicios de auditoría y del soporte a nuestro producto.

3.3 Plan de mercadeo

3.3.1.- Estrategia de precio

El costo de diseño o implementación de nuestro sistema tiene varios componentes:

- El costo del know-how, para el óptimo funcionamiento del mismo.
- El costo de los servicios de nuestros proveedores, Movistar y Skytel.
- El costo del cableado estructurado, lo que agrupa todo lo correspondiente a cada punto de red, como sería el conjunto de cables, canaletas, acometida física y demás gastos en que se incurre para llevar servicios de red a un equipo dentro de un edificio, este ítem puede ser eliminado por el cliente ya el puede encargarse la instalación, ya que la mayoría de las empresas cuentan con recursos dedicados a este tema.

A continuación se presenta los precios de Roca Technologies S.A.

Items	Observación	Valor
Computador	Opcional	500,00
Punto de red	Opcional	45,00
Softward	What´s Up	84,00
Base Celular	Opcional	100,00
Movistar	valor mensual a pagar	10,00
Skytel	Valor mensual a pagar	4,40
TOTAL	costos	743,40
	Precio Venta	1.170,00

Tabla 3.6.- precio del Producto

Items	Observación	Valor
Movilización personal	por 3 semanas	150,00
Herramientas informaticas		150,00
TOTAL		300,00
	Precio Venta	650,00

Tabla 3.7.- precios del servicio de Auditoria

Items	Observación	Valor
Movilización personal	2 ó 3 visitas	20,00
Herramientas informaticas		20,00
TOTAL	costos	40,00
	Precio Venta	120,00

Tabla 3.8.- precios del mantenimiento del producto

El sistema de pago por el producto será:

- El 60% del valor del contrato por adelantado.
- El 40% restante, contra entrega y luego de 15 días de prueba del servicio.

3.3.2.- Estrategia y tácticas de venta

Con la contratación de dos agentes de ventas se realizarán visitas a clientes potenciales para dar a conocer el P/S y el valor agregado que este ofrece. Como arma estratégica se realizarán demostraciones de posibles ataques a la red y se demostrarán sus efectos. Durante la venta se enfatizará en las ventajas competitivas que la empresa adquirirá al tener una red de datos protegida por un sistema de detección de intrusos.

Se realizará un mayor esfuerzo en las PyMes, será una forma de penetrar en el mercado, tratando de generar rentabilidad inmediata y un buen nombre entre los posibles clientes.

Una herramienta que nos ayudara a ganar prestigio es presentar a la empresa que nos sirvió de prototipo como referencia de nuestros servicios.

Para identificar los clientes potenciales, se usará una base de datos proporcionada por la superintendencia de compañías, se participará en ferias de informáticas, y una larga lista de contactos de los emprendedores.

La fuerza de venta estará formada por dos vendedores y también participarán los dos socios fundadores, para lo cual se dedicarán al menos al inicio a tiempo completo a visitar a clientes y a actividades de mercadeo.

3.3.3.- Estrategia Promocional

Las estrategias básicas de promoción que se usarán son:

- Reparto de folleto a color que describa a la empresa y el portafolio de servicios que brinda, esto acompañado con un CD-ROM con un demo del sistema.

- Envío masivo de emails, algo muy de moda hoy en día.
- Presencia en ferias empresariales e informáticas dirigidas al mercado objetivo.
- Contacto directo con empresas que distribuyan equipos de cómputo a los clientes potenciales.
- Publicación de página Web de la empresa donde se pueda descargar demos del sistema.
- Publicación en las principales revistas de ciencias y diarios nacionales.

3.3.4.- Políticas de Servicio.

En adición a un servicio de calidad prestado en el plazo estipulado, ROCA TECHNOLOGIES S.A. ofrece a sus clientes las siguientes ventajas:

- Respuesta rápida a las dudas, consultas o problemas que se presenten en su sistema.
- Al instalar el sistema se dará una capacitación de dos días.
- Luego de instalado el sistema se dará un periodo de prueba de 15 días.
- Garantía en los equipos y dispositivos instalados, según los términos ofrecidos por los proveedores.
- Garantía de 6 meses al sistema implantado.
- Soporte las 24 horas al sistema.

CAPITULO 4

ANALISIS LEGAL, ADMINISTRATIVO Y SOCIAL

4.1.- Análisis legal

Nuestra empresa la vamos a conformar como sociedad anónima.

Sociedad Anónima, que se puede definir como una sociedad mercantil que puede ser constituida por uno o más socios, que aporten entre todos un capital mínimo de \$ 5,000 dividido en acciones nominativas, acumulables e indivisibles, y que no asumen personalmente las deudas. En nuestro caso somos dos socios que aportaremos el 50 por ciento de capital cada uno.

Sociedad anónima es la forma jurídica que mejor se adapta a las necesidades de nuestro emprendimiento.

Veamos a continuación cuáles son los pasos necesarios para formalizar o constituir legalmente nuestra empresa.

