CAPÍTULO II.

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS.

2. Descripción General de la Universidad Técnica de Cotopaxi.

2.1 *Propósito.*

Tener profesionales con un perfil que responden a la realidad social, económica, política, cultural, científica y tecnológica de nuestro país; capaz de proyectar sus experiencias en beneficio nacional; diestro en la utilización de herramientas informáticas; diseña, opera, evalúa proyectos y procesos de desarrollo informático, redes de computadoras; es un eficiente administrador informático, capacitado para resolver grandes cambios tecnológicos y ponerlos a disposición de la colectividad.

La aceptación nos indica fundamentalmente que nuestra Universidad está cumpliendo el papel protagónico y el encargo social para lo que fue creada, esto es entregar profesionales sólidamente preparados dentro del plano científico, técnico y

humanístico encaminados a determinar y solucionar los problemas de diferente índole de la sociedad. Además nos da la pauta que la Carrera y nuestras especialidades están perfectamente diseñadas en función de las necesidades sociales reales que nos circunda.

Formar profesionales humanistas e investigadores de excelencia, creativos, críticos y con capacidad de liderazgo y un alto nivel científico – técnico contribuyendo al desarrollo del país.

Promover proyectos de investigación para generar ciencia y tecnología, orientados a solucionar los problemas y satisfacer las necesidades del país.

2.1.1 Misión.

Formar integralmente con principios humanísticos con la mas alta excelencia académica como respuesta a la demanda de la sociedad y del aparato reproductivo nacional, para que pueda participar en la búsqueda de soluciones a las diferentes problemas existentes sobre la base de una investigación científica orientada a llevar el nivel cultural y el bienestar de la comunidad, convirtiéndose en un factor de cambio de la sociedad.

2.1.2 Visión.

Es una Universidad alternativa de alcance regional y nacional con visión de futuro, sin fines de lucro que orienta su trabajo hacia los sectores populares del campo y la ciudad, buscando la afirmación de la identidad multiétnica y pluricultural del país. Asumimos con responsabilidad la producción y socialización del conociendo, así como el pensamiento democrático y progresista para el desarrollo de la conciencia antiimperialista del pueblo.

2.2 Conocimiento General Acerca De La Red De La Universidad Técnica De Cotopaxi.

La Universidad Técnica de Cotopaxi posee una red de tipo LAN la cual se encuentra distribuida en VLAN, las mismas que tienen limitaciones tanto para estudiantes, docentes y administrativos. Toda la red de banda ancha esta dividida en dos sectores el primero con mayor ancho de banda en el sector de San Felipe en la cual cuenta varias salas de cómputo que se encuentran por el momento con dos bloques académicos que son el bloque “A” y “B” los mismo que transfieren datos mediante Fibra Óptica y la segunda en el sector de Salache (CEYPSA) que tiene las mismas características de la antes mencionada con la mínima diferencia que es menor el ancho de banda por sus requerimientos.

LAN son las siglas de *Local Area Network*, Red de área local. Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios). Las redes LAN se pueden conectar entre ellas a través de líneas telefónicas y ondas de radio. Un sistema de redes LAN conectadas de esta forma se llama una WAN, siglas del inglés de wide-area network, Red de área ancha.

Debido a sus limitadas dimensiones, son redes muy rápidas en las cuales cada estación se puede comunicar con el resto. Suelen emplear tecnología de difusión mediante un cable sencillo (coaxial o UTP) al que están conectadas todas las máquinas. Operan a velocidades entre 10 y 100 Mbps.

FIGURA 1: RED LAN. (VER ANEXO 4 PAG. 113).

La administración, control y monitoreo de toda la red de la Universidad Técnica de Cotopaxi esta a cargo del Departamento de Servicios Informáticos que su oficina se encuentra en el Bloque "A" del edificio central del sector de San Felipe.

2.2.1 Tipo de Red que Utilizan las Salas de Cómputo.

La red de la Universidad Técnica de Cotopaxi como ya especificamos anteriormente es una red LAN que esta dividida en subredes virtuales conocidazas como VLAN en la que se encuentra distribuida puntos o nodos de VLAN tanto para estudiantes, docentes y administrativos cada uno de ellos con diferentes privilegios, en cada sala de cómputo.

