CAPÍTULO I.

FUNDAMENTACIÓN TEÓRICA.

1. Descripción General de un Cortafuego.

1.1 Cortafuego.

En la actualidad, las organizaciones son cada vez más dependientes de sus redes Informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones.

La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización.

La propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. En medio de esta variedad, han ido aumentando las acciones poco respetuosas de la privacidad y de la propiedad de recursos y sistemas. "Hackers", "Crakers", entre otros, han hecho aparición en el vocabulario ordinario de los usuarios y de los administradores de las redes.

Además de las técnicas y herramientas criptográficas, es importante recalcar que un componente muy trascendental para la protección de los sistemas consiste en la atención, vigilancia continua y sistemática por parte de los responsables de la red. Virus, programas espía, troyanos. Las amenazas cada vez son más numerosas y peligrosas. Extremar las precauciones y mantener el antivirus actualizado no puede ser suficiente.

Los cortafuegos pueden impedir eficazmente el acceso no autorizado a recursos personales en un ordenador con acceso de banda ancha. Se trata de programas o equipos que controlan cualquier comunicación que entre o salga del ordenador (o red). Los cortafuegos se pueden configurar para permitir que sólo ciertas aplicaciones puedan acceder a la conexión de banda ancha y rechazar ciertos tipos de solicitudes del exterior (tales como las exploraciones).

1.1.1 Reseña Histórica Del Cortafuego.

Según la dirección electrónica (http://www.monografias.com/trabajos14/firewalls/firewalls.shtml) el primer

cortafuego en un ordenador fue una máquina Unix que no realizaba tareas de encaminamiento con conexiones a dos redes distintas. Una tarjeta de red conectada a Internet y la otra al LAN (Red de área Local) privado. Si quería acceder a Internet desde la red privada, tenía que registrarse en un servidor (Unix) de cortafuegos. Por lo tanto, se utilizaban los recursos del sistema para acceder a Internet.

Conectar su Pc al Internet sin protegerla primero equivale a dejar su domicilio sin pasar la aldaba, ya que tarde o temprano, le registrará y lo despojará de sus prendas. Para hacer los puntos de entrada a su Pc más seguros en la Red, instale uno de los muchos programas cortafuegos gratuitos que se encuentran disponibles ahora, todo el mundo ha oído hablar alguna vez y su empleo es más o menos mayoritario, pero el término "Firewall" provoca desconcierto y desconocimiento en el que lo escucha.

La idea es muy sencilla y extraordinariamente útil e importante; tan importante que la presencia de un "Firewall" pasará a ser un estándar de cualquier equipo en el futuro; baste como prueba que Microsoft incluye de serie uno en su Windows XP.

Importante es también comprender el concepto de que no solamente es necesario controlar la información que llega a nuestro ordenador, sino también la que sale. Muchos 'troyanos' actúan libremente transmitiendo información de nuestro equipo a su creador, por no hablar aquí de la enorme cantidad de programas gratuitos cuyo precio a pagar es la comunicación de datos, sin nuestro conocimiento, sobre nuestra navegación en Internet a los creadores de ese programa, en lo que se denomina "spyware".

1.1.2 Concepto De Cortafuego.

Es un mecanismo para restringir acceso entre la Internet y la red corporativa interna. Típicamente se instala un Cortafuego en un punto estratégico donde una red (o redes) se conectan a la Internet.

Un buen Cortafuego para Internet puede ayudarle a impedir que extraños accedan a su Pc desde Internet. Los cortafuegos pueden ser de dos tipos, de software o de hardware, y proporcionan una frontera de protección que ayuda a mantener fuera a los invasores no deseados de Internet.

La existencia de un Cortafuego en un sitio Internet reduce considerablemente las probabilidades de ataques externos a los sistemas corporativos y redes internas, además puede servir para evitar que los propios usuarios internos comprometan la seguridad de la red al enviar información peligrosa (como passwords no encriptados o datos sensitivos para la organización) hacia el mundo externo.