4.1.1.- Búsqueda y reserva del nombre de la empresa en los Registros Públicos

Debemos en primer lugar acudir a la Oficina de Registros Públicos, y verificar que no exista en el mercado un nombre (razón social) igual o similar al que le queremos poner a nuestra empresa que es ROCA TECHNOLOGIES S.A.

Al buscar los nombres existentes, debemos asegurarnos de que éstos no se parezcan ni suenen igual al que vamos a usar, debe haber un mínimo de 3 letras diferentes lo cual ya fue consultado en línea en la página web de la superintendencia de compañías.

The screenshot shows the website header with the logo and name 'SUPERINTENDENCIA DE COMPAÑÍAS'. A navigation menu includes 'Inicio', 'Sector Societario', 'Centro Mediación', 'Mercado Valores', 'Ley Transparencia', 'Enlaces', 'Mapa del Sitio', and 'NITF'. The breadcrumb trail is 'www.supercias.gov.ec / Sector Societario / Consultas en Línea / Nombres Aproximados'. The main content area contains a search instruction: 'PARA BUSCAR LOS NOMBRES DE COMPAÑÍAS APROXIMADOS, USTED DEBE INGRESAR UNA PALABRA PECULIAR. POR EJEMPLO: LA COMPAÑÍA "ACERÍA DEL ECUADOR CA ADELCA" TIENE UNA PALABRA DISTINTIVA O PECULIAR QUE ES: ADELCA. LAS DEMÁS PALABRAS DENTRO DE ESTE NOMBRE SON DE CARÁCTER GENERAL. SI UD. INGRESA UNA PALABRA GENERAL, LA CONSULTA NO SERÁ ÚTIL, POR LO TANTO, ES INDISPENSABLE QUE INGRESE UNA PALABRA PECULIAR.' To the right, there is a label 'NOMBRE:' followed by a text input field containing 'ROCA TECHNOLOGIES' and a 'CONSULTAR' button.

Fig. 4.1.- Pantalla de búsqueda de nombres de compañías existentes

The screenshot shows the same website header and navigation menu as Fig. 4.1. The breadcrumb trail is 'www.supercias.gov.ec / Sector Societario / Consultas en líneas / Nombres Aproximados'. The main content area displays the message: 'No se han encontrado nombres de compañías conformados por palabras aproximadas a aquella que Ud. ingreso para realizar esta consulta.'

Fig. 4.2.- Pantalla no encuentra resultados para la búsqueda realizada

Una vez realizada la búsqueda y confirmado de que no existen nombres iguales o similares al que vamos a usar, debemos reservar nuestra razón social para que otra empresa no pueda inscribirse con ese nombre, siendo efectiva la reserva por un plazo de 30 días.

4.1.2.- Elaboración de la minuta

La minuta es un documento previo en el cual los miembros de sociedad manifiestan su voluntad de constituir la empresa, y en donde se señalan todos los acuerdos respectivos.

La minuta consta del pacto social y los estatutos, además de los insertos que se puedan adjuntar a ésta.

Los elementos fundamentales de una minuta son:

- los generales de ley de cada socio: sus datos personales, nombres, edad, documentos de identificación, etc.
- giro de la sociedad.
- tipo de sociedad: por ejemplo, S.R.L, S.A, etc.
- tiempo de duración de la sociedad: si es plazo fijo o indeterminado.
- cuándo se van a empezar las actividades comerciales.
- dónde va a funcionar la sociedad (domicilio comercial).
- cuál es la denominación o razón social de la sociedad.
- dónde van a funcionar las agencias o sucursales, si es que las hubieran.
- quién va a administrar o representar a la sociedad.
- los aportes de cada socio. Los cuales pueden ser:
 - *bienes dinerarios*: dinero y sus medios sustitutos tales como cheques, pagarés, letras de cambios, etc.
 - *bienes no dinerarios*: inmuebles o muebles tales como escritorios, sillas, etc.
- otros acuerdos que establezcan los socios.
- el capital social o patrimonio social (aporte de los socios).

Es recomendable elaborar la minuta con la ayuda de un abogado de confianza.

4.1.3.- Elevar la minuta a escritura pública

Consiste en acudir a una notaría y llevarle la minuta a un notario público para que la revise y la eleve a Escritura Pública.

Por lo general los documentos que debemos llevar junto con la minuta son:

- minuta de constitución.
- constancia o comprobante de depósito del capital aportado en una cuenta bancaria a nombre de la empresa.
- inventario detallado y valorizado de los bienes no dinerarios.
- certificado de Búsqueda Mercantil emitido por la Oficina de Registros Públicos de la inexistencia de una misma o similar razón social.

Una vez elevada la minuta, no se puede cambiar. Al final, se genera la Escritura Pública, Testimonio de Sociedad o Constitución Social, que es el documento que da fe de que la minuta es legal. Ésta debe ser firmada y sellada por el notario.

4.1.4.- Elevar la escritura pública en los Registros Público

Una vez que hemos obtenido la Escritura Pública, debemos llevarla a los Registros Públicos, en donde se realizarán los trámites necesarios para inscribir la empresa en los Registros Públicos.

