Facultad de Ingeniería

Tecnología en Redes y Telecomunicaciones

Seguridad informática, evaluación, comparación e implementación de equipos de seguridad

Trabajo de Titulación presentado en conformidad a los requisitos

Para obtener el título de tecnólogo en Redes y Telecomunicaciones

Profesor guía: Ing. Henry Burbano

Autor: Marco Castillo B.

2010

DECLARACIÓN DEL PROFESOR GUÍA

Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema y tomando en cuenta la Guía de Trabajos de Titulación correspondiente.

Henry Burbano
Ingeniero
C.C.1711476083

DECLARACIÓN DE AUTORIA DEL ESTUDIANTE

Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

Marco Castillo B.
C.C. 1714907621

AGRADECIMIENTOS

Mi sincera gratitud a mi profesor guía por su interés y dedicación para hacer que este trabajo sea mejor, para él mis mejores deseos. También quiero agradecer a la Universidad por haberme conducido por el camino del conocimiento y por todas las experiencias y vivencias que permanecerán por

DEDICATORIA

Este trabajo va dedicado de todo corazón a Dios y a mis padres por ser mi fuente de inspiración en mis fortalezas y debilidades.

RESUMEN

El principal objetivo de este trabajo es dar a conocer la importancia de la seguridad informática, que debería ser implementada en cualquier tipo de organización, sin importar su tamaño y actividad. Realmente son pocas las organizaciones que en un medio como Ecuador tienen implementada una política de seguridad informática adecuada, otras organizaciones la tienen implementada de una manera inadecuada porque no se hizo un análisis de riesgos, no se audito los procedimientos y operaciones del sistema informático entero, etc., y otras organizaciones simplemente no tienen ninguna política de seguridad informática.

Otro objetivo es dar una idea coherente y lógica de cómo implementar los recursos físicos, lógicos y de servicios, bajo normas y políticas de seguridad informáticas claras, acorde a los avances tecnológicos y a las necesidades y requerimientos de la organización y así ajustarse a su realidad.

Mediante un grupo de sistemas y recursos que combinan diversos componentes tanto a nivel de hardware como de software, se establece métodos de implementación y administración adecuados para cubrir las necesidades de seguridad de una organización en la parte informática en su conjunto y así reducir el riesgo frente a las diversas amenazas y ataques y estar siempre un paso al frente de posibles vulnerabilidades, a la vez que se busca que las organizaciones optimicen y aprovechen de mejor manera sus recursos informáticos para de esta forma contribuir a obtener una mejor productividad a menores costos.

También se hace una comparación de las soluciones que brindan una plataforma comercial y una plataforma libre, en cuanto a costos de implementación y mantenimiento, facilidad de implementación de los servicios y aplicaciones, nivel de seguridad, entre otras. Todo con el objetivo de dar una solución acorde a las necesidades reales de una organización.

ABSTRACT

The main objective of this work is to communicate the importance of computer security, which should be implemented in any company, regardless of its size and activity. Actually there are few companies in the business environment as Ecuador have implemented an appropriate security policy, other companies have implemented an improper, because it was a risk analysis, no audit procedures and operations of whole computer system, etc., and others companies simply do not have any computer security policy.

Another objective is to provide a coherent vision of how to implement logical and physical resources, software and services, under security standers and clear policies, in cutting edge with technological advances and the needs and requirements of the companies and conform its reality.

Through a set of systems and resources that combine various components both hardware and software, provides implementation and management methods appropriate to meet the security needs of a company at the computer as a whole and reduce the risk exposure to the various threats and attacks, and always one step ahead of potential vulnerabilities, while companies are seeking to optimize and better exploit their resources in this way to help achieve higher productivity to lower costs.

It also makes a comparison of the solutions that provide a commercial platform and a free platform, in terms of implementation and maintenance costs, ease of deployment of services and applications, security level, among others. All with the goal of providing a consistent solution to the real needs of a company.

INDICE

INTRODUCCIÓN

Son muchas las empresas que no están conscientes de la seguridad informática que deberían adoptar para hacer que sus sistemas de información sean menos vulnerables, esto dependerá de las necesidades de cada empresa, del tamaño y del tipo y la calidad de información que manejen las mismas. Si el internet es ahora visto como un modelo con un gran potencial para hacer negocios, la información es enviada y recibida a través de muchos computadores y siempre existirá una posibilidad de que alguien revise o robe información, esto podría afectar en algún momento a cualquier organización que trabaje parcial o totalmente en línea.

Si se pone un ejemplo, a nadie le gustaría que desconocidos abran su correspondencia, que hagan copias de las llaves de su casa, de las de su escritorio o las de su vehículo, que obtengan los datos de su tarjeta de crédito o débito. Pues todo esto es aplicable en la misma medida a las redes de datos.

Con la globalización de las conexiones a internet y el rápido desarrollo del software, la escalabilidad de tráfico, servicios y la interconectividad e interoperabilidad que proporcionan las nuevas tecnologías se está caminando hacia la *convergencia de redes*, por tanto la seguridad se convierte cada vez más en una cuestión importante, y esta ya es un requisito básico, debido a que la red global es insegura por definición y se hace necesario el conocimiento y el uso adecuado de las destrezas para un mejor aprovechamiento de las plataformas tecnológicas disponibles.

1. Capítulo I: Políticas de seguridad informática

1.1. ¿Qué es una política de seguridad informática

Una política de seguridad informática es establecer mecanismos y técnicas para mantener comunicaciones seguras, salvaguardar la información y los recursos de un equipo o de una red de datos de una organización, de daños intencionales o accidentales, destrucción y/o robo de la información, transferencia y/o modificación no autorizada de información, saturación de un sistema, virus y otros programas maliciosos, uso no autorizado de un sistema informático o hasta de intrusiones y/o ataques por simple diversión; por lo que para proteger la integridad de la información se lo debe hacer de forma oportuna, precisa, confiable y completa.

"Una política de seguridad es un enunciado formal de las reglas que los usuarios que acceden a los recursos de la red de una organización deben cumplir" *[RFC-2196].*

El concepto de seguridad informática puede variar en cierta medida de un autor a otro, pero lo que sí es importante señalar es que las políticas de seguridad informática por sí solas no constituyen una garantía para la seguridad de los recursos y la información de una organización, estas deben responder a los intereses y necesidades basadas en la visión de la organización.

Se entiende como información a un conjunto de datos que se transmiten y reciben a través de los *canales de comunicación*[1] de un mismo sistema informático o de varios sistemas informáticos.

1.1.1. Conceptos de seguridad informática

Existen dos conceptos de seguridad que están muy relacionados y van de la mano entre si y que engloban todo lo que es la seguridad informática.

[1] Los canales de comunicación son los dispositivos y demás componentes que permiten enviar y recibir la información de forma cableada o inalámbrica o entre una combinación de ambas.

1.1.2. Seguridad computacional

Es una gama de herramientas para controlar el acceso y proteger los componentes de un sistema computacional como son el software, el hardware y la información, de los atacantes, para así evitar amenazas a la confidencialidad, integridad y disponibilidad.

Con el surgimiento de las computadoras la información pasó a estar en formato electrónico, y la seguridad computacional ofrece herramientas automatizadas para proteger la información almacenada.

1.1.3. Seguridad de redes

Este concepto surge con la introducción de los sistemas distribuidos, que a su vez surgieron con el desarrollo tecnológico de las comunicaciones y el uso de las redes, pues con estas se obtienen los medios necesarios para transportar la información entre terminales de usuarios de una misma red de datos o entre redes distintas.

Por lo tanto la seguridad de redes es mantener bajo protección a un conjunto de dispositivos y la información con que estos cuentan, para que no corran riesgo de daños, sin dejar de proporcionar los servicios y sin dejar de compartir los recursos.

Se puede definir 3 tipos de recursos, que son los objetivos clave:

a. **Físicos:** computadores, impresoras, servidores, concentradores, ruteadores, etc.
b. Lógicos**:** sistemas operativos, base de datos y demás software de aplicación con los que trabaja una organización.
c. **Servicios:** página web, correo electrónico. [2]

[2] Subcapítulo y temas desarrollados a partir del libro: *Fundamentos de seguridad, pág. 1,2 y 4, autor: F. Vergara.*

1.2. Elementos para implementar una política de seguridad informática

Las políticas de seguridad informática deben permitir una comprensión clara, sin sacrificar su precisión, es así que deben ser redactadas en un lenguaje sencillo y entendible, libre de tecnicismos y ambigüedades.

Las políticas de seguridad informática deben ofrecer explicaciones comprensibles sobre la importancia de la información y los recursos, y sobretodo el por qué se toman ciertas decisiones, esto con la finalidad de disponer a una organización a conseguir el logro de una visión conjunta de una política de seguridad informática. También es importante que las políticas de seguridad informática sigan un proceso de actualización periódica debido a los avances tecnológicos, aparición de nuevas amenazas, desarrollo de nuevos servicios, cambios organizacionales, cambios en la infraestructura, entre otras.

1.2.1. Consideraciones iniciales

Es necesario establecer *objetivos claros* y *descripciones sencillas* de las políticas de seguridad informática, por lo que es indispensable que el área informática llegue a acuerdos con los altos mandos de una organización acerca de la necesidad y beneficios de buenas políticas de seguridad informática para evitar graves problemas de seguridad e innecesarios riesgos que comprometan la información y por tanto la imagen corporativa de la organización, he aquí la importancia de que el personal entienda y esté de acuerdo con los asuntos importantes de la seguridad informática y las decisiones que conllevan a los mismos; por eso se consideran los siguientes elementos básicos:

a. Las políticas para ser aceptadas en una organización por los que toman las decisiones y demás personal, deben integrarse a las estrategias del negocio, a su misión y visión.

b. Detallar de forma concreta los alcances y aplicaciones de las políticas incluyendo facilidades, equipos, sistemas y personal.

c. Responsabilidades por los servicios y recursos informáticos en cada uno de los niveles de la organización.

d. Proveer de una guía que permita establecer requerimientos mínimos para la implementación configuración y control de los recursos de la red de datos para determinar su conformidad con la política de seguridad informática.

e. Informar a los usuarios sus obligaciones para proteger los recursos de la red de datos.

1.2.2. Aspectos para establecer las políticas de seguridad informática

Se debe tener en cuenta que ninguna red de datos es 100% segura, debido a que esta se mueve bajo un concepto de riesgo estadístico; el único sistema seguro es aquel que no está conectado al internet o está apagado, lo que se puede hacer es aumentar la dificultad para los atacantes que quieren comprometer la seguridad de la red de datos, es decir estar siempre a un paso delante de ellos. Por eso es importante que una organización oriente sus esfuerzos para definir directrices de seguridad informática y concretarlas en documentos que canalicen las acciones de las mismas, con el fin de alcanzar el éxito, parte de este éxito se basa en una relación inversa entre seguridad y funcionalidad para establecer un equilibrio entre la facilidad de uso de los recursos y su seguridad. Entonces se debe considerar los siguientes aspectos:

a. Realizar un *análisis de riesgos* para determinar qué se necesita proteger (objetivos clave), de qué protegerlo (amenazas) y cómo protegerlo (políticas), esto, para valorar los activos y de esta forma adecuar las políticas de seguridad informática a la realidad de la organización.

b. Auditar periódicamente los procedimientos y operaciones de la organización de tal forma que las políticas de seguridad informática puedan actualizarse oportunamente.

c. Comunicar a todo el personal involucrado sobre el desarrollo de las políticas de seguridad informática, sus beneficios y riesgos relacionados con los recursos y los elementos de seguridad.

d. Dialogar con quién tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en salvaguardar los recursos críticos de sus áreas.

1.3. Estrategias para definir una política de seguridad informática

Ajustarse a una estrategia de seguridad informática es una decisión muy importante al momento de construir una solución de seguridad determinante en su estructura.

Existen algunas estrategias generales que responden a diferentes principios para llevar a cabo la implementación de una política de seguridad informática.

1.3.1. Servicios de seguridad de la información

Son los servicios de nivel básico que son utilizados como requisitos para combatir los diferentes tipos de ataques y mantener la privacidad de las redes de datos, estos servicios son: *autenticación, control de acceso, integridad, confidencialidad* y *no repudio* estos servicios no deben ser confundidos como mecanismos de seguridad, los cuales son implementaciones reales de estos servicios.

1.3.1.1. Autenticación.- Es la confirmación de la identidad declarada del usuario. Para apoyar este servicio se tiene el uso de la identificación y autenticación, la primera es para identificar al usuario que quiere ejecutar una aplicación o servicio y la segunda es para comprobar que el usuario es quien

dice ser. En los sistemas informáticos la autenticación se la hace por medio de una contraseña o clave, que es la identidad de un usuario, la que en ciertas ocasiones es establecida por el administrador de una red de datos.

Este servicio es clave porque si falla no se garantiza la integridad ni la confidencialidad por lo que son necesarios métodos adecuados para todos los servicios y aplicaciones. Entre los servicios y aplicaciones a autenticar y proteger se tiene: las transacciones comerciales y bancarias, la transferencia electrónica de fondos, proteger la integridad del software y las bases de datos, proteger la integridad de un sitio web, entre otros.

1.3.1.2. Control de acceso.- El control de acceso o *disponibilidad* significa que la información mantiene su utilidad y por tanto es accesible para los usuarios inclusive en casos de catástrofes naturales, cortes de energía eléctrica, ataques o daños accidentales a una red de datos. Los respaldos son la forma más simple de control de acceso, cuya intención es tener una copia de la información importante almacenada en una ubicación segura, con el fin evitar la pérdida completa de la información en caso de algún tipo de desventura como las descritas arriba. El control de acceso es importante cuando una avería de la red de datos puede provocar interrupciones o reacciones en cadena que afecten las operaciones de la organización. También están los sistemas de *recuperación de fallos*, que hacen uso de *hardware redundante*[3] para detectar las fallas y restablecer la capacidad a través de un proceso automático de recuperación.

1.3.1.3. Integridad.- Confirmación de que la información transmitida, recibida y almacenada es correcta y no ha sido alterada de ninguna forma por individuos no autorizados o ataques de intercepción y modificación; he aquí la importancia de las tecnologías de encriptación que son las que pueden evitar los ataques de modificación durante la transmisión.

[3] El hardware redundante consiste en dos o más equipos de cómputo o de red, que funcionan a la vez, por lo que si el equipo principal falla, asume el control el equipo secundario.

La integridad es importante en relación con la autenticación en los casos en que la exactitud de la información es crítica. La integridad se protege a través del control de acceso a los archivos, por lo que es importante identificar al usuario que pretende hacer uso de la información mediante el uso de la identificación y la autenticación.

1.3.1.4. Confidencialidad.- Es proteger y mantener bajo secreto las comunicaciones y la información contra un ataque de intercepción y/o la lectura por parte de usuarios no autorizados, por lo que para la primera es necesario el uso de tecnologías de encriptación y para la segunda el uso de la identificación y autenticación, de tal forma que la información almacenada y transmitida por medios electrónicos dependa de algún tipo de control. La confidencialidad es esencial en la transmisión, recepción y almacenamiento de información sensible.

1.3.1.5. No repudio.- El no repudio o *no rechazo* se encarga de establecer los mecanismos para que nadie pueda negar que ha realizado una determinada acción o comunicación.[4]

1.3.2. Principios fundamentales

Dentro de las políticas de seguridad informática es importante definir principios y procedimientos que expliquen la posición que asume una organización ante las amenazas. Esta posición no es más que las estrategias de seguridad enfocadas a la elección de reglas y medidas a tomar para proteger la red de datos y la información. La definición de estos principios y procedimientos es muy importante, si se quiere obtener una certificación ISO. Entre los principios para establecer estrategias para definir una política de seguridad informática se pueden destacar los siguientes:

---

[4] Tema y subtemas desarrollados a partir de las siguientes fuentes:
http://es.kioskea.net/contents/secu/secuintro.php3http://www.monografias.com/trabajos12/fichagr/fichagr.shtml#POLIT
Fundamentos de seguridad, autor: F. Vergara, pág. 6 y 7

1.3.2.1. Mínimo privilegio.- Esta es una de las estrategias más fundamentales de seguridad informática, consiste en conceder a cada objeto, sea un usuario o una aplicación, solo aquellos permisos que son necesarios para realizar sus tareas, bajo esto se determinará la seguridad obtenida. Esta estrategia limita los daños accidentales y los ataques y está basada en el razonamiento de que todos los servicios de la red están pensados para ser utilizados por algún perfil de usuario o aplicación, sin afectar el servicio prestado a los mismos usuarios de la red de datos. Esta estrategia debe contener características de diseño en los programas y protocolos que se utilicen para que sea fácil su implementación.

1.3.2.2. Defensa en profundidad.- Esta estrategia consiste en la redundancia de la protección; esto es, implementar varios mecanismos de seguridad informática para que refuercen a los demás, de forma que si uno falla, hay otros mecanismos que vencer, estos mecanismos deben ser cuidadosamente configurados para evitar que las fallas de un mecanismo se propaguen al resto; la idea de esta estrategia es hacerle más difícil y costoso a un atacante la idea de violar la seguridad de la red de datos. Por ejemplo se puede hacer uso de hardware redundante tanto en equipos de cómputo como de red y se pude hacer uso de la seguridad humana como la educación en seguridad informática para los usuarios de la red.

1.3.2.3. Punto de ahogo (acceso).- Esta estrategia consiste en depender de un único punto de acceso entre las comunicaciones de la red de datos privada y la red pública, por lo que los esfuerzos de control y mecanismos de seguridad informática se centran en monitorear un solo sitio de red; por eso, esta estrategia se considera como una solución todo en uno. En esta estrategia se deben utilizar mecanismos de protección redundantes y reforzar la seguridad de dicho punto, para así evitar que un atacante sea capaz de traspasar la seguridad de este único punto de acceso y tenga acceso a todos los recursos de la red de datos; también se debe utilizar un cortafuegos (firewall) perimetral que procese todo el tráfico que por el pase para que no se produzcan bajas en

el desempeño de las comunicaciones de la red de datos con el exterior y evitar por tanto que se vea superada la capacidad el punto de acceso de registrar los sucesos y controlar todo el tráfico de entrada y salida.

1.3.2.4. Enlace más débil.- Esta estrategia consiste en identificar aquellos enlaces débiles de acceso a la red de datos privada y tratar de eliminarlos, monitorearlos y/o reforzarlos, es por esto que responde a un principio de seguridad que, aplicado a redes de datos, dice que un sitio es tan seguro como lo es su enlace más débil; este enlace suele ser el objetivo de los ataques a la privacidad de la red de datos y debe ser lo suficientemente seguro en proporción al riesgo que implica que sea vulnerable.

1.3.2.5. Estado a prueba de fallos.- Esta estrategia determina una posición específica con respecto a decisiones de seguridad informática y políticas, sin embargo esta estrategia dice que “ninguna solución de seguridad es 100% segura”, por lo que la pregunta es ¿cómo responderá una red de datos a esta falla? Las aplicaciones como cortafuegos, ruteadores de filtrado de paquetes y servidores proxy, dejan de transmitir información si fallan, sin embargo los sistemas de filtrado basados en anfitriones, también llamados *hosts*, no lo hacen, porque poseen servicios mediante aplicaciones independientes del resto de estos sistemas, por lo que hay conexiones por este servicio; esto debe ser evitado porque no se llevaría a cabo esta estrategia y se permitiría puertas abiertas a posibles ataques.

En esta estrategia se establece la posición *rechazar por defecto,* lo que significa establecer cuáles son las comunicaciones que serán permitidas, si el mecanismo falla, cualquiera que no sea considerada será rechazada, por lo que está claro que esta posición es una estrategia a prueba de fallos. En esta posición es importante examinar los servicios a ofrecer a los usuarios, con el fin de permitir solo aquellos servicios necesarios y conocidos, que puedan ser protegidos de forma segura utilizando los mecanismos disponibles.

1.3.2.6. Protección universal.- En esta estrategia se plantea que los usuarios de una organización deben colaborar en mantener y cumplir las políticas de seguridad informática, de tal forma que se ofrezca una protección efectiva a la red de datos y a la información; de lo contrario un atacante podría aprovechar la vulnerabilidad de aquellos equipos a cargo de ciertos usuarios para poder llegar a los demás recursos de la red de datos. Más que una estrategia es un principio que debe cumplir toda organización.

1.3.2.7. Diversidad de la defensa.- Esta estrategia puede complementarse con la de defensa en profundidad. Consiste en el uso de diferentes tipos de sistemas para implementar los diferentes mecanismos de seguridad informática, siendo el objetivo reducir las posibilidades de fallas comunes en todos los sistemas prestados para proteger la red de datos, debido a errores propios de los sistemas o de configuración. Esta estrategia tiene la desventaja de un posible costo adicional, sea económico, de tiempo y de complejidad, debido a que se debe conocer el funcionamiento y manejo de varios productos. Ciertas consideraciones deben ser evaluadas para ver la conveniencia de aplicar esta estrategia.

1.3.2.8. Seguridad a través de oscuridad.- Esta estrategia consiste en ocultar la verdadera naturaleza de la red de datos, bajo un perfil bajo, o no hacerlo; así un atacante no lo notará o lo pasará por alto como una posible víctima. Esta estrategia es algo ingenua porque algunos estudios han demostrado que los ataques involucran varios sistemas y varias cuentas de usuario para poder ganar acceso no autorizado a otros sistemas y alcanzar sus objetivos reales, por lo tanto el interés de un atacante en un determinado sistema no solo consiste en el interés que este tenga en la información de la red de datos, esto porque un sistema puede ser comprometido solo para proveer un escenario de ataque a otros sistemas. Al principio de la vida de una red de datos esta estrategia puede ser útil, pero a largo plazo puede ser débil, debido a que la información tiende a filtrarse y los atacantes son hábiles para obtener la información del sistema.

1.3.2.9. Simplicidad.- Esta estrategia señala que las redes de datos a nivel de aplicación no deberían tener funcionalidades desconocidas y deberían mantenerse lo más simples posible. Se sabe que cuanto más grandes y complejos son los sistemas de una red de datos, más errores tendrán, serán más difíciles y costosos de probar. Posiblemente posean agujeros de seguridad no conocidos que un atacante puede explotar. Cuando una organización es grande o muy grande lógicamente compensa la reducción al mínimo de posibles agujeros de seguridad con equipos de computo y de red más costosos y sofisticados, un ejemplo son los grandes bancos y las transnacionales, aun así sus sistemas no deben contemplar funcionalidades desconocidas, con esto se deduce que la simplicidad es una escala de acuerdo al tamaño y tipo de organización.

1.3.2.10. Seguridad basada en anfitriones *(hosts)*.- Esta estrategia se enfoca en los sistemas finales de una red de datos, es decir que los mecanismos de seguridad informática son implementados en estos sistemas, y son ellos mismos los que deciden si aceptar o no los paquetes de una comunicación. Un problema en esta estrategia es en cuanto a puntos de ahogo y enlaces débiles, no existe un único punto de acceso porque ya existen múltiples conexiones, una para cada anfitrión y algunas pueden estar débilmente protegidas; otro problema es que no es escalable si no se considera un esquema de administración apropiado, por lo que solo es usado en ambientes pequeños, así esta estrategia no es rentable implementarla en redes grandes, debido a que requiere muchas restricciones.

1.3.2.11. Seguridad basada en red.- Esta estrategia se enfoca en controlar el acceso a la red y no en asegurar los anfitriones en sí mismos Esta estrategia aplica los mecanismos de protección en un lugar común por el que circula todo el tráfico desde y hacia los anfitriones, o sea los puntos de acceso a la red de datos. La ventaja sobre la estrategia de seguridad basada en anfitriones es una reducción en el costo, debido a que solo se necesita proteger unos pocos puntos de acceso, esta estrategia es escalable a medida que soporte los

cambios sin afectar su desempeño. La desventaja de esta estrategia es que es muy dependiente de pocos puntos de acceso, por lo que se puede producir reducciones en el desempeño del tráfico de entrada y salida.[5]

1.3.3. Procedimientos fundamentales

Entre los procedimientos que se deben considerar, se pueden destacar los siguientes:

1.3.3.1. Procedimiento de alta de cuentas de usuario.-Cuando un elemento de la organización requiere una cuenta de operación en el sistema, se debe considerar al menos los siguientes datos:

a. Nombre y Apellido.
b. Puesto de trabajo.
c. Jefe inmediato que avale el pedido, si lo hay.
d. Descripción de las tareas que se deben realizar en el sistema.
e. Consentimiento de que sus actividades pueden ser auditadas en cualquier momento y que se conoce las normas del buen uso de los recursos.
f. Explicaciones breves, pero claras de cómo elegir una contraseña.

Adicionalmente se debe considerar:

g. Tipo de cuenta de usuario.
h. Fecha de creación.
i. Fecha de expiración.
j. Datos referentes a los permisos de acceso por ejemplo, tipos de permisos a los diferentes directorios y/o archivos.
k. Si tiene o no restricciones horarias para el uso de algunos recursos y/o para el ingreso al sistema.
l.

[5] Tema y subtemas desarrollados a partir de la web: *http://www.textoscientificos.com/redes/firewalls-distribuidos/estrategias-seguridad.*

1.3.3.2. Procedimiento de baja de cuentas de usuario.- Se lleva a cabo cuando un usuario deja de trabajar parcial o definitivamente. Como todos los componentes de la política de seguridad informática, debe estar fuertemente apoyado por la parte gerencial de la organización. Por ejemplo si ante el alejamiento de un usuario de la organización, el departamento de RRHH debe informar acerca de la posición que éste ocupaba y el tipo de alejamiento (definitivo o no). Una vez llegada la información al departamento encargado de la administración de sistemas, este da de baja o inhabilita la cuenta del usuario. La definición de si se da de baja o se inhabilita es algo importante pues, si se da de baja, se deberían guardar y eliminar los archivos y directorios del usuario, mientras que si sólo se inhabilita, no pasa de esa acción.

1.3.3.3. Procedimiento para determinar buenas contraseñas.- En varias organizaciones la verificación de palabras claves efectivas no es algo frecuente. El procedimiento debe explicar las normas para elegir una contraseña, como son la cantidad de caracteres mínimos que debe tener, no debe tener relación directa con las características del usuario, debe constar de caracteres alfanuméricos y signos de puntuación.

1.3.3.4. Procedimiento de verificación de accesos.- Permite explicar la forma de realizar las auditorías de los archivos logísticos de ingresos a fin de detectar actividades anómalas, estableciendo el tiempo entre la auditoría y cómo actuar en caso de detectar anomalías; este trabajo es realizado por programas a los que se les dan normativas de qué y cómo comparar. Escanean archivos con diferentes fechas y ante la detección de un desvío, generan reportes informando el mismo. En el procedimiento debe quedar perfectamente indicado quién es el responsable del mantenimiento de estos programas.

1.3.3.5. Procedimiento para la revisión del tráfico de la red.- Permite conocer el comportamiento del tráfico en la red de datos, al detectar variaciones que pueden ser síntoma de mal uso de la misma. El procedimiento

debe indicar los programas que se ejecuten, con qué intervalos, con qué reglas de trabajo, quién se encarga de procesar y/o monitorear los datos generados por ellos y cómo se actúa en consecuencia.

1.3.3.6. Procedimiento para el monitoreo de los volúmenes de correo.- Permite conocer los volúmenes del tráfico de correo electrónico. El análisis de esta información permite conocer, entre otras cosas, el uso de los medios de comunicación, y si el servidor está recibiendo un correo “spam”. En este procedimiento debe estar explicado quién es el encargado del mantenimiento y del análisis de los datos generados, y qué hacer cuando se detectan anomalías.

1.3.3.7. Procedimientos para el monitoreo de conexiones activas.- Permite prevenir que algún usuario deje su terminal abierta y sea posible que alguien use su cuenta. El procedimiento es ejecutado por medio de programas que monitorean la actividad de las conexiones de usuarios. Cuando se detecta que una terminal tiene cierto tiempo inactiva, cierra la conexión y genera un log con el acontecimiento.

1.3.3.8. Procedimiento de modificación de archivos.- Permite detectar la modificación no autorizada y la integridad de los archivos y, en muchos casos, permite la traza de las modificaciones realizadas. Se debe determinar la responsabilidad de quién es el encargado del seguimiento y cómo actuar en caso de anomalías.

1.3.3.9. Procedimiento para el resguardo de copias de seguridad.- Permite establecer dónde se deben guardar las copias de seguridad y los pasos a seguir en caso de problemas. Para lograr esto, deben estar identificados los roles de los usuarios que interactúan con el área, a fin de que cada uno sepa qué hacer ante la aparición de problemas.

1.3.3.10. Procedimiento para la verificación de las máquinas de los usuarios.- Permite encontrar programas que no deberían estar en las máquinas de los usuarios y que, por su carácter, pueden traer problemas de licencias y fuente potencial de virus. El procedimiento debe explicitar los métodos que se van a utilizar para la verificación, las acciones ante los desvíos y quién o quiénes lo llevarán a cabo.

1.3.3.11. Procedimiento para el monitoreo de los puertos en la red de datos.- Se enfoca en saber qué puertos están habilitados en la red de datos y, en algunos casos, revisar la seguridad de los mismos. El procedimiento deberá describir qué programas se deben ejecutar, con qué reglas, quién estará a cargo de llevarlo a cabo y qué hacer ante las desviaciones detectadas.

1.3.3.12. Procedimiento de cómo dar publicidad a las nuevas normas de seguridad.- Este tipo de procedimiento no siempre es tenido en cuenta, sin embargo, en una organización es muy importante conocer las últimas modificaciones realizadas a los procedimientos. Se debe describir la forma de informar sobre las modificaciones, estás pueden ser mediante correo electrónico u otro medio. Es fundamental tener en cuenta este último punto ya que un porcentaje de los problemas de seguridad, según está demostrado en estudios, proviene del desconocimiento por parte de los usuarios de las normas y/o modificaciones.

1.3.3.13. Procedimiento para recuperar información.- Se enfoca en restablecer todo el sistema o parte de él, a partir de las copias de seguridad. En él, deben explicarse todos los pasos a seguir para restablecer el sistema a partir de los respaldos existentes, así como cada cuánto tiempo habría que llevarlos a cabo y quiénes son los responsables de esta tarea.[6]

---

[6] Tema y subtemas desarrollados a partir del libro: *Fundamentos de seguridad, pág. 16,17 18 y 19, autor: F. Vergara,*

1.3.4. Auditoría informática

El objetivo es dar un bosquejo sobre la importancia de la auditoria informática como una estrategia enfocada a la política de seguridad informática, se hace esta aclaración porque este tema es mucho más amplio y especializado y no es el tema principal de este trabajo.

En una política de seguridad informática se debe considerar a la auditoría informática como una estrategia importante de control para salvaguardar una red da datos y sus recursos y verificar el cumplimiento de las mismas políticas y procedimientos en una organización.

La definición de auditoría informática puede variar de un autor a otro, sin embargo se puede dar una definición general: "la auditoria informática es el proceso de agrupar y hacer un *análisis de riesgos* para evaluar si en los procedimientos y operaciones de la organización se salvaguardan los activos y la integridad de la información de un sistema informático, y si además se cumple con la adecuada utilización de los recursos disponibles con *eficacia* y *eficiencia* [7]para el mejoramiento continua de la rentabilidad y la seguridad ".

1.3.4.1. Alcance de la auditoria informática.- El alcance define con precisión el entorno y los límites en que va a desarrollarse la auditoría informática se complementa con los objetivos establecidos para la misma. El alcance debe definirse de forma clara en el informe final especificando los temas que fueron examinados y cuales fueron omitidos. Del alcance depende buena parte del éxito de la auditoria informática.[8]

1.3.4.2. Objetivos de la auditoria informática

a. Operatividad o control de la función informática.
b. Análisis de la eficiencia de las redes de datos.
c. Verificación del cumplimiento de las normativas en este ámbito.

---

[7] La eficacia es la consecución de metas con resultados, es hacer las cosas correctas.
La eficiencia es aprovechar los recursos con bajos costos, es hacer bien las cosas.

[8]Subtema desarrollado a partir de la web:http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

d. Revisión de la eficaz gestión de los recursos informáticos.

Haciendo una ampliación de la operatividad, está es una función de mínimos, consiste en que la organización y las máquinas funcionen al menos con los requerimientos mínimos, ya que no es admisible detener la maquinaria informática para descubrir los fallos y comenzar de nuevo, este objetivo debe cumplirse a nivel global y parcial en una auditoria informática.[9]

1.3.4.3. Importancia de la auditoria informática.- La importancia para llevar un control periódico bajo esta herramienta se deduce de varios aspectos, he aquí algunos:

a. Las computadoras tanto clientes como servidores, las redes de datos y los centros de procesamiento de información se convierten en blancos apetecibles por parte de diversos atacantes informáticos para llevar a cabo fraudes, espionaje, robo de información, sabotajes, entre otros tipos de ataques. Por ejemplo las bases de datos pueden ser propensas a atentados y acceso de usuarios no autorizados o intrusos.

b. Las computadoras que procesan y difunden resultados, pueden producir información errónea, si la calidad de datos de entrada es errónea o inexacta o hay mala manipulación de los mismos, sea intencional o accidental, esto afectaría seriamente a las operaciones de la red de datos, la toma de decisiones e imagen de la organización.

c. Una red de datos mal diseñada no permite la continuidad de las operaciones y administración, esto implicaría un serio riesgo para la organización.

d. El uso inadecuado de la red de datos y sus recursos como la computadora para usos ajenos a los de la organización, la copia de software especializado o exclusivo para uso indebido o con fines de

[9] Subtema desarrollado a partir de la web:
http://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica

comercialización, acceso a ciertas aplicaciones o bases de datos a las que no se tiene autorización, transferencia ilícita de tecnología.[10]

1.3.4.4. Metodología de la auditoria informática.- El método de trabajo del auditor informático pasa por las siguientes etapas:

a. Estudio inicial del entorno auditable u observación.
b. Alcance y objetivos de la auditoria informática.
c. Determinación de los recursos necesarios para realizar la auditoría informática.
d. Elaboración del plan de trabajo
e. Elaboración de los programas de trabajo como pueden ser: realización de cuestionarios auditados y no auditados, muestreo estadístico, flujo gramas, entre otros.
f. Confección y redacción del informe final.

El método de trabajo de un auditor informático puede variar un poco dependiendo del tamaño y del tipo de organización con la que se encuentre, pero los parámetros anotados arriba son básicamente los que se siguen.[11]

1.3.4.5. Algunos tipos de auditoría informática.- Hay varios tipos de auditoría informática, pero solo se toman las que interesan al tema de este trabajo.

a. Auditoría informática de sistemas.- Se ocupa de analizar y revisar los controles y efectividad de la actividad que se conoce como técnicas de sistemas en todas sus facetas y se enfoca en los *sistemas operativos, software básico, aplicaciones y administración de base de datos.* La

[10] Subtema desarrollado a partir de las siguientes webs:
http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml
http://www.monografias.com/trabajos12/fichagr/fichagr.shtml#POLIT
[11] Subtema desarrollado a partir de la web: http://www.monografias.com/trabajos/auditoinfo/auditoinfo.html

importancia creciente de las telecomunicaciones ha propiciado que las comunicaciones, líneas y redes de datos se auditen por separado, aunque formen parte del entorno general de sistemas, pero esto depende del tamaño y tipo de una organización.

b. **Auditoria informática de redes de datos.-** Se enfoca en la revisión de redes nodales, líneas, concentradores, multiplexores, redes locales, etc. que son el soporte físico-lógico del tiempo real, esta auditoría tropieza con la dificultad técnica del entorno y analiza situaciones y hechos algunas veces alejados entre sí, además está condicionada a la participación de la empresa telefónica; esta auditoría requiere de especialistas y expertos en comunicaciones y redes.

   Esta auditoría analiza cuáles son los índices de utilización de las líneas contratadas con información sobre tiempos de desuso, debe proveerse de la topología de la red de comunicaciones actualizada, obtener información sobre la cantidad de líneas existentes, cómo son y dónde están instaladas.

c. **Auditoria de la seguridad informática.-** Esta auditoría se basa en los conceptos de seguridad física y seguridad lógica. La seguridad física es la protección del hardware y los soportes de datos, así como de las instalaciones que los alberga, se contempla situaciones de incendio, robos, sabotajes, catástrofes naturales, etc. La seguridad lógica es la seguridad en el uso del software, procesos y programas, a la protección de la información y el ordenado y autorizado acceso de los usuarios a la información. Esta auditoría también previene sobre el uso de paquetes de software piratas, debido a que pueden contener virus o pueden dañar o borrar la información, implica sobre el cuidado que se debe tener para no transmitir y recibir virus al conectarse en red con otras computadoras o al salir al internet.

   Un método de protección son los paquetes de software de control de acceso que protegen contra el uso no autorizado, pues piden al usuario

una contraseña antes de permitirle el acceso a la información. Otro método de protección es el uso de medios criptográficos sofisticados. [12]

[12] Subtema desarrollado a partir de las siguientes webs: http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtmlhttp://www.monografias.com/trabajos12/fichagr/fichagr.shtml#POLIT

2. Capítulo II: Tipos de ataques y vulnerabilidades

2.1. Introducción a los ataques y vulnerabilidades

En seguridad informática cuando ya se ha establecido *qué se necesita proteger*, se pasa a analizar *de qué y de quién proteger*.

Una vez que las organizaciones empezaron a conectarse a internet y a poner a disposición del público servicios que dan acceso a información, a realizar transacciones comerciales, a intercambiar todo tipo de información, a comunicarse por correo electrónico, etc. surgieron nuevos tipos de amenazas, como son los piratas informáticos, las amenazas programadas como los códigos específicamente diseñados para atacar las medidas de seguridad de un sistema informático. Las amenazas programadas pueden entrar en varias categorías o combinar varios tipos de amenazas en un solo código; estas amenazas se las analizará más adelante.

Por lo tanto cualquier equipo conectado a una red de datos puede ser vulnerable a un ataque. El ataque consiste en aprovechar alguna vulnerabilidad de una red da datos, básicamente un sistema operativo de red, un sistema de usuario, una base de datos, una página web, etc.

Una planificación adecuada ayuda a conseguir excelentes niveles de seguridad, normalmente se quiere garantizar que la red da datos permanezca en funcionamiento de forma adecuada y que nadie pueda acceder o modificar una información a la que no tiene legítimo derecho, al mismo tiempo se querrá garantizar unas comunicaciones seguras. Se debe analizar una red de datos para saber qué se está protegiendo, de qué y de quién se lo está protegiendo, por qué se lo está protegiendo, qué valor tiene y quiénes tienen responsabilidad sobre la información y otros elementos.

Antes de intentar asegurar una red de datos se debe determinar contra qué nivel de amenaza se quiere proteger, qué riesgos existen y, como conclusión, cuan vulnerable es la misma.

2.1.1. El riesgo.- Es la posibilidad de que algún intruso intente acceder con éxito a un equipo o red de datos, basta tener una cuenta insegura para comprometer toda una red, porque un intruso que acceda a una cuenta, se puede hacer pasar por alguien de la organización. Cuando se habla de riesgo, cabe preguntar, ¿puede un intruso escribir en ficheros o ejecutar programas que puedan causar daño?, ¿puede robar o borrar información crítica?, estas preguntas básicas ayudan a prevenir que la organización pierda información y trabajo importante.

2.1.2. La amenaza.- Esta proviene de alguien que tiene motivos para obtener acceso no autorizado a un equipo o toda una red de datos. Las amenazas provienen de varios tipos de intrusos y es útil tener en cuenta sus diferentes características y motivaciones, como por ejemplo:

2.1.2.1. El malicioso.- Este tipo de intruso pretenderá hacer caer una red de datos, robar y/o borrar información, modificar una página web, acceder a una base de datos o cualquier otra acción que le cueste tiempo y dinero recuperar a la organización.

2.1.2.2. El curioso.- Este tipo de intruso se interesa básicamente en qué tipo de sistema informático e información posee una organización.

2.1.2.3. El intruso muy personalizado.- Este tipo de intruso busca usar una red de datos para ganar popularidad y fama, al igual que busca promocionar sus habilidades.

2.1.2.4. La competencia.- Este tipo de intruso está interesado en la información que tiene una red de datos, para sacar provecho y conseguir algo de valía comercial y/o financiera o de alguna otra utilidad.