Si el Cortafuego "observa" alguna actividad sospechosa: que alguien de fuera esté intentando acceder a nuestro Pc o que algún programa espía trate de enviar información sin consentimiento, el Cortafuego nos advertirá con una alarma en el sistema. Para entender el funcionamiento de este sistema, debes saber que el ordenador dispone de varias puertas de salida y entrada cuando se conecta a Internet.

1.1.3 Origen de la Palabra Cortafuego o Firewall.

El concepto de Firewall proviene de la mecánica automotriz, donde se lo considera una lámina protectora / separadora entre el habitáculo de un vehículo y las partes combustibles del motor, que protege a sus pasajeros en caso de incendio. Análogamente un Firewall en un sentido más informático, es un sistema capaz de separar el habitáculo de nuestra red, o sea, el área interna de la misma, del posible incendio de crackers que se produciría en ese gran motor que es Internet.

1.1.4 Funciones del Cortafuego.

Un cortafuego sirve para múltiples propósitos, entre otros podemos anotar los siguientes:

- Nos permite limitar la entrada de usuarios a puntos cuidadosamente controlados de la red interna.
- Notifica ante los intrusos que tratan de ganar espacio hacia el interior de la red y los otros esquemas de defensas establecidos.
- Localiza el uso de servicios tanto a usuarios internos como externos.

Todo el tráfico que viene de la Internet o sale de la red corporativa o institucional interna pasa por el Cortafuego de tal forma que él decide si es aceptable o no.

Un Cortafuego constituye una especie de barrera delante de nuestro equipo que examina todos y cada uno de los paquetes de información que tratan de atravesar.

El Cortafuego actúa de intermediario a nuestra red local e Internet, filtrando el tráfico que pasa por él. Para que cada uno de los paquetes de información pueda llegar a su destino, independientemente donde se encuentre las Pc´s que se comunican, debe llevar anexada la información referente a la dirección IP del puerto de cada Pc. La dirección IP es un dispositivo que identifica a la misma de manera única dentro de la red de igual forma el puerto nos ayuda a comunicarnos ya que lo podríamos compara con una frecuencia de una emisora radiofónica, ya que sin no sintonizamos bien su frecuencia no podemos escucharla, de la misma manera no podremos conectarnos a un servicio de otro equipo si no usamos el mismo puerto.

1.1.5 Beneficios Del Cortafuego.

Son el pilar de este sistema, informan a los usuarios de sus responsabilidades, normas de acceso remoto o local, políticas de acceso a los recursos de la red, reglas de encriptación, normas de protección de virus y entretenimiento.

La misión del cortafuego de Internet es garantizar la seguridad de nuestro equipo ante los peligros cibernéticos de la red de área local (LAN) o bien, mantener a los miembros de esa LAN al margen de las malignas intenciones de Internet.

Protege de intrusiones.

El acceso a ciertos segmentos de la red de una organización, sólo se permite desde máquinas autorizadas de otros segmentos de la organización o de Internet, además protege a los servidores propios del sistema de ataques de otros servidores en Internet.

Protección de información privada.

Permite definir distintos niveles de acceso a la información de manera que en una organización cada grupo de usuarios definido tendrá acceso sólo a los servicios y la información que le son estrictamente necesarios.

Administra la red definir un "choke point" (embudo), manteniendo al margen los usuarios no-autorizados, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red.

Optimización de acceso.

Identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea más directa. Esto ayuda a reconfigurar los parámetros de seguridad.

Concentra la seguridad.

El Cortafuego facilita la labor a los responsables de seguridad, dado que su máxima preocupación de encarar los ataques externos y vigilar, mantener un monitoreo.

Control y estadísticas.

Permite controlar el uso de internet en el ámbito interno y conocer los intentos de conexiones desde el exterior y detectar actividades sospechosas.

Genera alarmas de seguridad

El administrador del firewall puede tomar el tiempo para responder una alarma y examina regularmente los registros de base.

Audita y registra internet.

Permite al administrador de red justificar el gasto que implica la conexión a internet, localizando con precisión los cuellos de botella potenciales del ancho de banda.

1.1.6 Limitaciones del Cortafuego.

Únicamente puede autorizar el paso del tráfico, y él mismo podrá ser inmune a la penetración. Desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece en torno a éste.

