

INSTITUTO TECNÓLOGICO SUPERIOR AERONÁUTICO

CARRERA DE TELEMÁTICA

**IMPLEMENTACIÓN DE UN FIREWALL EN LOS EQUIPOS
INFORMÁTICOS DEL LABORATORIO DE INSTRUMENTACIÓN
VIRTUAL DEL ITSA**

POR:

CBOS. TÉC. AVC. ANALUISA VILLACRÉS HENRY JONNY

Trabajo de Graduación como requisito para la obtención del Título de:

TECNÓLOGO EN TELEMÁTICA

2009

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por el Sr. Cbos. Téc. Avc. ANALUISA VILLACRÉS HENRY JONNY, como requerimiento parcial a la obtención del título de TECNÓLOGO EN TELEMÁTICA.

.....
Ing. Francisco Vásquez

DEDICATORIA

Doy gracias a Dios, a mis padres y a mi familia que con amor y sacrificio, desde el lugar donde se encuentran supieron motivarme intelectual y espiritualmente para culminar mi carrera de tecnólogo y obtener un título, para con esto enfrentar la vida con seguridad y decisión.

Henry

AGRADECIMIENTO

La realización de este trabajo no hubiera sido posible sin el apoyo de todas las personas como son mi familia y amigos que siempre estuvieron brindándome su apoyo en todo momento y principalmente agradezco a Dios quien ha sabido iluminar mi camino por el sendero del bien para poder terminar con éxito una de mis metas que me propuse al principio.

Henry

ÍNDICE DE CONTENIDOS

| Contenido | Pág. |
|------------------------------------|-------------|
| Certificación | II |
| Dedicatoria | III |
| Agradecimiento | IV |
| Índice General de Contenidos | V |
| Índice General de Cuadros | IX |
| Índice General de Gráficos..... | X |
| Índice General de Figuras. | X |
| Índice General de Tablas. | XI |
| Índice General de Anexos. | XI |
| Resumen..... | 1 |
| Summary..... | 3 |
| Introducción..... | 5 |

CAPÍTULO I

EL PROBLEMA

| | |
|--------------------------------------|---|
| 1.1 Planteamiento del Problema..... | 6 |
| 1.2 Formulación del Problema | 7 |
| 1.3 Justificación e Importancia..... | 7 |
| 1.4 Objetivos..... | 8 |
| 1.4.1 General..... | 8 |
| 1.4.2 Especifico | 8 |
| 1.5 Alcance..... | 8 |

CAPÍTULO II

PLAN DE LA INVESTIGACIÓN

| | | |
|-------|--|----|
| 2.1 | Modalidad Básica de la Investigación | 9 |
| 2.2 | Tipos de Investigación | 9 |
| 2.3 | Niveles de la Investigación | 9 |
| 2.4 | Universo Población y Muestra | 10 |
| 2.5 | Métodos y Técnicas de la Investigación | 10 |
| 2.5.1 | Métodos..... | 10 |
| 2.5.2 | Técnicas | 10 |
| 2.6 | Recolección de Datos | 11 |
| 2.7 | Procesamiento de la Información..... | 12 |
| 2.8 | Análisis e Interpretación de Resultados..... | 13 |
| 2.9 | Conclusiones y Recomendaciones..... | 13 |

CAPÍTULO III

MARCO TEÓRICO

| | | |
|---------|--|----|
| 3.1 | Antecedentes de la Investigación | 14 |
| 3.2 | Fundamentación Científica | 15 |
| 3.2.1 | Optimización | 15 |
| 3.2.1.1 | Optimización de aplicaciones | 15 |
| 3.2.1.2 | Optimización de dispositivos | 15 |
| 3.2.2 | Recursos | 16 |
| 3.2.2.1 | Recursos Informáticos..... | 16 |
| 3.2.3 | Laboratorio | 16 |
| 3.2.4 | Red de computadoras | 17 |
| 3.2.5 | Firewall o Cortafuegos..... | 18 |
| 3.2.5.1 | ¿Qué es un firewall?..... | 18 |
| 3.2.5.2 | ¿Qué es una red firewall? | 19 |

| | | |
|-----------|---|----|
| 3.2.5.3 | ¿Porqué utilizar una red firewall? | 19 |
| 3.2.5.4 | Tipos de firewall | 19 |
| 3.2.5.4.1 | A nivel de red | 19 |
| 3.2.5.4.2 | A nivel de aplicación | 20 |
| 3.2.5.5 | Beneficios de los firewall | 20 |
| 3.2.5.6 | Como funciona un sistema firewall..... | 21 |
| 3.2.5.7 | Inconvenientes de un firewall | 21 |
| 3.2.5.8 | Bases para el diseño de un firewall..... | 21 |
| 3.2.5.9 | Políticas de un firewall..... | 22 |
| 3.2.5.10 | Firewall Kerio..... | 22 |
| 3.2.5.11 | Firewall de Windows XP..... | 24 |
| 3.2.5.12 | Firewall Windows Vista..... | 25 |
| 3.2.6 | Virus Informáticos..... | 25 |
| 3.2.6.1 | ¿Qué ocurre con los virus Informáticos? | 26 |
| 3.2.6.2 | ¿Cómo se producen las infecciones Informáticas? | 26 |

CAPÍTULO IV

EJECUCIÓN DEL PLAN METODOLÓGICO

| | | |
|-------|---|----|
| 4.1 | Modalidad Básica de la Investigación | 27 |
| 4.2 | Tipos de Investigación | 27 |
| 4.2.1 | Niveles de Investigación..... | 28 |
| 4.3 | Universo, Población y Muestra. | 28 |
| 4.4 | Métodos y técnicas de la investigación..... | 30 |
| 4.4.1 | Métodos..... | 30 |
| 4.4.2 | Técnicas..... | 31 |
| 4.5 | Recolección de datos..... | 32 |
| 4.6 | Procesamiento de la información..... | 33 |
| 4.7 | Conclusiones y Recomendaciones..... | 37 |
| 4.8 | Denuncia del tema..... | 38 |

CAPÍTULO V

FACTIBILIDAD

| | | |
|-------|---------------------------------------|----|
| 5.1 | Análisis de la situación actual..... | 39 |
| 5.2 | Alternativa de solución. | 40 |
| 5.3 | Determinación de la factibilidad..... | 40 |
| 5.3.1 | Técnica..... | 40 |
| 5.3.2 | Económica..... | 41 |
| 5.3.3 | Operativa..... | 43 |
| 5.3.4 | Legal..... | 44 |
| 5.3.5 | Apoyo. | 44 |
| 5.4 | Recursos | 44 |
| 5.5 | Presupuesto. | 45 |

CAPÍTULO VI

DESARROLLO DEL TEMA

| | | |
|---------|--|----|
| 6.1 | Listado de requerimientos no funcionales. | 47 |
| 6.2 | Manual de Usuario. | 49 |
| 6.2.1 | Instalación del firewall. | 49 |
| 6.2.2 | Configuración del firewall. | 51 |
| 6.2.2.1 | Ventana general. | 52 |
| 6.2.2.2 | Ventana de seguridad de red. | 53 |
| 6.2.2.3 | Ventana de Instrucciones. | 55 |
| 6.3 | Prueba de caja negra. | 58 |
| 6.4 | Informe de la fase de pruebas..... | 59 |
| 6.5 | Informe de aceptación de usuarios. | 59 |

CAPÍTULO VII

CONCLUSIONES Y RECOMENDACIONES

| | |
|------------------------------------|----|
| 7.1 Conclusiones..... | 60 |
| 7.2 Recomendaciones..... | 60 |
| BIBLIOGRAFÍA. | 62 |
| ABREVIATURAS. | 64 |
| GLOSARIO DE TÉRMINOS. | 65 |
| CRONOGRAMA. | 67 |

ÍNDICE DE CUADROS

| | | |
|-------------|--|----|
| Cuadro 4.1 | Número de estudiantes que facilitarán la información sobre la situación actual del Laboratorio de Instrumentación Virtual..... | 29 |
| Cuadro 5.1 | Características de las máquinas del Laboratorio de Instrumentación Virtual del ITSA..... | 40 |
| Cuadro 5.2 | Tiempo del investigador..... | 41 |
| Cuadro 5.3 | Costo de la hora del investigador. | 41 |
| Cuadro 5.4 | Costo mensual del investigador..... | 42 |
| Cuadro 5.5 | Costo total del investigador durante los 4 meses. | 42 |
| Cuadro 5.6 | Tiempo del asesor. | 42 |
| Cuadro 5.7 | Costo mensual del asesor. | 42 |
| Cuadro 5.8 | Costo del asesor durante los 4 meses..... | 43 |
| Cuadro 5.9 | Costo total de estudio. | 43 |
| Cuadro 5.10 | Recurso humano utilizado en el desarrollo del proyecto. | 44 |
| Cuadro 5.11 | Recurso material utilizado. | 45 |
| Cuadro 5.12 | Costo primario en el desarrollo del proyecto. | 45 |
| Cuadro 5.13 | Costo secundario en el desarrollo del proyecto..... | 45 |
| Cuadro 5.14 | Costo final del proyecto. | 46 |

ÍNDICE DE GRÁFICOS

| | | |
|-------------|--|----|
| Gráfico 4.1 | Porcentaje de los resultados de la pregunta 1 en la encuesta realizada. | 33 |
| Gráfico 4.2 | Porcentaje de los resultados de la pregunta 2 en la encuesta realizada. | 34 |
| Gráfico 4.3 | Porcentaje de los resultados de la pregunta 3 en la encuesta realizada. | 35 |
| Gráfico 4.4 | Porcentaje de los resultados de la pregunta 4 en la encuesta realizada. | 36 |

ÍNDICE DE FIGURAS

| | | |
|-------------|---|----|
| Figura 3.1 | Ejemplo de una red firewall. | 19 |
| Figura 3.2 | Firewall Kerio. | 23 |
| Figura 3.3 | Ventana de notificación del firewall kerio. | 24 |
| Figura 6.1 | Inicio de instalación del programa. | 49 |
| Figura 6.2 | Dirección del destino en el que se instalara el programa. | 50 |
| Figura 6.3 | Tipo de instalación simple o avanzada. | 50 |
| Figura 6.4 | Cuadro de configuración del firewall. | 51 |
| Figura 6.5 | Ventana de configuración del firewall. | 52 |
| Figura 6.6 | Estadísticas que muestra el firewall. | 52 |
| Figura 6.7 | Colocación de la clave de acceso. | 53 |
| Figura 6.8 | Parámetros del firewall en la conexión. | 54 |
| Figura 6.9 | Reglas predefinidas por el cortafuego. | 54 |
| Figura 6.10 | Colocación de la IP en el firewall. | 55 |
| Figura 6.11 | Como poner la IP en el firewall. | 55 |
| Figura 6.12 | Instrucciones de configuración del firewall. | 56 |
| Figura 6.13 | Configuración de las opciones de cada opción a ejecutarse. | 56 |
| Figura 6.14 | Ejecución de las reglas para cada aplicación. | 57 |
| Figura 6.15 | Editar una regla a través del edit. | 57 |
| Figura 6.16 | Ejemplo de la prueba de caja negra. | 58 |

ÍNDICE GENERAL DE TABLAS

| | |
|--|----|
| Tabla 4.1 Resultado de la pregunta 1, de la encuesta realizada a los estudiantes de la carrera de electrónica..... | 33 |
| Tabla 4.2 Resultado de la pregunta 2, de la encuesta realizada a los estudiantes de la carrera de electrónica..... | 34 |
| Tabla 4.3 Resultado de la pregunta 3, de la encuesta realizada a los estudiantes de la carrera de electrónica..... | 35 |
| Tabla 4.4 Resultado de la pregunta 4, de la encuesta realizada a los estudiantes de la carrera de electrónica..... | 36 |

ÍNDICE DE ANEXOS

| | |
|---|----|
| Anexo A Observación al Laboratorio de Instrumentación Virtual..... | 69 |
| Anexo B Encuesta realizada a los Estudiantes que utilizan el Laboratorio..... | 70 |
| Anexo C Comparación de precios y características de algunos firewall..... | 71 |
| Anexo D Informe de La fase de pruebas..... | 72 |
| Anexo E Informe de aceptación de usuario..... | 73 |

RESUMEN

En la primera parte del proyecto, se hace referencia al surgimiento del problema debido a la falta de Optimización a los Recursos Informáticos en el Laboratorio de Instrumentación Virtual del ITSA, así como también de la importancia que tiene el Instituto a nivel educativo, razón por la cual todos sus talleres y laboratorios deben estar acorde con el avance tecnológico del día a día. También se habla de los objetivos generales y específicos, planteados para el desarrollo del Proyecto.

En el Capítulo II, tenemos la investigación de campo no participante porque no formamos parte del lugar donde realizamos la indagación, además utilizamos la investigación bibliográfica documental, también se utilizó la investigación no experimental, como nivel de investigación se usó la descriptiva porque fue necesario conocer el sitio del problema a investigar. Como Universo, Población y Muestra, tenemos al ITSA, carrera de electrónica y a los 49 estudiantes encuestados. Dentro de los métodos y técnicas utilizamos el análisis, síntesis, observación documental, de campo, la encuesta. Para la recolección de datos se realizó mediante la técnica de la observación y mediante la encuesta que se efectuó a los estudiantes de la carrera de electrónica; para procesar la información utilizamos el programa SPSS (Statistical Package for the Social Sciences) mismo que nos permitió realizar la tabulación de los datos obtenidos de las encuestas.

El Capítulo III esta constituido de conceptos referentes al firewall el mismo que es un sistema que impone una política de seguridad entre la organización de una red; el firewall puede ser un dispositivo físico o un software sobre el sistema operativo; además de esto contiene definiciones de una red firewall, tipos de firewall, beneficios que nos brinda el firewall ya que este nos permite definir un filtro manteniendo al margen a los usuarios no autorizados.

En el Capítulo IV se habla de la ejecución del Plan de Investigación, las técnicas ocupadas en el desarrollo del Proyecto, el resultado de las encuestas realizadas, la tabulación de los datos.

En el Capítulo V se analizó la situación actual del Laboratorio para luego realizar la determinación de la factibilidad técnica, económica, operativa, legal y apoyo.

Por último tenemos la implementación del firewall en los equipos Informáticos del Laboratorio de Instrumentación Virtual del ITSA, donde se realiza toda la ilustración necesaria para instalar el programa así como también esta explicado detalladamente y mediante figuras la configuración y funcionamiento del mismo.

SUMMARY

In the first part of the project, reference is made to the emergence of the problem due to the lack of optimization to the computer resources in the Laboratory of Virtual Instrumentation of the ITSA, as well as of the importance that has the Institute at level educational reason for the one which all its shops and laboratories should be in agreement with the technological advance of the day by day. It is also spoken of the general and specific objectives, outlined for the development of the project.