2.1.3. La vulnerabilidad.'- Describe el nivel de protección de una red de datos frente a los riesgos y amenazas, básicamente cabe preguntar, ¿qué está en

juego si un intruso entra en una red de datos?, ¿cuánto tiempo llevaría recuperar y/o restaurar cualquier información que se ha perdido?, ¿se ha verificado la estrategia de copias de respaldo?, entonces el vislumbrar de manera adecuada las vulnerabilidades, ayudará a la organización a prevenir y rechazar posibles ataques de manera efectiva.[13]

2.2. Tipos de ataques y amenazas

Los ataques se pueden producir siempre y cuando exista una vulnerabilidad que pueda aprovecharse, esto debido a que hay una cadena de componentes, desde electricidad para suministrar alimentación a los equipos hasta los recursos físicos, lógicos y de servicios. Los ataques se pueden producir por diversos motivos:

a. Simple diversión.
b. Venganza.
c. Interés político y/o poder.
d. Codicia, como obtener acceso a la red de datos y robar información como secretos industriales o comerciales, propiedad intelectual, números de tarjetas de crédito, información de cuentas bancarias, información personal sobre un usuario, información acerca de una organización etc.
e. Para obtener acceso a la red de datos y modificar o borrar información.
f. Para saturar una red de datos y afectar el funcionamiento normal de la misma.
g. Para utilizar alguna máquina de una red de datos como un rebote para efectuar un ataque a otra red de datos.
h. Para utilizar los recursos y servicios de una red de datos, generalmente cuando esta tiene un ancho de banda considerable.

[13] Subcapítulo, temas y subtemas desarrollados a partir de la web: *http://www.iec.csic.es/CRIPTonOMICon/linux/proteger.html*

2.2.1. Tipos de atacantes e intrusos

Las redes de datos y sus recursos están en constante evolución, sin embargo a pesar de estos avances, surgen nuevas vulnerabilidades; los usuarios no autorizados con herramientas adecuadas y sofisticadas y con la capacidad y experiencia para usarlas, son una amenaza para las organizaciones y tienen grandes posibilidades de acceder a las redes de datos y sus recursos; la posibilidad de nuevos ataques e intrusiones también se debe al crecimiento de los sitios de internet relacionados con la piratería informática, los cuales ofrecen programas de fácil descarga. Existen algunos tipos de atacantes e intrusos, clasificados de acuerdo a su experiencia y motivaciones y con distintas connotaciones.

2.2.1.1. ¿Qué son los hackers?

En la actualidad el término hacker todavía no está definido en el diccionario. El término hacker a tenido más de un significado, al principio se lo usó positivamente para referirse a los expertos en programación y revolucionarios informáticos, algunos de ellos creadores de algunas de las tecnologías informáticas más innovadoras, además de fundadores de las empresas de Tecnologías de la Información (TI) más importantes; el término hacker también se lo usó negativamente para referirse a personas involucradas en la piratería de video juegos, que desactivaban las protecciones de estos y hacían copias para venderlos, así como para referirse a un pirata informático como alguien que irrumpe en sistemas informáticos. Pero libre de cualquier connotación y dando una definición general de lo que son los hackers, estos serían “aficionados a las computadoras totalmente apasionados por la programación y la informática que buscan de manera intensa extender sus capacidades y conocimientos y que disfrutan aprendiendo detalles de los sistemas informáticos y de programación y entre cuyos objetivos está acceder a un red de datos protegida como si se tratara de un reto personal sin querer causar daños, así como el de ayudar a mejorar los sistemas y las tecnologías informáticas, siendo casi siempre los responsables de los protocolos y herramientas informáticas más importantes para su uso general”.

2.2.1.2. Crackers.- Este término fue creado por la comunidad de hackers para referirse a aquellos que usan sus conocimientos con fines nada éticos. En consecuencia los crackers son hackers que utilizan sus conocimientos para realizar acciones maliciosas, como reventar programas, penetrar en una red de datos para robar o destruir información, saturar una red de datos, crear herramientas de software para *craquear* [14] la protección anti copia del software con licencia, etc. por lo tanto un cracker es lo que propiamente sería un pirata informático.

2.2.1.3. Hacktivistas.- Son hackers con motivaciones totalmente ideológicas, estos son una comunidad paralela en general llamada cultura underground.

2.2.1.4. Crashers.- También conocidos como script kiddies, lamers, packet monkeys, estos son usuarios de la red que buscan y bajan programas desde el internet, y que los utilizan casi siempre de forma incompetente, para dañar sistemas informáticos por diversión.

2.2.1.5. Carders.- Son piratas de tarjetas inteligentes que buscan atacar estos sistemas, como las tarjetas bancarias, con el fin de entender su funcionamiento y explotar sus vulnerabilidades.

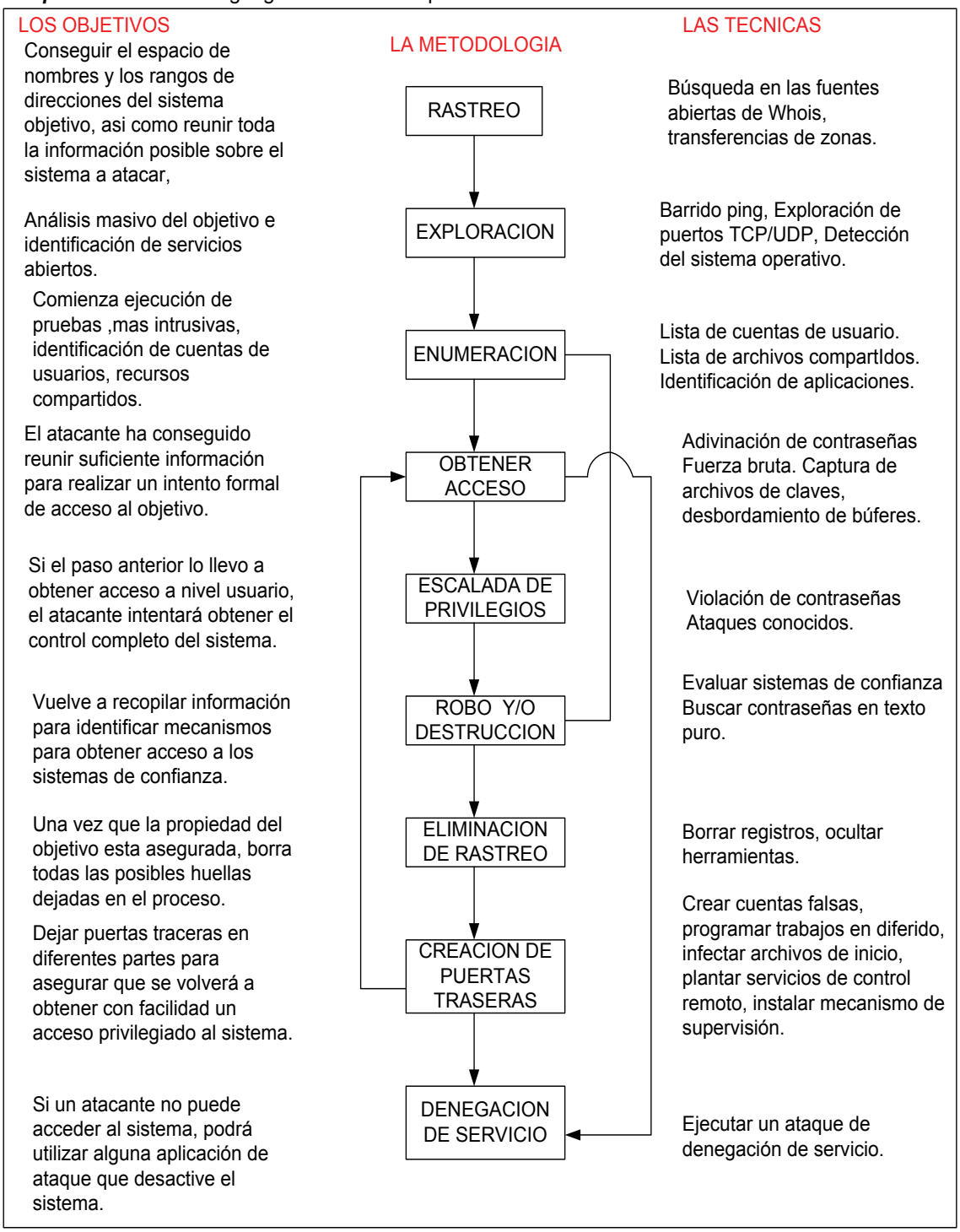
2.2.1.6. Phreakers.- Son piratas que usan la red telefónica conmutada (RTC) para hacer llamadas gratis a través de circuitos electrónicos como la *caja azul*, la *caja violeta*, etc. que conectan a la línea telefónica para manipular su funcionamiento. Por lo tanto, la palabra *phreaking* se usa para el pirateo de líneas telefónicas.

[14] Craquear es ejecutar un programa llamado crack, para modificar o actualizar un software original con el fin de descifrarlo y quitarle su protección y poder hacer copias de este.

2.2.2. Tipos de ataques y sus técnicas

Un pirata informático que pretende atacar una red de datos, primero buscará *fallas de seguridad*, es decir *vulnerabilidades* que afecten al sistema de protocolos y a los recursos, principalmente lógicos y de servicios e incluso a los usuarios de una organización. Es por eso que los ataques a la seguridad cada día sobrepasan todas las estimaciones; sin embargo la seguridad informática es un proceso continuo, que requiere prever hasta lo imprevisible, tener unos buenos hábitos y tomar buenas precauciones ayudarán de manera efectiva. Un pirata informático desde el momento de elegir a la red de datos para un ataque hasta cuando termina el mismo, debe seguir ciertos pasos generales, como los que se ve en el siguiente gráfico:

Esquema 2.1. Metodología general de un ataque[15]



Para obtener acceso no autorizado a una red de datos o hacer caer la misma, existen una variedad de ataques y técnicas que se deben tener en cuenta en

[15] Esquema obtenido y modificado del texto *Fundamentos de seguridad*, autor: F. Vergara, cap.3, pág. 21

todo tipo de organizaciones, tengan o no con un departamento de sistemas y/o un administrador de red.

2.2.2.1. Ingeniera social.- Es una técnica social que busca obtener el acceso no autorizado a una red de datos y su información, aprovechándose de la inocencia e ingenuidad de ciertos usuarios para manipularlos. La ingeniería social puede ser un arma potencial para penetrar completamente un sistema objetivo, pero toma tiempo y sobre todo talento, además es utilizada por piratas informáticos que tienen por objetivo una organización específica. La principal arma de los piratas informáticos que utilizan esta técnica, es la capacidad de mentir.

a. El pirata informático puede contactar a un usuario mediante ciertos medios como el teléfono, el correo electrónico, la mensajería instantánea, el correo tradicional o el contacto directo, para así obtener información acerca de la red de datos.

b. Así mismo y en referencia al punto anterior, el pirata informático puede hacerse pasar por el empleado de una organización, un técnico o un administrador y mediante la fuerza persuasiva, obtener información, como una clave de acceso u otro tipo de información confidencial, bajo cualquier pretexto.

c. Se puede crear una falla de seguridad en una red de datos al enviar un troyano a uno o varios usuarios, a la espera de que alguno de los usuarios abra el adjunto para que el pirata informático obtenga el acceso a la red de datos.
d. La menos improbable pero que no se debe descartar, es el hurto de computadoras o ciertos dispositivos específicos de las mismas, además de dispositivos de almacenamiento externo, que le permitan al pirata informático conocer más sobre una organización.

En la política de seguridad informática la mejor defensa contra la ingeniería social es el entrenamiento consiente y objetivo, además del sentido común, dado que el nivel de seguridad informática se caracteriza por su eslabón más débil. Por esta razón los usuarios deben estar adiestrados y contar con procedimientos claros y precisos en sus organizaciones, para evitar los inconvenientes señalados arriba.

2.2.2.2. Analizadores de red.-También conocidos como *rastreadores de red, rastreadores de puertos, analizadores de tráfico* o *sniffers*; estos son herramientas de software utilizadas para supervisar el tráfico de las redes de datos, determinar su topología, determinar las direcciones IP activas, capturar contraseñas u otra información en circulación**.** Los analizadores son usados por los administradores de red para diagnosticar problemas y para obtener información sobre el tráfico, por ejemplo los sistemas de detección de intrusos *(IDS)* se basan en un analizador que mediante una base de datos detectan y capturan paquetes sospechosos.

Los analizadores también son utilizados por los piratas informáticos para atacar e inmiscuirse en las redes de datos, siendo sus intenciones obvias, pero además el pirata informático debe conseguir que el conmutador dirija el tráfico al analizador y también debe provocar que el conmutador envíe todo el tráfico a todos los puertos. El analizador reúne información de los paquetes que circulan por la red, usando una tarjeta de red en *modo promiscuo*, [16]y no solo cuando los paquetes van dirigidos a esa NIC, sino también en redes de datos, o sea cuando se usan conmutadores. Este riesgo es mayor en redes de datos inalámbricas que en redes Ethernet, debido a que es difícil limitar las ondas de radio a un área. La mayoría de los protocolos de internet tienen información sin codificar, por lo tanto si un usuario consulta su correo electrónico a través del protocolo POP, IMAP, o navega en internet por sitios HTTP y no por sitios HTTPS, se puede interceptar toda la información que se reciba o envíe. Hay

[16] En el modo promiscuo una computadora conectada a una red da datos, tanto la basada en cable como la basada en tecnología inalámbrica, captura todo el tráfico que circula por ella. Este modo está muy relacionado con los sniffers, que se basan en este modo para realizar su tarea.

algunas técnicas que se pueden implementar para evitar problemas serios en las redes Ethernet o inalámbricas, debido al uso de analizadores de red.

a. Se debe usar protocolos cifrados para la información que sea confidencial.

b. Se debe usar un detector de analizadores de red, esta es una herramienta de software que analiza la red de datos en busca de tarjetas de red en modo promiscuo, sean estas tarjetas Ethernet o inalámbricas.

c. Se debe segmentar la red de datos para limitar la divulgación de información.

d. Las redes inalámbricas deben estar protegidas con contraseñas seguras tanto para el acceso al software de administración de los equipos inalámbricos, como para el acceso a la red completa.

e. En lo posible, las redes inalámbricas podrían reducir su alcance para cubrir solamente el área geográfica necesaria, para evitar que potenciales piratas informáticos supervisen la red; si una red inalámbrica cumple satisfactoriamente con los puntos *a, b* y *d,* no sería necesario este último punto, debido a que los avances tecnológicos en equipos inalámbricos tienden a conseguir un mayor alcance de la señal a una mayor velocidad, un ejemplo es la tecnología N, sustentada en la norma 802.11n *(ver Anexo 2)*.

2.2.2.3. Desbordamiento de búfer.- Estos ataques también son conocidos como saturación de búfer, están diseñados para ejecutar un código arbitrario en un programa al enviar demasiada información, mayor que el que puede soportar la memoria de un computador. La información ingresada en una aplicación se almacena en la memoria de acceso aleatorio en una zona que se

conoce como búfer. Por ejemplo, si se crea una variable que tenga 10 bytes y se intenta meter 11 bytes, el onceavo byte se sitúa en el espacio de memoria inmediatamente a continuación del décimo byte, y si se intenta meter más información extra en esa variable, finalmente se topará con algún espacio de memoria que sea importante para el funcionamiento del sistema. Las instrucciones y la información de un programa en ejecución se almacenan temporalmente en forma adyacente a la memoria, en una zona llamada pila o *stack* (en inglés), la información ubicada después del búfer contiene una dirección de retorno denominada *puntero de instrucción*, que le permite al programa continuar su tiempo de ejecución. El principio operativo del desbordamiento de búfer está relacionado estrechamente con la arquitectura del procesador en el que se ejecuta una aplicación vulnerable.

Un pirata informático puede colocar instrucciones en la variable local suficientemente extensas y asegurarse de que la dirección de memoria sobrescrita corresponda a una real, como una que esté ubicada en el mismo búfer; por lo tanto al ingresar las instrucciones en el búfer, o sea un código arbitrario, es fácil para el pirata informático ejecutar este procedimiento, ocasionando que otra aplicación se inicie, o cambiando un archivo de configuración como inetd. conf y por tanto accediendo utilizando la nueva configuración. La principal contramedida para evitar el desbordamiento de búfer es utilizar prácticas de programación seguras, por lo que es importante desarrollar aplicaciones que utilicen lenguajes de aplicación avanzados que garanticen la administración adecuada de la memoria asignada. Un programa con un diseño correcto debería estipular un tamaño máximo para los datos de entrada y garantizar que no superen ese valor. Existen también otras recomendaciones adicionales para evitar el desbordamiento de búfer:

a. Se deben aplicar todos los parches de un programa relacionados con la seguridad, debido a que es casi imposible que el código del mismo estese diseñado y escrito sin errores.

b. Se debe reducir la cantidad de código que se ejecuta con privilegios de súper usuario.
c. Desde el inicio, se debe diseñar un programa teniendo en cuenta la seguridad.
d. Se debe utilizar compiladores seguros con módulos que inmunicen los programas, para minimizar el impacto del desbordamiento de búfer.

2.2.2.4. DoS *(Denial of Service – Denegación de servicio)*.-

El ataque por DoS tiene como objetivo imposibilitar a los usuarios legítimos de una organización el acceso a los recursos de una red de datos, generalmente durante un período indefinido de tiempo; este tipo de ataque está dirigido en especial a los servidores de una organización, para que no puedan utilizarse ni consultarse, además pueden tener muchas formas y pueden ser lanzados desde sistemas informáticos individuales como desde sistemas informáticos múltiples. El ataque por DoS puede afectar a cualquier servidor de una compañía o cliente conectado a internet, la mayor parte de estos ataques se originan desde direcciones que se estuvieron husmeando o que fueron falsificadas, es por eso que la mayoría de estos ataques aprovechan las vulnerabilidades relacionadas con la implementación de un protocolo TCP/IP, este protocolo tiene una falla en su esquema de direccionamiento, no verifica la dirección de origen cuando se crea el paquete, por lo tanto el pirata informático puede modificar la dirección origen para ocultar su ubicación; los ataques por DoS envían paquetes IP o información de tamaño o formatos atípicos que saturan los equipos de destino o los vuelven inestables, por lo que impiden normal funcionamiento de los servicios de red que brindan. No se trata de un ataque en el que se busque acceder a la red de datos objetivo para robar o dañar la información, lo que se busca es dañar la reputación de las organizaciones con presencia en internet y potencialmente impedir el desarrollo normal de sus actividades.

La DoS por saturación, satura un equipo con solicitudes para que no pueda responder a las solicitudes reales, la DoS por exploración de vulnerabilidades, aprovecha una vulnerabilidad en la red de datos para volverla inestable.

La *técnica smurf* se basa en el envío de paquetes de ping (eco) a uno o más servidores de difusión mientras falsifica las direcciones IP de origen para dirigir las respuestas hacia un objetivo, un servidor de este tipo tiene la capacidad de multiplicar un mensaje y enviarlo a todos los equipos de una red de datos, con el fin de paralizarla. Mediante el ping que es una herramienta que aprovecha una vulnerabilidad del protocolo ICMP, el servidor transmite la solicitud a toda la red de datos, todos los equipos de la red de datos envían una respuesta al servidor de difusión, el servidor redirecciona las respuestas al equipo de destino.

La *técnica del ping de la muerta* es uno de los ataques más antiguos y consiste en enviar un datagrama IP cuyo tamaño real supere el máximo autorizado (65536 bytes), normalmente un paquete de ping contiene poca información o ninguna, pero el paquete de ping de la muerte contiene una gran cantidad de información, cuando esta información es leída por el sistema informático objetivo que contiene una pila de protocolos TCP/IP, este de derrumba por desbordamiento de búfer. Los sistemas informáticos más modernos ya no son vulnerables a este tipo de ataques.

La *técnica por fragmentación* es un ataque que consiste en saturar el tráfico de la red de datos para aprovechar el principio de fragmentación del protocolo TCP/IP, debido a que este protocolo se utiliza para fragmentar paquetes grandes en paquetes más pequeños, teniendo cada uno un número de secuencia de identificación común, por lo tanto esta técnica de ataque introduce información falsa en los paquetes fragmentados, quedando en consecuencia fragmentos vacios o superpuestos que pueden desestabilizar el sistema. Los sistemas informáticos más modernos ya no son vulnerables a este tipo de ataques.

La *técnica land* es un ataque que se efectúa a través de una usurpación de dirección IP que aprovecha las vulnerabilidades del protocolo TCP/IP en las redes de datos, este ataque consiste en enviar un paquete con la misma dirección IP y el mismo número de puerto en los campos fuente y destino de los paquetes IP, bloqueando o volviendo inestables a los sistemas. Los sistemas informáticos más modernos ya no son vulnerables a este tipo de ataques.

La *técnica SYN*, también llamada *inundación TCP/SYN*, es un ataque en el que el sistema informático fuente envía gran cantidad de número de paquetes TCP SYN hacia el sistema informático objetivo, con el fin de saturar el tráfico de la red de datos para aprovechar el mecanismo de negociación de tres vías del protocolo TCP. Los paquetes SYN son usados para iniciar una nueva conexión TCP. Cuando el objetivo recibe el paquete SYN, le responde con un paquete TCP SYN ACK, el origen recibe el paquete y le envía de regreso un SYN ACK para establecer la conexión. El ataque SYN consiste en enviar una gran cantidad de solicitudes SYN a través de una computadora con una dirección IP inexistente no válida, por lo que el equipo de destino no puede recibir un paquete ACK, se vuelve inestable y puede provocarse el reinicio del sistema.

El ataque por DoS no depende del ancho de banda que disponga el pirata informático, en este caso el mismo está consumiendo las estructuras de información del kernel, implicadas en establecer una conexión TCP.

Gráfico 2.1. Ejemplo de un ataque por DoS.

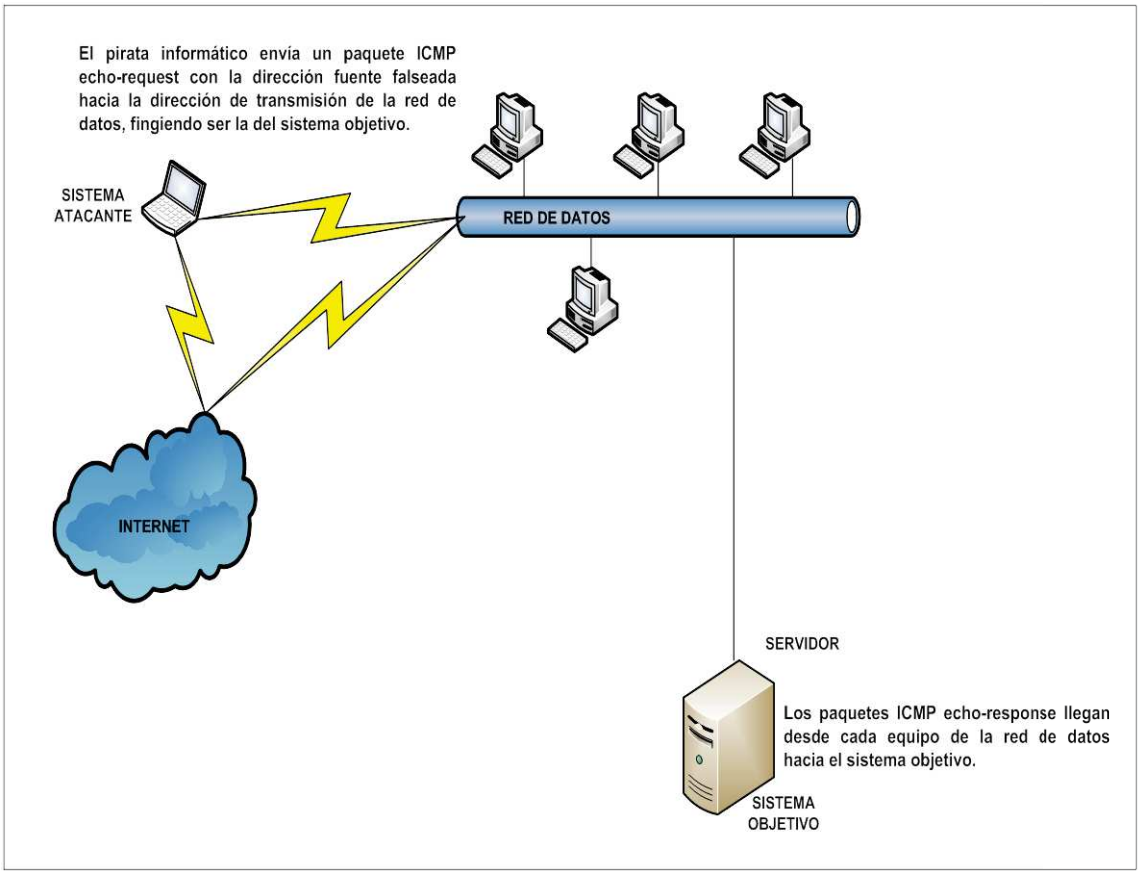


Gráfico realizado por Marco Castillo, autor del presente trabajo.

2.2.2.5. MitM *(Man in the middle – Hombre en la mitad)*. - Este ataque es una situación donde el pirata informático detecta y supervisa una comunicación entre dos usuarios y falsifica los intercambios para hacerse pasar por uno de ellos, la mayoría de estos ataques supervisan la red de datos con una herramienta llamada *rastreador de puertos*.

Un switch dirige el tráfico a los puertos basados en la *dirección MAC (Media Access Control – Control de Acceso al Medio)*, cada tarjeta de red tiene una dirección MAC única y el switch sabe cuales direcciones residen en que puerto. Los ataques MitM provocan que el switch redireccione el tráfico hacia otro destino, he aquí estos ataques.

El *ataque ARP*, busca aprovechar una debilidad de *ARP (Address Resolution Protocol - Protocolo de Resolución de Direcciones)*, este consiste en averiguar

la IP de un equipo a partir de la dirección MAC (dirección física) de la tarjeta de red, con el fin de interceptar dos equipos de la red de datos y enviarles a cada uno de ellos un paquete ARP falso, donde se establece que la dirección MAC del otro equipo ha sido modificada reemplazándola con la dirección del pirata informático, los dos equipos actualizarán su tabla dinámica; en este tipo de ataque hablamos de un envenenamiento de la caché ARP. De este modo si uno de los equipos quiere comunicarse con el equipo remoto, los paquetes serán enviados al pirata informático y este será quien los enviará de forma transparente. El ataque ARP funciona únicamente en la subred local debido a que los mensajes ARP no salen al exterior de la misma, por lo tanto el rastreador de puertos debe residir en la misma subred.

El *ataque de replay*, intercepta paquetes de datos y los reenvía al servidor tal como están, de esta forma el pirata informático se puede beneficiar de los derechos del usuario, por ejemplo el mismo usuario puede enviar un nombre de usuario y una contraseña cifrados a un servidor para registrarse, si un pirata informático intercepta la comunicación y reproduce la secuencia obtendrá los mismos derechos que el usuario, además si el sistema permite cambiar la contraseña, el pirata informático podría dejar al usuario sin acceso.

El *ataque por duplicación de MAC*, duplica la dirección MAC de un sistema objetivo; de tal forma que el switch envíe el tráfico hacia el rastreador, para esto el pirata informático debe cambiar la MAC en el rastreador para que sea igual a la del otro sistema en la red de datos. Modificar la dirección MAC de un dispositivo no es del todo imposible, se lo puede hacer en un sistema *Linux* utilizando el comando *ifconfig*, también ciertos utilitarios disponibles para modificar la MAC en sistemas *Windows*.

El *ataque por falseamiento del DNS,* busca engañar al sistema de envío para mandar el tráfico hacia la propia dirección MAC, mediante este mecanismo el rastreador envía respuestas a las solicitudes del DNS, estas respuestas proporcionan la dirección IP del rastreador, causando que el sistema de envío

mande todo el tráfico hacia el rastreador. El pirata informático debe ser capaz de ver todas las solicitudes DNS y responder a ellas antes de que el DNS real lo haga, esto implica que el rastreador está en la ruta de red desde el sistema en envío hacia el servidor DNS.

2.2.2.6. Suplantación de IP.- Esta técnica de ataque consiste en reemplazar la dirección de un paquete IP del remitente por otra dirección IP. Este ataque aprovecha que no hay validación de las direcciones IP en un paquete, por lo que un pirata informático puede modificar la dirección fuente para hacer parecer que este proviene de cualquier otro lugar, por lo tanto el pirata informático puede enviar paquetes de manera anónima, suplantando la dirección IP al enviar paquetes, más no cambiándola. Un proxy posibilita ocultar la dirección IP, sin embargo los proxies sólo envían paquetes, por lo que aunque la dirección IP este oculta, se puede encontrar a un pirata informático gracias al archivo de registro del sistema. Al intentar suplantar una dirección IP se debe tomar en cuenta, que el paquete de retorno desde un destino no regresaría a la máquina que envía. El encabezado TCP tiene un *ISN (Initial Sequence Number - Número de Secuencia Inicial)* que se utiliza para reconocer los paquetes y que para cada nueva conexión se lo supone seudo aleatorio. Si se conociera suficiente información acerca de las últimas ISN, podría predecirse el siguiente ISN y con esto se estaría en posibilidad de realizar un ataque de suplantación de IP. El pirata informático primero debe identificar su objetivo, mientras hace esto, debe determinar el incremento empleado en las ISN, esto se hace con una serie de conexiones legítimas hacia el objetivo y tomando nota con ISN que son devueltas. La técnica de suplantación de IP le permite al pirata enviar paquetes a una red de datos sin que el sistema de filtrado de paquetes del cortafuegos los intercepte. Los cortafuegos a menudo se basan en reglas de filtrado que indican las direcciones IP autorizadas a comunicarse con los equipos de la red de datos.

Si todo está hecho correctamente, el pirata informático logrará una conexión legítima hacia el sistema objetivo. La suplantación de IP es muy útil en aquellas

redes de datos cuyo acceso está restringido por IP como por ejemplo rlogin o rsh, cuando estos servicios están configurados en un sistema, como se ve en el gráfico 2b, es importante la dirección origen para determinar qué tipo de acceso se va a tener.

Gráfico 2.2. Conexión por suplantación de IP.

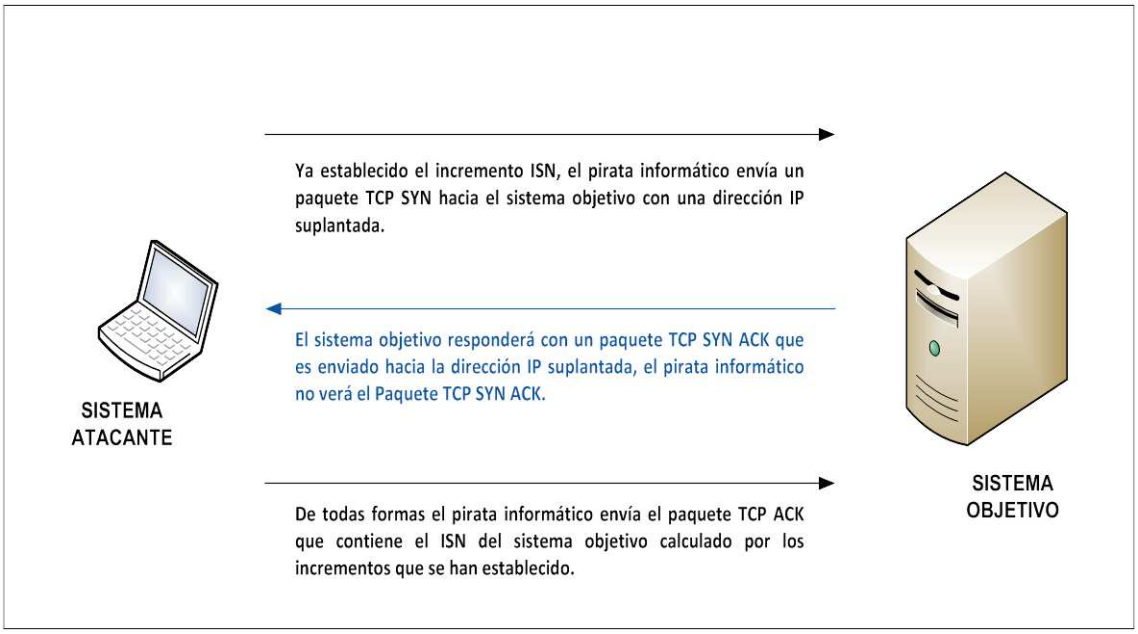


Gráfico realizado por Marco Castillo, autor del presente trabajo.

Un pirata informático puede encontrar una red de datos que tiene una relación de *fiabilidad* con otra y que puede estar a su alcance, entonces podrá hacer uso de la suplantación de IP para ingresar a esa red de datos, una vez adentro podrá ejecutar servicios para tener otro tipo de acceso usando su dirección original. Sin embargo hay un problema, el sistema objetivo enviará paquetes hacia la dirección IP suplantada, de acuerdo al funcionamiento de TCP, el sistema atacante que recibe esos paquetes al no conocer dicha conexión, enviará paquetes TCP RST para restablecer la conexión, entonces la conexión establecida por el pirata informático se caerá, pero este debe evitar que esto suceda y lo puede conseguir realizando un ataque de DoS en contra del sistema fiable.

2.2.2.7. Secuestro de sesión TCP.- Técnica de ataque conocida también como *hijacking* la cual consiste en interceptar una sesión TCP iniciada entre dos equipos para secuestrarla. La comprobación de la autentificación se hace solo al abrir la sesión, por lo que un pirata informático que inicie un ataque con éxito, puede controlar la conexión durante toda la sesión.

El *enrutamiento de origen del protocolo IP* es un método de secuestro inicial que consiste en especificar la ruta que los paquetes IP deben seguir a través del uso de una serie de direcciones IP que muestran los ruteadores que deben ser usados, por lo tanto el beneficio que obtiene el pirata informático es el indicarles a los paquetes una ruta de retorno bajo su control.

Cuando se deshabilita un enrutamiento de origen, hay un método llamado *ataque a ciegas* que consiste en enviar paquetes, sin buscar recibir respuesta y más bien buscando predecir una secuencia numérica.

Cuando un pirata informático está dentro de la red de datos, mediante el método llamado *MitM*, puede supervisar la misma y silenciar a uno de los usuarios al congestionar la red de datos o irrumpir en su equipo para tomar su lugar.

2.2.2.8. Correo electrónico no deseado.- También llamado *spam* o *correo basura*, este se define como el envío de correos electrónicos masivos, por lo general de publicidad, a usuarios destinatarios que no los han solicitado y cuyas direcciones de correo se las consiguieron generalmente por internet, su principal objetivo es publicar a través del *envío múltiple excesivo*. Los usuarios de internet que envían correos no deseados son llamados *spammers*. Los spammers a veces dicen de mala fe que sus usuarios destinatarios se registraron voluntariamente en sus bases de datos y que los correos electrónicos que reciben son fáciles de eliminar, los *spammers* usualmente recogen direcciones de correo electrónico del internet, como son en chats, foros, páginas web, etc. para esto utilizan programas llamados “robots” que

exploran páginas web y almacenan en bases de datos todas las direcciones de correo que encuentran.

Los efectos de correo no deseado son:

a. El ancho de banda que consume en la red de datos.
b. El espacio que ocupa en las casillas de correo de los usuarios.
c. Pérdida de tiempo en clasificar los correos electrónicos útiles para el usuario y eliminar los no deseados.
d. Dificultad para consultar los correos electrónicos personales o profesionales que están mezclados con los no deseados y el riesgo de eliminar por error o no leer los correos electrónicos importantes.
e. La naturaleza violenta o insultante que algunas veces suele acompañar a los correos no deseados.

El correo no deseado también genera costos adicionales para los proveedores de servicios de internet (ISP), que se ven reflejados en el costo a sus clientes, estos costos se relacionan con la configuración de sistemas antispam, el uso de equipos de filtrado, la capacitación y concientización a los usuarios.

Por lo general los *spammers* usan correos electrónicos falsos, por lo que es inútil responder, además una respuesta puede mostrarle al spammer que el correo electrónico está activo.

Para *combatir el correo no deseado* existen sistemas antispam basados en reglas modernas que permiten detectar y eliminar correos no deseados, por lo general el software antispam se divide en dos categorías:

a. **Los sistemas antispam para cliente.-** Utilizados por los usuarios del sistema de mensajería, estos sistemas presentan filtros de aprendizaje o filtros de identificación basados en reglas predefinidas (filtros Bayesianos). Estos sistemas pueden venir incluidos en las páginas de los correos

electrónicos de los usuarios, en cuya parte inferior o superior hay un botón que le da la opción de no recibir más este tipo de correo.

b. **Los sistemas antispam para servidor.-**Estos filtran el correo no deseado antes de que llegue al usuario destinatario, este sistema permite detener el correo basura en el nivel más alto y así evitar la congestión de las redes de datos y la saturación de los correos electrónicos.

Para *evitar el correo electrónico no deseado*, se debe suministrar la dirección de correo electrónico solo cuando sea realmente necesario, adicionalmente hay otros pasos sencillos pero efectivos para evitar el correo electrónico no deseado, por ejemplo:

a. No enviar mensajes de correo electrónico en que soliciten al usuario reenviarlos a tantos contactos como sea posible, esas listas son una bendición para los *spammers*, es posible reenviar el mensaje si el usuario se asegura de borrar o ocultar la dirección del usuario anterior.

b. Si es posible, se puede reemplazar la dirección de correo electrónico por una imagen, para así reducir en un buen porcentaje el riesgo de ser detectado por los spammers.

c. En lo posible hay que evitar publicar la dirección de correo electrónico en chats, foros u otras páginas web poco confiables.

d. Con respecto al punto anterior se puede crear una dirección desechable para usarlas en páginas web consideradas poco fiables, de tal forma que si se recibe un correo no deseado, sea fácil identificar el origen de la *filtración de la información*.

2.2.2.9. Bombardeo de correo electrónico.-Este ataque consiste en el envío de excesivos mensajes de correo electrónico idénticos a una dirección de

correo electrónico para desbordarla. Los correos se almacenan en un servidor de mensajería hasta que los lee el dueño de la dirección, y cuando este abre su correo, el último mensaje tardara demasiado tiempo en abrirse y la dirección quedará inutilizada. Para *combatir el bombardeo de correo electrónico*, se debe tomar ciertas medidas como por ejemplo tener una dirección de correo principal destinada a personas confiables y otra desechable para por ejemplo, registrarse en servicios en línea como chats, foros, búsqueda de amistades y otros servicios en línea; también se debe instalar un programa antispam para contrarrestar la recepción de varios mensajes idénticos.

2.2.2.10. Ataque a servidores web.- El protocolo *HTTP (Hiper Text Transfer Protocol – Protocolo de Transferencia de Hipertexto*) y el *HTTPS (HTTP Secure)*, representan la norma que permite la transferencia de páginas web a través de un sistema de solicitud y respuesta. Al ir corrigiendo gradualmente las vulnerabilidades de los conjuntos de protocolos TCP/I*P*, los ataques se dirigieron a las capas de aplicaciones y especialmente a la web, debido a que muchas organizaciones abrieron sus sistemas de cortafuegos al tráfico en internet; es por eso que hoy en día el protocolo HTTPy el HTTPS juegan un papel estratégico en la seguridad de las redes de datos y todos sus sistemas de información. Es importante que la seguridad de los servicios web se tenga en cuenta al momento del diseño y desarrollo, esto porque aunque los servidores web estén cada vez más protegidos, los ataques se están dirigiendo al aprovechamiento de las fallas de las aplicaciones web. Los ataques a los servidores web y sus aplicaciones se pueden clasificar así:

a. Manipulación de URL, que incluye la modificación manual de sus parámetros.
b. Aprovechamiento de las debilidades de los identificadores de sesión y sistemas de autenticación.
c. Inyección de código HTML y secuencia de comandos entre sitios.
d. Inyección de comandos SQL.

Los datos se pueden enviar por la URL de la página web, en encabezados HTTP y el HTTPS, en el cuerpo de la solicitud POST, a través de un *cookie*, se debe tener en cuenta como una idea primordial en que nunca se debe confiar en los datos enviados por el cliente.

Los ataques exitosos a los servidores web son muy dañinos porque pueden dañar la imagen y reputación de una organización, llegando a provocar el desfiguramiento de una página web, modificación de datos, robo de información, intrusión en el servidor web para modificar su comportamiento. Por eso es importante que las organizaciones, al menos las que manejen información sensible, cuenten con el Certificado de Seguridad *SSL* (*Secure Socket Layer – Capa de Conexión Segura)* de 128 bit, que es el máximo nivel de seguridad en páginas web.

2.2.2.11. Manipulación de URL.- Las direcciones web son también llamadas *URL´s(Uniform Resource Localizators* – Localizadores Uniformes de Recursos*)*, y en una aplicación web, la URL es el vector que identifica el recurso solicitado. Es una serie de caracteres ASCII dividida en las siguientes partes:

a. **Protocolo.-** lenguaje que se utiliza para comunicarse con la red, este puede ser HTTP, HTTPS o FTP.
b. **Usuario y contraseña.-** especifica parámetros seguros para acceder a un servidor seguro.
c. **Servidor.-** nombre de dominio de un computador que aloja el recurso solicitado.
d. **Puerto.-** número para indicar al servidor que tipo de recurso se está solicitando, el puerto que se vincula al protocolo de manera predeterminada es el 80.
e. **Ruta de acceso.-** indica al servidor dónde se encuentra el recurso.

