**ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL**


**ESCUELA DE DISEÑO Y COMUNICACIÓN VISUAL**

**MATERIA DE GRADUACIÓN**

**PREVIO A LA OBTENCIÓN DEL TÍTULO DE PROGRAMADOR DE SISTEMAS Y ANALISTA DE SOPORTE DE MICROCOMPUTADORES**

**TEMA**

# PROYECTO DE INVESTIGACIÓN PARA LA PRODUCCIÓN Y COMERCIALIZACIÓN DE SERVIDORES DE SEGURIDAD PARA LA CIUDAD DE GUAYAQUIL

**AUTORES**

MERCHÁN VACA EDISSON
YÉPEZ MONTESINOS MARGARITA SUSANA
VILLALVA PALMA SOFÍA LETICIA

**DIRECTOR**

ING. EDGAR SALAS L.

**AÑO**

2009

# DEDICATORIA

Dedico este trabajo a mis a mis Abuelos Maternos y a toda mi familia, quienes siempre me apoyaron en los momentos difíciles y que gracias a ellos y a su esfuerzo he llegado a ser lo que soy.

***Edisson Andrés Merchán Vaca***

# DEDICATORIA

A DIOS que con su misericordia nos permite seguir adelante con nuestros objetivos trazados; y por ser nuestra luz en este largo camino.
A mi familia y a todas las personas que quiero, que de una u otra forma me han enseñado a ser una mejor persona.

***Susana Margarita Yépez Montesinos***

# DEDICATORIA

A mi madre, porque gracias a ella he aprendido a ser consciente de mis defectos, he crecido bajo su esencia y su forma de ver la vida, gracias por inculcar en mí astucia y perseverancia. Gracias a mi madre sé lo que es apreciar una amistad, también aprendí “a su manera” cómo demostrar gratitud y amor.

***Sofía Leticia Villalva Palma*.**

# AGRADECIMIENTO

A toda mi familia, especialmente a mis padres, por ser siempre mi apoyo constante y por brindarme la seguridad y confianza cuando lo necesité.

***Edisson Andrés Merchán Vaca***

# AGRADECIMIENTO

A mis amigas y amigos que siempre han estado junto a mí, son gran parte de mi corazón, gracias por caminar a mi lado y permitirme caminar a su lado, gracias por compartir tantas experiencias lindas.

***Margarita Susana Yépez Montesinos***

# AGRADECIMIENTO

Este trabajo va dedicado especialmente a Dios, a mi padre, a mi madre y a mis compañeros de estudios por haberme ayudado tanto en esta etapa de mi vida y por haber sido mi mejor guía técnica y espiritual.

***Sofía Leticia Villalva* Palma**

# DECLARACIÓN EXPRESA

La responsabilidad del contenido de este Trabajo Final de Graduación me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral.

(Reglamento de Graduación de Pregrado de la ESPOL).

# FIRMA DE LOS AUTORES DEL PROYECTO DE GRADUACIÓN

**Edisson Andrés Merchán Vaca**

**Margarita Susana Yépez Montesinos**

**Sofía Leticia Villalva Palma**

## FIRMA DEL DIRECTOR DEL PROYECTO DE GRADUACIÓN

**Lcdo. Washington Quintana**
**Delegado de la Directora**

**Ing. Edgar Salas Luzuriaga**
**Profesor de la Materia**

# INDICE GENERAL

**CAPÍTULO 4**



**CAPÍTULO 5**

# INDICE DE FIGURAS

**CAPÍTULO 2**

# INDICE DE GRAFICOS

**CAPÍTULO 3**

# INDICE DE TABLAS

**CAPÍTULO 2**



**CAPÍTULO 3**



**CAPÍTULO 4**


# CAPÍTULO 1

# GENERALIDADES

## 1.1 ANTECEDENTES

Internet, con el pasar de los años se ha convertido en una herramienta esencial para hacer negocios, ya sea en la promoción de productos o servicios, para realizar transacciones monetarias, o para mantenerse en contacto con clientes frecuentes o potenciales de una manera más personal, eficaz, interactiva y económica.

Todo lo mencionado anteriormente es posible gracias a que *Internet* es, fundamentalmente, una gran Red que interconecta a una enorme cantidad de computadores alrededor del mundo, facilitando el intercambio libre de información entre ellos; y es la aplicación de este mismo concepto, pero en menor escala, lo que dió origen a lo que hoy en día conocemos como *Redes de Computadores.*

Pero Internet también tiene su lado obscuro, ya que a lo largo de toda su extensión podemos encontrar gran variedad de peligros tales como los Hackers o los Virus. Los *Hackers* son personas con gran conocimiento técnico acerca del funcionamiento de las redes, y que gracias a su habilidad, son capaces de escabullirse sin ser detectados en computadores que se encuentren sin algún tipo de protección. Los *Virus* en cambio, son programas dañinos, por lo general creados por los mismos Hackers, que tienen la capacidad de hacer daño al computador en donde se encuentren hospedados.

Para combatir estas amenazas se crearon los *Programas Antivirus* los cuales no son otra cosa que programas especializados en detectar, prevenir y detener la presencia de comportamiento anormal en nuestro equipo, esta solución funcionó bien durante un tiempo, pero a medida que la naturaleza de los ataques tanto de intrusos como de los virus fue evolucionando, los antivirus perdieron mucha de su efectividad, lo cual llevó a la creación de programas complementarios que asistieran a los antivirus en su lucha, *Firewalls* y *Antispyware*.

Estos programas complementarios se encargan, cada uno de luchar contra un tipo de amenaza específica para así ofrecer un nivel más elevado de protección, ya que mientras los *Firewalls* se dedican de manera exclusiva a detectar y bloquear acceso y envío de información no autorizada desde y hacia nuestro equipo además de permitir el bloqueo de sitios web y programas de nuestra elección, y los *Antispywares* detectan programas que pudieren estar recolectando información personal de nuestro equipo sin nuestro conocimiento, y que debido a su naturaleza aparentemente benigna, muchas veces pasan sin ser detectados, los A*ntivirus* se encargan sólo de detectar, detener y eliminar programas dañinos.

La unión de los tres programas antes mencionados provee un nivel de protección bastante aceptable tanto para usuarios individuales como para los que forman parte de una red pequeña (de 2 a 4 computadores), pero a medida que el tamaño y complejidad

de la red aumenta, así también aumenta el peligro, ya que estos programas protegen efectivamente a cada computador de manera individual pero no así a la red en conjunto.

Para comprender mejor de lo que estamos hablando vamos a usar la siguiente analogía: Supongamos que alguien nos cuenta un secreto y que una tercera persona intenta averiguar cuál este secreto, si esta persona nos llegase preguntar por él, no se lo vamos a decir porque nosotros sabemos cómo guardarlo, esos son nuestro antivirus y firewall trabajando, pero si luego decidimos confiarle ese mismo secreto a una persona de confianza, ¿qué impide que la persona de antes lo escuche?, es en ese momento que necesitamos de un medio de protección adicional para cuidarnos de un ataque de ese tipo, y es ahí que entran en juego los *Servidores de Seguridad*.

Los *Servidores de Seguridad* cubren el déficit de protección que se presenta durante la comunicación de información en una red de computadores además de reducir el número de ataques que pudiere recibir cada computador integrante de la red, en otras palabras, un Servidor de Seguridad protege tanto a los computadores en conjunto como de manera individual, ofreciendo una capa de seguridad adicional al área informática de cualquier empresa.

## 1.2 JUSTIFICACIÓN

La razón de ser tanto del Internet como el de las Redes se puede resumir en dos palabras, *Compartir* y *Comunicar*, pero al igual que en la vida real, para poder hacer ambas cosas es necesario un cierto nivel de apertura con las personas con las que queramos compartir recursos y comunicar información.

En el ámbito computacional es lo mismo, para poder compartir recursos y comunicarnos con otros computadores sin importar cuán cerca o lejos estén del nuestro, es necesario bajar nuestras defensas, abrir una *Puerta de Enlace* desde y hacia nuestro computador tanto para enviar como para recibir información, pero muchas veces no tomamos en cuenta que al abrir dicha Puerta nos exponemos a que algún intruso pueda ingresar sin ser detectado a nuestro computador e inclusive interceptar la información que estemos enviando o recibiendo.

La protección de la Puerta de Enlace tanto de cada computador de manera individual como de la Red en conjunto es algo sumamente importante, ya que por ese medio un intruso hábil es capaz no sólo de robar información, sino también Internet. Por increíble que parezca el robo de internet es algo muy real, ya que mediante el simple ingreso de un programa especial a un computador, dicho intruso puede usar parte del *Ancho de Banda (velocidad con la que nos conectamos a Internet)* de su empresa para su uso personal sin que siquiera lo notemos, perjudicando así la productividad de su personal.

Mediante la implementación de nuestros Servidores de Seguridad en las áreas críticas de su empresa puede tener la seguridad de que ninguna Puerta de Enlace en su red quedará desprotegida, así podrá tener la seguridad de que nunca será víctima de robos informáticos por parte de intrusos, y no sólo eso, sino que también quedará ampliamente protegido contra virus informáticos, ya que nuestros Servidores son capaces de interceptar entre un 70% y 80% de los programas malignos que circulan por Internet, quitándole así una gran carga de encima a los Antivirus instalados en cada uno de los computadores eliminando prácticamente el riesgo de que sus equipos se contagien, haciendo así que los virus sean cosa del pasado.

Pero las amenazas no sólo pueden venir de fuera, sino también de dentro, ya que un empleado, ya sea por ignorancia o negligencia puede también consumir una gran cantidad del Ancho de Banda de la empresa de manera irresponsable, ya sea accediendo a sitios de videos de Internet o mediante el uso indiscriminado de programas de descarga de música o aplicaciones, y no sólo eso sino que también es posible que pueda estar perdiendo tiempo valioso de trabajo ingresando a sitios web no afines con el trabajo de su empresa.

Nuestros Servidores pueden evitar que eso vuelva a ocurrir, ya que, implementando un sistema inteligente de gestión, filtrado y distribución de Ancho de Banda, se asegura de

que el acceso tanto a sitios de videos o música, páginas que pudieren contener contenido no afín a su empresa y programas de descarga estén restringidos para su personal, además de lograr de que cada uno de ellos tenga siempre la misma cantidad de Ancho de Banda que los demás, impidiendo así que se produzcan embotellamientos en su red, de este modo se maximiza la productividad de cada uno de sus empleados y por ende, de la empresa.

Otra de las preocupaciones que los administradores de empresas tienen es con respecto al robo de información por parte de personal de la compañía, ya que uno de ellos podría por ejemplo, tomar listas de precios, proveedores o de clientes de la compañía para venderlo a la competencia, aunque esto suene como algo sacado de una película de espías o de la imaginación de algún paranoico, es algo que sucede, especialmente en empresas más grandes.

Mediante un servicio ofrecido de manera independiente, somos capaces de quitarle a la empresa esa preocupación de encima, ya que por medio de la instalación programas especiales de monitoreo en cada uno de los computadores de la red podemos reportar acciones sospechosas que cualquier miembro de su personal pudiere estar efectuando con el fin de prevenir y detener cualquier tipo de robo o desvío de información crítica para su empresa.

## 1.3 OBJETIVOS DEL PROYECTO

### 1.3.1 Objetivo General

Determinar la factibilidad económica y financiera de la implementación de Servidores de Seguridad como medida preventiva en contra de la infiltración tanto de intrusos como de programas malignos.

### 1.3.2 Objetivos Específicos

- **Determinar el conocimiento y características deseadas en la implementación de los Servidores de Seguridad por parte del consumidor final.**

  Mediante la aplicación de encuestas y casos de estudio de determinarán que características y necesidades los potenciales clientes tienen con respecto a la Seguridad Informática de sus empresas.

- **Establecer estrategias adecuadas para llegar a la mente de los consumidores.**

  Implementaremos estrategias adecuadas para promocionar a la empresa en la mayor cantidad de medios posibles, con el fin de dar a conocer nuestro producto y nuestra visión a nuestro mercado potencial.