In the Chapter II, we have field non participant's investigation because we are not part of the place where we carry out the inquiry, we also use the documental bibliographical investigation, and the non experimental investigation was also used as investigation level we use the exploratory one because it was necessary to know the place of the problem to investigate. As Universe, Population and it Shows, we have the ITSA, career of electronic and to the 49 interviewed students. Inside the methods and techniques we use the analysis, synthesis, observation not participant, documental, of field, the survey. For the gathering of data she/he was carried out by means of the technique of the observation and by means of the survey that you makes the students of the career of electronic; to process the information we use the program SPSS (Statistical Package for Social the Sciences) same that allowed to be carried out the tabulation of the obtained data of the surveys.

The Chapter III this constituted of relating concepts to the firewall the same one that is a system that a politics of security imposes among the organization of a net, the firewall can be a physical device or a software on the operating system one; besides this it contains definitions of a net firewall, firewall types, benefits that it offers us since the firewall this she/he allows to be defined a filter maintaining to the margin to the not authorized users.

In the Chapter IV it is spoken of the execution of the Plan of Investigation, the techniques occupied in the development of the Project, the result of the carried out surveys, the tabulation of the data.

In the Chapter V the current situation of the Laboratory was analyzed she/he stops then to carry out the determination of the technical, economic, operative, legal feasibility and I support.

Lastly we have the implementation of the firewall in the Computer teams of the Laboratory of Virtual Instrumentation of the ITSA, where she/he is carried out the whole necessary illustration to install the program as well as this explained detailed and by means of figures the configuration and operation of the same one.

INTRODUCCIÓN

En el mundo interconectado actual, con computadoras accesibles y potentes, conexiones a Internet de alta velocidad y la diversidad de dispositivos móviles los usuarios participan de experiencias en línea enriquecida en torno a las comunicaciones; sin embargo con esta nueva interactividad surge una importante responsabilidad para garantizar que los usuarios de las computadoras confíen que su información personal se encuentra segura y privada.

La existencia de amenazas que afectan la disponibilidad, integridad y confidencial de los datos es real en nuestro País, es crítico para las organizaciones, Instituciones nacionales poder identificar estas amenazas y adoptar recomendaciones que permitan protegerse de ellas: el ataque informático puede ser por fines económicos, obtener cierto tipo de información, desmeritar el prestigio de la Institución. En ocasiones las infecciones informáticas no son detectadas debido a su naturaleza y porque el atacante, como todo intruso se cuida de no dejar huellas.

La seguridad informática en el Laboratorio de Instrumentación Virtual del ITSA no se queda atrás, razón por la cual la implementación de un firewall es prioritario, con esto se mantendrá al margen a toda actividad informática sospechosa que intente dañar en forma permanente o temporal el buen funcionamiento de los equipos informáticos del laboratorio y a la vez aprovechar al máximo los recursos que nos brindan mencionas equipos.

CAPÍTULO I

EL PROBLEMA

1.1 Planteamiento del problema

El Instituto Tecnológico Superior Aeronáutico es una institución creada para brindar servicios de carácter educativo a nivel tecnológico para alumnos civiles y militares en las Carreras de: Mecánica, Electrónica, Telemática, Logística, Seguridad Aérea y Terrestre; cabe señalar que para la formación de los estudiantes en el ámbito práctico cuenta con varios talleres y laboratorios, entre ellos se tiene el de Instrumentación Virtual, que fue creado para la aplicación práctica en el ámbito electrónico, de los conocimientos teóricos adquiridos en el aula.

Con el transcurso del tiempo y los avances tecnológicos el citado laboratorio ha venido presentando dificultades debido a la falta de Optimización de los Recursos Informáticos, lo que ha dado origen a un incorrecto inter-aprendizaje, pérdidas de tiempo, desmotivación de los estudiantes y personal que tiene relación con dicho Laboratorio.

De no darle la importancia necesaria a lo antes mencionado, los computadores seguirán funcionando con las deficiencias actuales, lo que afectaría directamente al estudiante y docentes en su proceso de inter-aprendizaje.

Por esta y muchas otras razones resulta necesaria la Optimización de los Recursos Informáticos en el Laboratorio de Instrumentación Virtual del Instituto Tecnológico Superior Aeronáutico.

1.2 Formulación del problema

¿Cómo mejorar el proceso de inter-aprendizaje, mediante la Optimización de los Recursos Informáticos en el Laboratorio de Instrumentación Virtual del Instituto Tecnológico Superior Aeronáutico?

1.3 Justificativo e Importancia

Tomando en consideración la trascendencia que tiene el Instituto Tecnológico Superior Aeronáutico dentro del ámbito educativo, es necesario que su nivel académico sea ampliamente competitivo ya que en los países desarrollados los procesos de inter-aprendizaje van de la mano con los avances tecnológicos, lo que les permite tener una ventaja competitiva frente a los países que carecen de tecnología.

Es por ello, que se debe Optimizar los Recursos Informáticos del Laboratorio de Instrumentación Virtual del Instituto Tecnológico Superior Aeronáutico, con esto se mejorará el proceso de enseñanza aprendizaje, se evitará la pérdida de tiempo, contribuirá al eficiente desempeño de las actividades académicas que en este se realizan.

Serán beneficiarios del presente trabajo de investigación, los docentes, estudiantes civiles, militares y policías de primero a sexto nivel de la Carrera de Electrónica, así como también el ITSA, que se encaminará por el sendero de su misión, que es la de formar los mejores profesionales aeronáuticos íntegros y competitivos, a través de su aprendizaje.

Por lo señalado anteriormente es prioritaria la Optimización de los Recursos Informáticos del Laboratorio de Instrumentación Virtual del Instituto Tecnológico Superior Aeronáutico, para mejorar el proceso de inter-aprendizaje en los estudiantes.

1.4 Objetivos

1.4.1 General

- Implementar el firewall Kerio que permita una seguridad de acceso al sistema informático del laboratorio de Instrumentación Virtual del ITSA.

1.4.2 Específicos

- Analizar y recopilar información referente a la situación actual del Laboratorio de Instrumentación Virtual, para la seguridad de acceso al sistema informático.
- Satisfacer las necesidades del administrador de la Red en lo referente a la seguridad informática.
- Instalar y configurar el firewall Kerio en las computadoras del Laboratorio.
- Comprobar el funcionamiento del firewall para identificar problemas y solucionarlos.
- Indagar la situación del Laboratorio antes nombrado en lo referente a la distribución física.

1.5 Alcance

La implementación del firewall Kerio en el Laboratorio, proporcionará mejor servicio de los equipos informáticos existentes. El beneficio de esta manera será para los docentes, estudiantes civiles, militares y policías de primero a sexto nivel de la Carrera de Electrónica, así como también al ITSA, que se encaminará por el sendero de su misión.

CAPÍTULO II

PLAN DE LA INVESTIGACIÓN

El presente plan de investigación ayudará a recopilar información precisa y detallada de los tipos de firewall ayudará analizar la situación actual del Laboratorio de Instrumentación Virtual del ITSA, lo que permitirá conocer con claridad las necesidades del administrador de la re en lo que se refiere a la seguridad informática.

2.1 Modalidad Básica de la Investigación

Se utilizará como modalidad básica, la investigación de campo no participante, ya que no se forma parte del lugar donde se realizará la investigación. Esta nos permitirá tener una visión más amplia sobre la situación vigente de los recursos informáticos del laboratorio.

Además se empleará la investigación bibliográfica documental, porque se indagará en libros, Proyectos de Grado e Internet con la finalidad de obtener información real y actualizada sobre firewalls, lo que servirá de base para el Marco Teórico.

2.2 Tipos de investigación

Igualmente se utilizará la investigación no Experimental porque las variables no pueden ser intervenidas, por lo que es necesario hacer una identificación clara de las causas y efectos que provocan el problema.

2.3 Niveles de Investigación

Se usará el nivel de investigación descriptiva ya que ayudará a analizar claramente la situación del problema de estudio. Es decir cuáles son y cómo

se manifiestan determinados fenómenos o procesos en el Laboratorio antes mencionado, referente a la Optimización de los Recursos Informáticos.

2.4 Universo, población y muestra

Para conseguir información convincente se tomará en consideración a todos los estudiantes civiles, militares y policías del tercer, cuarto, quinto y sexto nivel de la Carrera Electrónica, constituyéndose en la población de estudio para lo cual se hará uso de una fórmula probabilística (Ver Página 30), que permitirá obtener una muestra exacta de quienes van a ser encuestados.

2.5 Métodos y Técnicas de la Investigación

2.5.1 Métodos

Análisis

Se hará uso del método de análisis, mismo que permitirá desintegrar o descomponer el objeto de estudio en sus partes y de esta forma interpretar en forma ordenada cada uno de sus elementos, así como las relaciones entre sí y con el todo.

Síntesis

Además, se hará uso de la síntesis para que en la reunión de varios elementos dispersos se pueda obtener las partes más importantes y posteriormente sacar las conclusiones.

2.5.2 Técnicas

También se hará uso de las técnicas de observación y la encuesta, las cuales ayudarán a obtener información, que servirá de base sustentable para el desarrollo de la investigación.

Mediante el uso de los siguientes tipos:

Observación Documental

Permitirá la revisión documental bibliográfica que ayudará a un desarrollo sustentable del marco teórico.

Observación de campo

Se realizará en el Laboratorio de Instrumentación Virtual del ITSA, lugar en el que se producen los hechos.

La encuesta

Se empleará esta técnica de investigación, por que ayudará a recolectar información mediante el uso de cuestionarios, los cuales estarán propiamente estructurados mediante preguntas de estimación.

2.6 Recolección de datos

Para la investigación se tomará dos recursos (primarios y secundarios), para la recolección de los datos.

Los primarios se obtendrán por medio de la técnica de la observación, por ser fundamental en todos los campos de la ciencia. La observación consistirá en el uso sistemático de los sentidos lo cual permitirán captar la realidad de lo que está sucediendo con el Laboratorio de Instrumentación Virtual del Instituto Tecnológico Superior Aeronáutico. Estos datos surgirán del contacto directo con la realidad, es decir que serán obtenidos de una interacción con las personas y hechos en el sitio de la investigación.

Esta realidad se lo organizará de tal forma que pueda tener un panorama claro de la orientación al problema de investigación y como proponer una

solución a los inconvenientes presentado en el Laboratorio de Instrumentación Virtual del ITSA.

Los datos secundarios se obtendrán por medio de las encuestas y proyectos. La encuesta será específicamente a los encargados del Laboratorio y al personal que estuviese relacionado directa o indirectamente con este problema, esto será con el propósito de determinar los antecedentes y saber la situación actual de los recursos informáticos en el Laboratorio de Instrumentación Virtual del ITSA. Los proyectos son otros datos secundarios, los cuales estarán previamente compilados y organizados por sus respectivos autores. Esta investigación de proyectos realizados anteriormente en la Optimización de Recursos Informáticos, se hará con el objetivo de conocer quienes fueron los autores de estos proyectos, en que lugar lo realizaron, que material utilizaron y otros datos que a su momento se requiera.

Si los datos obtenidos durante la indagación del problema no son los suficientes para concluir con esta investigación se procederá a otra clase de ayuda la cual servirá para concluir exitosamente la investigación del proyecto.

2.7 Procesamiento de la información

Una vez obtenida toda la información se realizará el procesamiento de los datos de la siguiente forma:

En la observación se procederá a analizar los datos más importantes que contribuyan al direccionamiento del proyecto a efectuar.

Los datos obtenidos de los Proyectos de Optimización de Recursos Informáticos realizados para el Instituto Tecnológico Superior Aeronáutico se procederán a colocarlos en los antecedentes del proyecto, ya que es aquí donde se requiere esta información.

También utilizaremos el software SPSS (Statistical Package for the Social Sciences), mismo que nos permitirá la tabulación de los datos obtenidos de las encuestas mediante gráficos.

2.8 Análisis e Interpretación de los resultados

Para el análisis e interpretación de los resultados obtenidos en la investigación, se utilizarán tabulaciones mediante gráficos estadísticos y demostrativos de una forma clara dependiendo de los resultados del proceso de los datos.

2.9 Conclusiones y Recomendaciones

Las conclusiones se obtendrán individualmente con temas que tengan algo en común, para luego realizar las conclusiones generales que es donde se determinará el tema.

La recomendación se la hará en aquellas instancias en donde el problema de investigación no sea aplicable o en aquellos temas que representen un impedimento para la conclusión del proyecto, por ejemplo la factibilidad económica y técnica.

CAPÍTULO III

MARCO TEÓRICO

3.1 Antecedentes de la Investigación

Los antecedentes que se han tomado como referencia para la realización de este trabajo investigativo, son de Proyectos de Grado realizados en el Instituto Tecnológico Superior Aeronáutico, así como también de otras entidades que a continuación se detallan.

- Proyecto de Grado presentado por el Sr. Bravo Pachucho Jorge, cuyo tema es “CONFIGURACIÓN DE UN FIREWALL PARA LA ADMINISTRACIÓN DEL CONTROL DE ACCESO A INTERNET EN EL INSTITUTO TECNOLÓGICO SUPERIOR AERONÁUTICO”, el aporte de este proyecto al presente trabajo de investigación es dotar al investigador de una cantidad de conocimientos generales de la utilización de los firewall.
- Proyecto de Grado presentado por la Srta. María del Carmen Erazo, cuyo tema es “DISEÑO E IMPLANTACIÓN DE SEGURIDADES LÓGICAS EN REDES INALAMBRICAS DE DATOS FIJAS EN LOS LABORATORIOS DE LA FACULTAD DE SISTEMAS E INFORMÁTICA DE LA ESCUELA POLITÉCNICA DEL EJERCITO”, la información de este proyecto ayudó en la comprensión de los diversos firewall que se podría utilizar en nuestro problema.

3.2 Fundamentación Científica

Para ampliar la fundamentación científica y obtener las bases necesarias que respalden la presente investigación, se va a realizar un compendio de información de textos e Internet, relacionados con el tema.

3.2.1 Optimización¹

La optimización desde el punto de vista informático, es el proceso de mejorar el rendimiento de un sistema operativo, programa o dispositivo a partir de determinados cambios lógicos (software) o físicos (hardware).

El concepto optimización es muy amplio y abarca, optimización de aplicaciones, optimización de recursos, optimización de redes, optimización de dispositivos, etc.

3.2.1.1 Optimización de aplicaciones

Optimizar una aplicación es hacer algunos cambios, para que sea más eficiente, confiable, y además para que esta ocupe menos espacio en memoria.

La mejor optimización que puede hacerse a una aplicación es mediante un código fuente (cambios en las sentencias de programación).

