Universidad De San Carlos De Guatemala
Facultad De Ingeniería
Escuela De Ingeniería En Ciencias Y Sistemas

INTEGRACIÓN DE TECNOLOGÍAS DE SEGURIDAD PERIMETRAL PARA PROTECCIÓN DE REDES PRIVADAS EN INTERNET

HEBER EDUARDO CORZO MANZO

ASESORADO POR: ING. LUIS ALBERTO VETTORAZZI ESPAÑA

GUATEMALA, NOVIEMBRE DE 2003

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

INTEGRACIÓN DE TECNOLOGÍAS DE SEGURIDAD PERIMETRAL PARA PROTECCIÓN DE REDES PRIVADAS EN INTERNET

TRABAJO DE GRADUACIÓN

PRESENTADO A JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

HEBER EDUARDO CORZO MANZO
ASESORADO POR: ING. LUIS ALBERTO VETTORAZZI ESPAÑA

AL CONFERÍRSELE EL TÍTULO DE
INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, NOVIEMBRE DE 2003

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Sydney Alexander Samuels Milson
VOCAL I	Ing. Murphy Olympo Paiz Recinos
VOCAL II	Lic. Amahán Sánchez Alvarez
VOCAL III	Ing. Julio David Galicia Celada
VOCAL IV	Bach. Kenneth Issur Estrada Ruiz
VOCAL V	Bach. Elisa Yazminda Vides Leiva
SECRETARIO	Ing. Pedro Antonio Aguilar Polanco

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Herbert René Miranda Barrios
EXAMINADOR	Ing. Otto Amilcar Rodríguez Acosta
EXAMINADOR	Ing. Rolando Haroldo Alonzo Ordoñez
EXAMINADOR	Ing. Luis Alberto Vettorazzi España
SECRETARIA	Inga. Gilda Marina Castellanos de Illescas

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

INTEGRACIÓN DE TECNOLOGÍAS DE SEGURIDAD PERIMETRAL PARA PROTECCIÓN DE REDES PRIVADAS EN INTERNET

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha agosto de 2002.

Heber Eduardo Corzo Manzo

AGRADECIMIENTOS:

A DIOS Gracias mi Padre Celestial, por darme el aliento de vida de cada día, por la salud, protección y sabiduría. Gracias por ser mi inspiración y porque me has enseñado a creer en los imposibles.

A mis padres Un millón de gracias por su esfuerzo y ayuda incondicional en todo momento. Soy producto de su amor, sacrificio y oraciones. Gracias por los valores, principios, y por haberme mostrado el camino hacia Dios.

A mis hermanos Gracias Alex, por tu ejemplo, apoyo y múltiples consejos. Chito, gracias por compartir momentos de mi niñez y adolescencia que nunca olvidaré. Any y Sisy, por apoyarme en cada momento y estar cerca de mí.

A mis compañeros de universidad Gracias por compartir esos inolvidables momentos de U, donde me dieron la oportunidad de aprender lo mejor de ustedes. Gracias Maco, Jorge, Edgar y José Manuel, su amistad vale más que todo el dinero del mundo.

A mis amigos Gracias por extender su mano de amistad y permitirme vivir buenos momentos de alegría y tristeza. Gracias Sergio, Ferlandy, Gerson, Obed, Paolo, Neil, Mischell, Nora, Jeaneth, Alejandro, Checho, Elvin, Jorge, Miguel. Gracias a mis demás amigos, la lista nunca terminaría.

A los abuelos y familia Gracias por adoptarme y extenderme su brazo de amor. Abuela Wicha y abuelo Cheyo gracias por sus sabios consejos y mostrarme el camino hacia Dios. Gracias Chochy (nunca olvidaré aquellas cenas), Cheyo y Julia (por adoptarme como su hijo), Rodolfo, Elsio, Lupita y demás familia. Dios los bendiga.

A mis catedráticos Les agradezco por haber contribuido en mi formación profesional. Gracias Ing. Francisco Guevara (su trabajo docente ha dejado huellas), Ing. Luis Alberto Vettorazzi, Ing. Raúl Veliz.

A la universidad Gracias Universidad de San Carlos de Guatemala, porque me has dado la oportunidad de llegar a ser profesional. Gracias por darme la dicha de pertenecer al selecto grupo de profesionales de Ingeniería en Ciencias y Sistemas. Me esforzaré y sacrificaré para colocar tu nombre en alto.

A mi patria Gracias Guatemala, libre al viento tu hermosa bandera. Rincón de cielo azul y blanco que me viste nacer y que me has dado la oportunidad de sentirme orgulloso de ser chapín.

DEDICATORIAS:

A Jesucristo

Todos mis logros son para ti Jesús. Honra y gloria por siempre al Hijo de Dios.

A mi padre, Manuel Corzo

Dedico especialmente a vos este trabajo, porque me has enseñado con tu ejemplo a trabajar y a nunca desmayar a pesar de las circunstancias.

A mi madre, Sandra Manzo

Misión cumplida mamita. Te dedico este fruto y todas las cosechas de mi vida, porque son el resultado de las semillas de amor, esfuerzo, dedicación y sacrificio que sembraste en mí.

A mi amigo, Sergio Galindo

Es un honor dedicarte este trabajo, porque has sido mi hermano mayor, porque me has enseñado a ir hacia el frente, y porque me has dado tu ayuda incondicional en todo momento.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

ActiveX Medio ambiente del programa de *Microsoft* que incluye un número grande de programas (componentes) el cual activa y conecta aplicaciones diferentes en la computadora.

Applet Pequeño programa diseñado para ser ejecutado en otras aplicaciones.

Browser Programa de aplicación utilizado para ubicar y hojear páginas del WWW en Internet.

CGI (*Common gateway interface*) Interfase que permite a los programas ser ejecutados sobre un servidor *Web*.

Daemon Proceso que se ejecuta en segundo plano, realizando una operación específica en tiempos predefinidos o en respuesta a ciertos eventos.

Enrutador Dispositivo que envía paquetes de una red a otra, mediante el uso tablas y protocolos de enrutamiento.

Finger Programa de *Unix* que toma una dirección de un correo electrónico como entrada y devuelve

	información sobre el usuario de esa dirección de correo electrónico.
FTP (*File Transfer Protocol*)	Protocolo de red para la transferencia de archivos entre ordenadores en el Internet.
Host	Ordenador que provee servicios a otros ordenadores.
HTTP (*Hipertext transport protocol*)	Protocolo de transmisión del hipertexto, y que sirve para incursionar en los sitios de WWW en la Internet.
Java	Lenguaje de programación para las aplicaciones de las páginas de Internet.
JavaScript	Lenguaje desarrollado por *Netscape* que permite a los autores de páginas *Web* diseñar sitios interactivos.
Kernel	Módulo central del sistema operativo.
Mainframe	Sistema de cómputo grande y muy poderoso usado para tareas computacionales intensas.
Perl	Lenguaje de programación para procesamiento de textos.
RADIUS (*Remote authentication dial-*	Sistema utilizado por muchos proveedores de Internet para proveer autenticación y auditoría de usuarios.

***in user service*)**

RFC (*Request for comments*)	Serie de notas sobre Internet, documentos que contienen proposiciones, comentarios y los estándares relacionados con la tecnología de Internet propuesta por el IETF.
Script	Serie de instrucciones que pueden ser ejecutadas en orden para la automatización de rutinas.
SMTP (*Simple Mail Transfer Protocol*)	Protocolo que se utiliza para la transferencia de correo electrónico en la Internet.
SNMP(*simple network management protocol*)	Protocolo para la administración simple de una red.
String	Estructura de datos que representa una hilera o cadena de caracteres.
TACACS (*Terminal access control access control system*)	Protocolo de autenticación, que permite a un servidor de acceso remoto comunicarse con un servidor de autenticación para determinar si el usuario tiene acceso al a red.
TCP SYN	Código del protocolo TCP que indica una solicitud de

	conexión de un equipo en red.
Telnet	Protocolo para la emulación de pantalla en conexión con otro ordenador a través de la Internet o por línea telefónica.
Unix	Sistema operativo multitarea y multiusuario.
URL (*Uniform resource locator*)	Dirección global de documentos y otras fuentes en Internet.
VPN (*Virtual private network*)	Red de comunicación privada utilizada por la red pública, utiliza protocolo de eficiencia y seguridad de información para guardar la privacidad de la información.
WAN (*Wide Area Network*)	Red de comunicación extendida que conecta ordenadores dispersos en una amplia área geográfica.

RESUMEN

Este trabajo de graduación presenta una recopilación de los aspectos de tecnología de seguridad más relevantes que las organizaciones deben emplear en la actualidad para aprovechar al máximo las ventajas que ofrece Internet, dando a conocer aspectos de diseño, tecnologías y procedimientos para operar los recursos tecnológicos de las redes privadas dentro de un ambiente seguro.

El primer capítulo describe la arquitectura funcional de Internet dando a conocer sus componentes, tales como protocolos de comunicación, medios de acceso y servicios básicos. Además se describe el nacimiento y desarrollo de la red global que ha permitido a las compañías tomar ventajas de sus beneficios y oportunidades.

El segundo capítulo abarca el tema de la seguridad, da a conocer la evolución así como los aspectos que motivan su existencia y con los cuales debe luchar constantemente. Se destaca que para la seguridad, es importante conocer al enemigo, sus armas de ataque, los motivos que lo incitan y los riesgos de daños potenciales a los recursos de la red privada. También se describen las mejores prácticas de seguridad para las compañías, conocidas como políticas de seguridad y que son muy importantes porque definen un marco de trabajo general para la implementación de la seguridad, dando a conocer las conductas permitidas y no permitidas, los procedimientos, métodos y herramientas de seguridad precisos. Por otro lado se da a conocer la implicación de los riesgos de conexión de una red privada a Internet, describiendo un análisis de incidentes y tendencias de seguridad en Internet

con el propósito de hacer conciencia de los peligros que conlleva la conexión de una red privada.

El tercer capítulo abarca el estudio de la arquitectura de seguridad perimetral, exponiendo la funcionalidad y características de los sistemas de protección perimetral que se emplean en la actualidad. También se describe la aplicación de zonas perimetrales para contener y limitar la expansión de un ataque externo. Al final del capítulo se describe la integración de los segmentos de red, incluyendo zonas de perímetro, redes internas y redes externas mediante la aplicación estratégica de mecanismos de control de acceso.

El último capítulo describe un caso práctico de estudio, partiendo de la estrategia de negocio de una compañía, infraestructura de red, requerimientos de expansión en Internet y requerimientos de seguridad, para dar como resultado la definición de la política de seguridad perimetral, y llegar al diseño de la arquitectura de seguridad perimetral que permitirá llevar a cabo la estrategia de comercialización en Internet de la compañía de forma confiable, justificable y práctica.

Como punto final se hace la observación que es importante reconocer el cambio que ha tenido el papel de la seguridad informática, ya que en la actualidad resulta indispensable aplicarla en entornos de compañías que tienen conexión con redes externas como Internet. Esto significa que la seguridad es más permisiva desde el punto de vista que permite una mayor apertura de servicios para las compañías, desde luego, sin olvidar el fortalecimiento de las líneas de protección perimetral que necesitan ser reforzadas por políticas de seguridad que definan la dirección y lineamientos de cómo debe operarse y administrarse los recursos de las redes privadas.

OBJETIVOS

- **General**

  Presentar un estudio teórico-práctico de la aplicación de tecnologías de seguridad perimetral, que permitan a las organizaciones llevar a cabo sus estrategias de comercialización en Internet de forma segura, eficiente y justificable.

- **Específicos**

  1. Mostrar la arquitectura y funcionamiento de los componentes de Internet.
  2. Exponer los orígenes que han llevado a definir las tecnologías de seguridad informática.
  3. Presentar un análisis de las características de enemigos contra quienes una organización debe proteger los recursos informáticos.
  4. Analizar los mecanismos y tecnologías de actualidad utilizados en la protección perimetral de una red privada conectada a Internet.
  5. Proponer prácticas y lineamientos de diseño que deben aplicarse al establecer una red de protección perimetral.
  6. Mostrar que la aplicación de políticas de seguridad resulta ser de mucha importancia dentro de las organizaciones ya que permiten garantizar un ambiente de trabajo seguro.

INTRODUCCIÓN

La era de la información y las comunicaciones ha tenido un gran impulso en los últimos años, dando como resultado que las actividades sean mucho más sencillas. La evolución de las computadoras, las redes de datos e Internet ha revolucionado la forma en que se informa, comunica, trabaja, compra y vive.

Las redes de datos se han convertido en herramientas muy poderosas para incrementar la competitividad global de las compañías, permitiendo que los procesos de negocio sean ejecutados con mayor eficacia, eficiencia y agilidad. Las compañías han descubierto que Internet representa un punto de lanzamiento al mercado global de productos y servicios, llevando consigo una infinidad de oportunidades de negocio.

La red de Internet es la puerta a un universo de oportunidades, permitiendo la expansión de los mercados a nivel global, a través de herramientas como el comercio electrónico. Las compañías con el afán de crecimiento y expansión, se han volcado apresuradamente a la comercialización electrónica en Internet, teniendo cobertura mundial con clientes, proveedores y socios de negocios.

Esta rápida expansión de la red mundial, ha traído consigo algunos problemas que no fueron considerados en su diseño. El mismo protocolo TCP/IP, el cual es la base de la comunicación entre equipos de Internet, sufre de muchas debilidades de seguridad. Por otro lado, Internet es de acceso público y no existe algún ente rector que regule y controle las actividades en la red. Esto ha traído como consecuencia una gran cantidad de incidentes, que van desde la infección de virus de un computador, hasta destrucción de

información, provocando considerables pérdidas financieras para las compañías.

Como una contramedida de estos incidentes, en los últimos años se han desarrollado tecnologías de seguridad que tienen como objetivo permitir que las redes privadas de las compañías puedan conectarse a Internet para hacer negocios, en forma segura y garantizando la protección de los recursos de las amenazas cada vez en crecimiento.

Cuando se conecta una red privada a Internet, resulta muy importante conocer la implicación de los riesgos, los niveles de amenazas, las debilidades en la tecnología, las características y motivación de los intrusos. Se debe responder a preguntas como, ¿qué recursos de red se deben proteger?, ¿de quién se están protegiendo esos recursos? y, ¿cómo llevar a cabo dicha protección?

La seguridad perimetral es la implementación de tecnologías de seguridad, que permiten aislar los recursos de las redes privadas en Internet. Para que las tecnologías de seguridad sean efectivas, deben ser reforzadas mediante la aplicación de políticas de seguridad, que definan los métodos, procedimientos, mecanismos y direcciones de cómo manejar la seguridad para los recursos, servicios y sistemas dentro de la organización.

Las políticas de seguridad definen un marco de trabajo para la protección de los recursos de red, en el cual, directores, administradores de seguridad, operadores de sistemas y usuarios son guiados a través de las mejores prácticas para el mantenimiento de un ambiente seguro. También ayudan a la definición de la arquitectura tecnológica de seguridad, en la que tanto servicios

como mecanismos de seguridad son aplicados a la red, para el cumplimiento de los requerimientos de seguridad establecidos por la compañía.

Este trabajo de graduación presenta una recopilación medular de los aspectos de seguridad perimetral, que deben aplicar actualmente las compañías para conectar su red privada a Internet y garantizar un ambiente de operación seguro y funcional.

1. INTRODUCCIÓN A LA ARQUITECTURA DE INTERNET

Internet es una red mundial, en la cual cada computadora actúa como un cliente y un servidor. Su arquitectura modular basada en modelos de capas le permite integrar líneas de comunicación de alta velocidad, grupos de *hardware* y *software* dedicados a la administración de la comunicación, proveedores de servicios de acceso a Internet, terminales o computadoras, donde los usuarios tienen interacción con Internet, protocolos que permiten que dos computadoras puedan intercambiar información a través de pequeños mensajes de datos. La composición de esta red global de computadoras es compleja, por lo que resulta importante describir los componentes más importantes que integran esta arquitectura.

1.1. Fundamentos de la comunicación modular

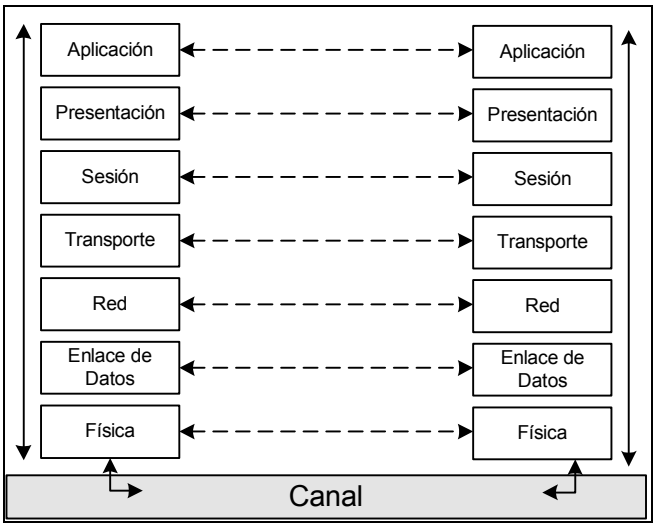
El modelo OSI se basa en una propuesta que desarrolló la Organización Internacional de Normas (ISO, por sus siglas en inglés) como primer paso hacia la estandarización internacional de los protocolos, que se usan en las diversas capas de la arquitectura de red. El modelo se llama modelo de referencia OSI (*open systems interconnection*, interconexión de sistemas abiertos) de la OSI puesto que se ocupa de la conexión de sistemas abiertos, esto es, sistemas que están abiertos a la comunicación con otros sistemas.

El modelo de referencia OSI tiene siete capas. Los principios que se aplicaron para llegar a las siete capas son los siguientes:

1. Se debe crear una capa siempre que se necesite un nivel diferente de abstracción.
2. Cada capa debe realizar una función bien definida.
3. La función de cada capa se debe elegir, pensando en la definición de protocolos estandarizados internacionalmente.
4. Los límites de las capas deben elegirse a modo de minimizar el flujo de información a través de las interfaces.
5. La cantidad de capas debe ser suficiente, para no tener que agrupar funciones distintas en la misma capa y lo bastante pequeña, para que la arquitectura no se vuelva inmanejable.

El modelo OSI en sí no es una arquitectura de red, porque no especifica los servicios y protocolos exactos que se han de usar en cada capa; sólo dice lo que debe hacer cada capa. Sin embargo, la ISO también ha elaborado estándares para todas las capas, aunque no sean parte del modelo de referencia mismo. La figura 1 muestra la estructura de las capas del modelo OSI.

FIGURA 1. Modelo de referencia OSI



Capa física. Se encarga de convertir la información lógica en señales eléctricas u ópticas, para transmitirla en un medio físico hacia su destino.

Capa de enlace de datos. Se encarga de organizar y estructurar los marcos de datos para la transmisión, y así detectar y corregir los errores que se presenten. Esta capa se subdivide en dos subcapas:

Control de enlace lógico (Logical Link Control), se encarga del tráfico, segmentación y confirmación de los marcos de datos.

Control de acceso al medio (Media Access Control), define la forma de acceder la información disponible en la capa física.

Capa de red. Se encarga de direccionar los paquetes, interpretar nombres y direcciones lógicas en direcciones físicas, determinar la ruta de la fuente al destino, así como manejar problemas de tráfico en la red.

Capa de transporte. Se encarga de todo lo relativo a la transmisión y recepción de mensajes, así como su empaquetamiento, el control del flujo, calidad en el servicio (velocidad de transferencia y tasa de errores residuales).

Capa de sesión. Su función es establecer una sesión entre dos equipos de la red, reconocer nombres, revisar seguridad, sincronización y verificación del proceso de comunicación.

Capa de presentación. Su función es manejar los formatos usados en la comunicación, encriptación, codificación, conversión y compresión de datos.

Capa de aplicación. Su función es manejar las aplicaciones del usuario, servicios y accesos a la red.

1.2. El modelo de capas de Internet

El modelo de TCP/IP nació con el uso de la red de computadoras ARPANET y su sucesora la Internet mundial. La ARPANET era una red de investigación patrocinada por el DoD (Departamento de defensa de los Estados Unidos). Al final conectó a cientos de universidades e instalaciones del gobierno, usando líneas telefónicas rentadas. Cuando más tarde se añadieron redes de satélite y radio, los protocolos existentes tuvieron problemas para interactuar con ellas, de modo que se necesitó una arquitectura de referencia nueva. Así, la capacidad de conectar entre sí múltiples redes de manera inconsútil fue uno de los principales objetivos de diseño desde el principio. Esta arquitectura se popularizó después con el modelo de referencia TCP/IP, por las iniciales de sus dos protocolos primarios. Este modelo se definió por primera vez en 1974.

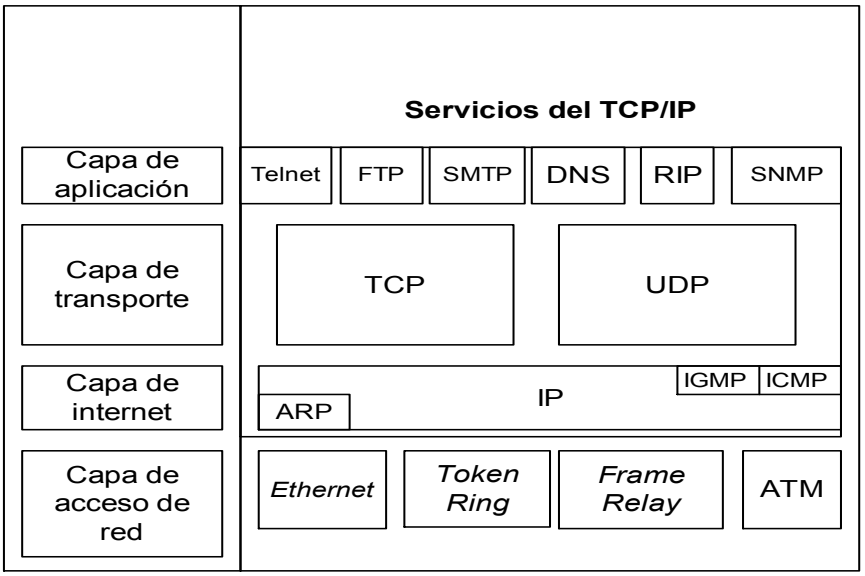
Debido a la preocupación del DoD porque alguno de sus costosos nodos, enrutadores o pasarelas de interredes pudiera ser objeto de un atentado en cualquier momento, otro de los objetivos principales fue que la red fuera capaz de sobrevivir a la pérdida del *hardware* de subred, sin que las conversaciones existentes se interrumpieran. En otras palabras, el DoD quería que las conexiones permanecieran intactas, mientras las máquinas de origen y destino estuvieran funcionando, aun si alguna de las máquinas o de las líneas de transmisión en el trayecto dejara de funcionar en forma repentina. Es más, se necesitaba una arquitectura flexible, pues se tenía la visión de aplicaciones con requerimientos divergentes, abarcando desde la transferencia de archivos hasta la transmisión de discursos en tiempo real.

1.2.1. La capa de interred

Todos estos requerimientos condujeron a la elección de una red de conmutación de paquetes, basada en una capa de interred carente de conexiones. Esta capa, llamada capa de interred, es el eje que mantiene unida toda la arquitectura. La misión de esta capa es permitir que los nodos inyecten paquetes en cualquier red y los hagan viajar de forma independiente a su destino. Los paquetes pueden llegar incluso en un orden diferente a aquel en que se enviaron, en cuyo caso corresponden a las capas superiores reacomodarlos, si se desea la entrega ordenada.

La capa de interred define un formato de paquete y protocolo oficial llamado IP (*Internet protocol*, protocolo de interred). El trabajo de la capa de interred es entregar paquetes IP a donde se supone que deben ir. Aquí la consideración más importante es claramente el enrutamiento de los paquetes, y también evitar la congestión. La figura 2 muestra la correspondencia.

FIGURA 2. Modelo de referencia TCP/IP



1.2.2. La capa de transporte

La capa que está sobre la capa de interredes en el modelo TCP/IP se llama usualmente ahora capa de transporte. Esta capa se diseñó para permitir que las entidades pares en los nodos de origen y destino, lleven a cabo una conversación, lo mismo que en la capa de transporte OSI. Aquí se definieron dos protocolos de extremo a extremo. El primero, TCP (*transmission control protocol,* protocolo de control de la transmisión) es un protocolo confiable, orientado a la conexión que permite que una corriente de *bytes* originada en una máquina, se entregue sin errores en cualquier otra máquina de la interred. Este protocolo fragmenta la corriente entrante de bytes, en mensajes discretos y pasa cada uno a la capa de interred. En el destino, el proceso TCP receptor reensambla los mensajes recibidos para formar la corriente de salida. El TCP también se encarga de control de flujo para asegurar que un emisor rápido no pueda abrumar a un receptor lento con más mensajes de los que pueda manejar.

El segundo protocolo de esta capa, el UDP (*user datagram protocol*, protocolo de datagrama de usuario), es un protocolo sin conexión, no confiable, para aplicaciones que no necesitan la asignación de secuencia ni el control de flujo del TCP y que desean utilizar los suyos propios. Este protocolo también se usa ampliamente para consultas de petición y respuesta de una sola ocasión, del tipo cliente-servidor, y en aplicaciones en las que la entrega pronta es más importante que la entrega precisa, como las transmisiones de voz o video. La relación entre IP, TCP y UDP se muestra en la figura 2. Desde que se desarrolló el modelo, el IP se ha implementado en muchas otras redes.

1.2.3. La capa de aplicación

El modelo TCP/IP no tiene capas de sesión ni de presentación. No se pensó que fueran necesarias, así que no se incluyeron. La experiencia con el modelo OSI ha comprobado que esta visión fue correcta: se utilizan muy poco en la mayor parte de aplicaciones.

Encima de la capa de transporte está la capa de aplicación, que contiene todos los protocolos de alto nivel. Entre los protocolos más antiguos están el de terminal virtual TELNET, el de transferencia de archivos FTP y el de correo electrónico SMTP, según se muestra en la figura 2.

1.3. Internet

Internet puede ser definida como una red de redes de computadoras que se encuentran interconectadas a lo largo del mundo, nadie es dueño de Internet simplemente cada usuario paga su conexión hasta llegar a la red.