La Persona Jurídica existe a partir de este paso, es decir, a partir de su inscripción en los Registros Públicos.

4.1.5.- Obtención del número de RUC

El RUC (Registro Único de Contribuyentes) es lo que identifica a una persona o a la empresa ante la Superintendencia de Compañías y Servicio de Rentas Internas para el pago de los impuestos.

Toda persona natural o jurídica está obligada a inscribirse en el RUC, de lo contrario serán sancionadas de acuerdo con el Código Tributario, igual que los inscritos en el RUC que no presenten la declaración.

Para obtenerlo debemos acudir al SRI, llenar un formulario de justificación, y esperar notificación.

4.1.6.- Elegir régimen tributario

En la misma SRI, a la vez que tramitamos la obtención de nuestro RUC, debemos determinar a cuál régimen tributario nos vamos a acoger para el pago de los impuestos, ya sea al Régimen Simplificado, al Régimen Especial de Impuesto a la Renta (RER), o al Régimen General.

Una vez que contamos con nuestro número de RUC, y elegido el régimen tributario al cual acogernos, podemos imprimir los comprobantes de pago (boleta y/o factura) que vamos a utilizar.

4.1.7.- Comprar y legalizar libros contables

En este paso compramos los libros contables necesarios dependiendo del régimen tributario al cual nos hayamos acogido; y posteriormente, acudimos a una notaria para que sean legalizados por un notario público.

4.1.8.- Legalizar el Libro de Planillas en el Ministerio de Trabajo (si fuera el caso)

Según la ley, todos los trabajadores de una empresa, no importa las horas que trabajen, deben estar en planilla (lo que implica recibir beneficios tales como gratificaciones, compensación por tiempo de servicio, etc.).

Para este paso, debemos acudir al ministerio de Trabajo, en donde se legalizarán las planillas.

4.1.9.- Inscribir a los trabajadores en el I.E.S.S.

Igualmente debemos registrar a los trabajadores en las oficinas de **I.E.S.S.** para que puedan acceder a sus servicios.

Los trámites se realizan en las oficinas de **I.E.S.S.** correspondiente a la jurisdicción.

Por lo general, los documentos a presentar son:

- Fotocopia del RUC.
- Planillas en blanco legalizadas.
- Fotocopia del DNI del representante.
- Formulario llenado en la oficina del **I.E.S.S.** para la inscripción de los trabajadores.

4.1.10.- Solicitud de licencia municipal

Consiste en acudir a la municipalidad del distrito en donde va a estar ubicado el negocio, y tramitar la obtención de la licencia de funcionamiento.

Por lo general, los documentos a presentar son:

- Fotocopia del RUC.
- Certificado de Zonificación (zona industrial, zona comercial, zona residencial, etc.).
- Croquis de la ubicación de la empresa.
- Copia de contrato de alquiler o título de propiedad.
- Fotocopia de la escritura pública.
- Recibos de pago por derecho por licencia.
- Formulario de solicitud.

Como dato adicional queremos señalar que en la actualidad existen centros o instituciones que nos pueden ayudar a realizar todos los pasos descritos anteriormente para constituir nuestra empresa, a un mínimo costo y en un corto periodo de tiempo.

4.2.- Equipo emprendedor

Nuestro grupo emprendedor está conformado por profesionales politécnicos, gente preparada y que ha tenido vasta experiencia en este campo, así mismo nuestros técnicos están motivados con este emprendimiento, y a la vez, están preparados para cualquier reto que se le pudiera presentar, a continuación damos un breve resumen de los socios emprendedores:

Dos Ingenieros Eléctricos que en este caso, serían a la vez los socios capitalistas cuyos nombres son:

- Christian Carranza Hidalgo
- Soni Rojas Quintero

Christian Carranza es un emprendedor que tiene bastante experiencia en finanzas y Marketing, con el papa tiene una empresa en las islas Galápagos por más de 12 años, la actividad principal de esta empresa es la comercial, tiene además experiencia en el sector financiero, cortes de cuenta, cierre de caja y otras actividades más, cabe recalcar que además de esto, ha desempeñado trabajos como técnico encargado en el área de sistemas por lo cual está empeñado en construir esta empresa

Soni Rojas tiene una experiencia laboral de 6 años en empresas multinacionales de telecomunicaciones dando servicios de tecnología de punta a empresas locales, con esta experiencia obtenida y su capacidad investigativa es capaz de evaluar y aportar al desarrollo de la infraestructura tecnológica de nuestros clientes. Cuenta con experiencia en el manejo de activos y recursos humanos teniendo a su cargo hasta 120 personas.

4.3.- Análisis administrativo

Roca Technologies S.A. se constituirá según el régimen de sociedad anónima. La sociedad está compuesta por dos socios fundadores, cuyos nombres son: Soni Rojas y Christian Carranza, ambos estudiantes egresados de la ESPOL, en calidad de socios fundadores.