La estructura básica de una URL es la siguiente:

http://dominio/directorio/archivo

Lo que sería: http://www.udla.edu.ec/ie_idiomas/index.htm
La URL envía parámetros al servidor colocando un signo de interrogación después del nombre del archivo y luego los datos en caracteres ASCII, por ejemplo:
http://www.udla.edu.ec/info/?cat=1&page=2

La *manipulación URL* consiste en que un pirata informático puede hacer que un servidor web le permita acceder a servicios web a los que no tenía acceso, en los sitios web los parámetros se transmiten a través de la URL, por ejemplo: http://target/info/?cat=2

Para modificar el parámetro manualmente de un vínculo propuesto, el pirata informático puede probar diferentes valores, por ejemplo:
http://target/info/?cat=8

De esta manera el pirata informático puede tener acceso a un área que generalmente está protegida, por lo que es importante que el diseñador prevea esta posibilidad.

Un pirata informático puede hacer que la página web procese un caso imprevisto, por ejemplo: http://target/info/?cat=**********

Por esto es importante que el diseñador prevea que los datos estén representados por un número, para evitar que la página web caiga en estado no previsto y pueda brindar información en un mensaje de error. Un pirata informático puede intentar la *prueba y error,* esto es probar directorios y extensiones de archivos al azar para encontrar información importante, por ejemplo:

a. Buscar directorios para administrar el sitio: http://target/admin.cgi

b. Buscar una secuencia de comandos para revelar información sobre el sistema remoto: http://target/phpinfo.php6
c. Buscar copias de seguridad a través de la extensión .bak , la cual no es interceptada de manera determinada por los servidores: http://target/.bak.
d. Buscar archivos ocultos en el sistema remoto: http://target/.bash_historyhttp://target/.ntaccess

Un pirata informático puede modificar la estructura del árbol de la ruta en la URL, de esta manera un usuario estaría obligado a retroceder en la estructura del árbol, principalmente cuando no tiene acceso al recurso, este método se denomina *cruce de directorio* o *cruce de rutas,* por ejemplo:
http://target/base/test/ascii.php3
http://target/base/test/
http://target/base/

El pirata informático puede aprovecharse de servidores vulnerables para retroceder por la ruta con varias cadenas, por ejemplo:
http://target/../../../../directory/file

Los piratas informáticos más avanzados codifican ciertos caracteres, por ejemplo:

a. Codificación URL: http://target/..%2F..%2F..%2Fdirectory/file
b. Notación Unicode: http://target/..%u2216..%u2216directory/file

Dado que los sitios dinámicos transfieren los nombres de las páginas a visualizarse, por ejemplo:
http://target/cgi-bin/script.cgi?url=index.htm

Si no se realizan las verificaciones necesarias de las vulnerabilidades, un pirata informático puede modificar la URL de manera manual con el fin de solicitar acceso a un recurso de página al que no tiene acceso, por ejemplo:
http://target/cgi-bin/script.cgi?url=script.cgi
Entre las contramedidas a tomar para proteger un servidor web contra la manipulación de URL, se debe controlar las vulnerabilidades y aplicar las actualizaciones que provee el editor del servidor web, además de los siguientes puntos:

a. Se debe impedir la navegación por páginas que estén bajo la raíz, mecanismo *chroot.*
b. Se debe deshabilitar la visualización de los archivos de un directorio que no contiene un archivo índice, navegación de directorio.
c. Se debe borrar directorios y archivos innecesarios, incluso los ocultos.
d. El servidor debe proteger el acceso a directorios que contiene información importante.
e. Se debe borrar las opciones de configuración innecesarias.
f. El servidor debe interpretar las páginas dinámicas con precisión, aún archivos de copias de seguridad como .bak.
g. Se debe eliminar los intérpretes de secuencia de comandos innecesarios.
h. Se debe impedir la visualización HTTP en páginas HTTPS accesibles.
i. Se debe obtener el Certificado de Seguridad SSL de 128 bit, que es el máximo nivel de seguridad en páginas web.

2.2.2.12. Secuestro de comandos entre páginas web.- Este ataque también es conocido como XSS o CSS *(Cross Site Scripting)* y está dirigido a páginas web que muestran de forma dinámica el contenido de los usuarios sin verificar ni codificar la información ingresada. Esto consiste en reemplazar el valor del texto que se mostrará con una secuencia de comandos de modo que aparezca en una página web, de esta manera un pirata informático puede inyectar un código arbitrario en una página web para que se ejecute en el equipo de un

usuario. Sin el navegador del usuario está configurado para ejecutar las secuencias de comandos, el código malintencionado tendrá acceso a todos los datos compartidos por la página web y el servidor del usuario, como por ejemplo campos de entrada, cookies, etc. Debido a las vulnerabilidades de las secuencias de comandos entre páginas web, un pirata informático puede usar esta técnica para recuperar datos intercambiados entre el usuario y la página web a la que ingresa, de esta forma el código inyectado en la página web se puede usar para engañar al usuario y hacer que ingrese información de autenticación, además la secuencia de comandos inyectada puede redireccionar al usuario a una página web controlada por el pirata informático y engañarlo utilizando una interfaz gráfica igual a la página web original. Así se deduce que si el contenido suministrado por el usuario no se verifica, es posible mostrar un código HTML arbitrario en una página web para cambiar su apariencia contenido o comportamiento. En este contexto se ve afectada por completo la relación de confianza que existía entre el usuario y la página web.

a. Los usuarios pueden protegerse contra este ataque configurando sus navegadores para impedir que se ejecuten lenguajes de secuencia de comandos, esto no brinda una solución óptima debido a que varias páginas web no funcionan adecuadamente cuando se prohíbe la ejecución de un código dinámico; la solución más precisa para detener este ataque consiste en diseñar páginas web sin vulnerabilidades, para esto es necesario verificar el formato de los datos ingresados por el usuario y codificar los datos viables del usuario reemplazando los caracteres especiales con sus equivalentes en HTML. Otra forma de protegerse es obteniendo el Certificado de Seguridad SSL de 128 bit, que es el máximo nivel de seguridad en páginas web.

2.2.2.13. Inyección de comandos SQL.- Este ataque va dirigido a las páginas web que dependen de bases de datos relacionadas, estas páginas web pasan los parámetros que se pasan a la consulta de SQL, algunos caracteres permiten coordinar varias consultas de SQL o ignorar el resto de la consulta.

Un pirata informático puede modificar la consulta para acceder a toda la base de datos e incluso modificar su contenido, además que al insertar un carácter en la consulta puede ejecutar potencialmente la consulta que elija. Por ejemplo SQL Server tiene procedimientos almacenados que permiten comandos de administración, esto es potencialmente peligroso porque algún usuario podría ejecutar comandos que pueden causar una posible intrusión. Por eso es importante que el diseñador verifique los parámetros que se pasan en la consulta de SQL.

Por ejemplo en una consulta que espera un nombre de usuario como parámetro:
*SELECT * FROM usuarios WHERE nombre="$nombre";*

Siendo así, un intruso necesitaría escribir un nombre, por ejemplo, “pepe” O 1= 1 O nombre=”pipo” para que la consulta quede así:
*SELECT * FROM usuarios WHERE nombre="pepe" OR 1=1 OR nombre=”pipo”;*

Con la cláusula *WHERE* se devolverá registros que corresponden a todos los usuarios.

Hay algunas reglas que pueden ayudar a proteger contra este tipo de ataques:

a. Mantener controlados los privilegios de las cuentas de los usuarios.
b. Verificar el formato de los datos de entrada, en especial si hay caracteres especiales.
c. Eliminar las cuentas de usuario que no se usan, como las predeterminadas.
d. No aceptar cuentas sin contraseñas.
e. Eliminar los procedimientos almacenados.
f. No permitir que se vean mensajes de error explícitos que muestren la consulta de SQL.

g. Se debe obtener el Certificado de Seguridad SSL de 128 bit, que es el máximo nivel de seguridad en páginas web.

2.2.2.14. Suplantación de identidad o phishing.- Técnica fraudulenta que usan los piratas informáticos para engañar a los usuarios de internet enviándoles un correo electrónico usurpando la identidad de una organización fiable como una página web bancaria o corporativa, y de esta manera conseguir información sobre cuentas bancarias, tarjetas de crédito, registros, contraseñas e incluso información personal, para luego usarla con destreza en su propio beneficio. En este tipo de ataque se invita al usuario a conectarse a través de un vinculo de hipertexto y a llenar un formulario en la página web falsificada, que es una copia exacta de la original, todo bajo el pretexto de actualizar datos, actualizar los servicios o hasta para soporte técnico etc. En la suplantación de identidad no se emplea una vulnerabilidad de las redes de datos, sino que se engaña al usuario utilizando la ingeniería social.

Si se recibe un mensaje que aparentemente proviene de la página web de un banco o de otra organización, hay que preguntarse si se ha dado la dirección de correo electrónico a esta organización, si el correo electrónico recibido tiene información personalizada que permita verificar su veracidad. Además se recomienda tomar las siguientes precauciones:

a. Tener cuidado con los formularios que soliciten información bancaria, porque es raro que un banco solicite información tan importante a través de un correo electrónico, lo mejor es descartar este correo electrónico o si se tiene dudas contactarse con el banco telefónicamente.

b. No hacer clic en el vínculo que aparece en el correo electrónico, es mejor ingresar a este servicio a través de la URL.

c. Asegurarse que la URL de la organización sea la que afirma ser, por ejemplo se debe prestar atención a la ortografía.

d. Que el navegador estese en modo seguro cuando se ingrese información importante, es decir que en lo posible la barra del navegador empiece con HTTPS y que además aparezca un candado en la barra de estado de la parte inferior del navegador.

2.2.2.15. Puertas traseras.- Del *inglés trap doors* o *back doors*, consiste en un mecanismo establecido por los astutos piratas informáticos para modificar el funcionamiento de un sistema informático y accederlo a su antojo, esquivando todas las medidas de seguridad establecidas cuando se usa el procedimiento normal. Existen muchas formas de crear puertas traseras con la finalidad de proporcionar una ruta directa y oculta de acceso a un sistema informático. Hay varios mecanismos que utilizan los piratas informáticos para tomar el control de los sistemas atacados.

a. Creación de cuentas de usuario.- Por ejemplo los piratas informáticos trataran de crear cuentas de usuario con nombres discretos pero que tiene privilegios de *superusuario* como *root* o *administrador.*

b. Archivos de inicio.-Este es uno de los mecanismos preferidos de los intrusos, debido a que se generan trampas que se reinician una y otra vez cuando un usuario reinicia el sistema. Los lugares donde por lo general se instalan estos programas como el *Back Orifice* en Windows son *HKLM\Microsoft\Windows\Current Version\ Run, Run Once, Run Once Ex, Run Services, Win Logon*. En cambio en Linux en los archivos *rc.d* y en el *inetd. conf*. Para detectar un archivo modificado en sistemas Linux o Windows se puede utilizar el programa *Trip Wire.*

c. Trabajos programados.-Aunque los archivos de inicio son lugares ideales para esconder puertas traseras, también lo son las colas de trabajos

programados. Los piratas informáticos pueden garantizar que siempre se estará ejecutando un servicio vulnerable que se pueda manipular, solamente con la implantación de una puerta trasera que se ejecuta a si misma de forma continua.

d. **Control remoto.-** Cuando se desactivan los servicios de acceso remoto como *telnet, ssh* o *escritorio remoto* una contraseña de *root* no sirve de nada. Mediante el uso de herramientas que crean *shells* remotas con facilidad, incluso puertas traseras gráficas, el intruso intentará habilitar algún acceso remoto; por ejemplo con *Netcat* se puede crear puertas traseras en *Linux* y *Windows.*

e. **Redireccionamiento de puertos.-** Cuando un cortafuegos bloquea el acceso directo al sistema objetivo, los piratas informáticos podrán superar estos obstáculos utilizando el redireccionamiento de puertos, este funciona escuchando ciertos puertos y enviando los paquetes en bruto a un sistema secundario específico, hay puertos que por lo general no los bloque un cortafuego como el 80 (HTTP) en Windows, 3128 (HTTP) en Linux, 25 (SMTP), 110 (POP3), y que el intruso los usa para escucharlos.

A veces las puertas traseras se pueden crear con el fin de permitir el acceso directo y fácil a determinados sectores del sistema en caso de fallo del mecanismo normal de acceso, a este mecanismo de acceso el administrador pudo haberle puesto una combinación de teclas, una secuencia definida de acciones o un usuario y contraseña particular, al distribuir la aplicación es aconsejable que el administrador elimine estas puertas traseras, por ejemplo la BIOS de las placas AWARD es un ejemplo de puerta trasera.

Aunque existen ciertas herramientas de software para detectar puertas traseras, encontrarlas y eliminarlas es todavía muy complejo, porque los piratas informáticos saben innumerables formas de crearlas, por el momento la forma más fiable para recuperarse después de un fuerte ataque por medio de una puerta trasera, es restaurar el Sistema Operativo y las aplicaciones junto con la

información de los usuarios. Otra arma aún más eficaz es la prevención y el monitoreo constante de los puertos por medio de un cortafuegos fiable que detecte y rechace el envío de ciertos paquetes peligrosos como los paquete enviados en bruto, sin la necesidad de bloquear ciertos puertos importantes.

2.2.2.16. Fraudes por correo electrónico.- Hay otro tipo de amenazas en el internet, que se enmarcan dentro del fraude y la estafa.

Entre estos fraudes está el *scam,* que es una práctica fraudulenta de origen africano y que consiste en obtener dinero de los usuarios de internet por coerción, al tentarlos con una suma de dinero prometiéndoles una parte. Este método consiste en recibir un correo electrónico del único hijo de un hombre rico que falleció recientemente, en vida el fallecido ha depositado varios millones de dólares en una aseguradora financiera y el individuo que se ha contactado necesita que un socio extranjero honesto le ayude a transferir los fondos, estando dispuesto a pagarle un porcentaje nada despreciable si la victima proporciona una cuenta donde transferir los fondos. Si el usuario cae en la trampa, hay dos posibles situaciones, la una es que al ganarse la confianza de la víctima a través del intercambio de correo electrónico, el delincuente le envía “documentos legales” y le solicitará anticipos de los fondos para los honorarios del abogado, tarifas bancarias, impuestos y tasas, etc., la otra es que el delincuente engatuse a la víctima para que viaje a su país y lleve dinero efectivo que tendrá que gastar en la estancia, sobornos, tarifas bancarias etc., y así sucesivamente; en el mejor de los casos la victima regresa a casa habiendo perdido su dinero y en el peor de los casos podría hasta perder la vida. Si se recibe este tipo de correo electrónico, lo ideal es borrarlo, porque definitivamente se trata de una tentativa de estafa, también se puede ayudar previniendo a otros usuarios sobre este tipo de engaños.

Otro tipo de fraudes son las *loterías internacionales*, que consiste en recibir un correo electrónico en el que se informa que se es el afortunado ganador de una lotería muy importante que otorga cientos de miles de dólares. Después de entrar en confianza con el usuario intercambiando algunos correos

electrónicos que incluyen certificados adjuntos en el que aseguran que el usuario es realmente el ganador, el remitente que es el delincuente, explica que para cobrar el premio se debe pagar tarifas y tasas administrativas y varios impuestos; si los usuarios muerden el anzuelo estos estafadores pueden conseguir significativas cantidades de dinero. La primera pregunta lógica que debe hacerse un usuario es ¿cómo se explica que para cobrar se tenga que pagar tanto dinero?, además las loterías tiene reglas claras y no cobran dinero para pagar y generalmente los descuentos por impuestos y otros rubros se los hace directamente del premio del ganador, lo mejor es borrar este tipo de correos electrónicos. [17]

2.2.3. Amenazas programadas

Una de las amenazas principales a la seguridad informática son las amenazas programadas, estas consisten en códigos diseñados para atacar las medidas de seguridad de un sistema informático. Existen distintos tipos de amenazas programadas, entendiéndose que algunos códigos pueden entrar en diversas categorías o combinar varios tipos de amenazas en un solo código. Se va a definir y diferenciar los tipos fundamentales de amenazas programadas.

2.2.3.1. Virus.- Los virus informáticos son programas que dependen de la ejecución de otros programas, en si los virus no están hechos para existir por sí solos. Los virus, por tratarse de programas, para su activación deben ser ejecutados y funcionar dentro del Sistema Operativo al menos una vez; los mismos ingresan al Sistema Operativo de forma inadvertida para el usuario y al ser ejecutados se activan y actúan con la computadora huésped. Hay varias definiciones para los virus informáticos, pero a continuación se va a dar una definición general:

“Un virus informático es una secuencia de códigos con instrucciones ejecutables, creado con el objetivo de alterar el correcto funcionamiento de un sistema, siendo capaz de auto replicarse y parasitar otras secuencias y así

[17] Tema, y subtemas desarrollados a partir de las siguientes fuentes:
Fundamentos de seguridad, pág. 28-40, autor: F. Vergara
http://es.kioskea.net/contents/attaques/attaques.php3

corromper o destruir parte o la totalidad de la información almacenada el disco duro o dispositivos externos".

El nombre real que corresponde a los virus es *código auto programado* pero por analogía con el campo de la biología se les dio el nombre de virus, debido a que no funcionan por si solos, sino que deben parasitar otros programas para poder funcionar, en este sentido es muy adecuado el uso del término virus, puesto que los virus biológicos también poseen esta característica.

Los piratas informáticos han logrado tres avances importantes que generan un nuevo nivel de riesgo. Primero, la funcionalidad del código metamórfico ha progresado, lo que quiere decir que los virus son más hábiles para auto modificarse y así evadir ser identificados. Segundo está la evolución de los rootkits, un tipo de virus que puede actuar por debajo del Sistema Operativo y cargarse durante el arranque de la máquina, esto le permite esconderse de todo tipo de detección estándar de antivirus. Tercero está la proliferación de botnets, estos son virus que infectan computadoras para permitir al pirata informático tomar control sobre ellas y formar redes para dirigir ataques, actualmente los piratas informáticos logran armar botnets con cientos de miles de computadoras. Los virus se reproducen al infectar *aplicaciones huésped,* esto significa que copian una parte del código ejecutable en un programa existente, para hacerlo incluyen una serie de bytes en la aplicación infectada, los cuales verifican si ya se ha producido la infección, esto se denomina firma de virus. Para detectar los virus, los programas antivirus dependen de esta firma, la que es única en cada virus, este método es conocido como *análisis de firma,* este método es fiable si la base de datos del virus del programa antivirus está actualizada e incluye las firmas de todos los virus conocidos, sin embargo este método no puede detectar virus que no fueron archivados por los editores del software antivirus.

Los programas antivirus también usan un *verificador de identidad* para controlar si se cambiaron las carpetas, el verificador de identidad crea una base

de datos que contiene información de los archivos ejecutables en el Sistema Operativo.

El método heurístico implica el análisis del comportamiento de las aplicaciones para detectar una actividad similar a la de un virus conocido, de esta manera un programa antivirus puede detectar virus incluso cuando la base de datos del antivirus no ha sido actualizada.

2.2.3.2. Gusanos.- Del inglés *worm*, los gusanos son programas independientes capaces de auto replicarse, se extienden por sus propios medios y se reproducen por sí solos, por lo que no necesitan parasitar otros programas para replicarse. Generalmente los gusanos actúan y se desarrollan en el entorno de una red de datos, reproduciéndose y viajando entre las distintas computadoras de la misma, pues se *arrastran* por todo el sistema informático sin necesidad de un programa que los transporte. Los gusanos se cargan en la memoria y se posesionan de alguna *dirección,* luego se copian en otro lugar y se borran del que ocupaban, y así sucesivamente, haciendo de esta manera, que queden borrados los programas o la información que encuentran a su paso por la memoria, lo que causa problemas de operación o pérdida de información.

La ejecución y distribución de los gusanos generalmente se basa en debilidades o errores de los protocolos de red o de los programas incluidos en los Sistemas Operativos, los gusanos tienden a replicarse en forma tal, que saturan los recursos de las máquinas, provocando un ataque por denegación de servicio. No sería raro que un gusano incluya como parte de su código algún virus o bomba lógica, que actúen sobre las computadoras en las que se establece.

2.2.3.3. Caballos de Troya.- Los caballos de Troya o troyanos son un fragmento de código que se esconde en el interior de un programa inofensivo, introduciéndose al sistema bajo una apariencia totalmente diferente a la de su

objetivo final, de esta manera los caballos de Troya ocultan su naturaleza maliciosa detrás de una fachada de algo útil o interesante; buena parte de los caballos de Troya contienen mecanismos para extenderse hacia nuevas víctimas. Un caballo de Troya podría ser un código escondido en una versión demostrativa de un software o en el interior de un juego, que el usuario pudo habérselo descargado del internet o mediante un dispositivo externo. El usuario al principio no tiene por qué notar la diferencia con un programa de calidad, sin embargo al ejecutar el programa, el caballo de Troya de modo oculto, estaría realizando otro tipo de acciones, como borrar código, obtener contraseñas, enviar información por internet, copiar fechas confidenciales, instalar un virus informático, entre otras operaciones maliciosas, no necesariamente los caballos de Troya se pueden ejecutar al mismo tiempo que se ejecuta el programa anfitrión, sino que al cabo de un tiempo y esperando una instrucción programada, despiertan y comienzan a ejecutarse a espaldas del usuario y a mostrar sus verdaderas intenciones.

A diferencia de los virus y los gusanos, los caballos de Troya son incapaces de replicarse y su funcionamiento se basa en la ejecución del programa original que lo contiene. El nombre de esta amenaza proviene de la táctica para vencer a los troyanos ideada por Ulises en la epopeya *La Ilíada* escrita por Homero, debido a que un caballo de Troya es un programa oculto dentro de otro, que ejecuta comandos furtivamente y que, por lo general, abre el acceso a la computadora y lo opera abriendo una *puerta trasera*, siendo esto lo peor, porque de esta manera un caballo de Troya puede crear una infracción intencional de seguridad dentro de la red de datos para que los piratas informáticos puedan acceder a áreas protegidas de la misma. Al cabo de un tiempo, la infección por parte de un caballo de Troya puede ser evidente si se presentan ciertas actividades anormales como que los datos se carguen aunque el usuario no registre actividad, reacciones extrañas del ratón, programas que se abren en forma inesperada, repetidos bloqueos, aunque no necesariamente estos pueden ser los síntomas de todos los caballos de Troya, debido a que unos son más hábiles que otros. La instalación de un cortafuegos

en teoría debería ser suficiente para proteger un sistema informático de esta amenaza programada, el cortafuegos pide la confirmación de la acción antes de iniciar una conexión si un programa cuyos orígenes se desconoce, intenta abrir una conexión, debido a que dicho programa podría contener un caballo de Troya.

2.2.3.4. Bombas lógicas.- Es una pieza de código que puede estar oculta dentro de un programa, preparada para atacar el sistema cuando se cumplan ciertas condiciones como la ejecución de un programa que contiene a código en una fecha determinada, arrancar el sistema un determinado número de veces, *puertas traseras,* pulsar una secuencia definida de teclas o incluso botones del programa que contiene al código, etc.

2.2.3.5.*Spyware.-*Son programas que recolectan información acerca del usuario y del equipo en el que están instalados, esta información puede ser de tipo personal, direcciones *URL* de sitios visitados, análisis de compras en línea, términos de búsqueda introducidos en los buscadores, análisis de pagos con tarjetas de crédito, débito, cuentas bancarias; luego esta información puede ser enviada a un editor de software a fin de obtener un perfil de los usuarios de internet. Generalmente los spyware suelen instalarse con programas gratuitos o de prueba, esto puede ser rentable para sus creadores porque estos programas se entregan sin recargo a cambio de información personal. En términos generales el *spyware* no vendría a ser ilegal porque en el contrato de licencia se deja en claro que este programa se instalara en la computadora, sin embargo los usuarios rara vez leen el extenso término del contrato y por tanto muy pocos saben que el software está creando un perfil de ellos. Pero aun así se puede hacer daño por la divulgación de información personal, adicionalmente el *spyware* puede causar otras dificultades como utilizar espacio en disco, consumir ciclos del procesador, consumir RAM, dañar otras aplicaciones, mostrar anuncios emergentes personalizados basados en los datos recolectados.

Generalmente hay dos categorías de spyware:

a. ***Spyware* interno.-** incluye líneas de código dentro de un programa, estas líneas recolectan información. Hay algunos programas que viene acompañados por uno o más programas de spyware como por ejemplo: *Babylon Translator, GetRight, Go! Zilla, Download Accelerator, Cute FTP, PKZip, KaZaA e iMesh.*

***b. Spyware* externo.-**son programas independientes de recolección de datos, algunos ejemplo de estos programas son: *Alexa, Aureate/Radiate, BargainBuddy, ClickTillUWin, Conducent Timesink, Cydoor, Comet Cursor, Doubleclick, DSSAgent, EverAd, eZula/KaZaa Toptext, Flashpoint/Flashtrack, Flyswat, Gator / Claria, GoHip, Hotbar, ISTbar, Lop, NewDotNet, Realplayer, SaveNow, Songspy, Xupiter, Web3000 y WebHancer*

Para protegerse de los *spyware* es recomendable no instalar ningún software del que no se tenga la certeza de su origen y fiabilidad, como por ejemplo aquellos que son gratuitos o de prueba y específicamente el software de intercambio de archivos punto a punto. Desinstalar estos programas solo en algunas ocasiones elimina el *spyware* con el que se instaló, lo que es peor su desinstalación puede provocar que otras aplicaciones no funcionen bien. La presencia de procesos de fondo sospechosos, archivos extraños, entradas de registro, pueden indicar la presencia de *spyware* en la computadora; aunque no se verifique minuciosamente la base de registro a diario, hay programas *antispywar*e para detectar y eliminar archivos, procesos y entradas de registro creadas por el *spyware*. La instalación de un cortafuego puede detectar *spyware* y prevenir que estos accedan a internet y así evitar que estos envíen datos recopilados.

2.2.3.6. Híbridos.- Estos son combinaciones de gusanos y caballos de Troya o de virus y caballos de Troya. Los gusanos y caballos de Troya como por ejemplo nimda, utilizan vulnerabilidades web y suelen extenderse a través del correo electrónico incluyendo un archivo adjunto en el que se tienta al usuario

para que lo abra. Los virus y caballos de Troya se diseminan como virus y abren puertas traseras como caballos de Troya, en máquinas infectadas.

2.2.3.7. Otras clases de amenazas programadas.- Hay otras amenazas programadas de menor incidencia, estas pueden ser:

a. Salami.- Son secuencias de códigos diseñados para alterar al mínimo algunos datos bancarios, como desplazar los puntos decimales para redondear las cantidades.

b. Polillas o *bugs*.-No son en sí una amenaza programada, sino un defecto del software de mala calidad, esto puede crear pérdida parcial de la información y puede producir daños en la estructura lógica del disco, todo esto causa pérdida de clúster o la aparición de enlaces cruzados.[18]

2.3. Vulnerabilidades más críticas en internet

Entre los errores de seguridad más habituales está la instalación de software del sistema sin quitar los servicios innecesarios, la mayoría de los atacantes se aprovechan de quienes no actualizan el software, casi siempre por pereza o por ignorancia. Las contraseñas con pocos caracteres o predefinidas por defecto son un problema de seguridad para cualquier organización.

Se debe utilizar y escoger contraseñas fuertes, como las que son difíciles o imposibles de suponer. Demasiados puertos abiertos, es contraproducente, se recomienda cerrar los puertos innecesarios y abrir los que realmente se necesiten. La *SANS Institute (System Administration, Networking and Security Institute)* y el FBI han publicado una extensa lista con sus actualizaciones periódicas con las vulnerabilidades más explotadas en la mayoría de los ataques a sistemas informáticos vía internet.

---

[18] Tema, y subtemas desarrollados a partir de las siguientes fuentes:
Fundamentos de seguridad, pág. 41, 42, autor: F. Vergara
http://es.kioskea.net/contents/attaques/attaques.php3
Diapositivas: Seguridades de Redes Empresariales, 21-48, autor: Ing. Henry Burbano

En estos artículos se muestran las vulnerabilidades tanto para Windows como para sistemas basados en Unix, las que son explotadas por programas maliciosos y diestros piratas informáticos. Estos artículos incluyen versiones en varios idiomas y en su listado completo incluye soluciones y sugerencias para cada vulnerabilidad.

2.3.1. Instalaciones por defecto de sistemas y aplicaciones

La meta de la mayoría de software, incluyendo Sistemas Operativos y aplicaciones, es dejar los Sistemas Operativos lo más rápido posible, con la mayor parte de funciones habilitadas y poca trabajo para el administrador, para conseguir todo esto los *scripts* suelen instalar más componentes de los que se necesita en realidad; por ejemplo en las aplicaciones, las instalaciones por defecto regularmente incluyen programas o *scripts* que no son realmente necesarios. Esto genera la mayoría de las vulnerabilidades de seguridad debido a que los usuarios no aplican los parches a los componentes de software que utilizan, siendo un porcentaje muy bajo los usuarios que aplican los parches, es más, muchos usuarios no son conscientes de lo que realmente están instalando en su sistema informático. Aquellos servicios a los que no se les han aplicado los parches son vías para que los atacantes accedan a un sistema informático y lo controlen a su antojo.

En los Sistemas Operativos, las instalaciones por defecto por lo general incluyen extraños servicios con sus respectivos puertos abiertos, esto permitiría a los piratas informáticos introducirse en un sistema informático y comprometer la red de datos por medio de dichos puertos; cuantos menos puertos se hallen abiertos, menos alternativas tendrían los piratas informáticos para comprometer a una organización. Los scripts de ejemplo son una de las vulnerabilidades más serias en los servidores web, debido a que lo piratas informáticos los usan para comprometer al sistema informático y obtener información acerca de éste. Los scripts de ejemplo son un problema porque generalmente no son sometidos al mismo proceso de control de calidad que otros programas, siendo muchos de los cuales extremadamente peligrosos, además en la mayoría de casos están

mal escritos y la revisión de errores habitualmente es olvidada, convirtiendo a un sistema informático en blanco fácil para un ataque por desbordamiento de buffer.

2.3.2. Cuentas sin contraseña y contraseñas débiles

La mayoría de los Sistemas Operativos se encuentran configurados para usar contraseñas como primera línea de defensa. Si un pirata informático puede determinar el nombre de una cuenta y su contraseña correspondiente, este puede entrar a la red de datos; los nombres de usuario no son tan difíciles de adivinar, además las contraseñas fáciles de adivinar, las contraseñas por defecto y las contraseñas en blanco pueden llegar a ser un gran problema, en especial esta última. En la práctica este tipo de contraseñas deben ser eliminadas, a la vez que se las debe sustituir por contraseñas seguras, las mismas que deben ser difíciles de adivinar para posibles intrusos y fáciles de recordar para el administrador y los usuarios de una red de datos. Generalmente se aconseja que las contraseñas para que sean seguras, contengan caracteres alfanuméricos y signos.

Algunos Sistemas Operativos contienen cuentas y contraseñas por defecto, estas cuentas a veces tienen la misma contraseña para ciertas aplicaciones, de esto suelen aprovecharse los piratas informáticos, por este motivo cualquier cuenta por defecto, debe ser identificada y eliminada del Sistema Operativo y sus aplicaciones.

2.3.3. Respaldos incompletos o inexistentes

Cuando ocurre un ataque en contra de una organización, la recuperación de la información requiere respaldos actualizados y métodos probados para restaurarla; varias organizaciones hacen respaldos diarios, pero no verifican si estos realmente están funcionando; otras organizaciones definen políticas de respaldo, pero no procedimientos de restauración. Otro problema que perjudica a los respaldos es la deficiente protección física del hardware de respaldo,

estos deben ser protegidos de la misma forma que se lo hace con la información en sí.

Se aconseja a las organizaciones que los respaldos se los realice al menos diariamente, el requerimiento mínimo sería realizar un respaldo completo una vez a la semana y *respaldos incrementales*[19]todos los días. Se debe verificar una vez por mes el soporte del respaldo mediante la restauración de un servidor de prueba que verifique si efectivamente se está respaldando correctamente la información.

Algunas organizaciones realizan respaldos totales varias veces al día. Como conclusión se saca que la mejor solución es un respaldo total y redundante a prueba de fallos *(failover)*, al menos para grandes sistemas informáticos críticos y de tiempo real, como organizaciones vinculadas a las finanzas, comercio electrónico, investigación, defensa, entre otras.

2.3.4. Demasiados puertos abiertos

Tanto los usuarios legítimos como los atacantes se conectan a los sistemas informáticos a través de puertos. Cuantos más puertos abiertos se encuentren más formas hay para que alguien se conecte; por esta razón es importante mantener abiertos solo los puertos imprescindibles para que el sistema informático no corra altos riesgos y funcione adecuadamente, el resto de los puertos deben ser cerrados.

Bloquear los puertos más comúnmente rastreados y vulnerados constituye tan solo un mínimo requisito para la seguridad perimetral y no es una configuración completa del cortafuegos ni una solución exhaustiva de seguridad, una mejor aproximación es bloquear todos aquellos puertos que no son utilizados, aun así no está por demás supervisarlos para detectar intentos de intrusión. Incluso si

[19] Los respaldos incrementales son archivos cuyo valor de atributo es “A” son respaldados y el atributo es borrado. Solo los archivos que han sido creados o modificados son respaldados; obtenido de las dispositivas: Introducción a Windows Server 2003, diapositiva 67.

los puertos están bloqueados, un pirata informático puede introducirse a una red de datos a través de otros medios como un caballo de troya adjunto a un archivo de correo electrónico, un gusano e incluso una persona interna de la organización, por estos medios se puede atacar los puertos si no son debidamente asegurados. A continuación se presentan los puertos más comúnmente vulnerables: RPC y NFS, Portmap/rpcbind (111/TCP y 111/UDP), NFS (2049/TCP y 2049/UDP), lockd (4045/TCP y 4045/UDP) X Windows, del 6000/TCP al 6255/TCP

Servicios de Nombres de Dominio, DNS (53/UDP) a todas las máquinas que no sean servidores de nombres, transferencias de zona DNS (53/tcp) excepto desde servidores secundarios externos, LDAP (389/TCP y 389/UDP)

Correo electrónico, SMTP (25/TCP) a todas las máquinas que no sean ruteadores de correos externos, POP (109/TCP y 110/TCP), IMAP (143/TCP)

Web, HTTP (80/tcp), (3128/TCP) y SSL (443/TCP) excepto a los servidores web externos, y también se puede bloquear otros puertos altos que son comúnmente utilizados para la ubicación de servicios HTTP (8000/TCP, 8080/TCP, 8888/TCP)

Pequeños servicios, puertos inferiores al 20/TCP y 20/UDP, y time (37/TCP y 37/UDP)

Otros, TFTP (69/UDP), finger (79/TCP), NNTP (119/TCP), NTP (123/UDP), LPD (515/TCP), syslog (514/UDP), SNMP (161/TCP y 161/UDP, 162/TCP y 162/UDP), BGP (179/TCP), SOCKS (1080/TCP)

2.3.5. Insuficiente filtrado de paquetes con direcciones de inicio y destino inadecuadas

Cada paquete contiene una dirección IP de origen que es suplantada de una máquina por parte de un pirata informático, estos paquetes falsificados son enviados para inundar a una máquina víctima generalmente deteniendo sus servicios o incluso los servicios de una red de datos completa; el conocido ataque *smurf* hace uso de una característica de los enrutadores para enviar una secuencia de paquetes a miles de máquinas. Es necesario utilizar un mecanismo de filtrado sobre el tráfico que entra en la red de datos *(ingress filtering)* y el tráfico que sale *(egress filtering)* ayudaría a lograr un alto nivel de protección.

2.3.6. Programas CGI vulnerables

Los programas *CGI(Common Gateway Interface)* proporcionan interactividad a las páginas web, habilitando funciones como recolección de información y verificación, la mayoría de los servidores web como *IIS (Internet Information Service)* de Windows y Apache de Linux, permiten el uso de estos programas. Desafortunadamente algunos programadores de CGI´s pasan por alto el hecho de que sus programas proporcionan un vínculo directo entre cualquier usuario o intruso de internet y el Sistema Operativo en la máquina que se encuentra ejecutando el servidor web. Los programas CGI vulnerables resultan atractivos para los piratas informáticos porque son fáciles de localizar y operar con los mismos privilegios que tiene el software del servidor web, siendo así, un pirata informático puede robar información de todo tipo, instalar puertas traseras que posteriormente le servirán para tener acceso a los sistemas informáticos comprometidos. Las aplicaciones en los servidores web son igualmente vulnerables a las amenazas, los programadores deben ser cuidadosos y estar bien instruidos. Es aconsejable que los programas de ejemplo sean eliminados de los servidores web.

2.3.7. Registro de eventos (logging) incompleto o inexistente

No se puede detectar un ataque si no se sabe que está ocurriendo en la red, los registros (logs) proporcionan los detalles de lo que está ocurriendo, por ejemplo que sistemas informáticos han sido comprometidos o cuales se encuentran bajo ataque. Una de las máximas de la seguridad es, “la prevención es ideal, pero la detección es fundamental”; mientras haya flujo entre la red de datos y el internet, la posibilidad de que un pirata informático llegue silenciosamente y la vulnere está latente. Una vez que una organización ha sido atacada y no tiene registros, hay bajas posibilidades de que se descubra que hicieron realmente los atacantes; cada semana se descubren nuevas vulnerabilidades y existen muy pocas formas de defenderse de los ataques que hagan uso de las mismas. Sin la información de registro, una organización solo tiene dos elecciones, una recargar completamente el Sistema Operativo desde el soporte original y esperar a que los respaldos se encuentren en buenas condiciones, o bien arriesgarse a seguir utilizando un sistema que un atacante controla.

Se recomienda enviar todos los registros a una central que escriba la información en un soporte que sólo admita una escritura, con el fin de que un pirata informático no pueda sobrescribir los registros para evitar la detección. El registro debe ser realizado de forma regular sobre todos los sistemas informáticos clave, porque nunca se sabe cuándo se puede necesitar.[20]

[20] Subcapítulo y temas desarrollados a partir de la web: *http://www.vsantivirus.com/20vul.htm*

3. Capítulo III: Soluciones de Seguridad Informática

3.1. Requerimientos funcionales de una solución de seguridad informática

La necesidad de compartir información entre usuarios y entre organizaciones al principio fue dirigida por dos fuerzas: los laboratorios y proyectos de investigación, que ante la necesidad de colaboración necesitaron compartir información entre diferentes grupos situados en lugares lejanos, llegando a desarrollar métodos como los protocolos de red para transferir datos, como por ejemplo TCP/IP; y por otro lado están las organizaciones corporativas, que ante la necesidad de mejorar el intercambio de información entre oficinas o edificios, también aportaron al desarrollo de varios protocolos de red.

Desde que las organizaciones y usuarios comenzaron a conectarse y comunicarse por internet, han surgido problemas de seguridad informática que afecta a los recursos e información que son mantenidos en las redes de datos locales, ya que mediante estas se envía información a sitios inclusive remotos a través de la red mundial. Un sistema de seguridad informática requiere el uso de funciones específicas que permitan asegurar la confidencialidad e integridad de los recursos e información de una red de datos contra los ataques de intrusos. Mientras estas conexiones permiten el uso de muchas aplicaciones útiles y grandes oportunidades para el intercambio de información, es posible que un intruso asuma la identidad de un anfitrión confiable para la red de datos y tenga acceso a recursos e información que de otra forma no tendría. De este planteamiento surgen algunas cuestiones que deberán ser resueltas al momento de implementar una solución de seguridad informática efectiva, todo esto, previo a la elección de las tecnologías a utilizar.

En respuesta a estos riesgos, una industria completa se ha formado para responder a las necesidades de las organizaciones que quieren tener las ventajas y los beneficios de conectarse a internet pero que requieren mantener la confidencialidad, integridad y disponibilidad de la información y los recursos

de la red de datos, esta industria se mueve alrededor de la tecnología firewall, así como en el manejo de ruteadores y puertas de enlace *(gateways)* para la transmisión de datos.

El objetivo de una solución de seguridad informática es aislar el segmento de la red de datos local del resto de internet y controlar el tráfico que entra y sale de ella, pero hay que tomar en cuenta un par de factores importantes:

¿Cuánta seguridad se puede afrontar? Es decir, el costo que una organización estaría dispuesta a cubrir, esto se relaciona en cierta forma con qué tan apetecidos pueden llegar a ser los recursos de red y la información de la organización para un posible intruso, aunque esto es un asunto muy relativo; también se debe considerar la conveniencia de una solución de seguridad informática y cómo afecta al desempeño del servicio brindado a los usuarios de una red de datos.