- No puede proteger contra aquellos ataques que se efectúen fuera de su punto de operación.
- No puede proteger de las amenazas a que está sometido por traidores o usuarios inconscientes.
- No puede prohibir que los traidores o espías corporativos copien datos sensitivos y los substraigan de la empresa.
- No puede proteger contra los ataques de la "Ingeniería Social", por ejemplo un Hacker que pretende ser un supervisor o un nuevo empleado despistado.
- No puede proteger contra los ataques posibles a la red interna por virus informativos a través de archivos y software.

1.1.7 Políticas del Cortafuego.

Un Cortafuego opera en las capas de red y transporte en cuyo caso examinan los encabezados IP y TCP, (paquetes entrantes y salientes), y rechazan o pasan paquetes con base a reglas de filtración de paquetes programadas.

Según la dirección electrónica (http://www.monografias.com/trabajos14/cortafuego.shtml) hay dos políticas básicas en la configuración de un cortafuego y que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

- ***Política restrictiva.***

  Se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafuego obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten.

  Asume que un Cortafuego puede obstruir todo el tráfico y cada uno de los servicios o aplicaciones deseadas necesariamente y ser aplicadas caso por caso.

- ***Política permisiva***.

  Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado.

Se ocupa de desplazar todo el tráfico y que cada servicio potencialmente peligroso necesitara ser aislado básicamente caso por caso.

La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por defecto.

Esto es importante, ya que debemos de notar que un Cortafuego de Internet no es justamente un ruteador, un servidor de defensa, o una combinación de elementos que proveen seguridad para la red. El Cortafuego es parte de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información.

Esta política de seguridad podrá incluir publicaciones con las guías de ayuda donde se informe a los usuarios de sus responsabilidades, normas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, normas de dial-in y dial-out, reglas de encriptación de datos y discos, normas de protección de virus, y entretenimiento. Todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad. Un Cortafuego de Internet sin una política de seguridad comprensiva es como poner una puerta de acero en una tienda.

1.1.7.1 Políticas Internas de Seguridad.

Un Cortafuego de Internet no está solo, es parte de la política de seguridad total en

una organización. Para que ésta sea exitosa, la organización debe conocer qué es lo se está protegiendo.

La política de seguridad se basara en una conducción cuidadosa analizando la seguridad, la asesoría en caso de riesgo. Las herramientas para complementar su seguridad en la red, mediante la imposición de políticas de seguridad, en el acceso a los recursos de la red y hacia la red externa, es importante establecer que un monitoreo constante de el registro base, nos permitirá detectar un posible intruso y así proteger la información. Es evidente que el costo de un cortafuego dependerá de los recursos que necesita proteger la empresa para así tomar la decisión de optar por la compra de un ellos o a su vez experimentar con un gratuito.

1.1.8 Costo del Cortafuego.

¿Cuánto puede ofrecer una organización por su seguridad?

- Un simple paquete de filtrado puede tener un costo mínimo.
- Un Cortafuego casero.
- Un sistema comercial.

Finalmente requiere de soporte continuo para la administración, mantenimiento general, actualización de software, reparación de seguridad, e incidentes de manejo. Para tener todos los derechos de un Cortafuego la organización debe comprar las licencias para el cortafuego sea instalado y administrado directamente desde su servidor y por sus administrativos.

1.2 Sistema Operativo Para Los Ordenadores.

1.2.1 Sistema Operativo Windows Xp Profesional.

Según la página electrónica (http://es.wikipedia.org/wiki/Windows_XP) Windows XP (cuyo nombre en clave inicial fue *Whistler*) es una línea de sistemas operativos desarrollado por Microsoft que fueron hechos públicos el 25 de octubre de 2001. Se considera que están en el mercado 400 millones de copias funcionando. Las letras "**XP**" provienen de la palabra 'e**XP**eriencia'.

Dispone de versiones para varios entornos informáticos, incluyendo computadoras domésticas o de negocios, computadoras portátiles, las llamadas "Tablet PC" y media center. Sucesor de Windows 2000 y Windows ME y antecesor de Windows Vista; es el primer sistema operativo de Microsoft orientado al consumidor que se construye con un núcleo y arquitectura de Windows NT y que se encuentra disponible en versiones para Pc de 32 y 64 bits.