Cada socio aportará con el 50% del capital inicial y estarán vinculados laboralmente a la empresa, son gente preparada de la ESPOL y como lo mencionamos anteriormente han tenido bastante experiencia, el resto del personal de la empresa no tendrá ninguna participación en lo que se refiere a las acciones de las empresa, solamente los socios emprendedores tendrán participación.

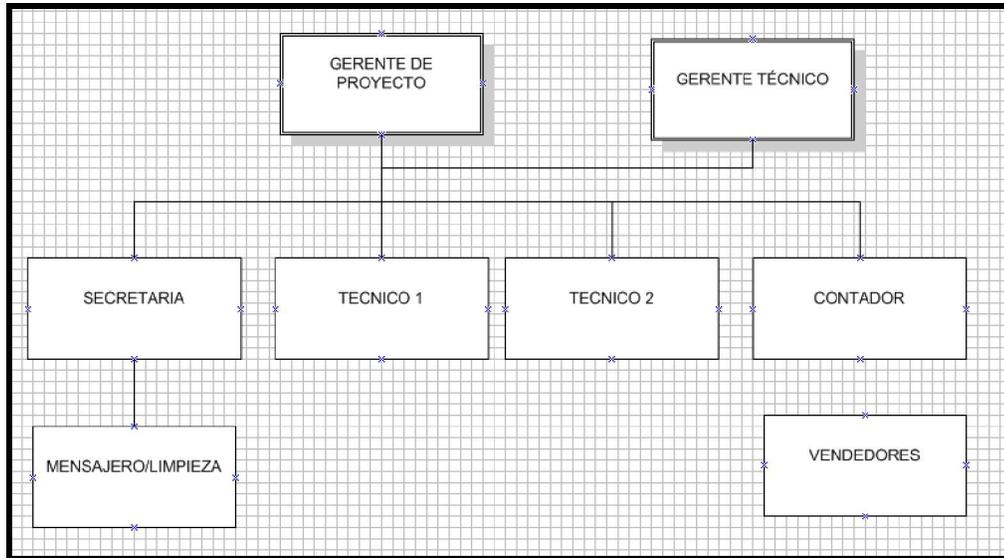


Figura 4.3.- Organigrama de ROCA TECHNOLOGIES S.A.

Los dos socios fundadores ocuparan el cargo de Gerente Técnico y Gerente de Proyecto respectivamente.

Se contratará una secretaria y un Contador Público que sería el encargado de llevar la contabilidad de la compañía. A su vez se necesitaría la colaboración de dos recursos que hagan las funciones de técnicos de mantenimiento correctivo y preventivo de nuestro producto y al mismo tiempo colaborarían en instalar el producto donde el cliente.

Por último también necesitaremos un conserje que será el encargado de la limpieza de la compañía y a su vez se encargue de la mensajería.

Es decir que este equipo de emprendedores estaría conformado por siete personas que serán las encargadas de sacar esta empresa adelante.

4.4.- Análisis Social

En las economías capitalistas de mercado los recursos financieros privados se mueven rápidamente, buscando siempre la MÁXIMA RENTABILIDAD A CORTO PLAZO.

Por ello, todos los esfuerzos que se han realizado hasta ahora para promover actitudes predominantemente éticas en las empresas han tenido un éxito muy limitado, pues los mercados sancionan con rapidez y dureza las iniciativas éticas de una empresa cuando éstas repercuten negativamente sobre sus resultados.

No obstante, en los últimos años se están haciendo esfuerzos por incorporar algunos indicadores éticos en los criterios de gestión empresarial, promoviendo la llamada **RESPONSABILIDAD SOCIAL CORPORATIVA (RSC)**. Se dice que una empresa ejerce su responsabilidad social cuando atiende a las expectativas sobre su comportamiento que tienen los diferentes **GRUPOS DE INTERÉS** (empleados, socios, clientes, comunidades locales, medio ambiente, proveedores, etc.) que pueden verse afectados por su actividad, con el propósito último de **CONTRIBUIR A UN DESARROLLO SOCIAL Y AMBIENTALMENTE SOSTENIBLE Y ECONÓMICAMENTE VIABLE**.

La RSC entraña: (i) el compromiso formal de adoptar políticas éticas, teniendo en consideración tanto el ámbito económico como el social y el medioambiental; (ii) la transparencia informativa sobre los resultados alcanzados en esos ámbitos; y (iii) el sometimiento voluntario a una evaluación externa de esos resultados.

El enfoque RSC es un nuevo modelo de gestión de las externalidades empresariales en lo económico, social y medioambiental, que busca el compromiso de los consumidores y los inversores para que, mediante la presión que suponen sus decisiones de gasto e inversión, obliguen a las empresas a adoptar paulatinamente criterios éticos. La atención pública sobre los impactos sociales y medioambientales de las empresas ha adquirido carácter universal desde los años ochenta, con casos como los de Bophal y Exxon Valdez, y, más recientemente, el de Nike y la fabricación de balones en Indonesia, el de

Shell y su connivencia con el régimen dictatorial de Nigeria, y el de Monsanto y la producción de organismos transgénicos.