1.3.1. Evolución

Internet nació en EEUU como un proyecto de la DARPA (*Defense Advanced Research Projects Agency,* Agencia de Proyectos de Investigación Avanzados de la Defensa). La misma buscaba intercambiar información entre los investigadores, científicos y militares, ubicados en distintos sitios distantes. La red debía soportar un ataque nuclear sin perder la conexión con el resto de los sitios, constaba de cuatro computadores interconectados y se llamaba DARPANET. En 1972 ya había conectado treinta y siete computadores y pasó a

denominarse ARPANET, la aplicación más utilizada en ésta era Telnet para luego pasar a ser el *e-mail* o correo electrónico.

Hacia 1984 la NSF (*National Science Foundation,* Fundación de Ciencia Nacional) estableció la NSFNET paralela a la ARPANET para la investigación académica que ya estaba saturada, también la NSFNET se saturó hacia mediados de 1987 y no precisamente por la actividad académica. En éste año se redimensionó totalmente la NSFNET, con un acceso más rápido, con modems y computadoras mas veloces, a ellas podían ingresar todos los países aliados de EEUU. En los 90 se empieza a conocer como en la actualidad, La red o Internet y se abrió para todo aquel que pudiera conectarse.

El protocolo utilizado en esta gran red es TCP/IP, TCP se encarga de contabilizar las transmisión de datos entre computadores y registrar si hay o no errores, mientas que IP es el que realiza realmente la transferencia de datos.

1.3.2. Arquitectura

Una red existe cuando hay dos o más ordenadores conectados de forma que puedan compartir y pasar información entre ellos. Cada una de estas máquinas se denomina *host* o nodo de la red. Si proporciona un servicio específico, tal como la verificación de contraseña, el ordenador se denomina servidor.

Los nodos de una red siguen un conjunto de reglas, denominados protocolos para intercambiar información, que a su vez sirve también para definir los servicios que pueden estar disponibles en un ordenador. Hay muchos tipos diferentes de protocolos, aunque los más habituales proporcionan conexiones TCP/IP que permiten que los usuarios se conecten a Internet. El protocolo de comunicaciones TCP/IP sirve como núcleo de Internet. Este protocolo de

comunicaciones permite conectar computadores que utilizan distintos sistemas operativos. Trabaja a nivel de capa de red y de transporte en la clasificación del modelo de la ISO/OSI.

Al esquema de direccionamiento en Internet se le conoce como direccionamiento IP. Una dirección IP es un número formado por cuatro octetos de la siguiente forma xxx.xxx.xxx.xxx donde cada xxx representa un número decimal entre 0 y 255 e identifica en forma única a cada dispositivo conectado a la gran red, por ejemplo 168.101.122.1 identifica una red y un *host* dentro de esa red.

Como a las personas les es difícil manejarse con números, se manejan mediante nombres, que la red se encarga de traducir a direcciones IP, así el nombre completo de una máquina puede ser uno.server.corporacion.com.gt. Los dominios que son agrupaciones de computadores o dispositivos del mismo tipo, origen o característica.

1.3.3. Servicios

El correo electrónico fue una de las primeras aplicaciones creadas para Internet y de las que más se utilizan. Este medio es rápido, eficiente y sencillo de administrar, llegando a ser el sistema más sofisticado de mensajería que hoy se conoce. El correo electrónico es más sencillo que escribir una carta o enviar un fax, funciona los trescientos sesenta y cinco días el año las veinticuatro horas del día, a no ser que caiga un servidor.

En caso de caídas de un servidor, no se pierden los mensajes enviados a dicho destino sino que se retienen en el último punto hasta que puedan seguir su camino hasta el buzón del destinatario, éste es global como Internet. Es

económico, ya que es más barato enviar un e-mail que una carta por vía aérea o hacer una llamada o fax, no requiere papel, es fácil de descartar y es ecológico, de lo único que se debe disponer es de una computadora y una conexión a Internet.

SMTP (*Simple Mail Transfer Protocol,* protocolo de transferencia de correo simple) es un protocolo de la familia del TCP/IP para la transmisión de correo electrónico, éste no es dependiente de ningún correo en especial sino que cualquier *software* de correo que genere un *e-mail* en el formato en que el protocolo lo estructura, será entendido por éste. Las distintas formas de conexión son:

1. Correr un programa residente y conectado continuamente a Internet teniendo todo en línea.
2. Conectarse a Internet a intervalos regulares y despachar el correo saliente y bajar el entrante o conectarse a Internet en forma irregular.

SMTP administra los mensajes en colas o *spool*, la forma de expresar una dirección de correo electrónico es: usuario@nombre.de.dominio

Ejemplos de direcciones:

a. mailto:Sistemas@corporacion.com.gt
b. mailto:*Web*master@corporacion.com.gt

Los programas de correo más populares son *Eudora*, *Outlook Express* de *Microsoft* y *Netscape*.

El POP3 (*Post Office Protocol 3,* protocolo de oficina de correos 3) es el protocolo que permite acceder a la casilla de correo de un usuario. Mediante

este protocolo, el cliente de *e-mail* se comunica al servidor de casilla de correo y puede recibir el correo que el servidor ha estado recibiendo y guardando para el usuario.

IMAP (*Internet Message Access Protocol,* protocolo de acceso de mensaje por Internet) es un método de acceso al correo electrónico que se mantiene en el servidor correspondiente. A diferencia del protocolo POP3 que retira los mensajes del servidor al conectarse y los almacena en el servidor local, IMAP4 los deja en el servidor remoto, con lo que es posible acceder a los mismos desde diferentes puntos (oficina, casa etc.).

Su particularidad es que deja crear múltiples buzones en la máquina remota, es útil para alguien que viaja para no tener la necesidad de llevarse un equipo consigo, sino poder bajar los mensajes desde cualquier otro equipo, e inclusive permite que varios usuarios entren al mismo buzón a la vez a ver los mismos mensajes.

FTP (*File Transfer Protocol,* protocolo de transferencia de archivo) permite la transferencia de archivo al y desde el servidor de FTP, se diseñó para permitir el intercambio de datos, archivos entre computadores *host* y cliente. La estructura de FTP es cliente/servidor, el servidor posee una estructura de directorios o carpetas en donde se encuentran alojados, los archivos de texto, gráficos, etc. , y el cliente accede mediante un utilitario de FTP o línea de comando para extraer archivos a su PC o enviarlos al servidor. Cuando se ingresa a un servidor FTP se puede hacer como usuario con permisos definidos o como usuario invitado, siempre y cuando el administrador del sistema habilite el mismo, luego puede recorrer las distintas carpetas hasta encontrar el archivo buscado, una vez encontrado este se transfiere a nuestro computador.

Al teléfono vía Internet se le sumó la transmisión de video en directo creando el nuevo concepto de videoconferencia. Existe en el mercado un programa denominado *CuSeeMee*, Comunicándonos en vivo. Por el momento las imágenes que transmite *CuSeeMee* son de resolución regular y se actualizan a intervalos regulares. La calidad del sonido, en cambio, es bastante superior a la del video pues el sonido es más fácil de enviar porque requiere menos recursos que el video. Además, el sistema permite transmitir textos e imágenes fijas, al mismo tiempo en que se habla y se ve la imagen en movimiento. Pasando del videoteléfono a la videoconferencia, *CuSeeMe* permite conectar ocho personas, cada uno frente al monitor de su PC en distintos puntos de la red. No caben dudas de que el sistema aún necesita muchas mejoras en cuanto a la calidad y la velocidad de transmisión. El límite más difícil de franquear es el que impone la propia estructura actual de Internet, con su ancho de banda bastante comprometido.

IRC (*Internet Relay Chat*) es un servicio que permite al usuario, por medio de mensajes, conversar con otros usuarios conectados a servidores de IRC. Aquí los usuarios hablan entre sí usando el teclado, digitando sus opiniones sobre los más diversos temas a través de miles de canales temáticos diferentes. Para participar en IRC hay que contar con un programa específico, que permite acceder a una serie de servidores públicos conectados en red, dedicados a este tipo de comunicación.

WWW (*World Wide Web, Web* mundial) convierte el acceso a la Internet en algo sencillo para el público en general, lo que da a ésta un crecimiento explosivo. Es relativamente sencillo recorrer la *Web* y publicar información en ella, las herramientas crecieron a lo largo de los últimos tres años hasta ser las más populares. Permite unir información que está en un extremo del planeta con otro en un lugar distante a través de algo que se denomina hipervínculo, al

elegir éste comunica con el otro sector del documento o con otro documento en otro servidor de información.

Nace en 1989 en un laboratorio europeo de física de partículas (CERN), los investigadores querían un método único que realizara la actividad de encontrar cierta información, traerla a la computadora y ver algún artículo y/o gráfico a través de una interfaz única, eliminando la complejidad de diversas herramientas.

A finales de 1990 los investigadores ya tenían un navegador en modo texto y uno en modo gráfico para la computadora NEXT. En 1992 se publica para el público en general y a medida que fue avanzando el proyecto, se agregaron interfaces a otros servicios.

La comunidad de Internet adoptó rápidamente esta herramienta y comenzó a crear sus propios servidores de WWW para publicar información, incluso algunos comenzaron a trabajar en clientes WWW. A finales de 1993 los navegadores se habían desarrollado para una gran variedad de computadoras y sistemas operativos y desde allí a la fecha, la WWW es una de las formas más populares de acceder a los recursos de la red.

Para acceder a la WWW se debe ejecutar en la computadora cliente un navegador, ésta es una aplicación que sabe como interpretar y mostrar documentos hipertextuales.

Un documento hipertextual es un texto que contiene vínculos con otros textos, gráficos sonido video y animaciones. Los navegadores más conocidos son el *Mosaic* (uno de los primeros) y actualmente *Netscape* y *Explorer* de *Microsoft*.

Cuando se recupera un documento de la WWW, este es con formato y puede ser visto en distintas computadoras, para asegurarse de que este se vea como se debe ver, existe un formato o lenguaje llamado HTML, que es un conjunto de instrucciones sencillas que indican como se estructura ese documento, el navegador interpreta los comandos HTML y presenta el documento formateado para su visión por el usuario.

En el mercado actual, parece que las empresas deben estar en la *Web*, también llamada telaraña mundial para tener una ventaja competitiva. Por lo tanto, no estar en la *Web* es tener una gran desventaja. Sin duda, si quiere que sus clientes consideren que su compañía esta al día, debe estar conectado. El método más importante para mostrar que está preparado para el próximo siglo es que su empresa esté conectada a Internet. Después de conectarse debe publicar información en la *Web* e invitar a sus clientes a ver los archivos y acceder a los recursos disponibles. Para muchas empresas la presencia en la *Web* se ha convertido en una necesidad, y ha demostrado que es un excelente potencial comercial y financiero y que ésta crecerá más cuando se impongan las técnicas de seguridad y codificación.

La *Web*, el correo electrónico, el ciber-dinero y la seguridad, están tan integrados en el mundo empresarial actual como en los catálogos impresos. Tanto el correo electrónico como la WWW son las aplicaciones más populares de Internet y el principal sustento del comercio electrónico, siempre y cuando estén soportados en un ámbito seguro. La *Web* se ha convertido en un gigante bazar de bienes y servicios, se puede encontrar lo que se quiera en ella, y los portales obtienen una ventaja de esto al agregar vínculos a sitios de comercio electrónico para que lo usuarios encuentren lo que quieren.

Por ejemplo *Shopping Guide* de Yahoo[1] incluye un buscador de precios bajos que permite buscar en toda la *Web* los precios más bajos de un artículo.

1.3.4. Conexión a Internet

Los elementos necesarios de *software* y de *hardware* que se necesitan son relativos al tipo de conexión que quiera establecer, pero como norma general, para que una organización se conecte a Internet se necesitará lo siguiente:

1. El arrendamiento de una línea dedicada con un ancho de banda de 128 Kbps, 256 Kbps, 512 Kbps, 1 Mbps o superior para establecer la comunicación con el ISP (*Internet Service Provider*, proveedor de servicios de Internet).
2. Un ISP que hace de nexo o puente a Internet.
3. Un ruteador para el enrutamiento paquetes entre la red privada e Internet.

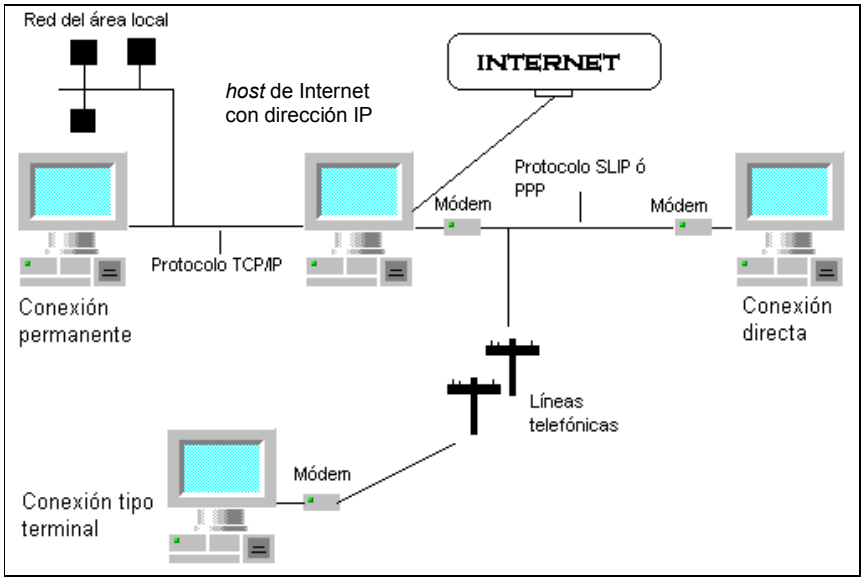
Para poder hacer uso de lo que Internet ofrece, se debe tener una conexión hacia ella mediante un ISP. El tipo de conexión del cual se disponga determina los servicios que se obtendrán, el grado de comodidad y el costo de la misma. Los tres tipos de conexiones disponibles más comunes se describen a continuación:

Conexión *mail*, esta es la forma más sencilla y básica de conexión, y el usuario lo único que puede realizar es enviar y recibir correos electrónicos. El usuario se conecta al ISP a través de medios como la red telefónica y establece la transferencia de mensajes de correo con el servidor de correo electrónico

[1] Yahoo es un motor de búsqueda e índice de contenidos *Web* en Internet

propiedad del ISP. El servidor de correo electrónico del ISP está interconectado con Internet (ver figura 3).

FIGURA 3. Esquemas de conexión a Internet



Por línea telefónica (*dial-up link*), este método es el que ofrecen los proveedores de Internet para el público en general y consta de una computadora conectada mediante un *modem* y una línea telefónica a un ISP mediante un sub-protocolo SLIP (*Serial Link Internet Protocol,* protocolo de Internet de enlace serial) o PPP (*Point to Point Protocol,* protocolo de punto a punto). El mecanismo de conexión es relativamente sencillo, se llama telefónicamente al proveedor ISP y éste hace a modo de servidor de acceso entre la computadora y la red, lo ideal en esto es constar de un *modem* de buena velocidad (56K en la actualidad) y de un proveedor que no esté continuamente saturado. Este servicio es comúnmente utilizado por usuarios individuales u organizaciones muy pequeñas, que no necesitan acceder grandes cantidades de información y que no necesitan publicar servicios en Internet.

Por línea dedicada (*leased lines*), cuando se dispone de este tipo de línea se está continuamente conectado a la red WAN mediante un ruteador, las velocidades de conexión varían desde 56K a 44Mbps. Este tipo de conexión es más cara que la anterior, ya que la empresa está conectada las 24 horas en línea directa a Internet, por lo cual el rendimiento es también mayor. Al disponer de esta línea también se puede ser un proveedor de información. Este tipo de conexión es recomendable para organizaciones que publican en Internet servicios como correo electrónico o comercio electrónico.

1.3.5. Ventajas

Son muchas las ventajas que Internet ofrece, podría llenarse páginas enteras de bondades, pero se tratará de citar las principales.

1. **Acceso global,** se ingresa a la red a través de una llamada telefónica o una línea alquilada directa a Internet y el acceso a la información no posee un costo de comunicación extra para la información, que puede ser localmente o en otro país.
2. **Acercamiento con los clientes,** mediante Internet y el correo electrónico, se tiene llegada a personas e información dentro y fuera de las empresas que para realizarlo por medio de otras tecnologías en algunos casos se tornaría imposible.
3. **Compatibilidades tecnológicas.** Puede accederse de equipos corriendo sistemas operativos gráficos como los sistemas *Windows*[2] o *Mac*[3], a sistemas operativos tipo carácter como algunas versiones de *Unix* y otros

[2] Los sistemas Windows son marca registrada de Microsoft Corp.
[3] Mac es un sistema de computadora personal fabricado por Apple Corp.

en forma transparente, ya que la red se encarga de resolver esta compatibilidad.

4. **Relaciones mediante hipervínculos,** con solo pulsar el botón del ratón se pasa de un servidor de información a otro, en forma transparente y gráfica, lo cual hace muy sencillo obtener información.
5. **Bajo costo,** el costo es relativamente bajo, ya que se abona el costo de una llamada local y el de un ISP que puede oscilar entre US $30 a US $350 mensuales en promedio, dependiendo del tipo de servicio.

2. SEGURIDAD EN REDES DE PERÍMETRO

La seguridad en redes de perímetro ha tomado en los últimos años un auge muy importante, ya que cada vez aumenta la necesidad de conexión de redes corporativas a redes desconocidas con el fin de obtener o proporcionar servicios de información. Muestra de ello es la interconexión de redes a la red mundial Internet.

La seguridad perimetral es la selección inteligente y aplicación de tecnologías de conectividad para asegurar los límites de la red en contra de intrusos. La seguridad perimetral comúnmente es utilizada para asegurar las conexiones a Internet para las redes corporativas, aunque las mismas tecnologías y técnicas pueden ser utilizadas para asegurar una parte de la red de otra. Como una muralla y un foso alrededor de un castillo medieval, la seguridad perimetral corresponde al equivalente de una muralla rodeando la red para protegerla en contra de intrusos.

La falta o debilidad de seguridad perimetral abre un agujero de seguridad en la red y origina que un intruso pueda aprovecharse de ello.

Una parte importante de la seguridad perimetral es identificar los límites de la red al especificar los dominios internos y externos de una red. Por lo general el dominio interno corresponde a la red corporativa o privada, y el dominio externo es el dominio de Internet. El dominio externo podría además ser un enlace para los socios de negocios o proveedores.

La seguridad perimetral usualmente utiliza una variedad de dispositivos y mecanismos de protección como *firewalls*, ruteadores de filtrado de paquetes, servidores de autenticación de usuarios, herramientas de auditoría y gestión de seguridad, etc.

Como parte de la seguridad perimetral, debe existir continua vigilancia de ataques y un plan de verificación regular del estado de las infraestructuras de seguridad. Un escáner de vulnerabilidades de red puede pro activamente identificar áreas de debilidad mientras que los sistemas de detección de intrusiones pueden vigilar y responder a eventos de seguridad en tiempo real. Los sistemas de detección de intrusiones y los escáneres de vulnerabilidades proveen un nivel adicional de seguridad de red. Mientras los *firewalls* permiten o deniegan tráfico basado en la fuente, destino, puerto, u otro criterio, ellos no analizan realmente el tráfico dañino o descubren en la red vulnerabilidades existentes.

La seguridad perimetral puede ser implementada en muchas formas diferentes, dependiendo sobre todo en: políticas de seguridad, recursos por proteger, el nivel de seguridad necesario, los presupuestos de seguridad y muchos otros factores.

Al principio del capítulo se comenzará describiendo los orígenes de la seguridad en redes de computadoras y la naturaleza de la misma.

2.1. Introducción a la seguridad de redes de computadoras

Durante las primeras décadas de su existencia, las redes de computadoras fueron usadas principalmente por investigadores universitarios para el envío de correo electrónico, y por empleados corporativos para compartir impresoras. En

estas condiciones, la seguridad no recibió mucha atención. Pero ahora, cuando millones de ciudadanos comunes usan redes para sus transacciones bancarias, compras y declaraciones de impuestos, la seguridad de las redes aparece en el horizonte como un problema potencial de grandes proporciones.

La seguridad en su forma más sencilla, se ocupa de garantizar que los curiosos no puedan leer, o peor aún, modificar mensajes dirigidos a otros destinatarios; se preocupa por la gente que intenta acceder a servicios remotos no autorizados. La seguridad también se ocupa del problema de la captura y reproducción de mensajes legítimos, y de la gente que intenta negar que ha enviado ciertos mensajes.

2.2. Origen de la seguridad

La mayoría de los problemas de seguridad son causados intencionalmente y por gente maliciosa que intenta ganar algo o hacerle daño a alguien. Es importante notar que hacer segura una red comprende mucho más que simplemente mantener los programas libres de errores; implica ser más listo que adversarios a menudo inteligentes, dedicados y a veces bien financiados. Debe quedar claro también que las medidas para detener a los adversarios casuales tendrán poco impacto sobre los serios.

Los problemas de seguridad pueden dividirse en términos generales en cuatro áreas interrelacionadas: secreto, validación de identificación, no repudio y control de integridad. El secreto tiene que ver con mantener la información fuera de las manos de usuarios no autorizados. Esto es lo que normalmente viene a la mente cuando la gente piensa en la seguridad de las redes. La validación de identificación se encarga de determinar con quién se está hablando antes de revelar información delicada o hacer un trato de negocios.

El no repudio se encarga de las firmas: ¿cómo comprobar que un cliente realmente colocó una orden electrónica por 10 millones en productos a 100 la unidad, cuando él alega que el precio era de 10?, o además, ¿cómo puede asegurarse de que un mensaje recibido realmente fue el enviado?, y no algo que un adversario malicioso modificó en el camino.

Todos estos problemas en las redes tienen su analogía en los sistemas tradicionales o manuales, con algunas variantes muy significativas. La gente puede por lo general distinguir entre un documento original en papel y una fotocopia, y con frecuencia esto es importante. Las personas pueden validar la identificación de otra gente al reconocer sus caras, voces y letra. Las pruebas de firmas se manejan mediante firmas de papel, sellos, etc. Generalmente puede detectarse la alteración de documentos con el auxilio de expertos en escritura, papel y tinta. Ninguna de estas opciones está disponible electrónicamente. Es obvio que se requieren otras soluciones.

2.3. Complejidades de seguridad

El arte de implementar una seguridad altamente efectiva dentro de una organización es un proceso que conlleva muchas actividades, algunas de ellas complejas. El crecimiento incontrolado de carga en sistemas de computación e infraestructuras de red ha sido mucho mayor al crecimiento y asignación de presupuestos para la protección de los recursos informáticos en las organizaciones. Las organizaciones actuales demandan servicios de sistemas externos a las organizaciones, tal es el caso de acceso a la *Web*. Las organizaciones están generando grandes cantidades de tráfico, sin premeditar las implicaciones que podrían resultar del uso incontrolado de los servicios en medios externos.

El problema de seguridad visto desde la organización, es que son requeridas sofisticadas defensas de seguridad para continuar con la protección de las últimas técnicas de *hackers* y reducir las vulnerabilidades de los negocios. Todavía la seguridad resulta complicada para implementarse debido a que se necesita de una solución amplia que deba cubrir toda la basta gama de productos utilizados actualmente en las redes.

Es dificultoso implementar la seguridad uniformemente en toda la organización, debido a que algunas soluciones solamente trabajan en el campo central, mientras otras solamente trabajan en las redes de área amplia (WAN). Algunas soluciones de seguridad trabajan bien para organizaciones pequeñas, pero resultan imprácticas en términos de esfuerzo, tiempo o costo, a la vez que la organización va en crecimiento. Este problema de seguridad está compuesto por la suma de vulnerabilidad creada por la conexión a Internet, la cual da una entrada potencial al intruso hacia la infraestructura de la organización.

Es importante hacer notar que el desafío en la implementación de seguridad no solamente implica tecnología, es muy importante que la organización posea políticas de seguridad en donde se haga de ver los diferentes roles del personal con el fin de dedicar el máximo esfuerzo en la administración de la seguridad.

Con mayor frecuencia surgen nuevas tecnologías de seguridad, las cuales son difíciles de implementar debido al ritmo acelerado con que éstas surgen. Parte de ello, origina que para satisfacer las necesidades de protección se apliquen demasiados recursos con el fin de lograr evaluar las tecnologías más efectivas.

2.4. Deficiencias de seguridad

Las redes centrales, de *dial-up* y redes que tienen acceso a Internet están siendo ampliamente implementadas en los entornos de negocio actuales. Todavía cada uno de estos entornos de red posee problemas y riesgos de seguridad de redes.

Hay tres razones primarias por las que se tienen deficiencias en la seguridad de las redes:

1. Debilidades de tecnología
2. Debilidades de configuración
3. Debilidades de políticas

Hay mucha gente ansiosa, dispuesta, y calificada para tomar ventaja de cada una de las debilidades de seguridad, y continuar descubriendo y explotando nuevas debilidades.

2.4.1. Debilidades de tecnología

Las tecnologías de computación y de red tienen debilidades de seguridad intrínsecas.

Debilidades del protocolo TCP/IP, el protocolo TCP/IP fue diseñado como un estándar abierto para facilitar las comunicaciones. Por ejemplo: El *daemon* de *Sendmail*[4] en el entorno del sistema operativo UNIX puede permitir acceso al directorio raíz de UNIX; el sistema de archivos de red (NFS) puede habilitar la

[4] Sendmail es un sistema de correo electrónico en sistemas Unix

validación insegura de acceso a los *hosts*. Muchos otros servicios de TCP/IP son inseguros.

Debilidades en sistemas operativos de red, cada sistema operativo tiene problemas de seguridad que deben ser corregidos. Por ejemplo: Los sistemas operativos UNIX, *Windows* NT[5], OS/2[6].

Debilidades en equipos de red, los equipos de red poseen debilidades de seguridad que deben ser reconocidas y protegidas en contra de: protección de contraseñas, falta de autenticación, protocolos para rutas de redes, hoyos en *firewalls*.

2.4.2. Debilidades de configuración

Los problemas de seguridad son muy frecuentemente causados por debilidades en la configuración:

Cuentas inseguras de usuarios, la información de las cuentas de usuario puede ser transmitida inseguramente a través de la red, exponiendo nombres de usuario y contraseñas a personas sin autorización.

Cuentas de sistema con contraseñas fácilmente adivinadas, este problema bastante común, es el resultado de la asignación de contraseñas de usuarios mal seleccionadas y fácilmente adivinadas.