Lo anterior se debe armonizar en que la protección de una red de datos contra amenazas no puede ser lograda por una sola tecnología o servicio, por lo que es necesario diseñar una estrategia balanceada que permita proteger los puntos débiles en la seguridad. Si además se comprende los mecanismos que se siguen en las conexiones en red y se mantiene actualizados los Sistemas Operativos y el software de aplicación, se puede tener un nivel de seguridad informática y una funcionalidad aceptables.

3.2. Sistemas para soluciones de seguridad informática

Después de haber decidido una estrategia de seguridad informática, y en función de ella una política de seguridad informática para una red de datos, es lógico y necesario llevar estás especificaciones a la implementación, tales implementaciones corresponden a las soluciones de seguridad informática.

3.2.1. Cortafuegos

Un cortafuegos, también conocido como *firewall*, es un sistema o grupo de sistemas que combina diferentes componentes, tanto dispositivos físicos (hardware) como programas (software) y actividades de administración, para llevar a cabo una política de seguridad informática y así proveer un punto de defensa entre una red de datos local y el internet. Un cortafuegos está diseñado para prevenir el acceso no autorizado de usuarios del internet hacia redes de datos conectadas al internet, sobre todo a las intranets, el principio fundamental de este postulado es que no todos los usuarios de internet mantienen actividades legales, además un cortafuegos también sirve para evitar que los propios usuarios internos de una organización no comprometan la seguridad de la red de datos al enviar contraseñas no encriptadas o datos sensitivos hacia la red pública. La función de un cortafuegos es tal que todo el tráfico de entrada y salida de la red de datos debe pasar a través de él, el tráfico permitido es autorizado mediante una evaluación a base de una política de seguridad informática.

El enfoque de los cortafuegos está basado en el concepto de permitir a los usuarios locales el uso de todos los servicios de la red de datos local, así como los servicios ofrecidos por el internet, y a la vez controlando y reduciendo considerablemente el acceso de posibles intrusos a la información y recursos de la red de datos.

Si el cortafuegos detecta alguna actividad sospechosa, como que alguien de fuera esté intentando acceder a una red de datos o que algún programa espía trate de enviar información sin consentimiento, el cortafuegos advertirá con una alarma en el sistema y bloqueará el tráfico potencialmente peligroso antes de que alcance otras partes de la red de datos, generalmente se efectúan registros de estas actividades. La determinación de que es peligroso para la red de datos local, es especificada en la política de seguridad informática adoptada.

Entre los principales objetivos de un cortafuegos para proteger la red de datos están:

a. Bloquear el tráfico no deseado.
b. Redireccionar el tráfico de entrada a sistemas internos de más confianza.
c. Ocultar de internet sistemas vulnerables que puedan ser asegurados.
d. Restricción de entrada de usuarios internos y externos a servicios y puntos cuidadosamente controlados de la red de datos local.
e. Registrar el tráfico desde y hacia la red de datos local.
f. Prevención ante los intrusos que tratan de ganar espacio hacia el interior de la red de datos y demás sistemas de defensa establecidos.
g. Ocultar de internet información como nombres de sistemas informáticos, topología de red, tipos de dispositivos de red e identificadores de usuarios internos.
h. Proveer autenticación más robusta que las aplicaciones estándares.

El control de acceso que ofrece un cortafuegos a una red de datos, permite que algunos servidores puedan hacerse disponibles desde el internet, mientras que otros son cerrados del acceso externo no deseado, previniendo de esta forma que los servicios vulnerables sean explotados por piratas informáticos, es posible que el uso de estos servicios son un riesgo reducido de exposición debido a que solo algunos protocolos seleccionados serán capaces de pasar a través del cortafuegos, sin embargo como repuesta a esto se puede realizar una inspección de contenido en el tráfico HTTP y SMTP incluyendo otros elementos.

3.2.1.1. Beneficios de los Cortafuegos

a. Permite la interconexión segura de una red de datos local con internet para aprovechar los servicios que este ofrece.

b. Administra los accesos posibles del internet a la red de datos local.

c. Protege a los servidores propios del sistema informático de ataques de piratas informáticos desde el internet.

d. Reduce costos si todo el software de seguridad es situado en un único sistema cortafuegos, en lugar de ser distribuido en cada servidor o máquina de la red de datos local.

e. Ofrece un punto donde la seguridad puede ser monitoreada, permitiendo al administrador de la red de datos definir un *choke point* o embudo, para mantener al margen a los usuarios no autorizados.

f. Es ideal para desplegar servidores Web y FTP cuando se quiere ofrecer un punto de reunión para la organización como por ejemplo entregar servicios de información a los consumidores y a los mismos usuarios de la red de datos local.

3.2.1.2. Limitaciones de los cortafuegos

a. No puede proteger contra las amenazas provenientes de puntos de acceso alternativos no previstos y ataques originados desde el interior de la red de datos.

b. No puede ofrecer protección una vez que un intruso los traspasa o permanece en torno a este.

c. Limitan el acceso desde y hacia el internet, pero es un precio que hay que pagar debido a que es una cuestión de análisis de costo/beneficio.

d. No puede impedir que traidores o espías corporativos copien datos sensitivos y los extraigan de la organización.

e. No puede proteger contra los ataques de ingeniería social.

f. No puede proteger contra posibles ataques a la red de datos local por amenazas programadas como virus a través de archivos o software, no al menos si alguna amenaza de este tipo se introdujo por medio de un dispositivo externo conectado a alguna máquina de la red datos, si el ataque es desde el internet hay la posibilidad de que en el filtrado de paquetes se bloquee este tipo de ataques.

3.2.1.3. Política de diseño de los Cortafuegos

La política de diseño es específica de cada cortafuegos. Aquí se define las reglas utilizadas para implementar la política de acceso a los servicios de red; se debe diseñar en relación a, y con conocimiento de características como son las limitaciones y capacidades del cortafuegos y tomando en cuenta la política interna propia de la organización para la seguridad total, junto a las amenazas y vulnerabilidades asociadas con las tecnologías utilizadas como TCP/IP, las políticas principales que generalmente implementan los cortafuegos son dos:

a. Permitir todo servicio, a menos que sea expresamente denegado.
b. Denegar todo servicio, a menos que sea expresamente permitido.

La primera política es la menos deseable, debido a que ofrece más vías por las cuales se puede acceder a un servicio, evadiendo al cortafuegos, mientras que la segunda es más fuerte y segura, aunque es más restrictiva para los usuarios, está política es la más utilizada en seguridad informática. Por lo tanto dependiendo de los requerimientos de seguridad y flexibilidad, ciertos tipos de cortafuegos son más apropiados que otros, o ciertos tipos de configuraciones en un mismo cortafuegos sean más apropiadas que otras; por eso es muy importante que la política de diseño sea considerada antes de implementar un cortafuegos, de lo contrario el mismo podría no cubrir las funcionalidades esperadas.

Dentro de una organización, un cortafuegos no está solo, es parte de la política de seguridad informática total de una organización, para que esta tenga éxito la organización debe conocer que es lo que está protegiendo.

Dentro de la política de diseño se debe tomar en cuenta el costo de los componentes o la construcción de secciones para implementar una solución cortafuegos, a lo que debe llevar esto es a establecer un correcto equilibrio costo/beneficio que satisfaga las necesidades de la organización. Dentro del costo/beneficio se debe contemplar que el cortafuegos requiere un soporte continuo para su mantenimiento, administración y actualización de software.

Gráfico 3.1. Diseño general de una solución cortafuegos.

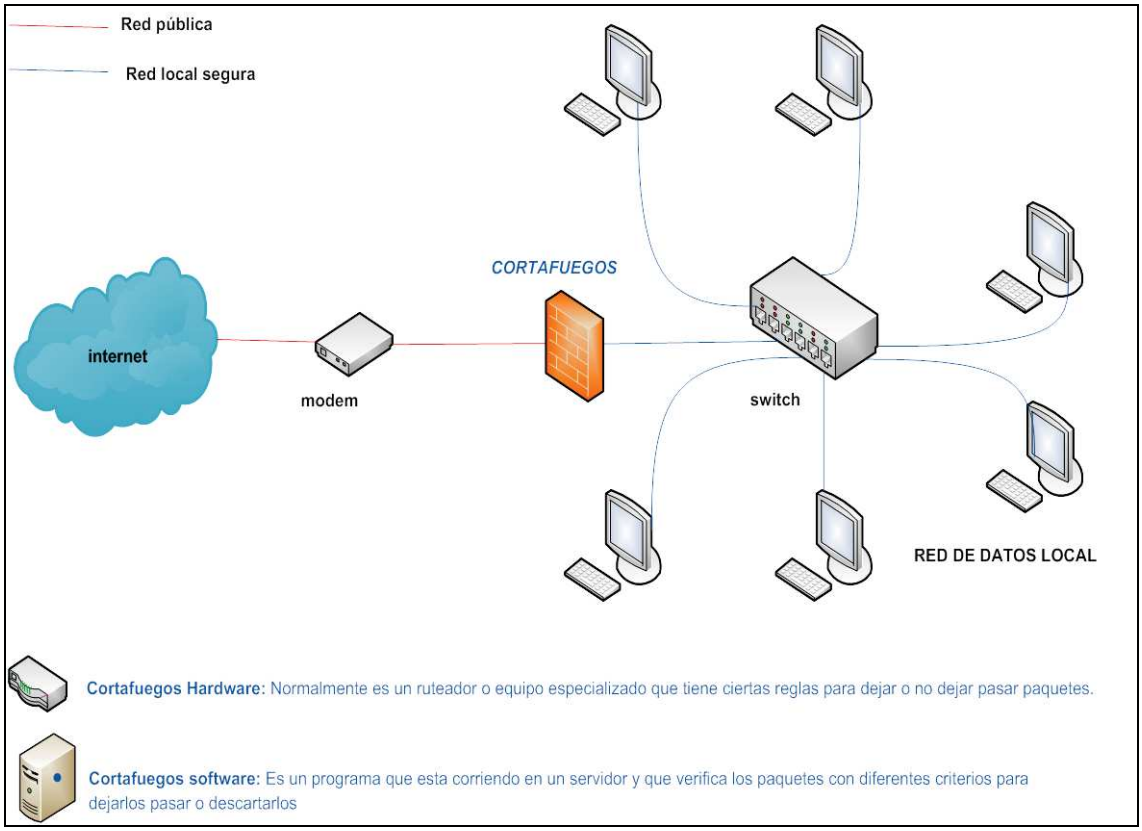


Gráfico realizado por Marco Castillo, autor del presente trabajo.

3.2.1.4. Estrategia e implementación de un cortafuegos

Debido a que todo el tráfico puede pasar por un cortafuegos, se puede considerar como el foco de todas las decisiones de seguridad. Concentrando las defensas en este punto, se reduce la sobrecarga de seguridad del sistema informático interno debido a que el esfuerzo se limita a unos pocos dispositivos que forman parte del cortafuegos en la red de datos. Así, el control de acceso es centralizado, los usuarios remotos pueden acceder a la red de datos local de forma controlada y segura, pasando a través del cortafuegos.

Es recomendable que un cortafuegos sea transparente a los usuarios para que no adviertan su existencia para poder acceder a la red de datos local; los cortafuegos suelen ser configurados para ser transparentes para los usuarios de la red interna, mientras que para los usuarios de la red externa, no.

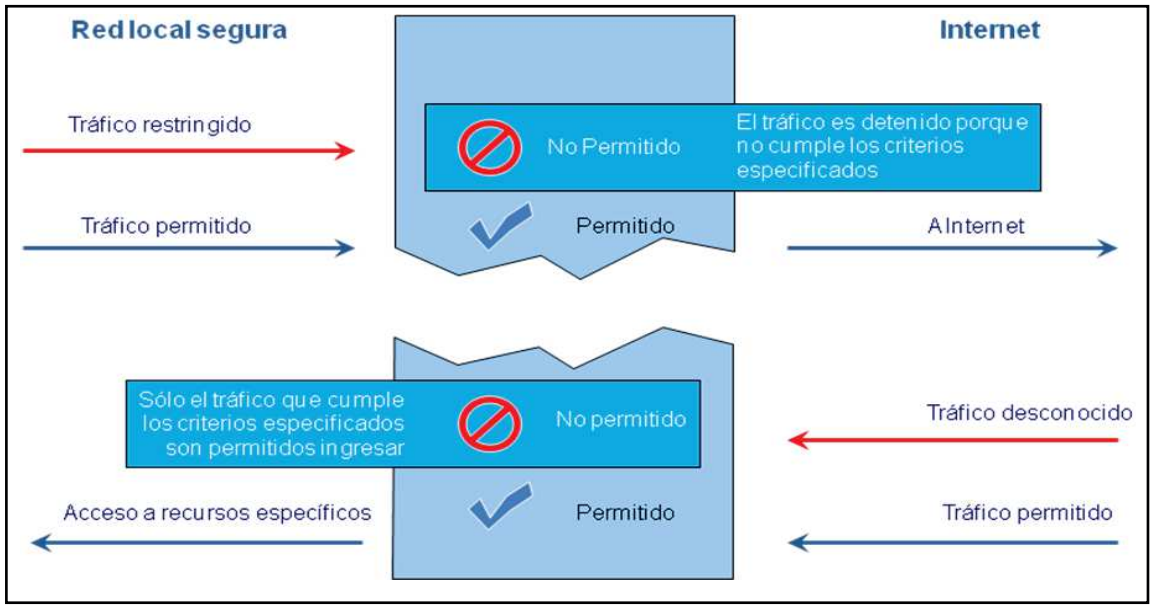
Es posible utilizar diferentes enfoques de implementación de cortafuegos para diferentes topologías de interconexión de redes, pero en cada caso, cada conexión (punto de acceso) de la red de datos local a internet estará equipada con un cortafuegos. Se vuelve a poner énfasis en que antes de definir qué tipo de cortafuegos se ajusta a las necesidades de la red de datos, primero se necesita analizar la topología de red para determinar si los componentes tales como switches, ruteadores y cableado son apropiados para un modelo de cortafuegos hardware específico, e incluso para una solución de software corporativo.

La red debe ser analizada a base de las diferentes capas del modelo OSI *(ver Anexo 3)*, un cortafuegos pasa a través de todas estas capas y actúa en aquellas responsables del envío de paquetes, establecimiento y control de la conexión y del procesamiento de las aplicaciones, por eso con un cortafuegos se puede controlar el flujo de información durante el establecimiento de sesiones, inclusive determinando que operaciones serán o no permitidas.

3.2.1.5. Fundamento y funcionamiento de los cortafuegos

Muchas organizaciones dependen de internet para publicitar sus productos y servicios, por lo que es necesario proteger los datos y transacciones de cualquier incidente, ya sea causado por actos maliciosos o no intencionales. Un cortafuegos no es una solución definitiva de seguridad informática, sin embargo da una respuesta al problema de ingeniería: configurar un gran número de sistemas de anfitriones para una buena seguridad, un cortafuego por sí solo no asegura una red, más bien es parte de un área más amplia dedicada a proteger un sitio y efectuar operaciones de red.

Esquema 3.1. Operación general de un cortafuegos.[21]



En un cortafuegos la decisión de filtrado de paquetes se lleva a cabo de acuerdo a un *ACL (Access Control List – Lista de Control de Acceso)* asociada a cada interfaz física por la cual se recibe el paquete; cada entrada de esta lista especifica valores para campos particulares de los encabezados del paquete, y acciones a ser tomadas si el paquete coincide con esos valores.

[21] Esquema obtenido y modificado de las diapositivas DEC Seguridad y VPN, Certificación D-Link, diapositiva 26.

Las tareas de inspección de un cortafuegos se realizan previamente a que el paquete alcance la capa de red. Los paquetes analizados por un cortafuegos corresponden al encabezado IP y de los protocolos de transporte TCP y UDP, los campos generalmente analizados son:

a. **Dirección IP origen y destino.-**Basándose en las direcciones IP, el cortafuegos es capaz de bloquear el acceso desde o hacia algún sitio o anfitrión no confiable.

b. **Tipo de protocolo.-**Indica si los datos encapsulados corresponden a TCP, UDP o ICMP.

c. **Puerto TCP o UDP de origen y destino.-**El cortafuegos hace uso de los puertos bien conocidos de TCP para permitir, denegar o encaminar el acceso a servicios de internet particulares; por ejemplo podría encaminar todo el tráfico web, cuyo puerto por defecto es el 80, a un anfitrión particular como un servidor web.

d. **Bit ACK.-**Indica si un paquete es una confirmación de un paquete TCP recibido.

3.2.1.6. Servicios adicionales proporcionados por los cortafuegos

Estos servicios son un valor agregado de los cortafuegos, los cuales facilitan las labores de protección y administración de la red de datos. Según el modelo y lo robusto que sea un cortafuegos estos servicios estarán disponibles en su totalidad o solo algunos de ellos; estos servicios también son parte importante a la hora de decidir por una solución e implementación.

a. **NAT.-**Los servicios de *NAT (Network Address Translation – Traducción de Direcciones de Red)* resuelven 2 problemas principales de seguridad e infraestructura de las redes de datos. Son una herramienta efectiva para esconder las direcciones de red reales de una red de datos local. También,

debido a la reducción al espacio de direcciones IPv4 disponibles, varias organizaciones usan NAT para permitir la navegación en internet de sus equipos de la red de datos local con pocas IP´s legalmente válidas *(RFC 1918),* así mismo en algunos países ya se empezó a trabajar con IPv6. Un cortafuegos que cumpla la función de NAT puede proveer filtrado y registro de tráfico para llevar un control de las comunicaciones que se lleven a cabo.

En NAT es posible hacer la traducción de red estática, en este sistema cada sistema interno de la red de datos local tiene su propia dirección IP exterior, con esto se logra esconder el esquema interno de la red de datos, más no la reducción de direcciones IP´s válidas para acceder al exterior, los cortafuegos que incluyen esta característica usan una tabla de correspondencia entre unas direcciones y otras.

En NAT también es posible hacer la traducción de puertos (PAT), con esto no es necesario usar la dirección externa del cortafuegos, sino que se puede crear otra dirección virtual para este propósito. El cortafuegos usa el puerto del cliente para identificar cada conexión entrante y constituye para tal efecto una tabla de traducciones; la traducción de puertos se realiza de forma secuencial o aleatoria dentro de un rango de puertos válidos. Este sistema es flexible, seguro y por lo tanto el más conveniente y usado. Un NAT dinámico ofrece un importante servicio de seguridad, debido a que solo son permitidas aquellas conexiones que se originen en la red de datos local, es decir que una computadora externa no puede iniciar un contacto a menos que un anfitrión de la red de datos local haya iniciado la comunicación, de lo contrario es rechazada por el cortafuegos.

b. DHCP.- *DHCP (Dynamic Hosts Configuration Protocol - Protocolo de Configuración Dinámica de Servidor*), es un servicio de asignación automática de direcciones IP con importantes y evidentes ventajas administrativas para mantener redes de datos pequeñas, medianas y

grandes, muchos cortafuegos, sobre todo los que trabajan en las capas 2, 3, 4 incluyen DHCP como valor agregado

c. **Administrador de ancho de banda.-** Es un servicio de valor agregado de los cortafuegos, el cual se emplaza en la red de datos local y la salida a internet, haciendo el papel de guardia de tráfico, mediante reglas se definen distintas colas, cada una de las cuales alberga un tipo distinto de tráfico como transferencia de ficheros, correos-e, video, audio, tráfico HTTP, etc. Cada cola de tráfico posee una prioridad distinta, de manera que se puede poner en primera prioridad a aquellas que correspondan al tráfico más crítico para una organización. El administrador de ancho de banda realiza la distinción entre los distintos tipos de tráfico, inspeccionando directamente las cabeceras para buscar identificar un determinado protocolo en función de los puertos a los que son dirigidos los paquetes, aunque a veces esto no es suficiente. Es posible que un sistema de ficheros use el puerto 80 para asemejar tráfico web, de igual forma es posible que un sistema use más de un puerto simultáneamente, también se pueden usar métodos similares a los de los antivirus y buscar patrones que identifiquen tráfico.

d. **Inspección de contenido.-** Es un servicio de valor agregado muy interesante, este servicio permite realizar una inspección de contenidos en el tráfico HTTP, SMTP, incluyendo los siguientes elementos: applets de java, ActiveX, java script, CGI, inspección de contenido de ciertos formatos, bloqueo de contenidos a base de URL´s y/o palabras clave, bloqueo de comandos específicos de determinadas aplicaciones

e. **Autenticación de usuarios.-** Es un servicio de valor agregado en el que se puede habilitar servicios de combinación usuario/contraseña.

f. **Alta disponibilidad.-** Es un servicio de valor agregado que ofrece redundancia mediante el balanceo de carga entre 2 o más dispositivos

cortafuegos, con esto se consigue mejorar el problema del rendimiento, además se ofrece alta disponibilidad y tolerancia a fallos en la política de seguridad informática.

g. IDS.- Un *IDS (Intrusion Detection System – Sistema de Detección de Intrusos)* es un sistema de valor agregado que ofrece herramientas o dispositivos que permiten inspeccionar la red de datos y generar alertas para conocer cuando alguien ha tratado de penetrar en la red de datos o lo ha conseguido, hay dos tipos de sistemas IDS, los de anfitrión que se basan en el análisis de las estadísticas del uso o el uso indebido de los recursos; los de red (distribuidos y no distribuidos) que buscan patrones sospechosos o mal formaciones en la estructura de los paquetes TCP/IP. Los IDS poseen tablas actualizables con los patrones característicos usados para entrar a una red de datos.

h. DMZ.- Llamada también zona desmilitarizada o subred protegida, es un sistema de valor agregado que se implementa en el caso de tener servidores con acceso a internet, la DMZ es un puerto adicional del cortafuegos, el mismo software del cortafuegos permite poner a los servidores fuera de la red de datos local mediante la misma DMZ, por lo tanto la LAN y la DMZ son subredes diferentes. La arquitectura DMZ permite aislar a los servidores de la red de datos interna para asegurar su integridad así como para protegerlos de posibles ataques provenientes del Internet. [22]

[22] Tema, y subtemas desarrollados a partir de las siguientes fuentes:
http://www.textoscientificos.com/redes/firewalls-distribuidos/firewalls
Diapositivas: Firewall, autor: Ing. Henry Burbano
DEC Seguridad Internet y VPN, pág. 41-44, Certificación D-Link.

Gráfico 3.2. DMZ.

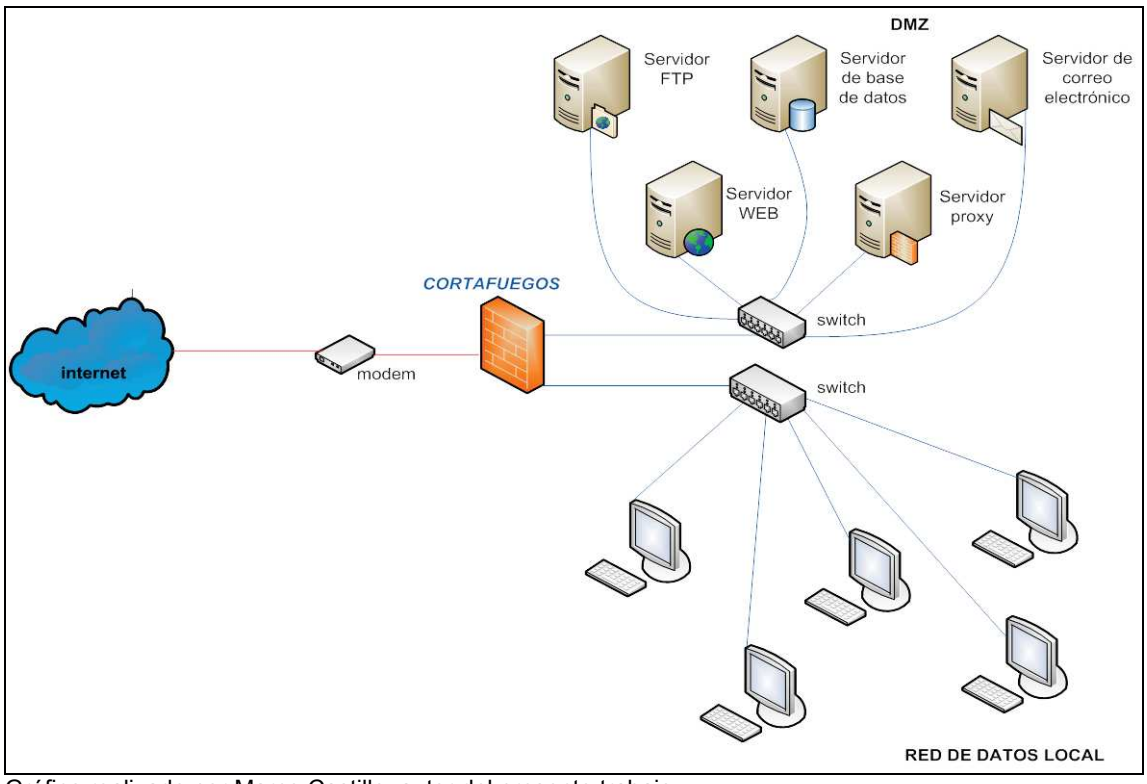


Gráfico realizado por Marco Castillo, autor del presente trabajo.

3.2.2. Tipos de cortafuegos y sus soluciones

Los cortafuegos se pueden configurar de diferentes formas, utilizando diferentes componentes, logrando varios niveles de seguridad a diferentes costos de instalación y mantenimiento, esto dependerá de las necesidades de la organización y de la evaluación de costo/beneficio de llevar a cabo la implementación.

3.2.2.1. Cortafuegos convencionales

También llamados cortafuegos perimetrales. En este tipo de cortafuegos existen diversas arquitecturas que permiten cubrir las necesidades básicas de una organización que desee proteger su red de datos local de los ataques provenientes de internet. Por ejemplo una de las variantes es utilizar más de un

anfitrión bastión ya sea para mejorar el desempeño de los servicios de la red de datos ampliando la capacidad de procesamiento de distintos servicios, aumentar redundancia para obtener un soporte de apoyo, sea de servicios o información, o separar servicios por razones de seguridad.

Los cortafuegos convencionales son útiles para proveer alguna medida de seguridad debido a que proveen mecanismos para aplicar ciertas políticas de seguridad informática; son el único mecanismo de seguridad aplicable a sistemas *legacy,* debido a que estos utilizan protocolos viejos y difíciles de proteger.

Adicionalmente, muchos protocolos no poseen características que permitan implementar aspectos de seguridad informática global, para estos casos los cortafuegos convencionales son la solución ya que proveen una barrera como primera medida de protección

También se puede crear una red perimetral utilizando un solo cortafuegos que cumpla las funciones de un cortafuegos externo y otro interno, para esto el cortafuegos debe ser suficientemente capaz de procesar todo el tráfico que reciba, esta configuración tiene la desventaja de que existe un único punto de falla.

El anfitrión bastión puede ser utilizado como cortafuegos externo si se conecta a 2 redes de datos a través de 2 interfaces de red, así el filtrado de paquetes y los servicios proxy son ejecutados en el mismo anfitrión, esto implica un costo en el desempeño de estos servicios, aunque las tareas de filtrado de un cortafuegos externo son mínimas; en esta configuración la única vulnerabilidad es que el anfitrión bastión queda más expuesto, por lo que deben considerarse medidas de seguridad mayores para dicho anfitrión. Otra alternativa sería utilizar un anfitrión con dos interfaces de red para actuar como bastión y cortafuegos interno, pero de esta forma se está eliminando el nivel de seguridad provisto por el cortafuegos interno si los niveles de seguridad más expuestos fallan.

Si la red de datos local se conectará a más de un red externa, puede utilizarse para cada una un cortafuegos externo distinto, de esta forma se mantendrá el desempeño de cada cortafuegos, agregando conectividad.

Si la red de datos local es de una dimensión importante, tal que pueda sobrecargar el cortafuegos interno, es posible utilizar múltiples cortafuegos conectados a 2 subredes, o sea, a segmentos diferentes correspondientes a la red de datos local.

Los cortafuegos convencionales son muy apropiados para proteger la red de datos de ataques de infraestructura, aunque todo depende de la arquitectura de implementación. La protección contra ataques de denegación de servicio es más efectiva en los puntos de acceso a la red de datos, lo que es un atributo importantísimo de estos cortafuegos. La efectividad de los cortafuegos convencionales también es altamente valorada para la detección de intrusos.

Sin embargo los cortafuegos tradicionales se basan en un dispositivo de interconexión de redes con un desempeño de transmisión de datos limitado, por lo que es un factor determinante en el desempeño de la red de datos y su posible expansión. Los cortafuegos convencionales causan una degradación en el desempeño si se excede su capacidad de procesamiento de paquetes por segundo, esto va contra los objetivos de toda organización que depende de la interacción con sus usuarios y otras organizaciones a través de internet.

El modelo planteado por este enfoque convencional funciona bien para redes pequeñas o medianas, pero no es aplicable bajo ciertas condiciones, como líneas de alta velocidad, extranets entre otras.

3.2.2.2. Servidor proxy

Un servidor proxy, también llamado servidor intermediario, es una aplicación situada entre una aplicación cliente y un servidor real y se define como un software de aplicación o dispositivo que ofrece un servicio de red, esto consiste

en permitir a los clientes realizar conexiones de red indirectas hacia otros servicios de red. Durante el proceso ocurre lo siguiente:

a. El cliente se conecta con el servidor proxy.
b. El cliente solicita una conexión a un recurso disponible en un servidor real
c. El servidor proxy proporciona el recurso ya sea conectándose hacia el servidor real especificado o sirviendo este desde un cache, con información previamente obtenida del servidor real.
d. El ciertos casos el servidor proxy puede alterar la solicitud del cliente o bien la respuesta del servidor real para diversos propósitos.

Generalmente un servidor proxy se lo hace trabajar como un cortafuegos operando en el nivel de red, actuando como filtro de paquetes, como son las *iptables*, o bien operando en el nivel de aplicación, controlando diversos servicios, como es el caso de *TCP Wrappers.* Dependiendo del contexto el cortafuegos se conoce también como *BPD (Border Protection Device)* o simplemente filtro de paquetes. De esta manera al actuar como cortafuegos, verifica si tales solicitudes o mensajes son permitidos y los rechaza en caso de que así se lo determine en función de las reglas que se hayan impuesto. También pueden mejorar en gran medida el desempeño de la red de datos para un grupo de usuarios ya que ahorra la obtención de los resultados, que son las consultas al servidor real, de todas las solicitudes para una cierta cantidad de tiempo. Otra ventaja de estos sistemas es el permitir monitorear y controlar toda la actividad de la red de datos que involucre comunicación con el exterior o en ambas direcciones, por ejemplo:

a. Comunicación cliente externo-servidor proxy.-Los anfitriones externos no deberán conocer la topología de red, así como tampoco las direcciones IP y los nombres de las máquinas conectadas a las red de datos local; solo deben conocer la dirección del sitio correspondiente al anfitrión que interconecta la red de datos local al internet, que será el responsable de

redirigir los paquetes al servidor proxy. Si el anfitrión externo conoce la dirección del servidor proxy, puede intentar contactarlo y acceder a la red de datos local, para prevenir esto se dispone de dispositivos de seguridad en el mismo servidor proxy para evitar cualquier intento de acceso no permitido.

b. **Comunicación cliente interno-servidor proxy.-** De igual forma que en el caso anterior, se evita la conexión directa entre el cliente de la red de datos local y el servidor real, para esto existen 2 tecnologías proxies: clásica y transparente. En la tecnología proxy clásica, se modifica el software cliente y se instruye al usuario efectuar procedimientos especiales para contactar al servidor real a través del servidor proxy. En la tecnología proxy transparente, se configura las tablas de enrutamiento de la red de datos local para que todos los paquetes destinados a un servidor externo sean redirigidos al servidor proxy que sabrá interceptar los paquetes y crear ambas conexiones.

   Los servidores proxies comprenden la sintaxis de un protocolo pero no implementan ninguna de sus funcionalidades, simplemente verifican que un mensaje proveniente de un anfitrión externo es apropiado, luego lo envía al sistema encargado de procesar los datos, o sea al servidor real al cual estaba dirigido el mensaje.
   Una aplicación común de los servidores proxies es funcionar como caché de contenido de red, principalmente HTTP, proporcionando a los clientes un caché de páginas y ficheros disponibles a través de la red de servidores HTTP reales, permitiendo a los usuarios de la red de datos local acceder a estos de forma más rápida y confiable. Cuando se recibe una petición para un recurso de red especificado en un URL, el servidor proxy busca el resultado del URL dentro del caché, si este es encontrado, el servidor proxy responde al cliente proporcionando inmediatamente el contenido solicitado, si el contenido seleccionado no estuviera en el caché, el servidor proxy lo traerá desde el servidor real, entregándolo al cliente que lo solicitó y

guardando una copia en el caché, el contenido en el caché es eliminado de acuerdo a la antigüedad, tamaño e historial de respuestas *(hits)*, como por ejemplo: LRU, LFUDA y GDSFdel servidor proxy de Linux, *Squid,* el cual se lo tratara como parte de un capitulo posterior. Un servidor proxy para contenido de red (web proxy) también puede funcionar como filtro de contenido, aplicando políticas de censura de acuerdo a criterios establecidos o arbitrarios.

3.2.2.3. Filtros de paquetes

Esta tecnología de cortafuegos analiza el tráfico de la red de datos basándose en los datos de los encabezados de los paquetes TCP/IP, cada paquete que entra o sale de la red de datos es inspeccionado de acuerdo a reglas que deniegan o aceptan los paquetes llamadas Lista de Control de Acceso (ACL). Básicamente los datos analizados son las direcciones IP y puertos TCP de origen y destino de los paquetes. El filtrado de paquetes es efectivo y transparente para los usuarios de la red. El tráfico desconocido sólo se permite hasta el nivel 3 del modelo TCP/IP *(ver Anexo 3).*

Los filtros son programas o dispositivos que generalmente se encuentran situados en los sistemas que proveen conectividad entre redes de datos, es decir los puntos de acceso. Las reglas para aceptar o rechazar un paquete son las siguientes:

a. Si no se encuentra una regla que aplicar, el paquete es rechazado.
b. Si se encuentra una regla que aplicar al paquete, y la regla permite el paso, se establece la conexión.
c. Si se encuentra una regla que aplicar al paquete, y la regla deniega el paso, no hay conexión.

Con la utilización de un filtro es posible restringir toda comunicación con ciertos sitios de internet para evitar comportamientos indeseados en los sistemas finales de la red de datos local, también se puede restringir todas las comunicaciones entrantes a ciertos servicios de la red para evitar el acceso a

recursos privados, además se puede habilitar alarmas o avisos que advierten que paquetes entran, salen o son rechazados.

3.2.2.4. Cortafuegos a nivel de circuito

Esta tecnología de cortafuegos valida que los paquetes pertenezcan ya sea a una solicitud de conexión o bien a una conexión entre 2 puntos, de acuerdo a un determinado conjunto de reglas, manteniendo el estado a lo largo de la transmisión, agrupando los paquetes que pertenecen a la misma conexión, además aplica mecanismos de seguridad cuando una conexión TCP o UDP es establecida, una vez que la conexión se establece los paquetes pueden ir y venir entre los 2 puntos sin necesitar ser revisados cada vez. Este tipo de cortafuegos son aplicaciones proxy que pueden estar presentes en la red de datos, los anfitriones de la red local no podrán establecer conexiones directas a destinos situados en el internet sino a través del proxy. El tráfico desconocido sólo se permite hasta el nivel 4 del modelo TCP/IP.

El cortafuegos mantiene reglas de conexiones válidas y permiten que los paquetes de la red pasen a través de ella si corresponden a algún registro de las reglas; una vez terminada la conexión las reglas se borraran y la transmisión de información entre dos puntos se cierra.

3.2.2.5. Cortafuegos a nivel de aplicación

Esta tecnología de cortafuegos examina la información de todos los paquetes de la red de datos y mantiene el estado de la conexión y la secuencia de la información, también se puede validar claves de acceso y algunos tipos de solicitudes de servicios, por lo que son aplicaciones específicas para aplicaciones y servidores de propósito especial que se ejecutan en un anfitrión para formar parte de un cortafuego; es posible extender el control de acceso del tráfico de red a las capas de aplicación, son también llamados aplicaciones o servidores proxies; debido a que toda la información entre el cliente y el servidor son ruteados a través del proxy de aplicación, además de controlar la

sesión, puede proveer funciones de registro de sucesos detalladas. El tráfico desconocido solo se permite hasta el nivel 5 del modelo TCP/IP.

Un servicio proxy es un programa especializado que aplica mecanismos de seguridad a ciertas aplicaciones, tales como HTTP o FTP; un servicio proxy incrementa el control de acceso, realiza chequeos detallados a los datos y genera auditorias sobre la información que se transmite.

3.2.2.6. Cortafuegos de inspección del estado completo de multicapas

También conocido como *Statefull Multilayer Inspección Firewall*, esta tecnología permite modificaciones a las reglas de seguridad sobre la marcha, suelen utilizarse dos o más técnicas para configurar el cortafuegos. El tráfico es filtrado en los niveles 3, 4 ,5 del modelo TCP/IP de acuerdo a un amplio rango de reglas de aplicaciones, sesiones y filtros de paquetes específicos: el tráfico desconocido solo se permite hasta el nivel 3 del modelo TCP/IP.

3.2.2.7. Cortafuegos distribuidos

Estos cortafuegos son aplicaciones de software de seguridad situados en los sistemas finales críticos de una red de datos, sean los servidores o las computadoras de los usuarios, con el fin de proteger contra posibles ataques desde el internet; las tareas de monitoreo y administración son hechas de forma central e integrada, con lo que se consigue optimización de recursos y practicidad. La diferencia principal con los cortafuegos tradicionales es el sitio en la red de datos donde se efectúa la aplicación de las soluciones de seguridad debido a que las soluciones tradicionales se sitúan en los puntos de acceso a la red de datos, mientras que las soluciones distribuidas se aplican en los sistemas finales que componen la red de datos. Los cortafuegos distribuidos funcionan en *modo kernel* [23] en el Sistema Operativo de cada anfitrión.

Los cortafuegos distribuidos están basados en la misma tecnología que los cortafuegos personales, pero están enfocados al mercado corporativo, debido a

[23] El modo kernel proporciona acceso directo a la memoria y se ejecuta en un área aislada de la misma.

que permiten integrar una solución distribuida. Estos cortafuegos ofrecen ventajas importantes: administración central, registro y control de acceso, estas características son importante y necesarias para la implementación de políticas de seguridad de forma uniforme e integrada en redes de datos de grandes organizaciones. Los cortafuegos distribuidos pueden ser aplicados en varios aspectos como por ejemplo:

a. Proteger a los servidores de infraestructura e información contra ataques desde e internet.
b. Ocultar la información y las aplicaciones del acceso no autorizado.
c. Fortalecer sistemas finales críticos.

Estos cortafuegos proveen una capa adicional de defensa para servidores localizados detrás de un cortafuegos convencional y también protege los servidores expuestos directamente al internet.

Básicamente, la instalación de un cortafuego distribuido consiste en la instalación del mecanismo de aplicación de la política de seguridad informática esta tarea es relativamente simple, similar a la de cualquier producto de software. También se instalará el módulo de administración central en una de las máquinas de la red de datos local.

Una ventaja de los cortafuegos distribuidos con respecto a los cortafuegos tradicionales es que al ser residentes de los sistemas finales, pueden filtrar el tráfico proveniente tanto del internet como de la red de datos local, debido a que se ha movido el punto de control de acceso del perímetro a cada anfitrión de la red de datos; por lo tanto el concepto de red no confiable se extiende a aquellos anfitriones situados en la red de datos local, para responder a la necesidad de ofrecer una protección contra uno de los ataques más comunes: aquellos que provienen de la red de datos interna, sean accidentales o intencionales.

Con un cortafuegos distribuido se incrementa la seguridad a través de la simplificación, diseñando reglas específicas para cada sistema, se logra una protección altamente especializada y su aplicación involucra solo a aquellos anfitriones relacionados con determinado tipo de protocolos con el que trabajen.

Debido a que los cortafuegos distribuidos son sistemas de software, pueden ser desplegados sobre una arquitectura de red existente, por lo tanto el costo de instalación en tiempo y dificultad es relativamente bajo, ya que no requiere una reconexión de la red de datos y consecuentemente no hay interrupción de las aplicaciones que están en ejecución.

Los cortafuegos distribuidos pueden mantener el desempeño de las comunicaciones y, el hecho de ser desplegados en servidores críticos para suplementar a un cortafuego convencional, aportando una solución de seguridad de múltiples niveles, sin un único punto de falla. Por ejemplo los cortafuegos distribuidos pueden ser desplegados junto a un cortafuego convencional en una DMZ, para proteger de forma individual a los anfitriones bastiones conectados a la misma. Esta arquitectura permite aislar a los servidores de la red de datos local para asegurar su integridad, así como proteger de posibles ataques provenientes del internet.