Para cumplir con lo estipulado por la RSC queremos recalcar que nuestro emprendimiento sería el sostén económico de 7 familias, a futuro este número crecerá pondremos todo nuestro esfuerzo por que sea a corto plazo.

La piratería de software es un problema que afecta gravemente a todos los países de Latinoamérica y del mundo, uno de los principales objetivos de nuestro emprendimiento es combatir este problema mundial.

Por todos es conocido que muchas empresas luego de dar de baja sus activos de sistemas recurren a botar a la basura equipos como monitores, CPUs, teclados y muchos otros equipos varios (en una empresa experimente como llenaron un volquete con estos), equipos que son una fuente importante de contaminación ambiental.

Como asesores en auditoria de sistemas les daremos a nuestros clientes mejores opciones, una de ellas es cómo recuperar ciertos equipos y donarlos a fundaciones o escuelas, otra opción es recurrir a empresas que tienen formas especializadas de desechar estos equipos. Ese sería el aporte económico, social y ambiental de nuestro emprendimiento.

CAPITULO 5

ANALISIS ECONOMICO

Este análisis identifica las necesidades de inversión, los ingresos, los costos, los gastos, la utilidad, los puntos de equilibrio y determina la posibilidad de que al vender el producto al precio establecido, el negocio deje un excedente adecuado, una ganancia razonable.

Aunque se afirma que estamos en la era del conocimiento y que el conocimiento es más importante que el capital, sigue siendo fundamental el contar con recursos económicos para iniciar un negocio, una microempresa. Un emprendedor debe ser capaz de conseguir los recursos adquiridos para iniciar el emprendimiento, es su primer desafío.

Muchas veces es difícil conseguirlo, pero debemos probar las capacidades que tenemos para conseguir el capital.

5.1.- Estructura accionarial y propuesta de inversión

El emprendimiento requiere una inversión de \$ 35000 los cuales serán aportados en un porcentaje de 50 y 50% por el grupo emprendedor, esto con el propósito de no incurrir en obligaciones financieras.

Nuestro aporte económico sumado a nuestro aporte en conocimiento equivale al 100 % de las acciones de la empresa, pero estamos dispuestos a vender el 20% de las acciones.

A continuación presentamos las proyecciones y presupuestos del emprendimiento

5.2.- Inversión de activos fijos

El cuadro # 4 del Anexo A presenta en detalle los requerimientos de inversión en activos fijos necesarios para operación del negocio, como son los equipos de oficina tales como: computadoras, impresoras, UPS, así también como muebles y otros enseres, cabe recalcar que todos estos equipos se adquirirán de contado.

Se necesita un vehículo que será utilizado para movilización de gerencia durante visitas a clientes y movilización de los técnicos.

Por ser una empresa de base tecnológica se necesitará comprar software para ser usado en la empresa y también como parte del producto a vender por la empresa.

5.3.- Inversión de capital de trabajo

Los cuadros # 11 y # 12 recogen toda la información de la inversión necesaria para la operación del negocio como arriendo, servicios públicos, seguro, impuestos, servicios básicos, depreciación y amortización.

De igual forma se detallan los gastos correspondientes a publicidad, transporte, suministros de oficina.

(Ver hoja de Excel, cuadro # 11 y # 12 del Anexo A)

5.4.- Presupuesto de ingresos

El cuadro # 5 del Anexo A recoge la información detallada de las ventas clasificadas por los productos que comercializamos que sería en este caso el “Sistema de Detección de Intrusos” y los servicios que ofrecemos, que son: Auditoría de Sistemas y

Mantenimiento del producto (SDI). Igualmente indica los efectos tributarios (IVA y retención en la fuente, RF) y determina los procesos de recuperación de cartera, ingresos efectivos y cuentas por cobrar en cada uno de los períodos considerados.

El primer año se ha elaborado en forma mensual para poder identificar mejor el desarrollo del emprendimiento. Se han incluido para los años 2 y 3 los ajustes debidos a fenómenos inflacionarios (3% y 3.5%) respectivamente.

El cuadro detalla en número de ventas que necesitamos realizar al mes para que nuestra empresa sea un éxito, esto sería 20 clientes para el producto y 12 clientes para los dos servicios a ofrecer.

(Ver hoja de Excel, cuadro # 5 de Anexo A)

5.5.- Presupuesto de materias primas, servicios e insumos

El cuadro # 2 del Anexo A presenta las materias primas, los componentes y gastos requeridos para la construcción de un ejemplar del producto que estamos comercializando. En el mismo cuadro se indica el valor cobrar por el servicio de Auditoría de Sistemas que es de \$650 y el valor a cobrar por el servicio de mantenimiento correctivo o preventivo del producto vendido.