[5] Windows NT es un sistema operativo registrado por Microsoft Corp.
[6] OS/2 es un sistema operativo registrado por IBM

Servicios de Internet mal configurados, un problema común es que al permitir Java y *JavaScript* en *browsers* de *Web*, permite que haya ataques vía *Applets host*iles.

Configuraciones inseguras por definición en los productos, muchos productos que tienen configuraciones por defecto activan hoyos de seguridad. Por ejemplo el servicio de *Internet Information Server*[7] de *Windows* 2000 trae consigo ejemplos que permiten a un intruso ejecutar comandos remotos.

Equipos de red mal configurados, la mala configuración de un equipo puede causar significativamente problemas de seguridad. Por ejemplo, por mala configuración en protocolos de rutas, o comunidades de SNMP pueden abrir grandes hoyos de seguridad.

Los administradores de red o ingenieros de red pueden aprender las debilidades que traen consigo los dispositivos de red y computación, así como la forma de cómo deben configurarse para eliminar éstas debilidades.

2.4.3. Debilidades de políticas de administración

Los problemas de seguridad pueden ser causados por debilidades en las políticas de seguridad, que la organización aplica para protección de los recursos informáticos. Un mayor detalle de las políticas será desarrollado posteriormente sobre este capítulo.

[7] Internet Information Server es un servicio de publicación *Web* fabricado por Microsoft Corp

a. Falta de una política de seguridad escrita.
b. Malos controles de acceso físico.
c. Controles de acceso lógico no aplicados.
d. Administración de seguridad floja, incluyendo el monitoreo y auditoría.
e. Instalación y cambios en el *hardware* y *software* no siguen las políticas.
f. Planes de contingencias no planeados.
g. Falta de continuidad, no se puede implementar una política eventualmente.

2.5. Conociendo al enemigo

Se puede proteger de mejor manera la red si se conocen las características de los intrusos. Los intrusos que tratarán de ganar acceso a la red corporativa podrían ser los siguientes:

a. Ex empleados *host*iles buscando venganza o provecho propio.
b. Empleados o usuarios persiguiendo actividades involuntarias, empleados que accidentalmente permiten un virus u otro programa dañino.
c. Empleados que mal administran los entornos de red, empleados que no usan contraseñas seguras, o que configuran mal los equipos de red.
d. Buscadores de emociones, muchos intrusos hacen su trabajo por emoción o para impresionar a la gente.
e. Competidores o espías que buscan tratar de ganar acceso a información confidencial, espionaje industrial.
f. Enemigos, a muchos gobiernos les preocupa la guerra de información.
g. Ladrones, intrusos quienes buscan información específica y valiosa.

Un intruso es un individuo que intenta ganar acceso a la red o recursos de computadoras sin autorización. El intruso puede ser mejor clasificado ya sea

como *craker* o como *hacker*. Por su localización, los intrusos pueden ser internos o externos. Un intruso externo se encuentra en la parte externa de la red privada, y es quien puede atacar sistemas tales como servidores *Web*, servidores de correo electrónico, etc. Ellos pueden también intentar atravesar el *firewall* para atacar máquinas dentro de la red interna.

Un *cracker* es cualquier individuo quien usa conocimiento avanzado para probar o comprometer la seguridad de la red sin autorización. Usualmente tiene intenciones maliciosas de robo o destrucción de información.

Un *hacker* es cualquier individuo que investiga la integridad y seguridad de un sistema operativo o red. Usualmente es un programador. Utiliza conocimiento avanzado de *hardware* y *software* para violar los sistemas de formas innovadoras. Libremente comparte su conocimiento con otros. Usualmente no tiene intenciones maliciosas.

La intrusión de red empezó con personas consiguiendo acceso sin autorización a los recursos de telecomunicaciones. Los primeros intrusos de red comúnmente tenían las siguientes habilidades y características:

a. Programación en lenguajes como: C, C++, Perl, CGI, *Microsoft Visual Basic*.
b. Conocimiento a fondo de TCP/IP.
c. Mucha experiencia al usar Internet.
d. Conocimiento íntimo de por lo menos dos sistemas operativos.
e. Trabajos utilizando computadoras o redes.

Las técnicas y herramientas de intrusión de red hoy en día son ampliamente conocidas y disponibles. El intruso de red actual tiene habilidades y características como las siguientes:

Puede obtener herramientas de *software* previamente escritas de *hackers* en Internet. Hay muchas de las herramientas de intrusión de red y de pruebas, las cuales su código fuente está disponible y cada día aumenta la cantidad.

Usa *scripts* previamente escritos y utilidades en formas creativas para introducir dentro de sistemas de red y computación. Es capaz de utilizar herramientas que automáticamente descubren debilidades de una red.

Pertenece a grupos que tienen el suficiente tiempo para experimentar y desarrollar técnicas. Puede ser un estudiante o un aficionado con su pasatiempo preferido y con un gran interés en tecnología.

El intruso tiene motivos para querer penetrar dentro de una red corporativa. Por ejemplo, un empleado interno de la compañía desde su casa podría querer ganar acceso interno a la corporación en horas inhábiles, motivado por el acceso a datos gerenciales de la compañía. Los siguientes corresponden a motivos por los cuales los intrusos hacen penetraciones en redes sin autorización:

a. Provecho o robo
b. Venganza, rencor
c. Vandalismo
d. Fanatismo
e. Anarquía
f. Guerra cibernética
g. Espionaje nacional
h. Espionaje industrial
i. Idealismo
j. Desafío
k. Aburrimiento

l. Ignorancia
m. Curiosidad
n. Aprendizaje
o. Necesidad de aceptación

Sin importar la motivación, se debe encontrar métodos para obstruir la penetración a los intrusos a las redes internas. Sin embargo, una vez el intruso haya violado la seguridad perimetral dependerá realmente el motivo que lo impulsa para ejecutar los planes que tiene previstos con los recursos de sistemas internos. El grado de riesgo en pérdidas y daños que podría ocasionar un intruso estará directamente relacionado con la motivación del intruso.

2.5.1. Tipos generales de amenazas

El vasto rango de amenazas de seguridad en redes que se encuentran conectadas a Internet desafía los esfuerzos para clasificarlas, entender qué son, e idear métodos para protegerse contra ellas. A continuación se describen grupos de amenazas de seguridad en redes e introducción de métodos específicos usados para penetración de redes.

Escuchar por detrás de la puerta. Un método común para hacerlo en comunicaciones, es capturar paquetes de TCP/IP u otros protocolos y decodificar los contenidos utilizando un analizador de protocolos o utilidades similares. Los intrusos de red pueden entonces identificar nombres de usuarios, contraseñas o información llevada en paquetes, tales como número de tarjetas de crédito o información personal sensible. La intromisión de redes y análisis de paquetes son términos comunes para esta amenaza. La

información obtenida por esta amenaza, puede entonces ser usada para plantear otros ataques a la red. Algunos métodos de esta amenaza:

a. Husmeadores de red y analizadores de protocolos.
b. Utilidades de captura de paquetes en computadores de red.

Un ejemplo de datos susceptibles a esta amenaza, son los *strings* de comunidad del SNMP (*Simple network management protocol,* protocolo de manejo de red simple) versión 1, los cuales son enviados en texto puro. Un intruso podría obtener información en las consultas de SNMP y aprender datos valiosos de configuración de los equipos de red. Otro ejemplo es la captura de nombres y contraseñas de usuarios cuando atraviesan la red.

Robo de información. Un método muy común para los intrusos es tomar archivos o usar recursos que no le pertenecen. Los ejemplos incluyen penetrar la seguridad de instituciones financieras y obtener números de tarjetas de crédito. Otro ejemplo es atacar una computadora para obtener sus propios archivos de contraseñas.

Acceso no autorizado. Un intruso de red puede ganar acceso no autorizado a computadoras de red o dispositivos de redes, mediante una variedad de medios. Una meta común del intruso es ganar acceso a la cuenta de *root* (UNIX) o administrator (*Windows* NT) de una computadora de red, donde el intruso tenga gran potencial de acceso a otras computadoras. Los siguientes representan algunos medios para ganar acceso:

Ataques de contraseñas. El intruso captura una contraseña cifrada en la red o copia de archivo de contraseñas de una computadora de red, y trata de obtener las contraseñas utilizando alguna herramienta especial de decodificación.

Ingeniería social. Un método para obtener información de dispositivos de seguridad es convencer a alguno para revelar información necesaria, tal como nombres de usuarios y contraseñas, u otra información importante.

Explotación de servicios de TCP/IP. Cómo usar el servicio de Sendmail para ganar acceso a la cuenta de *root*.

Explotación de agujeros en sistemas operativos. Cada sistema operativo tiene agujeros inherentes o vulnerabilidades que un intruso de red puede explotar para obtener acceso no autorizado.

Explotación de acceso válido en el sistema operativo. Una vez el intruso tiene acceso a la computadora de red, este acceso es explotado para ganar acceso a otras computadoras de red, usando las relaciones de confianza entre ambas computadoras.

Manipulación de datos. El intruso de red puede capturar, manipular, y volver a enviar los datos sobre el canal de comunicación. Los ejemplos incluyen los siguientes:

***Graffiti*.** Vandalismo sobre un sitio *Web* entrando al servidor de *Web* y alterando las páginas que publica.

Manipulación de datos sobre una computadora. El intruso entra en la computadora de red, y entonces altera archivos en la computadora, tales como archivos de contraseñas, permitiendo mayor acceso a la red.

Disfraz. El intruso de red puede manipular paquetes de TCP/IP para falsificar direcciones de IP, aparentando ser otro usuario. El intruso asume la identidad de un usuario válido y gana los privilegios de acceso del usuario a través de IP

spoofing, donde los intrusos pueden crear paquetes de datos IP con direcciones fuentes falsificadas.

Repetición de sesión. Una secuencia de paquetes o comandos de aplicación, pueden ser capturados, manipulados y vueltos nuevamente para causar una acción no autorizada, la cual explota debilidades en autenticación de usuarios o servicios.

Asalto de sesión. El intruso puede insertar paquetes de datos IP falsificados después del establecimiento de una sesión. Los métodos utilizados son los siguientes:

a. IP *spoofing*
b. Manipulación de direcciones fuente y destino sobre TCP/IP.
c. Predicción y alteración de números de secuencia, el intruso usa un analizador de protocolos o programa utilitario para observar, predecir y luego alterar y retransmitir números de secuencia de paquetes TCP/IP.

Cambio de ruta. Los paquetes de un usuario A son intencionalmente cambiados de dirección hacia el usuario B, para que el usuario B pueda interceptar los paquetes y hacer mal uso de ellos. Las actualizaciones de información de rutas de los enrutadores pueden ser manipuladas para hacer que el tráfico fluya hacia destinos no autorizados.

Repudio. Uno o más usuarios dentro de una comunicación, tal como una transacción financiera segura, puede negar haber participado, poniendo en peligro transacciones electrónicas y acuerdos de contratos de negocios.

Destrucción maliciosa. Intrusos pueden causar destrucción a computadoras de red al eliminar archivos vitales o corrompiendo registros de bases de datos. Las técnicas comunes son las siguientes:

a. Acceso de computadoras de red y eliminación de archivos de información y de sistema importantes o formateando unidades de discos.
b. Replicación de código de programas de virus que modifican código de programas ejecutables o dañan unidades de discos de computadoras de red.
c. Caballos de Troya, programas dañinos que se esconden dentro de programas legítimos y son activados durante la ejecución normal de programas legítimos.
d. Programas maliciosos realizados en lenguajes como Java, componentes de *ActiveX* o *JavaScript*.

Denegado de servicio. Intentos deliberados para degradar el rendimiento de un sistema de computación o red, e impedir a personal autorizado el uso de los recursos o acceso a servicios de sistemas de red. Los usuarios son afectados de muchas maneras. Algunas técnicas de denegado de servicio:

a. *Ping* de la muerte. Modifica la porción del encabezado de IP indicando que hay más datos en el paquete del que realmente hay, o excede el máximo tamaño del paquete permitido, causando que el sistema receptor quede sin comunicación.
b. Ataque SYN *flood*. En forma aleatoria abre muchos puertos TCP enviando peticiones de conexión ficticias al sistema de red. El sistema de red al llegar al máximo de conexiones abiertas soportadas colapsa, lo que origina una caída de las comunicaciones.

c. Bombas de correo electrónico. Existen muchos programas de forma gratuita, que envían grandes volúmenes de información a individuos, listas o dominios para degradar los servidores de correo electrónico.
d. Posesión del CPU, programas como caballos de Troya o virus (Java, *JavaScript* o *ActiveX*) que aumentan la carga de CPU del computador, memoria u otros recursos, denegando recursos a usuarios legítimos.
e. Deshabilitar tráfico de *Web* al borrar la configuración de ruteadores para cambiar de dirección el tráfico.
f. El ataque cargador, establece una conexión entre servicios de UDP, produciendo una alta salida de caracteres. El servicio del *host* cargado, es conectado de vuelta al servicio, ya sea en el mismo o diferente sistema, el cual causa congestión en la red con carga de tráfico en forma de eco.
g. Ataque fuera de banda *WinNuke*, envía datos fuera de banda al puerto 139 en sistemas *Windows* 95[8] o *Windows* NT mediante el conocimiento de la dirección IP de la víctima.
h. Land.C, este programa envía paquetes TCP SYN que especifica la dirección del *host* destino como ambos destino y fuente. El programa también usa el mismo puerto (113 o 139) en el *host* destino como ambos fuente y destino, el cual hace que el sistema destino pare de funcionar.

2.6. Política de seguridad perimetral

En un sentido general, la política está formada por declaraciones o interpretaciones generales que orientan o encauzan el pensamiento al tomar decisiones dentro de un marco de trabajo.

[8] Windows 95 es un sistema operativo registrado por Microsoft Corp.

La política de seguridad es la declaración de una estrategia administrativa, tomando en cuenta la seguridad como punto central. La política de seguridad está enfocada en áreas como corporación, recursos de información, personal, física y de entorno, redes y computadoras y planificación continua de negocios.

Una política de seguridad de redes es una declaración formal de reglas por seguir al definir el acceso a recursos de tecnología e información, dentro de una organización. Previo al diseño, implementación y control de seguridad de redes, se debe implementar una política de seguridad de redes global. Cuando se define una política de seguridad de red, se deben definir los procedimientos para resguardar los usuarios y recursos de la red contra daños y pérdidas. De esta perspectiva, una política de seguridad de red juega el rol de reforzar en conjunto la política de seguridad definida por la organización. Una política de seguridad de red se enfoca en controlar el tráfico y uso de la red. Identifica los recursos de red y amenazas, define el uso de la red y responsabilidades, y detalla planes de acción para cuando la política de seguridad es violada. Cuando se diseña una política de seguridad de red, se desea que sea estratégicamente reforzada con límites defendibles dentro de la red. Estos límites estratégicos son lo que se conocen como redes de perímetro.

La política de seguridad perimetral, se enfocan a definir el marco de trabajo y las normas bajo las cuales se determinará el acceso de recursos, dentro de las redes privadas y la forma en que se tomarán recursos de redes externas. La política de seguridad perimetral proporciona la base, al tomar una decisión del acceso a nuevos recursos y servicios, la cual afectará los recursos protegidos dentro de las redes corporativas. La política ayuda a las personas que se encargan de la protección de las redes de perímetro a definir los procedimientos necesarios, dependiendo de la situación que se presente.

2.6.1. Propósitos de la política

El propósito principal de una política de seguridad es informar a usuarios, equipo y administradores de sus requerimientos obligatorios para la protección de recursos de tecnología e información. La política debe especificar los mecanismos por medio del cual, estos requerimientos pueden ser cumplidos. Otro propósito es proveer una base al adquirir, configurar y auditar sistemas de computación y redes para cumplimiento con la política.

La política de seguridad aplicada a redes de perímetro provee muchos beneficios, razón por la cual es importante el tiempo y esfuerzo empleado para su desarrollo. A continuación se presentan algunas de las razones por las cuales se debe desarrollar la política de seguridad de red corporativa y perimetral:

a. Provee un proceso para auditar la seguridad de red existente, encontrar debilidades, fortalezas, riesgos, necesidades, etc.
b. Provee un marco de trabajo general para implementar la seguridad de red perimetral.
c. Define conductas permitidas y no permitidas.
d. Con frecuencia define el escenario, en términos de cuales herramientas y procedimientos de red son necesarios.
e. Ayuda a comunicar acuerdos generales entre divisiones de gerencia y definen las responsabilidades de usuarios y administradores.
f. Define un proceso para el manejo de incidentes.
g. Permite la implementación y aplicación de seguridad, no sólo del área perimetral sino también de áreas más generales.
h. Crea una base para acciones legales, en caso sea necesaria por razones de violación de la seguridad en el perímetro.

2.6.2. Características importantes de una política de seguridad

Para que exista buena protección de seguridad en las redes, se debe tener una buena política de seguridad, la cual a su vez debe cumplir con las siguientes características claves:

a. Debe ser capaz de ser implementada, tanto en el ámbito técnico, como en el organizacional.
b. Debe ser aplicable con herramientas de seguridad, donde conviene, con sanciones, donde la actual prevención no es técnicamente factible.
c. Debe definir claramente las áreas de responsabilidad de los usuarios, administradores y manejo.
d. La política debe ser flexible y conservable al adaptarse a cambios en el entorno.

2.6.3. Diseño de la política

Para desarrollar un plan de seguridad en el área de red que se protegerá, se deben tomar en cuenta, generalmente los siguientes aspectos:

a. Identificar qué se está tratando de proteger.
b. Determinar qué se trata de proteger.
c. Determinar la probabilidad de las amenazas.
d. Implementar medidas que protegerán los recursos en una forma costo-beneficio.
e. Revisar el proceso continuamente y hacer mejoras cada vez, a las debilidades encontradas.

Algunas prácticas sobre como crear un equipo de política de seguridad y diseño de un documento de política de seguridad:

a. Elegir el equipo para desarrollo de la política con derechos representativos.
b. Designar una persona para servir como el interpretador de la política oficial.
c. Decidir el alcance y metas de la política.
d. Decidir la especificidad y detalle de la política.

Se deben tomar las siguientes consideraciones, al diseñar y evaluar una política de seguridad:

a. Separación de servicios de red.
b. Permitir todo tráfico de red- política más abierta. Permitir todo, excepto lo que se está denegado.
c. Denegar todo tráfico de red- política más restrictiva. Denegar todo. excepto lo que está permitido. Permitir servicios específicos.
d. Identificar las necesidades reales de servicios.
e. Proteger la infraestructura.
f. Proteger la red.
g. Proteger los servicios.
h. Proteger la protección. Proteger los sistemas de seguridad claves.

2.7. Aspectos de seguridad en la conexión de una red corporativa a Internet

Hoy, muchas organizaciones están comprendiendo que para competir en un mercado *global* deben migrar sus procesos de negocios más importantes a la

Internet. Esta idea, denominada comúnmente como *e-business* o comercio electrónico, es una transformación a gran escala para muchos negocios, y a la vez necesaria. Las organizaciones están tomando ventajas de las tecnologías de Internet para ensanchar sus segmentos de mercados, para entrar dentro de nuevos o extendidos campos de negocios, para incrementar la productividad de empleados, y para construir relaciones entre socios de negocios no importando la localidad.

Sin embargo, mientras las organizaciones comienzan a explotar los beneficios de la Internet y las tecnologías de *Web*, están aprendiendo rápidamente que existen riesgos inherentes relacionados, al conectar sus redes organizacionales a la Internet.

Específicamente, el proceso de exponer valiosos sistemas corporativos y datos, a una amplia audiencia significativamente, incrementa el riesgo de ataque. Mientras esta transformación ocurre, significativamente incrementa la dependencia en la seguridad, disponibilidad y manejabilidad. Ahora, la seguridad no solamente juega el rol de protector sino también de hacer posible el *e-business*.

La Internet es generalmente reconocida, por tener muchas limitaciones de seguridad en la información, así como la incapacidad de prevenir la interceptación de mensajes, los cuales atraviesan redes inseguras. Esto es, debido al primer objetivo bajo el cual la Internet fue fundada, que era servir como un medio de comunicación entre investigadores, desarrolladores, científicos quienes necesitan rápido y fácil acceso a la información de otros. Los primeros usuarios de Internet estaban menos preocupados por los asuntos de seguridad y control en sus enlaces de comunicación, que en tener medios eficientes para compartir información. Como resultado, muchas infraestructuras

desprotegidas fueron desarrolladas para permitir compartir información y recursos.

Internet ha crecido, esto permite mayores formas de ataque a la seguridad en red, incluyendo los virus, Caballos de Troya y penetración de las redes internas. Una red conectada con el Internet abraza un nuevo conjunto entero de riesgos, algunos de los cuales sirven para excitar los problemas existentes. Las redes de las organizaciones que siguen siendo no relacionadas a la presión de la cara de Internet de hacer esa conexión, si apenas para el correo electrónico solamente. La presión de conectar se convierte a menudo tan fuerte, que algunos usuarios o departamentos individuales conectan con la Internet sin la autorización o el conocimiento superior de la gerencia.

Conectar con la Internet, es como abrir las cortinas en las ventanas de la oficina y dejar en el fulgor completo del sol del mediodía. Problemas previamente invisibles de la seguridad de la red se lanzan en el contraste sostenido. Por ejemplo, cuentas del usuario no protegidas y obviamente contraseñas con palabras de paso, no pudieron haber causado mucha señal de socorro cuando la red era visible solamente a iniciados. Pero, si la gente manipulará la red desde el exterior (algo experimentado por uno de cada seis respondedores en algunas encuestas), se puede apostar que estas debilidades serán explotadas. Las noticias de tales vulnerabilidades, conducen a los ataques y al abuso rápidamente de extensión del sistema.

El entendimiento de los riesgos asociados con la conexión a Internet y los servicios de información en Internet, deberían de ser mucho más importantes que evaluar propiamente las oportunidades de negocios, la cual acompaña una conexión a Internet.

Muchas organizaciones están interesadas en conectarse a la Internet, pero les preocupa el asunto de la seguridad y por eso limitan su uso a investigación, mercadeo y actividades de comunicación.

2.7.1. Debilidades de seguridad en Internet

No existe propietario o dueño de la Internet. Por esa razón, la responsabilidad por seguridad, es solamente tomada sobre quienes tienen interés y preocupación en asegurar sus servicios.

Una conexión a Internet puede proveer a externos el acceso a la información interna de una organización Los individuos fuera de alcance del control y jurisdicción legal de una organización pueden ganar conexión a la red de una organización. La Internet es frecuentemente utilizada por muchos individuos especializados en penetrar los sistemas de seguridad sin ser detectados, estos "*hackers*" pueden ser altamente persistentes en sus esfuerzos de ganar acceso sin autorización, a las redes protegidas de una organización.

La Internet provee una ruta cómoda para enviar información confidencial al resto del mundo. Esta información puede ser interceptada y leída por extraños (por ejemplo, *hackers*, competidores, administradores curiosos de red, o aun gobiernos extranjeros). La Internet provee fácil acceso a recursos y servicios, los cuales pueden conducir a improductividad para los empleados de la organización, a no ser que haya monitoreo y protección, los empleados podrían gastar valioso tiempo utilizando la Internet para entretenerse.

La Internet es más segura mientras existan menos enlaces de redes corporativas conectadas directamente hacia ella. Las organizaciones con muchas localidades necesitan asegurar la mínima conectividad a Internet, utilizando para ello un solo canal de comunicación hacia Internet. De otra manera, una simple localidad podría colocar a una organización entera en riesgo. Los tipos de servicios que una organización provee a los usuarios pueden también incidir en riesgos de seguridad.

2.8. Análisis de incidentes y tendencias de seguridad en Internet

Esta sección presenta algunos resultados de la encuesta anual "2003 CSI/FBI *Computer Crime and Security Survey*" que se relacionan con incidentes de seguridad en Internet. Esta encuesta es dirigida como un servicio público por el "Instituto de Seguridad Computacional", *Computer Security Institute* (CSI), con la participación del *San Francisco Federal Bureau of Investigation* (FBI) y abarca un estudio profundo sobre la frecuencia con que el crimen computacional ocurre y las pérdidas en que incurren las organizaciones. La meta de este esfuerzo es ayudar a alcanzar el nivel de conciencia de seguridad, así como asistir en la determinación del alcance del crimen computacional en los Estados Unidos.

Basado en las respuestas de quinientas treinta corporaciones, agencias de gobierno, instituciones financieras, instituciones médicas y universidades de los Estados Unidos, para el año 2003 se muestra que por primera vez desde 1999, ha habido disminución en la severidad y costos de los ataques, no obstante, la frecuencia de los ataques persiste.

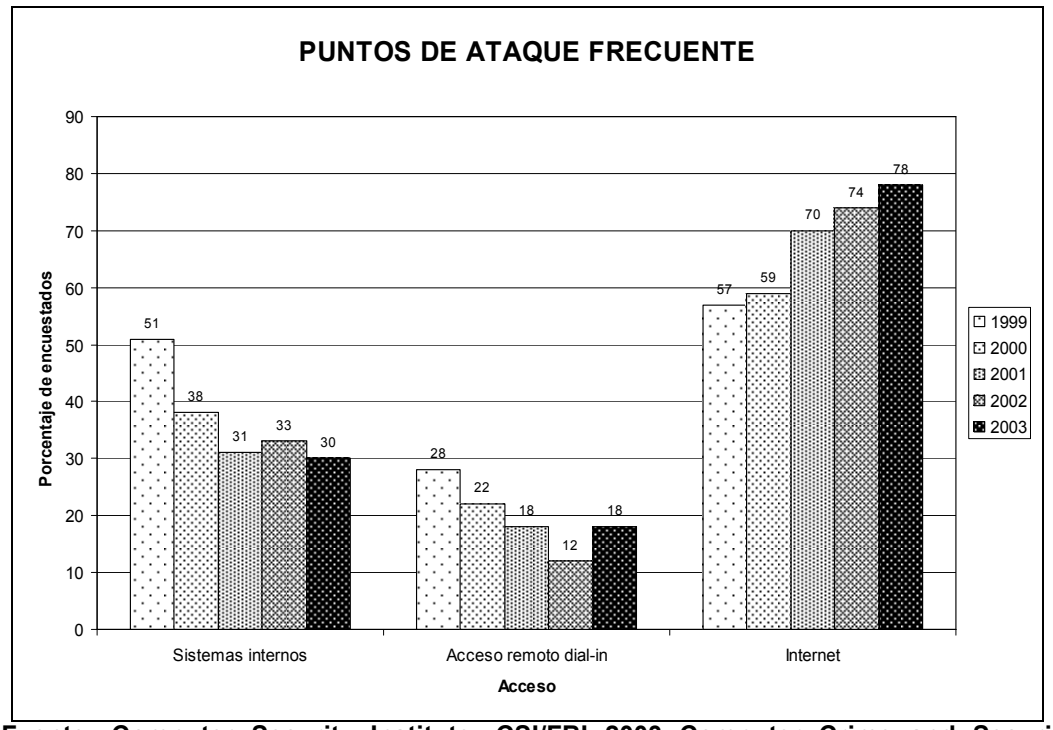
2.8.1. Resultados del riesgo de Internet

La encuesta muestra, que a pesar de que han disminuido las pérdidas financieras, la más importante conclusión, es que el riesgo de ataques en Internet continúa siendo alto y en crecimiento, según se observa en la figura 4. Aún organizaciones que han implementado un amplio rango de tecnologías de seguridad, pueden ser víctimas de pérdidas significantes.