VLANs (virtual LANs – LAN virtuales) se definen como LANs que mapean componentes unidos basados en un paquete de parámetros (por grupos de negocios, aplicaciones o áreas geográficas). Los dispositivos no tienen que localizarse en el mismo cable físico.

2.2.2 Ubicación Geográfica.

El campus universitario CEYPSA se encuentra en la panamericana sur vía Salcedo, llegando a la intersección de la gasolinera Silva vía a Salache.

FIGURA 2: UBICACIÓN GEOGRÁFICA (VER ANEXO 4 PAG. 114).

2.3 Métodos, Técnicas E Instrumentos Que Fueron Utilizados.

2.3.1 Metodología.

De acuerdo al nivel de la investigación la misma fue explicativa, ya que una vez definidas las categorías y sub categorías de análisis se conceptualizaron y operacionalizarón para implementar y evaluar el modelo en cuestión. Al describir la interrelación de las partes que definen el objeto de estudio, se realiza un análisis más profundo a los fines de establecer la estructura de la propuesta.

2.3.1.1 Método Descriptivo.

Este método para nosotros fue indispensable para nuestra investigación porque nos ayudo a puntualizar los problemas causas y efectos que tiene las salas de cómputo del campus CEYPSA de la Universidad Técnica de Cotopaxi

Nosotros como grupo investigativo vamos a definir los principales problemas con sus causas y efectos que ocurre este departamento.

- Actualización de antivirus, este problema se da porque el ancho de banda del CEYPSA es solamente de una mega mientras que el Campus Universitario de San Felipe es de tres megas y una mega está destinado para el Campus Universitario de la Mana.
- La falta de creación de usuarios y administrador en las Pc`s, esto es un grave error porque los estudiantes pueden manipular el Sistema como ellos crean conveniente.
- Incorrección del control en el filtrado de la información, ya que los estudiantes ingresan a paginas que se encuentran en un alto porcentaje de virus, troyanos y cyber ataques teniendo en cuenta que las Pc`s son un punto fácil para los mismos.
- La falta de instalación de un herramienta que permita el control de flujo de la información, como consecuencia de lo dicho anterior los estudiantes pueden hacer lo que sea en las Pc`s sin restricción alguna.

Dando como consecuencia un alto índice de virus, el mal funcionamiento de las maquinas es producidos por los mismos estudiantes, un rendimiento bajo en comparación de sus características, y por eso nuestra propuesta de instalar un cortafuego de tipo software para que esta herramienta nos ayuda a controlar estas falencias.

De la misma manera este método nos ha ayudado a detallar a fondo las características de cada uno de los cortafuegos a hacer analizados y por ende a la selección de uno de ellos.

2.3.1.2 ***Técnicas de Investigación.***

Mediante la observación podemos manifestar una realidad visual donde se basa nuestra tesis siendo de gran ayuda para familiarizarnos con el entorno y así detectar cuales son los principales problema que afectan a este departamento.

Donde nos encontramos obligados como grupo investigativo a encontrar soluciones a los diferentes problemas que presenta el mismo, como es el análisis de varios cortafuegos gratuitos que se encuentra en el mercado y la selección de uno de ellos, precipitándonos que no todos los cortafuegos analizados rindieron al cien por ciento, ya que observamos ventajas y desventajas de cada uno de ellos en su manejo y desempeño en las mismas.

Otra técnica de investigación que hemos utilizado es la encuesta que nos ayudo a la recopilación de información de varias personas como son estudiantes, docentes y administrativos, para lo cual nos apoyamos de un instrumento esencial como es el cuestionario, que se buscó determinar la posición o actitud que poseen los estudiantes, docentes y administrativos sobre el uso y conocimiento de cualquier Cortafuego que exista en el mercado.

Esta técnica fue aplicada a un total de 98 personas como: estudiantes, docentes y administrativos de la Unidad Académica CIYA especialización en Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi. De los cuales se obtuvo los siguientes datos.

2.4 Encuesta Dirigida A Los Estudiantes De Sexto A Octavo Ciclos, Docentes De La Unidad Académica CIYA De La Carrera Ingeniería En Informática Y Sistemas Computacionales Y Administrativos Del CEYPSA.