(Ver hoja en Excel, cuadro # 2 Anexo A)

5.6.- Presupuesto de personal

ROCA TECNOLOGIES tendrá en su nómina a 9 personas: los dos socios que cumplen con las funciones de Gerente de Proyecto y Gerente Técnico, tendrán un sueldo mensual de \$ 1,000 cada uno, dos Vendedores que tendrán un sueldo de \$ 600 cada uno, estos

serán los encargados de ofrecer nuestro producto/servicio a las empresas, dos Técnicos con un salario mensual de \$ 300 cada uno, un Contador que tendrá un sueldo de \$ 300, una Secretaria que tendrá un sueldo de \$ 250, y por último tendremos la colaboración de un conserje que tendrá un salario de \$ 200, este a su vez cumplirá con las labores de mensajería y limpieza de la empresa

Las prestaciones sociales y otros aportes legales ascienden a 22%. Algunas de ellas se pagan en forma mensual, otras semestralmente y otras anualmente. El cuadro # 9 del Anexo A muestra los detalles de los gastos de personal, también se detallan las obligaciones con el IESS., y los incrementos debido a la inflación.

(Ver hoja de Excel, cuadro # 9 Anexo A)

5.7.- Análisis de costos

El cuadro # 8 del Anexo A nos presenta la separación, año por año de los costos fijos y los costos variables, además nos muestra el costo total anual.

Aunque cada producto y servicio tiene una estructura de precios y costos diferentes, se ha calculado el precio de venta unitario y el costo variable unitario de una “venta” promedio (representativa de los Productos y Servicios que ofrecemos), dividiendo los valores totales por el número de “ventas” de cada año y con estos resultados se ha calculado el punto de equilibrio contable para cada año.

Se observa que desde el segundo año, se está por encima del punto de equilibrio contable, es decir, que hay utilidades desde ese momento.

(Ver hoja de Excel, cuadro # 8 Anexo A)

CAPITULO 6

ANALISIS FINANCIERO

El análisis financiero es una técnica de evaluación del comportamiento operativo del emprendimiento. Diagnóstico de la situación actual y predicción de eventos futuros y que, en consecuencia se orienta hacia la obtención de objetivos propiamente definidos.

El análisis financiero se lo realiza utilizando extractos financieros, que son los documentos esenciales de todo negocio. Los ejecutivos los utilizan para valorar el desempeño e identificar áreas en la que es requerida la intervención directiva. Los accionistas los utilizan para saber lo bien que se está dirigiendo su capital. Los inversores externos los utilizan para identificar oportunidades, y los prestamistas y proveedores los examinan rutinariamente para determinar la solvencia de las empresas con las que tratan.

Los extractos financieros esenciales que nos permiten realizar un análisis financiero son:

- Ü El flujo de caja
- Ü El estado de resultados (los ingresos & egresos)
- Ü El balance

6.1.- Flujo de caja

Es la herramienta que permite determinar las necesidades reales de capital en los distintos momentos de desarrollo del emprendimiento. Aquel compara los ingresos efectivamente recibidos y los egresos efectivamente pagados. Con base en el flujo de caja puede determinarse los momentos en los cuales los aportes de los promotores, los

socios inversionistas y los préstamos de inversores son absolutamente necesarios para mantener una caja final, al menos igual al colchón de efectivo.

El cuadro # 14 presenta el flujo de caja de nuestro emprendimiento.

(Ver hoja de Excel, cuadro # 14 Anexo B)

6.2.- Estado de Resultados

El cuadro “estado de resultados” o también llamado los “ingresos” indica los resultados de las operaciones durante un período específico. Indica si el emprendimiento está obteniendo beneficios, esto quiere decir, si tiene ingresos netos positivos o negativos, o sea “ganancias netas”. Por esto, los “ingresos” son referidos a veces como “estado de resultados” o como “pérdidas y ganancias”. Muestra la rentabilidad de una empresa al final de un tiempo determinado.

El contenido de este cuadro se puede representar por la ecuación:

Ingresos – Gastos = Ingresos netos (o pérdidas netas)

El cuadro # 15 del Anexo B presenta el estado de resultados de nuestro emprendimiento durante los tres años en que se han hecho proyecciones.

(Ver hoja de Excel, cuadro # 15 Anexo B)

6.3.- Balance General

Todas las empresas preparan sus balances, ya sea mensual, trimestral o al final del año fiscal, para ver como se encuentran financieramente en un momento determinado, de igual manera nosotros tendríamos que hacer un balance cada cierto tiempo, en nuestro

caso lo haremos de forma semestral, así de esta manera sabremos si nuestra empresa, está alcanzando las metas y objetivos que en un principio nos habíamos trazado.

El balance los activos controlados por el negocio y como esos activos son financiados mediante los fondos de los acreedores (obligaciones), con el capital de los emprendedores o socios, o con ambos.

Un balance refleja la siguiente ecuación básica de contabilidad:

$$\text{Activos} = \text{Obligaciones} + \text{Valor Patrimonial}$$

En el cuadro # 16 se muestra el balance general, durante 3 años de proyección.

(Ver hoja de Excel, cuadro # 16 Anexo B)

En el cuadro # 17 del Anexo B nos muestra los flujos de caja neto en los primeros tres años de operación, en el cual se aprecia una Tasa Interna de Retorno de 203,695% lo cual que el proyecto es un negocio con rentabilidad aceptable. En el mismo cuadro se indica el Valor Actual Neto que representa los flujos de caja de los tres primeros años de operación.