- **Establecer el monto de la inversión necesaria.**

  Se realizará un estudio detallado para determinar cuál es el monto de inversión inicial que se requiere para poner a la empresa en marcha, para ello se detallarán los valores de los gastos requeridos para el funcionamiento de la empresa durante el primer año.

- **Obtener la rentabilidad ofrecida por el proyecto.**

  En este punto se planea determinar, a través de cálculos de retorno de inversión, si es posible, financieramente hablando, implementar la empresa y si se obtendrán o no ganancias, y si obtendrán, dentro de que periodo de tiempo se logrará ese objetivo.

- **Realizar un Prototipo Promocional y un plan de marketing.**

  A fin de demostrar a los clientes e inversionistas la fiabilidad del producto se planea especificar dentro del documento las especificaciones, el funcionamiento y las limitaciones de nuestro producto, mediante simulaciones efectuadas en un prototipo del producto final.


# CAPÍTULO 2

# ESTUDIO TÉCNICO

## 2.1 ANTECEDENTES

Uno de los problemas más comunes que se presentan al querer implementar cualquier tipo de solución de seguridad en una empresa, ya sea esta una solución simple, como por ejemplo Antivirus, Antispywares o Firewalls, o una solución más compleja como los Servidores de Seguridad, es la falta de compatibilidad con la plataforma informática presente actualmente en la empresa, esto es, tanto equipos como programas y redes de computadores presentes.

Esto se debe en gran parte a que toda solución de seguridad por naturaleza tiende a ser un tanto "paranoica", refiriéndonos con esto, a que tiende a tomar todo archivo almacenado, todo programa en ejecución, y toda conexión proveniente de cualquier red, como una potencial amenaza. Esto es algo, hasta cierto punto, deseable en cualquier solución de seguridad que se precie, pero, el problema surge cuando, debido a esta paranoia, se comienzan presentar fricciones y choques tanto con los programas como con las redes, al punto que, la solución adoptada, termina por convertirse más en un problema.

Para evitar esto, muchas de las antes ya mencionadas soluciones incluyen *Módulos de Aprendizaje*, los cuales no son otra cosa que una especie de programa de entrenamiento para la solución, mediante el cual, esta es capaz de aprender a distinguir cuales archivos, programas, y conexiones de red son amenazas para el equipo y cuáles no, previa aclaración por parte del usuario. Y he aquí su talón de Aquiles, ya que los ya mencionados Módulos trabajan bajo la suposición de que el usuario es capaz de identificar cuáles contenidos, tanto de su equipo, como de la red, son potenciales amenazas, lo cual es pocas veces posible, esto debido a que son pocos los usuarios que cuentan con el conocimiento necesario para hacerlo, y por esa causa, muchas veces terminan cometiendo el error de permitirle el paso al equipo a una aplicación dañina o denegarle el acceso a un archivo o programa necesario para su trabajo diario.

Todo lo mencionado anteriormente es necesario para aclarar un punto fundamental en la implementación de cualquier solución de seguridad informática, que siempre es necesario un estudio previo a la implementación de la solución, con el objetivo de que esta se adapte correctamente al entorno informático, tanto de redes y programas, en la cual se pretende implementarla, todo esto para evitar cometer errores que puedan, a la larga, ocasionar pérdidas importantes a la empresa.

## 2.2 INGENIERÍA DE LA PRODUCCIÓN

### 2.2.1 Proceso de Producción

El Proceso de Producción de un Servidor de Seguridad, refiriéndonos al ensamblaje y configuración básica del Sistema Operativo y del Firewall, no es tan complejo como pudiere parecer a simple vista, de hecho, un técnico bien entrenado puede ensamblar, configurar y realizar pruebas básicas de rendimiento y estabilidad de un Servidor en aproximadamente tres horas, esto gracias a que los parámetros básicos tanto de instalación como de configuración están claramente definidos y son en su mayor parte, estándar.

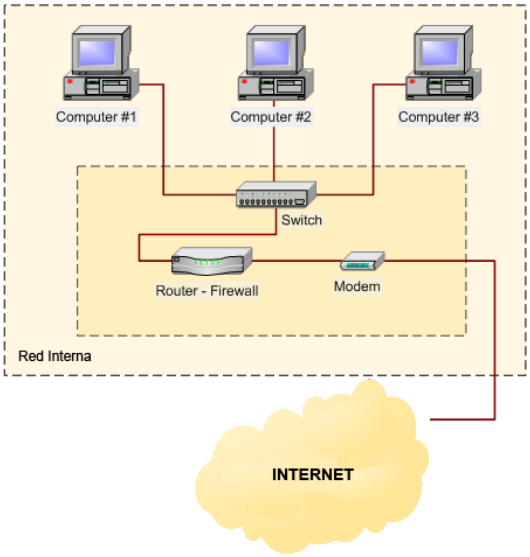


*Figura 2.1 : Esquema básico de una red*

Pero, como ya se explicó en el punto anterior, el implementar un Servidor de Seguridad en una empresa no es sólo cuestión de ir a un sitio, conectar el Servidor a la red, e irse; se requiere de un estudio previo de la infraestructura de red que posee la empresa: si esta es totalmente cableada, si es totalmente inalámbrica, o si es mixta (en parte cableada, en parte inalámbrica), si la empresa posee otros Servidores (de Datos, de Correo, etc.), en caso de tener varios departamentos, si estos utilizan una sola conexión global a internet o si cada departamento tiene su propia conexión de manera independiente, si el Internet es repartido a los computadores mediante Switches, Hubs, o Routers *(Figura 2-1)*, si existe algún problema de cualquier tipo en la red, como por ejemplo baja velocidad de conexión a Internet, lentitud en la transmisión de datos entre los equipos, o *Virus Persistentes* (los cuales son virus que a pesar de ser eliminados de uno o de todos los computadores, vuelven a aparecer al poco tiempo). Todos estos factores y otros más influyen mucho en la complejidad de la configuración final del Servidor y en la efectividad que este tenga al realizar su labor.

El estudio previo antes mencionado es necesario para la elaboración de las *Reglas* de funcionamiento del Servidor, estas Reglas son las que determinan el comportamiento del Servidor con respecto a la Red en el que este se desenvuelve, de tal modo que rara vez hay dos Servidores que compartan la misma configuración, ya que Redes y usuarios distintos, requieren de Reglas distintas.

Las Reglas entre otras cosas determinan que programas tienen acceso a la Red, esto se logra definiendo que *Puertos* (también llamados Puertas de Enlace) estarán abiertos para el uso de las aplicaciones, ya que cada aplicación instalada en cada computador necesita de uno o varios Puertos, distintos a los de otras aplicaciones, para conectarse a la Red o a Internet, por ello es muy importante abrir sólo los puertos absolutamente necesarios para evitar que algún intruso pueda ingresar sin ser detectado por algún Puerto que no esté siendo utilizado. Además de esto las reglas también determinan las aplicaciones, usuarios o equipos que pueden enviar o recibir información desde y/o hacia la Red Principal o desde Internet, de modo que si una aplicación, usuario o equipo que esté sólo autorizado para enviar información, de repente intente recibirla, verá sus intenciones bloqueadas por el Servidor de Seguridad.

Pero se debe tener mucho cuidado de no redundar al momento de implementar las Reglas, ya que esto puede provocar una carga innecesaria en los recursos del Servidor, lo cual a la larga puede provocar fallos en su funcionamiento, para evitar este problema, es necesario, *Optimizar y Organizar* tanto las Reglas como su orden de ejecución.

La *Optimización* consiste básicamente en denegar de manera predeterminada el acceso a todas las conexiones tanto entrantes como salientes (las conexiones a la Red entran y salen de cada computador por medio de las Puertas de Enlace o Puertos) de cada computador de manera individual, y luego abrir sólo los puertos que cada computador estrictamente requiera, lo que se pretende lograr con esto es que todas las aplicaciones que *todos los computadores tengan en común* (por ejemplo, Word, Antivirus, etc.) utilicen los mismos puertos que los de los demás computadores, y sólo abrir puertos nuevos para las aplicaciones que cada computador tenga de manera exclusiva (un empleado del área de diseño gráfico de una empresa, además de las aplicaciones básicas que todos los computadores poseen, tiene programas de uso exclusivo para su área, tales como Adobe Photoshop y Adobe Illustrator, los cuales usarán puertos dedicados sólo para ellos). Con la Optimización se evita al Servidor el tener que procesar una gran cantidad de puertos diferentes, muchos de los cuales están asignados a iguales aplicaciones pero en distintos computadores, ahorrando así recursos de memoria, ya que mientras menos Reglas haya y mientras menos complejas estas sean, mas rápido podrán ser procesadas, lo cual permite al Servidor ejecutar otras tareas, o agilizar las que ya se encuentren en ejecución.

El proceso de *Organización* se realiza luego de haber Optimizado las Reglas, ya que para organizarlas es necesario tener muy claro cuáles y que tan complejas son estas. Al

Organizar las Reglas en el Servidor, estas se deben programar en orden de complejidad, donde las menos complejas se ubican en los primeros puestos de ejecución, mientras que a las más complejas se las sitúa en las últimas posiciones, esto se hace con el fin de optimizar el tiempo de ejecución de las Reglas, ya que estas se ejecutan *estrictamente en el orden que se les asigne en el Servidor*, de modo que si algún computador realiza una petición al Servidor, este debe *ejecutar cada una de las reglas en la lista* hasta hallar la regla que coincida con la petición que le fué hecha. Entre las Reglas menos complejas se cuentan: la información de puerto de origen (número de identificación del puerto y del computador desde el cual surgió la información enviada a otro equipo o a Internet), definiciones de protocolo (qué protocolos de red tienen permitido el envío y recepción de información), y direcciones y horarios de protocolos de Internet (direcciones de Internet o de red accesadas o que estén recibiendo o enviando información y datos acerca de la hora, fecha y usuario que accesó a dicha dirección). Algunas de las reglas más complejas son: el tipo de contenido permitido (es un filtro que permite o niega el envío y recepción de información por parte de las aplicaciones), la lista de sitios web denegados de acceso, y la lista de usuarios permitida. Como se observa, las reglas menos complejas son las que se solicitan con mayor frecuencia, de ahí la conveniencia de colocarlas en las primeras posiciones, y la importancia de la Organización como un método para mejorar el rendimiento tanto del Servidor como de la Red misma.

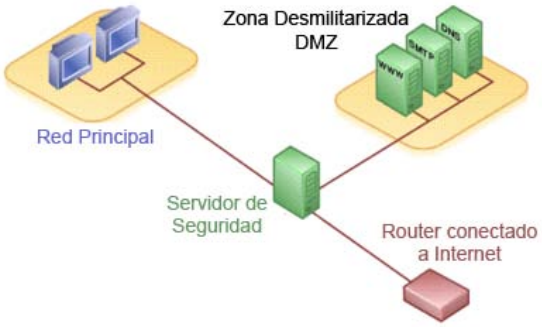


*Figura 2.2 : Esquema básico de una DMZ*

Otra consideración importante, en especial para empresas medianamente grandes o grandes es la implementación de una *Zona Desmilitarizada* o *DMZ (siglas para De-Militarized Zone) (Figura 2-2)*, la cual es una subred situada entre la Red Principal de la empresa e Internet, cabe destacar que esta subred puede ser tanto física (con computadores y/o servidores dentro de esta red) como lógica (creada de manera virtual en el Servidor de Seguridad). El objetivo de la Zona Desmilitarizada es el de proveer una capa adicional de protección a la Red Principal de la empresa colocando todos los servidores adicionales que la empresa posea en una subred separada de la Red Principal e impidiéndoles la comunicación directa con cualquier computador que se halle dentro de esta, de modo que todas las comunicaciones ente los servidores y la Red Principal son intermediadas de manera estricta por el Servidor de Seguridad. Los servidores se aíslan de la Red Principal a causa de que ellos son más propensos a recibir ataques de

fuentes externas, y en caso de que alguno de esos ataques tenga éxito, la Red Principal no se verá comprometida. Para que una DMZ se implemente de forma correcta se requiere de un conjunto de Reglas muy estrictas que regulen tanto la comunicación de los servidores con Internet, y en especial con la Red Principal, este puede llegar a ser un proceso un tanto complejo, pero asegura un incremento significativo en la protección de la Red Principal contra ataques externos.