El propósito de la presente investigación es presentar la organización e interpretación de los resultados obtenidos para el estudio de la factibilidad de la investigación sobre el tema de Tesis "Análisis e Implementación de un Cortafuego de Tipo Software para la Seguridad en la Red de Banda Ancha de las Salas de Computo del Campus CEYPSA de la Universidad Técnica de Cotopaxi, que Permita la Prevención de Intrusos no Deseados para el Mejor Funcionamiento de Cada Pc".

2.4.1 Análisis e Interpretación de los Resultados de la Encuesta Aplicadas a los Estudiantes.

Para la representación e interpretación de resultados utilizamos la estadística descriptiva permitiéndonos la representación de datos a través de los gráficos estadísticos como es el pastel.

1. ¿Conoce que es un cortafuego o firewalls?

Si_____

No_____

No sabe_____

TABLA 5: PORCENTAJE DE CONOCIMIENTO DE UN CORTAFUEGO A LOS ESTUDIANTES (VER ANEXO 2 PAG. 93).

GRÁFICO 1: PORCENTAJE DE CONOCIMIENTO DE UN CORTAFUEGO A LOS ESTUDIANTES (VER ANEXO 3 PAG. 103).

ANÁLISIS E INTERPRETACIÓN:

El 70% de la población estudiantes de los ciclos superiores del CIYA conocen acerca de un cortafuego o firewall, mientras que el 20% no conoce acerca de esta herramienta y el 10% restante no sabe lo que es. En estos porcentajes demuestran de que si conocen acerca de esta herramienta que es muy útil y sencilla tanto para lo que es en la red o en la instalación de software en la que nos indica si es malicioso o no.

2. ¿Cree usted que existe firewalls en la institución?

Si_____

No_____

No sabe_____

TABLA 6: PORCENTAJE DE CONOCIMIENTO DE LA EXISTENCIA DE UN CORTAFUEGO A LOS ESTUDIANTES (VER ANEXO 2 PAG. 93).

GRÁFICO 2: PORCENTAJE DE CONOCIMIENTO DE LA EXISTENCIA DE UN CORTAFUEGO A LOS ESTUDIANTES (VER ANEXO 3 PAG. 103).

ANÁLISIS E INTERPRETACIÓN:

En un 48% cree que existe un cortafuego en la Universidad, el 30% no conoce de la existencia de la misma y finalmente el 22% lo ignora. Al interpretar estos datos existe un alto porcentaje que creen que existe un cortafuego en la Universidad pero no saben el tipo de cortafuego que existe en la institución y muchos de ellos no saben que existe, porque los docentes y administrador no dan a conocer abiertamente de la misma, teniendo en cuenta que nosotros como informáticos debemos actualizar en la materia y conocer acerca de estas herramientas.

3. ¿Ha tenido incidentes al navegar en la red?

Si_____

No_____

No sabe_____

TABLA 7: PORCENTAJE DE INCIDENTES EN LA RED A LOS ESTUDIANTES (VER ANEXO 2 PAG. 94).

GRÁFICO 3: PORCENTAJE DE INCIDENTES EN LA RED A LOS ESTUDIANTES (VER ANEXO 3 PAG. 104).

ANÁLISIS E INTERPRETACIÓN:

Como podemos ver el 69% ha tenido inconvenientes al navegar en Internet, el 20% no la ha tenido y el 11% no se percatado de algún incidente. La mayoría de personas que navegan en la red de la institución han tenido muchos inconvenientes tanto en lo que en el interne, descargas programas tipo .exe que lo general vienen incluidos con virus, troyanos lo cuales afectan al rendimiento de las Pc’s e inclusive dañan el

sistema operativo y por últimas instancias se pierde toda la información y como peor de los casos toca formatearles.

4. **¿Cuál de estos cree usted que es más común para que se originen incidentes de seguridad en la red hágalo con porcentajes (%) del 1 al 100?**

   - Vínculos Externos_____
   - Accesos vía modem_____
   - Internet_____
   - Sistemas internos_____
   - Otros_____

TABLA 8: PORCENTAJE DEL ORIGEN DE LOS INCIDENTES EN LA RED A LOS ESTUDIANTES (VER ANEXO 2 PAG. 94).

GRÁFICO 4: PORCENTAJE DEL ORIGEN DE LOS INCIDENTES EN LA RED A LOS ESTUDIANTES (VER ANEXO 3 PAG. 104).