El cuadro # 17 indica el Periodo Pago Descontado de 1,4 lo que representa que la inversión del negocio se recupera en 1 año con 3 meses.

(Ver hoja de Excel, cuadro # 17 del anexo B)

CAPITULO 7

RIESGOS Y EVALUACION DEL EMPRENDIMIENTO

En este capítulo se analiza los efectos y que cambios potenciales, en las variables básicas del emprendimiento, pueden generar dificultades.

Los riesgos básicos y sus componentes son:

- Ü Riesgos de mercado: corresponden a cambios desfavorables en el sector, el surgimiento de mejores productos y la reducción de clientes. En nuestro caso uno de los principales problemas a tener es la piratería de software un problema global, otro problema sería el potencial incremento de la competencia.
- Ü Riesgos técnicos: se incluyen las fuentes de materia prima, obsolescencia de equipos y los problemas de mantenimiento. Como nuestro proyecto es basado en software y también hay equipos hardware que hacen lo mismo hay el riesgo de que estos últimos que abaraten precios y proliferen en el país. Otro riesgo técnico es que la tecnología usada por piratas informáticos avance tanto que pueden hacer nuestro producto obsoleto.
- Ü Riesgos económicos: corresponde al incremento en el costo de las materias primas y de la producción, además de una posible reducción en el precio del producto. En nuestro caso nuestros proveedores de software pueden incrementar el precio de la licencia del mismo. La competencia también es un riesgo económico ya que al ofrecer productos con precios inferiores nos puede afectar directa e indirectamente.

Ü Riesgos financieros: se incluyen el incremento del costo de capital, demoras en los aportes de los socios y los desembolsos de las entidades crediticias. En nuestro caso puede darse que a futuro la situación económica de la empresa demande inyección fuerte de capital y los socios podemos estar en situación de no poder reaccionar a corto plazo.

CONCLUSIONES Y RECOMENDACIONES

- 1) La seguridad en una red podríamos clasificarla de dos modos: activa y preventiva. La seguridad activa de un sistema consiste en protegerlo todo lo posible ante potenciales intentos de abuso del mismo. Por otro lado, la seguridad preventiva es aquella que implementamos en nuestro sistema para que nos informe si se presenta una incidencia de seguridad. Nuestro emprendimiento no pretende proteger la red al nivel de un Firewall, su función es alertar de que algo extraño está sucediendo en la red de la empresa para todos es conocido que el tiempo que este caído un enlace o un equipo por ejemplo un servidor en muchos casos representa pérdida de dinero. Un buen ejemplo de seguridad preventiva es un sistema de detección de intrusos.
- 2) La auditoria en informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática, de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de procedimientos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.
- 3) El objetivo final que tiene una auditoría de sistemas es dar recomendaciones a la alta gerencia para mejorar o lograr un adecuado control interno en ambientes de tecnología informática con el fin de lograr mayor eficiencia operacional y administrativa.

GLOSARIO

P/S	Producto o Servicio
SDI	Sistema de Detección de Intrusos
3GPP	Proyecto de tercera generación fase 1
3GPP2	Proyecto de tercera generación fase 2
ATM	Modo de transferencia asincrónica
AUC	Centro de autenticación
BER	Tasa de error de bit
BICC	Protocolo para control de llamada independiente
BSC	Controladora de estación base
BSS	Subsistema de estación base
BTS	Estación Base
CCITT	Comité Consultivo Internacional Telegráfico y Telefónico
CDMA	Acceso múltiple por división de código
CEPT	Conferencia Europea de Telecomunicaciones
DTX	Transmisión discontinua
DTM	Multaron discreto
EDGE	Tasas de datos realizadas para la evolución de GSM
EIR	Base de datos registradora de móviles
ETSI	Instituto Europeo de normas de telecomunicaciones

FDMA	Acceso múltiple por división de frecuencia FH Salto de frecuencia
GERAN	Red de acceso para red GSM con EDGE
GMSK	Modulación GMSK, Gaussian minimum shift keying
GPRS	General packet radio service
GSM	Sistema Global para comunicaciones móviles
H.248	Protocolo de Control para Multimedia Gateway
H.323	Protocolo para voz sobre IP
HLR	Registro local de móviles
HO	Traspaso de llamadas
HSCSD	High speed circuit-switched data
IETF	Internet engineering task force
ISDN	Red digital de servicios integrados
ITU	Unión Internacional de Telecomunicaciones.
IVR	Servicio de respuesta de voz interactivo
MAP	Protocolo MAP. Mobile application part
MEGACO	Protocolo de control para comunicación entre Medias gateway
MGCP	Protocolo de control entre Medias gateway
MGW	Multimedia gateway
MMS	Servicio de mensajes multimedia
MS	Estación Móvil
MSC	Centro de conmutación movil