De manera paralela al estudio inicial que se realiza para la elaboración de las Reglas se suele también ejecutar el proceso de *Endurecimiento* de los Computadores, lo cual no es otra cosa que el eliminar todas las posibles fallas y vulnerabilidades que cada equipo posea de manera individual, tanto en las aplicaciones que este posea como en su *Configuración de Red* (la Configuración de Red de cada equipo determina la manera en que este interactúa con los demás equipos en la Red), para ello se procede primero, a aislar completamente el equipo a tratar de la Red Principal de la empresa, luego se proceden a eliminar todos los virus, spyware y demás infecciones que este pudiere tener para después poder cerrar todos los agujeros de seguridad de las aplicaciones que el equipo posea, incluyendo el Sistema Operativo, mediante la instalación de actualizaciones y parches de seguridad, una vez concluido con esto, se procede a instalar programas Antivirus, Antispyware y de Firewall, y a configurarlos para que complementen el trabajo del Servidor de Seguridad. Una vez concluida esta labor con todos y cada uno de los equipos, ya es seguro volver a conectarlos a todos nuevamente a la Red.

## 2.2.2 Detalle del Proceso de Producción

### 2.2.2.1 Instalación del Sistema Operativo

*Figura 2.3 : Logo del Sistema Operativo pfSense*

Para la instalación del Sistema Operativo en el Servidor de Seguridad se utilizará la versión 1.2.2 de la distribución de BSD especializada en seguridad, pfSense *(Figura 2-3)*, la cual puede ser obtenida gratuitamente de la siguiente dirección :
*http://www.pfsense.org/index.php?option=com_content&task=view&id=43&Itemid=44*

La mayor parte del proceso de instalación es automatizado, por lo que no hay necesidad de configurar nada además de la ubicación donde deseamos instalar el Sistema Operativo, el formato y particiones del Disco Duro, y la dirección de red del Servidor.

#### 2.2.2.1.1 Configuración de la Ubicación de la Instalación, Formato y Particiones del Disco Duro


*Figura 2.4 : Consola de Configuración de pfSense*

Al insertar el Disco de Instalación de pfSense en el Servidor de Seguridad lo primero que se presentará en pantalla es la *Consola de Configuración (Figura 2-4)*, la cual nos permite entre otras cosas, ejecutar el proceso de Instalación del Sistema Operativo, realizar tareas pertinentes al Disco Duro, tales como *Dar Formato* (Preparar al Disco Duro o al Dispositivo de almacenamiento de nuestra elección para recibir información) y *Particionar* (Dividir el Disco Duro en varias partes con el objeto de organizarlo de una manera mas eficiente), y aplicar la configuración inicial de la Red Principal (LAN) e Internet (WAN).

Como paso inicial en la Consola de Configuración se debe escoger la *Opción 99 : Instalar pfSense en una Unidad de Disco Duro*.

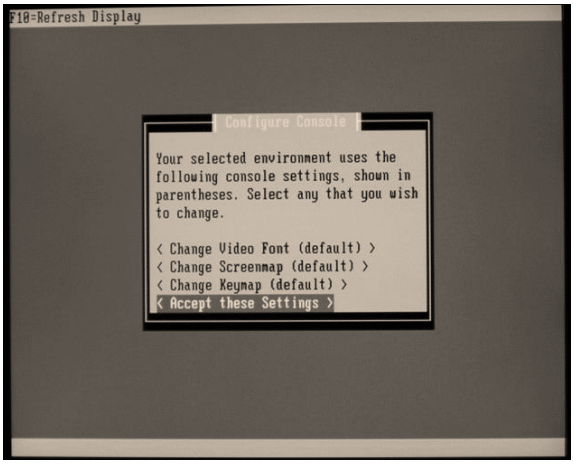


*Figura 2.5 : Configuración de la Consola de Instalación*

Luego de haber escogido la Opción 99, se presenta la siguiente pantalla, con la cual nos es posible configurar el aspecto gráfico de la *Consola de Instalación (Figura 2-5)*, la cual es el conjunto de pantallas que nos guiarán durante el proceso de Instalación, en nuestro caso no hay necesidad de realizar ningún cambio, por lo que se puede utilizar la opción por defecto : *Accept these Settings*.

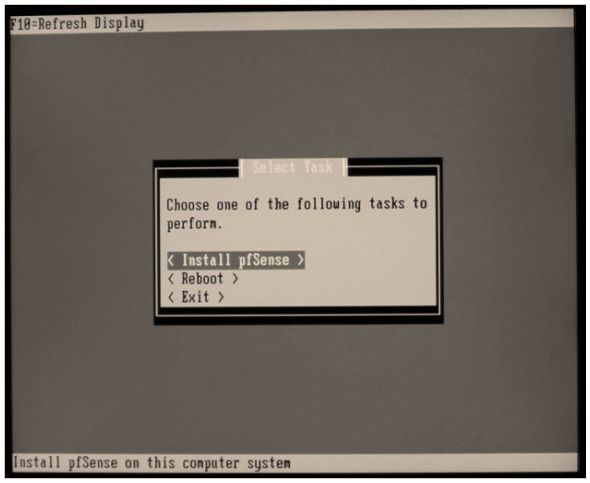


*Figura 2.6 : Inicio del Proceso de Instalación*

De manera seguida a la Configuración de la Consola, se nos presenta la pantalla de *Inicio del Proceso de Instalación (Figura 2-6)*, en la cual se nos presentan tres alternativas : Install pfSense (Instalar pfSense), Reboot (Reiniciar el Equipo), y Exit (Salir de la Instalación). Para poder proseguir, la opción a escoger es *Install pfSense (Instalar pfSense).*


*Figura 2.7 : Ubicación de la Instalación*

La siguiente panatalla que se nos presenta nos pide escoger la Ubicación en donde deseamos instalar el Sistema Operativo *(Figura 2-7)*, para lo cual debemos escoger la unidad de Disco Duro instalada en nuestro Servidor (por lo general es la única opción disponible).

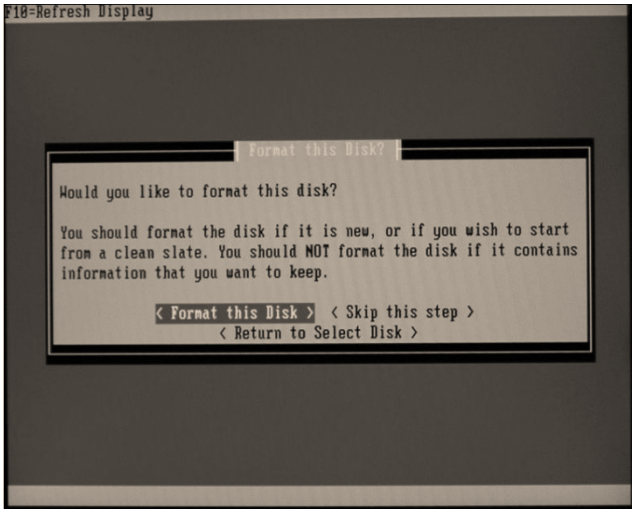


*Figura 2.8 : Formatear el Disco Duro*

A continuación se nos pregunta si deseamos Dar Formato al Disco Duro, y, ya que es necesario hacerlo para poder proseguir con la instalación del Sistema Operativo, escogemos la opción *Format this Disk (Formatear este disco) (Figura 2-8).*

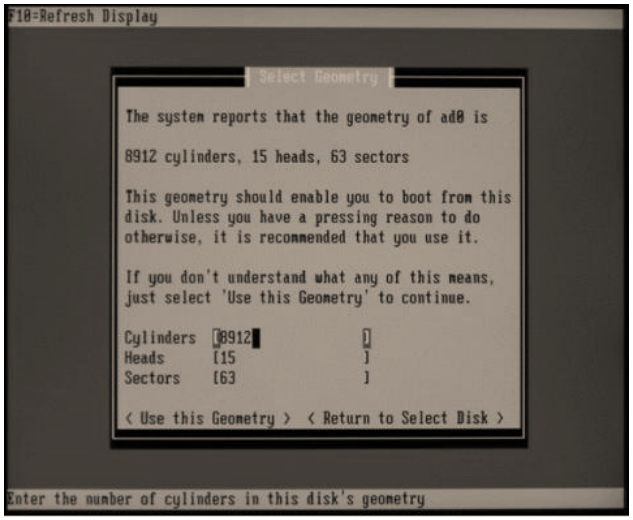


*Figura 2.9 : Geometría del Disco Duro*

En esta pantalla se nos consulta acerca de la *Geometría del Disco Duro* (este es el término utilizado para describir la forma en que el Disco Duro estructura la información que va a almacenar en su interior) *(Figura 2-9)*, como los parámetros de Geometría son propios para tipo de disco y vienen configurados de fábrica, no hace falta cambiarlos, por lo cual se debe escoger la opción *Use this Geometry (Utilice esta Geometría)*, con esto estamos indicando que deseamos que el programa de instalación utilice los valores por defecto (de fábrica) de Geometría del Disco.

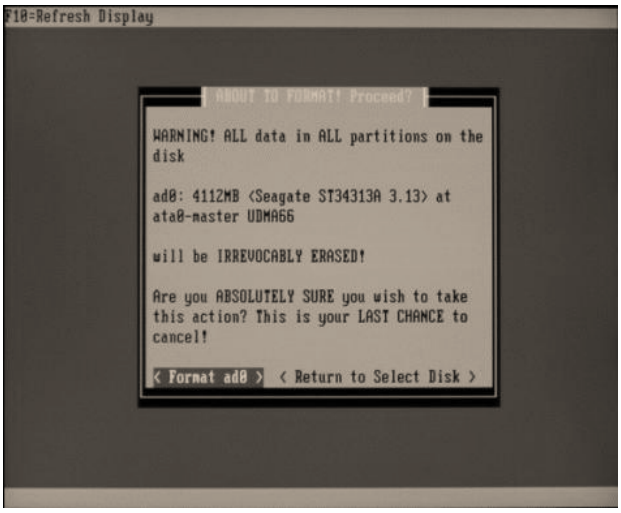


*Figura 2.10 : Confirmar Formato del Disco*

Seguido de la pantalla anterior el programa de instalación nos pide que confirmemos nuestro deseo de Dar Formato al Disco *(Figura 2-10)*, a lo cual deberemos responder afirmativamente mediante la opción *Format ad0 (Formatear ad0)*, cabe la aclaración de que *ad0* es un alias que dado por el programa de instalación a nuestro Disco.