ANÁLISIS E INTERPRETACIÓN:

Podemos ver que el incidente más común para el ataque a la seguridad de las Pc's es el Internet ya que tiene un porcentaje del 56%, como segundo tenemos vínculos externos con un 14% de riesgo, el tercero corresponde al acceso vía MODEM con un 12%, el cuarto es sistemas internos con el 10% y por ultimo tenemos otros tipos de riegos con un 8%.

5. ¿Cree usted que después de instalar software antivirus y un firewalls el ordenador está protegido?

Si_____

No_____

No sabe_____

TABLA 9: INSTALACIÓN DE ANTIVIRUS Y UN FIREWALL EN LAS PC'S A LOS ESTUDIANTES (VER ANEXO 2 PAG. 95).

GRÁFICO 5: INSTALACIÓN DE ANTIVIRUS Y UN FIREWALL EN LAS PC'S A LOS ESTUDIANTES (VER ANEXO 3 PAG. 105).

ANÁLISIS E INTERPRETACIÓN:

En este cuadro nos podemos dar cuenta que los estudiante no creen que al instalarse un cortafuego y antivirus en la Pc no están protegidos con un 46%, y ya que con un 41% cree que si está protegida, mientras el 13% no está al corriente. Nosotros como grupo investigativo nos hemos dado cuenta y concordamos con el grupo que la Pc está protegida con firewall y un antivirus siempre y cuando la maquina no contenga ningún virus antes de la instalación de estas herramientas.

6. ¿Los docentes de informática les han informado sobre firewalls?

Si _____

No _____

TABLA 10: PORCENTAJE DE INFORMACIÓN DE UN FIREWALL A LOS ESTUDIANTES (VER ANEXO 2 PAG. 95).

GRAFICO 6: PORCENTAJE DE INFORMACIÓN DE UN FIREWALL A LOS ESTUDIANTES (VER ANEXO 3 PAG. 105).

ANÁLISIS E INTERPRETACIÓN:

El 49% de estudiantes encuestados comentan que no les han informado acerca de un cortafuego ya que los ingenieros solo se rigen al pensul de estudio que tienen que cumplir, son muy pocos los que participan del avance tecnológico no solo tipo hardware sino de tipo software, es por eso que el 51% de estudiantes han tenido la oportunidad de conversar de esta herramienta. Con estos datos nos podemos dar cuenta ya la mayoría de los encuestados no conocen y por ende no saben utilizar herramienta que es muy útil.

7. ¿Qué tipo de usuario maneja?

Administrador del equipo_____
Usuario invitado _____

TABLA 11: TIPO DE USUARIO QUE MANEJAN LOS ESTUDIANTES (VER ANEXO 2 PAG. 96).

GRÁFICO 7: TIPO DE USUARIO QUE MANEJAN LOS ESTUDIANTES (VER ANEXO 3 PAG. 106).

ANÁLISIS E INTERPRETACIÓN:

Nos podemos dar cuenta que la mayoría de estudiantes de que un 76% manejan lo que es usuario invitado lo cual vemos de que existe seguridad en la Pc's, pero como podemos ver existe un 24% de estudiantes de una u otra manera utilizan la contraseña de administrador en el existe un alto riesgo que pueda ser manipulada erróneamente el sistema.

2.4.2 Análisis e Interpretación de los Resultados de la Encuesta Aplicadas a los Docentes.

1. ¿Sugiere usted a los alumnos (as) para manejar correctamente un firewalls?

Si _____

No _____

TABLA 12: SUGERENCIA DE UN FIREWALL DE LOS DOCENTES (VER ANEXO 2 PAG. 96).

GRÁFICO 8: SUGERENCIA DE UN FIREWALL DE LOS DOCENTES (VER ANEXO 3 PAG. 106).

ANÁLISIS E INTERPRETACIÓN:

En un 53% revelan que si sugieren a sus alumnos utilizar un firewall en sus Pc's mientras que el 47% restante no ha sugerido ni ha recomendado el uso del mismo. Por tal motivo nuestra investigación incita ha buscar nuevas alternativas para

salvaguardar la integridad de la red y por ende de las Pc`s., Además que la mayoría lo recomienda por ser una herramienta útil y muy fácil de usar.