Algo que además se menciona en la encuesta, es que el porcentaje de incidentes que han sido reportados a agencias legales permanece bajo, como consecuencia, los *hackers*, infieren en que las posibilidades de ser atrapados y procesados están a su amplio favor.

Como consecuencia, se resalta que la conexión a Internet es el causante directo del segundo crimen computacional, que ha provocado más pérdidas financieras, el cual corresponde al denegado de servicio, únicamente superado por el robo de información de propiedad intelectual.

FIGURA 4. Gráfica comparativa anual sobre los puntos de ataque

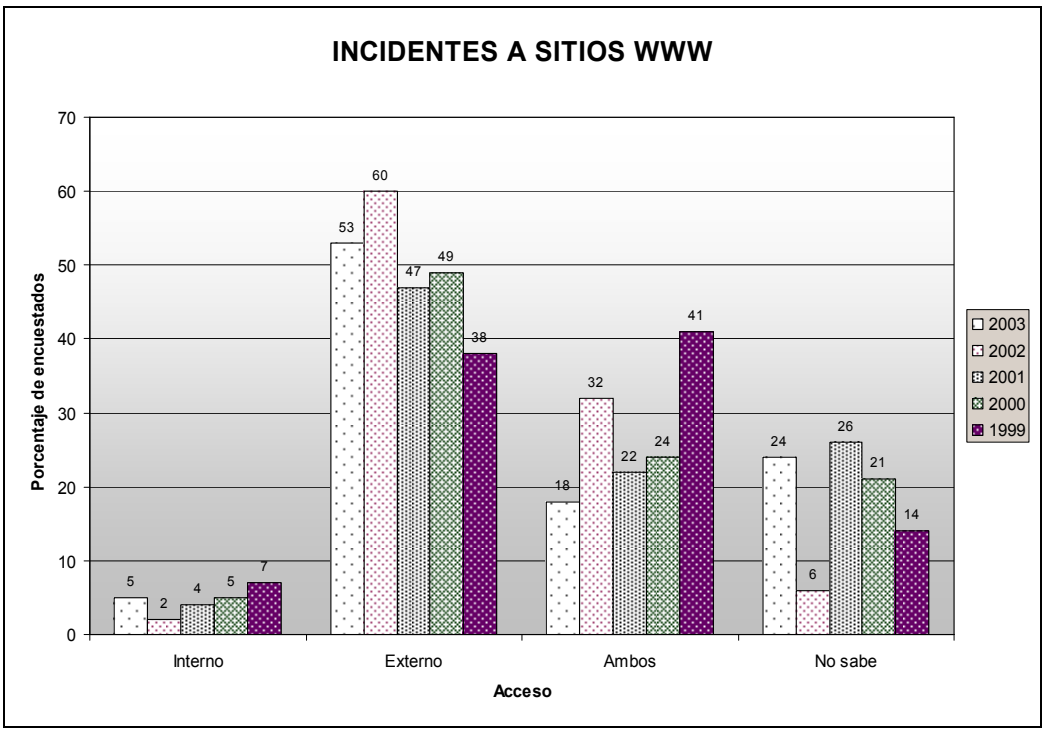


Fuente: Computer Security Institute. CSI/FBI 2003 Computer Crime and Security Survey

2.8.2. Resultados del riesgo en publicación de servicios WWW

Con relación a incidentes asociados con el servicio de red de más uso mundialmente, la *Web* (WWW), se ha registrado que Internet ha sido el punto de conexión desde donde se han efectuado la mayoría de estos ataques, según se puede observar en la figura 5. Al observar la tendencia anual de ataques desde Internet, se percibe que a nivel general el número de casos ha ido en incremento, dando como muestra que una vez más, Internet representa un riesgo a los servicios de publicación de información. De los incidentes a sitios *Web* se han registrado los siguientes tipos de acceso inautorizado: robo de información transaccional (6%), denegado de servicio (35%), fraude financiero (4%), vandalismo (36%), otros (19%).

FIGURA 5. Gráfica de incidentes a sitios *Web*



Fuente: Computer Security Institute. CSI/FBI 2003 Computer Crime and Security Survey

3. ARQUITECTURA DE SEGURIDAD PERIMETRAL

3.1. Introducción a las redes de perímetro

La seguridad en redes de perímetro define un conjunto de elementos y mecanismos de protección que deben ser combinados y colocados estratégicamente dentro de una zona de seguridad mediante la cual se reduzcan los riesgos de ser víctima de algún ataque. Actualmente muchos de los ataques son ya popularmente conocidos, lo que permite tener una ventaja en la protección de redes, sin embargo en este mismo momento se pueden estar construyendo otros tipos de ataques, que en el momento menos esperado, pueden llegar a ocasionar daños.

La arquitectura en redes de seguridad, trata la definición de un modelo que especifica los servicios de seguridad comunes, que serán cubiertos por la tecnología y otros mecanismos, algunos de los servicios típicos son: autenticación, confidencialidad, acceso, monitoreo de seguridad. También ayuda a reconocer que los mismos servicios de seguridad son necesarios para aplicaciones diferentes. A través de la arquitectura de seguridad se construye el diseño y estructura del modelo el cual está formado por componentes de protección, componentes protegidos y los mecanismos de integración que existen en entre ellos.

Es muy importante notar que no existe un modelo específico de seguridad que sea el más eficaz, ni tampoco un producto de seguridad que cubra todos los requerimientos de un modelo de seguridad. Aún cuando no se encuentre

con un modelo de seguridad totalmente seguro, se cuentan con algunas normas de diseño de redes que pueden ayudar a la implantación de redes perimetrales.

La arquitectura de seguridad es desarrollada por ambos equipos: los diseñadores de red y seguridad de tecnología de información. Es comúnmente integrado dentro de la red empresarial y es dependiente de los servicios de Tecnología de Información que son ofrecidos a través de la infraestructura de red. El acceso y requerimientos de seguridad de cada servicio de Tecnología de Información deberían ser definidos antes que la red sea dividida en módulos con niveles claramente identificados. La meta es tener un modelo de capas de seguridad que obligue a aislar el acceso "exitoso" de un intruso a una parte limitada de la red.

Tal como el diseño de un barco, donde su estructura con compartimentos separados con metal puede contener una filtración de agua para que el barco no se hunda completamente, el diseño de seguridad por capas limita los daños que una brecha de seguridad puede llegar a ocasionar sobre la salud de toda la red. Luego que las decisiones han sido realizadas, la arquitectura de seguridad debería desarrollarse en forma de fases, dirigiéndose primeramente a las áreas más críticas.

3.2. Componentes de una seguridad perimetral

La tecnología y componentes empleados como contramedida de seguridad son determinados por la política de seguridad de red, y merecen especial importancia. Deben encajar en la política, y por consiguiente concentrase en las amenazas a la red. Los componentes que se emplean actualmente en la protección de redes de son *firewalls*, dispositivos de encriptación de datos, dispositivos de detección de intrusos, dispositivos de autenticación, antivirus,

escáneres de vulnerabilidades, filtros de paquetes, seguridad propia de *hosts*, etc. En la actualidad existen muchos sistemas de diferentes tecnologías para la seguridad de redes, sin embargo los que tienen alto grado de aplicación dentro de una red perimetral son los *firewalls*, ruteadores de perímetro, *bastion host*, servidores *proxy*, sistemas de detección de vulnerabilidades y sistemas para detección de intrusiones.

3.2.1. *Firewall*

Los *firewalls* son barreras creadas entres redes privadas y redes públicas como Internet. Originalmente, fueron diseñados por los directores de informática de las propias empresas, buscando una solución de seguridad. Más recientemente, los *firewalls* proporcionados por terceras empresas, son la solución más escogida.

Los *firewalls* son simples en concepto, pero estructuralmente complejos. Examinan todo el tráfico de entrada y salida, permitiendo el paso solamente al tráfico autorizado. Los *firewalls* son diseñados de forma que todo lo que no es expresamente autorizado, es prohibido por defecto. Un *firewall* protege la red interna de una organización, al hacerlos invisibles de los usuarios que residen en redes externas. Un *firewall* permite el paso entre las dos redes a sólo los paquetes de información autorizados. Los *firewalls* pueden ser usados internamente, para formar una barrera de seguridad entre diferentes partes de una organización, por ejemplo a estudiantes y usuarios administrativos de una universidad.

Los *firewalls* reflejan un número de decisiones de diseño dependiendo del acceso, seguridad y transparencia. Un *firewall* es diseñado para entregar un acceso seguro a los servicios ofrecidos por la red Internet con un mínimo

esfuerzo adicional. La calidad de este "mínimo esfuerzo" es llamada la "transparencia" que significa que un usuario puede usar un gran número de *software* comercial sin modificaciones adicionales. Un *firewall* puede mejorar significativamente el nivel de seguridad en la red y reducir los riesgos filtrando la falta de seguridad inherente en los servicios de Internet. Un *firewall* implementa una política de acceso a la red, forzando que todas las conexiones a ésta, se realicen a través de él, mientras son examinadas y evaluadas.

3.2.1.1 Tipos de *firewalls*

Los primeros *firewalls* empezaron a aparecer hace unos diez años en la forma de simples enrutadores de filtrado de paquetes. Hoy, existen muchas variedades de tecnologías de *firewall* disponibles para la seguridad de redes. Mientras las líneas de distinción no sean tan claras como lo fueron alguna vez. Hay básicamente tres técnicas aproximadas a la arquitectura de *firewall*: *Packet Filter, Stateful Packet Inspection y Application Gateway*.

Los *firewalls* más antiguos tomaban la forma de simples filtros de paquetes. El término ***Packet Filter*** es muy usado frecuentemente para describir *firewalls* que bloquean o pasan tráfico, comparando con la información encontrada en el encabezado de cada paquete de salida o entrada contra una tabla de reglas de control de acceso. El *firewall* mira en el encabezado de cada paquete al entrar y compara la dirección IP y puerto TCP o UDP tanto fuente como destino y los compara contra las reglas básicas. Si la dirección e información de puerto son permitidas, entonces el paquete prosigue mediante el *firewall* directamente su destino. Si un paquete falla la prueba, es descartado por el *firewall*.

Considere la analogía de un guardia en una puerta de una casa muy grande. Cuando un camión de reparto llega con un paquete, el guardia "*packet filter*"

rápidamente busca una dirección válida del propietario de la casa, verifica el logotipo en el lado del camión para asegurarse que es válido, entonces envía el camión a través de la puerta para entregar su paquete.

Los *firewalls Packet Filtering* son rápidos, debido a que operan en la capa de red y hacen solamente verificaciones superficiales de la validez de una conexión dada. El protocolo HTTP, por ejemplo típicamente usa el puerto de TCP 80 para hacer conexiones *Web*. Si la política de seguridad de una organización permite a los empleados internos el acceso a la *Web*, un *firewall* de *Packet Filtering* podría probablemente estar configurado para permitir todas las conexiones a través del puerto 80, el puerto predeterminado. Desdichadamente, las suposiciones como ésta crean un riesgo de seguridad sustancial. Mientras un *firewall* de *Packet Filtering* puede razonablemente asumir que el tráfico llegando en el puerto 80 es usualmente una conexión estándar de *Web*, no tiene visibilidad de lo que realmente está ocurriendo en el nivel de aplicación. Cualquiera que esté enterado de esta exposición podría usar el puerto 80 para entrar sin autorización en la red privada y nunca ser detectado.

Los *firewalls Packet Filtering* también han sido criticados por muchos expertos de seguridad debido a que permiten conexión directa entre los puntos finales a través del *firewall*. Una vez la conexión ha sido aprobada por el *firewall*, el origen externo es permitido para conectarse directamente al equipo destino detrás del *firewall*, exponiendo potencialmente a un paquete en la red interna.

Luego del advenimiento del *firewall Packet Filter*, muchos expertos de seguridad, incluyendo agencias de gobierno como DARPA (*Defense Advanced Research Projects Agency*), la investigación central para el Departamento de Defensa de los Estados Unidos, empezaron a buscar un acercamiento a la

seguridad de *firewall*. Ellos pensaban que realmente la seguridad de *firewall* solo podría ocurrir si las conexiones directas a través del *firewall* fueran deshabilitadas y todos los datos entrantes fueran examinados en la capa más alta de la pila del protocolo. Para probar esta teoría, la DARPA contrató a una firma de investigación de seguridad avanzada conocida como *Trusted Information Systems* para desarrollar un *firewall* de ***Application Gateway***.

Un *Application Gateway* es un programa de aplicación que corre sobre un sistema de *firewall* entre dos redes denominado *proxy*. El *host* en el cual el *gateway* corre no necesita estar actuando como un ruteador. Cuando un programa cliente establece una conexión a través de un *gateway* a un servicio destino, primero establece una conexión directamente al programa de *gateway* en el servidor. El cliente entonces negocia con el *gateway* para que establezca una conexión en su nombre hacia el servicio destino. Si es satisfactorio, entonces se regeneran dos conexiones: una entre el cliente y servidor *gateway* y otra entre el servidor *gateway* y el servicio destino. Una vez establecida, el *gateway* recibe y envía tráfico en forma de dos vías entre el cliente y el servicio. El *gateway* hace todas las decisiones de establecimiento de conexión y reenvío de paquetes, cualquier función de rutas que están activas sobre el sistema *host* son irrelevantes al *gateway*.

Como con *Packet filtering*, los *Application Gateways* son disponibles en ambas modalidades, máquinas de propósito especial y computadoras de propósito general. Generalmente, los *Application Gateways* son más lentos que los *firewalls* de *Packet Filtering*, Sin embargo, los *Application Gateways* son, en alguna manera, inherentemente más seguros que los de *Packet Filtering*. Para todos los sitios, el alto grado de seguridad que provee el *Application Gateway* es importante, ya que garantiza que solo los servicios considerados confiables se permiten mediante el *firewall*. Esto también previene que otros servicios sin

autorización estén siendo utilizados a espaldas de los administradores de *firewall*.

Como resultado de hacer filtrados más complejos y decisiones de control de acceso, los *Application Gateways* puede requerir significantes recursos de cómputo y un *host* costoso sobre el cual ejecutarse.

Para vencer algunos de los más evidentes problemas de seguridad con el modelo básico de *packet filtering*, algunos fabricantes de *firewalls packet filtering* inventaron un concepto conocido como ***Stateful Packet Inspection***. Basado en la tecnología de *Packet Filtering*, el modelo de *Stateful Packet Inspection* agrega más verificaciones de seguridad en un intento para simular las verificaciones de seguridad de un *firewall* de *Application Gateway*. En lugar de simplemente ver las direcciones de cada paquete de entrada, el *firewall* de *Stateful Packet Inspection* intercepta los paquetes de entrada en la capa de red hasta que se tiene la suficiente información para hacer algunas determinaciones sobre el estado del intento de conexión. Estos paquetes son entonces inspeccionados en un módulo de inspección propietario dentro del *kernel* del sistema operativo del *host*. La información de estado requerida para la decisión de seguridad es examinada en este módulo de inspección, y luego es guardada en tablas de estado dinámico para evaluar los subsecuentes intentos de conexión. Los paquetes eliminados son luego reenviados dentro del *firewall*, permitiendo contacto directo entre los sistemas internos y externos. Debido la mayoría de la evaluación ocurre en el *kernel*, los *firewalls* de *Stateful Packet Inspection* son frecuentemente más rápidos que los *firewalls* de *Application Gateway*.

Aunque la tecnología de *Stateful Packet Inspection* ha mejorado significativamente la seguridad de los *firewalls* de *Packet Filtering*, no puede simular la visibilidad total que una revisión de nivel de aplicación provee. Un

firewall Stateful Packet Inspection, por ejemplo, comúnmente fallará en las verificaciones que requieren la colección de paquetes en largas unidades como URLs o archivos. Mientras que un *firewall Application Gateway* tiene visibilidad total, debido a que opera en la pila de protocolo más alta, los *firewalls Stateful Packet Inspection* debe hacer decisiones seguras sin la misma información. Cuando un fabricante de *firewall* de *Application Gateway* dice que soporta *Microsoft* SQL *Server*, por ejemplo, se sabe que ninguna conexión remota hacia una base de datos de SQL *Server* debe hacer primero una inspección completa en la capa de aplicación a través del *proxy* dedicado a *Microsoft* SQL. Con un *firewall Stateful Packet Inspection* al permitir a los empleados en una oficina remota acceder bases de datos de SQL detrás del *firewall* es evidentemente más riesgoso.

Semejante a cualquier *firewall Packet Filtering*, el modelo *Stateful Inspection* también introduce riesgo al permitir contacto directo entre sistemas internos y externos. A menos que un *firewall* utilice el método de *proxy* en la conexión, las fuentes externas al *firewall* tendrán acceso directo en la red interna al hacer una conexión.

Si se asume que el guardia de seguridad es ahora un "*Stateful Packet Inspection*", cuando los paquetes lleguen, en vez de solo verificar la dirección, el guardia examina la nota de envío para ver si algo dentro del paquete es prohibido. Mientras esto es mucho mejor, es claro que no es tan seguro como abrir el paquete y examinar su contenido. Si el paquete se ve aceptable, el guardia abre la puerta y permite al camión de reparto entrar al complejo.

3.2.1.2 Funciones del *firewall*

Actualmente son muchas las funciones que vienen definidas en un sistema de *firewall*. Algunas funciones proporcionan protección de manera directa, mientras que otras se orientan a la administración. Si se comparan las tres tecnologías de *firewalls* actuales, se puede decir que los *firewalls* de aplicación son los que normalmente traen más funciones. En los *firewalls* de aplicación es común que operen sobre la base de un computador, mientras que los otros operan en *hardware* específico. Los *firewalls* que operan sobre un computador normalmente utilizan la base de sistemas operativos como Unix, aunque hoy ya se tienen sistemas que operan sobre plataforma NT de *Microsoft* y *Novell Netware*[9]. Las funciones que traen los *firewalls* comúnmente sin importar la tecnología se describen a continuación.

NAT (*Network address translation*, traducción de direcciones de red*)*, esta funcionalidad permite que el *firewall* transforme las direcciones IP de los *hosts* que se encuentran protegidos por el *firewall* hacia otro esquema de direcciones con el fin de que en el medio externo no se conozcan las direcciones que poseen los equipos internos.

Debido a los peligros inminentes que se contraen al conectar equipos de redes internas a Internet, el NAT ayuda a que los equipos que se encuentran en redes privadas tengan la capacidad de que puedan ser accedidos desde Internet sin comprometer los servicios internos. El NAT también permite a los equipos de redes privadas que utilizan direcciones de red no válidas en Internet sean proyectados en Internet con direcciones válidas, permitiendo a los equipos proporcionar servicios sin cambiar su esquema de direcciones. El PAT (*Port*

[9] Novell Netware es un sistema operativo para redes de área local fabricado por la empresa Novell.

address translation, traducción de direcciones a puertos), es una función de NAT que permite que muchas direcciones de una red sean trasladas a una única dirección IP. Normalmente el PAT es útil para que las redes que están protegidas por el *firewall* puedan utilizar los servicios de Internet sin restricciones que cada usuario tenga una dirección válida de Internet. Esto permite el ahorro de direcciones de Internet, lo cual ha sido limitado en los últimos días. El *firewall* tanto en NAT como en PAT maneja en la memoria una tabla que permite asociar a una dirección interna con su equivalente en el medio externo. El NAT estático significa que una dirección IP interna siempre será traducida a una dirección de Internet específica. El NAT dinámico significa que la dirección IP de un *host* interno será traducida a la primera dirección externa disponible en el *firewall*.

Registro y reportes. El *firewall* viene con un sistema de registro del tráfico que fluye a través del *firewall* desde una red hacia otra. Normalmente traen consigo secciones donde se definen alertas de conexiones, que atentan contra los recursos protegidos, el tráfico que es permitido ya sea de conexiones sobre *proxies* o en el caso de conexiones *Stateful*. Presentan información sobre estadísticas de uso de determinados servicios, por ejemplo, el más común es el servicio de *Web* el cual puede resultar útil conocer los sitios que son más visitados en Internet, o mejor aún en un servicio de correo electrónico conocer cuantos mensajes entran y salen en determinado período de tiempo. Los *firewalls* de *hardware* comúnmente utilizan los servicios *Syslog* para enviar mensajes informacionales a sistemas basados en plataformas *Unix*. Además los últimos *firewalls* permiten enviar todo el tráfico hacia un buzón de correo electrónico por medio del servicio SMTP. Actualmente también es posible que se definan para cierto tipo de alertas críticas enviar notificación a través de servicio de *pager*, a localizadores de los administradores de red en el momento real que se generan los ataques.

Consola de administración. Esta sección corresponde a un programa de computadora que permite la administración de parámetros que se definen al *firewall*. Los *firewalls* de *hardware* traen consigo este tipo de programas, para que se instalen en computadoras y que puedan accederse por medio de la red interna. La seguridad de acceso de la consola está definida normalmente por la misma del sistema operativo. Hoy día, todas las consolas de administración vienen en interfaz GUI (*Graphical user interface*, interfaz de usuario gráfica), lo cual facilita la interacción con el programa y da como resultado mejor administración por parte del usuario. Las consolas además traen implícita la ayuda al usuario, la cual normalmente está asociada a la sección que se esté consultando. Otras consolas de *firewall* traen consigo algunos asistentes que permiten de forma muy intuitiva y sencilla, la definición de reglas y parámetros de control de tráfico IP. La administración remota también es una funcionalidad importante, ya que se puede acceder a la configuración del *firewall* desde cualquier computadora de la red.

Interprete de comandos. Esta sección define un entorno de trabajo del *firewall,* donde el usuario puede efectuar cambios en la configuración, análisis de tráfico, recibir información de alertas, mantenimientos, etc. Cualquier acción está basada en instrucciones compuestas por uno o más comandos definidos en la memoria del *firewall*. El uso de este entorno requiere de más control y concepto de los comandos, sin embargo es muy útil en caso de que no se disponga de un programa de consola, instalado en una computadora. El acceso a este modo puede hacerse de dos maneras, el primero es localmente, casi todos los *firewalls* basados en *hardware* traen un conector de consola serial que puede conectarse a cualquier puerto de comunicaciones de una computadora personal. El otro método de acceso es a través de la red, por medio del uso del servicio Telnet del puerto 23 de TCP.

Filtros de contenido. Los *firewalls* además de separar una de otra red y controlar el tráfico de paquetes, también analizan el contenido de los paquetes para los servicios de red más comunes. Por ejemplo, para el servicio de *Web* el *firewall* puede filtrar programas basados en *JavaScript* o *ActiveX*. También pueden revisar y limpiar virus contenidos el tráfico de *Web* o FTP. Algunos *firewalls* también pueden restringir el contenido de las páginas de *Web* a las que acceda el usuario o evitar el acceso a ciertos sitios de Internet especificados ya sea por el nombre de dominio o por la dirección IP.

Encriptación de datos. Con la llegada de las VPNs (*Virtual private networks*, redes privadas virtuales) que utilizan como protocolo de comunicaciones el IPSec, el *firewall* debe de hablar este protocolo. La encriptación de datos permite que se puedan realizar comunicaciones seguras en infraestructuras de comunicaciones inseguras, como Internet. Los *firewall* se pueden comunicar de forma segura ya sea con otros *firewalls*, ruteadores, o con computadoras que tengan algún *software* para VPNs.

Autenticación de usuarios. El *firewall* posee un mecanismo para asegurar que el tráfico proveniente de un usuario pase a otra red, dependiendo si tiene o no los permisos definidos previamente. El *firewall* al detectar tráfico, verifica ya sea en su base de datos local si el tipo de tráfico debe ser autenticado, si lo es, el *firewall* solicita al usuario el nombre de usuario y la contraseña para que pueda acceder al servicio. Hay casos en que la base de datos de usuario crece mucho o se desean reutilizar los usuarios del sistema de red, entonces para ello existen protocolos tales como el *RADIUS* o *TACACS* que permiten interactuar con el *firewall* para determinarle si el usuario en cuestión puede o no acceder al servicio solicitado. El método más común de autenticación de usuario es por medio de la dirección IP que posee su computador, la cual es asociada con los

servicios a los que puede acceder. Cuando el número de usuarios es considerable este método resulta ser difícil de administrar.

Actualización de versiones. Debido a que el *firewall* está compuesto por una parte de *software* o programas, existen muchas razones para desear actualizar la versión de dicho *firewall* a una más reciente. La razón principal es para habilitar más funcionalidades, por ejemplo encriptación de datos. Sin embargo, una razón muy necesaria para actualizar el *software* de un *firewall* es corregir debilidades de funcionalidad del programa, lo cual podría originar el acceso inautorizado de intrusos. La actualización puede ser completa o parcial, si es completa todo el *software* del *firewall* es quitado del sistema y es remplazado por una versión más reciente. Cuando la actualización es parcial, son reemplazados ciertos programas o archivos de librerías o ejecutables que representan alto grado del funcionamiento del *firewall*.

El ***failover*** es un sistema de redundancia a fallos en el que se tienen dos dispositivos de *firewall* (uno activo y otro pasivo) y que permite el paso continuo de tráfico de una red a otra de forma transparente en caso que uno de ambos *firewalls* tenga fallas de *hardware* o *software*. Muchas aplicaciones debido a que son críticas para el negocio de la organización, son protegidas mediante un sistema redundante a fin de garantizar el máximo de disponibilidad en el tráfico de paquetes de red. Los *firewalls* que traen consigo esta características necesitan un puerto de red adicional, con el fin de servir como el punto de enlace para el canal de comunicaciones de la información de control para el estado de ambos *firewalls*.