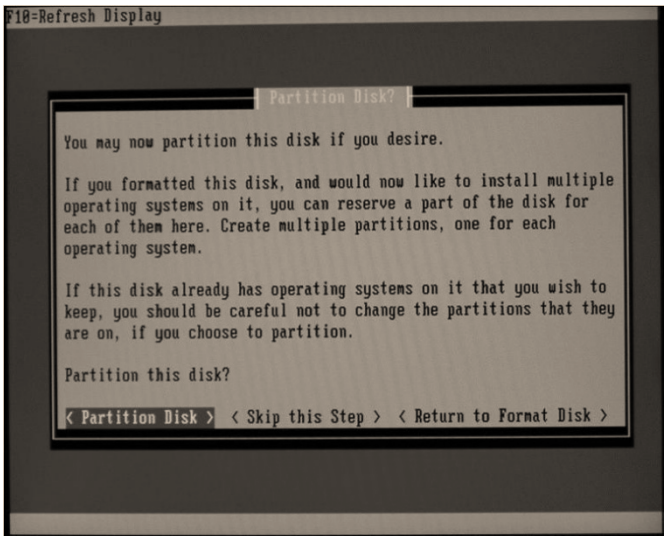


*Figura 2.11 : Particionar el Disco Duro*

Luego de concluído el proceso de Formato del Disco Duro, el programa de instalación nos pregunta si deaseamos crear particiones en nuestro Disco *(Figura 2-11)*, lo cual, como expresamos al principio, es necesario para organizar el Disco de una manera mas eficiente, ya que mientras mas eficientemente trabaje el Disco, mejor será su rendimiento, en especial cuando este deba procesar grandes cantidades de información. Por estos motivos es recomendable escoger la opción *Partition Disk (Particionar el Disco)*. Cabe mencionar que todo Disco Duro formateado bajo Linux (pfSense es una versión de Linux especializada en Seguridad) requiere de al menos dos particiones, la *Partición Principal o Primaria*, que es donde se va a alojar el Sistema Operativo, y la *Partición (a veces llamada Subpartición) SWAP*, la cual es un espacio reservado en el Disco con el objetivo de almacenar los archivos que el Sistema Operativo requiera con mayor frecuencia con el objeto de poder acceder a ellos más rápidamente, además de actuar como facilitador o intermediario entre el Disco y la memoria RAM (memoria especial del computador destinada a ejecutar procesos, como por ejemplo, abrir programas).


*Figura 2.12 : Crear Partición Primaria*

Como se explicó en el punto anterior, Linux requiere de al menos dos particiones, la Primaria y la SWAP, en esta pantalla se nos pide seleccionar la partición del disco a la que deseemos destinar el rol de Partición Primaria *(Figura 2-12)*, pero como hasta el momento sólo hemos creado una partición, esa será la que deberemos escoger.

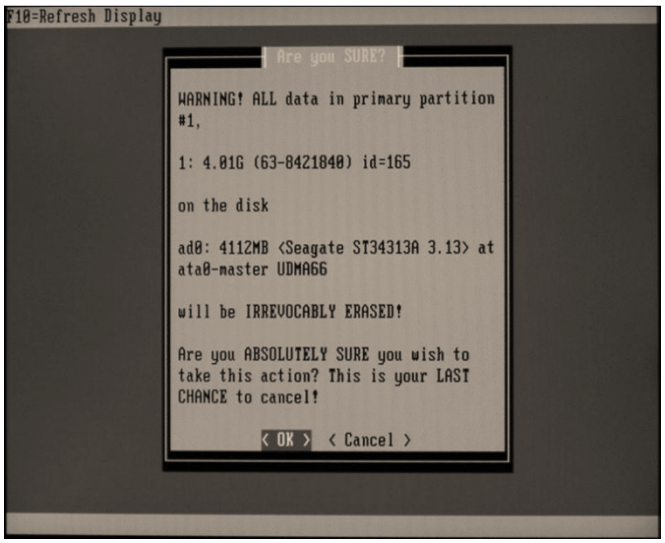


*Figura 2.13 : Confirmación de Creación de Partición Primaria*

En esta pantalla simplemente se nos pide confirmar la creación de la Partición Primaria *(Figura 2-13)*, sólo basta con escoger *OK* para poder proseguir.

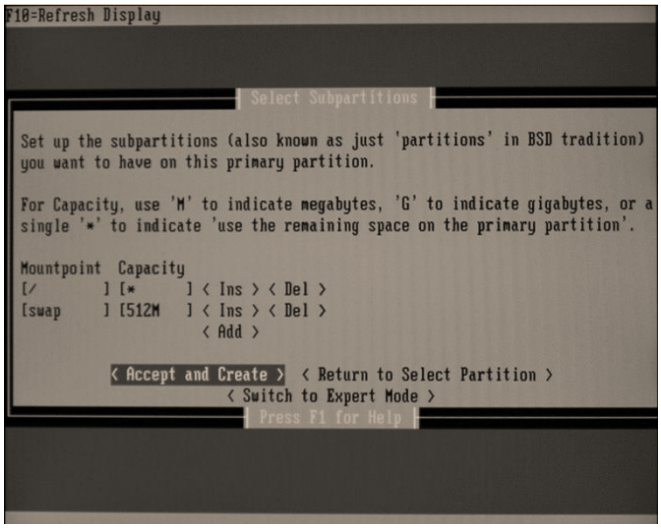


*Figura 2.14 : Creación y Configuración de la Partición SWAP*

Luego de haber creado la Partición Primaria, es necesario crear la Partición SWAP, los valores por defecto funcionan bien para nuestra configuración, por lo cual no es necesario alterarlos, simplemente debemos seleccionar la opción *Accept and Create (Aceptar y Crear) (Figura 2-14)* y el programa de instalación se hará cargo del resto.

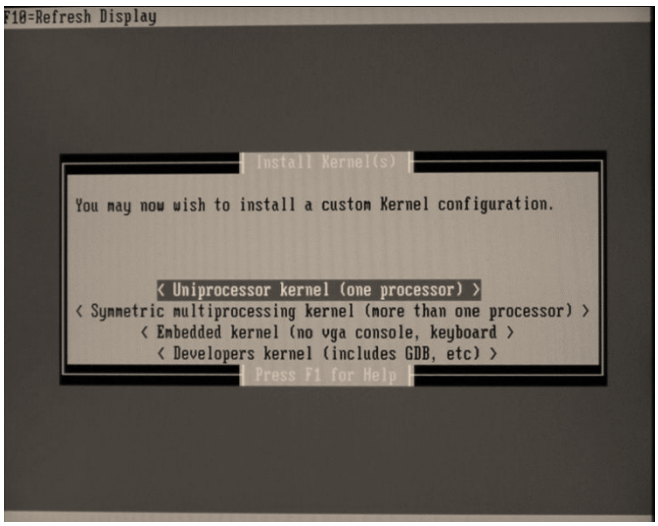


*Figura 2.15 : Elección del Tipo de Kernel*

Una vez creada y configurada la partición SWAP, se debe proceder a escoger el *Tipo de Kernel* a utilizar *(Figura 2-15)*, el *Kernel*, el cual es considerado como el corazón o núcleo del Sistema Operativo, es el programa que hace posible la interacción entre los Programas y el Hardware (por ejemplo, cuando se envía a imprimir un documento de Word, el Kernel es el que permite que el Programa Word, haga uso del Hardware Impresosa para crear una copia sólida del documento de Word almacenado en el computador). El Tipo de Kernel a escoger depende estrictamente del tipo de Hardware a usar, así hay Kernel para computadores con un procesador, con varios procesadores, con o sin adaptadores de Video, etc. En nuestro caso vamos a escoger la opción de Kernel para un solo procesador *(Uniprocessor Kernel)*, que es la que corresponde a nuestro Servidor.

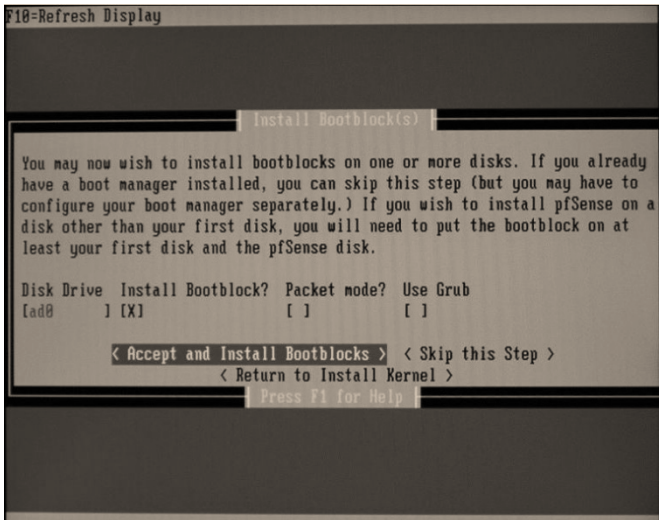


*Figura 2.16 : Instalación del Bootblock*

Finalmente, es necesaria la instalación del *Bootblock (Figura 2-16)*, el cual es un area especial del Disco Duro, reservada única y exclusivamente con el propósito de almacenar toda la información necesaria para que el el Servidor pueda iniciar el Sistema Operativo, el cual almacena entre otras cosas, todas las configuraciones hechas anteriormente.

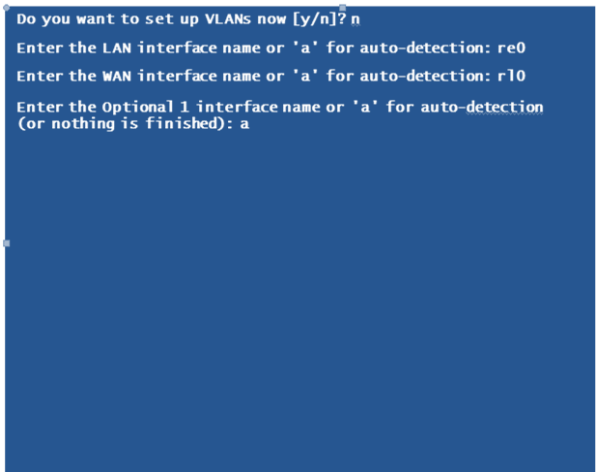


*Figura 2.17 : Asignación de Adaptadores de Red*

Concluida la instalación del Sistema Operativo, es necesario *Asignar a cada uno de los extremos de la red a su Adaptador, o Interfaz, correspondiente (Figura 2-17)*, siendo los extremos de la red, la LAN, o en otras palabras, la red ubicada en el interior de la empresa, y la WAN, que en este caso es la conexión de Internet de la misma. Los Adaptadores de Red antes mencionados son cada una de las Tarjetas de Red instaladas en el Servidor, cada tarjeta está encargada de administrar cada uno de los extremos de la Red, así que en total tenemos dos tarjetas de red.

Los valores recomendados son, para la LAN, *re0*, el cual corresponde al primer Adaptador de Red, y *rl0*, el segundo, para la WAN. Como el Servidor no cuenta con ningún adaptador de red adicional, se recomienda asignarle a este la opción *a* para que el programa omita la búsqueda de estos.

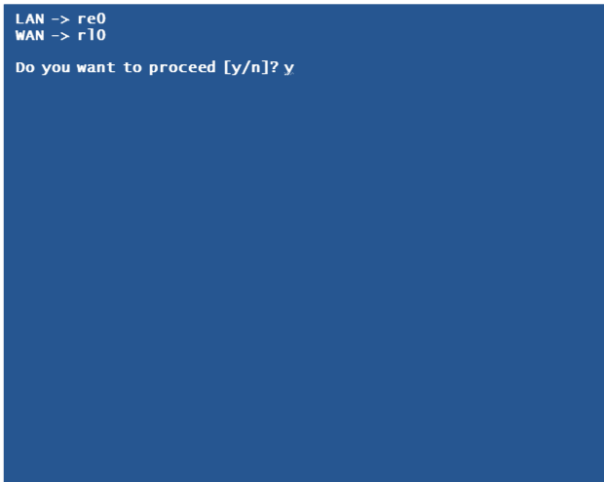


*Figura 2.18 : Confirmar la Asignación de Adaptadores de Red*

Acto seguido a la asignación de los Adaptadores o Interfaces de Red a su correspondiente extremo de red, LAN y WAN respectivamente, se pide *confirmar la operación*, a lo cual se deberá responder de forma positiva, *y*.