2. ¿Cree usted que se ejecutan planes de contingencia de acuerdo al estado de la red?

Si_____

No_____

No sabe_____

TABLA 13: PORCENTAJE DE CONOCIMIENTO DE UN PLAN DE CONTINGENCIA A LOS DOCENTES (VER ANEXO 2 PAG. 97).

GRÁFICO 9: PORCENTAJE DE CONOCIMIENTO DE UN PLAN DE CONTINGENCIA A LOS DOCENTES (VER ANEXO 3 PAG. 107).

ANÁLISIS E INTERPRETACIÓN:

Nos podemos dar cuenta que un 53% de docentes están informados acercan de la red que utilizan para dar clases a los estudiantes ya que es muy importante saber a los riegos que se expone a la red y a un más que existe como remediarlo, pero el 40% revela no conocer que exista un plan de contingencia y el 7% restante no se encuentra informado.

3. ¿Recomienda a sus alumnos (as) instalar un firewalls?

Si_____

No_____

Por que

TABLA 14: RECOMENDACIÓN DE UN FIREWALL DE LOS DOCENTES (VER ANEXO 2 PAG. 97).

GRÁFICO 10: RECOMENDACIÓN DE UN FIREWALL DE LOS DOCENTES (VER ANEXO 3 PAG. 107).

ANÁLISIS E INTERPRETACIÓN:

Un 73% de ingenieros han recomendado a sus alumnos la utilización de un firewall porque instalado y configurado correctamente brinda protección de datos y dispositivos del equipo o del servidor, mientras que el 27% cree que no los alumnos manejen archivos dentro de la institución. Al analizar lo antes mencionado podemos decir que los archivos que manejan los estudiantes por lo general son bajados de la red de la institución.

4. **¿Sabe usted si los recursos que requieren protección se encuentran aislados, para reducir el nivel de riesgo que puedan tener?**

Si_____

No_____

No sabe_____

TABLA 15: PORCENTAJE DE CONOCIMIENTO DE LA PROTECCIÓN DE DATOS A LOS DOCENTES (VER ANEXO 2 PAG. 98).

GRÁFICO 11: PORCENTAJE DE CONOCIMIENTO DE LA PROTECCIÓN DE DATOS A LOS DOCENTES (VER ANEXO 3 PAG. 108).

ANÁLISIS E INTERPRETACIÓN:

Como podemos ver 47% no está al tanto de que se encuentren o no aislados los recursos que necesiten protección para así reducir el nivel de riesgo, mientras un 46% dicen que si tienen su debida protección y el 7% lo ignora por varias razones adversas a la misma.

5. ¿Qué actividad implica un mayor riesgo de exposición del ordenador a un virus?

A. Visitar sitios Web que no son seguros.

B. Descargar archivos de medios o software de Internet.

C. Especificar información personal o realizar compras en línea.

D. Permitir a amigos y familiares que utilicen el ordenador.

TABLA 16: PORCENTAJE RIESGO DEL ORDENADOR A LOS DOCENTES (VER ANEXO 2 PAG. 98).

GRÁFICO 12: PORCENTAJE RIESGO DEL ORDENADOR A LOS DOCENTES (VER ANEXO 3 PAG. 108).

ANÁLISIS E INTERPRETACIÓN:

Podemos decir que la mayoría de ingenieros coinciden con un 33% que al descargar archivos o software implica mayor riesgo para la Pc, el segundo que implica mas riego con el 27% al visitar sitios web que no son seguros, como tercero y cuarto coinciden con un 20% que al realizar compras en línea y permitir amigos y familiares utilicen el ordenador es menos riesgoso que los anteriores.

6. ¿Es necesario eliminar todas las cookies para proteger ordenador para una mejor navegación en el Internet?

Si_____

No_____

TABLA 17: ELIMINACIÓN DE COOKIES A LOS DOCENTES (VER ANEXO 2 PAG. 99).

GRÁFICO 13: ELIMINACIÓN DE COOKIES A LOS DOCENTES (VER ANEXO 3 PAG. 109).

ANÁLISIS E INTERPRETACIÓN:

El 53% de ingenieros encuestados coincide que no es necesario eliminar los cookies ya que no representan ningún riesgo al ordenador, pero un 47% cree que si ya que no al eliminarse podrían otros estudiantes ingresar y utilizar de forma maliciosa, además de ocupar espacio en la memoria.