La arquitectura de los cortafuegos distribuidos provee un alto grado de flexibilidad para ambientes de negocios sobre internet debido a que no dependen de un único punto de acceso y realizan las funciones normales sin degradar los servicios de la red de datos, esta flexibilidad permite cubrir las diversas necesidades de los clientes de la misma.

Los cortafuegos distribuidos pueden solucionar ciertas limitaciones de los cortafuegos convencionales, bajo este nuevo modelo parte de la política de

seguridad informática es definida centralmente y distribuida a cada sistema final de forma independiente para su aplicación.[24]

3.2.3 Criptografía

La criptografía es cifrar o encriptar la información mediante mecanismos y claves para modificar un mensaje que se transmite de un extremo a otro, de tal forma que no sea comprensible directamente, de esta manera solo quienes establezcan una comunicación encriptada puedan tener acceso a la información original. La criptografía se asegura que solo el receptor deseado sea capaz de leer el mensaje recibido aplicando el proceso inverso de encriptación.

Así, dos sistemas finales como son un emisor y un receptor, que establezcan una comunicación con información encriptada a través de internet, reducirán el riesgo de que la información sea expuesta a entidades no deseables, de esta manera quien llegase a interceptar un mensaje encriptado no será capaz de saber qué es lo que tiene en su poder. Un mecanismo de encriptación consiste en una operación o algoritmo que utiliza una llave (clave) para transformar un mensaje de su formato original (interceptado como texto plano) a un mensaje encriptado (texto cifrado).

La criptografía ofrece otra funcionalidad como es la *autenticación*. ¿Se sabe con quién se comunica en internet? ¿Es confiable la otra parte? La criptografía agrega a las comunicaciones sobre internet un rasgo de seguridad muy

[24] Tema, y subtemas desarrollados a partir de las siguientes fuentes:
http://www.textoscientificos.com/redes/firewalls-distribuidos/firewalls
Diapositivas: Firewall, autor: Ing. Henry Burbano
DEC Seguridad Internet y VPN, pág. 41-44, Certificación D-Link.

importante como es el tener la certeza de la identidad de terceros con quien se comunica e intercambia información; el poder desencriptar un mensaje correctamente por parte del receptor deseado, da la seguridad de quién lo ha enviado ya que solo tal entidad pudo encriptar el mensaje que ha sido recibido. De esta forma se podrá detectar si un tercero intenta modificar el mensaje o inyectar uno falso, debido a que no posee los mismos medios que el emisor original para encriptar el mensaje. Entonces los objetivos de la criptografía son:

a. Mantener la confidencialidad de la información del mensaje.
b. Garantizar la originalidad del mensaje así como del par emisor/receptor.
c. Mostrar que cualquier ataque que tiene la probabilidad de romper la encriptación requiere de una enorme cantidad de computación.

3.2.3.1. Criptografía asimétrica o de llave pública

La criptografía asimétrica conocida también como de llave pública, se basa en el manejo de un par de llaves (claves) separadas para encriptar y desencriptar, este par de llaves se conocen como llave pública y llave privada. La llave privada es únicamente conocida por su propietario, mientras que la llave pública se publica abiertamente pero sigue asociada al propietario. Estas llaves tienen una característica única, el mensaje encriptado con una llave solo puede desencriptarse con la otra llave del par, de tal manera que un mensaje encriptado con la llave pública de una entidad no puede ser desencriptado con la misma llave, pero puede ser desencriptado con la llave privada a la que corresponde. El proceso de utilización de pares de llaves se basa en la aplicación del concepto de función unidireccional con trampa, que solo permite desencriptar al poseedor de la clave secreta (trampa), que de no conocerla, requiere solucionar un problema matemático de un elevado costo computacional. La criptografía asimétrica disminuye el riesgo de que información privada sea interceptada, permite que ambas partes se identifiquen positivamente una con otra a través de firmas digitales, permite que el receptor autentifique al emisor del mensaje, la llave pública de la pareja de llaves se

puede distribuir en un servidor sin temor de que esto comprometa el uso de la llave privada. En el proceso de comunicación, el receptor crea un par de llaves, pública y privada, y distribuye libremente la llave pública a quien quiera enviarle información, mientras la llave privada queda en posesión de quien la creo, asegurándose que nadie más la conocerá; siendo así, no es un problema que un tercero se haga de la llave pública, pues la única forma de desencriptar un mensaje encriptado con la misma, es con la llave privada que solo posee el receptor deseado del mensaje. La principal ventaja de la criptografía asimétrica es el incremento de seguridad que proporciona, pues la llave privada nunca es trasmitida o revelada a nadie.

El protocolo *Diffie-Hellman*, llamado también protocolo acuerdo de llaves exponenciales, fue desarrollado por sus homónimos en 1976, este protocolo permite a dos entidades intercambiar una llave secreta sobre un medio inseguro sin tener acuerdos preestablecidos. Diffie-Hellman no se usa para encriptar información, se usa para intercambiar de forma segura las llaves que encriptan los datos, esto se logra generando un *secreto compartido* también llamado *llave de encriptado de llave* entre las 2 partes, este secreto compartido luego encripta la llave privada usando algunos algoritmos de cifrado como DES, 3DES, IDEA, CAST, BLOWFISH, para asegurar la transmisión. A cada lado de la comunicación se tiene una llave privada y una llave pública del otro lado. Diffie-Hellman genera llaves compartidas idénticamente iguales en ambos lados de la comunicación con la llave privada local y la llave pública del lado remoto. El intercambio de llaves usando Diffie-Hellman es vulnerable a ataques de intrusos que podrían interceptar la comunicación, haciéndose pasar por el lado remoto y enviando al emisor su llave pública haciéndose pasar por el receptor. La solución es usar firmas digitales que aseguren que la entidad con la cual se está estableciendo la comunicación es realmente quien dice ser.

Una infraestructura de llaves públicas: *PKI (Public Key Infrastructure)* son los servicios y políticas que rigen el esquema de vinculación de una identidad con una llave pública y la posterior redistribución de ese vínculo. Una PKI tiene 3

procesos: *certificación*, que es la vinculación de una identidad con una llave pública; *validación*, que es el proceso de comprobar la autenticidad del certificado y asegurarse que el contenido del mismo es confiable; y *revocación*, que es el proceso de desconocer un certificado antes de su fecha de expiración.

3.2.3.2. Criptografía simétrica o de llave privada

La criptografía simétrica conocida también como de llave privada, es un sistema en que tanto el emisor como el receptor poseen la misma llave secreta para encriptar y desencriptar la información. Para garantizar la seguridad de la información transmitida, se debe proteger la llave, la cual debe ser solo conocida por aquellos que participan en la comunicación. Hablando en términos computacionales el sistema simétrico es rápido y eficaz, existiendo algoritmos muy robustos y potentes para realizar este tipo de criptografía. Las llaves utilizadas no son muy largas y el grado de protección de la información es directamente proporcional a la longitud de la llave secreta, por esta razón es recomendable cambiar la clave con frecuencia. Los algoritmos de llave simétrica más usados son: DES, 3DES, IDEA, CAST, RC2, RC4, RC5, Twofish, Blowfish, IDEA, AES, MMB, GOST, NewDES, SAFER, MADRYGA, LOKI, entre otros. El sistema simétrico permite emplear una llave para transformar la información en bits, de manera que el resultado final solo es conocido por los entes participantes, y este resultado solo puede ser interpretado por quien conoce la llave.

Por ejemplo si usamos la llave MARCO
MARCO= 1001101 1000001 1010010 1000011 1001111

Para encriptar/desencriptar se suma el mensaje original a la llave, suma binaria XOR.

Texto limpio= HOLA
Texto ASCII= 1001000 1001111 1001100 1000001

Llave= 1001101 1000001 1010010 1000011 1001111
Criptograma: 0000101 0001110 0011110 0000010 1001111

Una desventaja de este sistema es que ambas partes deben estar de acuerdo para usar la misma llave, otra desventaja es que si el emisor tiene n receptores debe guardar el registro de las llaves de cada receptor. Pero el mayor inconveniente es la autenticación, debido a que la identidad del emisor no puede ser comprobada por el receptor, esto se debe a que ambas partes poseen la misma llave, es decir que cualquier de ellos puede encriptar un mensaje y decir que la otra persona se lo envío, la manera de resolver este inconveniente es usar el sistema de criptografía asimétrica.

3.2.3.3. Firma digital

La firma digital es un conjunto de datos como firmas o claves criptográficas privadas que se añaden a una unidad de datos para proteger un mensaje de cualquier falsificación, permitiendo al receptor comprobar el origen y la integridad de la información. El método de criptografía asimétrica hace posible el uso de firmas digitales y certificados digitales, para proporcionar autenticidad a los mensajes transmitidos. Para esto se encripta la unidad de datos junto con algún componente secreto del firmante, y se obtiene un valor de control ligado al resultado encriptado. Mediante el encriptado de un menaje se puede asegurar la privacidad de la información enviada; pero ¿podría saber el receptor de quien proviene el mensaje? El origen de un mensaje es tan importante como su contenido.

La firma digital se puede utilizar para verificar la fuente de un mensaje y la integridad de la información, estos son implementados mediante llaves públicas y privadas: el emisor de un mensaje utiliza la llave privada para firmarlo y esa firma es única, debido a que solo el dispone de la llave privada; el receptor puede verificar la firma utilizando la llave pública correspondiente emitida por el emisor, esta es una propiedad de la llave de criptografía asimétrica llamada *de no repudio* puesto que cada usuario tiene la responsabilidad de proteger su llave privada.

La firma digital funciona de la siguiente manera: para personalizar un mensaje el usuario A encripta un mensaje utilizando la llave privada y lo envía al destinatario, únicamente la llave pública de A permitirá desencriptar el mensaje, por lo tanto se comprueba que efectivamente A fue quien envió el mensaje, un mensaje así puede ser desencriptado por cualquiera que tenga la llave pública de A.

Con este proceso se proporciona autenticación para el mensaje enviado, pero no seguridad mediante el encriptado, porque cualquiera puede disponer de la llave pública correspondiente para recuperar el mensaje original; se debe aplicar adicionalmente el proceso normal de encriptado seguro, es decir encriptar el mensaje con la lleva pública del receptor deseado. Considerando la carga computacional de los algoritmos de llave pública, basados en cálculos aritméticos de grandes números, podemos ver que no es la mejor solución. Para resolver esto se utiliza solo un fragmento del mensaje a cifrar, para aplicar la firma digital y luego cifrarlo con la clave pública del receptor, con esto se reduce el costo computacional de todo el proceso.

La firma digital tiene las siguientes ventajas:

a. La firma es auténtica,porque cuando un usuario usa la clave pública del emisor para desencriptar un mensaje, el usuario confirma que fue el emisor original y solamente el emisor original quien envió el mensaje.

b. La firma no puede ser violada,porque solamente el emisor conoce su llave secreta.

c. El documento firmado no puede ser alterado,porque en caso de existir cualquier alteración en al mensaje cifrado, este no podrá ser desencriptado con el uso de la llave pública de A.

d. La firma digital no es reutilizable,debido a que la firma es una función del documento y no puede ser transferida para otro documento.

Aunque la firma digital tiene varias ventajas y cada usuario tenga un par de llaves únicas, siempre existe el riesgo de un ataque a la integridad de los datos por parte de un pirata informático o algún otro tipo de intruso. En caso de un ataque, el receptor no puede estar seguro de que el emisor original del mensaje lo envió. Para verificar que efectivamente el emisor original envió el mensaje y utilizó su clave privada, existen las Autoridades de Certificación.

Existen algoritmos que reducen los documentos al mínimo, este tipo de algoritmo es conocido como de *mensaje reducido,* y es una manera de confundir al atacante; con estos algoritmos se toma cualquier tamaño de documento y se crea una reducción única, la cual tendrá siempre la misma longitud. Un mensaje reducido no puede revertirse, por lo tanto alguien debe tener el documento original que creó la reducción. La firma digital basada en mensaje reducido funcionas así:

a. Usando la clave privada, el emisor crea una reducción del mensaje y encripta dicha reducción.

b. Luego encripta el documento, es decir el mensaje original, usando la clave pública.

c. Tanto el mensaje encriptado que está contenido en el documento firmado, como la reducción encriptada se envían al destinatario.

d. El receptor aplica la llave pública del emisor a las dos firmas digitales que recibió.

e. Luego el receptor crea una nueva reducción del mensaje utilizando el mensaje original que recibió y compara la longitud obtenida con la

longitud que estaba dentro de la firma digital. Si las longitudes de las reducciones son iguales, entonces el mensaje fue verdaderamente enviado por el remitente y ha llegado sin haber sido alterado.

Los anteriores pasos son usados por el software para firmar, enviar, recibir y verificar. Estas tareas son totalmente automatizadas. El usuario simplemente ve el documento que firma y envía, o que recibe y verifica. Para la firma digital también se aplica los *Servicios de seguridad de la información,* que son: *autenticación, control de acceso, integridad, confidencialidad* y *no repudio (véase capítulo 1, subcapítulo 1.4, tema 1.4.2)*

3.2.3.4. Función *Hash*

La función Hash también conocida como función de resumen, sirve para garantizar la autenticidad de la información, genera una cadena de longitud fija llamada resumen o *fingerprint,* a partir de un mensaje de tamaño variable. La función es de un solo sentido, imposible de invertir y realiza el resumen de forma que, mensajes casi idénticos producen resúmenes muy diferentes entre sí. De esta forma hay una forma de control de integridad para detectar modificaciones al mensaje original que ha sido interceptado por algún tercero. Se puede ver en un ejemplo: el código ASCII. El código ASCII asigna un número a cada letra o signo de puntuación, es una clave simétrica estándar internacional y la utilizan todos los computadores. Se puede sustituir cada carácter de un texto por su código ASCII. Los códigos ASCII de un texto se pueden utilizar para hacer cualquier cálculo, por ejemplo cada 3 caracteres con sus códigos ASCII se opera (1º-2º)*3º, que es la suma de la primera letra más la segunda letra, por la tercera letra. La suma de los resultados es una función Hash que identifica perfectamente el texto:

Esquema 3b. Función Hash.[25]

E	n		u	n		r	i	n	c	ó	n		d	e	
69	110	32	117	110	32	114	105	110	99	243	110	32	100	101	
		-1312			**224**			**990**			**-15840**			**-6868**	**-22806**

	l	a		M	a	n	c	h	a		d	e		c	
32	108	97	32	77	97	110	99	104	97	32	100	101	32	99	
		-7372			**-4365**			**1144**			**6500**			**6831**	**2738**

u	y	o		n	o	m	b	r	e		n	o		q	
117	121	111	32	110	111	109	98	114	101	32	110	111	32	113	
		-444			**-8658**			**1254**			**7590**			**8927**	**8669**
															-11399

El resultado de la función Hash es -11399.

Cualquier modificación del texto provoca un cambio en el valor de la función Hash, por ejemplo si cambiamos una palabra por otra, el valor de la función Hash variará. La función Hash puede aplicarse en la firma digital al resultado, o sea una función Hash aplicada al mensaje en vez de al mensaje completo, ahorrando en tiempo y capacidad de procesamiento debido a que el resumen siempre es menor que el mensaje del cual se generó.Un mensaje con función Hash enviado entre dos entes asegura la integridad de la información:

a. El emisor envía un mensaje al receptor, al final del mensaje se añade la función Hash del texto, según una función en la que se han puesto previamente de acuerdo.

b. El receptor recibe el mensaje y calcula el valor Hash, si coincide con el que ha enviado el emisor, puede estar seguro que el mensaje no ha sido modificado.

   Entre las funciones Hash más importantes, están: MD2, MD4 y MD5. MD5 es resultado de la mejora de las versiones anteriores y por lo tanto, la más utilizada por ser considerada segura. MD5 trabaja en

[25] Esquema obtenido del documento DEC Seguridad y VPN, Certificación D-Link, pág. 49.

modo de bloques, la entrada es dividida en bloques de 512 bits y la salida es una cadena de 4 bloques de 32 bits.

3.2.3.5. Certificados digitales

Mediante un certificado digital, se provee de un mecanismo de autenticación para las llaves públicas que son distribuidas. Por lo tanto un certificado digital vincula la identidad de una entidad a su llave pública.

Un certificado digital es un documento que acredita que la llave pública que contiene es de quien dice ser. Para avalar tal información, este documento es respaldado por una *CA (Certification Authority – Autoridad de Certificación*) a través de su firma digital. Las CA´s son organismos seguros e independientes que emiten certificados de autenticidad de llaves públicas, es decir permiten ahorrar el trabajo demasiado difícil de comprobar con quien se está comunicando. Un certificado consta de la clave pública que certifica, del nombre del propietario, el periodo de validez, el nombre de la Autoridad de Certificación que lo emite, un número de serie, entre otros datos. El certificado digital viene firmado digitalmente por el emisor, con su llave privada.

Si se tiene la correspondiente llave pública, también en forma de certificado, se puede comprobar. Los navegadores traen incorporados las claves públicas en forma de certificados, de las CA´s más importantes: Thawte, VeriSign, entre otras; así, si se establece una conexión con alguna entidad que ha certificado su clave pública con alguna de estas CA´s, la comunicación se realizará de forma segura y transparente. Para establecer una conexión segura, el emisor contacta al receptor, quien le envía su clave pública junto con el certificado digital que acredita que la clave es de quien dice ser.

Varias normas describen la información que debe estar contenida en el certificado, cómo debe ser organizada dentro del mismo y cómo se firma el certificado. Los métodos más usados son X.509 y PGP.

a. **Certificados digitales X.509.-**La X.509 define los lineamientos de los certificados de llaves públicas, donde se vincula un nombre con una llave pública y una revocación para los certificados emitidos que no sean confiables. Esta norma no especifica un infraestructura de llaves públicas (PKI) totalmente, solo provee las bases sobre las cuales una PKI podrá ser construida. La X.509 debe contener al menos un nombre y una llave pública. El formato X.509v3 es el conjunto y la mejora de los formatos X.509v1 y X509v2.

b. **Certificados digitales PGP.-** Un certificado digital *PGP (Pretty Good Privacy)*, es construido de un número de registros etiquetados llamados paquetes. Este bloque apilado es una forma usual de enviarle a alguien un certificado digital PGP o para que alguien obtenga el certificado de otra entidad desde un sitio web. Un certificado digital PGP puede corresponder a su versión ASCII. Un certificado PGP incluye la siguiente información:

   a) Versión PGP: versión de PGP usada para crear la llave asociada con el certificado.
   b) La llave pública del portador del certificado y su algoritmo: RSA, DH (Diffie-Hellman) o *DSA (Digital Signature Algorithm)*.
   c) Información del portador del certificado: nombre usuario, su identificación *(user ID)*, etc.
   d) La firma digital del propietario del certificado.
   e) El periodo de validez del certificado.
   f) El algoritmo de encriptado simétrico preferido para la llave: CAST, IDEA o 3DES.

      En el Sistema de Administración de Certificados *(Certificate Management System)* interactúan todos los componentes de una PKI que manejan la creación, renovación, mantenimiento y revocación de certificados digitales. Estos componentes son:

a. Autoridad de Certificación.-Esta entidad emite y revoca los certificados, entre sus funciones están:

a) Creación y administración de las llaves públicas y privadas de la propia CA.
b) Creación de parejas de llaves públicas y privadas para los usuarios que así las necesitan.
c) Creación de un certificado vinculando la llave pública del usuario a la identidad del mismo.
d) Revocación de certificados.
e) Creación de la lista de certificados revocados.
f) Administración de una base de datos de información segura donde reside la historia de los certificados emitidos y revocados.
g) Manejo de un completo registro *(log)* de mensajes para propósitos de auditoría.

b. Autoridad de Registro.-La verificación de la información de un usuario, el requerimiento de un certificado, la generación de la llave y el almacenamiento de la misma, son funciones que hace la CA sin requerir la llave privada del usuario. Una o más RA´s (Register Authority - Autoridades de Registro) son empleadas para realizar estas funciones. Una CA puede tener algunas RA´s estratégicamente localizadas para proveer una alta disponibilidad y mantener estable el nivel de servicio. Cada RA debe ser certificada por la CA y debe comunicarse con la misma y con las otras RA´s que tienen que ver con la verificación y revocación de los certificados que ella maneja.

c. Depósitos de certificados y CRL´s.- Cuando un certificado es emitido a un usuario, la CA puede también publicar una copia de este certificado en un depósito. Así mismo cuando es necesario invalidar un certificado antes de su fecha de expiración, la CA debe publicar la revocación en su CRL. Lo más conveniente es mantener la CRL en la lista de certificados en el mismo

depósito. Un certificado no puede ser declarado válido hasta no ser revisado con la CRL, por lo tanto, es vital que un depósito de CRL´s tenga siempre un fácil acceso. Sin embargo, el facilitar este acceso puede hacer que el depósito sea vulnerable a los ataques por Denegación de Servicio *(véase capítulo, subcapítulo 2.2, tema 2.2.2)*. Se deben tomar medidas apropiadas para reducir este riesgo e incrementar la robustez de la PKI. Es de utilidad tener múltiples depósitos redundantes.

3.2.3.6. Encriptación a nivel de paquete

Este modo de operación también es conocido como sistema de cifrado de bloques, opera en bloques de bits u octetos, por lo general de 64 bits u 8 octetos. Es usado en aplicaciones de transferencia masiva de datos. Los tipos de encriptación a nivel de paquete son:

a. **Encriptación a nivel de enlace.-**Es la forma de protección criptográfica más transparente tanto para los controladores de los dispositivos como para las aplicaciones. Esta protección solo afecta a un enlace individual. La ventaja principal es que el paquete es encriptado por completo, incluyendo las direcciones de origen y destino lo que deja fuera de riesgo la comunicación. Sin embargo solo protege un enlace en particular, si un mensaje debe atravesar más de un enlace, será vulnerable en el nodo intermedio y en el siguiente enlace, si éste no está protegido. Por lo tanto, el encriptado a nivel de enlace es útil para proteger solo tráfico local o unas pocas líneas de enlace muy vulnerables o críticas, como por ejemplo circuitos satelitales.
b. **Encriptación a nivel de paquete y a nivel de red.-**El protocolo *NLSP (Network Layer Security Protocol - Seguridad de la Capa de Red)* y el protocolo *TLSP (Transport Layer Security Protocol - Seguridad de la Capa de Transporte)* permiten a los sistemas comunicarse de forma segura sobre Internet. Estos son transparentes para la mayor parte de las aplicaciones. La función de encriptado afecta a todas las comunicaciones que ocurran a lo largo de diferentes sistemas; ambos protocolos están basados en el concepto de *id de llave* o *key-id*; éste es transmitido sin encriptar junto con el paquete encriptado. Permite controlar el comportamiento de los

mecanismos de encriptado y desencriptado, especifica el algoritmo de encriptado, el tamaño del bloque de encriptado, el mecanismo de control de integridad usado, el período de validez de la clave, etc. Utiliza un mecanismo de administración de claves para intercambiar llaves e id´s de llaves. TLSP está limitado a conexiones individuales tales como circuitos virtuales creados en TCP. Diferentes circuitos entre el mismo par de anfitriones pueden ser protegidos con diferentes claves. El segmento TCP completo, incluyendo el encabezado el cual es encriptado. Este nuevo segmento es enviado al protocolo IP, con un identificado de protocolo diferente. Al recibir el paquete, IP envía el paquete a TLSP, que luego de desencriptar y verificar el paquete lo pasa a TCP.

NLSP ofrece más opciones que TLSP. Puede ser instalado en un ruteador, y proteger así la red de datos completa. NLSP opera por encapsulación o modo túnel. En modo túnel, el paquete IP es encriptado y luego es adjuntado a un nuevo paquete IP. La dirección IP en este encabezado puede diferir de aquella del paquete original ofreciendo una defensa contra el análisis de tráfico. La encapsulación es suficiente si los dos sistemas finales de una comunicación NLSP están conectados a la misma red de datos. La creación del nuevo encabezado IP es omitida, el paquete NLSP encriptado es enviado directamente a la capa subyacente. Estos protocolos no exigen ninguna restricción de comunicación, es decir, cualquier anfitrión protegido puede comunicarse con cualquier otro. Los patrones de comunicación son una cuestión administrativa, estas decisiones son aplicadas por los sistemas de encriptado y los mecanismos de distribución de claves.

3.2.3.7. Encriptación a nivel de aplicación

Este modo de operación también es llamado como sistema de cifrado continúo, opera en cadenas de datos, esto es bits u octetos; es usado en comunicaciones de aplicaciones interactivas. Ofrece un servicio transparente involucrando al usuario en las tareas necesarias. El alcance y la intensidad de

la protección pueden ser diseñados para cubrir las necesidades específicas de cada aplicación. Los tipos de encriptación a nivel de paquete son:

a. **Telnet.-**Es una de las áreas más críticas debido a que existe la necesidad de prevenir que las contraseñas sean enviadas sin protección a través de internet. Esto podría ser solucionado encriptando la sesión telnet. La principal desventaja en este enfoque es que utiliza capacidad de procesamiento innecesaria debido que solo las contraseñas necesitarían ser protegidas. Además debe tenerse en cuenta que el encriptado requiere de la distribución de las claves para lo cual se necesita algún tipo de autenticación. Telnet requiere de la autenticación pero en una forma flexible. El mecanismo de encriptado propuesto para Telnet tiene integrada la opción de autenticación. Las tecnologías de autenticación son fáciles de instalar y resuelven algunos problemas críticos. Al comienzo de una conexión, los dos lados negocian qué algoritmo de encriptado y autenticación será usado y por quién. Luego puede activarse y desactivarse el encriptado en cualquier momento de la sesión. Cada dirección es encriptada independientemente, lo que permite que solo los mensajes de entrada al servidor sean encriptados y no los de salida, con el mismo desempeño.
b. **SNMP *(Simple Network Management Protocol - Protocolo Simple de Administración de Red)*.-** Es un protocolo de la capa de aplicación, utilizado para controlar ruteadores, VPN´s y otros dispositivos de red. Es clara la necesidad de autentificar las solicitudes de SNMP y también los paquetes relacionados a las tareas de autenticación. Existe una opción de seguridad para este protocolo. El problema de autenticación es resuelto usando funciones hash seguras, ambas partes comparten una cadena de 16 bytes que es adjuntada a la solicitud SNMP, esta cadena se genera mediante MD5. El cifrado es realizado utilizando DES en modo de bloques en cadena, la clave consiste de 2 números de 8 bytes, uno es la clave DES y el otro es usado para el modo de boques de cadena. Se realiza además un resumen del mensaje con MD5 para control de integridad. Los mensajes

SNMP seguros incluyen un *timestamp* para evitar ataques de *repetición,* el cual consiste en el reenvío de un mensaje legítimo capturado por un intruso, reinsertándolo en la red de datos.

c. **Servicio de correo electrónico.-**Este tipo de servicio concierne más a los usuarios finales, que desean que la información que envíen a través del correo electrónico no esté expuesta. Entre los más destacados se encuentran *PEM (Privacy-Enhanced Electronic Mail)*, el estándar oficial de la familia de protocolos de TCP/IP, PGP desarrollado fuera de EEUU para evitar el alcance de la patente de RSA; y RIPEM, basado en una implementación libre de RSA, habilitado con el consentimiento de los dueños de la patente. Todos estos utilizan un sistema de llave privada para encriptado y un sistema de distribución de llaves basado en los sistemas de criptografía asimétrica. La seguridad del correo electrónico depende críticamente de la seguridad del Sistema Operativo; cualquier sistema de correo debe ser ejecutado en un sistema final que esté protegido físicamente y electrónicamente. PEM tiene una estructura bastante elaborada, utiliza DES como algoritmo de encriptación del cuerpo de un mensaje, RSA para encriptar las claves DES y los certificados distribuidos y genera resúmenes de los mensajes utilizando MD5.

3.2.3.8. Sistemas de autenticación

Los sistemas de autenticación están basados en tres atributos, que son: lo que tiene el usuario (por ejemplo una llave), lo que sabe el usuario (por ejemplo una contraseña), lo que es el usuario (por ejemplo una credencial). Generalmente es aceptado el uso de un método sencillo de autenticación, como es la contraseña, pero no es suficiente para proteger sistemas informáticos; se recomienda los sistemas de autenticación complejos, los cuales deben usar por lo menos dos de los atributos de autenticación señalados anteriormente.

a. **Contraseñas tradicionales.-** Son la forma más simple de autenticar, sin embargo es un método inadecuado para garantizar la seguridad en el

acceso a una red de datos, debido a que las contraseñas pueden ser adivinados e interceptados durante las transmisiones. Por ejemplo, servicios como FTP y Telnet transmiten los nombres y las claves en texto plano, haciéndolos fácilmente interceptables.

b. **Contraseñas únicas.-**Los sistemas de contraseñas únicas restringen el uso de una contraseña a una sola sesión de comunicación, lo que quiere decir que se requiere una contraseña nueva para cada nueva sesión; estos sistemas como S/KEY, facilitan al usuario la elección de una nueva contraseña para la siguiente sesión, generando una lista de posibles contraseñas. S/KEY usa una contraseña secreta encriptada generada por el usuario, para crear la secuencia de contraseñas únicas. La contraseña del usuario nunca atraviesa la red de datos, por lo tanto la contraseña no es sujeta de ataques. Con esto se logra que las contraseñas únicas que son generadas por esta clave y que pudieron ser interceptadas para luego ser utilizadas no le sirvan al atacante. La primera contraseña única es producida aplicando al mensaje original una función HASH n veces, donde n es un número especificado por el usuario. La siguiente contraseña única es generada aplicando al mensaje original la misma función HASH n-1 veces y así sucesivamente hasta generar n contraseñas únicas. Cuando un usuario intenta entrar a la red de datos, el servidor en el cual está habilitado el S/KEY genera una respuesta que consiste de un número y una cadena de caracteres, la cual es llamada *seed*. En respuesta al mensaje enviado por el servidor, el usuario usa el número y el *seed* que le ha llegado. El software generador S/KEY que corre en el computador se encarga de combinar los tres elementos y de iterarlos tantas veces como el número que le ha llegado en el mensaje de respuesta del servidor. La contraseña única resultante es enviada al servidor de autenticación el cual también lo itera tantas veces como él se lo haya indicado al cliente en funciones HASH, luego lo compara con la contraseña única que tenía almacenada. Si hay una concordancia, al usuario se le permite el ingreso a la red de datos. Los sistemas de contraseñas únicas como el S/KEY

requieren que el software del servidor sea modificado para realizar los cálculos requeridos y que cada computador remoto tenga una copia de un software cliente. Estos sistemas no son muy escalables dado que se dificulta administrar listas de contraseñas para un gran número de usuarios.

c. **PAP *(Password Authentication Protocol - Protocolo de Autenticación por Contraseña).-*** Fue diseñado originalmente como una manera sencilla para qué un computador se autenticara en otro, cuando los mismos usan un protocolo de comunicación punto a punto como PPP, por lo tanto PAP es un protocolo de dos vías. PAP es utilizado por muchos *ISP´s (Internet Service Providers - Proveedores de Servicio de Internet)*. El cliente se autentica a si mismo enviando un nombre de usuario y una contraseña al servidor, la contraseña se puede encriptar de manera opcional. Luego la contraseña es comparada por el servidor (autenticador) con su base de datos de claves o secrets, cuando el computador remoto está autenticado, aprueba la comunicación. PAP es un protocolo de autenticación que puede ser usado al comienzo del establecimiento de un enlace PPP, o bien durante el transcurso de la sesión PPP para reautenticar el enlace. PAP no es seguro porque la información de autenticación es transmitida en texto plano, esto hace vulnerable a que atacantes obtengan información de nombres de usuario y claves de manera fácil, escuchando en una línea serie y haciendo sucesivos intentos por el método de prueba y error.

d. **CHAP *(Challenge Handshake Authentication Protocol - Protocolo de Autenticación por Reto).-*** Es muy similar al PAP pero es más seguro para autenticar enlaces PPP. CHAP es un protocolo de tres vías y de la misma forma que PAP, puede ser usado al comienzo de un enlace PPP y ser repetido cuando ya se haya establecido el enlace. CHAP incorpora los siguientes pasos para la autenticación de un enlace:

a) El autenticador envía un mensaje al nodo remoto.

b) El nodo calcula un valor usando una función HASH y lo envía de regreso al autenticador.
c) El autenticador avala la conexión si la respuesta concuerda con el valor esperado.

El proceso puede repetirse en cualquier momento del enlace PPP para asegurarse que la conexión no ha sido tomada por otro nodo. A diferencia de PAP, en CHAP el servidor controla la reautenticación.

Con CHAP, el servidor (autenticador) envía al cliente una cadena de reto generada aleatoriamente, junto a su nombre de computadora. El cliente utiliza el nombre de la computadora para buscar la contraseña apropiada, la combina con el reto, y encripta la cadena utilizando una función de codificación de un solo sentido; el resultado es devuelto al servidor junto con el nombre de la computadora cliente. El servidor realiza ahora la misma computación y advierte al cliente si obtiene el mismo resultado. CHAP no solicita autenticación al cliente solamente al comienzo de la sesión, sino que envía retos a intervalos regulares para asegurarse de que el cliente no ha sido reemplazado por un intruso.

e. RADIUS *(Remote Authentication Dial-In User Service - Servicio de Autenticación Remota del Usuario)*.- Usa una arquitectura cliente-servidor e incluye dos componentes: un servidor de autenticación y un protocolo cliente; el protocolo cliente es implementado en el *NAS (Network Access Server - Servidor de Acceso a la Red)*. RADIUS también puede emplear una arquitectura distribuida en que el NAS deba soportar autenticación para múltiples dominios, para esto el RADIUS se configura en modo proxy.

Esta función permite a las diferentes ISP´s hacer *roaming*[26]con sus similares, para esto el usuario que necesite hacer roaming escribe su

[26] En redes inalámbricas, **roaming** se refiere a la capacidad de cambiar de un área de cobertura a otra sin interrupción en el servicio o pérdida en conectividad.

nombre de usuario en el formato *“usuario@dominio.com ”,* de esta manera el servidor RADIUS del ISP envía el requerimiento hacia el servidor RADIUS del ISP remoto para que éste ejerza las labores de autenticación. De la misma manera que un *RAS (Remote Access Service - Servicio de Acceso Remoto)* y un servidor RADIUS usan claves compartidas, dos servidores RADIUS en modo proxy usan otra clave compartida para proteger la comunicación entre ellos. El proceso de autenticación con RADIUS tiene los siguientes pasos:

a) Un usuario remoto marca a un RAS, cuando la conexión al modem se completa, el RAS pregunta por un nombre de usuario y la contraseña.

b) Una vez recibido el nombre de usuario y la contraseña, el RAS crea un paquete de datos llamado requerimiento de autenticación; este paquete incluye información como son el nombre del usuario, la contraseña, el módem de conexión. Para evitar que un pirata informático escuche la información, el RAS actúa como un cliente del servidor RADIUS, cifrando el mensaje con una clave compartida predeterminada entre el RAS y el servidor RADIUS.

c) El requerimiento de autenticación es enviado por medio de una red de datos local o internet hasta el servidor RADIUS. Si el servidor RADIUS no puede ser alcanzado, el cliente RADIUS puede enviar el requerimiento a un servidor alternativo.

d) Cuando un requerimiento de autenticación es recibido, el servidor RADIUS valida el requerimiento y verifica la información del nombre de usuario y la contraseña. Esta información también puede ser transmitida a un sistema de seguridad apropiado que soporte los archivos de autenticación, por lo general bases de datos.

e) Si el nombre de usuario y la contraseña son correctos, el servidor envía un reconocimiento de autenticación que puede incluir información del

usuario en la red de datos local o internet y los servicios que el requiere. Por ejemplo, el RADIUS le puede decir al NAS que el usuario requiere una dirección IP estática o que obtiene su dirección IP de un rango dinámico de direcciones, también puede contener información sobre los filtros que pueden limitar al usuario a acceder ciertos recursos específicos de la red como por ejemplo el uso de un servidor proxy.

f) Si en este punto del proceso la autenticación no tiene éxito, el servidor RADIUS envía un mensaje de desconexión al RAS y al usuario se le niega el acceso a la red de datos, como por ejemplo a un pirata informático.

Gráfico 3.3. Autenticación en servidor RADIUS.

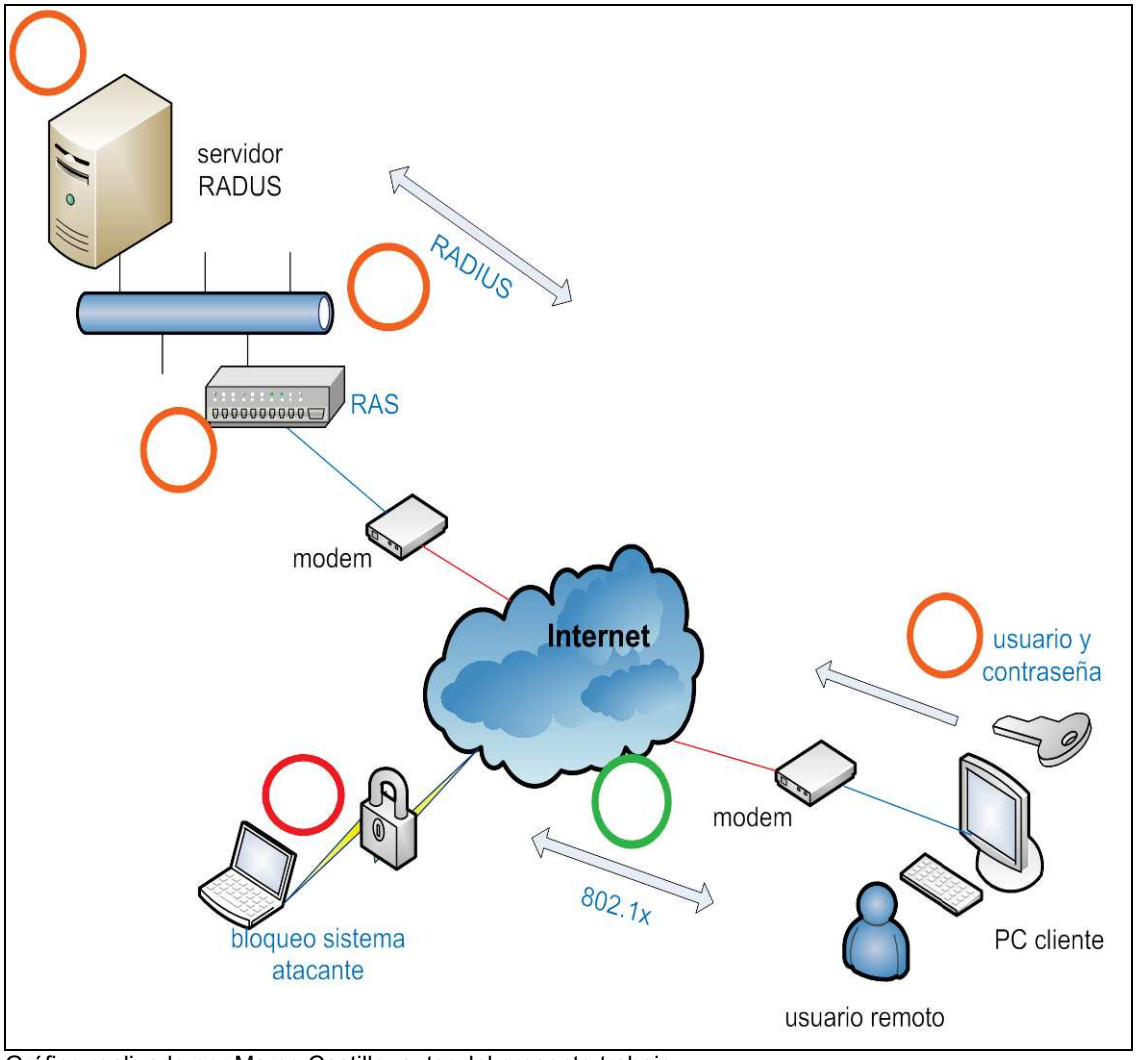


Gráfico realizado por Marco Castillo, autor del presente trabajo.

La norma 802.1x *(ver Anexo 2)* es usada en una arquitectura cliente-servidor RADIUS, permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o previniendo el acceso por ese puerto si la autenticación falla. Una versión extendida de la norma IEEE 802.1x, que permite múltiples autenticaciones en paralelo, controla el acceso a los servicios, pero es necesario un nuevo mecanismo para la configuración dinámica de los clientes. El protocolo *ECP (Extended Configuration Protocol)*, el cual guarda una estrecha relación con el proceso de autenticación, trata de dar respuesta a esta carencia logrando configurar correctamente a los clientes en función de los requisitos específicos de cada servicio.