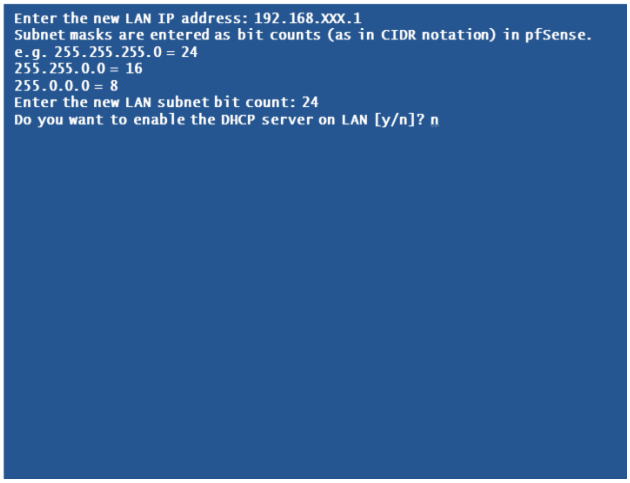


*Figura 2.19 : Asignación de Dirección IP y Mascara de Subred*

Para finalizar, el Sistema Operativo nos pide *asignar tanto la dirección IP genérica del Servidor de Seguridad en la LAN, así como su Máscara de Subred (Figura 2-19)*. Estos valores, el IP *192.168.XXX.1* y la Máscara *255.255.255.0*, que es seleccionada al escoger la opción *24*, tienen la función de permitir la correcta identificación del Servidor dentro de la red además de brindar acceso a su interfaz de configuración.

Por último se nos pregunta si deseamos que el Servidor de Seguridad asuma la función de *DHCP (Dynamic Host Configuration Protocol, ó Protocolo de Configuración Dinámico de Huéspedes, donde los huéspedes a los que hace referencia el nombre son los computadores Clientes de la Red)*, o sea que este sea el encargado de asignar a cada uno de los equipos de la red los parámetros necesarios para interactuar en la misma, tales como son las direcciones IP, Máscaras de Subred, Puertas de Enlace, y la dirección del Servidor DNS. Deberemos responder negativamente, *n*, a esta pregunta, ya que esta función ya es realizada por el Router.

## 2.3 BALANCE DE EQUIPOS DE OFICINA

### 2.3.1 Muebles y servicios para oficina

| | CARACTERISTICAS | COSTO | CANT | TOTAL |
|---|---|---|---|---|
| **Escritorios** | Para PCs | $ 126.00 | 9 | $ 1134.00 |
| **Sillas** | Giratorias | $ 58.00 | 9 | $ 522.00 |
| **Fax** | Samsung | $ 80.00 | 1 | $ 80.00 |
| **Telefonos** | Samsung | $ 18.00 | 3 | $ 54.00 |
| **Lineas** | Telefónicas | $ 125.00 | 2 | $ 250.00 |
| **Central** | Samsung | $ 400.00 | 1 | $ 400.00 |
| **A/a split** | 24000BTU | $ 760.00 | 1 | $ 760.00 |
| **Internet** | Banda ancha 2.5mb | $ 111.88 | 1 | $ 100.00 |
| | | | **TOTAL** | **$ 3300.00** |

*Tabla 2.1 : Muebles y Servicios de Oficina*

### 2.3.2 Equipos

#### 2.3.2.1 Computadores para uso de Oficina

| | CARACTERISTICAS | COSTO | CANT | TOTAL |
|---|---|---|---|---|
| **Procesador** | Intel ¡Core2Duo e7500 | $ 146.00 | 9 | $ 1314.00 |
| **Memoria** | Ram DDR2-800 1GB. | $ 19.00 | 9 | $ 171.00 |
| **Disco** | 320gb Samsung móvil SATA 5400rpm | $ 64.00 | 9 | $ 576.00 |
| **Multimedia** | DVD-Writer LG GH22NS50 | $ 25.00 | 9 | $ 225.00 |
| **Monitor** | Flat panel 15” | $ 160.00 | 9 | $ 1440.00 |
| **Ups** | 600 – 750w | $ 65.00 | 9 | $ 585.00 |
| | | | **TOTAL** | **$ 4311.00** |

*Tabla 2.2 : Muebles y Servicios de Oficina*

#### 2.3.2.2 Servidores

Los Servidores de Seguridad se dividen en 2 grupos, 1 Servidor para uso de Oficina, y 4 Servidores para Stock en Bodega con la finalidad de hacer reemplazos de emergencia en caso de ser necesario.

| | CARACTERISTICAS | COSTO | CANT | TOTAL |
|---|---|---|---|---|
| **Procesador** | Intel Atom_230 1.6GHZ | $ 260.00 | 5 | $ 1300.00 |
| **Memoria** | 2gb ddr2 pc-667 | | | |
| **Disco** | 160gb Seagate móvil SATA 5400RPM | | | |
| **Optico** | DVD-RWriter Samsung SE-S084b slim. | | | |
| **Ups** | APC 750w | $ 87.00 | 5 | $ 435.00 |
| | | | **TOTAL** | **$ 1735.00** |

*Tabla 2.3 : Servidores*

### 2.3.2.3 Equipo Adicional

| | CARACTERISTICAS | COSTO | CANT | TOTAL |
|---|---|---|---|---|
| **Switch** | Switch DLink DES-1016d 16 Puertos | $ 78.00 | 1 | $ 78.00 |
| **Impresora** | Samsung Laser Multifunción SCX-4521 | $ 159.00 | 1 | $ 159.00 |
| | | | **TOTAL** | **$ 23700** |

*Tabla 2.4 : Equipo Adicional*

### 2.3.2.4 Equipo Táctico para Trabajo Técnico Móvil (ET3M)

| | CARACTERISTICAS | COSTO | CANT | TOTAL |
|---|---|---|---|---|
| **Monitor** | Flat panel 15” | $ 160.00 | 1 | $ 160.00 |
| **Teclado** | Ps/2 | $ 10.00 | 1 | $ 10.00 |
| **Mouse** | Ps/2 | $ 7.00 | 1 | $ 7.00 |
| **Herramientas** | Destornilladores :<br>1 plano, 1 estrella | $ 5.00 | 1 | $ 5.00 |
| | Brocha grande | $ 3.00 | 1 | $ 3.00 |
| | Lata de aire comprimido | $ 7.00 | 1 | $ 7.00 |
| | Testeador de red | $ 25.00 | 1 | $ 25.00 |
| | Voltímetro | $ 10.00 | 1 | $ 10.00 |
| | Fuente de poder | $ 25.00 | 1 | $ 25.00 |
| | Mochila de laptop | $ 28.00 | 1 | $ 28.00 |
| **Memoria** | RAM DDR2-800 1GB | $ 19.00 | 1 | $ 19.00 |
| | RAM DDR2-800 2GB | $ 38.00 | 1 | $ 38.00 |
| | | | **TOTAL** | **$ 337.00** |

*Tabla 2.5 : ET3M*

## 2.4 BALANCE DE PERSONAL

| | FUNCIÓN | SUELDO | CANT | TOTAL |
|---|---|---|---|---|
| **Operador(a)** | Secretaria/Recepcionista | $ 250.00 | 1 | $ 250.00 |
| **Técnicos** | Fijos y móviles | $ 320.00 | 3 | $ 960.00 |
| **Administrador de seguridad y monitoreo** | Administradores de red | $ 450.00 | 3 | $ 1350.00 |
| **Vendedores** | Telemercadeo – fijo | $ 480.00 | 1 | $ 480.00 |
| | Telemercadeo – móvil | $ 650.00 | 1 | $ 650.00 |
| | | | **TOTAL** | **$ 3690.00** |

*Tabla 2.6 : Balance de Personal*


# CAPÍTULO 3

# INVESTIGACIÓN DE MERCADO

## 3.1 Perspectivas de la Investigación

En la siguiente Unidad se pretende diseñar e implementar una investigación de mercado que permita identificar los problemas de productividad y seguridad que el cliente enfrenta en el área informática de su empresa, y el costo, tanto de tiempo como de dinero, que estos problemas le causan.

Esta investigación permitirá formarnos una idea clara de las necesidades básicas que nuestros clientes potenciales poseen, lo cual nos ayudará a ajustar nuestro producto, nuestra estrategia de ventas, y el enfoque que deberá tener nuestra empresa para poder satisfacer dichas necesidades, enfatizando en todo momento, el ahorro de recursos tanto monetarios como de tiempo que implica la implementación de una solución preventiva, como la que ofrecemos, con respecto a la corrección de un problema ya existente.

La investigación de mercado que planeamos implementar va dirigida en particular a los gerentes y subgerentes de empresas pequeñas y medianas, y aunque, estamos en capacidad de servir también a empresas de mayor tamaño, ellas no son nuestro mercado primordial. Esto se debe a que las empresas pequeñas y medianas, al no contar con las misma cantidad de recursos que las empresas más grandes, no tienen la posibilidad de contar con un departamento de sistemas que se encargue de proteger a la empresa contra los problemas de índole informática que pudieren presentarse.

A causa de lo mencionado anteriormente, nuestra empresa apunta a satisfacer la necesidad de protección informática que tanto las empresas pequeñas y medianas poseen, y, a la cual, debido en gran parte al alto costo que esta tiene, normalmente no tienen acceso.

## 3.2 Planteamiento del Problema

Si se analizaran detalladamente todos y cada uno de los problemas que por lo general sufren las empresas, como por ejemplo, lentitud en las transacciones realizadas diariamente, pérdidas de información, desvíos de fondos, o disminución de la producción, nos daríamos cuenta que muchos, sino todos estos problemas, que anualmente cuestan a las empresas importantes sumas de dinero, tienen su origen en el área informática.

Esto se debe a que en la actualidad todo el trabajo que dichas empresas necesitan realizar para seguir funcionando, sin importar su tamaño, depende de forma directa o indirecta de los computadores, y estos a su vez, dependen de las Redes Informáticas para permanecer actualizados respecto a la situación de la empresa, ya sea para abastecer su stock y pagar a sus respectivos proveedores, o para despachar pedidos y realizar cobros. Por lo tanto, cualquier problema que se presente en el área informática, terminará, tarde o temprano afectando las labores de la empresa en general y de cada uno de sus integrantes en particular.

Pero, a pesar de la gran importancia en la empresa moderna, el área informática es la que generalmente recibe menos cuidado tanto en su planeación como en la asignación de recursos para su mantenimiento, por lo cual no resulta extraño encontrarse con empresas que sufren grandes pérdidas monetarias, retrasos en el despacho de mercaderías, o errores en el reabastecimiento de sus inventarios causados, muchas veces, por fallas en el equipo informático usado, y por ende, en la calidad de información que este produce.

Con el pasar de los años, y debido al creciente interés de la población general con respecto al tema de los Virus Informáticos, muchos gerentes han empezado a prestarle más atención al área informática de las empresas que administran, pero, a pesar de los esfuerzos que han realizado para mejorar la situación de la misma, se han encontrado con el infranqueable muro económico que representa el tener un buen nivel de protección a corto, mediano y largo plazo, y ese muro es precisamente el que nuestra empresa pretende derribar, ofreciendo un muy elevado nivel de protección, que debido a su alto costo, antes sólo era asequible para empresas grandes o multinacionales.

Frente a todo lo expuesto anteriormente, hemos decidido, que nuestro nicho de mercado estará conformado por empresas medianas y pequeñas solamente, ya que, como mencionamos anteriormente, son dichas empresas las que actualmente no se encuentran en posibilidades de adquirir soluciones de Seguridad Informática debido a su costo y a que no existen, en la actualidad, empresas que les brinden ese servicio.

## 3.3 Objetivos de la investigación

### 3.3.1 Objetivos Generales

- Determinar la existencia de un nicho de mercado para Servidores de Seguridad en las Empresas Medianas y Pequeñas

- Identificación de las oportunidades de mercado para la oferta de los Servidores de Seguridad

- Definición del segmento de mercado para los Servidores de Seguridad

### 3.3.2 Objetivos Específicos

- Determinación de gustos y preferencias del consumidor potencial.

- Frecuencia de con la que el cliente solicita ayuda técnica externa para solucionar los problemas informáticos presentados en la empresa

- Percepción del cliente con respecto al problema de tipo informático que sufre su empresa

## 3.4 Plan de Muestreo

### 3.4.1 Definición de la Población

La población, por definición, es el conjunto total de personas naturales y/o jurídicas que representa a todas las mediciones de interés para el estudio a realizar. La muestra, en cambio, es un subconjunto del total de la población mediante el cual es posible inferir la conducta o tendencia general de la población en conjunto.