3.2.1.2 Optimización de dispositivos

Se lo puede realizar a nivel de hardware o software, pero también se lo puede hacer paralelo a su rutina, es decir la optimización puede estar relacionada con el uso del propio usuario.

¹ <http://www.desarrolloweb.com/articulos/513.php>

3.2.2 Recursos

Conjunto de personas, bienes materiales o técnicos con que cuenta una dependencia u organización para alcanzar sus objetivos y producir los bienes o servicios que son de su competencia.

3.2.2.1 Recursos Informáticos

Son todos aquellos componentes de Hardware y Software que son necesarios para el buen funcionamiento y la optimización del trabajo con ordenadores y periféricos, tanto a nivel individual y colectivo u organizacional.

Por defecto en un hogar no se tendría las mismas necesidades que en una empresa. Un hogar tendría suficiente con un PC, una impresora, Conexión a Internet, Sistema Operativo y sus aplicaciones (Office, Antivirus) además de un acceso único a todos estos sistemas. Pero cuando hablamos de los Recursos Informáticos en una empresa, entran en juego mucho más factores que los señalados anteriormente como por ejemplo la inversión económica que se hace con ellos.

3.2.3 Laboratorio

Es un lugar equipado con diversos instrumentos de medida o equipos donde se realizan experimentos o investigaciones diversas, según la rama de la ciencia a la que se designe. También puede ser una aula o dependencia de cualquier centro docente acondicionada para el desarrollo de clases prácticas relacionadas con la enseñanza.

Su origen data del siglo XIX que es aquí donde se construyeron los primeros laboratorios semejantes a los existentes en la actualidad, con bancos, armarios.

En la actualidad tanto la disposición de los bancos como la distribución en ellos de los servicios y los sistemas de seguridad son muy diferentes según el tipo de laboratorio.

Su importancia sea en investigaciones o en cualquiera de sus trabajos, radica en el hecho de que las condiciones ambientales están controladas y normalizadas de modo que:

- Se puede asegurar que no se produzcan influencias extrañas que alteren el trabajo de estudio o experimento.
- Se garantice que el trabajo realizado sea repetible, obteniendo el mismo resultado como es el caso del Laboratorio de Instrumentación Virtual en el cual los trabajos realizados son confiables y garantizados.

3.2.4 Red de computadoras

Conjunto de técnicas, conexiones físicas y programas informáticos empleados para conectar dos o más ordenadores o computadoras con el fin de comunicarse, transmitir datos entre ellas y compartir los recursos.

Funciones

Es la de establecer, conducir y finalizar la comunicación de datos entre dos o más computadoras.

Beneficios

Los beneficios que tenemos al crear una red son los siguientes:

- Acceso simultáneo a programas e información.
- Equipos periféricos compartidos.

- Proceso de respaldo más efectivo.

3.2.5 Firewall o Cortafuegos

Es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de una red privada y el Internet. “El firewall determina cual de los servicios de red pueden ser accedidos dentro de esta por los que están afuera, es decir quien puede entrar a utilizar sus recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información; el firewall podrá únicamente autorizar el paso de información y será inmune a la penetración.”² Desafortunadamente este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.

3.2.5.1 ¿Qué es un Firewall?

Es un dispositivo que filtra el tráfico entre redes. El firewall puede ser un dispositivo físico o un software sobre un sistema operativo, en este Proyecto se implementará un firewall el cual se configurará bajo el mismo Sistema Operativo Instalado en las máquinas del laboratorio; en general se verá como una caja con dos o mas interfaces de red en la que se establecen una regla de filtrado con las que se decide si una conexión determinada puede establecerse o no. Incluso puede ir más allá de realizar modificaciones sobre las comunicaciones. Esta sería la definición genérica, hoy en día un firewall es un hardware específico con un sistema operativo que decide si un paquete pasa, se modifica, se convierte o se descarta. Para que un firewall entre redes funcione como tal deben tener al menos dos tarjetas de red; esta sería la topología clásica de un firewall.

² Tesis 104 Telemática

3.2.5.2 ¿Qué es una red firewall?

Es aquel sistema o conjunto combinado de sistemas que crean una barrera segura entre 2 redes, (Ver figura 3.1).

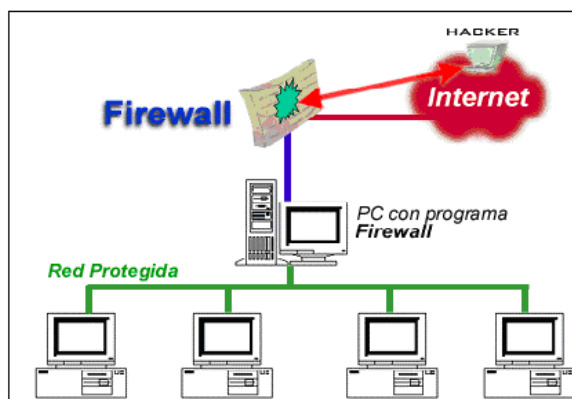


Figura 3.1 Ejemplo de una red firewall

3.2.5.3 ¿Por qué utilizar una red firewall?

El propósito de una red firewall es dar una seguridad a nuestros equipos conectados en red evitando así que las computadoras sean vulnerables a los virus informáticos.

3.2.5.4 Tipos de firewall ³

3.2.5.4.1 A Nivel de Red

Toman decisiones según su dirección de procedencia, dirección de destino y puerto de cada uno de los paquetes IP.

Los actuales cortafuegos de nivel de red permiten mayor complejidad a la hora de decidir; mantienen información interna acerca del estado de las conexiones que pasan por el, los contenidos de algunos datos. Estos sistemas, como es lógico han de tener una

³ http://www.angelfire.com/electronic2/ronald_melara/FireWall2.html

dirección IP válida. Este tipo de firewall ocupa la capa 3 del modelo OSI (Open System Interconnection) que es la Interconexión de sistemas abiertos, la cual se ocupa de la transmisión de paquetes y de encaminarlos cada uno en la dirección adecuada, pero no se ocupa para nada de la pérdida o errores de los de los datagramas⁴.

3.2.5.4.2 A Nivel de Aplicación

Generalmente son Host con servidores Proxy, que no permiten el tráfico directamente entre dos redes, sino que realizan un seguimiento detallado del tráfico que pasa por él. Estos tipos de firewall pueden ser usados como traductores de red, según pasa el tráfico de un lugar a otro.

3.2.5.5 Beneficios de los firewall

- Permiten al administrador de la red definir un filtro, manteniendo al margen a los usuarios no autorizados (hackers, crackers⁵, espías), protegiendo potencialmente la entrada o salida de aplicaciones.
- Un firewall ofrece un punto donde la seguridad puede ser monitoreada y si aparece alguna actividad sospechosa, este generará una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el tránsito de los datos.

Debido a todo lo anterior, “un firewall” más “actualizaciones periódicas del software” más “responsabilidad” hace que un conjunto hagan una gran defensa para conexiones en red o individuales.

⁴ http://www.zator.com/Hardware/H12_2.htm

⁵ Jose A. Carvaller (2006) “Firewall Seguridad de la Banda Ancha”, México.

3.2.5.6 Como funciona un sistema firewall

Un sistema firewall contiene un conjunto de reglas predeterminadas que le permiten al sistema.

- Autorizar la conexión (permitir).
- Bloquear la conexión (denegar).
- Rechazar el pedido de conexión sin informar al que lo envió (negar).

3.2.5.7 Inconvenientes de un firewall

Normalmente el firewall detecta que programas quieren comunicarse a través de un determinado puerto y lo que hace es preguntar al usuario si desea permitirlo.

De esto deducimos dos inconvenientes del firewall:

- El usuario tiene la responsabilidad de decidir cuidadosamente que programas permitimos comunicarse y cuales no. Esto requiere un pequeño mantenimiento y esfuerzo del usuario.
- Cuando se permite a un programa utilizar un puerto, recae sobre este programa la responsabilidad de evitar cualquier ataque de seguridad a través de él.

3.2.5.8 Bases para el diseño de un firewall

Cuando se diseña un firewall de Internet, se tiene que tomar algunas decisiones que pueden ser asignadas por el administrador de red:

- La política interna propia de la organización para la seguridad total.
- El aspecto económico al momento de implementar un firewall dentro de una empresa.

3.2.5.9 Políticas de un firewall

Las actitudes del sistema firewall describen la filosofía fundamental de la seguridad de la organización. Estas dos posturas son diametralmente opuestas de la política de un firewall de Internet puede tomar:

- “No todo lo específicamente permitido esta prohibido”
- “No todo lo específicamente prohibido esta permitido”

La primera postura asume que un firewall puede obstruir todo el tráfico y cada uno de los servicios o aplicaciones deseadas necesariamente para ser implementadas básicamente caso por caso.

La segunda asume que el firewall puede desplazar todo el tráfico y que cada servicio potencialmente peligroso necesitara ser aislado básicamente caso por caso. Esta propuesta crea ambientes más flexibles al disponer mas servicios para los usuarios de la comunidad, además, el administrador de la red está en capacidad de incrementar la seguridad en el sistema.

Como es el caso del firewall que instalaremos en las máquinas del laboratorio antes mencionado, el cual inmediatamente después de ejecutar una aplicación nos permite la opción de autorizar, denegar o bloquear cierta ejecución.

3.2.5.10 Firewall Kerio⁶

Es una aplicación pensada tanto para principiantes como para usuarios más avanzados que deseen controlar la seguridad de su PC para evitar que un usuario o un equipo remoto acaben con la estabilidad del Sistema Operativo, (Ver figura 3.2).

⁶ http://www.ciao.es/Kerio_personal_firewall__Opinion_1102133



Figura 3.2 Firewall Kerio

Este firewall evita troyanos, accesos no autorizados a la red, entrada de archivos no deseados; mediante una sencilla configuración el administrador de la red pueden decidir que aplicación permitir, denegar, bloquear.

Además con este firewall podemos restringir sitios Web en caso de que fuera necesario, un ejemplo de esto son: páginas pornográficas, Chat.

Su instalación es muy sencilla, permite elegir en que lugar del disco instalar; tiene dos modos de instalación simple o avanzada.

Ventajas del firewall kerio

- Excelente interfaz gráfica.
- Completo tutorial de ayuda.
- Fácil de Instalar y configurar.

Desventaja del Firewall

- Manual de usuario en Inglés

Bloqueo de Tráfico con el firewall Kerio

Las primeras alertas aparecen aun sin estar conectados a Internet, este es el caso del Laboratorio de Instrumentación Virtual el mismo que no cuenta con el servicio de Internet.

Por ejemplo cuando un programa solicita la ejecución de otro, inicio de una aplicación, en cualquiera de estos casos se detalla qué aplicación se abre y a causa de quien, (Ver figura 3.3).

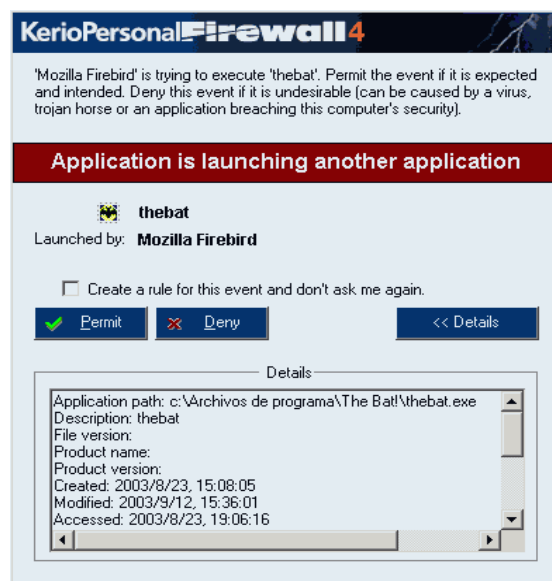


Figura 3.3 Ventana de notificación del firewall kerio

3.2.5.11 Firewall de Windows XP⁷

El firewall que viene incluido en la instalación de Windows XP Service Pack 2 (SP2), ha sido muy mejorado. Las anteriores versiones de Windows XP, incluso Windows 2000 era un firewall muy simple que realmente no tenían ninguna utilidad.

⁷ http://www.principiantes.info/seguridad/guia_firewall.php

Una limitación importante de este firewall es que solo controla los paquetes que llegan a nuestro ordenador y no los que se envían. Es importante saber que por defecto todos los programas están bloqueados.

Cuando ejecutamos un programa y este va a recibir datos desde el Internet, el firewall nos permite inmediatamente autorización, entonces podemos optar por “Desbloquear” o “Continuar bloqueado”.

3.2.5.12 Firewall Windows Vista

El firewall del Windows Vista viene configurado como el del XP. Es decir controla las aplicaciones de entrada, pero de las salidas no tiene ningún control.

3.2.6 Virus informáticos⁸

Son programas generalmente destructivos, que se introducen en el ordenador (al leer un dispositivo extraíbles o al ingresar a una red de Internet), que pueden provocar la pérdida de información almacenada en el disco duro o el mal funcionamiento del ordenador.

Las mayores incidencias se dan en el Sistema Operativo Windows debido a:

- Su gran popularidad entre los ordenadores personales, este gran renombre basado en la facilidad de uso sin conocimiento previo.
- Falta de seguridad en esta plataforma por lo cual Microsoft está dando en los últimos años mayor prioridad.

Lo importante es mantener protegida a la computadora (Antivirus, Firewall), una vez infectada la computadora con un virus la primera necesidad es eliminarlo sin tomar en cuenta el tipo o método de infección.

⁸ http://es.wikipedia.org/wiki/Virus_inform%C3%A1tico

3.2.6.1 ¿Qué ocurre con los virus informáticos?

Las redes firewall no pueden proteger muy bien contra los virus. Hay demasiados modos de codificación binaria de ficheros para transmitirlos a través de la red y también son demasiadas las diferentes arquitecturas y virus que intentan ingresar a través de ellas.

En el tema de los virus, la mayor responsabilidad recae como casi siempre en los usuarios de la red, los cuales deberían tener gran control sobre los programas que ejecutan y donde se ejecutan.

3.2.6.2 ¿Como se producen las infecciones informáticas?

Existen dos grandes clases de producir las infecciones:

- Los virus informáticos se difunden cuando las instrucciones o código ejecutable pasan de un ordenador a otro, o por medio de un dispositivo (diskette, flash memory).

Los virus funcionan, se reproducen y liberan sus cargas activas cuando se ejecutan, normalmente un usuario no ejecuta concientemente un código informático sin embargo los virus engañan concientemente al sistema operativo o al usuario informático para que ejecute el programa viral⁹.

- El programa malicioso actúa replicándose a través de las redes como es el caso de los gusanos informáticos.