A diferencia de sus versiones anteriores presenta mejoras en la estabilidad y de la eficacia. Tiene una Interfaz gráfica de usuario (GUI) perceptiblemente reajustada, un cambio de Microsoft promovido para un uso más fácil que en las versiones anteriores. Es también la primera versión de Windows que utiliza la activación del producto para reducir la piratería del software, una restricción que no sentó bien a algunos usuarios. Ha sido también criticado por las vulnerabilidades de seguridad, integración de Internet Explorer, la inclusión del reproductor Windows Media Player y aspectos de su interfaz.

Windows XP está construido en el código de Windows 2000 con una nueva interfaz gráfica (llamada *Luna*), el cual incluye características ligeramente rediseñadas, algunas de las cuales se asemejan al entorno de escritorio presente en Mac OS X. La pantalla de login gráfica con imágenes para cada usuario es un buen ejemplo.

El desarrollo de Windows XP parte desde la forma de Windows Neptune. Windows XP fue desarrollado en 18 meses, desde diciembre de 1999 hasta agosto de 2001. Windows XP fue lanzado el 25 de octubre de 2001.

Microsoft producía dos líneas separadas de sistemas operativos. Una línea estaba dirigida a las computadoras domésticas basada en un Núcleo de MS-DOS y representada por Windows 95, Windows 98 y Windows Me, mientras que la otra, basada en un Núcleo "NT" es representada por Windows NT y Windows 2000, estaba pensada para el mercado corporativo y empresarial e incluía versiones especiales para servidores. Windows ME "Millenium" fue un intento por parte de Microsoft de ofrecer un único sistema operativo multiuso, aunque falló por poseer el núcleo de arranque de MS-DOS con el código NT de Windows, Windows XP fue la verdadera fusión de un sistema operativo único basado enteramente en la arquitectura NT contando con la funcionalidad de MS-DOS, con el, se eliminó definitivamente el soporte para los programas basados en MS-DOS del sistema operativo.

1.2.2 Características de Windows Xp.

Windows XP introdujo nuevas características, incluyendo:

- Ambiente totalmente gráfico.
- Secuencias más rápidas de inicio y de hibernación.
- Capacidad del sistema operativo de desconectar un dispositivo externo, de instalar nuevas aplicaciones y controladores sin necesidad de reiniciar.
- Una nueva interfaz de uso más fácil, incluyendo herramientas para el desarrollo de temas de escritorio.
- Uso de varias cuentas, que permite un usuario guarde el estado actual y aplicaciones abiertos en su escritorio y permita que otro usuario abra una sesión sin perder esa información.
- ClearType, diseñado para mejorar legibilidad del texto encendido en pantallas de cristal líquido (LCD) y monitores similares.
- Escritorio Remoto, que permite a los usuarios abrir una sesión con una computadora que funciona con Windows XP a través de una red o Internet, teniendo acceso a sus usos, archivos, impresoras, y dispositivos;
- Soporte para la mayoría de módems ADSL y conexiones wireless, así como el establecimiento de una red FireWire.

1.2.3 Interfaz de Windows Xp.

Windows XP, ofrece una nueva interfaz gráfica. El menú del comienzo y capacidad de indexación de directorios de Windows fue reajustado y muchos efectos visuales fueron agregados, incluyendo:

- Un rectángulo azul translúcido en la selección de los archivos.
- Un gráfico en los iconos de la carpeta, indicando el tipo de información que se almacena.

- Sombras para las etiquetas del icono en el tablero del escritorio.
- Capacidad de agrupar aplicaciones similares en la barra de tareas.
- Capacidad para prevenir cambios accidentales.
- Destaca programas recién instalados en el menú de inicio.
- Sombras bajo los menús (Windows 2000 tenía bajo el puntero del mouse, pero no en los menús).

Windows XP analiza el impacto del funcionamiento de efectos visuales y mediante esto determina si debe o no permitirlos, para evitar que la nueva funcionalidad consuma recursos en forma excesiva. Los usuarios pueden modificar más estos ajustes para requisitos particulares.