MSS	Servidor de sistema multimedia	NSS	Subsistema de conmutación de red
O&M	Operación y mantenimiento		
OMC	Centro de operación y mantenimiento		
OSS	Sistema de soporte de operaciones		
PLMN	Public land mobile network		
PSTN	Public switched telephone network		
QoS	Calidad de servicio		
RNC	Radio network Controller		
SIGTRAN	Protocolo de señalización		
SIP	Protocolo de inicio de sesión		
SS7	Sistema de señalización número 7		
SVA	Servicio de valor agregado.		
TDD	Duplex por división de tiempo		
TDM	Multiplexación por división de tiempo		
UMTS	Universal mobile telecommunications system		
USSD	Unstructured supplementary service data		
UTRAN UMTS	terrestrial radio access network.		
VLR	Registro de móviles visitantes		
WAP	Protocolo de acceso inalámbrico		
WCDMA	Wideband acceso múltiple por división de código.		

BIBLIOGRAFIA

- (1) Chávez J, Protocolos de Red: Protocolo TCP/IP,
<http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml>,
mayo17/2008.
- (2) Lowgren J, Hacker and Hacking, <http://es.wikipedia.org/wiki/Hacker>;
mayo25/2009.
- (3) Cobos T, Avances en seguridad informática,
<http://www.universia.net.co/tesisdegrado/avances-en-seguridadinformatica>,
mayo27/2009.
- (4) R-Beter, Tipos de Ataque-Seguridad informática básica, <http://foro.el-hacker.com/index.php/topic,24573.msg88292.html#msg88292>, mayo25/2009.
- (5) Juskiewicz L, Manual FTP, <http://www.monografias.com/trabajos29/manual-ftp/manual-ftp.shtml>, mayo27/2009
- (6) Pereira J, Virus Computadoras y la Organización,
http://www.wikilearning.com/recursos_redes-wkk-760.htm, mayo27/2009.
- (7) Superintendencia de compañías, Anuarios Estadísticos,
http://www.supercias.gov.ec/paginas_htm/societario/anuarios.htm, mayo15/2009.
- (8) Romero A, Análisis social económico y financiero de la empresa,
http://www.educa.madrid.org/web/ies.camilojosecela.pozuelodealarcon/economia/apuntes2/2bac_tema13.pdf, junio3/2009
- (9) Superintendencia de compañías, consulta de compañías,
<http://www.supercias.gov.ec/web/publico/extranet/cgi/clientes>, julio13/2009
- (10) Crece Negocios, Constitución legal de empresas,
<http://www.crecenegocios.com/pasos-para-constituir-una-empresa>, julio14/2009.

ANEXO A ANALISIS ECONOMICO

cuadro # 0

	%		Clientes potenciales 1er ano	
			%	# clientes
Compañías en el Guayas		19.946,00		
Compañías con mas de 3 PCs	80%	15.956,80		
Compañías con hasta 3 PCs	20%	3.989,20		
segmento 1				
Interesados en Seguridad Informatica	40,00%	6.382,72		
Interesados sin servicio	70,00%	4.467,90	5,0%	223
		-		
segmento 2				
Interesados en Seguridad Informatica	25%	997,30		
Interesados sin servicio	50%	498,65	5%	25
Total				248

cuadro # 1

Proyeccion de clientes en el primer ano

Empresas con mas de 4 PCs

	Mercado	%	mercado
P/S	potencial		objetivo
Producto:			
Sistema de Deteccion de Intrusos	4.468	5%	223
			-
Servicios:			-
Auditoria de Sistemas	4.468	3%	134
Mantenimiento del SDI	4.468	3%	134

Empresas con 3 PCs o menos

Producto:			
Sistema de Deteccion de Intrusos	499	5%	25
			-
Servicios:			-
Auditoria de Sistemas	499	1%	5
Mantenimiento del SDI	499	1%	5

Sumando los 2 segmentos

Producto:			
Sistema de Deteccion de Intrusos			248
			-
			-
Servicios:			-
Auditoria de Sistemas			139
Mantenimiento del SDI			139
			-

cuadro # 2

Precios del producto y servicio

	Precio	
Producto:		
Sistema de Deteccion de Intrusos	\$ 1.170,00	
Servicios:		
Auditoria de Sistemas	\$ 650,00	
Mantenimiento del SDI	\$ 120,00	

Costos del Producto SDI

Items	Observación	Valor
Computador	Opcional	500,00
Punto de red	Opcional	45,00
Softward	What´s Up	84,00
Base Celular	Opcional	100,00
Movistar	valor mensual a pagar	10,00
Skytel	Valor mensual a pagar	4,40
TOTAL	costos	743,40
	Precio Venta	1.170,00

Costos del Servicio 1

Items	Observación	Valor
Movilización personal	por 3 semanas	150,00
Herramientas informaticas		150,00
TOTAL		300,00
	Precio Venta	650,00

Costos del Servicio 2

Items	Observación	Valor
Movilización personal	2 ó 3 visitas	20,00
Herramientas informaticas		20,00
TOTAL	costos	40,00
	Precio Venta	120,00