⁹ Marcus Gocalves (2002) "Manual de Firewalls", México.

CAPÍTULO IV

EJECUCIÓN DEL PLAN DE INVESTIGACIÓN

En este punto se realizó la ejecución de todo el plan metodológico que se propuso, lo que ha permitido tener un conocimiento especificado y global del problema planteado.

4.1 Modalidad básica de la investigación

Se utilizó la investigación de campo no participante, con la cual se pudo acudir varias veces al sitio donde se originó el problema, lo que nos ayudó a saber que el Laboratorio actualmente cuenta con ocho computadores que no están conectados en red, no cuentan con un sistema de seguridad informática, el espacio físico no se encuentra bien distribuido, y que el control del uso de los mismos es realizado por parte del docente encargado.

Además, mediante la investigación bibliográfica documental, se logró recopilar información valiosa sobre los distintos tipos de firewall que existen y que pueden ayudar a la optimización de recursos informáticos en un laboratorio. Esta también se utilizó en la estructura del marco teórico, y fue realizada mediante el uso de la consulta en libros¹⁰, Proyectos de Grado (Ver Pág. 14), de las bibliotecas de la ciudad de Latacunga (ESPEL e ITSA), así como también se obtuvo información del Internet (Bibliografía).

4.2 Tipos de Investigación

Se utilizó la investigación no experimental, con la cual se pudo conocer que los problemas suscitados (ingreso de virus, mal uso de los máquinas, insatisfacción por parte de los estudiantes y docentes, uso de programas ajenos a la actividad que este se realiza) en el Laboratorio de Instrumentación

¹⁰ Carvallar Falcón José. (2006) "Firewall Seguridad de la Banda Ancha.
Bruce Alexander (2005) "Manual de Redes". Espel Latacunga.
Chapman David W. y Fox Andy (2002) "Firewall PIX de Cisco", Madrid.

Virtual del ITSA por la falta de Optimización de sus ordenadores se deben a la inexistencia de un sistema

de control informático que permita establecer reglas de uso, instalación de software, control de virus, además de la falta de un mantenimiento preventivo de los equipos está provocando efectos negativos en el proceso de inter-aprendizaje de los estudiantes.

4.2.1 Niveles de Investigación

Investigación Descriptiva

Gracias al empleo de este tipo de investigación se logró describir el problema, detallando situaciones y eventos, es decir: Cuáles son y cómo se manifiestan determinados fenómenos en el “Laboratorio de Instrumentación Virtual del ITSA”, tal es el caso de la inexistencia de un sistema de control mediante un software en las máquinas para su correcto uso, lo que trae consecuencias de pérdida de tiempo y deterioro de las máquinas, por el uso desmedido e inapropiado. También la inadecuada ubicación de los equipos informáticos, que no permite el correcto aprovechamiento del espacio físico. La falta de una conexión en red entre las computadoras, que trae consigo un desperdicio de recursos. La falta de capacitación al personal encargado del laboratorio, que genera inconformidad de parte del alumnado; así como también la falta de un mantenimiento preventivo a los computadores.

4.3 Universo, Población y Muestra

Universo

Es el Instituto Tecnológico Superior Aeronáutico.

Población

De la cual se extrajo la información necesaria para realizar la investigación fue de 112 estudiantes de la Carrera de Electrónica, de los niveles tercero, cuarto, quinto, sexto, así como también de 2 de sus docentes lo que constituyó

en el estudio una población total de 114, entre estudiantes y docentes, (Ver Cuadro 4.1).

Cuadro 4.1 Número de estudiantes que facilitarán la información sobre la situación actual del Laboratorio de Instrumentación Virtual del ITSA.

| NIVEL | No DE ALUMNOS |
|--------------|---------------|
| TERCERO | 27 |
| CUARTO | 22 |
| QUINTO | 29 |
| SEXTO | 34 |
| DOCENTES | 02 |
| TOTAL | 114 |

Fuente: Secretaria Académica ITSA

Realizado por: Cbos. Analuisa Henry

Muestra

En la investigación a desarrollar, la población se clasificó en dos grupos, estudiantes y docentes, tomando en cuenta que los 2 Docentes de la Carrera de Electrónica del ITSA, pertenecen a una población finita, por lo cual no se aplica el cálculo para determinar el tamaño de la muestra.

Con relación a la población de los estudiantes es un total de 112, siendo esta población grande se considera necesario determinar el tamaño de la muestra aplicando la siguiente fórmula:

$$n = \frac{Z \times P \times Q \times N}{[(N \mp 1)E^2] \pm (Z^2 \times P \times Q)}$$

De donde las dimensiones estadísticas son:

n = Tamaño de la muestra para que sea representativa

N = Conjunto universo

PQ = 0.25 x N Constante que representa la cuarta parte del universo.

Z = 96% = 1.96 Desviación estándar.

$N - 1 =$ Constante de corrección para cálculo de muestras grandes

$E =$ (0.01 al 0.05 %: o sea entre 1 y 5 %) Error admisible.

$$n = \frac{Z \times P \times Q \times N}{[(N \mp 1)E^2] \pm (Z^2 \times P \times Q)}$$

$$n = \frac{(1.96)^2 \times 0.5 \times 0.5 \times 112}{(112 - 1)(0.05)^2 \pm (1.96)^2 (0.5^2)}$$

$$n = \frac{3.8 \times 0.25 \times 112}{(111 \times 0.0025) \pm (3.8 \times 0.25)}$$

$$n = \frac{107.52}{1.2375}$$

$$n = 86.8$$

Aplicando el factor de corrección:

$$n' = \frac{n}{1 \pm [(n-1) \div N]}$$

$$n' = \frac{86.8}{1 \pm [(86.8 - 1) \div 112]}$$

$$n' = \frac{86.8}{1.77}$$

$$n' = 49$$

Esta fórmula ayudó a determinar con exactitud el número de estudiantes a quienes se les debía realizar la encuesta, dando como resultado 49 estudiantes.

4.4 Métodos y Técnicas de la Investigación

4.4.1 Métodos

Análisis

Fue necesario partir del análisis ya que permitió desglosar el problema permitiendo así verificar cuales son las causas y efectos del problema investigado, siendo el principal origen la falta de Optimización de los Recursos Informáticos del Laboratorio de Instrumentación Virtual del ITSA, lo que esta produciendo, perdida de tiempo, deficiente proceso de inter-aprendizaje, insatisfacción por parte de los estudiantes de la Carrera de Aviónica.

Síntesis

Ayudó unir todos los criterios alcanzados en el análisis y sacar una idea general como es la Optimización de los Recursos Informáticos , permitiendo llegar establecer la necesidad real del problema sin omitir nada, así como también permitió la elaboración de las conclusiones y recomendaciones del problema que se investigó.

4.4.2 Técnicas

Observación Documental

Por medio de la cual se logró obtener información de libros (Carvallar Falcón José. (2006) "Firewall Seguridad de la Banda Ancha", Goncalves Marcus (2002) "Manual de Firewalls") y Proyectos de Grado (Proyecto presentado por el Sr. Bravo Pachucho Jorge "CONFIGURACIÓN DE UN FIREWALL PARA LA ADMINISTRACIÓN DEL CONTROL DE ACCESO A INTERNET EN EL INSTITUTO TECNOLÓGICO SUPERIOR AERONÁUTICO", Proyecto presentado por la Srta. María del Carmen Erazo, "DISEÑO E IMPLANTACIÓN DE SEGURIDADES LÓGICAS EN REDES INALAMBRICAS DE DATOS FIJAS EN LOS LABORATORIOS DE LA FACULTAD DE SISTEMAS E INFORMÁTICA DE LA ESCUELA

POLITÉCNICA DEL EJERCITO”, aplicando uno de nuestros sentidos como es la vista. Este tipo de observación aportó a redactar los antecedentes de la investigación y adquirir un conocimiento global sobre el problema, además se obtuvo información del Internet¹¹, es así que se encontró un manual del firewall recomendado anteriormente, el cual está resumido en el Capítulo VI.

Observación de Campo

Ya que se efectuó en el Laboratorio de Instrumentación Virtual del ITSA y ayudó a obtener información (sobre la situación actual del lugar antes mencionado) por parte del encargado Ing. Pablo Pilatasig, el mismo que tiene relación directa con el mencionado Laboratorio, para ello se elaboró una guía de observación, (Ver Anexo A).

Además se realizó una visita a CINTY COMPU de la ciudad de Quito, donde se dialogó con el encargado de redes, el cual después de la conversación nos supo informar que lo que necesitaba el Laboratorio de Instrumentación Virtual era un Software Anticongelante, pero como su costo era elevado (1200 dólares) entonces me recomendó instalar el Firewall Kerio, el cual satisfacía la necesidad (Seguridad Informática) del Ing. Pablo Pilatasig encargado del Laboratorio.

La Encuesta

Se realizó una encuesta a los estudiantes de los niveles tercero, cuarto, quinto, y sexto de la Carrera Electrónica, a través de un cuestionario previamente estructurado, con preguntas de selección múltiple, misma que permitió obtener una idea clara sobre el criterio de los encuestados en relación a la Optimización de Recursos Informáticos del ITSA, (Ver Anexo B).

4.5 Recolección de Datos

La recolección de datos permitió identificar las fuentes de información mencionadas anteriormente, y determinar las condiciones actuales en las que se encuentran los dispositivos informáticos del Laboratorio de Instrumentación

¹¹ http://nautopia.coolfreepages.com/kerio4/kpf4_networksecurity.htm

Virtual del ITSA, como es la mala distribución física de los equipos, no poseen una seguridad informática para el uso de los mismos; esta actividad se llevó a cabo mediante las encuestas realizadas a los estudiantes y la guía de observación a los docentes de la Carrera de Electrónica.

4.6 Procesamiento de información

Este proceso conllevó a la revisión crítica de la información que se recopiló mediante los instrumentos anteriormente mencionados, descartando información contradictoria, confusa e incompleta. Una vez obtenida información primaria se procedió a su tabulación a través del programa SPSS, mediante gráficos (pasteles), que a continuación se observa.

Pregunta 1

¿Cree usted que los recursos informáticos del Laboratorio de Instrumentación Virtual del "ITSA" están siendo aprovechados adecuadamente?, (Ver Tabla 4.1).

Tabla 4.1 Resultado de la pregunta 1, de la encuesta realizada a los estudiantes de la carrera de electrónica.

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|-----------------------|-----------|--------------|---------------|--------------------|
| Valid BASTANTE | 6 | 12,2 | 12,2 | 12,2 |
| POCO | 19 | 38,8 | 38,8 | 51,0 |
| NADA | 24 | 49,0 | 49,0 | 100,0 |
| Total | 49 | 100,0 | 100,0 | |

Fuente: Investigación de campo
Realizado por: Cbos. Analuisa Henry

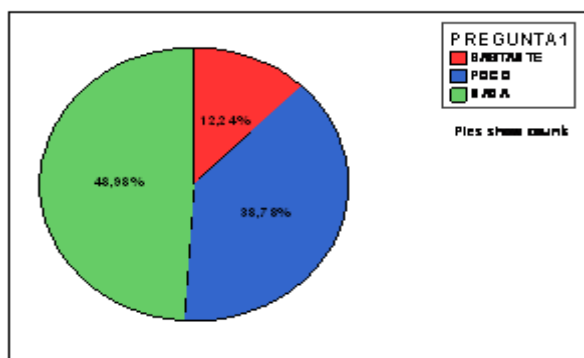


Gráfico 4.1 Porcentaje de los resultados de la pregunta 1 en la encuesta realizada.

Análisis estadístico de los datos:

El 49% es decir veinte y cuatro (24) estudiantes cree que nada de los recursos informáticos del Laboratorio de Instrumentación Virtual del "ITSA" se están siendo aprovechados adecuadamente, el 39% o sea diecinueve (19) piensa que poco, mientras que un 12%, seis (6) opina que Bastante.

Interpretación de los resultados:

La mayoría de los encuestados que representa el 49%, opina que los Recursos Informáticos del Laboratorio de Instrumentación Virtual del "ITSA" no están siendo aprovechados adecuadamente, (Ver Gráfico 4.1)

Pregunta 2

¿Piensa usted que las computadoras del Laboratorio de Instrumentación Virtual del "ITSA", necesitan tener un sistema de control para el uso adecuado de las mismas?, (Ver Tabla 4.2).

Tabla 4.2 Resultado de la pregunta 2, de la encuesta realizada a los estudiantes de la carrera de electrónica.

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|--------------|-----------|--------------|---------------|--------------------|
| Valid | Si | 26 | 53,1 | 53,1 | 53,1 |
| | No | 23 | 46,9 | 46,9 | 100,0 |
| | Total | 49 | 100,0 | 100,0 | |

Fuente: Investigación de campo
Realizado por: Cbos. Analuisa Henry

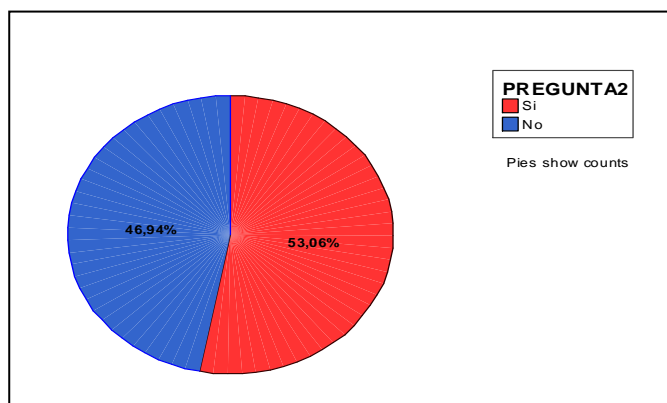


Gráfico 4.2 Porcentaje de los resultados de la pregunta 2 en la encuesta realizada.

Análisis estadístico de los datos:

Se observa en la grafica que un 53% o sea veinte y seis (26) encuestados piensa que las computadoras del Laboratorio de Instrumentación Virtual del "ITSA", si necesitan tener un sistema de control para el uso adecuado de las mismas mientras que un 47% es decir veinte y tres (23) opina lo contrario.

Interpretación de los resultados:

Según el análisis estadístico el 53% de los encuestados dice que en el Laboratorio de Instrumentación Virtual del "ITSA", debe implementarse un sistema de control para el uso adecuado de las mismas, (Ver Gráfico 4.2).

Pregunta 3

¿Considera usted que la conexión actual de los equipos informáticos del Laboratorio de Instrumentación Virtual del "ITSA" es?, (Ver Tabla 4.3).

Tabla 4.3 Resultado de la pregunta 3, de la encuesta realizada a los estudiantes de la carrera de electrónica.