802.1x está disponible en ciertos conmutadores de red y puede configurarse para autenticar nodos que están equipados con software suplicante. Esto elimina el acceso no autorizado a la red al nivel de la capa de enlace de datos. Se recomienda que se utilice la autenticación 802.1X siempre que se conecte a una red inalámbrica 802.11 *(ver Anexo 2).* 802.1X es un estándar IEEE que mejora la seguridad y la implementación al proporcionar compatibilidad con la identificación de usuarios, la autenticación, la administración de claves dinámicas y la creación de cuentas de manera centralizada. [27]

3.2.4 VPN *(Virtual Private Network – Red Privada Virtual)*

Una VPN es una conexión que tiene la apariencia y muchas de las ventajas de un enlace dedicado, pero también trabaja sobre una red pública. La comunicación entre sitios a través de internet es vulnerable a ataques de *escuchas.* El uso de una VPN garantiza que todo el tráfico existente entre diferentes puntos de comunicación remotos interconectados, sea privado.

Una VPN consiste en un conjunto de sistemas y dispositivos interconectados a través de canales seguros sobre una red pública, permitiendo el acceso remoto a los recursos y servicios de la red de datos local de forma transparente y segura, como si los usuarios estuvieran conectados de forma local. Para este propósito se usa una técnica llamada túnel o *tunneling*, los paquetes de datos son enrutados por la red pública, como internet o alguna otra red comercial, en un túnel privado que simula una conexión punto a punto. Este recurso hace que por la misma red de datos local puedan crearse muchos enlaces por diferentes túneles virtuales a través de la misma infraestructura. Una VPN ofrece una alternativa sobre líneas dedicadas y el acceso remoto tradicional debido a que utiliza los canales de comunicación ya existentes de internet, permitiendo conectar usuarios remotos mediante el uso de servidores VPN para que

---

[27] Tema, y subtemas desarrollados a partir de las siguientes fuentes:
http://www.textoscientificos.com/redes/firewalls-distribuidos/soluciones-seguridad
Diapositivas: Firma Digital, autor: Ing. Henry Burbano.
Diapositivas: Autenticación PAP y CHAP, autor: Ing. Henry Burbano
DEC Seguridad Internet y VPN, pág. 54-73, Certificación D-Link.

diferentes usuarios y conexiones puedan establecerse en diferentes momentos y compartir la misma infraestructura. También hace universales para su transporte los diferentes protocolos LAN como son TCP/IP, IPX, Appletalk y Netbeui, de allí la característica de multiprotocolo que hace sumamente universal la tecnología de las VPN´s.

Las VPN´s generalmente suelen ser implementadas en cortafuegos, como parte de una solución de estos, debido a que un dispositivo de VPN opera a nivel de red (véase Anexo 3), a través de conexiones seguras utilizando encapsulación, encriptado y autenticación; de esta manera se transportan de forma segura paquetes IP mediante internet, estableciendo túneles en ambos puntos de conexión que negocian un esquema de encriptado y autenticación previo al transporte. También los servidores VPN suelen estar detrás de un cortafuegos perimetral, para proteger la red de datos de la organización. En estos esquemas un usuario remoto solicita un recurso autenticado de la red de datos local de la organización y crea una conexión lógica al servidor VPN, este autentifica al cliente y efectúa operaciones de encriptado y encapsulación sobre las transmisiones entre el cliente y los recursos de la red de datos local; la conexión al servidor VPN utiliza un protocolo de túnel que permite a la organización extender su red de datos local mediante canales privados encriptados sobre internet, de tal forma que la organización pueda usar la red pública debido a que los paquetes están protegidos antes de ser enviados por un canal no seguro como es internet. Existen varias tecnologías para implementar VPN´s, pero la principal es la criptografía.

3.2.4.1. Razones del auge de las VPN´s

Con el auge que ha tenido internet y por el cada vez menos costo para acceder a esta gran red mundial y el significado que ha adquirido como el principal medio de comunicación, las VPN´s han hecho su aparición ganándose un espacio dentro del cambiante mundo de las redes de datos. Tradicionalmente un enlace privado se ha hecho por medio de tecnologías WAN como X.25, Frame Relay, ATM, enlaces Clear Channel o enlaces conmutados. Ahora es

posible utilizar un protocolo como TCP/IP, sin importar la tecnología WAN que lo soporte para disfrutar de los servicios y ventajas que ofrecen los enlaces privados entre redes de datos. Y mientras que las tradicionales redes de datos locales se han hecho fuertes en las conexiones LAN-to-LAN, no han sido capaces de atacar el mercado de los usuarios individuales o pequeñas oficinas y sucursales, y es aquí principalmente donde han surgido con fuerza las soluciones basadas en VPN´s sobre IP, pues su implementación resulta sencilla y bastante económica. El hecho que las VPN´s se construyan sobre infraestructuras públicas ya creadas ha hecho que las empresas ahorren más del 50% del costo que antes tenían que pagar en llamadas de larga distancia y en equipos físicos de acceso remoto o en alquiler de enlaces privados o dedicados.

3.2.4.2. Características fundamentales de las VPN´s

Las VPN´s se caracterizan por los siguientes atributos:

a. Transparencia en la comunicación con el empleo de túneles.
b. Autenticación de usuarios para el acceso a la VPN.
c. Independencia del nivel del enlace a internet empleado para el acceso a la VPN como: RTC, ISDN, ADSL, etc.
d. Mecanismos de encriptado como IPsec, PPTP, T2L, L2F, L2TP.
e. Algoritmos de encriptado como RC2, RC4, DES, 3DES, IDEA, CAST.
f. Mecanismos de negociación e intercambio de claves para encriptado como ISAKMP, SKIP.
g. Algoritmos para intercambiar claves para el encriptado como RSA, Diffie-Hellman.

Todas estas características deben funcionar de forma coordinada para poder integrar una correcta funcionalidad para una VPN.

3.2.4.3. Componentes de las VPN´s

La forma de comunicación entre las partes de la red de datos local a través de la red pública se hace estableciendo túneles virtuales entre dos puntos para los cuales se negocian esquemas de encriptación y autenticación que aseguran la confidencialidad e integridad de los datos transmitidos. Cuando se usa internet, es necesario prestar la debida atención a las cuestiones de seguridad, que se aborda a través de estos esquemas de encriptación y autenticación.

a. **Túneles.-** Un túnel es un canal virtual, configurado entre dos sistemas remotos que se encuentran en diferentes redes, sobre una conexión real que involucra más de un nodo intermedio. La tecnología de túneles o *tunneling* es un modo de transferir información en la que se encapsula un tipo de paquetes de datos dentro del paquete de datos de algún protocolo, no necesariamente diferente al del paquete original. Al llegar al destino, el paquete original es desempaquetado volviendo así a su estado original. En el traslado a través de Internet, los paquetes viajan encriptados. De esta forma el paquete puede "saltar" la topología de una red. El túnel es creado encapsulando un protocolo de red dentro de los paquetes del mismo protocolo para ser llevados por la red real. De esta manera el túnel es simplemente la ruta que toman los paquetes encapsulados y encriptados, dentro de un paquete del mismo protocolo entre las dos redes de datos. Un pirata informático podría interceptar los mensajes que viajen por el túnel, pero los datos encapsulados están encriptados y solo pueden ser recuperados por el destinatario final. Gracias a esto, una organización puede usar de forma segura y confiable una red pública para comunicarse con sus usuarios o pares, debido a que los paquetes son encriptados antes de ser enviados a través del túnel. Dentro de los protocolos que se usan en la tecnología de túneles se encuentran *PPTP (Point-to-Point Tunneling Protocol), L2FP (Layer-2 Fowarding Protocol), modo túnel de IPSec. y el L2F (Cisco´s Layer Two Forwarding).*

b. **Autenticación.-** La autenticación es el acto de verificar la identidad de alguien o algo en un contexto definido, no es suficiente simplemente declarar que se es quien se dice ser, se debe probarlo. Las técnicas de autenticación son esenciales en las VPN´s porque aseguran a los participantes de la misma que están intercambiando información con el usuario o dispositivo correcto. La autenticación en VPN´s es conceptualmente parecido al ingreso a un sistema con nombre de usuario y contraseña, pero con necesidades mayores de aseguramiento de validación de identidades. La mayoría de los sistemas de autenticación usados en VPN´s están basados en un sistema de llaves compartidas.Si la información de autenticación está totalmente bajo el control de las dos entidades, el esquema de autenticación es llamado Esquema de Autenticación Compartido *(two-party)*. Sin embargo, en muchos casos es más seguro y escalable ayudarse de una tercera parte o de más para la autenticación, estos esquemas son llamados de Confianza en Terceras Partes *(trusted third-party)*.Otro factor a tener en cuenta es la integridad y confidencialidad de la información de autenticación. Estas medidas de seguridad no solo deben ser tomadas en el establecimiento del túnel, sino durante el transcurso del intercambio de datos. En las VPN´s esto es muy importante porque la información de autenticación es transmitida a través de internet.

c. **Integridad.-** La autenticación también es usada para asegurar la integridad de la información. La información es procesada con un algoritmo de *hashing* para derivar un valor incluido en el mensaje como *checksum*. Cualquier desviación en el *checksum* indica que la información fue corrupta en la transmisión o interceptada y modificada en el camino.

d. **Encriptación.-** Todas las VPN´s tienen algún tipo de tecnología de encriptación que esencialmente empaqueta la información en un paquete seguro. La encriptación es considerada tan esencial como la autenticación porque protege los datos transportados del poder ser vistos y descifrados

en el viaje de un extremo a otro de la conexión. Existen dos tipos de técnicas de encriptación que se usan en las VPN: criptografía de llave privada, o secreta y criptografía de llave pública, ya explicadas anteriormente. En las VPN´s la encriptación debe ser realizada en tiempo real, por eso, los flujos encriptados a través de una red de datos son encriptados utilizando criptografía de llave privada con claves que son solamente buenas para sesiones de flujo.

3.2.4.4. Intranet VPN LAN-TO-LAN

Tradicionalmente, para conectar dos o más oficinas remotas de una misma compañía se necesitaba contratar Enlaces Dedicados o Circuitos Virtuales Permanentes (PVC´s) Frame Relay.Con una arquitectura Intranet VPN se puede lograr el mismo objetivo de interconectar dos o más sitios de una red de datos local, a un costo mucho menor. La economía se ve reflejada tanto en equipos que se tienen que adquirir o arrendar para el montaje inicial de la topología, como en cargos fijos que se tienen que pagar mes a mes. El único equipo que tiene que adquirir la compañía para cada lugar a conectar es un VPN que por lo general tiene un puerto LAN, sea Ethernet o Fast Ethernet para conectarse a la LAN Corporativa, y un puerto WAN para conectarse hacia el ISP. Muchos de estos equipos VPN trabajan como cortafuegos. Solo se necesita un último kilómetro por oficina, por ahí viajan todos los túneles VPN que se necesiten.

Gráfico 3.4. VPN LAN-TO-LAN. Los túneles VPN en color celeste son enlaces lógicos.

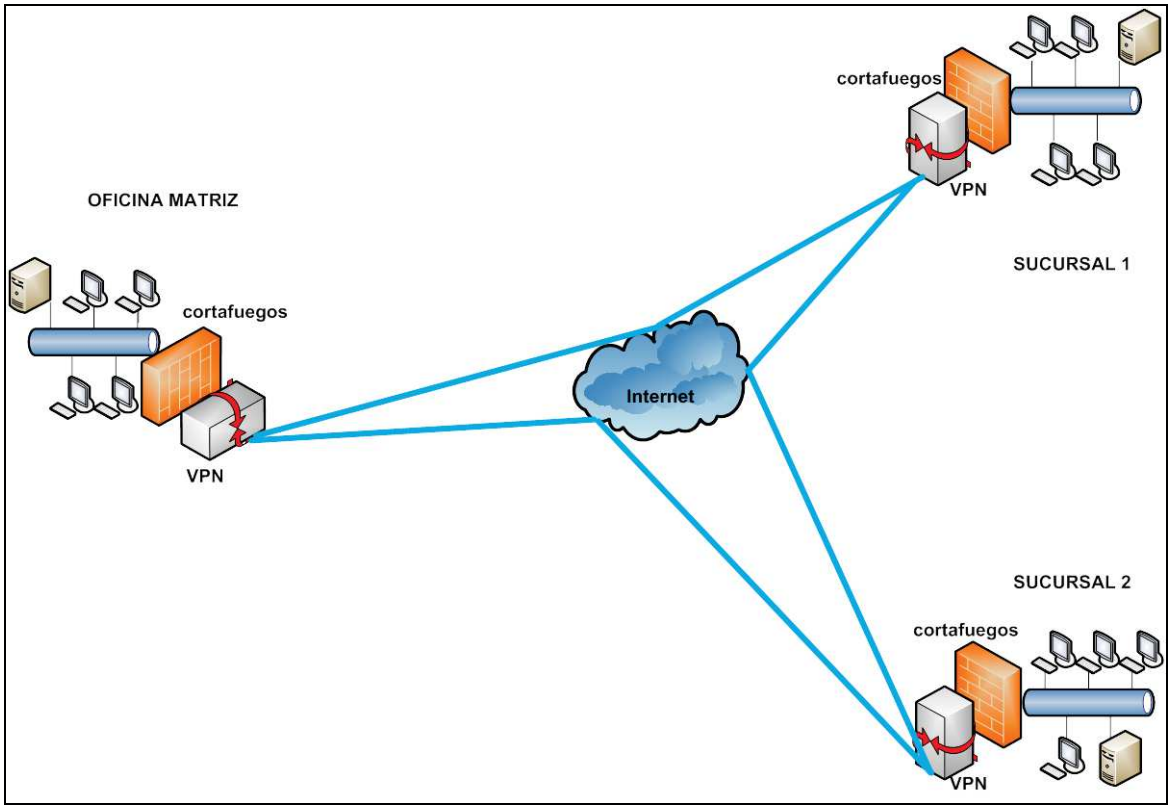


Gráfico realizado por Marco Castillo, autor del presente trabajo.

3.2.4.5. Acceso Remoto VPN

Consiste en usar algún RAS que preste servicio de conexión a internet como punto de acceso a una red de datos local también conectada a internet por medio de un equipo VPN conectado al ISP. Esta fue la primera aplicación que se le dio a la emergente tecnología de las VPN´s.Esta solución nació de la necesidad de los usuarios para poder acceder a los recursos de la red de datos local desde cualquier ubicación, incluso a nivel mundial; con el Acceso Remoto VPN, los RAS corporativos quedaron olvidados, pues su mantenimiento era costoso. Otra de las grandes ventajas del Acceso Remoto VPN sobre el tradicional acceso remoto es poder usar tecnologías de acceso de última milla como xDSL y cable módem para poder acceder a gran velocidad a la red de datos de una organización.

Gráfico 3.4. Acceso Remoto VPN.

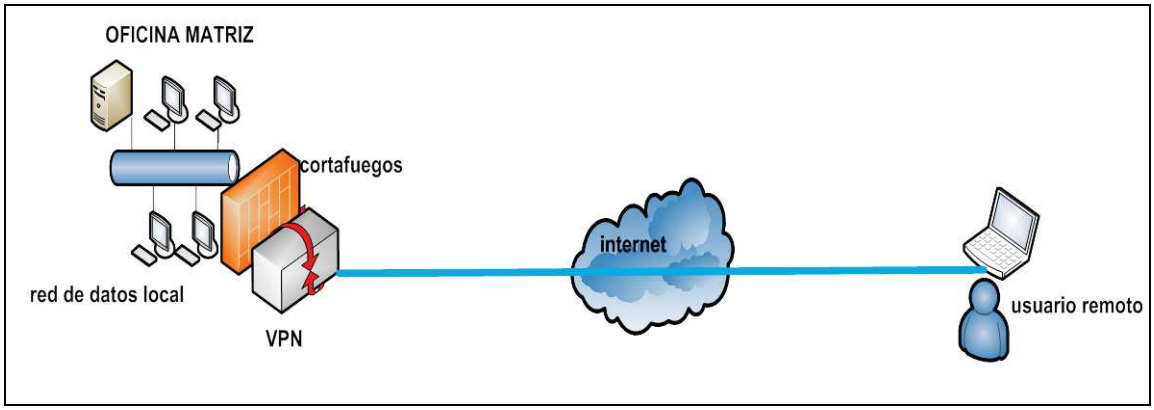


Gráfico realizado por Marco Castillo, autor del presente trabajo.

3.2.4.6. Extranet VPN

Las organizaciones necesitan intercambiar información y realizar transacciones no solamente entre sitios de su misma organización sino también con otras organizaciones. Por ejemplo una organización que quisiera permitirle al sistema de sus distribuidores acceder a su red de datos local, la misma organización también podría acceder a la red de datos de sus proveedores, en ambos casos para poder ordenar y despachar fácil y automáticamente algún tipo de pedido. Ciertamente con una arquitectura de Extranet VPN, cada organización debe controlar muy meticulosamente el acceso a los recursos de su red de datos y la información que van a intercambiar con sus socios de negocios. Implementar una topología Extranet VPN implica incrementar la complejidad de los sistemas de control de acceso y de autenticación. Al igual que en una arquitectura VPN LAN to LAN es necesario un equipo VPN que se instala en la red de datos local. Los túneles son creados a través de internet entre ambos equipos VPN situados en la red de datos de cada lado.

Gráfico 3f. Extranet VPN.

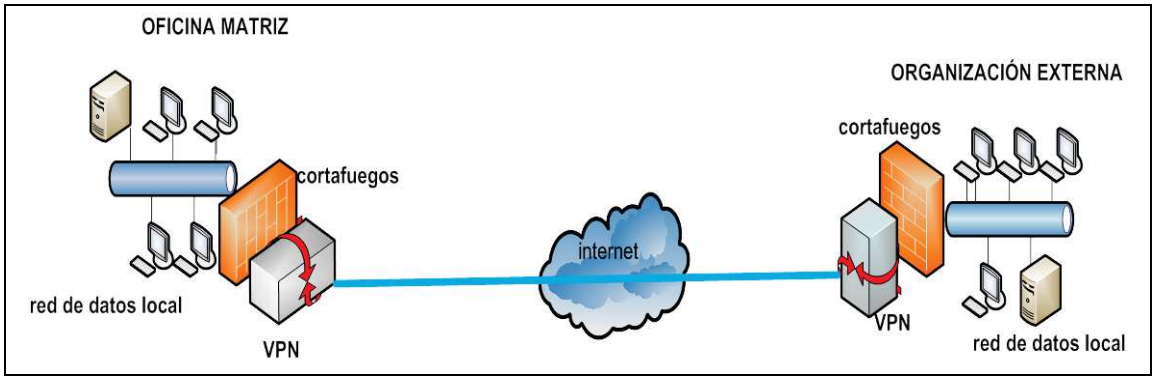


Gráfico realizado por Marco Castillo, autor del presente trabajo.

3.2.4.7. Clasificación de las VPN´s

Desde el punto de vista del modelo OSI se puede crear una VPN con tecnologías de la capa de enlace (véase Anexo 3) como PPTP y L2TP, y con tecnologías de la capa (véase Anexo 3) de red como IPSec.

a. **PPTP *(Point to Point Tunneling Protocol - Protocolo de Túnel Punto a Punto).-***Por lo general es usado por organizaciones pequeñas para realizar sus VPN´s LAN-to-LAN, y en topologías de acceso remoto por *teletrabajadores(teleworkers)*, los cuales se mantienen en constante movimiento por fuera de la organización.El protocolo más comúnmente usado para acceso conmutado a Internet es el protocolo punto a punto (PPP). PPTP es soportado por toda la funcionalidad que PPP le brinda a un acceso conmutado para construir sus túneles a través de internet. PPTP encapsula paquetes PPP usando una versión modificada del GRE *(Generic Routing Encapsulation - Encapsulamiento Ruteado Genérico)*. Según lo anterior, PPTP no solo es capaz de encapsular paquetes IP, sino IPX y NETBEUI, los protocolos de red local más usados. PPTP utiliza los mecanismos de autenticación que generalmente están asociados a PPP tales como PAP y CHAP. Una de las ventajas que tiene PPTP por ser un protocolo de nivel de enlace, es que puede transmitir protocolos diferentes a IP en sus túneles, a diferencia de IPSec que se restringe a trabajar únicamente con paquetes IP.

PPTP depende del protocolo PPP para crear la conexión conmutada entre el cliente y el servidor de acceso a la red. PPTP confía las siguientes funciones a PPP:

a) Establecimiento y finalización de la conexión física.
b) Autenticación de los usuarios.
c) Creación de datagramas PPP.

Después que el enlace PPP es creado, el protocolo PPTP define dos diferentes tipos de paquetes: paquetes de control y paquetes de datos, cada uno de los cuales es asignado a diferentes canales lógicos. PPTP separa los canales de control y de datos usando un flujo de control que corre sobre TCP y un flujo de datos que está encapsulado con cabeceras IP usando GRE. La conexión TCP es creada entre el cliente y el servidor PPTP. Esta conexión es usada para intercambiar mensajes de control. Los paquetes de datos contienen los datos del usuario, o sea los datagramas del protocolo de capa de red usado. Los paquetes de control son enviados periódicamente para revisar el estado del enlace y las señales de manejo entre el cliente y el servidor PPTP. Los mensajes de control establecen, mantienen y finalizan un túnel PPTP. Después de que el túnel PPTP se ha establecido, los datos del usuario son transmitidos entre el cliente y el servidor PPTP. Estos datos son transmitidos en datagramas IP contenidos dentro de los paquetes PPP; los datagramas IP son creados usando una versión modificada del protocolo GRE; esta modificación consiste en incluir un identificador de los anfitriones que puede ser usado para controlar los privilegios de acceso y la capacidad de reconocimiento, la cual es usada para monitorear la tasa de transferencia a la cual los paquetes están transmitiéndose en el túnel. La cabecera GRE es usada para encapsular el paquete PPP dentro del datagrama IP. La carga útil del paquete *(payload)* es esencialmente el paquete PPP original enviado por el cliente. Debido a que PPTP opera con un protocolo de nivel de enlace, debe incluir una cabecera que

depende del medio en el cual el túnel está transmitiendo, esta puede ser Ethernet, Frame Relay o PPP.

b. **L2TP *(Layer 2 Tunneling Protocol - Protocolo de Túnel de Capa 2)*.-** fue creado como el sucesor de PPTP y L2F. Las dos compañías que crearon estos protocolos, Microsoft por PPTP y Cisco por L2F, acordaron trabajar en conjunto para la creación de un único protocolo de capa 2 (véase Anexo 3) y así lograr su normalización por parte de la *IETF (Internet Engineering Task Force)*. Al igual que PPTP, L2F fue diseñado como un protocolo de entunelamiento usando para ello encapsulamiento de cabeceras. Una de las grandes diferencias entre PPTP y L2F, es que el entunelamiento de éste último no depende de IP y GRE, permitiéndole trabajar con otros medios físicos, por ejemplo Frame Relay. Paralelamente al diseño de PPTP, L2F utilizó PPP para autenticación de usuarios accediendo vía telefónica conmutada, pero también incluyó soporte para *TACACS+(Terminal Access Controller Access Control System - Sistema de control de acceso del controlador de acceso a terminales)* y Radius. Otra gran diferencia de L2F con respecto a PPTP es que permite que un único túnel soporte más de una conexión. Hay dos niveles de autenticación del usuario: primero, por el ISP antes de crear el túnel; segundo, cuando la conexión está configurada y la autenticación la realiza el equipo VPN corporativo. Todas las anteriores características de L2F han sido transportadas a L2TP. Como PPTP, L2TP utiliza la funcionalidad de PPP para proveer acceso conmutado que puede ser tunelizado a través de internet a un sitio destino. Sin embargo, como se ha mencionado anteriormente, L2TP define su propio protocolo de entunelamiento basado en L2F permitiendo el transporte sobre una amplia variedad de medios de empaquetamiento tales como X.25, Frame Relay y ATM. Debido a que L2TP es un protocolo de nivel de enlace, ofrece a los usuarios la misma flexibilidad de PPTP de soportar otros protocolos aparte de IP, tales como IPX y NETBEUI. Ya que L2TP usa PPTP en enlaces conmutados, incluye mecanismos de autenticación

nativos de PPP como PAP y CHAP. Las mejoras de L2TP con respecto a PPTP son evidentes.

c. **IPSec *(Internet Protocol Security - Seguridad del Protocolo de Internet)*.-** está diseñado para proveer seguridad basada en criptografía robusta, es de alta calidad e interoperable para IPv4 e IPv6, de hecho IPsec está incluido en IPv6. Entre los servicios de seguridad ofrecidos en IPsec están: control de acceso, integridad de los datos en comunicaciones sin conexión, autenticación del origen de los datos, protección contra ataques de repetición y confidencialidad de los datos mediante encriptado, entre otros. Estos servicios son provistos en la capa IP, ofreciendo protección para esta y las capas superiores. Entre las ventajas de IPSec están la modularidad del protocolo, debido a que no depende de un algoritmo criptográfico específico. Antes del envió de tráfico IPsec, cada ruteador/cortafuegos/anfitrión debe ser capaz de verificar la identidad de su par. El conjunto de protocolos de seguridad utilizados y la forma en que son empleados estará determinado por requerimientos del sistema y de seguridad de las aplicaciones y usuarios. IPSec es un conjunto de protocolos definidos por la IETF para proporcionar seguridad IP a nivel de red. Los mecanismos utilizados por IPSec están diseñados para ser independientes de los algoritmos empleados, esta modularidad permite la selección de diferentes conjuntos de algoritmos sin afectar las otras partes del sistema, de todos modos IPsec propone un conjunto de algoritmos por defecto para ser usados y proveer interoperabilidad en internet.

Una VPN basada en IPsec consta de las siguientes partes:

a) **IKE *(Internet Key Exchange protocol - Protocolo de Intercambio de Llave en Internet).-*** Establece una política de seguridad compartida y claves autenticadas para los servicios que las requieran. Para encriptar y autenticar la información solo se necesita algoritmos y llaves usados con

ellos. IKE es usado como un método para distribuir estas *llaves de sesión*, además de proporcionar una forma para que los puntos extremos de la VPN se pongan de acuerdo en cómo los datos deberían ser protegidos.

En la primera parte, IKE es la fase de negociación inicial, donde los dos extremos de la VPN se ponen de acuerdo en qué métodos serán usados para proporcionar seguridad al tráfico IP. Además IKE es usado para administrar conexiones, definiendo un conjunto de *SA´s (Asociaciones de Seguridad - Security Associations)*, para cada conexión. Las SA´s son unidireccionales, por lo que se necesitarán al menos dos SA´s por conexión IPSec.

La segunda parte corresponde a la data IP que actualmente está siendo transferida, usando métodos de encriptación y autenticación negociados en la fase IKE. Esto se puede lograr de diferentes formas usando protocolos IPSec: ESP, AH o una combinación de ambos. El flujo de eventos puede ser descrito como sigue:

a) IKE negocia cómo el IKE debería ser protegido.
b) IKE negocia cómo IPSec debería ser protegido.
c) IPSec transporta los datos en el túnel VPN.

Tareas desarrolladas por IKE:

a) Proporcionar un medio de autenticación a los puntos extremos.
b) Establecer nuevas conexiones IPSec (crear pares de SA´s).
c) Administrar conexiones existentes.

IKE mantiene un registro de las conexiones asignando un conjunto de SA´s, para cada conexión. Una SA describe todos los parámetros asociados con una conexión en particular, incluye al protocolo IPSec usando ESP/AH/ambos, las llaves de sesiones usadas para encriptar/desencriptar y/o autenticar la información transmitida. En la mayoría de los casos, donde solo un ESP o AH

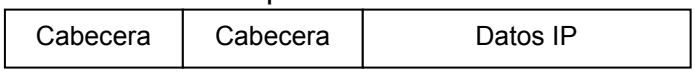
es usado, se crearán dos SA´s por cada conexión, una describiendo el tráfico de entrada, y la otra el de salida. En aquellos casos en que el ESP y el AH son usados en conjunto, se crearán 4 SA´s.

Tanto las conexiones IKE como las IPSec tienen tiempos de vida limitados, descritos en segundos o kilobytes, estos tiempos de vida previenen que una conexión sea usada demasiado tiempo. El tiempo de vida de IPSec es generalmente más corto que el del IKE. Esto permite que las conexiones IPSec generen otra llave simplemente realizando otra negociación.

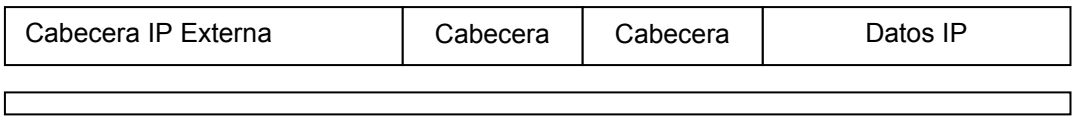
b) **AH *(Authentication Header - Encabezado de Autenticación).-*** Provee integridad para comunicación sin conexión y autenticación del origen de datos para datagramas IP y para protección contra ataques de repetición. AH es un protocolo usado para autenticar un *data stream*. Usa una función criptográfica hash para producir una MAC del dato en el paquete IP, esta MAC es luego transmitida con el paquete, permitiendo al equipo VPN remoto verificar la integridad del paquete original, asegurándose que el dato que no ha sido saboteado en su camino a través de internet.

Paquete IP original

AH en modo transporte



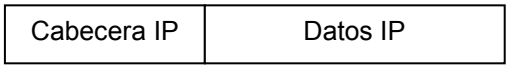
AH en modo túnel



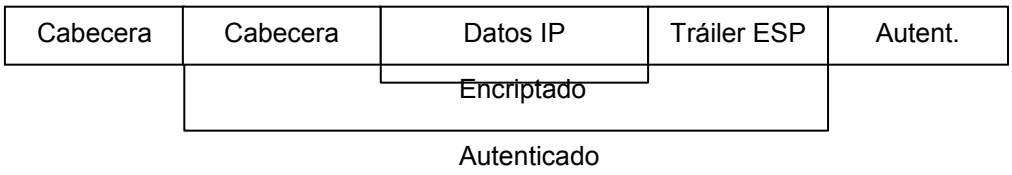
AH provee autenticación para la mayor parte de la información del encabezado IP y para los protocolos del nivel superior; no todos los campos del encabezado IP son protegidos debido a que son modificados en el tránsito. AH puede ser aplicado solo, en combinación con ESP, o de forma anidada a través del uso del modo túnel.

c) **ESP *(Encapsulating Security Payload - Carga Útil de Seguridad de Encapsulación).-*** Se usa en la encriptación y autenticación del paquete IP. Puede también usarse ya sea solo para encriptación o solo para autenticación. La principal diferencia entre la seguridad provista por ESP y AH es el alcance de la protección, ESP no protege ningún campo del encabezado IP, excepto en modo túnel, donde los datos encriptados por ESP corresponden a otro paquete IP.

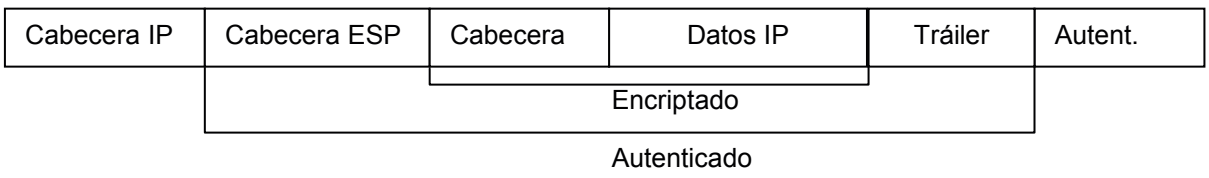
Paquete IP original



ESP en modo transporte



ESP en modo túnel



La diferencia con el AH es que el ESP también proporciona encriptación de los paquetes IP. La fase de autenticación también difiere en que el

ESP sólo autentica los datos después de la cabecera ESP; de manera que la cabecera IP externa queda desprotegida.

d) **NAT trasversal.-** El IKE y los protocolos IPSec no fueron diseñados para operar a través de NAT. Debido a esto, han aparecido los NAT trasversales. El NAT trasversal es un agregado al IKE y protocolos IPSec que permite que operen adecuadamente cuando están siendo nateados.

   El NAT trasversal se divide en:

   a) Adiciones al IKE que permite a ambos IPSec informarse que ellos soportan NAT trasversal y la versión que ellos soportan.

   b) Cambios en la Encapsulación ESP. Si se usa NAT trasversal el ESP es encapsulado en UDP, dando más flexibilidad del NAT.

El NAT trasversal solo se usa si ambos extremos lo soportan. En este caso, el NAT trasversal sabe que un equipo VPN comunica al otro extremo que asimiló el NAT trasversal, y qué versión específica soporta.

Ambos servidores IPSec envían hashes de su propia dirección IP en conjunto con el puerto UDP de origen usada en las negociaciones IKE. Esta información es usada para ver si la dirección IP y puerto origen que cada par usa es el mismo que el otro par ve. Si la dirección y puerto origen no han cambiado, entonces el tráfico no ha sido nateado a lo largo del trayecto, y por lo tanto el NAT trasversal no es necesario. Si la dirección y/o el puerto origen han cambiado, entonces el tráfico ha sido nateado, por lo tanto debe usarse NAT trasversal. Una vez que los pares IPSec han decidido que NAT trasversal es necesario, la negociación IKE se cambia del puerto UDP 500 al 4500.

Otro problema que resuelve el NAT trasversal es que el protocolo ESP es un protocolo IP, no existe información del puerto como TCP y UDP, lo que hace imposible tener más de un cliente nateado conectado al mismo equipo VPN remoto y al mismo tiempo. Debido a esto, los paquetes ESP son encapsulados en UDP. El tráfico ESP-UDP es enviado por el puerto 4500, el mismo puerto usado por IKE cuando se usa NAT trasversal. Una vez que el puerto ha sido

cambiado, todas las comunicaciones IKE siguientes son hechas en el puerto 4500. También se envían periódicamente paquetes para mantener el mapeo NAT activo.[28]

[28] Tema, y subtemas desarrollados a partir de las siguientes fuentes:
http://www.textoscientificos.com/redes/redes-virtuales/vpn
DEC Seguridad Internet y VPN, pág. 46-53 y 75-94, Certificación D-Link

4. Capítulo IV: Implementación y pruebas

4.1. Prueba de las funciones de seguridad del Kypus™ Server Appliance

Kypus es un servidor comercial de red basado en el núcleo de GNU/Linux, proporciona múltiples funciones de administración y seguridad de red, focalizadas a las necesidades de cualquier tipo de organización. Kypus ofrece herramientas intuitivas y fáciles de utilizar, en las cuales se puede administrar una selección amplia de servicios de red en aplicaciones dedicadas. Esta característica de aplicaciones dedicadas puede ser hasta cierto punto una ventaja en comparación a un servidor GNU/Linux o un Windows Server.

Gráfico 4.1. Vista de inicio de una consola de administración Kypus.

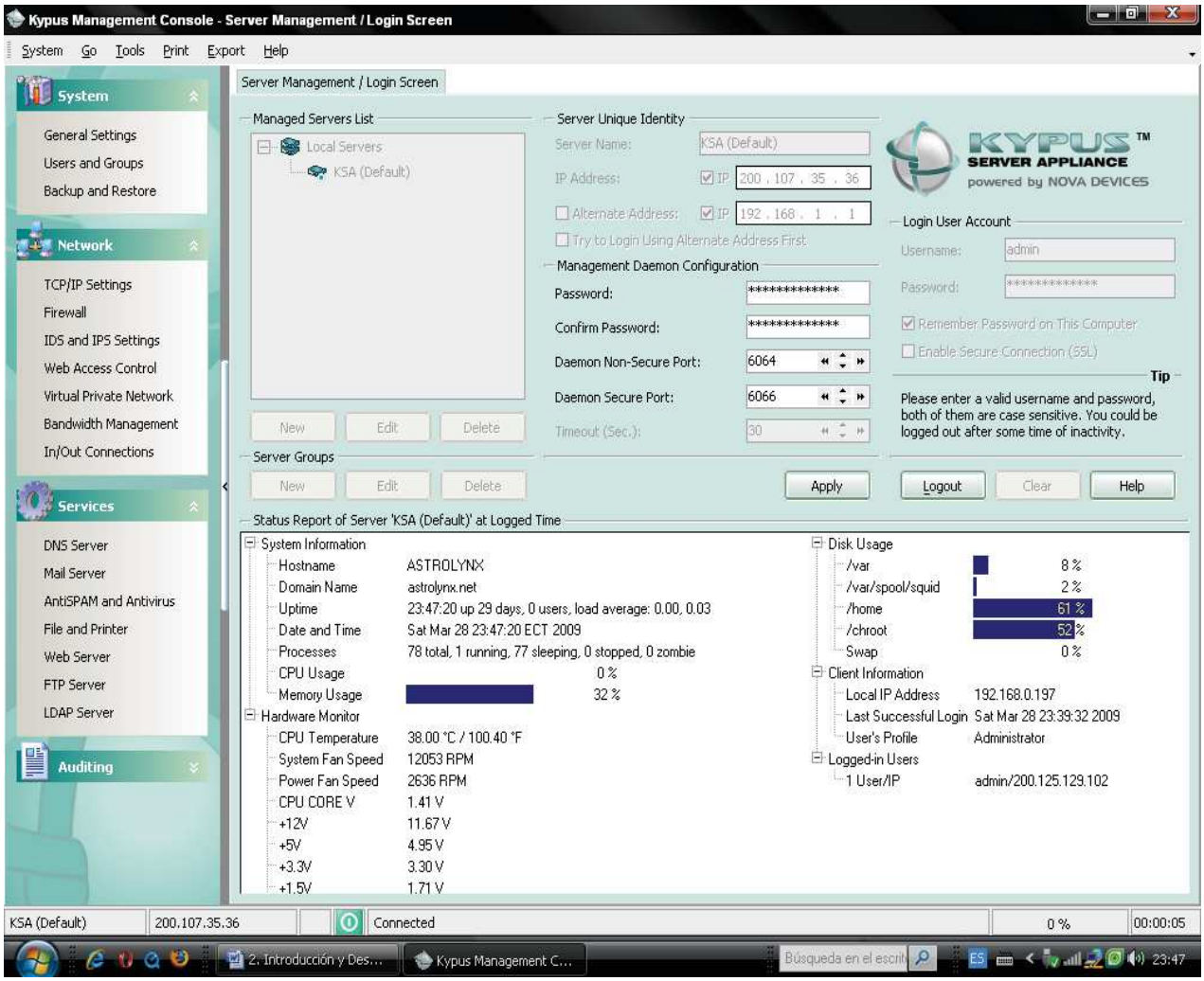


Gráfico obtenido de la consola de administración del servidor Kypus.

Al lado izquierdo se aprecian las aplicaciones de red y de servicios. Una opción interesante es que la consola para la administración de un servidor Kypus se

puede instalar en cualquier computadora de la red de datos. El hecho de que se instale de manera sencilla la consola de entrenamiento del servidor Kypus en un computador, para luego accederlo remotamente mediante internet, demuestra que es una herramienta muy operativa y libre de las complicaciones de espacio y tiempo. El acceso remoto se encuentra bien protegido por las debidas seguridades que por lógica se debe utilizar, esto es el uso de *usuario* y *contraseña,* los mismos que son creados y administrados en el servidor principal de Nova Devices. Para el caso que una organización base su solución en un servidor Kypus, el principio sería el mismo para acceder de manera remota al servidor que propiamente se hallaría ya en la organización.

La aplicación de múltiples funciones de red y seguridad así como servicios, está construida de modo que todas las tecnologías trabajen juntas de la manera más eficiente con una arquitectura extensible que permita que las nuevas capacidades sean agregadas rápida y fácilmente al presentarse la necesidad. Cabe señalar que a pesar de lo sencillo que resulta el manejo de un equipo Kypus, se debe tener un conocimiento previo de redes de datos y seguridad informática. Entre las varias funciones de red y de servicios se tomara aquellas que están enfocadas a proteger la red de datos de una organización y que más interesan a los propósitos de este trabajo. Además el servidor Kypus cuenta con una opción de ayuda en la que se halla la documentación en inglés, donde se describen todas las funciones de administración y seguridad de la red de datos.

4.1.1. *Cortafuegos (Firewall)*

Al momento de probar el cortafuegos del servidor Kypus, se puede ver que las opciones están dispuestas de una manera bastante práctica, lo que permite al administrador tan solo habilitar o deshabilitar las opciones de acuerdo a las necesidades y requerimientos de la red de datos de la organización.

Gráfico 4.2. Vista de inicio de la consola de configuración del cortafuego.