La población considerada para el presente estudio de mercado se concentra en la ciudad de Guayaquil, ya que es allí donde funcionará la empresa que se desea implementar.

En base al listado de empresas registradas en la Cámara de la Pequeña Industria del Guayas (CAPIG), se determinó que las empresas pequeñas y medianas que funcionan actualmente en la ciudad son :

| Ciudad | Año 2009 |
|---|---|
| Guayaquil | 1.718 |

*Cuadro 3.1 : Población Guayaquil*

Pero, analizando los datos más detalladamente, encontramos que del total de empresas registradas, tan solo el 46,91% se dedica a algún tipo de actividad comercial en la cual es posible la implementación de los Servidores de Seguridad, ya que el resto se dedica a actividades comerciales de menor escala, como por ejemplo restaurantes, bazares, y venta de joyería o de artículos varios. Por lo tanto, la población objetivo quedaría definida de la siguiente forma :

| Ciudad | Año 2009 | 46,91% Aplicable |
|---|---|---|
| Guayaquil | 1.718 | 806 |

*Cuadro 3.2 : Población Aplicable*

## 3.4.2 Definición de la Muestra

Luego de haber analizado los datos proporcionados por la Cámara de la Pequeña Industria del Guayas (CAPIG), obtuvimos como resultado que del 100% de las empresas registradas, tan sólo el 46,91% son aplicables al estudio a realizar.

Para facilitar el proceso de muestreo, de encuesta y de análisis de resultados, se clasificó a las empresas aplicables según su actividad comercial, por lo cual quedaron segmentadas de la siguiente forma :

| Actividad Comercial | Cant. |
|---|---|
| Producción e Importación y Distribución de insumos Agrícolas | 58 |
| Producción e Importación de Juguetes y Artículos de Bazar | 7 |
| Proveedores de Servicios Administrativos y Consultorías | 54 |
| Importación y Comercialización Autos y material Automotriz | 30 |
| Comercialización y Explotación de Bienes Raíces | 115 |
| Importación de Equipo y Suministros de Oficina y Computación | 53 |
| Venta al por mayor de Equipo y Suministros de Oficina y Computación | 11 |
| Producción e Importación de Equipo y Materiales de Construcción | 96 |
| Venta al por mayor de Equipo y Materiales de Construcción | 58 |
| Publicidad y Medios de Comunicación | 33 |
| Proveedores de Servicios Litográficos a mediana y gran escala | 59 |
| Producción e Importación de Equipo material Industrial | 16 |
| Importación de Equipo Fotográfico, Óptico y de Precisión | 5 |
| Explotación, Importación y Exportación de Madera y derivados | 18 |
| Electro y Metalmecánica Aplicada a la Ingeniería y a la Industria | 193 |
| *TOTAL EMPRESAS* | *806* |

*Cuadro 3.3 : Población Aplicable segmentada por Actividad Comercial*

Como se aprecia en la tabla, las empresas aplicables al estudio están divididas en 15 categorías sumando 806 en total, y, con el objeto de que la muestra a tomar sea lo más equilibrada posible, hemos decidido encuestar a 2 empresas por cada categoría, lo que nos dá un total de 30 empresas a estudiar.

## 3.5 Diseño de la Encuesta

**Pregunta 1.- Ha tenido problemas de Pérdidas de Información, caídas en el Sistema Administrativo ó Virus Informáticos en su empresa durante el último año?**

Si___ No___

**Pregunta 2.- Aproximadamente, cuántos problemas de los mencionados anteriormente ha tenido su empresa durante el último año?**

Menos de 10___ Entre 10 y 20___ Entre 20 y 30___ Más de 30___

**Pregunta 3.- Mensualmente, con qué frecuencia su empresa solicita de Asistencia Técnica externa para resolver los ya mencionados problemas informáticos?**

Menos de 3 veces___ Entre 3 y 7 veces___ Más de 7 veces___

**Pregunta 4.- En el caso de un ataque de Virus, aproximadamente cuánto tarda el Técnico Informático en dar solución al problema?**

Menos de 1 hora___ De 1 a 3 horas___ Más 3 horas___ Hasta el día siguiente___

**Pregunta 5.- Cuánto invierte mensualmente en Asistencia Técnica Externa?**

Menos de 50 dólares___ Entre de 50 y 60 dólares___

Entre de 60 y 70 dólares___ Más de 70 dólares___

**Pregunta 6.-** **En términos generales, se encuentra satisfecho con el rendimiento del Área Informática de su empresa?**

Si___ No___

**Pregunta 7.-** **Qué tanta prioridad le dá usted al Área informática de su Empresa en la asignación anual de recursos?**

Prioridad Alta___ Prioridad Normal___ Poca Prioridad___ Baja prioridad___

**Pregunta 8.-** **Estaría interesado en adoptar una solución rápida y permanente para solucionar sus problemas en el Área Informática?**

Si___ No___

**Pregunta 9.-** **Cuánto estaría dispuesto a pagar por una solución capaz de inmunizar todos sus computadores contra Virus Informáticos, acelerar notablemente su acceso a Internet, e incrementar tanto el rendimiento como el control que usted es capaz de ejercer sobre el Área Informática de su empresa?**

300 dólares___ Entre 300 y 350 dólares___ 350 dólares___

**Pregunta 10.-** **Cuánto estaría dispuesto a pagar mensualmente por el monitoreo diario de la Seguridad Informática de su empresa?**

25 dólares___ Entre 25 y 35 dólares___ 35 dólares___

## 3.6 Presentación de Resultados

**Pregunta 1.- Ha tenido problemas de Pérdidas de Información, caídas en el Sistema Administrativo ó Virus Informáticos en su empresa durante el último año?**

Las empresas encuestadas, en su totalidad, confesaron haber tenido problemas de pérdida de información, caídas en su sistema administrativo o infecciones por virus informáticos, durante el último año.


*Gráfico 3.1 : Problemas de tipo informático presentados durante el último año*

**Pregunta 2.- Aproximadamente, cuántos problemas de los mencionados anteriormente ha tenido su empresa durante el último año?**

El 23,33% de las empresas encuestadas han presentado menos de 10 problemas informáticos, otro 23,33% de esas mismas empresas ha presentado de 10 a 20 problemas, lo que es todavía considerado normal para el periodo de tiempo tomado en cuenta.

Mientras tanto, el 33,33% ha presentado entre 20 y 30 problemas, y el 20% restante ha presentado más de 20 problemas, lo cual es ya, una cifra elevada en relación al periodo estudiado, hecho que resulta preocupante.


*Gráfico 3.2 : Número de problemas de tipo informático presentados durante el último año*

**Pregunta 3.- Mensualmente, con qué frecuencia su empresa solicita de Asistencia Técnica externa para resolver los ya mencionados problemas informáticos?**

El 23,33% de las empresas encuestadas solicitan menos de 3 veces al mes la asistencia de un técnico para resolver sus problemas informáticos, en este grupo se encuentran las empresas que sufren menos de 10 problemas informáticos al año.

El 56,67% del total de empresas solicitan asistencia de 3 a 7 veces al mes, y el 20% restante solicita de esta misma asistencia más de 7 veces al mes, como es de suponer, las empresas que mas asistencia técnica solicitan, son las que mayor número de problemas sufren, o sea más de 20.

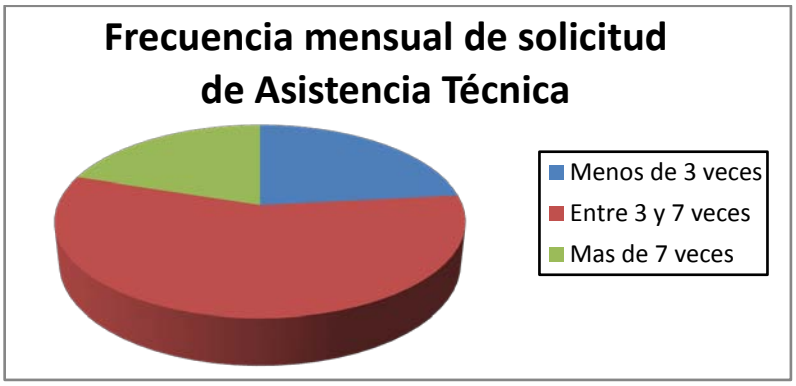


*Gráfico 3.3 : Frecuencia mensual de solicitud de asistencia técnica*

**Pregunta 4.- En el caso de un ataque de Virus, aproximadamente cuánto tarda el Técnico Informático en dar solución al problema?**

En el 23,33% de empresas los problemas informáticos se resuelven en menos de 1 hora, este porcentaje, si se compara con el porcentaje de empresas que tienen menos de 10 problemas al año, se nota que es prácticamente el mismo, lo cual nos lleva a concluir que los problemas presentados en esas empresas no son realmente graves.

El 33,33% empresas confiesa que sus problemas se resuelven en promedio de 1 a 3 horas, mientras que el 30% dice que sus problemas se resuelven en más de 3 horas, ahora, si se observa detenidamente, la suma de estos porcentajes son casi los mismos que los de las empresas que tienen entre 10 y 20 problemas y los de las que tienen entre 20 y 30 problemas al año.

El 13% restante confiesa que sus problemas suelen tardar hasta el día siguiente en resolverse, lo cual, si se sigue con la tendencia que los porcentajes anteriores presentan, nos lleva a pensar que corresponde a los de las empresas que presentan más de 30 problemas al año.

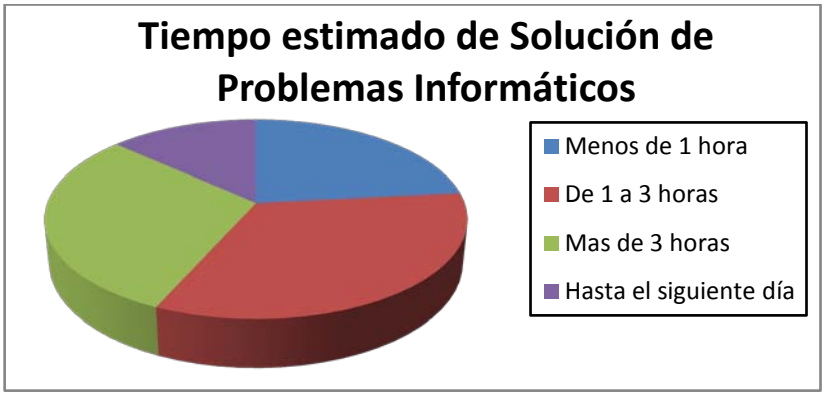


*Gráfico 3.4 : Tiempo estimado de solución de Problemas Informáticos*

**Pregunta 5.- Cuánto invierte mensualmente en Asistencia Técnica Externa?**

El 23,33% de las empresas dice gastar menos de 50 dólares al mes en asistencia, lo cual, si se observa la tendencia hasta el momento, corresponde a las empresas que presentan menos de 10 problemas al año.

El otro 23,33% de empresas encuestadas gasta entre 50 y 60 dólares, mientras que el 33,33% de ellas asegura gastar entre 60 y 70 dólares al mes en asistencia, lo cual corresponde casi al mismo porcentaje de empresas que presentan entre 10 y 20 problemas y entre 20 y 30 problemas al año.

El 20% restante, por ende, corresponde a las empresas que presentan un mayor número de problemas al año, o cuyos problemas sean de mayor gravedad que los de las demás.