Algunos efectos, tales como mezcla alfa (transparencia), son dirigidos enteramente a muchas tarjetas de vídeo más nuevas. Sin embargo, si la tarjeta gráfica no es capaz, el funcionamiento puede verse reducido substancialmente y Microsoft recomienda la característica de apagado manualmente. Windows XP agrega la capacidad para el uso de “estilos visuales” para cambiar la interfaz gráfica. Sin embargo, los estilos visuales son firmados mediante criptografía por Microsoft para funcionar.

El estilo *Luna* es el nombre del nuevo estilo visual por defecto de Windows XP para máquinas con más que 64 MB de RAM. *Luna* se refiere solamente a un estilo visual particular, no a todas las nuevas características del interfaz de usuario de Windows XP en su totalidad.

El papel tapiz por defecto, es una fotografía BMP de un paisaje en valle de Napa, California, con colinas verdes, un cielo azul y nubes cirros. El interfaz “clásico” del Windows 2000 puede ser utilizado en lugar de otro si está preferido. Existen varias utilidades de terceros que proporcionan centenares de diversos estilos visuales. Además, Microsoft creó el tema, llamado "Energy Blue", que fue incluido con la edición Media center de Windows XP y también fue lanzado para otras versiones de Windows XP, pero más adelante fue quitado del paquete original de Microsoft Nueva Zelanda.

El tema clásico de las ventanas es extensamente popular en los países del Tercer Mundo (debido a la familiaridad con las versiones anteriores de Windows), no obstante las ventanas “clásicas” utilizan el mismo interfaz que el otro tema estándar de Windows XP y no afectan el funcionamiento.

1.3 Banda Ancha.

Según la dirección electrónica (http://es.wikipedia.org/wiki/Banda_ancha) define banda ancha, a la transmisión de datos en el cual se envían simultáneamente varias piezas de información, con el objeto de incrementar la velocidad de transmisión efectiva.

Comúnmente se relacionan una serie de características a la banda ancha, en lo que a Internet se refiere, son:

- Conexión permanente, permitiendo a su vez la utilización de otra banda diferente del medio para otros fines (servicios de voz, TV).

- Conexión mediante TCP/IP de cara al cliente, conectando internamente por medios de alta velocidad del tipo **ATM** (*Asynchronous Transfer Mode*). Ancho de banda dedicado de al menos 1Mbps (aunque por diferentes cuestiones se denominan conexiones de banda ancha a aquellas que van a velocidades superiores a los 256Kbps).
- Conexión normalmente asincrónica, en la que la velocidad de bajada (tráfico de datos entre el operador y el cliente) es muy superior a la de subida (tráfico de datos entre el cliente y el operador).
- Normalmente se asocia su conexión a una Tarifa plana, en la que se paga una cantidad fija por la conexión y por el ancho de banda contratado, independientemente del tráfico de datos que se realice.

1.4 Rendimiento De La Pc.

El objetivo fundamental de esta investigación es proporcionar una serie de conocimientos básicos para cómo mantener unos niveles razonables de seguridad en un PC. Además aprenderán a instalar, configurar y administrar un cortafuego que ayudarán a estar más protegido en Internet, y a la vez, a que nuestro PC no se convierta en una fuente de inseguridad para amigos y colegas. Asimismo, se desarrollan una serie de estrategias y consejos básicos sobre cómo mantenernos informados y seguros en Internet.

Donde protegeremos los recursos de las mismas como son los siguientes:

- Protegiendo tus datos.
- Protegiendo tu correo electrónico.

- Protegiendo tu navegación.

Con el manejo de este cortafuego nosotros podemos mejorar el rendimiento de la Pc, con el no autorizado de códigos maliciosos, ataques de IMCP (protocolo de control de mensajería de internet) no solicitados, la perdida de información, la desactivación de iconos de acceso directo y la prohibición de instalación de software que requiere el usuario.

Para así ayudar a proteger y a mejorar el rendimiento de la Pc, pero no solo depende de un cortafuego sino también de varios factores como son:

- Mantener actualizado el sistema.
- Realiza copias de seguridad periódicas.
- Controla el acceso a Internet desde la PC.
- Gestionar contraseñas.
- Usar un antivirus.
- Utilizar herramientas de desinfección, etc.