7. ¿En la institución se maneja a las Pc's usuarios con privilegios de invitados?

Si_____

No_____

TABLA 18: MANEJO DE USUARIOS DE LOS DOCENTES (VER ANEXO 2 PAG. 99).

GRÁFICO 14: MANEJO DE USUARIOS DE LOS DOCENTES (VER ANEXO 3 PAG. 109).

ANÁLISIS E INTERPRETACIÓN:

El 87% de ingenieros utilizan los privilegios de administrador ya que ellos requieren el ingreso para la instalación y configuración de programas, pero en un 13% dicen que no manejan el administrador sino solo trabajan como usuario invitado teniendo restricciones en la Pc's.

2.4.3 Análisis e Interpretación de los Resultados de la Encuesta Aplicadas a los Administrativos de las Salas de Cómputo.

1. ¿Cuándo cree usted que está más vulnerable la Pc cuando se navega en la red?

a) Cuando se descarga archivos…….
b) Cuando se chatea…….

c) Al ingresar a páginas de alto contenido…….

TABLA 19: PORCENTAJE DE CONOCIMIENTO DE LA VULNERABILIDAD DE LA PC A LOS ADMINISTRATIVOS (VER ANEXO 2 PAG. 100).

GRÁFICO 15: PORCENTAJE DE CONOCIMIENTO DE LA VULNERABILIDAD DE LA PC A LOS ADMINISTRATIVOS (VER ANEXO 3 PAG. 110).

ANÁLISIS E INTERPRETACIÓN:

En un 75% de los administrativos encuestados afirman que cuando se descargan archivos del Internet se encuentra más vulnerable la Pc, mientras el 25% restante cree que al ingresar a las páginas de alto contenido se puede infectar la Pc y por ultimo un 0% creen que cuando se a chatea no se está expuesto a ningún riesgo.

2. **¿Cree usted que el cortafuego que posee Universidad abarca todos los requisitos necesarios para la seguridad de la red?**

a) Si…….
b) No……

TABLA 20: PORCENTAJE DE CONOCIMIENTO DEL FIREWALL DE LA UNIVERSIDAD A LOS ADMINISTRATIVOS (VER ANEXO 2 PAG. 100).

GRÁFICO 16: PORCENTAJE DE CONOCIMIENTO DEL FIREWALL DE LA UNIVERSIDAD A LOS ADMINISTRATIVOS (VER ANEXO 3 PAG. 110).

ANÁLISIS E INTERPRETACIÓN:

En el 75% de los administrativos creen que el cortafuego que posee la Universidad no protege la seguridad de la red, mientras que el 25% restante dice lo contrario. Con estos valores podemos concluir que necesario la instalación de esta herramienta ya que el cortafuego de la universidad no es completamente seguro.

3. ¿Cree usted que es necesario la instalación de un firewall tipo software?

a) Si…….
b) No……

TABLA 21: NECESIDAD DE INSTALACIÓN DE UN FIREWALL TIPO SOFTWARE EN LA UNIVERSIDAD A LOS ADMINISTRATIVOS (VER ANEXO 2 PAG. 101).

GRÁFICO 17: NECESIDAD DE INSTALACIÓN DE UN FIREWALL TIPO SOFTWARE EN LA UNIVERSIDAD A LOS ADMINISTRATIVOS (VER ANEXO 3 PAG. 111).

ANÁLISIS E INTERPRETACIÓN:

En este cuadro estadístico podemos observar que el 75% cree que es necesaria la instalación de un cortafuego de tipo software, y el 25% restante cree que no es ineludible la instalación del mismo. Con esto podemos asegurar que nuestra investigación se fundamenta con todo lo desarrollado anteriormente

4. ¿Usted ha manipulado o se familiariza con un firewall?

a) Si…….
b) No……

TABLA 22: INTERACCIÓN DE UN FIREWALL A LOS ADMINISTRATIVOS (VER ANEXO 2 PAG. 101).

GRÁFICO 18: INTERACCIÓN DE UN FIREWALL A LOS ADMINISTRATIVOS (VER ANEXO 3 PAG. 111).