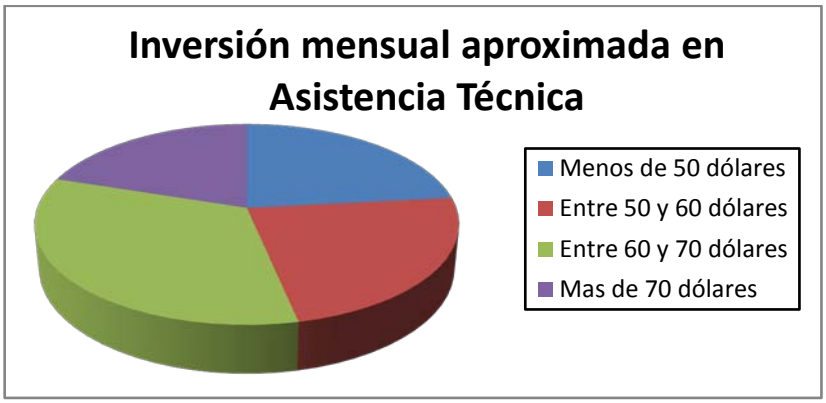


*Gráfico 3.5 : Inversión mensual aproximada en asistencia técnica*

**Pregunta 6.- En términos generales, se encuentra satisfecho con el rendimiento del Área Informática de su empresa?**

Del total de empresas encuestadas, tan solo el 13,33% de ellas se encuentran satisfechas con el rendimiento actual de su área informática, este porcentaje corresponde a los de las empresas que presentan menos de 10 problemas al año y que gastan menos de 50 dólares al mes en asistencia.

Mientras que el 86,67% restante se muestran poco satisfechos con su área informática, tanto por la cantidad de problemas que se presentan en ella durante el año, como por el gasto que se debe hacer mensualmente para mantenerla funcionando.


*Gráfico 3.6 : Satisfacción percibida del rendimiento del área informática*

**Pregunta 7.- Qué tanta prioridad le da usted al Área informática de su Empresa en la asignación anual de recursos?**

Según lo encuestado, el 40% de empresas le da alta prioridad a la asignación de recursos para su área informática, lo cual implica que las personas a cargo de la administración de la empresa le dan gran importancia a esta área, ya que la consideran vital para el correcto desempeño de la actividad laboral de la empresa.

El 43,33% de empresas le da prioridad normal a la asignación de recursos, esto quiere decir que dichas empresas consideran importante a su área informática, pero no más importante que otros departamentos de la empresa, lo cual es hasta cierto punto, aceptable.

Entre tanto que el 13,33% de empresas dan poca prioridad a la asignación de recursos para el área informática, ya que por lo general esta es una de las últimas en recibir recursos, mientras, que el 3,33% de las empresas le dan baja prioridad a la asignación de dichos recursos para esta área, tanto así que esta área es la última en recibir recursos, y casi siempre termina recibiendo los sobrantes de las asignaciones a otros departamentos. Esto demuestra la poca importancia que ciertas empresas le dan a esta área, lo cual se traduce en problemas constantes y baja calidad de información.


*Gráfico 3.7 : Satisfacción percibida del rendimiento del área informática*

**Pregunta 8.- Estaría interesado en adoptar una solución rápida y permanente para solucionar sus problemas en el Área Informática?**

El 86,67% de las empresas encuestadas han probado varias soluciones para dar fin a sus problemas informáticos, pero hasta el momento no han hallado una que les dé una solución definitiva y económica a estos, por eso demuestran gran interés en una potencial solución que los libre definitivamente de este problema.

Entre tanto el 13,33% restante no demuestra interés en adoptar otras soluciones, ya que las que utilizan actualmente les brindan resultados satisfactorios y relativamente económicos. Cabe destacar la observación de que este porcentaje de empresas es virtualmente el mismo que el porcentaje de empresas que presenta menos de 10 problemas al año y que gasta menos de 50 dólares al mes en asistencia, lo cual explica su poco interés en otro tipo de soluciones.


*Gráfico 3.8 : Disposición de empresas a adoptar otra solución para sus problemas informáticos*

**Pregunta 9.-** **Cuánto estaría dispuesto a pagar por una solución capaz de inmunizar todos sus computadores contra Virus Informáticos, acelerar notablemente su acceso a Internet, e incrementar tanto el rendimiento como el control que usted es capaz de ejercer sobre el Área Informática de su empresa?**

De acuerdo a la encuesta, el 66,67% de las empresas están dispuestas a pagar 300 dólares por la solución de seguridad detallada en el estudio, lo cual, según los resultados anteriores, es un ahorro muy significativo en cuanto a gastos de mantenimiento del área informática.

En tanto que el 26,67% de las empresas están dispuestas a pagar una suma entre 300 y 350 dólares por la solución, mientras que el 6,67% de ellas está dispuesta a pagar 350 dólares. El valor que las empresas están dispuestas a pagar está en función tanto de sus posibilidades económicas como del gasto en que actualmente estas incurren por concepto de mantenimiento.

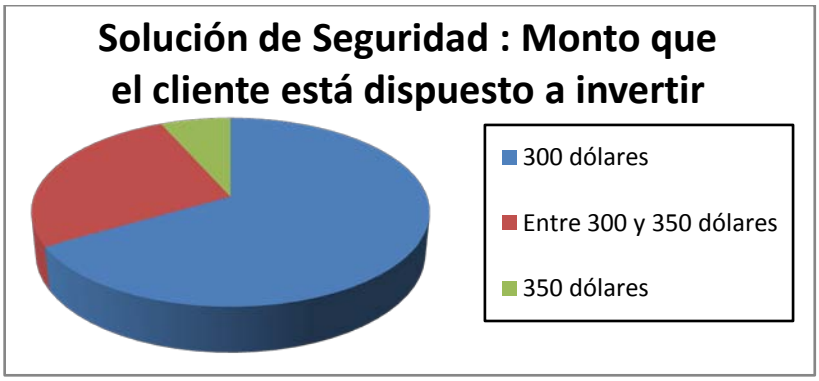


*Gráfico 3.9 : Monto que el cliente está dispuesto a invertir en la Solución de Seguridad*

**Pregunta 10.-** **Cuánto estaría dispuesto a pagar mensualmente por el monitoreo diario de la Seguridad Informática de su empresa?**

El 73,33% de las empresas encuestadas están dispuestas a pagar 25 dólares mensualmente por el monitoreo, en horarios de oficina, de la solución por parte de nuestra empresa.

Mientras que el 23,33% de ellas están dispuestas a pagar una cifra entre 25 y 35 dólares al mes por concepto de monitoreo, en tanto que el 3,33% restante está dispuesto a pagar 35 dólares por el mismo servicio. Dichas cifras están, tal y como lo mencionamos en la pregunta anterior, en función del gasto en que las empresas estudiadas actualmente incurren por concepto de mantenimiento de su área informática.

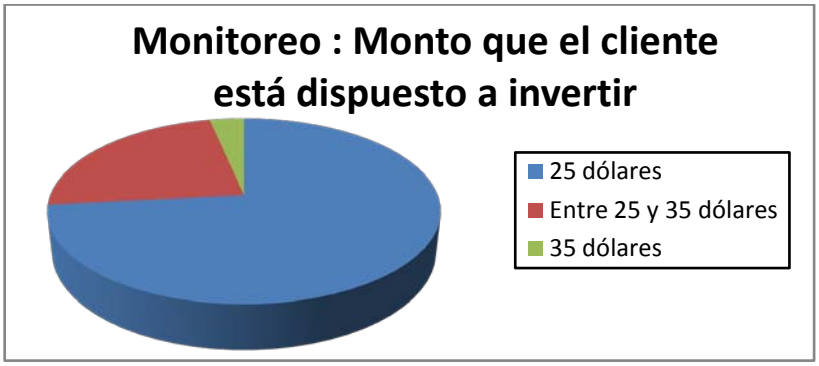


*Gráfico 3.10 : Monto que el cliente está dispuesto a invertir por concepto de Monitoreo de la Solución*

## 3.7 Conclusiones de la Investigación

La investigación realizada demostró que actualmente existe un nicho de mercado que no ha sido aún explotado en la ciudad en la que se aplicó el estudio, el de los Servidores y Servicios de Seguridad Informática orientados a Empresas e Industrias medianas y pequeñas; y, además que la mayor parte de las empresas estudiadas están dispuestas a adoptar la solución propuesta.

Dichas empresas están dispuestas a adoptar la solución presentada a causa de la gran cantidad de problemas de operación que muchas de ellas presentan en la actualidad, y que, mediante un análisis detallado de dichos problemas, han concluido que estos se deben en gran parte a fallos en el área informática.

Todas las empresas encuestadas utilizan actualmente uno o más métodos de protección contra problemas informáticos, pero han notado que esto no es suficiente, y, a causa de la persistencia de dichos problemas, muchas se han visto en la necesidad de invertir más fondos en mantenimiento del área informática de lo que anteriormente invertían, lo cual no sólo provoca la asignación de recursos adicionales a esta área, que bien podrían ser invertidos en otra que más lo necesite, sino que también casusa pérdida de tiempo valioso de trabajo.

Una conclusión general que se obtuvo del estudio es que, las empresas que invierten más, y con más celeridad en su área informática, son las que tienden a tener la menor cantidad de problemas; mientras que las que invierten menos, y con mayor tardanza, son las que por lo general presentan más problemas.

A pesar de que esto suene como algo lógico, en realidad no lo es tanto, ya que un porcentaje reducido de empresas encuestadas invierten poco capital en el mantenimiento de su área informática, pero a pesar de ello, no suelen tener mayores problemas, esto es debido a diversos factores, tales como la calidad de los equipos de computación con los que cuenta, la efectividad de la solución que actualmente utilizan, las políticas de la empresa (algunas prohíben expresamente el uso de pendrives o medios de almacenamiento externo), y quizá el más importante de todos, el buen juicio y la experiencia de los colaboradores de la empresa.


# CAPÍTULO 4

# PRESUPUESTO DE GASTOS Y COSTOS

## 4.1 Equipos de Oficina

Para la instauración de este proyecto se deben incorporar en el primer año los siguientes equipos de oficina :

| | COSTE UNIT. | CANT | COSTE TOTAL |
|---|---|---|---|
| Impresora Laser | $ 159,00 | 1 | $ 159,00 |
| Computadores (CPU+Monitor+Teclado+Mouse) | $ 479,00 | 9 | $ 4311,00 |
| Servidores de Seguridad | $ 300,00 | 5 | $ 1500,00 |
| Switch | $ 78,00 | 1 | $ 78,00 |
| Sillas | $ 58,00 | 9 | $ 522,00 |
| Escritorios | $ 126,00 | 9 | $ 1134,00 |
| Teléfonos | $ 18,00 | 3 | $ 54,00 |
| Fax | $ 80,00 | 1 | $ 80,00 |
| Central Telefónica | $ 400,00 | 1 | $ 400,00 |
| Aire Acondicionado Central | $ 760,00 | 1 | $ 760,00 |
| UPS 750W | $ 87,00 | 10 | $ 870,00 |
| Monitor Flat panel 15” | $ 160,00 | 3 | $ 480,00 |
| Teclado Ps/2 | $ 10,00 | 3 | $ 30,00 |
| Mouse Ps/2 | $ 7,00 | 3 | $ 21,00 |
| Destornilladores (1 plano+1 estrella) | $ 5,00 | 3 | $ 15,00 |
| Brocha grande | $ 3,00 | 3 | $ 9,00 |
| Lata de aire comprimido | $ 7,00 | 3 | $ 21,00 |
| Testeador de red | $ 25,00 | 3 | $ 75,00 |
| Voltimetro | $ 10,00 | 3 | $ 30,00 |
| Fuente de poder | $ 25,00 | 3 | $ 75,00 |
| Mochila de laptop | $ 28,00 | 3 | $ 84,00 |
| Ram ddr2-800 1gb | $ 19,00 | 3 | $ 57,00 |
| Ram ddr2-800 2gb | $ 38,00 | 3 | $ 114,00 |
| | **TOTAL GASTO MAQUINARIA. Y EQUIPOS** | | **$ 10.889,00** |

*Tabla 4.1 : Equipos de Oficina*

## 4.2 Gastos de Constitución

Son considerados como Gastos de Constitución todos, aquellos desembolsos que resultan necesarios para la Constitución Legal de una sociedad mercantil, estos tienen su devengo antes de que dicha constitución legal se haya formalizado.