***Backup* o sistema de respaldo**, los *firewalls* traen consigo opciones que permiten hacer copias de seguridad o respaldo sobre el *software* y parámetros de configuración del sistema. También los *firewall* traen una opción para restaurar algún archivo que haya sido generado previamente con un *backup*.

Este proceso permite ya sea restaurar el sistema operativo completamente, o simplemente restaurar la configuración actual del sistema. En los casos en que se haya reiniciado la configuración del *firewall* debido a una instalación nueva por ejemplo es posible recuperar la configuración previa, lo cual reducirá considerablemente el tiempo de preparación del *firewall* a producción.

3.2.2. Ruteador de perímetro

Un ruteador es un componente de la red, que permite la interconexión entre dos o más redes no necesariamente de la misma tecnología física. El ruteador por concepto se conoce que trabaja hasta la capa de red del modelo de referencia OSI. Dentro de un esquema de seguridad perimetral de Internet, el ruteador juega el papel de proveer el acceso a la Internet, así como de representar la primera línea de defensa en contra de intrusos. También se puede decir que representa el punto de separación entre los recursos propios de la corporación y los que no le pertenecen, normalmente del proveedor de acceso a Internet.

Para efectos de seguridad, los ruteadores poseen la capacidad de seleccionar paquetes con base en criterios como el tipo de protocolo, los campos de dirección de origen y dirección de destino para un tipo particular de protocolo y los campos de control que son parte del protocolo. A esos ruteadores también se les llama ruteadores de selección, ruteadores *firewall*. Esto puede proporcionar un mecanismo poderoso para controlar el tipo de tráfico de red que puede existir en cualquier segmento de una red. Al controlar ese tipo de tráfico, los ruteadores de selección pueden controlar el tipo de servicio que puede existir en un segmento de red. Por lo tanto, pueden restringirse servicios que pueden poner en peligro la seguridad de la red, tales como:

a. Prevenir ataques directos en la interfaz externa del *firewall* interno.
b. Prevenir el IP *spoofing*.
c. Prevenir ataques de denegado de servicio sobre el *firewall* interno.
d. Desactivar todas las conexiones a redes internas excepto a aquellos que se permiten mediante la política de seguridad.
e. Permitir acceso de Telnet por direcciones IP específicas.
f. Proveer traducción de direcciones de red.
g. Registrar todos los eventos especificados.

Los ruteadores de selección, pueden discriminar entre el tráfico de red con base en el tipo de protocolo y en los valores de los campos del protocolo en el paquete. A la capacidad del ruteador para discriminar entre paquetes y restringirlos en sus puertos con base en criterios específicos de protocolo se le denomina filtrado de paquetes. Por esta razón, los ruteadores de selección son llamados también ruteadores de filtración de paquetes.

3.2.2.1 Filtrado de paquetes

Los ruteadores de selección pueden utilizar la filtración de paquetes como medio para mejorar la seguridad de la red. La función de selección también puede ser desarrollada por muchos productos de *firewall*. Sin embargo, pueden programarse muchos ruteadores para desarrollar la filtración. La filtración de paquetes se hace para restringir el tráfico de red para los servicios que habrán de rechazarse.

Por lo general, un filtro de paquetes se coloca entre uno o más segmentos de red. Estos segmentos de red están clasificados como segmentos de red externos o internos. Los segmentos de red externos conectan su red con redes

externas como Internet. Los segmentos de red internos se utilizan para conectar los *hosts* de la organización y otros recursos de la red.

En un modelo simple se tiene un dispositivo de filtración de paquete, que solo tiene conectados dos segmentos de red. Por lo general uno de esos segmentos de red es un segmento de red externo y el otro es un segmento de red interno.

En las operaciones de filtrado de paquetes casi todos los dispositivos de actuales (ruteadores de selección o *gateways* de filtración de paquetes) operan de la siguiente manera:

a. Los criterios de filtrado de paquetes, deben almacenarse para los puertos del dispositivo de filtrado de paquete. A los criterios de filtrado de paquetes se les llama reglas de filtrado de paquetes.
b. Cuando el paquete llega al filtro, se analizan los encabezados del paquete. La mayoría de los dispositivos de filtrado de paquete examinan los campos solo encabezados de IP, TCP o UDP.
c. Las reglas de filtrado de paquetes se almacenan en un orden específico. Cada regla se aplica al paquete en el orden en el que la regla de filtrado de paquetes se almacena.
d. Si una regla bloquea la transmisión o la recepción de un paquete, este no es permitido.
e. Si una regla permite la transmisión o la recepción de un paquete, a dicho paquete se le permite proceder.
f. Si un paquete no satisface alguna regla, se le bloquea.

Cuando se diseñan reglas de filtrado de paquetes es útil tener en mente las definiciones de asociación completa, media asociación y extremos. Esto ayuda a la mejor comprensión de reglas de filtrado de paquetes. Una asociación

completa muestra que una conexión de TCP entre dos *hosts* puede describirse con la siguiente información:

1. Tipo de protocolo
2. Dirección de IP local
3. Número de puerto de TCP local
4. Dirección de IP remota
5. Número de puerto de TCP remoto

La regla de la filtración de paquetes puede describir varios tipos diferentes de circuitos de TCP. Esto permite que una regla de filtración de paquetes implante una política de seguridad de la red describiendo varios tipos diferentes de conexiones de TCP.

Para la implementación de las reglas de filtrado de paquetes en el ruteador, una vez que ha diseñado las reglas de filtración de paquetes y se han tengan por escrito se tiene que implementar en el ruteador de selección o en la *firewall* (si permite que se especifiquen reglas de filtración de paquetes).

Cada tipo de dispositivo de filtrado de paquetes tiene su propio conjunto de reglas y de sintaxis para programar las reglas de filtrado de paquetes. Por lo tanto, se debe leer la documentación del dispositivo y se deben aprender las peculiaridades de la sintaxis de las reglas de filtración de paquetes para ese dispositivo. Si cambia el fabricante del dispositivo de filtración de paquetes, tendrá que aprender un conjunto diferente de reglas de sintaxis.

3.2.3. *Bastion host*

Un *bastion host* es un sistema de *hardware* y *software* que está colocado en una red en la que se espera habrá ataques desde redes desconocidas como Internet y que ha sido configurado para resistir cualquier tipo ataques. Con frecuencia, los *bastion host* son utilizados como plataforma para *firewalls*, *gateways* de aplicaciones internas, para servidores de servicios de acceso público tales como *Web*, FTP, DNS, SMTP, o mediadores de servicios de Internet para *hosts* internos. Normalmente, un *bastion host* está ejecutando alguna aplicación sobre un sistema operativo de propósito general (por ejemplo *Unix*, *VMS*[10], *Windows* NT, etc.).

Un *bastion host* es colocado en los perímetros de red más cercanos a Internet, lo que lo hace más vulnerable de ataques, para ello la seguridad de sus servicios del sistema de red y aplicaciones se encuentran afinados lo mejor posible.

Cuando son utilizados como *gateways* representan el punto de separación de la red interna y la externa. Esto permite que la conexión no se haga directamente hacia los servidores de aplicaciones internos, sino hacia el *bastion host*, el cual a su vez se comunica con los servidores internos. Un *bastion hosts* debe ser muy vigilado por el administrador del sistema para detectar atentados que puedan comprometer su integridad.

[10] VMS es un sistema operativo nativo de Digital Equipment Corporation´s para computadoras VAX.

3.2.4. Servidor *proxy*

Un *proxy server* es una computadora sencilla cuyo propósito es concentrar los servicios de aplicación. Típicamente una computadora sencilla (*bastion host*) que actúa como un *proxy server* para una variedad de protocolos (Telnet, SMTP, FTP, HTTP, etc.) aunque existen computadoras individuales para un solo servicio.

En lugar de conectarse directamente aun servidor externo, el cliente se conecta al *proxy server* el cual deja iniciar una conexión al servidor externo solicitado. Dependiendo del tipo de *proxy server* usado, es posible configurar los clientes internos para hacer esta redirección de forma automática, sin conocimiento para el usuario, otro pueden requerir que usuario se conecte directamente al *proxy server* y luego inicie la conexión a través del formato especificado.

Hay beneficios significantes de seguridad los cuales pueden ser derivados de usar servidores de *proxy*. Es posible agregar listas de control de acceso a protocolos, requerir usuarios o sistemas para proveer algún nivel de autenticación antes que el acceso sea dado. Los servidores de *proxy* inteligentes, algunas veces llamados *Application Layer Gateways*, pueden ser escritos con conocimiento de protocolos específicos y pueden ser configurados para bloquear solo sub-secciones del protocolo. Por ejemplo, un *Application Layer Gateway* para FTP puede determinar la diferencia entre el comando "*put*" y el comando "*get*"; una organización podría desear permitir a usuarios hacer descargas de archivos desde Internet, pero no ser capaz para colocar archivos internos en servidores remotos. Por contraste, un filtrado de ruteador podría ya sea bloquear todo el acceso FTP, o ninguno, pero no un subconjunto. Los *proxy server* pueden también ser configurados para encriptar cadenas de datos

basados en una variedad de parámetros. Una organización puede usar estas características para permitir encriptar conexiones entre dos localidades, sus únicos puntos de acceso están en Internet.

3.2.5. Sistema de detección de intrusos

Los sistemas de detección de intrusos o IDS (*Intrusion Detection Systems*) actúan como una segunda línea de defensa contra cualquier actividad que no haya sido identificada por los sistemas de seguridad tradicionales como *firewalls*. El objetivo de la detección de intrusos es identificar en tiempo real cualquier actividad sospechosa, mal uso o abuso de los sistemas informáticos, tanto si tienen su origen en usuarios de la red interna, como si se trata de ataques externos. El nivel de sofisticación en la identificación de ataque varía desde violaciones aisladas, sucesos que a lo largo del tiempo acaban constituyendo una violación, y hechos secuenciales que suponen una violación. La detección de intrusos supone un gran reto debido a la proliferación de los tipos de conexiones entre redes e Internet, la mezcla de sistemas operativos, la variedad de protocolos y la diversidad de aplicaciones de dominio público y privadas.

Los *firewalls* están diseñados para filtrar el tráfico "normal" de la red, basándose en atributos tales como las direcciones de origen y de destino, números de puerto, etc. Si bien los *firewalls* más modernos también se preocupan por los requisitos de los protocolos populares, como DNS, con frecuencia no manejan correctamente el tráfico de red "incorrecto", catalogado de malicioso. Normalmente, tienen la opción de poner un alerta cuando algún tráfico prohibido intenta ingresar.

En comparación, un IDS que analiza la red se ocupa de lo que constituyen paquetes de la red legales y de los ilegales y puede generar alertas cuando se detectan estos últimos. Dependiendo de muchos factores un IDS puede responder reactivamente o pasivamente ante tal tráfico ilegal. Sin embargo, generalmente, un IDS no previene ni contesta un ataque

Rango de cobertura. Los sistemas de detección de intrusos pueden categorizarse, en un primer nivel, de la siguiente manera:

a. NIDS: sistemas que analizan el tráfico de la red completa.
b. HIDS: sistemas que analizan el tráfico sobre un servidor o estación de trabajo.

Los sistemas que analizan la red (NIDS) examinan los paquetes individuales que viajan por ella. A diferencia de los *firewalls*, los que, típicamente, solo miran las direcciones IP, los puertos y los tipos de ICMP, los NIDS son capaces de comprender todas las diferentes banderas y opciones que pueden coexistir dentro de un paquete de red. Por lo tanto, un NIDS puede detectar paquetes armados maliciosamente y diseñados para no ser detectados por las relativamente simplistas reglas de filtrado de las barreras corta fuego. Habitualmente, los *hackers* arman ese tráfico para componer un "mapa" de la red, como una forma de reconocimiento pre-ataque.

Los NIDS son capaces de buscar al generador de la intrusión dentro del paquete, o sea, ver cual es el programa en particular del servidor de *Web* al que se está accediendo y con cuales opciones, y producir alertas cuando un atacante intenta explotar alguna falla de esa codificación.

Los NIDS miran todo el tráfico que fluye por la red, mientras que los sistemas de detección de intrusos, basados en el tráfico sobre un servidor específico

(HIDS) se preocupan de lo que está ocurriendo en cada computadora individual o "*host*". Son así capaces de detectar cosas, tales como la ocurrencia de repetidos intentos fallidos de acceso o de modificaciones en archivos de sistema considerados críticos.

Mecanismos de detección del mal uso o uso sospechoso. Un segundo nivel de categorización de los sistemas de detección de intrusos es entre aquellos que se basan en:

1. La detección del mal uso.
2. La detección del uso anómalo.

La detección del mal uso en un IDS involucra la verificación sobre tipos ilegales de tráfico de red; por ejemplo, combinaciones de opciones dentro de un paquete que nunca podrían ocurrir legítimamente. Además se lleva a cabo a partir de modelos de ataque bien definidos, que utilizan fallos conocidos del sistema. Estos modelos pueden preverse y son más fácilmente detectables. Por ejemplo, la utilización de los *bugs* del *Sendmail* y del *Finger* que llevó a cabo el ``gusano'' de Internet, entraría dentro de este tipo de ataques. Esta técnica pretende la detección de comportamiento anómalo a partir del conocimiento de cómo puede ser dicho comportamiento. Intenta detectar la intrusión de forma directa. El fundamento de este sistema de detección, es la creencia de que existen ataques que pueden ser codificados de forma precisa, de manera que se consiguen agrupar reorganizaciones y variaciones de las actividades que explotan el mismo punto vulnerable. En la práctica no todas las posibles formas de llevar a cabo un ataque pueden ser codificadas de la forma adecuada. La primera limitación de esta idea es el hecho de que sólo va a buscar intrusiones que aprovechen brechas conocidas y por tanto no tendrán mucho uso en la

detección de futuras intrusiones desconocidas. Se dan otras limitaciones a la hora de decidir qué datos van a ser recogidos.

La detección de actividad anómala se apoya en que el sistema conoce cual es el tráfico "regular" en la red y por ende el que no lo es. Un tráfico anómalo en un HIDS podría ser el acceso interactivo fuera del horario normal de oficina.

Un ejemplo de tráfico anómalo en un NIDS, es el acceso que se intenta repetidamente desde una máquina remota a muchos servicios diferentes de uno o más de los sistemas internos, todos en rápida sucesión. Esto es indicativo de que alguien está haciendo un "rastreo de puertos" del sistema.

Las intrusiones se detectan a partir de la caracterización anómala del comportamiento y del uso que hacen de los recursos del sistema. Esta detección pretende cuantificar el comportamiento normal de un usuario. Para una correcta distinción hay que tener en cuenta las tres distintas posibilidades que existen en un ataque atendiendo a quién es el que lo lleva a cabo:

1. **Penetración externa.** Que se define como la intrusión que se lleva a cabo a partir un usuario o un sistema de computadores no autorizado.
2. **Penetraciones internas**. Son aquellas que llevan a cabo usuarios autorizados de sistemas de ordenadores, que no están autorizados al acceso a los datos que se están siendo comprometidos.
3. **Abuso de recursos**. Se define como el abuso que un usuario lleva a cabo sobre unos datos o recursos de un sistema al que está autorizado su acceso.

La idea central de este tipo de detección, es el hecho de que la actividad intrusiva es un subconjunto de las actividades anómalas. Esto puede parecer razonable por el hecho de que si alguien consigue entrar de forma ilegal en el

sistema, no actuará como un usuario comprometido, seguramente el comportamiento se alejará del de un usuario normal. Sin embargo en la mayoría de las ocasiones una actividad intrusiva resulta del agregado de otras actividades individuales, que por sí solas no constituyen un comportamiento intrusivo de ningún tipo. Idealmente el conjunto de actividades anómalas es el mismo del conjunto de actividades intrusivas, de todas formas esto no siempre es así:

a. **Intrusivas pero no anómalas**. Se les denomina *falsos negativos* o errores de tipo I. En este caso la actividad es intrusiva pero como no es anómala no se conseigue detectarla. Se denominan *falsos negativos* porque el sistema erróneamente indica ausencia de intrusión.
b. **No intrusivas pero anómalas.** Se denominan *falsos positivos* o errores de tipo II. En este caso la actividad es no intrusiva, pero como es anómala el sistema decide que es intrusiva. Se denominan *falsos positivos*, porque el sistema erróneamente indica la existencia de intrusión.
c. **Ni intrusiva ni anómala**. Son negativos verdaderos, la actividad es no intrusiva y se indica como tal.
d. **Intrusiva y anómala**. Se denominan positivos verdaderos, la actividad es intrusiva y es detectada.

Los primeros no son deseables, porque dan una falsa sensación de seguridad del sistema, el intruso en este caso puede operar libremente en el sistema. Los falsos positivos se deben minimizar, en caso contrario lo que puede pasar es que se ignoren los avisos del sistema de seguridad, incluso cuando sean acertados. Los detectores de intrusiones anómalas requieren mucho gasto computacional, porque se siguen normalmente varias métricas para determinar cuánto se aleja el usuario de lo que se considera comportamiento normal.

Muchos sistemas modernos usan una combinación de motores de detección del mal uso y del anómalo.

Pasivos frente a reactivos. Un tercer nivel de categorización de los sistemas de detección de intrusiones es según su naturaleza:

a. Pasiva
b. Reactiva

Los sistemas pasivos simplemente detectan la potencial violación de seguridad, registran la información y generan un alerta.

Los sistemas reactivos, por el otro lado, están diseñados para responder ante una actividad ilegal, por ejemplo, sacando al usuario del sistema o mediante la reprogramación del *firewall* para impedir tráfico de red desde una fuente presumiblemente *host*il.

Si bien se podría pensar que un sistema reactivo es la solución ideal - ¿porqué emplear personal o contratar a alguien cuando la máquina puede efectuar la acción requerida? - existen serias desventajas en ese tipo de sistemas. Analícese la siguiente situación:

Un atacante, con mucha astucia, arma tráfico de red dirigido al sistema de correo electrónico. El tráfico está esquematizado de tal manera, que pareciera provenir del sistema de correo del proveedor de servicios de Internet (ISP). El NIDS detecta este tráfico anómalo y reprograma el *firewall* para impedir todo tráfico que provenga de ese sistema. Ahora la empresa está incapacitada para recibir algún correo desde el proveedor ISP.

Esta es la razón por la que el personal calificado, propio o de una consultora especializada, es un elemento importante en cualquier sistema de detección de intrusiones.

Siguiendo con el ejemplo anterior, un analista de detección de intrusos adecuadamente capacitado debería poder identificar el tráfico "falsificado" o, si ello no fuese técnicamente factible, podría conectarse con el ISP para establecer el origen del problema.

Los sistemas de detección de Intrusos tienen la capacidad de:

a. Aumentar el nivel de seguridad general del entorno.
b. Vigilar el tráfico de red dentro de los *firewalls*.
c. Examinar los contenidos de los mensajes de red; por lo tanto, detectando los tipos de ataque, por ejemplo, de "desborde de *buffer*".
d. Detectar los cambios en archivos y directorios.
e. Detectar tiempos de acceso anormales.

Los sistemas de detección de intrusos no tienen la capacidad de:

a. Proporcionar una solución mágica, que elimine los problemas de seguridad.
b. Reemplazar al personal calificado o la ayuda externa especializada.

3.3. Representación gráfica de redes perimetrales

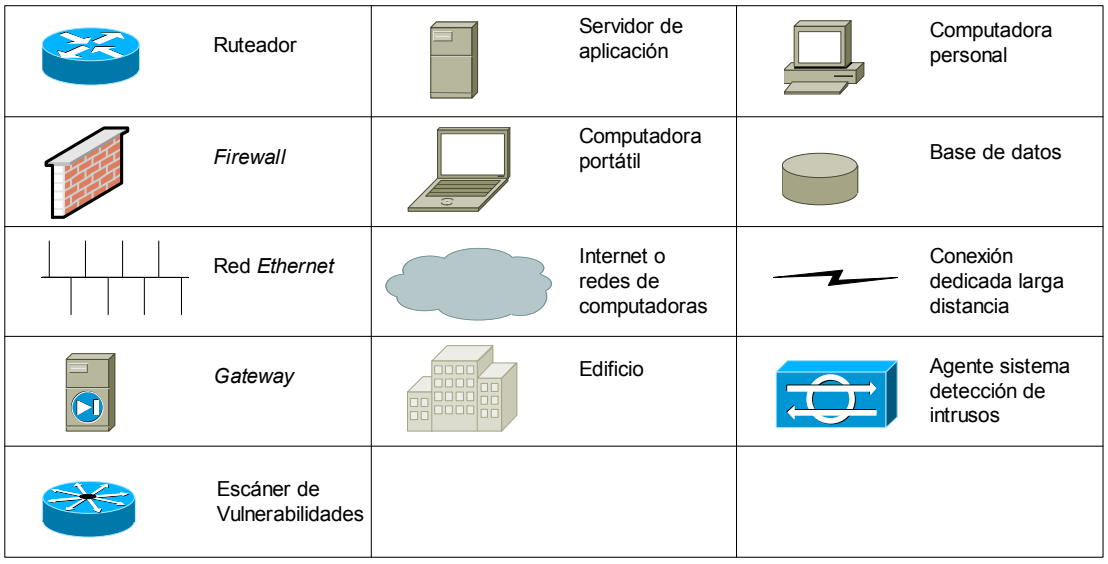
La representación gráfica de una red abarca actividades de diagramación en planos lógicos o físicos de la red, utilizando símbolos, conectores y descripciones concisas. El empleo de diagramas resulta ser muy útil para la

representación de la red perimetral, ya que proporciona al personal administrativo una visión general de los perímetros de seguridad aplicados a la red privada.

Otro beneficio muy importante de los diagramas, es que permiten definir varios niveles de información con el propósito de documentar la interconexión entre los distintos componentes de las redes. Para la representación del plano lógico de la red perimetral se emplea la capa de red, ya que define los diferentes segmentos de red y el esquema de direccionamiento IP, para proveer una mayor comprensión de lo que se tiene en la red y la forma en que interactúa con otros equipos.

Mediante el uso de símbolos, es posible representar gráficamente los sistemas que protegen y los sistemas protegidos. La siguiente figura presenta los símbolos de los elementos más comunes dentro de redes perimetrales:

FIGURA 6. Símbolos de redes de perímetro



3.4. Segmentación de redes

3.4.1. Zona desmilitarizada

Uno de los aspectos más importantes de seguridad asociados con la conexión de redes privadas en Internet es la contención. Se necesita separar cada sistema y servicio para prevenir la corrupción o compromiso de unos de llevar a la corrupción o compromiso de otros. La solución es una zona de amortiguado controlada entre los servicios extremos y el entorno interno. Esta es la razón por la cual se define la zona desmilitarizada o DMZ (*Desmilitarized zone*).

La DMZ es una red aislada que contiene servicios que están directamente accesibles de Internet. La DMZ es un amortiguador entre la red corporativa y el mundo externo. La DMZ tiene un único número de red que es diferente del número de red corporativo. Solamente la red DMZ es visible al mundo externo. Un lado está conectado a Internet, mientras el otro está conectado a la red interna. Ambos lados están protegidos por *firewalls*, los cuales están configurados para limitar los protocolos, direcciones origen y destino de paquetes que pasan entre todas las redes.

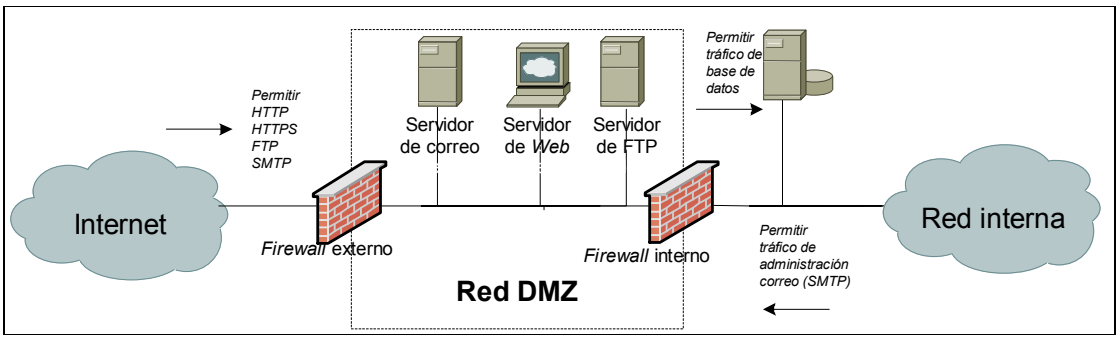
La DMZ es creada por los dispositivos de seguridad de perímetro trabajando juntos para componer un sistema de *firewall*. Los dispositivos que contiene son los siguientes:

a. Computadores de servicios de red
b. Ruteadores
c. *Bastion hosts*

d. *Firewall*

e. Detectores de intrusos - IDS

FIGURA 7. Esquema de red con zonas DMZ



3.4.2. Red externa

Las redes externas o no confiables, son aquellas redes que se conocen que están en el lado externo del perímetro de seguridad. Estas son no confiables debido a que están fuera del control de la organización. No se tiene control sobre la administración o políticas de seguridad para estos sitios.

La conexión desde una red externa, proviene de redes privadas de otras organizaciones, de sitios públicos de Internet, de usuarios conectados a través de conexiones telefónicas, de redes universitarias, etc. Los millones de usuarios que provienen de estas redes representan una amenaza inminente para los recursos internos de la organización.

Equipos de comunicaciones, tales como ruteadores de perímetro y *firewalls* de perímetro definen la segmentación entre tales redes y otras redes como las desmilitarizadas o las internas. Para el control de tráfico desde esta clase de

redes hacia las redes internas son utilizadas políticas externas, especializadas definidas en ruteadores de perímetro o *firewalls* de perímetro.

3.4.3. Red interna

Las redes internas comúnmente son conocidas dentro de un marco operacional como las redes privadas pertenecientes a una organización en particular. La administración de dichas redes está bajo algún departamento de tecnología de información, comunicaciones o infraestructura y contiene los recursos más valiosos de toda una red organizacional. Es común encontrar en estas redes recursos como:

a. ***Hardware*.** CPUs, componentes electrónicos, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, discos de almacenamiento, líneas de comunicaciones, servidores de terminal, ruteadores.
b. ***Software*.** Fuentes de programas, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas de comunicación.
c. **Datos.** En tiempo real, almacenamiento en línea, almacenamiento fuera de línea, copias de respaldo, bitácoras de auditoría, bases de datos, en tránsito sobre el medio de comunicación.
d. **Documentación.** En programas, *hardware*, sistemas, procedimientos administrativos.