ANÁLISIS E INTERPRETACIÓN:

La mayoría de los administrativos que es 75% de la población encuestada ha manipulado esta herramienta ya que esta a la mano además de ser gratuito, se lo puede encontrar fácilmente en el Internet y apenas un 25% no los ha utilizado.

5. ¿Cree usted que un firewall mejorara el rendimiento de las Pc's?

a) Si…….
b) No……

TABLA 23: RENDIMIENTO DE LAS PC'S CON UN FIREWALL A LOS ADMINISTRATIVOS (VER ANEXO 2 PAG. 102).

GRÁFICO 19: RENDIMIENTO DE LA PC'S CON UN FIREWALL A LOS ADMINISTRATIVOS (VER ANEXO 3 PAG. 112).

ANÁLISIS E INTERPRETACIÓN:

Podemos darnos cuenta que el 75% nos da a conocer que firewall mejorara el rendimiento de la Pc's y el 25% restante cree que no.

2.5 Análisis Comparativo Técnico De Los Firewalls.

2.5.1 Análisis.

En este punto detallaremos en diferentes tablas los datos de descarga, las reglas de filtrado, comprobación de datos de uso y una de fase de prueba de cada uno de los cortafuegos para ver así su desempeño.

2.5.2 Descarga e Instalación.

Son todos muy fáciles y rápidos de instalar, su idioma es el español.

TABLA 1: DATOS DE DESCARGA E INSTALACIÓN.

Programa	Proceso de descarga	Tamaño de descarga	Dificultad de instalación	Tamaño de programa instalación	Tipo de archivo	Reinicio de sistema
Pc Tools	Sencillo	6,40 MB	Sencillo	18.26 MB	Ejecutable (EXE)	Si
Agnitum Outpost Free	Sencillo	2,49 MB	Sencillo	7 MB	Ejecutable (EXE)	Si
Sunblet Personal	Sencillo	5,72 MB	Sencillo	11 MB	Ejecutable (EXE)	Si
Ashampoo	Sencillo	4,08 MB	Sencillo	20 MB	Ejecutable (EXE)	Si

Características.

Si bien todos apuntan a lo mismo, cada uno lo hace o lo presenta de manera diferente y se destaca por algún punto. Algunos se manejan por zonas seguras o no y otros por niveles de seguridad. Todos tienen acceso desde la barra de herramientas de Windows y su icono resulta multifunción, permite acceder al programa pero también informa sobre estado de conexión, tráfico y elementos bloqueados (cambia de color, titilan, cambian de forma, etc.).

2.5.3 Formas de Acceso.

TABLA 2: CARACTERÍSTICAS Y TIPOS DE FILTRADO.

Reglas de Filtrado					
Programa	**Protocolo y puerto**	**Aplicación**	**Sitios de confianza**	**Dirección IP**	**Idioma**
Pc Tools	Opcional	Si	Si	No	Español
Agnitum Outpost Free	No	Si	No	No	Español
Sunblet Personal	No	Si	No	No	Español
Ashampoo	No	Si	Si	No	Español

Interfaces y menús.

Todos los programas presentados tienen excelentes interfases, muy claras y accesibles, pero los que se destacan son Pc Tools y Outpost porque están en español y muy bien traducidas.

Operaciones.

Todos manejan su configuración con el uso mediante alarmas o alertas en forma de carteles que piden una acción a seguir. Esa acción puede configurar una regla para siempre o no según lo que determine el usuario. Además permiten modificar o crear reglas “manualmente “desde su configuración.

TABLA 3: COMPARACIÓN DE DATOS DE USO.

Programa	Uso y aprendizaje	Interfaz	Licencia	Desinstalador
Pc Tools	Por tener mas opciones de ayuda es intuitivo	Excelente y en español	Gratuito	Si
Agnitum Outpost Free	Por tener mas opciones, su aprendizaje no es tan intuitivo	Muy buena y en español	Gratuito, limite de 30 días	Si
Sunblet Personal	Complicado	Excelente y en español	Gratuito	SI
Ashampoo	Fácil	Muy bueno y en español	Gratuito	Si

2.5.4 Fase de Prueba entre los Cortafuegos.

Un cortafuego para cada Pc's siempre y cuando sea lo mejor y debe ser probado para ver si se amolda a las necesidades de la Institución y sobre todo si son un habitual usuario de protocolos o aplicaciones de red particulares.