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|------------------------|-----------|--------------|---------------|--------------------|
| Valid Muy buena | 18 | 36,7 | 36,7 | 36,7 |
| Buena | 13 | 26,5 | 26,5 | 63,3 |
| Deficiente | 18 | 36,7 | 36,7 | 100,0 |
| Total | 49 | 100,0 | 100,0 | |

Fuente: Investigación de campo
Realizado por: Cbos. Analuisa Henry

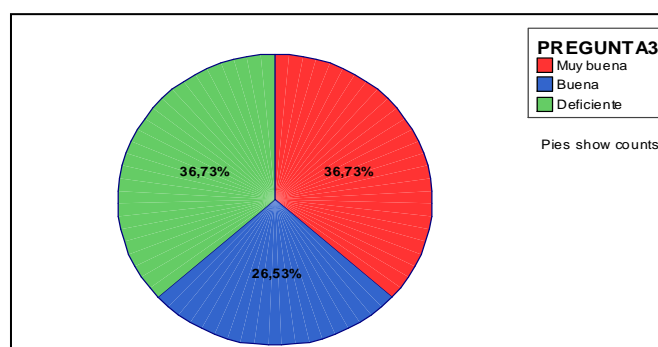


Gráfico 4.3 Porcentaje de los resultados de la pregunta 2 en la encuesta realizada.

Análisis estadístico de los datos:

Se puede ver en el gráfico que un 37% es decir dieciocho (18) encuestados considera que la conexión actual de los equipos informáticos del Laboratorio de Instrumentación Virtual del "ITSA" es Muy Buena, un 26% o sea trece (13) considera que es buena, quedando un 37% equivalente a dieciocho personas (18) que lo considera deficiente.

Interpretación de los resultados:

El 37% de los encuestados opina que la conexión actual de los dispositivos informáticos Laboratorio de Instrumentación Virtual del "ITSA" no esta en buenas condiciones, (Ver Gráfico 4.3).

Pregunta 4

¿Piensa usted que es importante realizar una reubicación de los equipos informáticos del Laboratorio de Instrumentación Virtual del "ITSA", para aprovechar eficazmente el espacio físico?, (Ver Tabla 4.4).

Tabla 4.4 Resultado de la pregunta 4, de la encuesta realizada a los estudiantes de la carrera de electrónica.

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|-----------------------------|-----------|--------------|---------------|--------------------|
| Valid Muy importante | 21 | 42,9 | 42,9 | 42,9 |
| Importante | 17 | 34,7 | 34,7 | 77,6 |
| Nada importante | 11 | 22,4 | 22,4 | 100,0 |
| Total | 49 | 100,0 | 100,0 | |

Fuente: Investigación de campo
Realizado por: Cbos. Analuisa Henry

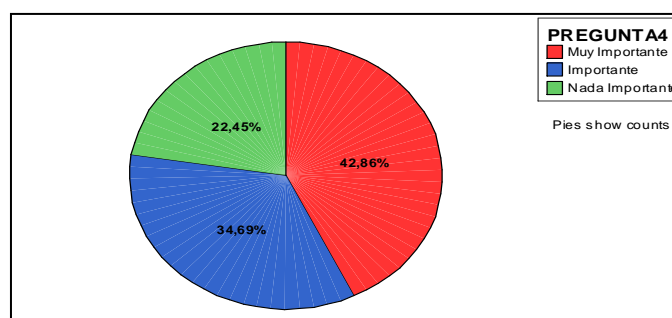


Gráfico 4.4 Porcentaje de los resultados de la pregunta 3 en la encuesta realizada.

Análisis estadístico de los datos:

El 43% equivalente a veinte y un (21) encuestados piensa que es muy importante realizar una reubicación de los equipos informáticos del Laboratorio de Instrumentación Virtual del "ITSA", para aprovechar eficazmente el espacio físico, un 35% o sea diecisiete (17) encuestados piensan que es importante, mientras que un 22% es decir a once (11) encuestados, piensan que es importante.

Interpretación de los resultados:

Según la encuesta realizada el 43% dice que los espacios del laboratorio del Laboratorio de Instrumentación Virtual del "ITSA", no están siendo aprovechados eficazmente por lo que es muy importante realizar una reubicación de los equipos informáticos, (Ver Gráfico 4.4).

4.7 Conclusiones y Recomendaciones

Conclusiones

- Se analizó y se recopiló información mediante la consulta en Proyectos de Grao, Internet, Libros, así como también mediante el uso de la encuesta.
- Se determinó que la solución al problema es la Implementación del Firewall Kerio, para la Optimización de los Recursos Informáticos del Laboratorio de Instrumentación Virtual del ITSA, para así controlar la instalación de programas no deseados (juegos, virus), restringir el a ciertas aplicaciones de la máquina (Panel de Control, Internet Explorer, Editor de Registro).
- El espacio físico del Laboratorio no se encuentra aprovechado adecuadamente.
- Por el estado en el que se observó las computadoras se notó que estas no reciben un mantenimiento preventivo periódicamente.

Recomendaciones

- Es necesario y prioritario la implementación de un firewall el cual servirá para controlar el uso de los equipos informáticos existentes en el Laboratorio de Instrumentación del ITSA, ya que actualmente las máquinas no cuentan con esta seguridad informática (Firewall).
- Colocar en red a todos los equipos existentes en mencionado Laboratorio para así optimizar sus recursos y aprovechar de mejor manera sus servicios.
- Es recomendable la reubicación de las máquinas dentro del Laboratorio para con eso aprovechar de mejor manera el espacio físico existente.
- Realizar un mantenimiento preventivo de las máquinas para así evitar el mal funcionamiento de los equipos informáticos.

4.8 Denuncia del tema

Tomando en consideración la importancia del Laboratorio de instrumentación Virtual del ITSA, en el proceso de ínter-aprendizaje de los estudiantes de la carrera de Electrónica es necesario y prioritario la **“IMPLEMENTACIÓN DE UN FIREWALL EN LOS EQUIPOS INFORMÁTICOS DEL LABORATORIO DE INSTRUMENTACIÓN VIRTUAL DEL ITSA”**

CAPÍTULO V

FACTIBILIDAD

Después de definir la problemática presente y establecer las causas que ameritan la ejecución del tema planteado, es pertinente hacer un estudio de factibilidad sobre la implementación de un sistema de seguridad informática, además de los costos, beneficios y grado de aceptación que la propuesta genera en la institución.

Este análisis permitió determinar las posibilidades de implementar el Firewall Kerio y su puesta en marcha; los aspectos tomados en cuenta para este estudio fueron clasificados en tres áreas:

- Análisis de la situación actual.
- Alternativa de solución.
- Determinación de la factibilidad.

5.1 Análisis de la situación actual

Mediante la ejecución del plan metodológico propuesto se llegó a determinar la situación actual del laboratorio de Instrumentación Virtual del ITSA; el cual se encuentra ubicado en la planta baja del Instituto Tecnológico Superior Aeronáutico, junto al laboratorio de Motores.

Este laboratorio cuenta con 8 máquinas, las mismas que en la actualidad no cuentan con un servicio de seguridad informática (firewall). Esto hace que sean vulnerables a los ataques de virus o a la instalación de programas que no corresponden a las actividades académicas que en estas se realizan afectando así el correcto funcionamiento de las mismas.

5.2 Alternativa de solución

Se propone como solución la instalación y configuración del firewall Kerio a nivel de software, en cada una de las computadoras lo que permitirá tener un mejor control en el uso de las mismas y así brindar un mejor servicio a los estudiantes y docentes que están relacionados con dicho laboratorio.

Además la adquisición de 4 mesas para colocar las computadoras en un mejor lugar y así aprovechar de mejor manera el espacio físico del Laboratorio.

5.3 Determinación de la factibilidad

5.3.1 Técnica

El Laboratorio de Instrumentación Virtual cuenta con 8 computadoras de las siguientes características, (Ver Cuadro 5.1).

Cuadro 5.1 Características de las maquinas del Laboratorio de Instrumentación Virtual del ITSA

| PC | Modelo | Procesador | Memoria RAM | Disco Duro |
|-----------|---------------|-------------------|--------------------|-------------------|
| 4 | Pentium IV | 2.6 GHz. | 1 GB | 80 GB |
| 1 | Pentium IV | 3.0 GHz. | 512 MB | 20GB |
| 3 | Celeron | 2.6 GHz | 1 GB | 80GB |

Fuente: Investigación de campo

Realizado por: Cbos. Analuisa Henry

Las mismas que basándose en las características antes mencionadas permiten la implementación del Firewall antes mencionado para controlar el correcto uso de los equipos informáticos existentes en el mencionado Laboratorio, por lo tanto es técnicamente factible y viable la instalación de dicho programa (Firewall), que se puede adquirir en el mercado informático, además cuenta con personal altamente capacitado conocedores del tema.

Para la compra del firewall se realizó un cuadro comparativo entre los distintos tipos de cortafuegos existentes en el mercado informático, (Ver Anexo C), determinando que el Firewall personal Kerio es uno de los mejores por sus características y precio.

5.3.2 Económica

Se analiza el aspecto económico, que permitirá solventar las carencias que se tenga al momento de la implementación del software, y determinar si los recursos financieros son viables para llevar a cabo la instalación de un Firewall en los equipos informáticos del Laboratorio de Instrumentación Virtual del ITSA.

El recurso económico que se necesita esta al alcance para ejecutar el proceso de implementación siguiendo la planificación establecida, razón por la cual se concluye que es económicamente factible la instalación del Firewall en las 8 computadoras del Laboratorio de Instrumentación Virtual del Instituto Tecnológico Superior Aeronáutico.

Tiempo del investigador, (Ver Cuadro 5.2).

Cuadro 5.2 Tiempo del investigador

| Horas diarias | Horas semanales | Horas mensuales |
|----------------------|------------------------|------------------------|
| 8 | 40 | 160 |

Fuente: Investigación de campo

Realizado por: Cbos. Analuisa Henry

Costo de la hora del investigador, (Ver Cuadro 5.3).

Cuadro 5.3 Costo de la hora del investigador

| Sueldo Dólares | Cálculo | Costo de la hora |
|----------------------------------|-----------------------------------|-------------------------|
| 690 (confidencial FAE) | Sueldo/Hrs.Mensuales (690/160) | 4.31 Dólares |

Fuente: Investigación de campo

Realizado por: Cbos. Analuisa Henry

Costo mensual del investigador, (Ver Cuadro 5.4).

Cuadro 5.4 Costo mensual del investigador

| Cálculo | Costo Mensual |
|--|----------------------|
| Hrs. Mensuales x Costo de la hora (160 x 4.31dólares) | 689.6 Dólares |

Fuente: Investigación de campo

Realizado por: Cbos. Analuisa Henry

Costo total del investigador durante los 4 meses de trabajo, (Ver Cuadro 5.5).

Cuadro 5.5 Costo total del investigador durante los 4 meses

| Costo mensual (dólares) | Meses de investigación | Costo total (dólares) |
|------------------------------------|-----------------------------------|------------------------------|
| 689.6 | 4 | 2758.4 |

Fuente: Investigación de campo

Realizado por: Cbos. Analuisa Henry

Tiempo del Asesor, (Ver Cuadro 5.6)

Cuadro 5.6 Tiempo del Asesor

| Tiempo del asesor (Hrs.) | Hrs. semanales | Hrs. mensuales |
|-------------------------------------|-----------------------|---------------------------|
| 1 | 3 | 12 |

Fuente: Investigación de campo

Realizado por: Cbos. Analuisa Henry

Costo mensual del asesor, (Ver Cuadro 5.7).

Cuadro 5.7 Costo mensual del Asesor

| Cálculo | Costo Mensual |
|--|----------------------|
| Hrs. Mensuales x Costo hora de un Ing. (12 x 5.50) Dólares | 66 Dólares |

Fuente: Investigación de campo

Realizado por: Cbos. Analuisa Henry

Costo del Asesor durante los 4 meses, (Ver Cuadro 5.8).

Cuadro 5.8 Costo del asesor durante los 4 meses

| Costo mensual del asesor(dólares) | Meses de investigación | Costo del asesor (dólares) |
|--|-------------------------------|-----------------------------------|
| 66 | 4 | 264 |

Fuente: Investigación de campo

Realizado por: Cbos. Analuisa Henry

Costo total de estudio, (Ver Cuadro 5.9).

Cuadro 5.9 Costo total de estudio

| Cálculo | Costo total |
|---|--------------------|
| Costo del asesor + Costo del Investigador 264 + 2758.4 | 3022.4 Dólares |

Fuente: Investigación de campo

Realizado por: Cbos. Analuisa Henry

Nota: Por ser Trabajo de Graduación como requisito para la obtención del título de Tecnólogo en Telemática, el ITSA no tiene ningún aporte económico.

5.3.3 Operativa

La implementación del Firewall permitirá controlar de mejor manera el uso de los equipos informáticos existentes dentro del Laboratorio, de la siguiente manera:

- Limitará el uso de archivos autoejecutables.
- Notificara al usuario cuando un programa este a punto de ejecutarse.
- El usuario tendrá la opción de permitir o denegar la modificación de un programa o archivo.

- Restringirá el acceso a diversas aplicaciones de la computadora según su configuración.

También se realizará un manual de usuario que servirá de ayuda para el Docente que utilice los equipos informáticos.

5.3.4 Legal

Conesup

“**Art.49.-** Los estudiantes, egresados o titulados de los institutos superiores técnicos o tecnológicos podría solicitar el reconocimiento de las materias aprobadas y matricularse en otras instituciones del Sistema Nacional de Educación Superior, sujetándose al cumplimiento de los requisitos académicos establecidos en la entidad elegida”.¹²

5.3.5 Apoyo

Para la ejecución de este proyecto se cuenta con el apoyo de varias personas tales como el Departamento de Sistemas del Instituto Tecnológico Superior Aeronáutico, Director de Proyecto de Grado, que tienen un amplio conocimiento de los firewall, lo que facilitará y permitirá la correcta ejecución del mismo.

5.4 Recursos

Talento Humano, (Ver Cuadro 5.10).

Cuadro 5.10 Recurso humano utilizado en el desarrollo del proyecto.

| N.- | Nombre | Cargo |
|------------|------------------------|--------------|
| 1 | Cbos. Analuisa Henry | Investigador |
| 2 | Ing. Francisco Vázquez | Asesor |

Fuente: Investigación de campo

Realizado por: Cbos. Analuisa Henry

¹² <http://www.conesup.net/capitulo7.php>

Material, (Ver Cuadro 5.11).

Cuadro 5.11 Recurso material utilizado en el desarrollo del proyecto.

| N.- | Material |
|------------|----------------------|
| 1 | Derecho de grado |
| 2 | Impresiones |
| 3 | Anillado, empastados |
| 4 | Varios |

Fuente: Investigación de campo
Realizado por: Cbos. Analuisa Henry

5.5 Presupuesto

Costo Primario, (Ver Cuadro 5.12).