Cada uno de estos recursos, representa un activo muy valioso para la organización y como tales deben protegerse al máximo con el fin de evitar pérdidas y situaciones que pongan en riesgo la organización.

El control de estas redes están totalmente poseídos por la organización y sus políticas de seguridad pueden ser manejadas libremente para un mejor uso de los recursos.

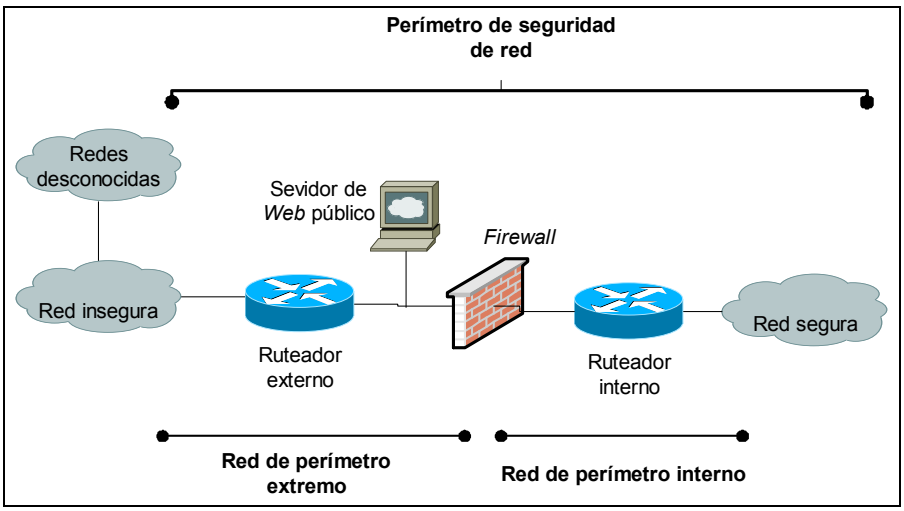
La política de seguridad para estas redes, establece que no deben permitirse conexiones desde redes desconocidas hacia algún recurso localizado dentro de ellas, lo más usual para estos casos, es que las conexiones desde redes inseguras lleguen hasta los servidores localizados en zonas desmilitarizadas, lo cual provee un nivel adicional de seguridad. La política interna en estas redes, es permitir que las conexiones sean originadas en equipos localizados dentro de ellas y vayan a cualquier red no importando a donde pertenece tal red.

3.5. Integración de redes perimetrales

Para definir varias redes de perímetro, se deben designar los segmentos de redes de computadoras que se desean proteger, y definir los mecanismos de seguridad de red que ellas protegerán. Para tener un perímetro de seguridad de redes efectivo, los *firewalls* deben ser el puente para todas las comunicaciones entre redes protegidas, redes externas y no conocidas.

Una red corporativa puede contener múltiples redes de perímetro. Cuando se describe, como es que las redes de perímetro son posicionadas relativamente con otras, tres tipos principales de redes perimetrales están presentes: el perímetro extremo, perímetros internos, y el perímetro más profundo. La figura 7 describe la relación entre varios perímetros. Notar que los múltiples perímetros internos son relativos a un particular medio, tal como el perímetro interno que está solo dentro el *firewall*.

FIGURA 8. Esquema de redes de perímetro



El perímetro de red extremo identifica el punto de separación entre los recursos que se tienen control y los recursos no se tiene el control, usualmente este punto es el ruteador que se usa para separar la red privada de la red del ISP. Las redes de perímetro internas presentan límites donde se deben tener otros mecanismos de seguridad instalados, tal como *firewalls* de *intranets* y ruteadores de selección.

La figura 8 describe dos redes de perímetro (una red de perímetro extremo y una red de perímetro interno), definido por la colocación de ruteadores internos y externos y un *firewall* de aplicación.

El posicionamiento del *firewall* entre los ruteadores interno y externo, provee algo de protección adicional de ataques sobre ambos lados, y reduce grandemente la cantidad de tráfico que el sistema de *firewall* debería evaluar, el cual podría incrementar el redimiendo del *firewall*. Desde la perspectiva de usuarios en una red externa, el sistema de *firewall* representa todas las computadoras accesibles en la red protegida. Esto define el punto de enfoque,

o punto de ahogo, mediante el cual todas las comunicaciones entre las redes deberían pasar.

El perímetro de red extremo, es el área de mayor inseguridad de la infraestructura de red. Normalmente, esta área es reservada para ruteadores, *firewalls*, y servidores de Internet públicos, tales como servidores *Web*, FTP y SMTP. Esta área de la red es la más fácil para ganar acceso, y por ello, es la más atacada con frecuencia, usualmente en un intento para ganar acceso a las redes internas. La información sensible de compañías que es para uso interno solamente no debería ser colocada en la red de perímetro extremo. Seguir ésta precaución ayuda a evitar robos o daños en la información sensible.

3.6. Sistema de direcciones IP en Internet

El direccionamiento lógico o de red de los equipos que se encuentren conectados a Internet debe de cumplir ciertas guías de diseño para evitar problemas de comunicaciones.

Como lo definen los estándares del protocolo IP, cada equipo perteneciente a una red debe contener una dirección compuesta por una porción de red y una porción de nodo o *host*. La porción de red representa a todos los equipo se encuentren conectados en el mismo segmento físico, y es común para todos los nodos contenidos dentro del mismo segmento físico. La porción de nodo representa el identificador único dentro del mismo segmento físico para cada equipo conectado a la red. Cuando se fusionan ambas porciones se obtiene un identificador único para cada equipo, esto significa que la dirección IP de un *host* no puede repetirse ni en el mismo segmento físico ni en otro segmento conectado directa o indirectamente.

Cuando una red privada perteneciente a cualquier organización se conecta a la red Internet, también existe el riesgo de que un nodo de la red tenga la misma dirección IP de algún nodo conectado a Internet. Como resultado estos dos nodos jamás podrán establecer una conexión directa entre ellos, a menos que se utilice algún método de traducción de direcciones IP.

Para evitar este tipo de problemas en redes privadas, se han definido algunos lineamientos de diseño en el contexto de direccionamiento IP. El documento que describe detalladamente estos lineamientos es el RFC 1918. Lo más importante de este estándar es presentado a continuación:

La "autoridad de números asignados en Internet", *Internet Assigned Numbers Authority* (IANA), ha reservado los tres siguientes bloques de direcciones IP para el uso en redes privadas:

10.0.0.0 - 10.255.255.255 (prefijo 10/8)
172.16.0.0 - 172.31.255.255 (prefijo 172.16/12)
192.168.0.0 - 192.168.255.255 (prefijo 192.168/16)

Una empresa que decida usar direcciones IP del espacio de direcciones definido anteriormente, puede hacerlo sin tener que coordinarse con la IANA o con un registro de Internet. De esta manera el espacio de direcciones puede ser usado por muchas empresas. Las direcciones de este espacio de direcciones privado sólo serán únicas dentro de la empresa, o el conjunto de empresas que elijan colaborar sobre este espacio para que puedan comunicarse con las demás en su propia Internet privada.

Como antes, cualquier empresa que necesite espacio de direcciones globalmente único necesita obtener tales direcciones de un registro de Internet.

Una empresa que solicite direcciones IP para su conectividad externa nunca recibirá direcciones de los bloques definidos arriba.

Para usar el espacio de direcciones privado, una empresa necesita determinar qué máquinas no necesitan disponer de conectividad de nivel de red hacia el exterior de la empresa en un futuro previsible y así poder clasificarlas como privadas. Tales máquinas usarán el espacio de direcciones privado, definido anteriormente. Las máquinas privadas pueden comunicarse con el resto de máquinas de la empresa, tanto públicas como privadas. Sin embargo, no pueden tener conectividad IP a ninguna máquina fuera de la empresa. Aunque no dispongan de conectividad IP externa (fuera de la empresa), las máquinas privadas aún pueden tener acceso a servicios externos mediante el uso de *firewalls* (por ejemplo, *firewalls* de nivel de aplicación).

El resto de máquinas serán públicas y usarán espacio de direcciones globalmente únicas, asignadas por un registro de Internet. Las máquinas públicas pueden comunicarse con otras máquinas dentro de la empresa, tanto públicas como privadas, y pueden tener conectividad IP con máquinas públicas fuera de la empresa. Las máquinas públicas no tienen conectividad con las máquinas privadas de otras empresas.

Puesto que las direcciones privadas no tienen significado global, la información de encaminamiento acerca de las redes privadas no se propagará en los enlaces entre empresas, y los paquetes con direcciones origen o destino privadas no deberían ser reenviados por dichos enlaces. Se supone que los enrutadores en las redes que no usen espacio de direcciones privadas, especialmente aquellos situados en los proveedores de servicios de Internet, estarán configurados para rechazar (filtrar) la información de encaminamiento acerca de redes privadas. Si uno de estos enrutadores recibe tal información, el rechazo no será tratado como un error en el protocolo de encaminamiento.

4. CASO DE ESTUDIO: DEFINICIÓN DE POLÍTICAS Y TECNOLOGÍAS DE SEGURIDAD PARA UNA COMPAÑÍA DE COMERCIO ELECTRÓNICO

El siguiente capítulo trata de un caso de estudio en el que se definen las condiciones de una compañía que comercializa productos a través de Internet. Con base en las condiciones, carácter de la compañía y requerimientos de negocio se desarrollarán las políticas de seguridad que deberán utilizarse para la definición de la arquitectura de seguridad tecnológica, la cual estará conformada por la definición de un esquema de seguridad perimetral que integre tecnologías de protección para garantizar seguridad en las operaciones de la compañía.

4.1. Descripción de la compañía

La compañía Mimbres, S.A. de tamaño mediano de 1000 empleados dedicada a la manufactura de artículos para el hogar en materiales de mimbre, tiene una presencia notable a nivel de América Central y ha decido expandir su mercado hacia Norteamérica principalmente a los Estados Unidos de América.

La dirección de la compañía ha decidido emplear varias estrategias de mercadeo para poder incursionar en mercados extranjeros, entre las que destacan la comercialización de sus productos a través de Internet. Para llevar a cabo dicha estrategia, Mimbres, S.A. ha decido montar su propia infraestructura para la comercialización de sus productos en Internet. La compañía se encuentra constituida en tres localidades: oficinas centrales,

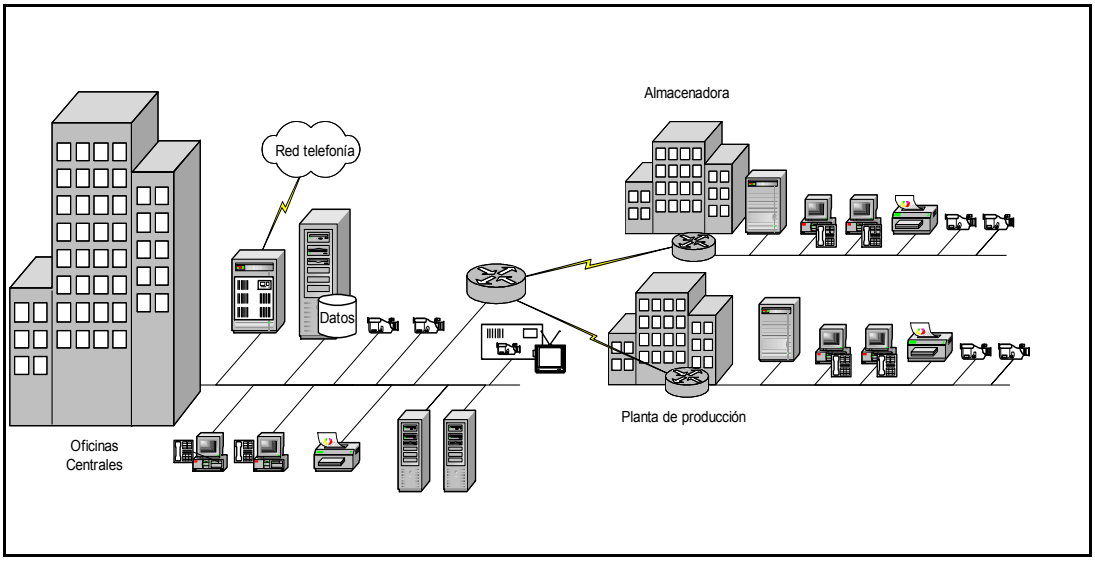
planta de manufactura y planta de almacenamiento. Las tres localidades se encuentran interconectadas a través de una red de datos extensa, la cual permite la sincronización de la información que se genera diariamente y la comunicación telefónica entre las localidades, así como otros servicios de colaboración y acceso. La compañía ya cuenta con un servidor de procesamiento de tecnología RISC para el manejo de las bases de datos que sirven de repositorio para el sistema central, el cual es utilizado para el control de inventarios, compras, ventas y la contabilidad.

Hasta el momento, la dirección de la compañía no había respaldado la conexión de la compañía a Internet, con excepción de algunas pocas estaciones de trabajo que se conectan ocasionalmente vía *dial-up*. La dirección no ha respaldado formalmente el uso de políticas de seguridad, para la protección de los recursos informáticos y como consecuencia se tiene un esquema de tecnologías de seguridad débil, tanto en infraestructura como en servicios de red. Para llevar a cabo la estrategia de negocio, la dirección reconoce los peligros que implica conectar su red privada a Internet y como contramedida de ello han definido una serie de políticas generales, que enmarcan los límites de la apertura de los recursos de red a Internet. Tomando como base los requerimientos de servicios informáticos de Internet, para la estrategia de negocio y los lineamientos de las políticas de seguridad se definirán las tecnologías de seguridad que más se ajusten con el propósito de resguardar los recursos privados y hacer posible la estrategia de comercialización de productos a nivel global. La compañía está dispuesta a invertir en las tecnologías de seguridad, que sean necesarias siempre y cuando el monto de la inversión no exceda el 20% del costo total del riesgo de ser víctima de un fraude o ataque.

4.2. Descripción de la red de datos

La compañía cuenta actualmente con una red de datos basada en protocolo IP, que se encarga de permitir el acceso al sistema central y del manejo de servicios de infraestructura como mensajería de correo electrónico, publicación de documentos, repositorio de archivos, sincronización entre bases de datos, servicios de impresión, telefonía IP, video para vigilancia, entre otros. La red cuenta con tres segmentos o redes de área local que son: red de oficinas centrales, red de planta almacenadora y red de planta de producción tal como se observa en la figura 9.

FIGURA 9. Diagrama general de red de datos



En el diagrama se puede observar que cada red local cuenta con sus propios recursos y proporciona servicios tanto a los usuarios de la red local como a las otras redes. Las redes de planta de producción y planta almacenadora dependen de los servicios de red de la red de oficinas centrales, por lo que se tienen arrendados dos servicios de enlaces dedicados de 512 Kbps cada uno.

Para la descripción de los servicios y recursos informáticos con que cuenta cada red se muestran las tablas I, II y III. Según se observa en las tablas, la red que cuenta con una cantidad mayor de usuarios y recursos de red es la de oficinas centrales, ya que la mayor parte de las actividades del negocio se realizan desde estas instalaciones, sin embargo se deben considerar los recursos de las otras redes, porque también forman parte de la infraestructura de comunicaciones de la compañía.

Tabla I. Servicios y recurso de red en oficinas centrales

RED DE OFICINAS CENTRALES	
Servicios	**Recursos**
Impresión de documentos	(5) impresoras departamentales, (2) servidores departamentales de servicios
Acceso al sistema central de operaciones	Información confidencial en bases de datos, *software* manejador de bases de datos, *software* cliente para interfaz del sistema, servidor central de bases de datos.
Telefonía	*Software* de manejo de llamas, servidor central de manejo de llamadas, (80) teléfonos IP, *software* de telefonía IP, mensajes telefónicos en servidor, contactos de usuarios de telefonía, servidor de telefonía.
Compartimiento de archivos	(2) servidores departamentales de servicios, información confidencial en carpetas compartidas como: informes de ingresos, egresos y utilidades de la compañía, esquemas y diagramación de diseños de productos, documentos de planificación, documentos de estrategias de mercadeo, documentación de infraestructura de red, fuentes de programas del sistema central

Continuación

Sincronización de bases de datos remotas	Bases de datos de ventas, inventarios de productos, recursos humanos
Mensajería de correo electrónico	Servidor departamental de servicios, mensajes de correo electrónico confidenciales, información exclusiva publicada, *software* de manejo de servicios de correo electrónico
Video para vigilancia local	(10) Cámaras de video IP, consola de administración de vigilancia IP,
Autenticación de usuarios de red	(2) servidores departamentales de servicios, información confidencial de cuentas y contraseñas de usuarios, *software* de autenticación de usuarios, usuarios de red
Publicación de información *Web*	Motor de publicación de páginas *Web*, servidor departamental de servicios, documentos y páginas *Web* confidenciales
Administración de equipos	*Software* de administración y monitoreo de equipos de red, información confidencial sobre la red, estación de monitoreo
Respaldo de datos	Unidad de cintas, *software* de respaldo de datos
Comunicaciones e infraestructura	La red cuenta actualmente con (90) estaciones de trabajo con sistema operativo MS *Windows*, (2) servidores departamentales de tecnología CISC con sistema operativo MS *Windows* 2000, (1) servidor central de bases de datos RISC con sistema operativo *Unix*, (4) *switch* L2 para acceso de 24 puertos, (1) *switch* de fibra de 8 puertos, (1) ruteador mediano con controladoras seriales.

Tabla II. Servicios y recursos de red en planta de producción

RED DE PLANTA DE PRODUCCIÓN	
Servicios	**Recursos**
Impresión de documentos	(2) impresoras departamentales, servidor departamental
Acceso al sistema central de operaciones	Información confidencial en bases de datos, *software* manejador de bases de datos, *software* cliente para interfaz del sistema, servidor departamental.
Telefonía	(20) teléfonos IP, *software* de telefonía IP en estaciones de trabajo
Compartimiento de archivos	Servidor departamental, información confidencial en carpetas compartidas como: gastos, diseños de productos, documentos de planificación, control de producción, automatización de productos.
Sincronización de bases de datos con oficina central	Bases de datos de ventas, inventarios de productos, recursos humanos
Mensajería de correo electrónico	Mensajes de correo electrónico confidenciales en estaciones de trabajo
Video para vigilancia local	(10) Cámaras de video IP, consola de administración de vigilancia IP.
Autenticación de usuarios de red	Información de cuentas de usuario y contraseñas, usuarios de red
Respaldo de datos	Unidad de cintas, *software* de respaldo de datos

Continuación

Comunicaciones e infraestructura	La red cuenta actualmente con (1) servidor departamental con sistema operativo MS *Windows* 2000, (40) estaciones de trabajo con sistema operativo MS *Windows*, (2) *switch* L2 para acceso de 24 puertos, (1) ruteador pequeño con una controladora serial para el enlace WAN, (2) *Wireless Access Point* para acceso a red.

Tabla III. Servicios y recursos de red en planta almacenadora

RED DE PLANTA ALMACENADORA	
Servicios	**Recursos**
Impresión de documentos	(2) impresoras departamentales, servidor departamental
Acceso al sistema central de operaciones	Información confidencial en bases de datos, *software* manejador de bases de datos, *software* cliente para interfaz del sistema, servidor departamental.
Telefonía	(20) teléfonos IP, *software* de telefonía IP en estaciones de trabajo
Compartimiento de archivos	Servidor departamental, información confidencial en carpetas compartidas como: informes de egresos de la compañía, esquemas y diagramación de diseños de productos, documentos de planificación, documentos de estrategias de mercadeo, control de producción, automatización de productos.
Sincronización de bases de datos con oficina central	Bases de datos de ventas, inventarios de productos, recursos humanos
Mensajería de correo electrónico	Mensajes de correo electrónico confidenciales en estaciones de trabajo

Continuación

Video para vigilancia local	(10) Cámaras de video IP, consola de administración de vigilancia IP.
Autenticación de usuarios de red	Información de cuentas de usuario y contraseñas, usuarios de red
Respaldo de datos	Unidad de cintas, *software* de respaldo de datos
Comunicaciones e infraestructura	La red cuenta actualmente con (1) servidor departamental con sistema operativo MS *Windows* 2000, (30) estaciones de trabajo con sistema operativo MS *Windows*, (2) *switch* L2 para acceso de 24 puertos, (1) ruteador pequeño con una controladora serial para el enlace WAN, (1) *Wireless Access Point* para acceso a red

4.3. Requerimientos para la estrategia de negocio

La compañía planea a corto plazo, contar con una estrategia de comercialización global que le permita extender su mercado a Norteamérica. Sus clientes potenciales serán distribuidores localizados en los países de Estados Unidos y México. Para llevar a cabo tal estrategia, la compañía se fundamenta en la reestructuración de procesos y utilización de las herramientas de comercio electrónico.

Para proporcionar un nivel de mayor agresividad en el mercado, invertirá en su propia infraestructura de comercio electrónico utilizando como base la infraestructura que ya posee, con ello logrará obtener los siguientes beneficios:

a. Flexibilidad y adaptabilidad en los cambios del sistema de comercio electrónico.

b. Mantenimiento y operabilidad de los sistemas de forma continua.
c. Confiabilidad en el sistema.
d. Capacidad de crecimiento futuro.

Entre las medidas que han tomado para la reestructuración de la arquitectura tecnológica se describen:

a. Contratar un canal de datos de 1 Mbps que le permita tener conexión a Internet todo el tiempo.
b. Para agilizar el proceso de producción se contratará un canal de datos dedicado, de 128 Kbps para la solicitud en línea de materia prima con un proveedor local Fibras Naturales, S.A.
c. Fortalecer la seguridad de la red perimetral, diseñando una política de seguridad que permita la protección de los recursos e integre las tecnologías de seguridad más efectivas.
d. Construir una aplicación *Web* para la tienda virtual en Internet.
e. Adquirir dos servidores CISC para el sistema de tienda virtual.
f. Adquirir un *switch* de aplicación para la distribución del procesamiento de trafico *Web* y encriptamiento.
g. Adquirir un certificado digital para la comercialización en Internet.
h. Habilitación del sistema de tienda virtual en Internet.
i. Habilitación de los servicios de correo electrónico a Internet.
j. Habilitación de los servicios de resolución de nombres en Internet.
k. Habilitación del servicio de navegación de los usuarios de la compañía en Internet.

4.4. Requerimientos para la política de seguridad perimetral

Una vez definidos los aspectos de estrategia de negocios, infraestructura de comunicaciones, composición de red de datos, servicios y recursos se definirán los requerimientos de seguridad para el desarrollo de una política de seguridad perimetral, que permita proteger los recursos de la red a través de tecnologías de seguridad perimetral, mecanismos y procedimientos para monitorear, reforzar y auditar continuamente la seguridad.

La dirección de la compañía, conociendo los riesgos y peligros de interconectar la red de la organización a Internet, ha impuesto criterios de seguridad estrictos. Se ha determinado que la nueva estrategia de negocios se mantendrá en pie, solamente cuando los riesgos de posibles problemas de seguridad, tales como accesos no autorizados o robos de información, sean absolutamente minimizados.

Los requerimientos de seguridad que la dirección de la compañía ha propuesto en torno a los cambios de infraestructura son los siguientes:

1. Aislar la red privada local de la red pública de Internet, para prevenir el acceso inautorizado de intrusos a los recursos informáticos.
2. Aislar la red privada local de la red del proveedor Fibras Naturales, S.A. para prevenir el acceso inautorizado de usuarios a los recursos informáticos.
3. Habilitar los servicios de la aplicación de tienda virtual en Internet para que posibilite el proceso de ventas globales, garantizando integridad, confidencialidad y disponibilidad en transacciones e información de los clientes como los números de tarjetas de crédito así como la aplicación de tienda virtual.

4. Habilitar el servicio de mensajería de correo electrónico en Internet, con filtrado de mensajes anómalos, protección confidencial de los mensajes y protección del sistema de mensajería.
5. Habilitar los servicios de resolución de nombres en Internet, que garanticen la máxima disponibilidad de servicio y que proteja la integridad del repositorio de información que maneja.
6. Habilitar el servicio de navegación para algunos usuarios de la red interna de las tres localidades y que permita:
    a. Decidir que usuario tiene acceso al servicio.
    b. Decidir el tipo de acceso para el usuario, como por ejemplo: navegar en páginas, descargar archivos tipo multimedia.
    c. Decidir los contenidos que el usuario podrá ver en Internet, como por ejemplo: noticias, deportes, ocio, finanzas, etc.
    d. Decidir el horario en que el usuario podrá utilizar el servicio
7. Mantener continuamente un proceso de vigilancia y monitoreo.
8. Mantener un proceso regular de auditoría de seguridad de los recursos.
9. Formar una división dentro de la compañía encargada de la seguridad de los recursos informáticos con los siguientes roles:
    a. Creación de las políticas de seguridad informáticas.
    b. Actualización permanente de las políticas de seguridad.
    c. Distribución de las políticas de seguridad a nivel operacional.
    d. Supervisión del cumplimiento de las políticas de seguridad en todo nivel.
    e. Definición de procesos y mecanismos de seguridad.
    f. Definición de la arquitectura de seguridad.
    g. Soporte para toma de decisiones en seguridad informática.
    h. Manejo de incidentes de seguridad.
10. Proteger la confidencialidad e integridad de las bases de datos del sistema central.

11. Contratar anualmente los servicios de una firma de seguridad externa que certifique los mecanismos de protección de la red perimetral.
12. Mantener un proceso continuo de reforzamiento de la seguridad, para los sistemas informáticos, actualizando continuamente los componentes con fallas de seguridad y corrigiendo configuraciones vulnerables.
13. Garantizar la confidencialidad de la información secreta.
14. Aplicar controles de seguridad física.
15. Definir los mecanismos para el manejo de incidentes de seguridad.

4.5. Política de seguridad perimetral

El objetivo de la política de seguridad perimetral de Textiles, S.A. es definir los lineamientos para proteger todos los elementos de la red interna, incluyendo *hardware*, *software*, datos, etc. de cualquier amenaza que sea originada desde el exterior, a la vez, que se garanticen niveles de confianza, permitiendo selectivamente el acceso de determinados usuarios externos a determinados servicios y denegando cualquier tipo de acceso a otros.