Entre los Gastos de Constitución que consideramos para la realización de nuestro proyecto están los siguientes :

| | **COSTE** |
|---|---|
| Registro de marcas | $ 200,00 |
| Permisos de funcionamiento | $ 130,00 |
| Honorarios profesionales/evaluador | $ 500,00 |
| **TOTAL GASTOS DE CONSTITUCION** | **$ 830,00** |

*Tabla 4.2 : Gastos de Constitución*

## 4.3 Gastos de Alquiler

Los gastos considerados por concepto de Alquiler del local comercial donde fungirá la empresa son los siguientes :

| | **ALQUILER MENSUAL** | **ALQUILER ANUAL** |
|---|---|---|
| LOCAL | $ 500 | $ 6000 |

*Tabla 4.3 : Gastos de Alquiler*

## 4.4 Gastos de Servicios Básicos

Los gastos aproximados de servicios básicos que se consumirían durante el año son los siguientes :

| | **TARIFAS MENSUALES** | **MESES** | **TARIFAS ANUALES** |
|---|---|---|---|
| Luz | $ 95,00 | 12 | $ 1.140,00 |
| Teléfono | $ 53,00 | 12 | $ 636,00 |
| Agua | $ 30,00 | 12 | $ 360,00 |
| Internet 2,5mb | $ 111,88 | 12 | $ 1.342,56 |
| | **TOTAL ANUAL GASTOS SERVICIOS BASICOS** | | **$ 3.478,56** |

*Tabla 4.4 : Gastos de Servicios Básicos*

## 4.5 Gastos de Publicidad

El gasto de publicidad, se limita a las salidas de efectivo por concepto de anuncios publicitarios en revistas de circulación a nivel nacional, campañas de marketing y anuncios y banners publicitarios en diferentes medios de comunicación electrónicos y de internet.

| | FRECUENCIA ANUAL | COSTE UNIT. | COSTE TOTAL ANUAL |
|---|---|---|---|
| Periódicos | 6 | $ 200 | $ 1200 |
| Revistas | 8 | $ 300 | $ 2400 |
| Televisión | 2 | $ 3000 | $ 6000 |
| Banners | 50 | $ 100 | $ 5000 |
| Folletos | 1000 | $ 0,5 | $ 500 |
| | **TOTAL ANUAL GASTOS DE PUBLICIDAD** | | **$ 15100** |

*Tabla 4.5 : Gastos de Publicidad*

## 4.6 Sueldos y Salarios

A continuación se detallan los sueldos y salarios del personal que integrará la empresa :

| | SALARIO MENSUAL | OCUPANTES DEL CARGO | SALARIO ANUAL |
|---|---|---|---|
| Gerente general | $ 1000 | 1 | $ 12000 |
| Contador | $ 600 | 1 | $ 7200 |
| Operadora | $ 300 | 1 | $ 3600 |
| Técnicos | $ 320 | 3 | $ 11520 |
| Monitores | $ 450 | 3 | $ 16200 |
| Vendedores | $ 250 | 2 | $ 6000 |
| Guardián | $ 280 | 2 | $ 6720 |
| | **TOTAL GASTOS DE SUELDOS Y SALARIOS** | | **$ 63240** |

*Tabla 4.6 : Gastos de Sueldos y Salarios*

## 4.7 Gastos

En base a los cuadros antes detallados se presenta el siguiente cuadro resumen :

| | |
|---|---|
| Gastos de maquinarias y equipos | $ 11889 |
| Gastos de constitución | $ 830 |
| **TOTAL GASTOS INV. INICIALES** | **$ 12719** |
| Gastos de sueldos y salarios | $ 63240 |
| Gastos de servicios básicos | $ 3478,56 |
| Gastos de alquiler | $ 6000 |
| Gastos de publicidad | $ 15100 |
| **TOTAL GASTOS OPERATIVOS** | **$ 87818,56** |

*Tabla 4.7 : Resumen de Gastos*


# CAPÍTULO 5

# CONCLUSIONES Y RECOMENDACIONES

# 5.0 CONCLUSIONES Y RECOMENDACIONES

A lo largo de este documento se presentó un estudio preliminar con el objeto de determinar la factibilidad de la implementación de una solución de Seguridad Informática basada en Servidores de Seguridad, construidos específicamente con el fin de satisfacer las necesidades tanto de las Empresa como de las Industrias medianas y pequeñas, pero que son lo suficientemente flexibles para poder adaptarse tanto a necesidades futuras como a necesidades más específicas de seguridad que cualquier empresa pudiere tener.

Esto fue posible mediante el estudio de cuatro campos importantes de investigación, revisados en los capítulos anteriores.

En primer lugar, mediante la experiencia de cada uno de los miembros involucrados en el estudio, se dio lugar a una tormenta de ideas, mediante la cual se plantearon problemas comunes que existen en las áreas informáticas de todas las empresas, y se pensó en estrategias que se podían implementar para darles solución, esto dió lugar al primer prototipo de nuestro producto, y, mediante un estudio detallado de las posibles plataformas en las que se podía montar nuestra solución nos inclinamos por Linux, por ser la más económica, rápida y segura de las que analizamos, y, junto con el detalle de nuestro prototipo inicial se planteó el proceso de implementación de la plataforma escogida en el mismo, dando resultados satisfactorios en las primeras pruebas ejecutadas.

Ya con nuestro prototipo inicial en funcionamiento, procedimos a depurarlo con la información obtenida mediante un estudio hecho a varias empresas, pudiendo así reducir costos de fabricación e implementación, con el objeto de satisfacer las necesidades tanto tecnológicas como económicas de nuestro mercado potencial. La respuesta obtenida de varios de los potenciales clientes con respecto a la nueva versión de nuestro prototipo, moldeado por las necesidades, quejas, y recomendaciones obtenidas, fué positiva.

El último aspecto a estudiar fué el económico, en el cual, haciendo uso de la experiencia recopilada a lo largo del presente estudio, fué bastante sencillo, ya que simplemente nos adaptamos a un modelo de trabajo similar al de las compañías de Seguridad Física, en el respecto que vendemos nuestra solución y luego cobramos una tasa mensual por el monitoreo de la misma.

Para detallar un poco mejor nuestra experiencia en este capítulo se presentarán :

1. Conclusiones
2. Limitaciones del estudio
3. Recomendaciones

## 5.1 CONCLUSIONES

Actualmente existe una creciente preocupación de las empresas por con respecto a la Seguridad Informática, lo cual queda demostrado por el hecho de que, el 100% de empresas encuestadas utiliza al menos algún método de protección contra amenazas a dicha seguridad, siendo el Antivirus el más común de ellos.

Otra prueba que demuestra el creciente interés por la Seguridad Informática, es que de todas las empresas estudiadas, el 76,67%, no deja de invertir menos de 50 dólares al mes en mantenimiento de su área informática, o sea, que la gran mayoría de ellas invierte al menos 600 dólares al año en su área informática.

Esto nos da a entender que las personas encargadas de administrar dichas empresas consideran importante al área informática, y que, en caso de tener acceso a una mejor solución para sus problemas informáticos, estarían dispuestos a adoptarla, siempre y cuando su costo no exceda su presupuesto establecido, lo cual ha quedado determinado, que es de al menos 600 dólares al año.

Por tanto, el costo de nuestra solución, con el objeto de adaptarse a dicho presupuesto, ha quedado establecido en 300 dólares por el Servidor de Seguridad y 25 dólares al mes por concepto de monitoreo del mismo, valor que al año suma 300 dólares al año. Esto quiere decir, que la empresa que adopte nuestra solución, el primer año deberá invertir 600 dólares, lo cual es lo mínimo que esta invierte al año en seguridad, pero, a partir del segundo año, dicha empresa gastará tan solo 300 dólares por el mismo concepto, lo cual implica un ahorro del 50% con respecto a la inversión mínima que dichas empresas actualmente realizan.

El ahorro substancial de recursos, el mayor nivel seguridad y compatibilidad que nuestra solución brinda, sumadas a la necesidad actual de las empresas de reducir costos, nos indican que claramente existe un mercado lleno de posibilidades para nuestra solución, y, si la tendencia de la ciudad en la que fue realizado este estudio es, según la percepción general de los empresarios encuestados parece indicar, similar para otras ciudades, entonces podríamos afirmar que nuestra solución es aplicable no sólo a nivel local, sino que también a nivel nacional, lo cual podría crear un mercado totalmente nuevo de Soluciones de Seguridad orientadas a la pequeña y mediana Empresa e Industria.

Nuestra solución pretende romper efectivamente el paradigma actual con respecto a Soluciones de Seguridad, de que a mayor inversión, se presentan menos problemas, y de que sólo las empresas e industrias más lucrativas tienen acceso a soluciones de seguridad verdaderamente efectivas que las vuelvan más productivas. Al destruir este paradigma, todas las empresas e industrias, sin importar su tamaño, podrán ser igual de competitivas, informáticamente hablando.

## 5.2 LIMITACIONES DEL ESTUDIO

El presente estudio está hecho con el objetivo de ofrecer los servicios sólo dentro de la ciudad en donde este fue realizado, pero, con algo más de tiempo y recursos para efectuar la investigación, es posible expandir la investigación a otras regiones del país.

Otro aspecto que no se tomó en cuenta fue la realización de prototipos para sectores de menor actividad económica que podrían hacer uso de nuestra solución, como es el caso de los comerciantes minoristas, pero, al ya existir soluciones en el mercado que apuntan a esos sectores en específico, y, a causa de no poseer más recursos para investigación, no se efectuó.

## 5.3 RECOMENDACIONES

Para futuras investigaciones es recomendable invertir más en equipos para mejorar los prototipos actuales, esto con el objetivo de fabricar Servidores más económicos que sean capaces de brindar las mismas prestaciones que los actuales.

Además se recomienda hacer revisiones a futuro de los gastos en los que la empresa incurre con el fin de abaratarlos y así aumentar, de ser posible, el margen de ganancia.

# BIBLIOGRAFÍA


[1]. BOUTELL : DMZ FAQ & Setup
*http://www.boutell.com/newfaq/creating/dmz.html*

[2]. ITSECURITY : Securing Firewalls
*http://www.itsecurity.com/whitepaper/pdf/firewall-service_7-07.pdf*

[3]. MICROSOFT TECHNET : OS Hardening
*http://technet.microsoft.com/es-ar/library/dd574128.aspx*

[4]. IPCOP : Features
*http://ipcop.org/index.php?module=pnWikka&tag=IPCop14xFeatures*

[5]. PFSENSE :

- Features :
  *http://www.pfsense.org/index.php?option=com_content&task=view&id=40&Itemid=43*

- Versions :
  *http://www.pfsense.org/index.php?option=com_content&task=view&id=43&Itemid=44*

- Common Deployments :
  http://www.pfsense.org/index.php?option=com_content&task=view&id=71&Itemid=81

[6]. CÁMARA DE LA PEQUEÑA INDUSTRIA DEL GUAYAS : Afiliados al 2009
*http://www.compim.net/capig/*

[7]. CISCO :

- Cisco IOS Firewall :
  *http://www.cisco.com/en/US/products/sw/secursw/ps1018/index.html*

- Cisco ASA 5500 Series Firewall :
  *http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/prod_brochure0900aecd8048dba8.html*

- Cisco 3800 Series Integrated Services Routers :
  *http://www.cisco.com/en/US/products/ps5855/index.html*

- Cisco 2800 Series Integrated Services Routers :
  *http://www.cisco.com/en/US/products/ps5854/index.html*

- Cisco Routing Performance :
  *http://www.cisco.com/web/partners/downloads/765/tools/quickreference/routerperformance.pdf*

[8]. WIRESHARK : About & FAQs
*http://www.wireshark.org/about.html*

[9]. SLICEHOST FORUM : PFSense vs IPCop
*http://forum.slicehost.com/comments.php?DiscussionID=3688&page=1#Item_0*

[10]. SNORT : Documentation
*http://www.snort.org/docs*