Cuadro 5.12 Costo primario para el desarrollo del proyecto.

| N.- | Recurso | Valor unitario | Valor total |
|------------|----------------|-----------------------|--------------------|
| 1 | Firewall | 140 dólares | 140 dólares |
| | | TOTAL | 140 dólares |

Fuente: Investigación de campo
Realizado por: Cbos. Analuisa Henry

Costo Secundario, (Ver Cuadro 5.13).

Cuadro 5.13 Costo secundario usado en el desarrollo del proyecto.

| N.- | Material | Costo | |
|------------|------------------|--------------|--------------------|
| 1 | Derecho de grado | 290 dólares | |
| 2 | Impresiones | 70 dólares | |
| 3 | Anillados | 60 dólares | |
| 4 | Internet | 20 dólares | |
| 5 | Varios | 40 dólares | |
| | | TOTAL | 480 Dólares |

Fuente: Investigación de campo
Realizado por: Cbos. Analuisa Henry

Costo Total del Proyecto, (Ver Cuadro 5.14).

Cuadro 5.14 Costo final del proyecto.

| | |
|------------------|--------------------|
| Costo primario | 140 dólares |
| Costo secundario | 480 dólares |
| TOTAL | 620 dólares |

Fuente: Investigación de campo

Realizado por: Cbos. Analuisa Henry

CAPÍTULO VI

DESARROLLO DEL TEMA

6.1 Listado de requerimientos no funcionales

Los requerimientos no funcionales hacen relación a las características del programa que será usado en este Proyecto las cuales se aplican de manera general, tales como:

Funcionabilidad.- El programa es un instrumento que brinda una seguridad informática de manera real, a los equipos informáticos del Laboratorio, para responder a las necesidades del administrador de la red.

Exactitud.- El control del correcto uso de los equipos informáticos en el Laboratorio de Instrumentación Virtual del ITSA, debe tener una falla mínima en el uso de las máquinas. Esta en capacidad de dar respuesta a las aplicaciones del usuario dándole la opción de permitir o denegar la petición que el estudiante o docente realice.

Seguridad.- El acceso al firewall esta restringido por medio del uso de una clave asignada al programa que únicamente tendrá conocimiento el administrador de la red, esto le hace confidencial a los usuarios de a las restricciones realizadas por el administrador.

Fiabilidad.- La implementación del firewall Kerio se realizará en las 8 maquinas que computadoras actualmente existen en el Laboratorio de Instrumentación Virtual del Instituto Tecnológico Superior Aeronáutico, el mismo que podrá

funcionar con el número de máquinas que sea necesario.

- Eficiencia.-** Los resultados obtenidos después de la implementación del firewall deberán ser satisfactorios y por ende aceptado por el Docente encargado (Ing. Pablo Pilatasig) de mencionado laboratorio.
- Mantenibilidad.-** Para mantener en buen estado el funcionamiento del firewall es recomendable tener activada la protección por contraseña con esto se mantendrá restringida cualquier modificación no autorizada dentro del cortafuego.
- Estabilidad.-** Las modificaciones y restricciones que se realicen no serán notorias para el usuario, únicamente tendrá control de estas el encargado directo.
- Portabilidad.-** La plataforma de este programa será dentro de Sistema Operativo en Windows SP 2, con la capacidad de ejecutarse en cualquier otra como Linux.
- Instalación.-** El programa es fácil de instalar en todas las plataformas de hardware y software definidas por el área de Sistemas, así como permitir su instalación con diferentes tipos de configuración. El firewall será instalado en el sistema operativo Windows XP Service Pack 2, sin causar inconvenientes.

6.2 Manual de Usuario

6.2.1 Instalación del firewall

El programa se instaló en las 8 computadoras existentes en el Laboratorio de Instrumentación Virtual del ITSA.

Lo primero que se hace es colocar el icono de instalación del programa, en el escritorio de las Pc's.

Dar doble clic en el icono, aparecerá la siguiente ventana de bienvenida a la instalación del programa, donde pulsaremos en el botón de "Next", (Ver Figura 6.1).

Figura 6.1 Inicio de la instalación del programa

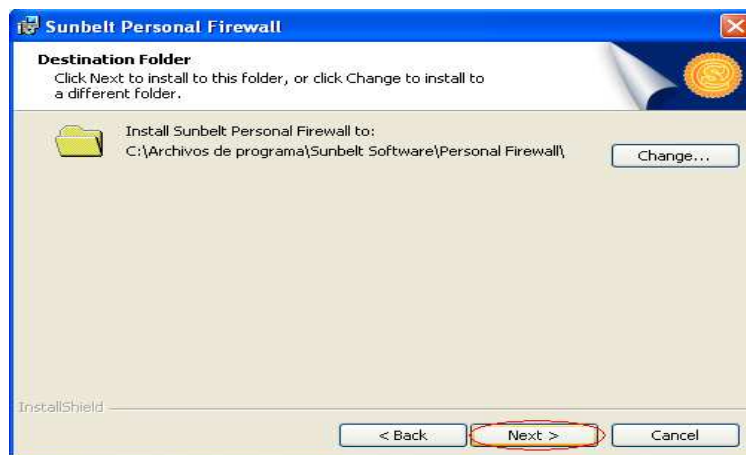


Realizado por: Cbos. Analuisa Henry

Luego la siguiente ventana será donde tenemos que aceptar los términos de licencia del programa.

Lo siguiente que visualizamos es el lugar donde se va a instalar el programa por lo general es en el directorio C:/Archivos de programa/Sunbelt Software/Personal Firewall. Pulsamos el icono de Next, (Ver Figura 6.2).

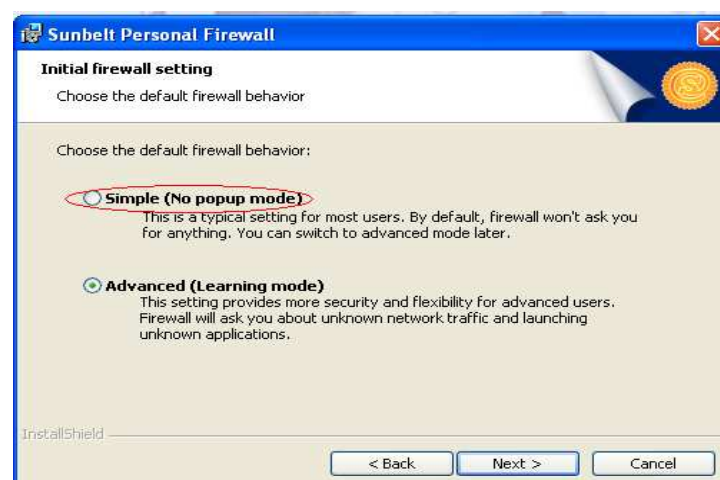
Figura 6.2 Dirección en el que se instalará el programa



Realizado por: Cbos. Analuisa Henry

Luego nos pide elegir el tipo de Instalación Simple o Avanzada, nosotros escogeremos la Simple y pulsamos "Next", y por ultimo "Install", (Ver Figura 6.3).

Figura 6.3 Tipo de Instalación Simple o Avanzada



Realizado por: Cbos. Analuisa Henry

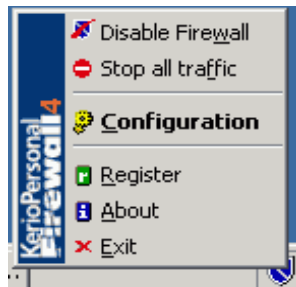
Por último nos pedirá reiniciar la computadora.

6.2.2 Configuración del firewall

Ahora nos fijamos en la barra de tareas de Windows, junto al reloj tenemos un nuevo icono con forma de escudo azul.

Haciendo clic con el botón derecho del Mouse abrimos el cuadro de dialogo donde visualizamos las siguientes opciones, (Ver Figura 6.4).

Figura 6.4 Cuadro de configuración del firewall

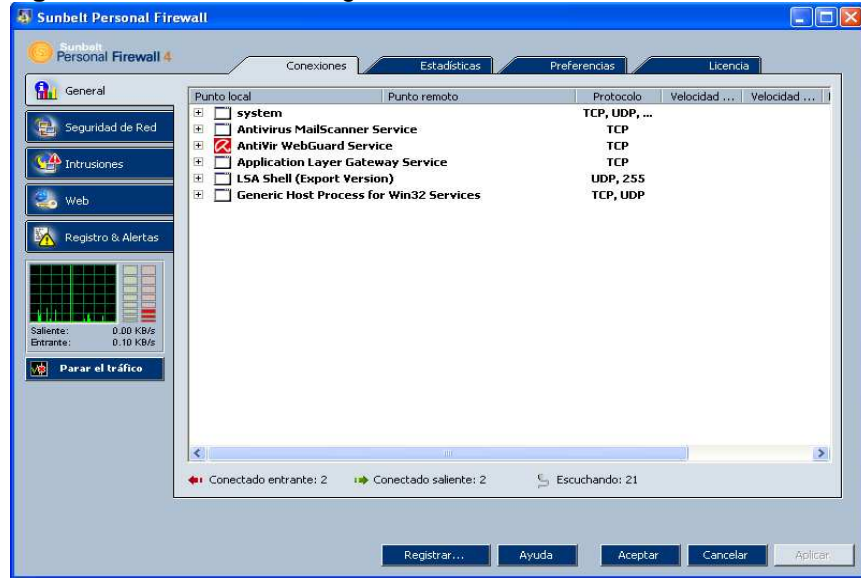


Realizado por: Cbos. Analuisa Henry

Configuración.- Abre la ventana de configuración del Kerio Personal Firewall, es la que explicaré a continuación, (Ver Figura 6.5).

6.2.2.1 Ventana general

Figura 6.5 Ventana de configuración del firewall

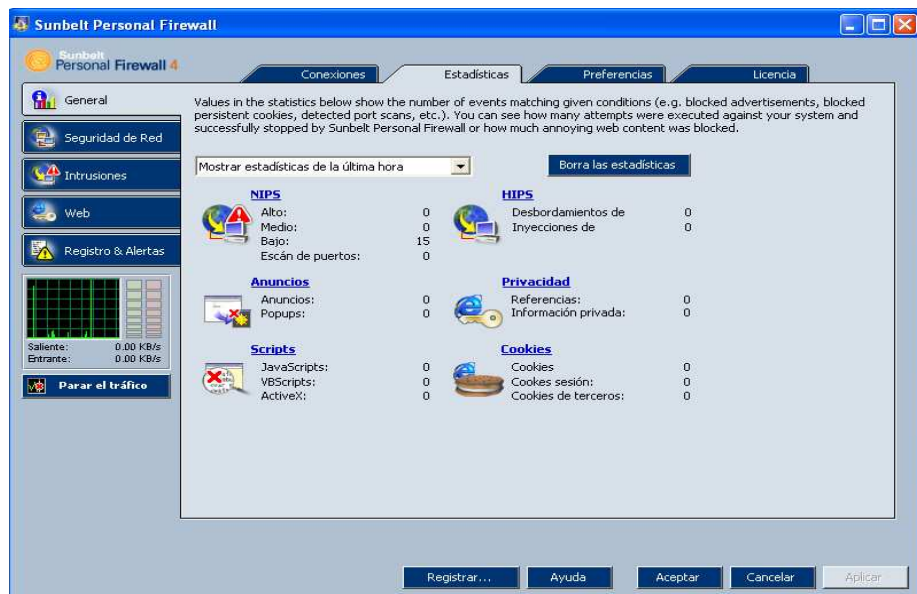


Realizado por: Cbos. Analuisa Henry

Conexiones.- Proporciona información de las conexiones establecidas y puertos abiertos por cada aplicación.

Estadísticas.- Informa al usuario el número de objetos bloqueados por el filtro de conexiones, (Ver Figura 6.6).

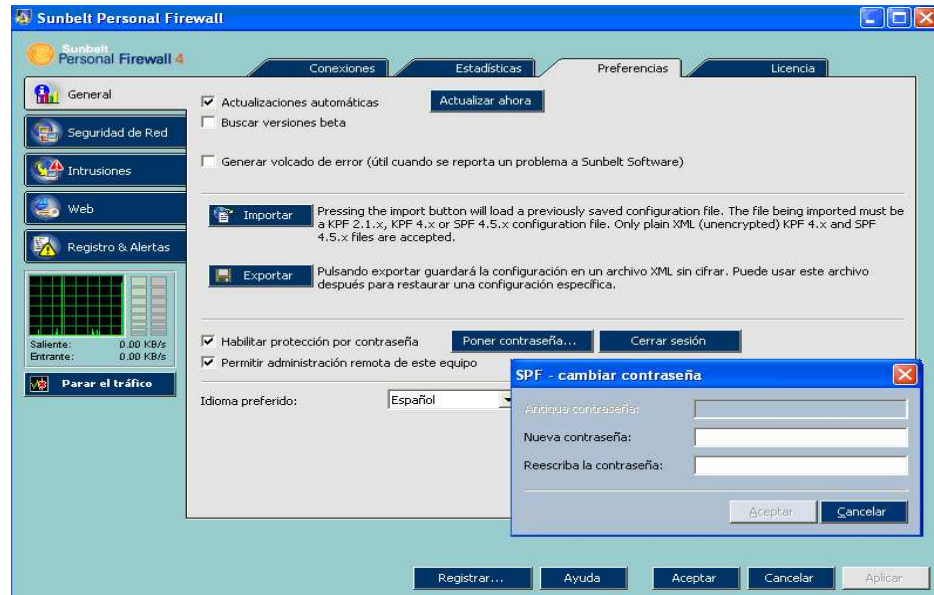
Figura 6.6 Estadísticas que muestra el firewall



Realizado por: Cbos. Analuisa Henry

Preferencias.- Nos permite importar / exportar configuraciones del cortafuegos, además nos permite poner una clave de usuario, (Ver Figura 6.7).