4.5.1. Identificación de recursos que protege

Tabla IV. Clasificación de riesgo en recursos de datos

Cantidad	Recurso	Sensibilidad	Amenaza
3	Bases de datos sistema central	Muy alta	Media
30	Mensajes en buzones telefónicos	Media	Baja
7500	Mensajes de correo electrónico en buzón	Alta	Alta
800	Publicación de documentos en sistema de mensajería	Alta	Alta
4800	Documentos y páginas *Web*	Alta	Alta
25	Documentos de información de la red y configuración de equipos	Media	Media

Continuación

1500	Documentos de informes de ingresos, egresos y utilidades de la compañía, diseño de productos, planificación, estrategias de mercadeo, infraestructura de red, código fuente sistema central en oficinas centrales	Muy alta	Media
2	Bases de datos planta	Muy alta	Media
350	Documentos de gastos, diseños de productos, planificación, control de producción, automatización de productos en planta	Muy alta	Media
22000	Mensajes de correo electrónico en estaciones de trabajo	Alta	Alta
3200	Documentos de trabajo en estaciones de trabajo	Media	Alta
150	Cuentas de usuario y contraseñas	Muy alta	Alta
450	Documentos de gastos, inventarios de productos, planificación en almacenadora	Alta	Media
75	Bases de datos del sistema en almacenadora	Muy alta	Baja

Tabla V. Clasificación de riesgo en recursos de *hardware*

Cantidad	Recurso	Sensibilidad	Amenaza
9	Impresora	Media	Baja
4	Servidor departamental de servicios	Alta	Baja
1	Servidor central de bases de datos	Muy alta	Baja
120	Teléfono IP	Baja	Baja
1	Servidor de telefonía IP	Alta	Baja
30	Cámara de video IP	Muy alta	Alta
3	Consola de administración de video	Muy alta	Alta
6	Unidad de cintas	Baja	Baja
160	Estación de trabajo	Media	Baja
8	*Switch* L2 para acceso	Alta	Media
1	*Switch* L3 para *core*	Alta	Media
1	Ruteador mediano con controladores seriales	Media	Media
2	Ruteador pequeño con puerto serial	Media	Media
3	*Wireless Access Point*	Media	Media

Tabla VI. Clasificación de riesgo en recursos de *software*

Cantidad	Recurso	Sensibilidad	Amenaza
1	Manejador de bases de datos central	Alta	Media
130	Interfaz cliente de sistema central	Media	Media
1	Manejador de llamadas	Alta	Baja
35	Cliente de telefónico	Baja	Baja
1	Manejo de servicios de correo electrónico	Alta	Alta
3	Manejador de consola de administración de video	Muy alta	Media
1	Servicio de publicación de páginas *Web* de la *Intranet*	Alta	Alta
1	Administración y monitoreo de equipos de red	Alta	Alta
6	Respaldo/recuperación de datos	Media	Baja
160	Sistema operativo cliente MS *Windows*	Baja	Media
1	Sistema operativo *Unix* en servidor base de datos central	Alta	Media
4	Sistema operativo MS *Windows* 2000 Server	Alta	Media
1	Manejador de bases de datos en planta	Alta	Baja
1	Manejador de bases de datos en almacenadora	Alta	Baja

Tabla VII. Clasificación de riesgo de recursos para comercio electrónico

Cantidad	Recurso	Tipo	Sensibilidad	Amenaza
1	Servidor CISC para procesamiento de aplicación de tienda virtual	*Hardware*	Media	Media
1	Base de datos de tarjetas de crédito e información de clientes	Dato	Muy Alta	Muy Alta

Continuación

1	Motor de operación *Web* para aplicación de tienda virtual	*Software*	Alta	Muy alta
350	Paginas dinámicas de aplicación de tienda virtual	*Software*	Alta	Muy alta
1	Ruteador para enlace a Internet	*Hardware*	Media	Alta
3	Ruteador para enlace a Fibras Naturales	*Hardware*	Media	Baja
1	Sistema operativo de usuarios con acceso a Internet	*Software*	Alta	Alta
1	Servicio de resolución de nombres en Internet	*Software*	Alta	Alta
5	Registros del servicio de resolución de nombres en Internet	Dato	Alta	Alta
1	*Switch* de aplicación para distribución de tráfico *Web*	*Hardware*	Alta	Alta

4.5.2. Identificación de amenazas externas

Tabla VIII. Clasificación de amenazas externas

Num.	Fuente de ataque	Tipo de ataque	Posibilidad
1	Ex empleados *host*iles	Denegado de servicio, robo de información, destrucción de información	Media
2	Proveedores	Operación accidental o involuntaria, denegado de servicio, robo de información, destrucción reinformación	Baja
3	Competidores	Robo de información	Alta
4	*Hackers*	Denegado de servicio, alteración de información, destrucción de información, robo de información	Muy alta

Continuación

1	Virus/gusanos	Denegado de servicio, corrupción de sistema, robo de información, destrucción de información, alteración de información	Muy alta
3	Ladrones profesionales	Robo de información, fraude financiero	Muy alta

4.5.3. Conexión a Internet

Se utilizará un canal de acceso permanente a Internet de 1 Mbps de ancho de banda. El canal deberá ser de uso exclusivo de la compañía y deberá ser utilizado por los siguientes motivos:

a. Para permitir que la página www.mimbresa.com.gt sea publicada en Internet, y la cual contiene el aplicativo de tienda virtual para las compras de productos en línea.
b. Para la transferencia de mensajería de correo electrónico en Internet.
c. Para la navegación de usuarios autorizados en Internet, cuya información consultada esté relacionada con el negocio de la compañía.
d. Para actualización en línea de productos de *software* de red, que necesite constantemente actualizarse.
e. Para la publicación del servicio de DNS, el cual contiene los registros de nombres de dominio.

El uso inapropiado del canal de Internet por parte de algún usuario de la red será registrado y sancionado, notificando el hecho al jefe inmediato superior. Cualquier actividad en Internet desde la red interna será registrada y se entregará un reporte mensual a cada jefe de área sobre el uso del mismo. Se prohíbe terminantemente el uso del canal para:

a. Descarga de música en formatos de archivos mp3, o similar.
b. Descarga de *software* gratuito que no represente ningún beneficio para las actividades de los usuarios.
c. Descarga de programas como juegos, videos, películas.
d. Escuchar música en línea.
e. Ver videos en línea.
f. Consulta de material ofensivo, violencia, sexo, fanatismo, etc.
g. Charlar en línea.
h. Compartir material como música, *software*, videos a usuarios externos.

4.5.4. Conexión a redes externas de proveedores, socios de negocios y clientes

Para la interconexión entre la red privada y otras redes externas de entidades como proveedores, socios de negocios y clientes deberán estar aisladas por barreras de protección de control de acceso, de tal forma que el acceso a todos los recursos de la red interna deberán estar bloqueados con excepción de los servicios de sincronización y transferencia de información de aplicaciones.

Los ruteadores que serán utilizados para estas conexiones deberán estar configurados con listas de control de acceso por protocolo IP, deberán tener desactivados todos los servicios innecesarios de red, deberán estar protegidos contra ataques de denegado de servicio, tendrán que registrar todos los eventos de desempeño y seguridad.

La conexión física de estos enlaces deberá ser a un segmento de red desmilitarizada definido por el *firewall* perimetral.

Tanto el ruteador del enlace como el *firewall* y otros dispositivos empleados para este tipo de conexiones deberán ser propiedad de la compañía y administrados por personal interno. Las cuentas y claves de acceso serán conocidas solo por personal autorizado de la compañía y bajo ninguna circunstancia deberán ser compartidas con personal externo o personal inautorizado.

4.5.5. Equipo de protección para zona perimetral

4.5.5.1 Ruteador para conexión a Internet

Se utilizará un ruteador perimetral para unir la red del proveedor de servicios de Internet y la zona perimetral externa de la compañía. La seguridad de este ruteador deberá estar configurada apropiadamente de tal forma, que se reduzca considerablemente el riesgo de un ataque desde redes externas. El ruteador deberá estar configurado con:

a. Listas de control de acceso, que eviten el tráfico desde redes con direcciones IP privadas según el RFC 1918, direcciones IP de diagnóstico 127.0.0.0, IP *spoofing*,
b. Inhabilitación de servicios de red informativos como *finger*, SNMP, *whois*, NMAP, etc.
c. Restricción de acceso a consola por medio de protocolos con encriptamiento de datos como SSH. El acceso a consola deberá ser habilitado exclusivamente para ciertos usuarios desde un grupo predefinido de direcciones IP.
d. Restricción del paso de tráfico con protocolos de descubrimiento de topología de red y denegado de servicio.
e. Habilitación de servicios para registro de eventos y auditoría.

f. Habilitación de servicios para monitoreo de eventos y comportamiento del tráfico entrante y saliente.

El ruteador deberá estar bajo el control de acceso físico, ya que el acceso inautorizado al equipo podría comprometer la seguridad.

4.5.5.2 *Firewall* de perímetro para conexión a redes externas

Como barrera entre la red perimetral y la red interna de la compañía deberá haber instalado un *firewall,* el cual se encargará de garantizar control de acceso de tráfico desde y hacia Internet. Este dispositivo permitirá esconder todos los recursos de la red interna actuando como una barrera perimetral y dejará publicar los servicios del sistema de tienda virtual, mensajería de correo electrónico y resolución de nombres. También permitirá la salida de tráfico que se origine desde la red interna hacia Internet, principalmente para la navegación de usuarios, garantizando que los usuarios puedan tener acceso a los recursos externos de Internet de forma tal que no comprometa la seguridad de los recursos informáticos de la red interna. El *firewall* deberá incluir las siguientes funcionalidades:

a. *Firewall* de tecnología *Stateful Packet Inspection* independiente de sistema operativo convencional.
b. Sistema de traducción de direcciones estática y dinámica.
c. Capacidad para registrar eventos del sistema y generación de reportes.
d. Con capacidad para ser manejado a través de un *software* de definición de políticas de seguridad.
e. Capacidad de reglas de tráfico IP.
f. Soporte de filtros de contenido *Web* como *ActiveX*, *Applets* para protección de los usuarios internos.
g. Autenticación, autorización y auditoría de usuarios.

h. Soporte de actualización del sistema operacional para mejoras de funcionalidad y protección de vulnerabilidades.
i. Capacidad de adaptarse a esquema de *failover.*
j. Respaldo y recuperación de la configuración del sistema.

4.5.5.3 Sistema de detección de intrusos para Internet

Se deberá habilitar un sistema de detección de intrusos de red, basado en un sistema de supervisión de tráfico de red, en tiempo real con la capacidad de detectar tráfico malicioso y alertar a los administradores sobre cualquier posible amenaza. Este equipo deberá estar localizado físicamente en el segmento perimetral entre el ruteador y el *firewall* para que pueda escuchar todo el tráfico que viene desde Internet y se dirige a la red interna. El detector de intrusos deberá cumplir con estas características generales:

1. El rango de cobertura deberá ser para analizar tráfico de red completa, de tal forma que tenga la capacidad de escuchar todo el tráfico IP que se pase a través del canal de datos.
2. El sistema de detección deberá ser de tipo reactivo para que tenga la capacidad de responder ante una actividad ilegal.
3. Vigilar el tráfico de red que se dirige a los recursos de la red interna, atravesando el *firewall*.
4. Examinar todo el contenido de los paquetes IP.
5. Mantener una base de datos local de firmas de ataques, que se encuentre actualizada en forma automática y que servirá para que el detector pueda comparar patrones de tráfico ilícito.
6. Rendimiento para analizar tráfico en tiempo real al menos a 45 Mbps.
7. Algoritmos de detección heurística y anómala.

8. Protección de ataques de denegado de servicio (DoS), gusanos o virus, saturación de *buffer*, ataques de fragmentación de paquetes, ataques a servicios protocolos como ICMP, FTP, WWW, SMTP, DNS, robos de sesión.
9. Capacidad para personalizar firmas de ataques.
10. Envió de alarmas a sistemas por correo electrónico, SNMP, *pager*.
11. Interfaz de administración gráfica con canal protegido.
12. Protección de técnicas de evasión anti-IDS.
13. Capacidad de respuesta activa, modificando listas de acceso en ruteadores y *firewalls*, finalizando sesiones TCP.

4.5.6. Acceso perimetral a servicios de publicación de tienda virtual

Para permitir el acceso de conexión de los clientes externos desde Internet hacia la aplicación de tienda virtual, se deberán habilitar ciertos accesos del protocolo en el *firewall* de perímetro. Los protocolos de TCP que deberán habilitarse son el WWW y SSL y deberán estar habilitados exclusivamente para la dirección IP local del servicio *Web* y SSL. La dirección IP local del servicio de publicación de la aplicación de tienda virtual deberá ajustarse al estándar RFC 1918 y será traducida a una dirección IP pública de Internet por medio del mecanismo de traducción de direcciones del *firewall* perimetral, de tal forma que la dirección IP real nunca sea conocida por un usuario externo. Esta política de control de acceso perimetral deberá habilitarse en el *firewall* e indicará:

a. Permitir a cualquier dirección IP de Internet tener acceso al protocolo TCP del puerto 80 asociado con el IP local del servicio *Web*.
b. Permitir a cualquier dirección IP de Internet tener acceso al protocolo TCP del puerto 443 asociado con el IP local del servicio SSL.
c. Denegar cualquier otro tipo de tráfico.

4.5.7. Acceso perimetral a servicios de mensajería de correo electrónico y resolución de nombres de dominio en Internet

Para permitir la transferencia de mensajes de correo electrónico, entre los usuarios de la red interna e Internet y la publicación de nombres del dominio mimbresa.com.gt deberá definirse los accesos correspondientes en el *firewall*. El protocolo de TCP que deberá ser habilitado para el servicio de correo electrónico es el SMTP y para la publicación de nombres de dominio deberá ser el protocolo UDP llamado DNS *domain*. La dirección IP local de ambos servicios deberá ajustarse al estándar RFC 1918 y será traducida a una dirección IP pública de Internet por medio del mecanismo de traducción de direcciones del *firewall* perimetral, de tal forma que la dirección IP real nunca sea conocida por un usuario externo.

Esta política de control de acceso perimetral deberá habilitarse en el *firewall* e indicará:

a. Permitir a cualquier dirección IP de Internet tener acceso al protocolo TCP del puerto 25 asociado con el IP local del servicio SMTP.
b. Permitir a cualquier dirección IP de Internet tener acceso al protocolo UDP del puerto 53 asociado con el IP local de publicación DNS.
c. Denegar cualquier otro tipo de tráfico.

4.5.8. Acceso perimetral a servicios de navegación en Internet de usuarios internos

Se deberá habilitar la salida de navegación a usuarios de la red interna, a través de una cuenta de usuario de red, de tal forma que el acceso no sea dependiente de una dirección IP o dirección física de *hardware,* ya que el

sistema de asignación de direcciones IP para estaciones de trabajo será dado a través de un servidor de direcciones dinámicas.

Para el control de acceso a Internet se deberá utilizar una herramienta basada en *software* con las siguientes funcionalidades:

1. Autenticar a grupos de usuarios o usuarios individuales, de tener acceso en Internet a través de cuentas de usuario, nombre de estación de trabajo, dirección IP de trabajo y por subred IP.
2. Autorizar a grupos de usuarios o usuarios individuales de tener acceso en Internet con los protocolos WWW, SSL, FTP, SMTP, POP3, DNS.
3. El sistema deberá delimitar el contenido de páginas *Web* que un grupo de usuarios o usuario individual pueda acceder en Internet. Esto significa que el sistema debe manejar una base de datos de categorías de contenidos y deberá ser actualizada automáticamente cada semana en horario no hábil. Las categorías mínimas que la herramienta deberá operar son: noticias, finanzas, tecnología, deportes, ocio, sexo, religión, *software*, violencia, juegos, cine, comercio, banca, telecomunicaciones, herramientas de Internet. La herramienta también deberá definir reglas para denegar o permitir sitios específicos de Internet y podrán ser agrupados en categorías conforme el criterio del administrador.
4. El sistema deberá permitir configurar para un usuario o grupo de usuarios el horario de acceso a Internet y permitirá definir el intervalo de tiempo máximo que un usuario podrá hacer.
5. Delimitar el ancho de banda máximo que un usuario o grupo de usuarios podrán hacer uso en Internet.
6. Generación de reportes de navegación clasificado por usuario, utilización de ancho de banda, categoría de contenido *Web*, servicios de navegación. El sistema deberá permitir obtener la lista de los usuarios con

mayor uso de recursos de Internet de tal forma que se pueda llevar un control mensual del nivel de utilización de los usuarios en Internet.

7. La herramienta deberá tener la capacidad de comunicarse con el *firewall* perimetral, para indicar si el *firewall* deniega o permite el acceso de salida a Internet de un usuario en particular.

El *firewall* también deberá definir el control de acceso de salida a Internet. Este control de acceso permitirá delimitar la dirección IP de la red interna y redes remotas que tendrán el acceso a Internet. Para llevar a cabo la traducción de direcciones locales a direcciones públicas de Internet se deberán asociar las direcciones de red IP internas con la dirección IP, que tendrá asociada el adaptador de red externa del *firewall*, logrando con ello hacer uso eficiente de las direcciones IP públicas. La política de acceso a definir en el *firewall* debería incluir lo siguiente:

1. Permitir a la red interna y redes remotas tener acceso a cualquier *host* de Internet a los protocolos WWW, SSL, FTP, SMTP, POP3, DNS, ICMP.
2. Solicitar al servidor de *software* de control de navegación la autenticación y autorización de accesos de usuarios para la red interna y redes remotas.
3. Filtrado de componentes *JavaScript* y *ActiveX* de la red interna y redes remotas para eliminar la posibilidad de violaciones de seguridad en estaciones de trabajo mientras se navega en Internet.

4.5.9. Proceso de vigilancia y monitoreo de los recursos de red

Se deberán habilitar mecanismos que garanticen la vigilancia continua de los equipos de protección perimetral, así como recursos de la red interna con posibilidades de sufrir daños desde Internet.

Para llevar a cabo el proceso de vigilancia, deberá habilitarse un sistema de detección de intrusos, el cual ha sido descrito con anterioridad. Mediante este sistema se podrá vigilar continuamente y en tiempo real cualquier intrusión maliciosa desde Internet de tal forma que el personal de seguridad informática pueda recibir notificaciones inmediatamente y pueda tomar medidas adecuadas para impedir daños.

El sistema de detección de intrusos deberá estar preparado para analizar cualquier patrón de tráfico, que pueda ser considerado dañino para red interna. El proceso de vigilancia deberá estar habilitado las veinticuatro horas del día los 365 días del año y permitirá analizar todo tráfico sobre la red dirigido a la red interna y recursos de protección perimetral.

Deberá haber personal especializado en el proceso de monitoreo continuo en tiempo real de los eventos de seguridad, que puedan reportarse en la red perimetral e interna. El sistema de detección de intrusos, deberá alertar al personal por medio de mensajes de correo electrónico, de tal forma que el personal pueda reaccionar inmediatamente evaluando el nivel de impacto de los ataques para tomar medidas de reacción que permitan resguardar los recursos de la red.

Se instalará una herramienta de *software* para obtener datos de tráfico de los ruteadores de Internet y los enlaces WAN a través del protocolo SNMP, a intervalos regulares y que permitirá la representación gráfica a través de páginas HTML, con lo cual se tendrá una idea bastante aproximada del nivel de carga de la red en los distintos periodos del día. Esta monitorización del tráfico ayudará a detectar actividades sospechosas, si se detectara mucho tráfico a horas no habituales.

4.5.10. Proceso de auditoría de seguridad

4.5.10.1 Inspección de actividades en sistemas

La auditoría de seguridad será un proceso regular, que deberá utilizarse para mejorar continuamente la seguridad de la red. No solamente proporcionará el medio para identificar quién ha accedido a los sistemas sino que también permitirá indicar como es que los sistemas han sido utilizados por usuarios autorizados y externos a la compañía.

Los sistemas de red deberán ser configurados, de tal forma que puedan registrar en un repositorio central cualquier evento que tenga que ver con seguridad y deberá ser utilizado para el proceso de auditoría. El repositorio central deberá estar formado por bitácoras de seguridad o archivos tipo *Log* y deberá incluir la información de equipos de red tales como ruteadores, *firewall*, *switch* y detectores de intrusos. Adicionalmente, los sistemas operativos, servicios *Web*, bases de datos, aplicaciones y otros sistemas deberán ser configurados con políticas de auditoría para dejar registro de los accesos a los sistemas.

Las bitácoras deberán ser analizadas dos veces al día, con el propósito de verificar si la seguridad de los recursos ha sido comprometida en algún momento. Este procedimiento de análisis permitirá conocer si han existido intentos de acceso inautorizado a los equipos y permitirá tomar decisiones de fortalecimiento de la seguridad en los equipos. Los equipos deberán ser configurados para que cada evento sea registrado en las bitácoras con su respectiva fecha y hora en que ha ocurrido. Para que la fecha y hora de los sistemas sea la misma se deberá sincronizar el reloj con el servicio de NTP (*Network Time Protocol*, Protocolo de tiempo de red), esto permitirá que al

analizar la información de bitácoras de distintos equipos se pueda llevar un orden cronológico global en que sucedieron los eventos.

Toda información de bitácoras de eventos de seguridad, deberá ser respaldada con el objetivo de poder reconstruir los hechos en caso sea necesaria una auditoría de eventos de seguridad. La información deberá ser clasificada por equipo, año, mes y día. La información deberá almacenarse físicamente en una caja fuerte y no podrá destruirse por ningún motivo.

4.5.10.2 Detección de vulnerabilidades en sistemas

El proceso de auditoría también involucra el análisis activo de detección de vulnerabilidades y debilidades de seguridad en los sistemas instalados en la red perimetral. Debido a que la seguridad es de carácter dinámico, se deberá evaluar el nivel de salud de la seguridad de los sistemas, tanto, desde el perímetro externo como en la misma red interna. Este proceso de manejo de vulnerabilidades deberá implementar la evaluación sistemática y regular de vulnerabilidades de sistemas, redes, aplicaciones y bases de datos. El proceso permitirá dar a conocer las vulnerabilidades detectadas en los sistemas y proporcionará el nivel de riesgo medido en cada una de ella con el propósito de tomar medidas de acción que ayuden a reformar la seguridad de la red.

Para fortalecer este proceso de manejo de vulnerabilidades deberá apoyarse en una herramienta de *software* de detección de vulnerabilidades con las siguientes características:

a. La herramienta deberá simular por medio de programas predefinidos, distintos tipos de ataques a la seguridad de los sistemas bajo condiciones controladas.

b. Capaz de evaluar la seguridad de un sistema particular, grupo de servidores o toda una red.
c. Capaz de detectar vulnerabilidades en servidores *Web*, servidores de archivos, servidores de aplicación, servidores de *Intranet/Extranet*, *firewalls*, ruteadores, *switch*, *hubs*, servidores de acceso remoto, bases de datos, aplicaciones, sistemas operativos de red.
d. Manejo de una base de datos de vulnerabilidades conocidas que permita la actualización periódica en forma automática
e. Capaz de generar instrucciones paso a paso sobre la corrección de las vulnerabilidades detectadas en los sistemas.
f. Capaz de generar información de análisis de riesgo de las vulnerabilidades detectadas en los sistemas con el propósito de toma de decisiones en la protección de los sistemas. Por cada vulnerabilidad encontrada deberá asociar información como: nivel de impacto, grado de complejidad de corrección, grado de complejidad de que sea explotada por un intruso, nivel de posibilidad de ser ejecutada, nivel de conocimiento en Internet.

Los administradores de seguridad podrán hacer uso de esta herramienta, para automatizar el proceso de auditoría y detección de vulnerabilidades en los sistemas, obteniendo como resultado una lista completa de las debilidades encontradas en los sistemas de la red para un posterior análisis de riesgos y toma de decisiones para el reforzamiento de la seguridad.

Este proceso deberá ser ejecutado con una periodicidad trimestral y será llevado a cabo en horas inhábiles de trabajo, para no interrumpir con las actividades de negocio de la compañía. Es muy importante tomar en cuenta que los sistemas que estén inhabilitados en la red, no podrán ser analizados por la herramienta y que mientras sea llevado a cabo el análisis de detección de

vulnerabilidades ningún usuario final deberá acceder a los sistemas. Otra consideración a tomar en cuenta es que un sistema pueda resultar inoperable producto de la aplicación del análisis de detección de vulnerabilidades aplicado por la herramienta.

4.5.10.3 Inspección de configuración en sistemas

Deberá implementarse un proceso periódico de inspección de la configuración de sistemas, con el propósito de descubrir posibles debilidades en la configuración que puedan comprometer los recursos de la red. Este proceso deberá ser habilitado principalmente en sistemas como: sistemas operativos de servidor, servicios de *Web*, privilegios y acceso de usuario, archivos de configuración de aplicación, *firewall*, ruteadores, *switch*, sistemas de detección de intrusos, bases de datos y cualquier otro sistema que opere y actúe a través de la configuración predefinida.

Esta inspección deberá habilitarse trimestralmente y deberá proporcionar la información obtenida de forma clasificada como: debilidad de configuración, sistema asociado con la debilidad, nivel de impacto, complejidad de corrección. Esta información obtenida deberá ser utilizada por la dirección del departamento de seguridad de red para la toma de decisiones y medidas de acción que permitan reforzar la configuración de los sistemas.

4.5.10.4 Inspección de componentes de *software* en sistemas operativos

El administrador encargado de la seguridad de los sistemas operativos deberá implementar un proceso con periodicidad semanal en el que se inspeccione minuciosamente los componentes de *software* que están operando

sobre los sistemas en la línea perimetral, esto con el objetivo de describir posibles programas como virus, gusanos o troyanos. Estos programas dañinos pueden comprometer seriamente la seguridad de la red y si no es implementado un proceso de inspección regular nunca podrían ser detectados.

Este proceso deberá ser complementado con la instalación de una herramienta antivirus, que deberá ser instalado en el sistema operativo de los servidores críticos. La base de datos de registro de virus del programa deberá ser actualizada dos veces por semana y será un proceso automático en el que la actualización sea obtenida de un servidor de la red.

El administrador también deberá utilizar herramientas de rendimiento para inspeccionar el uso de recursos de *hardware* como procesador, memoria física, memoria virtual, utilización de la red, discos duros. Esta inspección permitirá identificar el uso irregular que se pueda estar dando en algún servidor y permitirá determinar posibles programas dañinos, que puedan estar ocasionando estos comportamientos anormales.