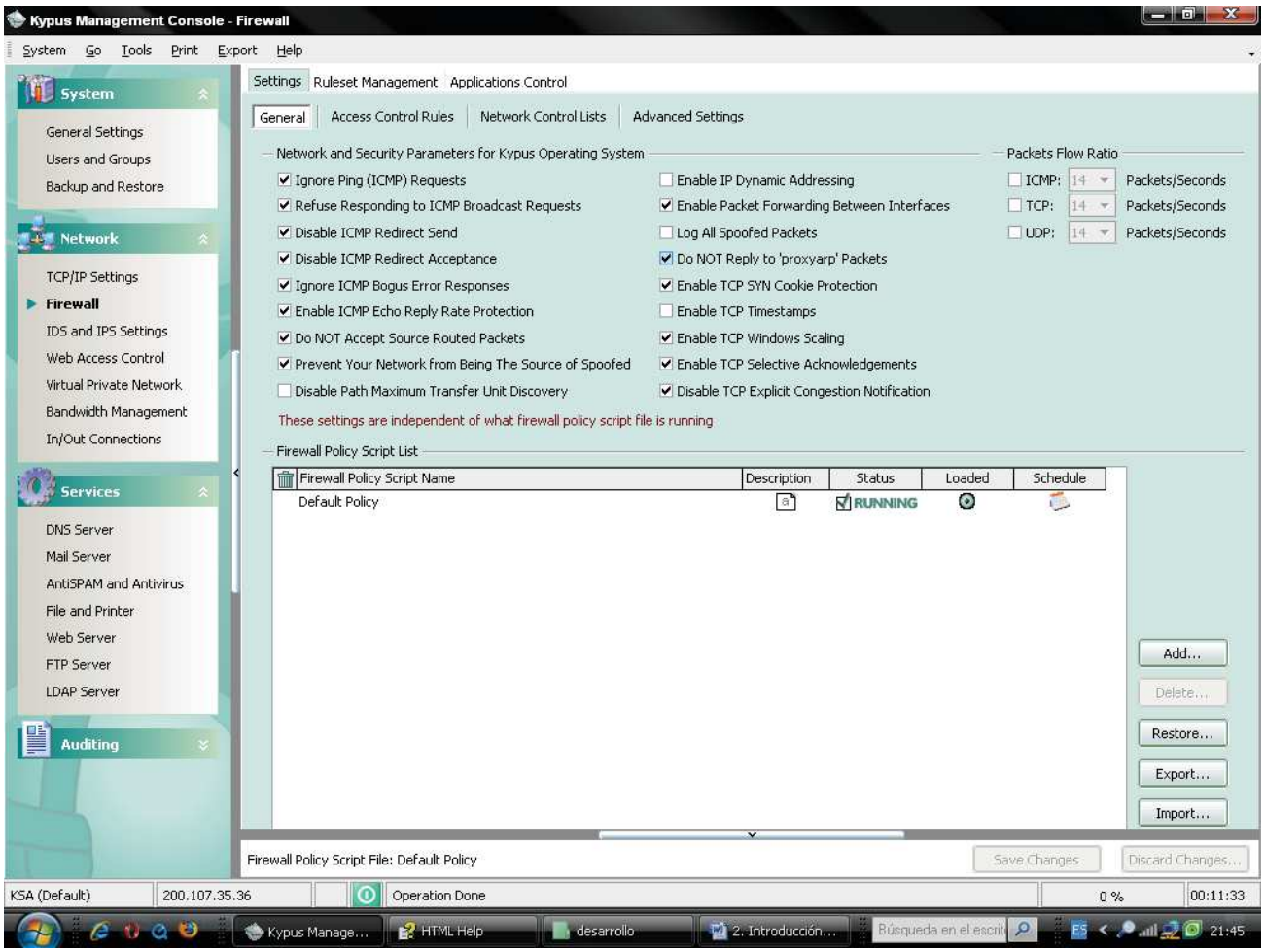


Gráfico obtenido de la consola de administración del servidor Kypus.

El cortafuegos presenta algunas mejoras significativas para la seguridad y rendimiento de la red de datos. Algunos ajustes ya vienen habilitados por defecto, de todos modos la organización es la que debe procurarse una mejor seguridad, insistiendo de nuevo, de acuerdo a sus necesidades y requerimientos.

Llevando a la práctica las funciones del cortafuegos, primero en la pestaña de *Settings-General,* se puede modificar las opciones habilitadas por defecto, observando si algunas son necesarias o no y si se ajustan y cumplen con lo que la red de datos requiere en ese momento, por ejemplo la opción *Ignore Ping (ICMP)Request,* se la puede habilitar para ver que computadora de la red de datos está conectada, si se considera que no es necesario esta opción ya

sea porque con algunas versiones de ping se puede enviar paquetes de forma excesiva; otro ejemplo es la opción *Enable IP Dynamic Addressing, la* cual es aconsejable habilitar si se consigue IP´s dinámicamente. Kypus está pensado para esto, para ajustarse a las necesidades de los usuarios a la vez que ofrece una alta tasa de seguridad para una red de datos.

En el cortafuego en la pestaña de *Settings-Access Control Rules* se puede decidir si se permite el acceso externo a un servidor de aplicación, sea de manera total o limada, mediante una lista de usuarios identificados con una dirección IP, todo esto habiendo definido en *TCI/IP Settings* la lista de anfitriones *(hosts)*. En la pestaña *Settings-Network Control List* se puede crear listas de direcciones IP´s reservadas, privadas, de multicast [29]y listas negras, también se tiene una lista de IP ofensivas, esto es, que son muy dañinas, las cuales se van actualizando automáticamente del internet. En la pestaña *Ruleset Management* se puede agregar, habilitar o deshabilitar las reglas del sistema como las reglas de aplicación; en la pestaña *Aplications Control* se puede decidir a qué tipo de aplicaciones tiene acceso cada usuario.

Es muy importante que se entienda como configurar el cortafuegos para el acceso seguro a internet, esto significa el entendimiento de la tecnología, así como de la filosofía detrás del diseño de este cortafuego, es necesario instruirse sobre la ayuda que proporciona el propio servidor Kypus, pero también puede ser necesario y útil tener ya un conocimiento previo del funcionamiento general de los cortafuegos, de lo contrario es recomendable investigar sobre esto.

4.1.2. *Web Access Control (Control de Acceso Web*)

Es un filtro de internet para supervisar, administrar en forma transparente el uso de internet por parte de los usuarios. El servidor Kypus es proactivo y flexible en la administración del uso de internet en una organización, por ejemplo las descargas de audio y vídeo y las sesiones de chat en flujo

[29] IP Multicast o multidifusión es un método para transmitir datagramas IP a un grupo de receptores interesados.

continuo, requieren de bastante ancho de banda e influyen en la velocidad y rendimiento de la red de datos. Esta función permite bloquear sitios que se consideren no apropiados al menos en las horas de trabajo y así racionalizar el uso del ancho de banda y mejorar el rendimiento de la red de datos.

De esta manera la organización aumenta la productividad de los usuarios, fortalece la seguridad de la red de datos y optimiza el uso de los recursos de TI (Tecnologías de la Información).

Gráfico 4.3. Vista de la consola de configuración del *Control de Acceso Web*.

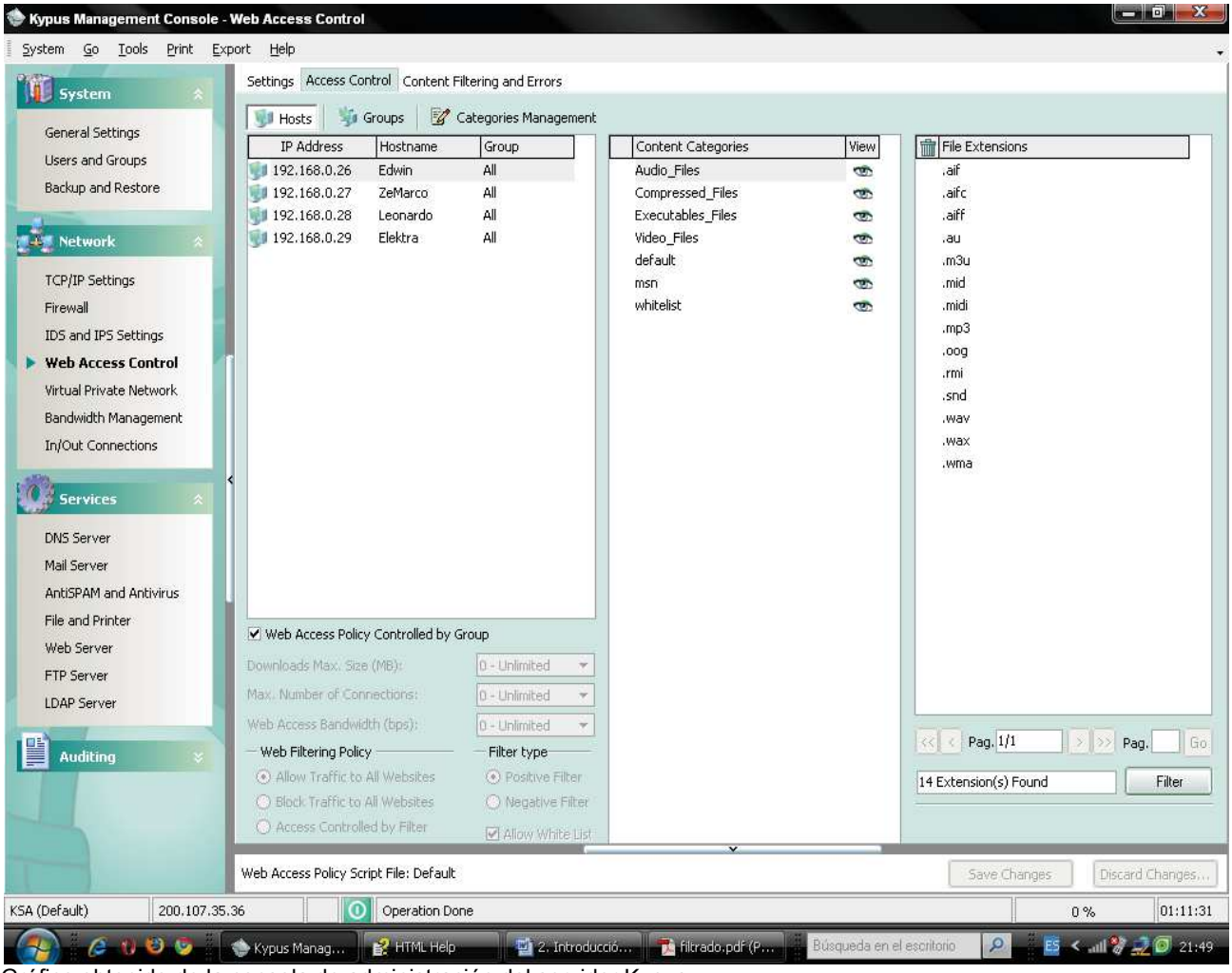


Gráfico obtenido de la consola de administración del servidor Kypus.

En la pestaña *Settings*, se bloquea sitios web *(URL´s)* infectados con *MMC (Mobile Malicious Code - Código Móvil Malicioso)*, bloqueo de spyware, virus caballos de troya, gusanos y otros códigos nocivos.

La pestaña *Access Control* regula la descarga de archivos por nombre, extensión y tipo, incluyendo audio, video e imágenes; se puede extender el filtrado a sitios web que contengan en el *URL* palabras como *sex* o *porn*, hay como establecer políticas de uso por usuario, grupos de usuarios, computadoras o grupo de computadoras, dinamizando el acceso en la organización; los usuarios pueden ser identificados de forma transparente y automática; ciertos usuarios pueden acceder a webs no relacionadas con su trabajo por una cantidad fija de tiempo; se puede implementar el uso de internet por horas del día

En la pestaña *Content Filtering and Errors,* se personaliza la página, incluyendo algún texto o imagen cuando un usuario quiere acceder a una web bloqueada.

En esta función se obtienen reportes generados por horas del día, por webs visitadas, por usuarios, por grupos de usuarios, por computadoras, por grupos de computadoras, por tiempo de navegación. También se programan reportes con entrega automática, sea por día, por semana, por mes, y entregar los mismos a una dirección web preestablecida.

Además esta función protege a la organización de las transmisiones de spyware y captura de teclado *(keyloggers)* a los sitios anfitriones, así como también protege de fraudes como el phishing.

4.1.3. Virtual Private Network (VPN)

Gráfico 4.4. Vista de la consola de configuración del *Virtual Private Network (VPN).*

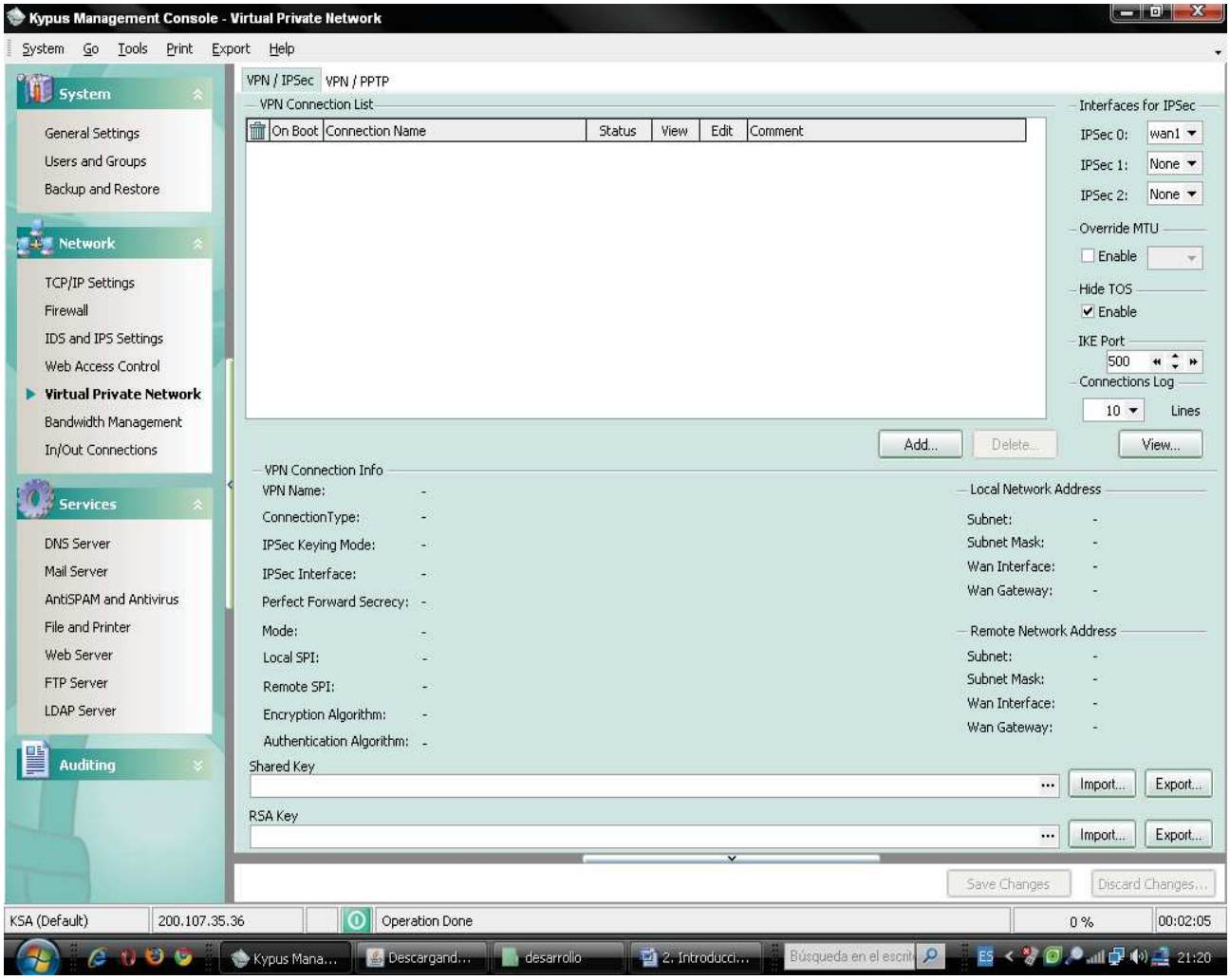


Gráfico obtenido de la consola de administración del servidor Kypus.

El servidor Kypus provee una solución VPN de bajo costo y muy fácil de configurar para organizaciones de todo tamaño y sus sucursales, manteniendo un alta seguridad sin la dependencia constante personal calificado. La funcionalidad VPN del servidor Kypus utiliza normas de la industria como IPSec y PPTP *(ver el capítulo 3, subcapítulo 3.2.4)* dando flexibilidad y garantizando la compatibilidad con otros equipos de otros fabricantes.

El servidor provee soluciones para tres tipos de conexiones:

a) VPN de acceso remoto o cliente-red basado en IPSec.
b) VPN de acceso remoto o cliente-red basado en PPTP.
c) Red-red basado en IPSec.

El servidor Kypus permite crecer a las organizaciones sin la complejidad de las soluciones tradicionales, las cuales involucran varios sistemas de hardware y software cuyos costos directos y de mantenimiento suelen ser altos.

4.1.4. Antispam and Antivirus

El servidor Kypus ofrece protección a nivel de servidor con soporte para analizar el contenido de los correos electrónicos y antivirus, esta herramienta funciona como un cortafuego de correo electrónico. El servidor Kypus es una solución viable para organizaciones que desean incrementar la seguridad de su correo electrónico corporativo.

En la pestaña *Settings* se encuentra el motor antivirusel cual mejora y permite filtrar virus en archivos adjuntos; detener amenazas de correo electrónico para analizar y desactivar scripts HTML, archivos .exe, entre otros; protección contra ataques de denegación de servicio y de diccionario, protección contra ataques de desbordamiento de buffer *(ver el capítulo 2, subcapítulo 2.2)*

En la pestaña *Mail Filtering* se hace la revisión de contenidos de correo electrónico y de archivos adjuntos, escudo frente a abusos para detener las intrusiones de correo electrónico. En la pestaña *SPAM Filtering* se tiene el sistema de protección integrada antispam que incluye filtro bayesiano y chequeo contra listas negras; protección contra ataques de phishing.

Todas estas pestañas interactúan entre sí, es decir que hacen funciones coordinadas, incluyendo a la pestaña *Notices Settings,* la cual notifica el estado

del correo electrónico según las necesidades de seguridad de los usuarios y las circunstancias. [30]

Gráfico 4.5. Vista de la consola de configuración de *Antispam and Antivirus.*

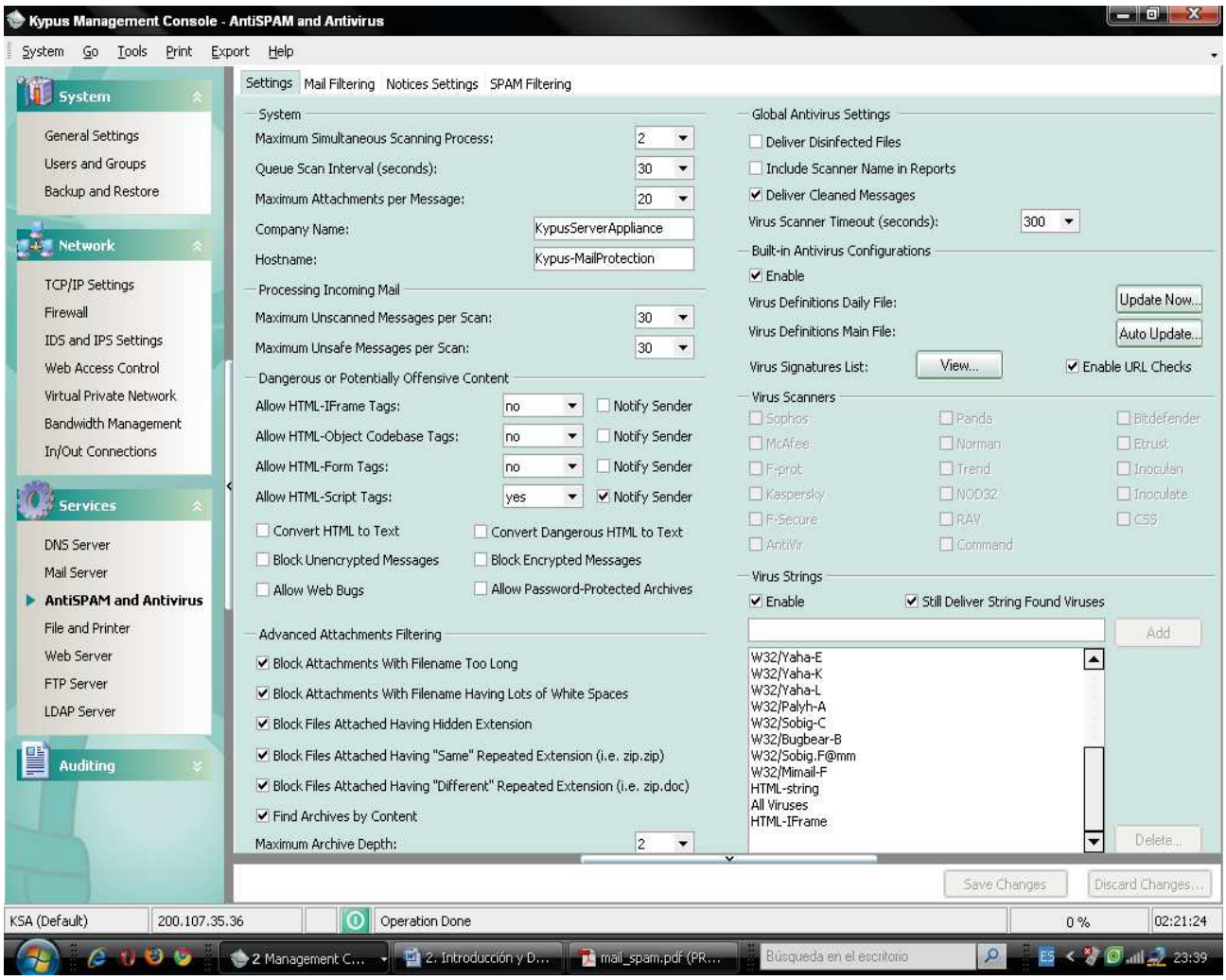


Gráfico obtenido de la consola de administración del servidor Kypus.

4.2. Prueba de las funciones de seguridad del Servidor GNU/Linux

GNU/Linux es un Sistema Operativo gratuito y de libre distribución inspirado en el sistema Unix. Unix fue desarrollado en 1970 por un grupo de empleados de AT&T en los Laboratorios Bell. En 1975 Unix v6 fue difundido y con este código la Universidad de California en Berkeley crea *BSD (Berkeley Software*

[30] Subcapítulo y temas desarrollados a partir de la bibliografía detallada en la pág. 173, en la parte titulada: Sobre Kypus.

Distribution). En 1984 Richard Stallman inicia el proyecto GNU, “GNU no es Unix”, GNU tenía como objetivo la creación de un Sistema Operativo Unix de libre distribución, este proyecto conto con la ayuda de cientos de programadores que hicieron posible, compilador GNU en C (gcc), librerías GNU en C (glinc), Emacs, *Bash(Bourne Again Shell)*. En 1991 en la Universidad de Helsinki, Finlandia, Linus Torvalds escribe la primera versión del núcleo *(kernel en inglés)* de Linux; esto inicio como un proyecto de investigación en un procesador 80386 *(Memory Management Unit: correr varios procesos simultáneamente),* basando el Linux en una pequeña implementación de Unix para PC con fines didácticos llamada Minix y haciendo uso de los avances de GNU y otras herramientas y con la ayuda de varios programadores pudo construir un Sistema Operativo completo. En 1992 aparecen las primeras distribuciones de GNU/Linux, núcleo pre-compilado, compilador C pre-compilado, algunas herramientas pre-compiladas, programas de instalación. La mayoría del software incluyendo su núcleo utiliza la licencia *GPL(GNU Public Licence).*

El solo hecho de tener el código del núcleo abierto es probablemente la más importante contribución para el crecimiento de GNU/Linux y demás software libre. Cualquiera puede obtenerlos, analizarlos y modificarlos; este modelo de desarrollo abierto, que siguen tanto GNU/Linux como la mayoría de las aplicaciones que se ejecutan sobre él, conduce a altos niveles de seguridad.

Es cierto que cualquiera puede acceder al código fuente para encontrar las debilidades, pero no es menos cierto que el tiempo que tarda en aparecer la solución para cualquier debilidad se mide más fácilmente en horas que en días. Gracias a esto, GNU/Linux es conocido por su alto nivel de estabilidad que parte del propio núcleo del Sistema Operativo, lo que propiamente es GNU/Linux.

También desde el inicio del proyecto GNU ya apareció el término *copyleft* en obvia oposición a *copyright*, desde el desarrollo de Linux como tal se mantuvo esta filosofía; bajo *copyleft* es posible copiar el software, obtener el código

fuente, alterar el código fuente y recompilarlo, distribuir el código fuente alterado y obtener ganancias, cambiar la licencia: todos los usuarios deben tener los mismos derechos. De esta manera el movimiento GNU se extendió por la red y empezó a dar sus frutos, y así nació GNU/Linux, línea a línea, programa a programa, el Sistema Operativo del pingüino (la mascota de GNU/Linux, cuyo nombre es Tux) se convirtió en poco tiempo en el producto más famoso de código abierto y, paradójicamente, en la apuesta de más de una multinacional en el sector informático, como IBM, Intel, Corel.

GNU/Linux es un Sistema Operativo multitarea y multiusuario, lo que quiere decir que es capaz de ejecutar varios programas o tareas de forma simultánea y albergar a varios usuarios de forma simultánea. Luego de la instalación original, es posible instalar o desinstalar software sin necesidad de reiniciar todo el sistema, por lo que no se necesita de reinicios frecuentes; no es necesario reiniciar el sistema cada vez que alguien estornuda, por lo que inicia/termina servicios sin afectar o interrumpir otros; es posible cambiar la versión de GNU/Linux y seguir utilizando el mismo software, por lo que el software es portable; si la distribución no posee la aplicación deseada es posible descargarla de internet usando comandos muy simpes como *yum* o *apt*; una vez aprendida la configuración a través de archivos de texto, el usuario puede ajustar el sistema a sus necesidades, por lo que no existe información oculta; el sistema de entorno gráfico X Window (no X Windows) fue desarrollado antes que Microsoft Windows, además los escritorios KDE y GNOME poseen entornos gráficos tan potentes como los de Microsoft.

A pesar que GNU/Linux tiene muchas menos vulnerabilidades en comparación con tecnologías relacionadas con Microsoft, siempre es necesario preocuparse por cualquier computador conectado a internet, por lo que es indispensable seguir buenas políticas de seguridad informática. GNU/Linux puede correr sobre cualquier plataforma como sistemas embebidos, laptops, computadoras de escritorio, megaclusters y supercomputadoras. Cabe aclarar que todas las aplicaciones escritas para GNU/Linux corren en todas las distribuciones.

Además un shell siempre será un shell, porque sin importar la distribución el intérprete de comandos será muy similar

4.2.1. Instalación del Sistema Operativo Linux Ubuntu

Uno de los conceptos principales a tener en cuenta antes de la instalación es la partición. Cada Sistema Operativo organiza la información de los ficheros que contiene de forma diferente, utilizando cada uno su propio sistema de archivos. En ese caso se utilizará Linux Ubuntu 10.04.

Para instalar Linux es necesario arrancar desde el CD/DVD de instalación, es necesario activar en la BIOS la opción para arrancar desde el CD/DVD, o dependiendo de la máquina bastará pulsar F8 o F12. A continuación se presenta de manera concisa los pasos para la instalación de Linux Ubuntu:

1) Escoger si la instalación se hará en modo gráfico o en modo texto. En Linux Ubuntu Server la instalación es solo en modo texto.
2) Escoger el idioma, están disponibles todos los idiomas del mundo.
3) Escoger la zona horaria.
4) Escoger la distribución el teclado.
5) Preparar la partición del disco duro.
6) Configurar usuarios y autenticación, lo cual resulta ser muy intuitivo.
7) Confirmación de los datos.
8) Empieza a instalarse los componentes del Sistema Operativo, en promedio en 20 minutos, pero eso dependerá de la computadora y de la conexión a internet.
9) Luego aparece un cuadro para reiniciar el equipo.
10) Instalar los paquetes.

Cabe destacar que originalmente se instaló la versión Linux Ubuntu 9.04, pero esta versión se ha ido actualizando desde internet a la versión 9.10 y posteriormente a la versión 10.04, si bien no de forma automática porque el Sistema Operativo preguntó mediante el Gestor de Actualizaciones si se

deseaba la actualización a una nueva versión. El proceso de instalación de Linux Ubuntu es sencillo e intuitivo y en general para todas las distribuciones la instalación es cada vez más sencilla, sin embargo es necesario y de mucha importancia aclarar algunos de los pasos de instalación de Linux Ubuntu. Es interesante comentar que en el caso de la distribución de la familia Linux Ubuntu, las actualizaciones de una versión a otra del Sistema Operativo se las hace 2 veces al año, en abril y en octubre, por ejemplo si se tiene la versión Linux/Ubuntu 10.04, el 10 significa el año y el 04 significa el mes de la respectiva actualización, es necesario aclarar que el Sistema Operativo constantemente ofrece actualizaciones de seguridad y de programas independientemente de la versión de Linux Ubuntu instalada. Para poder hacer cualquier tipo de actualización desde el internet, es necesario primero habilitar los repositorios que están en el fichero */etc/apt/sources.list,* borrando los comentarios (#) adelante del *deb* y solamente frente a estas líneas. Un repositorio es la dirección de un servidor de cualquier parte del mundo, el cual sirve para proporcionar actualizaciones y soporte para las distribuciones de GNU/Linux y sus versiones.

En lo referente al paso 5 se puede hacer hasta 4 particiones primarias, mientras que una partición extendida en teoría se puede tener hasta un número ilimitado de particiones lógicas. Una partición principal puede ser utilizada como partición extendida y albergar un número ilimitado de particiones lógicas. GNU/Linux limita el número de particiones lógicas a 59 usando discos duros IDE, y a 11 usando discos SCSI o SATA.

El primer disco IDE en GNU/Linux es /dev/hda, mientras que la primera partición lógica sería /dev/hda5/

El primer disco SCSI en Linux es /dev/sda/, mientras que la primera partición lógica sería /dev/sda5/

Linux/Ubuntu y la mayoría de las demás distribuciones de GNU/Linux definen dispositivos hasta /dev/hda16/, pero si se necesitan más entradas /dev se lo

debe hacer usado el comando *mknod* desde la *terminal*, la cual es el equivalente al *símbolo de sistema* en Microsoft Windows.

En Linux/Ubuntu en la Etapa 4 de 6 de preferencia escogemos la opción *Manual* para particionar el disco. Primordialmente se necesita hacer dos tipos de particiones, estás son:

a) *Swap* (*área de intercambio)*, debe tener el doble de la capacidad de memoria RAM de la máquina. El swap utiliza una parte del disco duro como si fuese una memoria, la finalidad de esta partición es ampliar de forma virtual la memoria de la computadora, almacenando los datos que ya no caben en la memoria RAM física.

b) *Punto principal de montaje*, que es el directorio raíz y que se representa como /. En el punto de montaje cada partición se integra en el sistema de almacenamiento con la finalidad de formar parte de un solo juego de archivos y directorios; esto se consigue asociando una partición con un directorio. Montar una partición significa disponer de su capacidad de almacenamiento comenzando en el directorio especificado. Generalmente esta partición va en el directorio raíz(/). Los directorios van como sigue:
   /
   /home.- es el área de trabajo de todos los usuarios.
   /usr.- (unix system resources), elementos parecidos a los de raíz (/).
   /opt.- registra aplicaciones opcionales.
   /etc.- almacena todos los servicios, configuraciones y demonios del S.O.
   /var.- almacena todo tipo de elementos variables del S.O.
   /bin.- almacena todos los archivos ejecutables del S.O.
   /sbin.- se tienen aplicaciones secundarias del S.O.

4.2.2. Utilidades y comandos básicos para el manejo de la seguridad de red en Linux Ubuntu

En todas las distribuciones de GNU/Linux los comandos son iguales en cuanto a su sintaxis y utilidad, a excepción de pocos comandos de una distribución a otra únicamente la variación es de sintaxis. Más adelante se presentará de forma didáctica la variación de comandos de una distribución a otra. A continuación algunos comandos útiles:

ls.- lista archivos
ls-l.- lista archivos en detalle
ls-la.- lista archivos ocultos
cd.- cambia de directorio, ejemplo: $ cd /etc/X11
cat.- mira el contenido de un archivo, ejemplo: $ cat *nombre de archivo* |more
startx.- visualiza servicio gráfico
touch.- crea nombre de archivos, ejemplo: $ touch *nombre de archivo*
vi.- edita un archivo, ejemplo: $ vi *nombre de archivo*
stop.- detiene los procesos que se están ejecutando
cp.- copia un archivo a otro
adduser.- crea usuarios
mkdir.- crea directorios
rmdir.- borra directorios
hostname.- para saber el nombre de un archivo
testparm.- para saber si hay o no problemas en la configuración del Sistema Operativo
man.- para buscar manuales o servicios, ejemplo: $ man *nombre de archivo*
fdisk –l.- para ver el particionamiento del disco

Cuando se ejecuta el comando *ls* o cualquiera de sus variantes, aparece el tipo de permiso de cada archivo, por ejemplo: -rw-r--r-x, en donde:

-: sin permiso (0)
r: permiso de lectura (4)

w: permiso de grabación (2)
x: permiso de ejecución (1)

Los valores entre paréntesis indican el nivel de importancia de cada letra o carácter, por ejemplo si un archivo estuviera como rwxr--r--, esto quisiera decir que el permiso total equivale a 744. El permiso de un archivo se divide en 3 partes, por ejemplo si se tiene rw-r-x-w-, esto quiere decir:

rw-: permiso del dueño del archivo
r-x: permiso del usuario que pertenece al mismo grupo del dueño del archivo.
-w-: permiso del resto de usuarios globales.

Los comandos que habitualmente se utilizan con estos permisos son:

chown.- para cambiar de dueño de archivo, ejemplo: $ chown root *nombre de archivo*
chmod.- para cambiar los permisos de un archivo, ejemplo: $ chmod 711 *nombre de archivo*

Para ejecutar desde la terminal algún servicio, comando o consola en modo administrador, es decir con la clave del mismo en el caso de Linux Ubuntu de cualquier versión se antepone *sudo*, ejemplo: *sudo gedit*, para consolas. En otras distribuciones como Red Hat Enterprise Linux se utiliza *up2date* y en CenTOS y White Box Enterprise Linux se utiliz*a yum –y*.

La utilidad *sudo gedit* sirve para poder editar, eliminar, agregar, grabar, etc archivos y carpetas en modo gráfico, pero con privilegios de administrador. Esta utilidad se la ejecuta desde la terminal, al igual que para ejecutar junto a un servicio o comando. Cabe aclarar que solo con los comandos que requieren privilegios de administrador se ejecutará *sudo.*

Hay otros comandos que son muy útiles para instalar o desinstalar aplicaciones o programas:

Para instalar, *sudo apt-getinstall nombre del programa.*
Para desinstalar, *sudo apt-get remove nombre del programa*
Para borrar completamente, *sudo apt-get remove --purge nombre del programa.*

4.2.3. Servidor Squid

Squid es un servidor proxy de alto desempeño que se ha venido desarrollando desde hace mucho tiempo y es muy popular y ampliamente utilizado en los Sistemas Operativos GNU/Linux y derivados de Unix. Es muy confiable, robusto y versátil y se distribuye bajo los términos de la Licencia Pública General (GNU/GPL); siendo de código libre, está disponible el código fuente para quien lo requiera. Squid también puede funcionar como caché de contenido de red para los protocolos HTTP, FTP, GOPHER Y WAIS, proxy de SSL, caché transparente, WWCP, aceleración HTTP, caché de consultas DNS y otras más como control de acceso por IP y por usuario, filtro de contenido.

A través de un parámetro: caché_replacement_policy, Squid incluye soporte para los siguientes algoritmos para el caché:

a. ***LRU* (*Least Recently Used- Menos Recientemente Utilizado).-*** En este algoritmo los objetos que no han sido accedidos en mucho tiempo son eliminados primero, manteniendo siempre en el caché a los objetos más recientemente solicitados. Esta política es utilizada por Squid de modo predefinido.

b. ***LFUDA* (*Least Frequently Used with Dynamic Aging- Menos Frecuentemente Utilizado con Envejecimiento Dinámico).-*** Con este algoritmo los objetos más solicitados permanecen en el caché sin importar su tamaño, optimizando la eficiencia (hit rate) por octetos

(bytes) a expensas de la eficiencia misma, de tal forma que un objeto grande que se solicite con mayor frecuencia impedirá que se pueda hacer caché de objetos que se soliciten con menor frecuencia.

c. ***GDSF (Acrónimo de Greedy Dual Size Frequency - Frecuencia de Tamaño Dual Codiciosa).-*** Este algoritmo optimiza la eficiencia (hit rate) por objeto manteniendo en el caché los objetos pequeños más frecuentemente solicitados, de modo que hay mejores posibilidades de lograr respuesta a una solicitud (hit). Tiene una eficiencia por octetos (bytes) menor que el algoritmo LFUDA debido a que descarta del caché objetos grandes que sean solicitados con frecuencia.

   Para poder llevar a cabo los procedimientos de configuración de Squid se recomienda tener previamente configurado el servidor *Samba,* en caso de que el servidor Linux Ubuntu se interconecte con estaciones de trabajo Microsoft Windows. También es necesario tener instalado *Apache,* en este caso se tiene la última versión httpd 2.2.11 ubuntu2, esto como auxiliar de caché con aceleración. También es necesario tener todos los parches de seguridad disponibles para la versión del Sistema Operativo que se esté utilizando.

El servidor Squid en su última versión que se instaló para este trabajo es la 2.7STABLE3-4.1 ubu.

Para el Sistema Operativo Linux Ubuntu 10.04 y versiones anteriores de la familia Linux Ubuntu se ejecuta lo siguiente desde la terminal:
sudo apt-get install squid

A continuación se pide la clave de administrador y se ejecuta el comando.

Para poder ejecutar la descarga de aplicaciones, como la anterior, es necesario tener habilitados los repositorios en el fichero */etc/apt/sources.list.*

Es importante tener actualizado el núcleo del Sistema Operativo por diversas cuestiones de seguridad, se debe actualizar el núcleo a la versión más reciente disponible para la distribución que se esté utilizando, la forma de hacerlo para inux Ubuntu desde la terminal es la siguiente:
sudo apt-get update, y luego
sudo apt-get upgrade

Squid utiliza el fichero de configuración localizado en */etc/squid/squid.conf*, y se podrá trabajar sobre este, el cual es un editor de texto. Existen varios parámetros de los cuales se recomienda configurar los siguientes:

a. http_port
b. cache_mem
c. cache_dir
d. ftp_user
e. Al menos una Lista de Control de Acceso
f. Al menos una Regla de Control de Acceso
g. httpd_accel_host
h. httpd_accel_port
i. httpd_accel_with_proxy

De acuerdo a las asignaciones de la *IANA,* los puertos registrados del rango del 1024 al 49151, recomendados para servidores Proxies pueden ser el 3128 y el 8080 a través de TCP. Por defecto Squid utiliza el puerto 3128 para atender peticiones, sin embargo se puede especificar que lo haga en cualquier otro puerto disponible o bien que lo haga en varios puertos disponibles, siendo así, se pude localizar la sección de definición de *http_port,* y especificar:

#
 # You may specify multiple socket addresses on multiple lines.
#
 # Default: http_port 3128

http_port 3128
http_port 8080

Si se quiere incrementar la seguridad, se puede vincular el servicio a una IP que solo se pueda acceder desde la red local, por ejemplo si el servidor utilizado posee la IP 192.168.0.254, se debe hacer lo siguiente:

#
 # You may specify multiple socket addresses on multiple lines.
#
 # Default: http_port 3128
http_port 192.168.0.254:3128
http_port 192.168.0.254:8080

Una vez terminada una configuración, se ejecuta el siguiente mandato en el terminal para iniciar por primera vez Squid:
sudo /etc/init.d/squid start

Si se necesita reiniciar el servicio para probar hechos en la configuración, se ejecuta en el terminal el siguiente mandato:
sudo /etc/init.d/squid restart
Es necesario establecer *Listas de Control de Acceso* que definan una red o bien ciertas máquinas en particular. A cada Lista se le asignará una *Regla de Control de Acceso* que permitirá o denegará el acceso a Squid.