Figura 6.7 Ventana donde nos permite colocar una clave de acceso



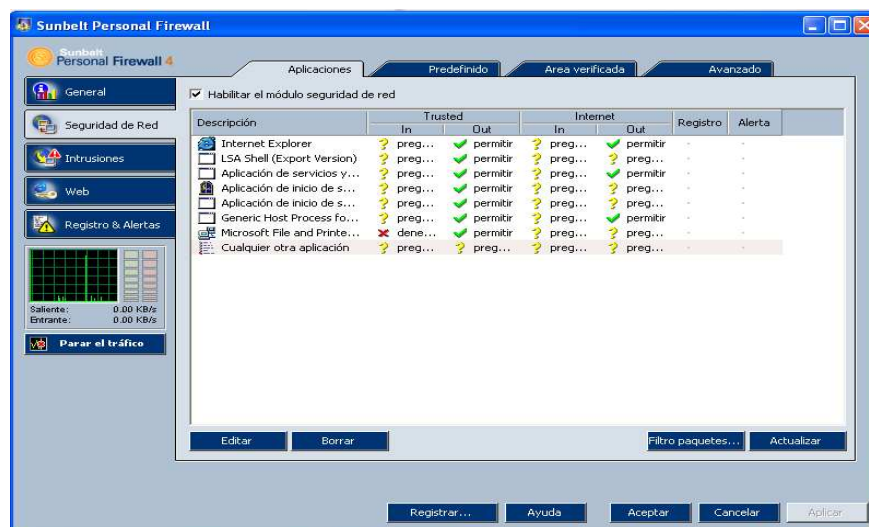
Realizado por: Cbos. Analuisa Henry

Colocar una clave que nos servirá para tener acceso al firewall, esta clave solo tendrá conocimiento el docente encargado del Laboratorio.

6.2.2.2 Ventana de seguridad de red

Aplicaciones.- Nos presenta el icono y la descripción de la aplicación, establece los parámetros del comportamiento del cortafuego para la conexión, (Ver Figura 6.8).

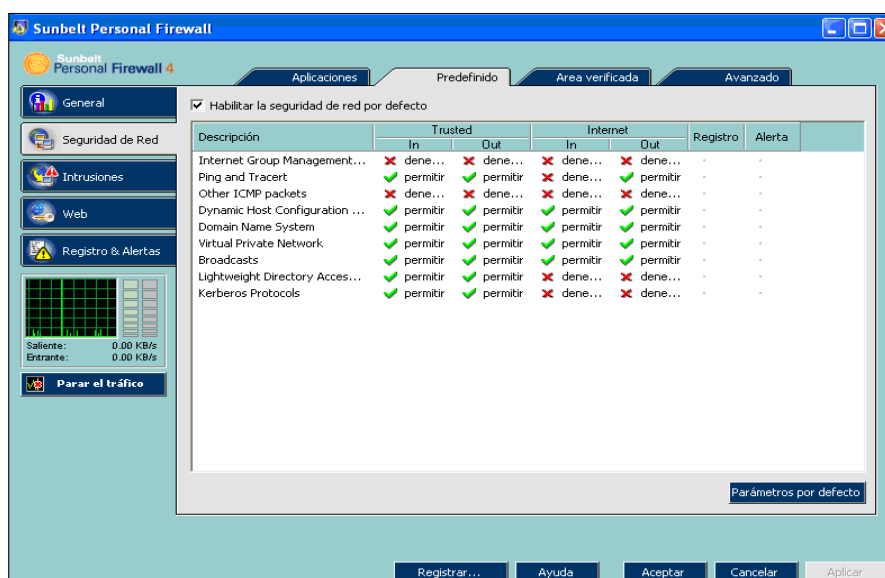
Figura 6.8 Parámetros del firewall en la conexión



Realizado por: Cbos. Analuisa Henry

Reglas predefinidas.- Incluye por defecto un grupo de reglas predefinidas, el usuario define si estas reglas serán usadas o no, (Ver Figura 6.9).

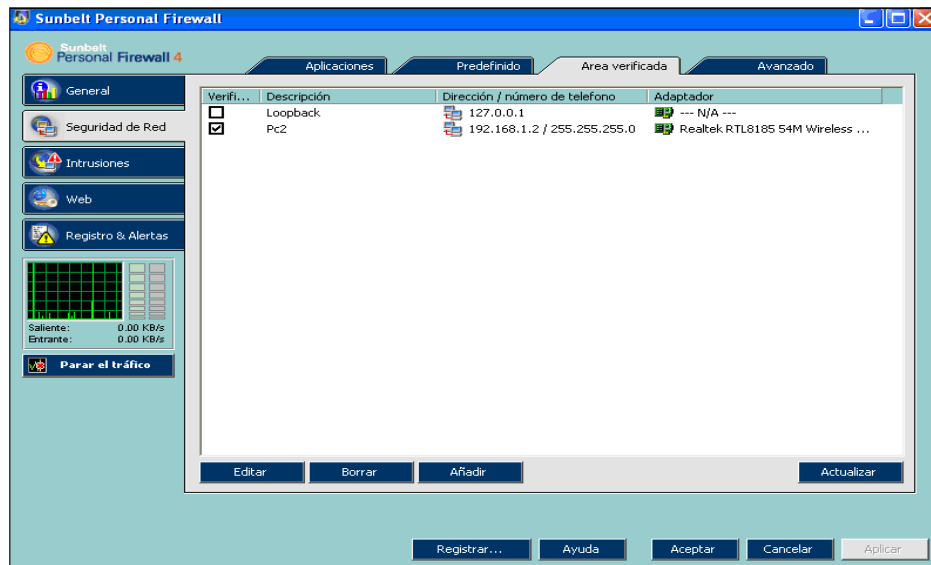
Figura 6.9 Reglas predefinidas por el cortafuego



Realizado por: Cbos. Analuisa Henry

Área verificada.- Es un grupo de IP definidas por el usuario, aquellas que no están definidas en el trusted serán consideradas como del área de Internet, (Ver Figura 6.10).

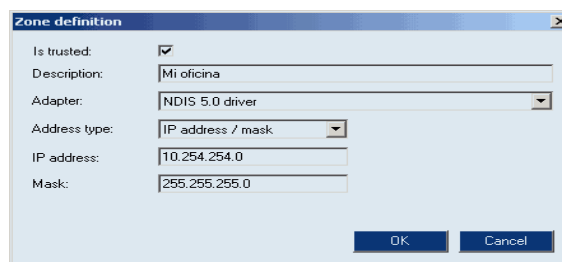
Figura 6.10 Colocación de la IP en el firewall.



Realizado por: Cbos. Analuisa Henry

Usando los botones editar, añadir podemos colocar una IP trusted, (Ver Figura 6.11).

Figura 6.11 Como poner la IP en el firewall

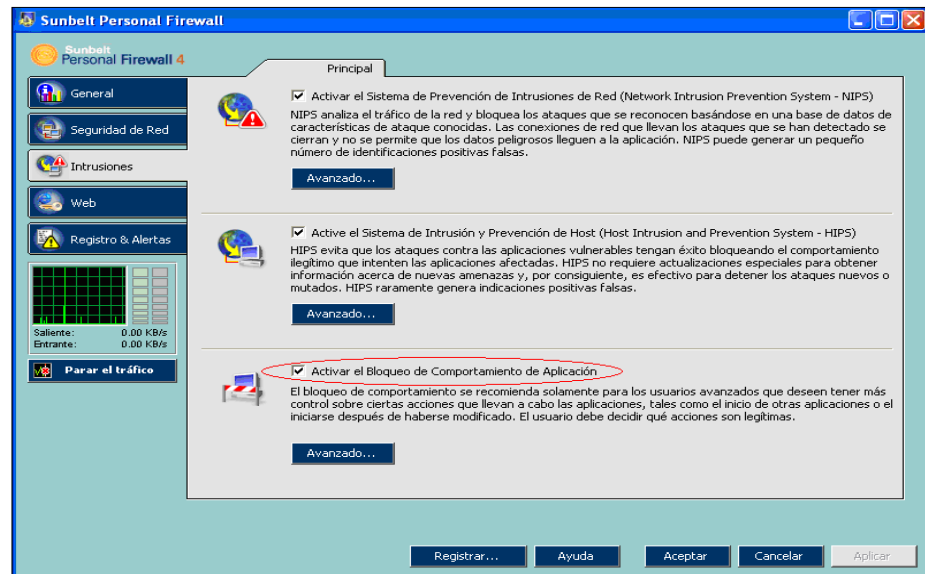


Realizado por: Cbos. Analuisa Henry

6.2.2.3 Ventana de Instrucciones

Principal.- Tenemos tres opciones de configuración (NIPS, HIPS, Activar el bloqueo de comportamiento de aplicación), las dos primeras vienen por defecto configuradas, nosotros tenemos que configurar la tercera, (Ver Figura 6.12).

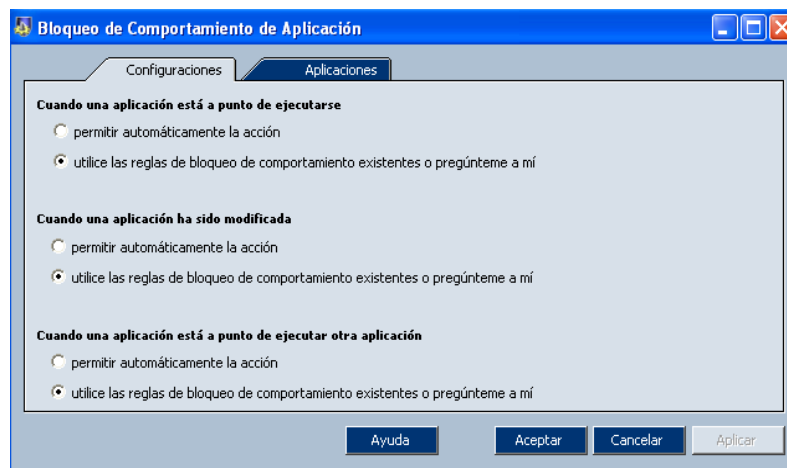
Figura 6.12 Instrucciones de configuración del firewall



Realizado por: Cbos. Analuisa Henry

Procedemos a dar un clic en el icono de Avanzado de la tercera opción. Está nos despliega la siguiente ventana, (Ver Figura 6.13).

Figura 6.13 Configuración de las opciones de cada acción a realizarse



Realizado por: Cbos. Analuisa Henry

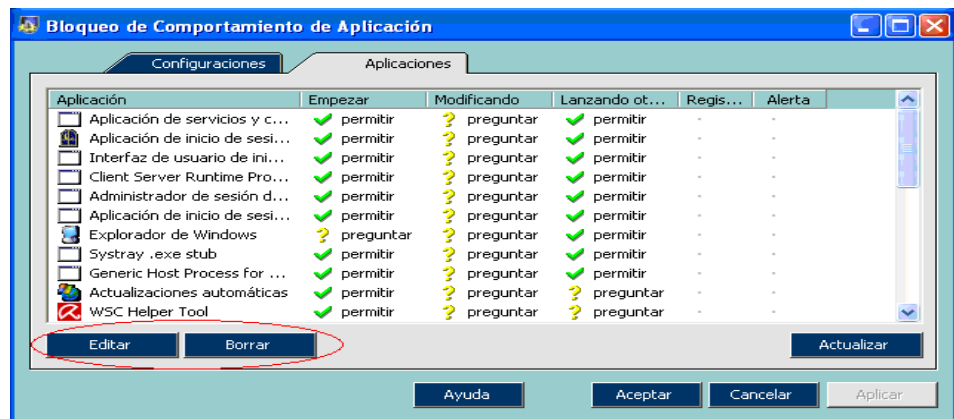
Configuraciones.- El firewall nos despliega tres opciones de configuración:

- Cuando una aplicación está a punto de ejecutarse.
- Cuando una aplicación ha sido modificada.

- Cuando una aplicación está a punto de ejecutar otra aplicación.

Aplicaciones.- Desde esta ventana podemos ver y editar las reglas de ejecución y cambio de cada aplicación, las reglas no pueden ser creadas a mano, solo se puede editar o borrar, (Ver Figura 6.14).

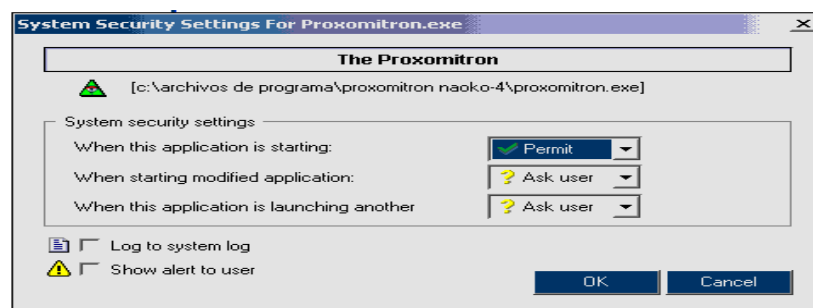
Figura 6.14 Ejecución de las reglas para cada aplicación.



Realizado por: Cbos. Analuisa Henry

Para editar una regla seleccionamos la opción "edit" nos despliega el siguiente cuadro, (Ver Figura 6.15).

Figura 6.15 Editar una regla mediante la opción "edit"



Realizado por: Cbos. Analuisa Henry

En la parte superior junto al triángulo verde podemos observar la dirección del archivo ejecutable.

Y después los tres rectángulos donde colocaremos la regla para que se aplique al archivo ejecutable seleccionado.

6.3 Prueba de caja negra

Las pruebas de caja negra son las cuales nos indican que un programa hace lo que en realidad queremos sin necesidad de conocer cuales son los procesos internos para desplegar la respuesta.¹³

Esta prueba se lo realizó en las 8 máquinas del Laboratorio de Instrumentación Virtual del ITSA, lugar donde se instaló el firewall.

En la prueba realizada se pudo observar que, cada vez que el usuario ejecuta en acción mediante en interfaz (teclado, Mouse) sea esta, instalación o desinstalación de programas, abrir programas del explorador del Windows, insertar en dispositivo extraíble (Flash memory), realizar en cambio en las configuraciones del equipo, ingreso a la máquina mediante la opción ejecutar, el firewall actúa inmediatamente mostrándole las siguientes opciones en pantalla de acuerdo a la aplicación ejecutada, (Ver Figura 6.16).

Figura 6.16 Ejemplo de la prueba de caja negra.



Realizado por: Cbos. Analuisa Henry

¹³ [http://es.wikipedia.org/wiki/Aplicaci%C3%B3n_\(inform%C3%A1tica\)](http://es.wikipedia.org/wiki/Aplicaci%C3%B3n_(inform%C3%A1tica))

Permitir 

Denegar 

Crear una regla para esta aplicación

6.4 Informe de la Fase de Pruebas

Las pruebas son la parte muy significativa del proyecto, por su importancia en el logro de los resultados, en la fase de pruebas es el usuario final quién da la aceptación del programa.

Una vez realizado la prueba del literal 6.3 verificamos el correcto funcionamiento del firewall en cada una de las máquinas existentes en mencionado Laboratorio. (Ver Anexo D).

6.5 Informe de Aceptación de Usuario

La aceptación del usuario es una parte importante dentro del desarrollo del proyecto, ya que mediante este informe (Ver Anexo E), el usuario demuestra que esta absolutamente de acuerdo con el funcionamiento del firewall.