TABLA 4: CARACTERÍSTICAS PRINCIPALES DE LOS FIREWALLS EN SU FASE DE PRUEBA.

	Sunblet Personal	Pc Tools	Ashampoo	Agnitium Outpost
Niveles de seguridad	Sin conexión, restrictivo, normal y permisivo	Sin conexión y normal	Sin conexión, alto, medio, bajo y desactivado	Desactivado, medio y alto
Desactivación	Fácil y rápida	Cerrando el programa	Fácil y rápida	Cerrando el programa
Reglas configurables	Sí, muchas opciones	Sí	Sí, por programa, dirección, ámbito de la red y hora	Muy básicas
Registro de conexiones	Sí	Sí	Sí, completo	No
Estadísticas	Sí, desglosado por programas	Sí, y también para cada programa	Sí	Sí, muy escasas
Consumo memoria	Muy bajo	Bajo	Bajo	Normal - Alto
Uso de CPU	Prácticamente nulo	Muy bajo	Bajo	Prácticamente nulo
¿En español?	Sí	Si	Si	Si
Nota	8.0	8.5	8.0	7.0

2.5.5 Conclusiones Acerca de los Cortafuegos.

Los cortafuegos, como seguridad pasiva, se esperan de él que sea precisamente eso, pasivo, y que no tome mucho protagonismo en nuestro equipo y nos deje trabajar, funcionando él mientras tanto de forma transparente y sin intervenir.

Pc Tools.

Sin dudas el mejor de todos. Tiene todo lo que tiene que tener, hace todo y bien, excelente interfaz, tiene un manual de ayuda. Eso si, no es recomendable para iniciados y aún puede resultar confuso para experimentados por la apabullante cantidad de funciones y opciones. Además está totalmente en español.

Agnitum Outpost Free.

La instalación, ayudas están en español, el programa tiene interfaz y alarmas en español. Tiene más funciones y posibilidades de configuración que otros Firewalls lo que lo hace recomendable para usuarios más expertos, su interfaz no es brillante desde el diseño pero si en cómo están organizadas sus funciones. Lo más interesante son sus plug ins, también gratuitos, que potencian al programa con bloqueadores de pop ups, banners, etc.

Además presenta opciones más o menos equilibradas, ni muy avanzadas, ni demasiado simples, aunque en general Agnitium, en su peculiar estructuración de la interfaz, algo desfasada, presenta más opciones, si bien son menos accesibles.

Sunblet Personal Firewall.

Tan bueno como el anterior pero totalmente en español. Lo mejor: es muy fácil de usar, excelente interfaz y tiene enlace directo al sitio de Sygate que analiza la Pc en busca de vulnerabilidades.

Ashampoo.

Es el menos potente pero resulta el más indicado para quienes nunca hayan utilizado un Firewall y no tengan demasiada experiencia en este terreno o en general. Esto gracias a su excelente interfaz y múltiples ayudas totalmente en español. Además tiene pocas opciones de configuración lo que tal vez no es muy interesante para los más experimentados pero muy útil para los novatos. Sus alarmas son muy claras y si hay dudas enlaza directamente con su sitio donde recomienda la acción a seguir. Brillante en cuanto a la asistencia al usuario.

2.6 Verificación De La Hipótesis.

Nuestra hipótesis fue la siguiente"La Implementación De Un Cortafuego De Tipo Software Permitirá La Seguridad De La Red De Banda Ancha, Renovando El Rendimiento De Cada Pc".

Dado con los resultados de las encuestas hace necesario tener un cortafuego de tipo software en la Universidad ya que la mayoría que navegamos en la red tenemos alguna complicación especialmente en la que son descargas, con este cortafuego que nosotros queremos implementar tendremos más confiabilidad en la navegación

asegurar la red de invasiones no deseadas y por ende mejorara el rendimiento de las Pc’s del laboratorio, en el que este nos permite escoger se queremos o no descargar cualquier programa, sabiendo que en las descargas hay un alto grado de que la Pc se infecte de virus y en peor de las casos que ingrese un troyano al sistema.

Con lo antes mencionado podemos verificar que la hipótesis se cumple con todas las metas establecidas, comprobando así que un firewall tipo software es necesario.