4.2.3.1. ***ACL (Access Control List – Lista de Control de Acceso).-*** Si se desea establecer una lista de control de acceso que abarque a toda la red local, se define la IP correspondiente a la red y la máscara de la sub-red. Por ejemplo, si se tiene una red donde las máquinas tienen direcciones IP 192.168.1.**n** con máscara de sub-red 255.255.255.0, se puede utilizar lo siguiente:
acl redlocal src 192.168.1.0/255.255.255.0

También se puede definir una Lista de Control de Accesoespecificando un fichero localizado en cualquier parte del disco duro, el cual contiene una lista de direcciones IP:
acl permitidos src "/etc/squid/permitidos"

El fichero */etc/squid/permitidos*a manera de ejemplo contendría lo siguiente:

192.168.1.1
192.168.1.2
192.168.1.4
192.168.1.17
192.168.1.19
192.168.1.22
192.168.1.35

Lo anterior estaría definiendo que la Lista de Control de Accesodenominada permitidosestaría compuesta por las direcciones IP incluidas en el fichero */etc/squid/permitidos.*

4.2.3.2. Reglas de Control de Acceso.- Estas definen si se permite o no el acceso hacia Squid. Se aplican a las Listas de Control de Acceso. Deben colocarse en la sección de reglas de control de acceso definidas por el administrador, es decir, a partir de donde se localiza la siguiente leyenda:

#
 # INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#

En el siguiente ejemplo se considera una regla que establece acceso permitido a Squid a la Lista de Control de Acceso denominada *“permitidos”*:

http_access allow permitidos

También pueden definirse reglas valiéndose de la expresión: la cual significa no. Pueden definirse, por ejemplo, dos listas de control de acceso, una denominada lista1 y otra denominada lista2, en la misma regla de control de acceso, en donde se asigna una expresión a una de estas. La siguiente establece que se permite el acceso a Squid a lo que comprenda lista1 excepto aquello que comprenda lista2:

http_access allow lista1 !lista2

Este tipo de reglas son útiles cuando se tiene un gran grupo de IP dentro de un rango de red al que se debe permitir acceso, y otro grupo dentro de la misma red al que se debe denegar el acceso.

Una vez comprendido el funcionamiento de la Listas y las Regla de Control de Acceso, se procede a determinar cuáles utilizar para la configuración.

Caso 1.

Considerando como ejemplo que se dispone de una red *192.168.1.0/255.255.255.0*, si se desea definir toda la red local, se utilizara la siguiente línea en la sección de Listas de Control de Acceso:

acl todalared src 192.168.1.0/255.255.255.0

Habiendo hecho lo anterior, la sección de Listas de Control de Acceso debe quedar del siguiente modo:

#

 # Recommended minimum configuration:

acl all src 0.0.0.0/0.0.0.0

acl manager proto cache_object

acl localhost src 127.0.0.1/255.255.255.255

acl todalared src 192.168.1.0/255.255.255.0

A continuación se procede a aplicar la Regla de Control de Acceso:
http_access allow todalared

Habiendo hecho lo anterior, la zona de Reglas de Control de Acceso queda de este modo:
#
 # INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
http_access allow localhost
http_access allow todalared
http_access deny all
La regla *http_access allow todalared*permite el acceso a Squid a la Lista de Control de Acceso denominada *todalared*, la cual está conformada por *192.168.1.0/255.255.255.0*. Esto significa que cualquier máquina desde *192.168.1.1* hasta *192.168.1.254* podrá acceder a Squid.

Caso 2.

Si solo se desea permitir el acceso a Squida ciertas direcciones IP de la red local, se debe crear un fichero que contenga dicha lista. Se debe Generar el fichero */etc/squid/listas/redlocal*, dentro del cual se incluirán solo aquellas direcciones IP que se desea conformen la Lista de Control de acceso:

192.168.1.1
192.168.1.2
192.168.1.4
192.168.1.17
192.168.1.19
192.168.1.22
192.168.1.35

Denominaremos a esta lista de control de acceso como redlocal:
acl redlocal src "/etc/squid/listas/redlocal"

Habiendo hecho lo anterior, la sección de Listas de Control de Acceso debe quedar del siguiente modo:
#
 # Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl redlocal src "/etc/squid/listas/redlocal"

A continuación se procede a aplicar la Regla de Control de Acceso:
http_access allow redlocal

Habiendo hecho lo anterior, la zona de Reglas de Control de Acceso queda de este modo:

#
 # INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
http_access allow localhost
http_access allow redlocal
http_access deny all

La regla *http_access allow redlocal*permite el acceso a Squid a la Lista de Control de Acceso denominada *redlocal*, la cual está conformada por las direcciones IP especificadas en el fichero */etc/squid/listas/redlocal*. Esto significa que cualquier máquina no incluida en */etc/squid/listas/redlocal*no tendrá acceso a Squid.Finalmente bastará reiniciar Squid para que tomen efecto los cambios y se puedan hacer pruebas.

4.2.3.3. Restricciones y permisos a sitios web.- Denegar el acceso a ciertos sitios web permite hacer un uso más racional del ancho de banda. El funcionamiento es verdaderamente simple, y consiste en denegar el acceso a nombres de dominio o sitios Web que contengan patrones en común, como por ejemplo:
www.sitioporno.com
www.sitioindeseable.com
napster
porn
sex
xxx
warez

Esta lista, la cual deberá ser completada con todas las palabras y sitios web que el administrador considere pertinentes, se la guardará como */etc/squid/sitios-denegados*.

Se debe definir una Lista de Control de Accesoque a su vez defina al fichero */etc/squid/sitios-denegados*. Esta lista se la llama como *"sitiosdenegados"*. De modo tal, la línea correspondiente quedaría del siguiente modo:
acl sitios-denegados url_regex "/etc/squid/sitios-denegados"

Hecho lo anterior, de debe tener en la sección de Listas de Control de Accesolo siguiente:

 # Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl redlocal src 192.168.1.0/255.255.255.0
acl sitios-denegados url_regex "/etc/squid/sitios-denegados"

A continuación se especifica una Regla de Control de Accesoexistente agregando con un símbolo de *!* que se denegará el acceso a la Lista de Control de Accesodenominada "*sitios-denegados"*:
http_access allow redlocal !sitios-denegados

Cabe aclarar que la Regla de Control de Acceso también puede quedar:
http_access deny sitios-denegados

Cualquiera de las dos Reglas anteriores permite el acceso a la Lista de Control de Accesodenominada *redlocal*, pero niega el acceso a todo lo que coincida con lo especificado en la Lista de Control de Accesodenominada *sitios-denegados*.

Habiendo hecho lo anterior, la zona de Reglas de Control de Acceso queda de este modo:
#
 # INSERT YOUR OWN RULE(S) HERE TO allow ACCESS FROM YOUR CLIENTS
#
http_access allow localhost
http_access allow redlocal !sitios-denegados
http_access deny all

Si por ejemplo el incluir una palabra en particular afecta el acceso a un sitio web, también puede generarse una lista de dominios o palabras que contengan un patrón que se considere como apropiados.Se va a suponer que dentro de la Lista de Control de Accesode sitios denegados está la palabra *sex*, esta denegaría el acceso a cualquier nombre de dominio que incluya dicha cadena de caracteres, como
www.extremesex.com. Sin embargo también estaría bloqueando a sitios como www.sexualidadjoven.com, el cual no tiene que ver con pornografía, sino

orientación sexual para la juventud. Podemos añadir este nombre de dominio en un ficheros que denominaremos */etc/squid/sitios-permitidos*.

Este fichero será definido en una Lista de Control de Accesodel mismo modo en que se hizo anteriormente con el fichero que contiene dominios y palabras denegadas.
acl sitios-permitidos url_regex "/etc/squid/sitios-permitidos"

Se especifica la Regla de Control de Acceso:
http_access allow sitios-permitidos

La regla anterior especifica que se denegará el acceso a todo lo que comprenda la Lista de Control de Accesodenominada sitios-*denegados* exceptolo que comprenda la *Lista* de Control de Accesodenominada *sitios-permitidos* es decir, se podrá acceder sin dificultad a www.sexualidadjoven.com manteniendo la restricción para la cadena de caracteres *sex*.

Solo bastará reiniciar Squid para que tomen efecto los cambios y se pueda hacer pruebas:
sudo /etc/init.d/squid restart

4.2.3.4. Restricción de acceso por extensión.- Denegar el acceso a ciertos tipos de extensiones de fichero permite hacer un uso más racional del ancho de banda. El funcionamiento es verdaderamente simple, y consiste en denegar el acceso a ciertos tipos de extensiones que coincidan con lo establecido en una Lista de Control de Acceso.

Lo primero será generar en un editor de texto una lista con las extensiones a bloquear:

\.avi
\.mp4

\.mp3
\.mpg
\.mpeg
\.mov
\.rar
\.ram
\.rm
\.rpm
\.vob
\.wma
\.wmv
\.wav
\.doc
\.mbd
\.ace
\.bat
\.exe
\.lnk
\.pif
\.scr
\.sys
\.zip

Esta lista, deberá ser completada con todas las extensiones de fichero que el administrador considere pertinentes se la guardara como */etc/squid/lista-extensiones*.

Se debe definir una Lista de Control de Accesoque a su vez defina al fichero */etc/squid/lista-extensiones*. Esta lista se denominará como *"lista-extensiones"*. La línea correspondiente quedaría así:
acl lista-extensiones urlpath_regex "/etc/squid/lista-extensiones"

Hecho lo anterior, se debe tener en la sección de Listas de Control de Accesolo siguiente:

#
 # recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl redlocal src 192.168.1.0/255.255.255.0
acl sitios-denegados url_regex "/etc/squid/sitios-denegados"
acl lista-extensiones urlpath_regex "/etc/squid/lista-extensiones"

A continuación se especifica una Regla de Control de Accesoexistente agregando con un símbolo de *!* que se denegará el acceso a la Lista de Control de Accesodenominada "*lista-extensiones"*:
http_access allow redlocal !lista-extensiones

Cabe aclarar que la Regla de Control de Acceso también puede quedar:
http_access deny lista-extensiones

Cualquiera de las dos Reglas anteriores permite el acceso a la Lista de Control de Accesodenominada *redlocal*, pero niega el acceso a todo lo que coincida con lo especificado en la Lista de Control de Accesodenominada *lista-extensiones*.

Habiendo hecho lo anterior, la zona de Reglas de Control de Acceso queda de este modo:
#
 # INSERT YOUR OWN RULE(S) HERE TO allow ACCESS FROM YOUR CLIENTS
#
http_access allow localhost

http_access allow redlocal !sitios-denegados !lista-extensiones
http_access deny all

Solo bastará reiniciar Squid para que tomen efecto los cambios y se pueda hacer pruebas:
sudo /etc/init.d/squid restart

4.2.3.5. Restricción de acceso por horario.- Denegar el acceso en ciertos horarios permite hacer un uso más racional del ancho de banda. El funcionamiento es verdaderamente simple, y consiste en denegar el acceso en horarios y días de la semana.

Los días de la semana se definen con letras, las cuales corresponden a la primera letra del nombre en inglés, de modo que se utilizarán del siguiente modo:

S - Domingo
M - Lunes
T - Martes
W - Miércoles
H - Jueves
F - Viernes
A - Sábado
Por ejemplo:

acl clase-matutina time MTWHF 09:00-14:00
acl horario-matutino time MTWHF 09:00-14:00
Esta regla define que los miembros de la Lista de Control de Acceso denominada *clase-matutina* tengan permitido acceder al internet en un horario que se denomina *horario-matutino,* el cual es una lista que comprende un horario de 09h00 a 14h00 de lunes a viernes.

En la Regla de Control de Acceso se permite o se deniega el acceso en el horario definido en la Lista de Control de Acceso:
http_access allow horario-matutino clase-matutina

Lo anterior significa que quienes conformen *clase-matutina* podrán acceder a internet de lunes a viernes de 09h00 a 14h00 horas.

4.2.3.6. ClamAV.- Es un guión auxiliar para Squid, para examinar contenido en busca de virus para una lista de extensiones definidas. El guión se encarga de la petición tal y como es solicitada hacia Squid, examinando esta en busca de virus. Es un antivirus *open source* (GPL) cuyo principal objetivo es la integración con servidores de correo (análisis de ficheros adjuntos).

ClamAV tiene las siguientes características:

a) Distribuido bajo los términos de GPL/GNU.
b) Cumple con las explicaciones de la familia de normas POSIX (Portable Operating System Interface for UNIX – Interfaz Portable de Sistemas Operativo para UNIX).
c) Exploración rápida.
d) Detecta más de 44.000 virus, gusanos y troyanos incluyendo virus para Windows
e) Capacidad para examinar contenido de ficheros.
f) Soporte para explorar ficheros comprimidos.
g) Avanzada herramienta de actualización con soporte para firmas digitales y consultas basadas sobre DNS.
   ClamAV se puede instalar desde la terminal:
   sudo apt-get install clamav

El fichero en el que se almacena es */etc/clamav/clamd.conf.*

ClamAV se puede ejecutar en línea de comandos. Para ejecutar un escaneo bajo demanda, se debe ejecutar el comando:
clamscan –r /home

Para estar seguros de que se está ejecutando, se ejecuta en una consola el comando:
ps-ef\grep clam

y se verá que hay un proceso ejecutando llamado *"freshclam"* del tipo:
/usrbin/freshclam –p /var/run/clamav/freshclam.pid –d –quiet

Si se desea ejecutar ClamAV de forma gráfica y después de haberlo instalado como se indica arriba, se ejecuta en la terminal lo siguiente:
sudo apt-get install klamav

Aunque el Sistema Operativo GNU/Linux es casi invulnerable a todo tipo de virus y otras amenazas programadas, en comparación con otros Sistemas Operativos como Windows, siempre hay la posibilidad de que pase algún tipo de amenaza, aunque sea una de cada mil. Dadas las características de GNU/Linux, ClamAV se mantiene poco operativo en cuanto a detectar virus y otras amenazas, lo cual no quiere decir que no estese alerta ante cualquier posible amenaza y que no se actualice automáticamente.

4.2.4. Servidor de correo electrónico Postfix

Postfix es un *MTA(Mail Transport Protocol – Protocolo de Transporte de Correo),* y es la versión libre de *Secure Mailer* de IBM. Postfixfue desarrollado como un reemplazo para *Sendmail,* el cual posee un mal historial en seguridad, en cambio Postfix es menos complicado de configurar, es más rápido, fácil de administrar y seguro. Postfix trabaja por defecto dentro de una *jaula(chroot)* localizada en */var/spool/Postfix,* y por tal motivo es todavía más seguro

reduciendo enormemente los riesgos para la red de datos y todos sus sistemas, en el caso del surgimiento de una vulnerabilidad.

Se puede instalar Postfix desde Synaptic o desde la terminal como sigue:
sudo apt-get install postfix

Y se instala la versión *postfix 2.5.5-1.1*, en el fichero */etc/Postfix,* el fichero principal de configuración es *main.conf.*

Se puede acceder al correo utilizando los protocolos IMAP o POP3 gracias a Dovecot. Se instala mediante:
sudo apt-get install dovecot-pop3d
sudo apt-get install dovecot-imapd
Dado que se recomienda un acceso cifrado (IMAP/POP3), se crean los certificados necesarios:

mkdir /etc/dovecot/ssl
cd /etc/Dovecot/ssl
openssl req-new –x509 –nodes –out dovecot.pem –keyout dovecot.pem –days 3650

Ahora se configura Dovecot editando */etc/dovecot.conf*, se indica que se quiere activar los protocolos IMAPs y POP3s (cifrados).

protocols = pop3
listen = *
pop3_uidl_format = %08Xu%08Xv
disable_plaintext_auth = no

Para activarlo:
dovecot - -exec-mail pop3
Se reinicia el servicio:

/etc/init.d/dovecot start

Ahora ya es posible acceder al correo mediante un cliente. Si se utiliza el protocolo POP3 el correo se bajará a la máquina y se eliminará del servidor, sin embargo, si se usa IMAP se podrá acceder a los correos de forma remota, conservándose en el servidor.

Ahora se instala los protectores colaborativos contra spam, Pyzor y Razor. Ambos calculan un hash del mensaje y consultan a un servidor de internet si corresponde a un mail de publicidad. Este paso es opcional.

sudo apt-get install pyzor

sudo apt-get install razor

Se instala el bloqueador de correo basura spamassassin:

sudo apt-get install spamassassin

Las siguientes son funciones adicionales de Postfix:

a) Recepción de un mensaje dirigido a un alias de usuario:
   Añadir alias de usuario en /etc/aliases

b) Recepción de un mensaje dirigido a un alias de una lista:
   Envío a un conjunto de usuarios de una lista
   Crear lista en fichero de alias /etc/aliases

c) Recepción de un mensaje dirigido a una dirección falsa.

d) Rechazar el envío de un mensaje a un usuario externo:
   relayhosts =
   mynetworks = 127.0.0.0/8

e) Rechazar el envío de un mensaje de spam enviado porun usuario vetado:
   Crear tabla hash sender_access

Cambiar en Postfix
smtp_sender_restrictions = check_sender_access
hash:/etc/postfix/sender_access

f) Rechazar el envío de un mensaje de spam dirigido a unusuario vetado:
Conexión rechazada con el campo rcpt to:
Tabla hash recipient_access
smtp_recipient_restrictions = check_recipient_access
hash:/etc/postfix/recipient_access

g) Rechazar un mensaje de spam con la palabra xxx en el Subject:
Crear el fichero header_check
Añadir en main.cf
header_checks =regexp:/etc/postfix/header_check

h) Rechazar un mensaje de spam con la palabra xxx en el Body:
Crear el fichero body_check
body_checks = regexp:/etc/postfix/body_check

Postfix utiliza SASL para la autenticación de usuarios, por tanto se debe instalar los ejecutables que gestionan SASL:
sudo apt-get install sasl2-bin

Se descomenta de */etc/default/saslauthd* la línea:
START = yes
Se inicia el demonio:
/etc/init.d/saslauthd start

Ya se puede probar el envío de correos con algún cliente, desde el cual se podrá especificar que el servidor SMTP requiere autenticación.[31]

[31] Subcapítulo y temas desarrollados a partir de la bibliografía detallada en la pág. 172 - 173, en la parte titulada: Sobre Linux.

5. Capítulo V: Conclusiones y Recomendaciones

5.1. Conclusiones:

1) La seguridad informática, que incluye a la seguridad computacional y a la seguridad de redes, permite proteger a la información de cualquier tipo de amenaza interna o externa.

2) Contrario a lo que en algunas organizaciones puedan creer, la implementación de una política de seguridad informática no representa gasto innecesario alguno, por el contrario ayuda a optimizar recursos y ahorrar costos.

3) La implementación de una política de seguridad informática exige analizar todo el sistema informático para dar el debido valor a la información, a los Sistema Operativos y al software de aplicación, así como al hardware y demás dispositivos de la red de datos.

4) Debido a que siempre existirá la posibilidad de que alguien ingrese sin autorización a una red de datos y la manipule a su conveniencia y antojo, las diferentes tecnologías criptográficas aportan la solución más adecuada para minimizar el riesgo de intrusión.

5) Kypus a pesar de que está basado en el núcleo de Linux es un servidor comercial que posee herramientas de red más intuitivas que un servidor Linux Ubuntu, debido a que solo basta con un solo clic para habilitar o deshabilitar una opción.

6) Kypus es un servidor que ya viene integrado con su propio hardware, el mismo que viene adecuado para el tamaño y necesidad de cada organización, en cada uno de sus modelos, *ver sub numeral 3.9 del Anexo 1.*

7) La consola de administración de un servidor Kypus se la puede instalar en cualquier computadora de la red de datos, como un programa más del Sistema Operativo anfitrión.

8) Todas las funciones de seguridad y administración de redes ya vienen integradas en el servidor Kypus, conjuntamente con sus manuales, además Kypus es más sencillo de configurar que Linux Ubuntu; *ver sub numeral 3.9 del Anexo 1.*

9) En un servidor Kypus las actualizaciones de servicios y seguridades desde internet son automáticas en cambio en un servidor Linux Ubuntu son semiautomáticas porque el sistema avisa al administrador cuando hay actualizaciones disponibles, y el administrador con el ingreso de la contraseña procede a descargar gratuitamente las actualizaciones.

10) El servidor Linux Ubuntu al ser instalado no viene con la mayoría de aplicaciones de red ni sus manuales, estas se las descarga gratuitamente desde internet.

11) Linux Ubuntu puede ser instalado en casi cualquier tipo de máquina, en cuanto a sus características técnicas se refiere, sin embargo dependerá del tamaño y necesidades de una organización para escoger el hardware adecuado e instalar el Sistema Operativo; *ver sub numerales 2.2 y 2.3 del Anexo 1.*

12) Tanto el servidor Linux como el servidor Kypus ofrecen funciones de red importantes como VPN y Cortafuegos, lo cual ayuda a reducir el costo en equipos extras con estas funciones; *ver sub numerales 1.3, 2.1 y 3.1 del Anexo 1.*

13) Tanto Linux Ubuntu como Kypus ofrecen la seguridad de la contraseña por defecto para iniciar el servidor, lo cual es algo fundamental en un sistema basado en Unix.

14) En ambos servidores se debe tener una contraseña robusta, para evitar que sea descubierta por posibles atacantes, sin embargo en Kypus se ingresa una vez la contraseña para acceder a todos los servicios del sistema, mientras que en Linux Ubuntu pide la contraseña no solo para el acceso inicial, sino cuando se quiere acceder y hacer cambios en archivos importantes del sistema, para hacer descargas y actualizaciones.

15) Tanto Linux Ubuntu y Kypus tienen el debido soporte continuo de las organizaciones que los respaldan, Canonical y Nova Devices, sin embargo Linux Ubuntu también recibe el aporte de la comunidad a nivel mundial; *ver sub numeral 3.3 del Anexo 1.*

16) En las pruebas hechas a los servidores Linux Ubuntu y Kypus, ambos ofrecen óptimas seguridades y ambos en general se adaptan a las necesidades de cada organización, *ver sub numerales 2.1, 3.1 y 3.7 del Anexo 1.*

17) A pesar de que ambos ofrecen óptimas seguridades, Linux Ubuntu es más amplio que Kypus, en cuanto a la variedad de aplicaciones y servicios que ofrece, un ejemplo es el servidor LAMP (**L**inux, **A**pache, **M**ySQL, **P**HP), además se pueden instalar y ejecutar en una gran cantidad de variantes Unix; *ver sub numeral 3.5 del Anexo 1.*

18) Si a los servidores Linux Ubuntu y Kypus se los compara con un Windows Server, el costo de implementar ambos es mucho más reducido que Windows Server, porque las aplicaciones de red en ambos están libres de costosas licencias; *ver sub numerales 1.3, 3.1 y 3.6 del Anexo 1.*

19) El servidor Kypus en general tiene la ventaja de costos más bajos a mediano y largo plazo, facilidad de instalación, de administración e implementación de servicios y de tener modelos específicos para pymes y SOHO, lo que reduce el nivel de dependencia de personal calificado, todo esto se debe a la propia arquitectura tanto del hardware como del software que ya vienen integrados en el servidor; *ver sub numerales 1.3, 3.7, 3.9 y 3.10 del Anexo 1.*

20) Aunque el Sistema Operativo Linux Ubuntu es muy robusto y sus aplicaciones y servicios son más variados y se los descarga con facilidad desde internet, el costo del hardware y de la configuración de los servicios se incrementará mientras más grande sea la organización o mientras más servicios requiera, lo cual mantiene un cierto nivel de dependencia de personal calificado; *ver sub numerales 1.3 y 3.10 del Anexo 1.*

5.2. Recomendaciones:

1) Toda organización de cualquier actividad y tamaño, debe implementar políticas de seguridad informática claras y precisas, acorde a sus necesidades; ninguna organización debe pasar por alto la importancia de esto.

2) Las organizaciones deben actualizar periódicamente sus políticas de seguridad informática, debido a los avances tecnológicos, desarrollos de nuevos servicios, la aparición de nuevas amenazas, entre otras.

3) Las políticas de seguridad informática deben ser claras y comprensibles para todos los integrantes de una organización, sin restar precisión y eficacia en su aplicación, además para su implementación deben cumplir con ciertos estándares de seguridad y calidad; *ver Anexo 2.*

4) Todos los integrantes de una organización deben ser concientizados y capacitados sobre el manejo y la importancia de los recursos y la información que componen un sistema informático.

5) Dependiendo del tipo de organización y del tipo de información que manejen, los distintos tipos de ataques representan más riesgo para ciertas organizaciones que para otras, sin embargo toda organización sin excepción debe manejar cierto nivel de riesgo de ataques.

6) En las organizaciones, los responsables de sistemas y redes siempre deben estar actualizados de las nuevas vulnerabilidades que aparecen en los sistemas informáticos, de la aparición de nuevas amenazas y de las nuevas herramientas para combatir las mismas, por ejemplo hay que mantener actualizados los Sistemas Operativos servidores y clientes con los parches de seguridad proporcionados por el fabricante.

7) Toda organización de acuerdo a sus necesidades y requerimientos, debe usar algún tipo de cortafuegos para protegerse y reducir el riesgo de ataques.

8) Es muy importante que en las organizaciones se esté al tanto de los métodos de encriptación y autenticación para la protección de la información, para poder aplicarlos con eficiencia y eficacia de acuerdo a las necesidades y requerimientos.

9) Es necesario tener instalado y actualizado un antivirus en todas las computadoras de una red de datos, siendo recomendable que este estese en el rango de los 10 mejores antivirus, esto se lo puede verificar en los motores de búsqueda; también es recomendable tener las funcionalidades completas y una licencia a largo plazo, tener instalada una versión comercial a una gratuita de un antivirus, al menos en los Sistemas Operativos Windows.

10) Se recomienda ignorar y borrar correos electrónicos que supuestamente provienen de ciertas organizaciones financieras y comerciales, en los mismos que se pide ciertos datos confidenciales como # de cuentas bancarias, # de tarjetas de crédito o débito, claves de uso bancario, etc., este tipo de organizaciones no pide estos datos a sus clientes y tienen procedimientos diferentes para verificar los datos de los mismos, al recibir este tipo de correos electrónicos hay la segura intención de estafar.

11) Se recomienda mantener actualizado el hardware a través del *firmware,*[32] al menos los dispositivos y periféricos que sean actualizables. Se

[32] Firmware o programación en firme, es un bloque de instrucciones de programa para propósitos específicos, grabado en una memoria de tipo no volátil (ROM, EEPROM, flash, etc.), que establece la lógica de más bajo nivel que controla los circuitoselectrónicos de un dispositivo de cualquier tipo. Al estar integrado en la electrónica del dispositivo es en parte hardware y en parte software. Funcionalmente, el firmware es el intermediario (interfaz) entre las órdenes externas que recibe el dispositivo y su electrónica, debido a que es el encargado de controlar a ésta última para ejecutar correctamente dichas órdenes externas. *Definición tomada de:* http://es.wikipedia.org/wiki/Firmware.

encuentra firmware en memorias ROM de los sistemas de diversos dispositivos periféricos, como en monitores de video, unidades de disco, impresoras, BIOS de una computadora etc., pero también en los propios microprocesadores, chips de memoria principal y en general en cualquier circuito integrado.

12) En general se recomienda utilizar el servidor Linux Ubuntu donde se requiera de una gran variedad de aplicaciones sin embargo se debe tomar en cuenta el hardware a ser utilizado, ya que este factor puede incrementar el costo de la solución; *ver sub numerales 1.1, 2.2, 3.1 y 3.5 del Anexo 1.*

13) Se recomienda instalar un servidor KYPUS donde se requiera facilidad de administración y seguridad y no sea necesario la instalación de software adicional; ve*r sub numerales 1.1, 2.2, 3.7 y 3.9 del Anexo 1.*

BIBLIOGRAFÍA:

Sobre ataques y vulnerabilidades, políticas y soluciones de seguridad informática

- **Documento pdf:**

- Vergara, F.: Fundamentos de seguridad, laboratorio de Redes y Telecomunicaciones de UDLA

- **Diapositiva:**

- Burbano, H.: Seguridades de Redes Empresariales
- Burbano, H.: Firewall
- Burbano, H.: Firma Digital
- Burbano, H.: Autenticación PAP y CHAP
- Microsoft TechNet Ecuador: Introducción a Windows Server 2003
- Certificación D-Link: DEC Seguridad Internet y VPN

- **Páginas web:**

- VSantivirus: Las 20 vulnerabilidades más críticas en Internet, URL: http://www.vsantivirus.com/20vul.htm, Descargado15/09/08
- Kioskea.net: Introducción a los ataques, URL: http://es.kioskea.net/attaques/attaques.php3, Descargado 15/11/08
- Slideshare: Seguridad en redes, URL: http://www.slideshare.net/guapacasa/seguridad-en-redes, Descargado 15/11/08
- Monografías.com: Auditoría de sistemas y políticas de seguridad informática, URL: http://www.monografias.com/trabajos12/fichagr/fichagr.shtml#POLIT, Descargado 30/11/08
- Monografías.com: Auditoría informática, URL: http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml, Descargado 02/12/08
- Wikipedia: Auditoría informática: Auditoría informática, URL: http://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica, Descargado 02/12/08
- Textos Científicos: Redes y Telecomunicaciones, URL: http://www.textoscientificos.com/redes, Descargado 10/12/08

- GMS: Soluciones, URL: http://www.gms.com.ec/php/index.php?arb=ARB0000003, Descargado 15/01/09
- Terra: IEEE.802.X, URL: http://www.terra.es/tecnologia/glosario/ficha.cfm?id_termino=501, Descargado 12/02/10
- Wikipedia: IEEE, URL: http://es.wikipedia.org/wiki/IEEE_802, Descargado 12/02/2010

Sobre LINUX

- **Libros:**
- Grupo de Usuarios Linux de Canarias: Curso de Introducción a Linux para alumnos,Hora editorial S.A., España,2008
- García de Jalón, J; Aguinaga, I; Mora, A: Aprenda Linux como si estuviera en primero, editorial de la Universidad de Navarra, España,2008
- **Diapositiva:**
- González, David: Conceptos básicos de Linux
- **Páginas web:**
- IEC-CSIC: Seguridad en Linux, URL: http://www.iec.csic.es/CRIPTonOMICon/linux/intro.html, Descargado 18/03/09
- Linux para todos: Manuales de Ubuntu Linux, URL: http://www.linuxparatodos.net/portal/staticpages/index.php?page=manuales-ubuntu-linux, Descargado 18/03/09
- Canonical: Ubuntu Server Edition, URL: http://www.ubuntu.com/server, Descargado 10/04/09
- Canonical: Ubuntu for bussiness, URL: http://www.canonical.com/about-ubuntu/for-business, Descargado 10/04/09
- CENCYT, Quito-Ecuador: Introducción a Linux, URL: http://www.cencyt.org/index.php?option=com_content&view=article&id=22&Itemid=34, Descargado 16/05/09
- CENCYT, Quito-Ecuador: Administración de Redes con Linux, URL: http://www.cencyt.org/index.php?option=com_content&view=article&id=45&Itemid=61, Descargado 16/05/09

- **Software:**

- CENCYT-CANONICAL: Linux Ubuntu

Sobre KYPUS

- **Documento pdf:**

- Nova Devices: Kypus vs caja con Linux, 2009, laboratorio Kypus

- **Páginas web:**

- Nova Devices: Kypus Server Appliance Resources, URL:http://www.novadevices.com/index.php?option=com_content&view=category&id=50&Itemid=64, Descargado 25/03/09

- Nova Devices: Datasheets, URL: http://www.novadevices.com/index.php?option=com_content&view=category&id=49&Itemid=63, Descargado 25/03/09

- **Software:**

- Nova Devices: Acceso remoto al servidor Kypus

ANEXO 1

Guía comparativa a tomar en cuenta al momento de adquirir un servidor

Es importante que una organización al adquirir una solución de seguridad perimetral, tome en cuenta ciertos parámetros acordes a sus requerimientos, parámetros que le ayudaran a optimizar y aprovechar de mejor manera los recursos de su sistema informático.

1. Costos

1.1. Costo de instalación del software, tanto Sistema Operativo, servicios de red y seguridad, en base a los requerimientos reales de la organización.

1.2. Costo del hardware en base a los requerimientos reales de la organización.

1.3. Es importante no solo tomar en cuenta el costo inicial de una solución para buscar un supuesto ahorro, sino también hay que tomar en cuenta los costos a mediano y largo plazo.

2. Rendimiento y fiabilidad

2.1. Tomar en cuenta que el software debe ser lo suficientemente robusto como para cubrir las expectativas y necesidades de la organización, esto es capacidad operativa y fiabilidad del Sistema Operativo y de cada uno de los servicios de red y seguridad requeridos por la organización.

2.2. Se debe tomar en cuenta que un Sistema Operativo de red debe ser instalado en un hardware apropiado, esto es, en un hardware que cumpla con las especificaciones técnicas para ser un servidor, y de esta manera conseguir un rendimiento óptimo de todo el sistema en su conjunto.

2.3. Ver si el hardware es lo suficientemente robusto como para cubrir las expectativas y necesidades de una organización, esto es capacidad operativa y especificaciones técnicas adecuadas de los componentes principales como es el procesador, el disco duro, la memoria, las interfaces de red y la fuente de poder, los mismos que deben ajustarse al menos de manera general a los requerimientos propios de la organización.

3. Garantías

3.1. Se debe tomar en cuenta que el software en su conjunto, tanto el Sistema Operativo como los servicios requeridos, deben presentar garantías en cuanto a calidad, flexibilidad, robustez, tolerancia a fallos, fácil actualización y adaptabilidad a nuevas tendencias tecnológicas, total control y administración de los usuarios de una red de datos, reducción de costos de licenciamiento, administración remota en caso de ser requerida.

3.2. Se debe tomar en cuenta que el hardware en su conjunto debe presentar garantías en cuanto a calidad y compatibilidad con dispositivos de red, tiempo de vida útil, optimización del consumo eléctrico, ahorro de espacio físico, ruido mínimo o nulo, disponibilidad de repuestos y respuesta inmediata cuando se los requiera, tolerancia a fallos, robustez.

3.3. Tanto el hardware como el software deben presentar la garantía del respectivo soporte técnico, en cuanto a tiempo de respuesta sea presencial o remoto, calidad del soporte a brindarse, capacidad y experiencia del ofertante, que el personal está debidamente calificado, tiempos mínimos de interrupción del servidor en caso de requerir un soporte que así lo amerite.

3.4. El hardware y el software deben ser instalados, configurados y probados de acuerdo a los requerimientos y necesidades de la organización, así como con los estándares nacionales e internacionales.

3.5. El servidor integrado como tal, debe estar preparado para trabajar con soluciones integradas de datos y ser compatible con cualquier plataforma de software a nivel de cliente, así como debe ser compatible con cualquier solución de correo electrónico que utilice la organización.

3.6. El servidor debe permitir la reducción o el crecimiento de usuarios y servicios de red de manera flexible, rápida y efectiva, en cuanto al crecimiento de usuarios y servicios se debe buscar un ahorro en costos de licenciamiento.

3.7. El servidor en su conjunto debe ser una solución confiable y escalable, en la que se pueda confiar y que estese al alcance del presupuesto de la organización, sin escatimar la confiabilidad de los servicios de red y seguridad.

3.8. El ofertante debe contar como valor agregado, con un plan de capacitación inicial sobre el manejo de las funcionalidades y servicios del

servidor, en caso de que este sea requerido por la organización o se considere necesario hacerlo.

3.9. Un servidor debe integrar todos los requerimientos de red y comunicaciones en un solo equipo, y así evitar múltiples dispositivos de hardware y software que involucren costos directos altos y costos altos de mantenimiento.

3.10. En una solución se debe buscar reducir a niveles mínimos la dependencia de personal calificado, tanto a mediano y largo plazo, todo esto mediante la búsqueda de una solución altamente funcional y confiable y de esta manera reducir costos de mantenimiento y posibles tiempos de interrupción del servidor.

ANEXO 2

Normas IEEE 802.X

Es un conjunto de normas que definen las características físicas de las redes, dictadas por el IEEE (Institute of Electrical and Electronic Engineers). En estas normas definen el control de acceso al medio (MAC).

- 802.1 - Estándar definido relativo a los algoritmos para enrutamiento de cuadros o frames (la forma en que se encuentra la dirección destino).

- 802.2 - Define los métodos para controlar las tareas de interacción entre la tarjeta de red y el procesador (nivel 2 y 3 del modelo OSI) llamado LLC.

- 802.3 - Define las formas de protocolos Ethernet CSMA/CD en sus diferentes medios físicos (cables).

- 802.4 - Define cuadros Token Bus tipo ARCNET.

- 802.5 - Define hardware para Token Ring.

- 802.6 - Especificación para redes tipo MAN.

- 802.7 - Especificaciones de redes con mayores anchos de banda con la posibilidad de transmitir datos, sonido e imágenes.

- 802.8 - Especificación para redes de fibra óptica time Token Passing/FDDI.

- 802.9 - Especificaciones de redes digitales que incluyen video.

- 802.11 - Estándar para redes inalámbricas con línea visual.

- 802.11a - Estándar superior al 802.11b, pues permite velocidades teóricas máximas de hasta 54 Mbps, apoyándose en la banda de los 5GHz. A su vez, elimina el problema de las interferencias múltiples que existen en la

banda de los 2,4 GHz (hornos microondas, teléfonos digitales DECT, BlueTooth).

- 802.11b - Extensión de 802.11 para proporcionar 11 Mbps usando DSSS. También conocido comúnmente como Wi-Fi (Wireless Fidelity): Término registrado promulgado por la WECA para certificar productos IEEE 802.11b capaces de ínter operar con los de otros fabricantes. Es el estándar más utilizado en las comunidades inalámbricas.

- 802.11e - Estándar encargado de diferenciar entre video-voz-datos. Su único inconveniente es el encarecimiento de los equipos.

- 802.11g - Utiliza la banda de 2,4 GHz, pero permite transmitir sobre ella a velocidades teóricas de 54 Mbps. Se consigue cambiando el modo de modulación de la señal, pasando de 'Complementary Code Keying' a 'Orthogonal Frequency Division Multiplexing'. Así, en vez de tener que adquirir tarjetas inalámbricas nuevas, bastaría con cambiar su firmware interno.

- 802.11i - Conjunto de referencias en el que se apoyará el resto de los estándares, en especial el futuro 802.11a. El 802.11i supone la solución al problema de autenticación al nivel de la capa de acceso al medio, pues sin ésta, es posible crear ataques de denegación de servicio (Dos).

- 802.11n - La velocidad real de transmisión podría llegar a los 600 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología MIMO (Multiple Input – Multiple Output), que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación

de varias antenas, además puede trabajar en las bandas de frecuencias de de 2.4 GHz y 5 GHz.

- 802.12 - Comité para formar el estándar de 100 base VG que sustituye CSMA/CD por asignación de prioridades.

- 802.14 - Comité para formar el estándar de 100 base VG sin sustituir CSMA/CD.

- IEEE 802.15 -WPAN (Bluetooth)

- IEEE 802.16 - Redes de acceso metropolitanas sin hilos de banda ancha (WIMAX).

- IEEE 802.17 - Anillo de paquete elástico.

- IEEE 802.18 - Grupo de Asesoría Técnica sobre Normativas de Radio.

- IEEE 802.19 - Grupo de Asesoría Técnica sobre Coexistencia.

- IEEE 802.20 - Acceso inalámbrico de banda ancha móvil.

- IEEE 802.21 - Media Independent Handoff.

- IEEE 802.22 - Red de área regional inalámbrica.

ANEXO 3

Modelo *OSI (Open System Interconnection – Interconexión de Sistema Abierto)*

El Modelo OSI es un lineamiento funcional para tareas de comunicaciones muchos estándares y protocolos cumplen con los lineamientos del Modelo OSI. El modelo es considerado una arquitectura de redes porque especifica el protocolo que debe ser usado en cada capa, y suele hablarse de modelo de referencia porque es usado como una gran herramienta para la enseñanza de comunicación de datos. Este modelo está dividido en siete capas que empiezan desde abajo hacia arriba:

Aplicación	Servicio de red a aplicaciones
Presentación	Representación de datos
Sesión	Comunicación entre los dispositivos de la red
Transporte	Conexión extremo a extremo y fiabilidad de los datos
Red	Direccionamiento lógico y determinación de ruta
Enlace	Direccionamiento físico (MAC y LLC)
Física	Señal y transmisión binario

Modelo TCP/IP

El modelo TCP/IP es una de las dos variantes principales disponibles en la red Internet, siendo un modelo de transporte de información. El modelo TCP/IP tiene la ventaja sobre el modelo OSI porque simplifica el esquema, limitando el problema de la comunicación entre maquinas a 4 pasos:

Aplicación	Servicio de red a aplicaciones
Transporte	Conexión extremo a extremo y fiabilidad de los datos
Internet	Empaquetación de datos en datagramas IP
Red	Direccionamiento lógico y determinación de ruta