CAPÍTULO VII

CONCLUSIONES Y RECOMENDACIONES

7.1 Conclusiones

- El objetivo planteado al inicio de este proyecto se desarrolló satisfactoriamente, cabe indicar que se cumplió a cabalidad en lo referente a lo teórico-práctico.
- Con la instalación y configuración del Firewall los equipos informáticos tienen mayor seguridad en lo referente al uso de los mismos.
- Se implementó el firewall Kerio en las máquinas del Laboratorio de Instrumentación Virtual del ITSA, para controlar las aplicaciones entrantes y salientes en el PC, así como también hacerles invulnerables a los virus informáticos que pueden presentarse durante su uso.
- La configuración del firewall se lo hizo de una forma detallada de manera que fue explicada mediante interfaces gráficas durante el desarrollo del proyecto, permitiendo así mantener en correcto funcionamiento a los equipos Informáticos existentes en mencionado Laboratorio.
- La comprobación del funcionamiento del cortafuego una vez instalado y configurado permitió observar que satisface las necesidades del administrador de la red, en lo referente a la seguridad Informática del Laboratorio.
- El Laboratorio no cuenta con un cronograma de mantenimiento para las computadoras.

7.2 Recomendaciones

- Para llevar a cabo una excelente investigación es recomendable el uso de un Plan Metodológico el cual ayuda a llevar sistemáticamente el desarrollo de una investigación.

- Revisar el manual de usuario para tener una guía detallada de información sobre la configuración del firewall.
- El usuario debe tener cuidado con los programas instalados y a instalarse ya que pueden perjudicar al correcto funcionamiento de los equipos informáticos existentes en el Laboratorio antes mencionado.
- Tener activada la configuración del firewall mediante la clave del usuario, para así evitar modificaciones de la seguridad Informática configurada dentro del cortafuego.
- La seguridad informática depende también del antivirus por lo que se recomienda actualizar periódicamente y realizar un análisis semanal de las máquinas.
- Coordinar con el Departamento de Sistemas a fin de establecer un cronograma para dar mantenimiento a los equipos informáticos.

BIBLIOGRAFÍA

- **BRUCE ALEXANDER** (2005) "Manual de Redes", Espel Latacunga.
- **CODESIS** (2005) "Técnico en Redes y Comunicaciones de Computadoras", Colombia.
- **CARVALLAR FALCÓN JOSÉ A.** (2006) "Firewall Seguridad de la Banda Ancha", México.
- **GONCALVES MARCUS** (2002) "Manual de Firewalls", México.
- **CHAPMAN DAVID W. Jr. y FOX ANDY** (2002) "Firewall PIX de Cisco", Madrid.

INTERNET:

- **Definición de un firewall:**
<http://www.desarrolloweb.com/articulos/513.php>
- **Funcionamiento e inconvenientes de un firewall:**
http://www.principiantes.info/seguridad/guia_firewall.php
- **Definición de los requerimientos no funcionales:**
<http://trevinca.ei.uvigo.es/~ebalonso/asignaturas/esx/guiones/esxClase9.pdf>
- **Crack del firewall Kerio:**
<http://www.cracks.am>
- **Firewall Kerio, ventajas, desventajas, bloqueo del tráfico**
http://www.ciao.es/Kerio_personal_firewall__Opinion_1102133
- **Configuración del firewall kerio:**
http://nautopia.coolfreepages.com/kerio4/kpf4_primeros_pasos.htm
- **Firewall Windows XP y Windows Vista:**
<http://multingles.net/docs/jmt/wvsalidas.html>

➤ **Ventajas, limitaciones y políticas de un firewall:**

[http://es.wikipedia.org/wiki/Cortafuegos_\(inform%C3%A1tica\)](http://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica))

➤ **Definición de Aplicación:**

[http://es.wikipedia.org/wiki/Aplicaci%C3%B3n_\(inform%C3%A1tica\)](http://es.wikipedia.org/wiki/Aplicaci%C3%B3n_(inform%C3%A1tica))

➤ **Modelo OSI:**

http://www.zator.com/Hardware/H12_2.htm

➤ **Virus Informáticos:**

http://es.wikipedia.org/wiki/Virus_inform%C3%A1tico

ABREVIATURAS

| | |
|----------------|---|
| CONESUP | Consejo Nacional de Educación Superior. |
| ESPEL | Escuela Superior Politécnica del Ejército sede Latacunga |
| HIPS | Host Intrusion and prevention system. - Sistema de intrusión y prevención de Host. |
| IP | Internet Protocol. - Protocolo de Internet. |
| ITSA | Instituto Tecnológico Superior Aeronáutico. |
| NIPS | Network Intrusion Preventor System.- Sistema de prevención de intrusiones de red. |
| OSI | Open System Interconnection, Interconexión de Sistemas Abiertos. |
| SPSS | Statistical Package for the Social Sciences, Programa estadístico Informático usado en las ciencias sociales. |

GLOSARIO DE TÉRMINOS

A

Aplicación Es un tipo de programa informático diseñado para facilitar al usuario la realización de un determinado tipo de trabajo.

C

Crackers Es alguien que viola la seguridad de un sistema informático.

D

Deficiente Que tiene algún defecto o que no alcanza el nivel considerado normal.

Desmotivación Falta o pérdida de motivación.

F

Factibilidad Cualidad o acción de factible. Que se puede realizar.

Firewall Dispositivo de seguridad, que opera como una pared entre redes, que permite o deniega las transmisiones de una red a otra.

H

Hackers Expertos relacionados con la informática.

Hardware Conjunto de los componentes que integran la parte material de una computadora.

Host Es un ordenador que funciona como el punto de inicio y final de la transferencias de datos.

I

Indagación Intentar averiguar, inquirir algo discurrendo o con preguntas.

Ip Es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo dentro de una red.

O

Optimización Buscar la mejor manera de realizar una actividad.

S

Software Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

SPSS (Statistical Package for the Social Sciences), Programa estadístico informático.

Sistemático Que sigue o se ajusta a un sistema.

CRONOGRAMA

| N. Act. | Actividades | MESES | | | | | | | | | | | | | | |
|------------|------------------------------------|------------|--|---|---------|---|-----|-----------|-----|-------|-----------|--|-------|-------|-----|--|
| | | Septiembre | | | Octubre | | | Noviembre | | | Diciembre | | | Enero | | |
| 1 | Planteamiento del problema | | | X | | | | | | | | | | | | |
| 2 | Recolección y análisis de datos | | | | X | | | | | | | | | | | |
| 3 | Presentación del primer avance | | | | | X | | | | | | | | | | |
| 4 | Presentación segundo avance | | | | | | X X | | | | | | | | | |
| 5 | Entrega Anteproyecto | | | | | | | X | | | | | | | | |
| 6 | Corrección Anteproyecto | | | | | | | | X X | | | | | | | |
| 7 | Implementación del Firewall | | | | | | | | | X X X | | | | | | |
| 8 | Pruebas del firewall | | | | | | | | | | X X | | | | | |
| 9 | Predefensa y Defensa | | | | | | | | | | | | X X X | | | |
| 10 | Entrega de ejemplares y empastados | | | | | | | | | | | | | | X X | |

 Cbos. Téc. Avc. Analuisa Henry
Investigador

 Ing. Francisco Vásquez
Director Del Trabajo de Investigación

ANEXOS

ANEXO "A"

INSTITUTO TECNOLÓGICO SUPERIOR AERONÁUTICO

CARRERA TELEMÁTICA

LABORATORIO DE INSTRUMENTACIÓN VIRTUAL

OBSERVACIÓN:

DATOS INFORMATIVOS:

Lugar:

Fecha:

Observador: Cbos. Analuisa Villacrés Henry Jhonny

OBJETIVO:

1.-Observar la situación actual del Laboratorio de Instrumentación Virtual del Itsa.

OBSERVACIONES:

.....
.....
.....
.....
.....
.....
.....
.....

ANEXO "B"

INSTITUTO TECNOLÓGICO SUPERIOR AERONÁUTICO

CARRERA: TELEMÁTICA

ENCUESTA REALIZADA A LOS ESTUDIANTES Y DOCENTES QUE UTILIZAN EL LABORATORIO DE INSTRUMENTACIÓN VIRTUAL

Objetivo: Investigar el criterio de los estudiantes y docentes, con relación a la comunicación entre ordenadores en el Laboratorio de Instrumentación Virtual del ITSA.

Indicaciones:

- Lea detenidamente las preguntas
- Conteste con sinceridad
- Marque con una X en la Respuesta que usted crea conveniente

1.- ¿Cree usted que los recursos informáticos del Laboratorio de Instrumentación Virtual del "ITSA" están siendo aprovechados adecuadamente?

BASTANTE POCO NADA

2.- ¿Piensa usted que las computadoras del Laboratorio de Instrumentación Virtual del "ITSA", necesitan tener un sistema de control para el uso adecuado de las mismas?

SI NO

3.- ¿Considera usted que la conexión de red actual de los equipos informáticos del Laboratorio de Instrumentación Virtual del "ITSA" es?

MUY BUENA BUENA DEFICIENTE

4.- ¿Piensa usted que es importante realizar una reubicación de los equipos informáticos del Laboratorio de Instrumentación Virtual del "ITSA", para aprovechar eficazmente el espacio físico?

MUY IMPORTANTE IMPORTANTE NADA IMPORTANTE

GRACIAS POR SU COLABORACIÓN

ANEXO "C"

COMPARACIÓN DE PRECIOS Y CARÁCTERÍSTICAS DE ALGUNOS FIREWALL

| TIPOS DE FIREWALL INVESTIGADOS | | | | |
|--------------------------------|--|---------|-----------------------------|--|
| NOMBRE | CARACTERÍSTICAS | PESO | COMPATIBILIDAD | PRECIO |
| Cómodo firewall | <ul style="list-style-type: none"> ➤ Evitar ataques de los hackers. ➤ Controlar que programas tienen acceso a Internet. ➤ Mostrar avisos cuando de presente alguna actividad. | 18.2 MB | Windows XP SP2 | Gratis (Versión demo) 160 Dólares la licencia |
| Ciber Boss 4 | <ul style="list-style-type: none"> ➤ Se usa a nivel de ciber cafés. ➤ Uso limitado de máquinas. ➤ Necesita dos aplicaciones para su instalación software servidor y software cliente. | 8.4 MB | Windows XP SP2 | Versión demo 190 dólares licencia |
| Kerio personal firewall | <ul style="list-style-type: none"> ➤ Protege el ordenador en Internet y redes locales. ➤ Previene ataques y accesos mediante el DOS. ➤ Muestra avisos cuando una aplicación es ejecutada. ➤ Evita ataques internos como virus. | 5.72 MB | Windows XP Windows Vista | 140 dólares |

ANEXO “D”

INSTITUTO TECNOLÓGICO SUPERIOR AERONÁUTICO

CARRERA: TELEMÁTICA

INFORME DE LA FASE DE PRUEBAS REALIZADA DESPUÉS DE LA “IMPLEMENTACIÓN DE UN FIREWALL EN LOS EQUIPOS INFORMÁTICOS DEL LABORATORIO DE INSTRUMENTACIÓN VIRTUAL DEL ITSA”

Objetivo: Conocer el resultado de la fase de pruebas realizadas después de la instalación y configuración del firewall en el Laboratorio de Instrumentación Virtual del ITSA.

El uso del firewall contiene un conjunto de reglas predeterminadas que le permiten al usuario Autorizar, Bloquear, Rechazar, todas estas reglas implantan un método de filtrado que depende de la configuración que se realizó al firewall. Es así que la fase de pruebas se lo realizó en el Laboratorio antes mencionado, junto con el Ing. Pablo Pilatasig encargado directo de dicho laboratorio, mediante esta fase de pruebas se pudo conocer el correcto funcionamiento del firewall instalado en las 8 máquinas.

Para la veracidad de este informe contamos con la firma del Ing. Pablo Pilatasig Docente encargado del Laboratorio de Instrumentación Virtual del ITSA.

ATENTAMENTE:

**ING. PABLO PILATASIG
DOCENTE ENCARGADO**

ANEXO “E”

INSTITUTO TECNOLÓGICO SUPERIOR AERONÁUTICO

CARRERA: TELEMÁTICA

INFORME DE ACEPTACIÓN DE USUARIO DESPUÉS DE LA “IMPLEMENTACIÓN DE UN FIREWALL EN LOS EQUIPOS INFORMÁTICOS DEL LABORATORIO DE INSTRUMENTACIÓN VIRTUAL DEL ITSA”

Objetivo.- Conocer el criterio del usuario final luego de comprobar el funcionamiento del firewall instalado en las máquinas existentes en el laboratorio mencionado anteriormente.

Yo, Ing. Pablo Pilatasig en calidad de Docente encargado y usuario final de mencionado laboratorio, y después de haber comprobado el funcionamiento del firewall en cada una de las máquinas existentes en el laboratorio a mi responsabilidad; estoy absolutamente de acuerdo con el trabajo realizado por el Sr. Cbos. Analuisa Villacrés Henry cuyo tema es **“IMPLEMENTACIÓN DE UN FIREWALL EN LOS EQUIPOS INFORMÁTICOS DEL LABORATORIO DE INSTRUMENTACIÓN VIRTUAL DEL ITSA”**.

ATENTAMENTE:

**ING. PABLO PILATASIG
DOCENTE ENCARGADO**

HOJA DE VIDA

NOMBRES Y APELLIDOS: Cbos. Téc. Avc.
Analuisa
Villacrés Henry
Jonny

LUGAR Y FECHA DE NACIMIENTO: Latacunga, 13 de
Febrero de 1986

EDAD: 23 Años

ESTADO CIVIL: Soltero

DIRECCIÓN: La Maná – Parroquia El Carmen

TELÉFONO: 032- 688745/099470933

CÉDULA DE IDENTIDAD: 050311844-0



ESTUDIOS REALIZADOS

PRIMARIA: Escuela Fiscal Mixta La Maná

SECUNDARIA: Instituto Tecnológico Superior La Maná

TÍTULO: Bachiller en Físico Matemático

ESPECIALIDAD: Físico Matemático

CURSOS REALIZADOS

CURSO DE MILITARIZACIÓN: Escuela Técnica de la Fuerza Aérea

CURSO DE SUFICIENCIA Instituto Tecnológico Superior

EN INGLÉS: Aeronáutico

PRÁCTICAS LABORALES

COMANDO GENERAL FAE: Dirección de Sistemas de Información y
Comunicación (Informática)

BASE AÉREA COTOPAXI: Sección Informática

HOJA DE LEGALIZACIÓN DE FIRMAS

ELABORADO POR:

CBOS. TÉC. AVC. ANALUISA VILLACRÉS HENRY JONNY

DIRECTOR DE LA CARRERA DE TELEMÁTICA

ING. KARLA VASCO