4.5.10.5 Certificación externa de seguridad perimetral

El sistema de seguridad perimetral, deberá ser puesto a prueba por alguna entidad certificadora externa especializada en la detección de vulnerabilidades. Este proceso de certificación deberá apoyarse en un análisis de seguridad, llamado prueba de intrusión, el cual consiste en contratar los servicios profesionales de una compañía de seguridad con experiencia en el rompimiento de los sistemas de seguridad en Internet. El proceso deberá realizarse con una periodicidad semestral y permitirá poner a prueba las barreras y escudos de seguridad de la red contra ataques controlados, efectuados por un equipo con alta especialización en los conocimientos de *hackers* e intrusos de seguridad.

Los beneficios de efectuar este proceso serán: reducir el riesgo de violación de los sistemas de seguridad, implementación confiable de la estrategia de comercio electrónico planteada por la compañía comprendiendo claramente las amenazas potenciales, incrementar la disponibilidad y fiabilidad de aplicaciones e información crítica. La prueba de intrusión deberá cumplir con los siguientes requerimientos:

1. La compañía que efectúe la prueba deberá tener al menos cinco años de experiencia comprobada y de preferencia norteamericana.
2. La prueba deberá ser ejecutada por personal con alto grado de especialización en materia de seguridad perimetral.
3. La prueba deberá ser efectuada desde Internet y deberá incluir la evaluación controlada de los siguientes sistemas: ruteador, *firewall*, detector de intrusos, servidor *Web*, aplicación *Web*, sistema operativo.
4. La prueba deberá incluir el descubrimiento, explotación y análisis de las vulnerabilidades de la red perimetral.
5. La prueba deberá incluir las mismas herramientas y técnicas del momento que emplean los *hackers* profesionales.
6. El resultado de la prueba deberá incluir un reporte detallado de las debilidades, análisis de riesgos y métodos de corrección recomendados.
7. El servicio de evaluación deberá permitir la recurrencia cíclica de evaluar-corregir hasta llevar a un nivel aceptable de seguridad, en el que el riesgo de seguridad sea mínimo.
8. El personal de administración de seguridad perimetral, deberá corregir las debilidades encontradas en los sistemas, en el menor lapso de tiempo con el propósito de agilizar el proceso de evaluación-corrección.

4.5.11. Procedimientos de manejo de cuentas de acceso en sistemas perimetrales

Los procedimientos para el manejo de cuentas son importantes en la prevención de acceso inautorizado a los sistemas de la compañía. Las claves de acceso para administración de sistemas localizados en la zona perimetral deberán ser mantenidos con máxima seguridad y deberán cumplir con los siguientes requerimientos:

a. El *password* o contraseña no deberá ser menor a los diez caracteres.
b. La contraseña no deberá ser compuesta por el nombre de la cuenta de usuario, por los nombres propios del usuario o por el nombre de la esposa e hijos y cualquier otra información que sea fácilmente adivinable.
c. La contraseña deberá ser fácilmente memorizable, para que no haya necesidad de almacenarlo.
d. Utilizar una contraseña que se pueda digitar rápidamente, de forma que no sea necesario ver el teclado.
e. La composición de la contraseña deberá ser de letras, números y caracteres especiales como símbolos de puntuación. Las contraseñas deberán cambiarse con una periodicidad de tres meses y podrá ser cambiada antes del tiempo predeterminado en caso sea comprometida.
f. Los accesos a los sistemas perimetrales, deberán ser exclusivamente manejados por personal de administración de seguridad de sistemas.
g. Evitar en lo posible colocar las claves de acceso en archivos almacenados en sistemas abiertos que tengan conexión a la red. Las claves de acceso no deberán ser almacenadas en sistemas que estén expuestos a amenaza directa.
h. Las claves de acceso no deberán ser almacenadas en archivos de texto *plano* que puedan ser fácilmente identificadas, sino, deberán ser

almacenadas en archivos encriptados con algoritmos de llaves asimétricas de al menos 2048 *bits*.

i. Las claves de acceso a sistemas nunca deberán ser utilizadas en protocolos de texto plano que no apliquen criptografía al proceso de autenticación. Para acceso de terminal en los sistemas deberá aplicarse protocolos como SSH (*Secure Shell*).
j. Bajo ningún motivo deberán ser compartidas las contraseñas con personal externo de la compañía, como: proveedores, socios de negocios, proveedores o clientes. Tampoco deberán ser compartidas a personal de otras áreas de la compañía.
k. Bajo ningún motivo se permitirá utilizar claves de acceso con contraseñas en blanco.
l. Cada clave de acceso es responsabilidad individual de cada administrador de seguridad.

4.5.12. Reforzamiento permanente de sistemas de la red perimetral

Es importante considerar el reforzamiento continuo de las barreras de seguridad, sistemas y aplicaciones con el propósito de garantizar la protección contra nuevas debilidades encontradas en la tecnología, configuración y políticas de seguridad.

La naturaleza de la seguridad es dinámica y cambiante, es decir, la seguridad empleada hace cinco, diez o veinte años ya es obsoleta. Esto significa que tanto los sistemas tecnológicos de protección como *firewalls*, ruteadores y sistemas de detección de intrusos deberán actualizarse regularmente. De la misma forma la configuración de sistemas nuevos y existentes deberá ir mejorando continuamente, ya que una débil configuración en un sistema perimetral podrá comprometer los recursos de toda la red interna.

El resultado del proceso de auditoría de seguridad de red perimetral también podrá indicar un reforzamiento a la seguridad de los sistemas perimetrales. El proceso de auditoría tendrá el papel de velar porque los sistemas de seguridad se encuentren libres de debilidades de seguridad y que puedan garantizar niveles de riesgo muy bajos. El proceso de reforzamiento de la seguridad será el complemento indispensable de la auditoría ya que permitirá corregir todos los problemas que la auditoría haya descubierto en la red.

4.5.13. Actualización de *software* en *firewall* y ruteadores de perímetro

El sistema operacional de *firewalls* y ruteadores de perímetro deberán ser actualizados regularmente con una periodicidad trimestral. Estos sistemas deberán estar suscritos a contratos de soporte de actualización del sistema operacional con el fin de tener cobertura a nuevas versiones. Por otro lado, el personal de administración de seguridad deberá estar suscrito a servicios de notificación de alertas de seguridad de cada fabricante de los equipos para estar al tanto de las nuevas vulnerabilidades que se descubran en los equipos. El personal de administración de seguridad deberá tomar inmediatamente la decisión de actualizar una versión de sistema operacional una vez de reciba alguna alerta de vulnerabilidad detectada.

4.5.14. Actualización de sistemas detectores de intrusos

Los sistemas de detección de intrusos realizan el proceso de identificación de tráfico malicioso, utilizando una base de datos de firmas de ataques. Esta base de datos de firmas de ataques deberá ser actualizada dos veces por semana, realizándose el proceso de actualización en forma

automática en horas inhábiles de trabajo. La actualización deberá realizarse dentro de un rango de tiempo aleatorio con un canal seguro de comunicación ya que será a través de medios públicos como Internet. El sistema de detección de intrusos deberá estar bajo un contrato de cobertura de actualización de la bases de datos de firmas para tener derecho a realizar la actualización en los periodos determinados. Así mismo, el sistema operacional que utilizarán los sistemas de detección de intrusos deberá estar bajo un contrato de cobertura de actualización de versiones del fabricante para garantizar acceso a nuevas versiones por alguna vulnerabilidad crítica que se detecte en los sistemas.

4.5.15. Actualización de sistemas operativos y motor de servicios *Web*

Los componentes de sistema operativo y motor de servicios *Web* deberán ser actualizados con regularidad para reducir el riesgo de explotación de vulnerabilidades descubiertas en los sistemas. La mayoría de amenazas de seguridad son realizadas al sistema operativo o servicios *Web* e incluye ataques tales como denegado de servicio, troyanos o virus que explotan vulnerabilidades detectadas en sistemas. Una vulnerabilidad explotada podrá permitir el acceso ilegal de un intruso a los recursos de la red, el control remoto del sistema operativo o la caída de los sistemas. Estos componentes de *software* deberán actualizarse, una vez el fabricante haya confirmado la vulnerabilidad y haya producido algún paquete de actualización o servicio para eliminar tales vulnerabilidades. También deberá implementarse un ambiente de pruebas, donde se instalen previamente los paquetes de actualización y se analice los efectos secundarios con el propósito de evitar caídas en los sistemas.

4.5.16. Configuración de seguridad en sistemas

Tal como se ha visto en los capítulos anteriores, la debilidad de configuración en sistemas perimetrales puede llegar a comprometer de forma muy directa la seguridad de los recursos de red. Aún teniendo un arsenal de servicios y sistemas de protección perimetral, no significa que le protección será efectiva, ya que tales sistemas y servicios deberán estar configurados apropiadamente, considerando la seguridad como un factor indispensable.

El personal de administración de seguridad de sistemas deberá actuar cuidadosamente con la configuración de sistemas tales como: motor de servicios *Web*, sistemas operativos, bases de datos, *firewalls*, ruteadores y sistemas de detección de intrusos. Se deberá tener especial cuidado cuando se realicen actividades como re-configuración de sistemas de protección, ya que un error involuntario podría ser fatal para el resguardo de los recursos de red.

La configuración de los sistemas perimetrales deberá ser respaldada con una periodicidad mensual y es recomendable que se encuentre almacenada en un equipo de las capas mas internas de la red.

Por otro lado, el proceso de auditoría también podrá indicar medidas de acción en contra de debilidades de configuración de sistemas, demandando a la administración de seguridad cambios o ajustes en la configuración de los sistemas. Previo a realizar cualquier cambio en la configuración de sistemas se recomienda hacer copias de respaldo de configuración para ser capaz de regresar a una versión anterior de la configuración en caso se presentaren problemas consecuentes.

4.6. Arquitectura de seguridad perimetral

Una vez definidos los aspectos de estrategia de negocio, requerimientos de seguridad y políticas de seguridad perimetral, se procederá a construir el modelo de servicios de protección perimetral, tales como autenticación, control de acceso, separación de servicios, confidencialidad e integridad con el propósito de reforzar las políticas de seguridad descritas previamente.

Se establecerá un modelo de protección perimetral que defina el diseño de la red perimetral e incluya sistemas tales como *firewall*, ruteadores, servidores *Web*, servidores DNS, sistema de detección de intrusos, herramientas de monitoreo y detección de vulnerabilidades, servidores de bases de datos, *switch* de aplicación, y algunos otros sistemas que garanticen el cumplimiento de las políticas de seguridad y permitan poner en marcha la estrategia comercial de la compañía. La arquitectura de seguridad perimetral estará compuesta de los siguientes aspectos:

4.6.1. Contención de redes

Uno de los aspectos más importes en la seguridad perimetral, es la separación de sistemas y servicios en distintos segmentos de red. Esta regla de diseño de seguridad perimetral evita que la corrupción de un sistema comprometa la seguridad de recursos más valiosos en la red.

Para poner en marcha esta regla se proseguirá a determinar los distintos segmentos de red necesarios para poner en marcha el plan de actualización tecnológica y comercio electrónico de la compañía. Para este fin, comenzaremos definiendo las distintas redes remotas con las que habrá comunicación desde la red central. La red central tendrá conexión de red con

Internet, socios, sucursales. Considerando las redes anteriores se puede determinar que los niveles de control, administración y políticas de seguridad serán distintos en estos segmentos, por lo que debe separarse en diferentes segmentos. La separación de segmentos será puesto en marcha por un sistema de *firewall* perimetral que garantice aislamiento y control de acceso entre cualquier segmento de red.

Como consecuencia de la contención, se crearán cinco segmentos con niveles de control, administración, y seguridad distintos. Estos segmentos serán: red interna, donde se encuentran los recurso más valiosos de la red corporativa, red socios que permite la comunicación con socios de negocio, red sucursales que permita el acceso de comunicación con redes de bodega y almacenadora, red DMZ, que contiene todos los servicios de acceso público, y red externa que permitirá la conexión con Internet.

Por otro lado, con el propósito de aislar los servicios y sistemas más comprometidos con los menos comprometidos y de mayor valor, se creará otro segmento de red tipo DMZ, donde se publicarán todos los servicios que serán accedidos a través de Internet. Dentro del sistema de nomenclatura de red, este segmento será llamado DMZ o red desmilitarizada.

4.6.2. Direccionamiento IP en segmentos de red

Para la identificación de los distintos segmentos de red a nivel del protocolo IP, se definirá el número de red exclusivo para cada segmento. Como regla de diseño en redes corporativas y privadas se utilizará el estándar RFC 1918 para definir la dirección IP para cada subred. La distribución de los números de subred IP corresponde a la clase B y se describe en la tabla IX.

Tabla IX. Direccionamiento IP para subredes

Núm.	Nombre de red	Dirección IP de subred	Máscara de subred
1	Interna	172.25.1.0	255.255.0.0
2	DMZ	172.26.1.0	255.255.0.0
3	Socios	172.27.1.0	255.255.0.0
4	Sucursales	172.28.1.0	255.255.0.0
5	Externa	IP Pública	Dependerá del rango de IPs públicas

4.6.3. Control de acceso

Tal como lo define la política de seguridad perimetral, deberá existir aislamiento entre los sistemas de los distintos segmentos descritos anteriormente. Para llevar a cabo esta implementación es necesario un mecanismo de control de acceso de sistemas de red, que permita la ejecución de políticas de seguridad para definir qué sistema tendrá acceso a qué servicio de un sistema en particular localizado en otro segmento.

El dispositivo de red que proveerá este servicio es el *firewall* perimetral y operará como un mediador entre los distintos segmentos de red, definidos previamente. El *firewall* permitirá esconder los recursos más valiosos de la red corporativa y a la misma vez permitirá acceder a servicios e información de sistemas entre segmentos para la ejecución de la estrategia de comercialización en Internet.

Para definir las reglas de control de acceso, que deberán estar configuradas en el *firewall* se utilizarán los identificadores de red tanto de origen como destino para identificar los objetos, y para determinar los servicios de red se utilizará el número de puerto del protocolo TCP y UDP. Según la política de

seguridad perimetral definida previamente se utilizarán los servicios de red definidos en la tabla X.

Tabla X. Servicios de red

Núm.	Servicio	Protocolo	Número de puerto
1	*Web*	TCP	80
2	Mail	TCP	25
3	*Web* seguro (SSL)	TCP	443
4	DNS – transferencia de zonas	TCP	53
5	DNS – consultas de nombres de dominio	UDP	53
6	Acceso a base de datos	TCP	Dependerá del motor de base de datos
7	FTP	TCP	21

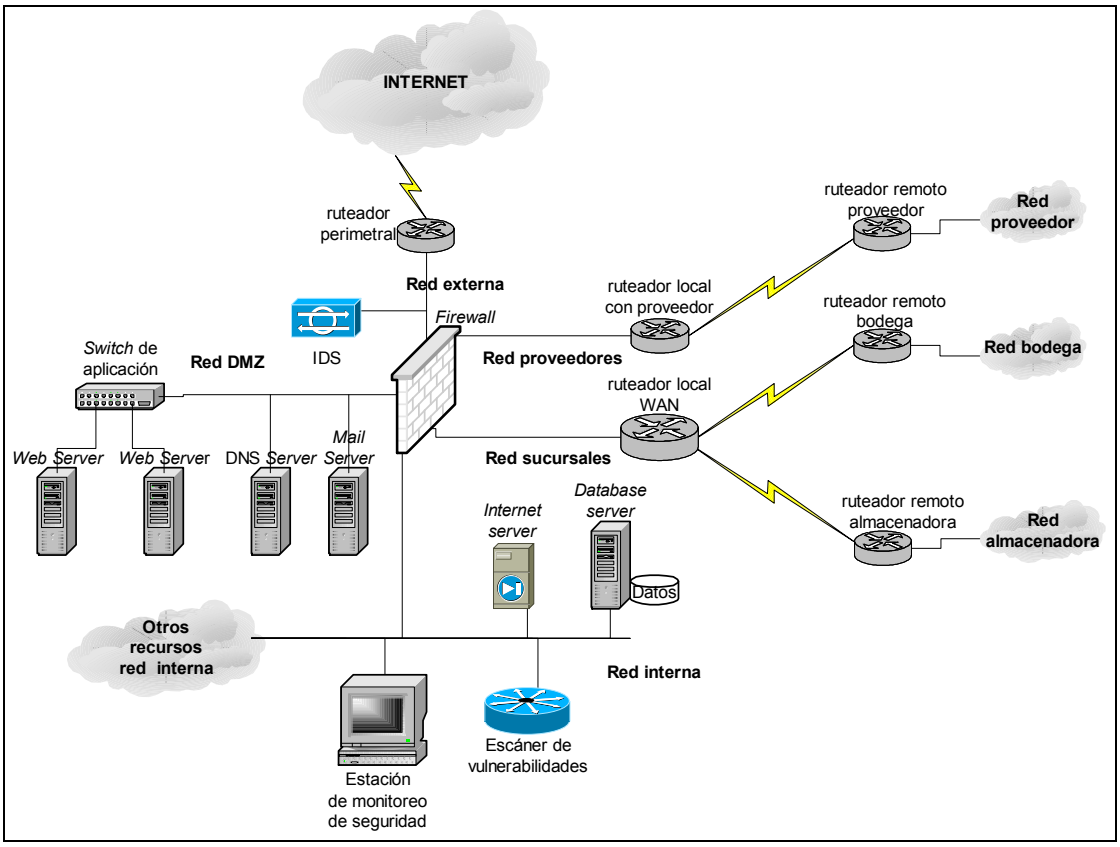
4.6.4. Diagrama de interconexión de red

La simbolización gráfica de los componentes de la red perimetral, es un reflejo de los aspectos de arquitectura de seguridad de red planteados previamente. El diagrama de red se enfoca principalmente en las zonas de perímetro y en los puntos de interconexión de la red privada a redes externas. Esta zona de perímetro define la línea divisoria entre las redes controladas y las no controladas, y por la misma razón es acá donde se concentra la seguridad de red perimetral. La figura 10 describe el diagrama de la red perimetral, compuesto por los cinco segmentos de red descritos con anterioridad.

Cada segmento de red, está interconectado físicamente por medio del *firewall* perimetral y contiene los dispositivos de red necesarios para la definición de la arquitectura de red planteada por la compañía. En la red

Interna es donde se concentran la mayoría de recursos, descritos en las tablas IV, V, VI y VII, y por consiguiente es la de mayor protección en la arquitectura de seguridad. Los servicios públicos han sido colocados en el segmento de la red DMZ con el propósito de no comprometer la integridad de los recursos de la red interna, en caso ocurra algún incidente en la red de acceso público.

FIGURA 10. Diagrama de red perimetral



4.7. Plan de manejo de incidentes de seguridad perimetral

La arquitectura de seguridad perimetral descrita anteriormente, define el modelo de servicios de red perimetral de Mimbres S.A., que reducirán el riesgo y limitarán el daño que intrusiones exitosas puedan causar. Sin embargo, ninguna arquitectura de seguridad puede eliminar completamente el riesgo y las intrusiones en la red. La compañía deberá estar preparada para manejo de riesgo a través de la implementación de un plan de manejo de incidentes. El estándar RFC 2196[11] establece responsabilidades y procedimientos en el manejo de incidentes para asegurar una rápida, efectiva y ordenada respuesta a incidentes de seguridad. Incidentes de seguridad pueden ocurrir en cualquier momento, pueden causar caídas de sistemas, daño, y pérdidas financieras considerables. Por estas razones la compañía describe a continuación un plan de manejo de incidentes basado en la política y arquitectura de seguridad perimetral.

4.7.1. Preparación y planificación

Los objetivos generales del manejo de incidentes se definen como:

a. Protección de los recursos que pueden ser comprometidos.
b. Prevenir el uso de los recursos de la compañía de ataques, en contra de otros sistemas.
c. Minimizar el potencial por exposición negativa.

Los objetivos específicos del manejo de incidentes se definen como:

[11] RFC 2196 es un estándar de diseño de políticas y procedimientos de seguridad informáticas para organizaciones con sistemas en Internet.

a. Comprender cómo ha ocurrido el incidente.
b. Encontrar cómo evitar una explotación futura de la misma vulnerabilidad.
c. Reducir el rango de impacto del incidente.
d. Evaluar el impacto y daño del incidente.
e. Recuperación del incidente.
f. Actualización y corrección de políticas de seguridad.
g. Encontrar el autor del incidente si es posible.

Prioridades de punto de arranque para el manejo de incidentes en la compañía compañía:

1. Proteger la vida humana y seguridad del personal.
2. Proteger datos sensibles, prevenir la explotación de sistemas de red sensibles que ocasionen pérdidas financieras a la compañía.
3. Prevenir daño a la funcionalidad de sistemas y alteración a archivos del sistema, daño a dispositivos de almacenamiento.
4. Minimizar la interrupción de servicios y procesos.

4.7.2. Notificación y puntos de contacto

Con el propósito de establecer los contactos del personal interno y externo que deberá ser notificado antes de que ocurra un incidente real, se definen los siguientes puntos de contacto (PDC):

1. Operador local
2. Administrador de sistema
3. Administrador de seguridad
4. Administrador financiero
5. Consultor externo de seguridad

6. Agencia especializada de servicios de soporte

Deberá establecerse una lista de contactos que incluya nombre, número telefónico móvil, número telefónico de trabajo, número telefónico de vivienda, correo electrónico. La notificación de un posible incidente debe realizarse confidencialmente con el propósito de evitar un ambiente de pánico en la organización y entidades externas.

4.7.3. Personal de manejo local

Deberá definirse un responsable del rol de PDC perteneciente a la unidad de administración de seguridad informática con experiencia técnica para coordinar los esfuerzos de los administradores de sistema y usuarios envueltos en el monitoreo y reacción ante un ataque. El PDC coordinará las actividades de todas las partes envueltas en el manejo del incidente. Deberá tener la función de contactar agencias externas que puedan proporcionar apoyo técnico y legal en caso sea necesario.

4.7.4. Agencias de investigación y legales

Será importante mantener una estrecha relación con una agencia investigación de seguridad privada con el propósito de llevar a cabo todos aquellos incidentes que tengan consecuencias legales. Si el incidente llega a afectar directamente a terceros, incluyendo clientes, proveedores y socios de negocio, se deberá notificar a través de la agencia de investigación de seguridad el incidente ocurrido con el propósito de llegar a un acuerdo sobre los daños. El incidente no deberá notificarse abiertamente al público en general, ya que afectará negativamente la imagen de la corporación. Para la compañía es

más importante mantener la disponibilidad de los servicios y reputación externa que la colaboración con actividades de investigación criminales con agencias de seguridad gubernamentales para llegar a dar con autores del hecho.

4.7.5. Comunicación interna

Mientras ocurra un incidente, deberá manejarse con sensibilidad la información que se les proporcione a los usuarios y departamentos de la compañía. Se deberá tener precaución ya que si se proporciona toda la información a los empleados, estos, pueden replicar la información con clientes y socios indicando declaraciones como “el sistema está caído”, o, “el sistema fue atacado por un intruso y se están restableciendo los servicios”. A los empleados internos deberán darse declaraciones como “el sistema no está disponible y están bajo mantenimiento para un mejor servicio”.

4.7.6. Relaciones públicas

La gerencia financiera de la compañía, deberá decidir si conviene notificar al público en general sobre un incidente ocurrido. Si la gerencia decide proporcionar la noticia, esta, deberá darse en un lapso no menor de un mes después, y será dada a través del personal de relaciones públicas de la compañía a personal de medios escritos del diario oficial. La información que se proporcionará no deberá dar los detalles técnicos del incidente, tampoco fuentes posibles, o motivos del ataque. La información deberá ser mínima y en forma general.

4.8. Identificación de un incidente

4.8.1. Confirmación del incidente

Esta actividad define la identificación de un comportamiento anómalo en los sistemas y la confirmación de un incidente de seguridad. Deberán utilizarse las siguientes herramientas de monitoreo definidas previamente en las políticas de seguridad:

a. Detectores de intrusos perimetrales
b. Alertas y bitácoras de *firewall*, ruteador
c. Auditoría de eventos de bases de datos, sistemas operativos y servicios *Web*

Para reconocer efectivamente un incidente se dan a conocer algunos de los síntomas e indicaciones, en los cuales deberá poner especial atención y cuidado el personal de administración de sistemas y seguridad:

1. Caídas inesperadas del sistema.
2. Aparecimiento de nuevas cuentas de usuario.
3. Aparecimiento de nuevos archivos en el sistema.
4. Cambios en los parámetros de un archivo como fecha y longitud.
5. Intentos inautorizados de escrituras al sistema.
6. Desaparecimiento o modificación de datos.
7. Denegado de servicio que impida tener acceso al sistema.
8. Bajo rendimiento del sistema, tiempos de respuesta muy altos.
9. Recepción de alarmas audibles, mensajes cortos, mensajes de correo electrónico indicando violación de seguridad.
10. Pruebas de acceso al sistema sospechosas.
11. Inhabilidad de un usuario de acceder al sistema.

12. Tráfico excesivo en la red local o enlaces dedicados

4.8.2. Tipo y alcance del incidente

Deberá identificarse el tipo y rango de alcance del incidente, ya que permitirá efectivamente dirigir los esfuerzos y prioridades de respuesta. Para determinar el impacto y alcance se definen algunos criterios de evaluación:

1. ¿Es este un incidente multi-sitio?
2. ¿Hay muchas computadoras en el sitio afectadas por el incidente?
3. ¿Es sensible la información implicada?
4. ¿Cuál ha sido el punto de entrada del incidente? (red interna, *Internet*, red externa de la WAN, servicios *Web*, servicio *E-mail*)
5. ¿Cuál es el daño potencial del incidente?
6. ¿Cuál es el tiempo estimado para cerrar el incidente?
7. ¿Qué recursos podrán ser requeridos para manejo del incidente?
8. ¿Estará envuelta la prensa?
9. ¿Estarán envueltas agencias gubernamentales?

4.8.3. Evaluación del daño y extensión del incidente

Tan rápido como la brecha de seguridad haya ocurrido, todo el sistema y componentes deberán ser considerados sospechosos. Es importante notar que la preparación previa en los sistemas es esencial para determinar los daños ocurridos. En sistemas de *software* deberán efectuarse análisis de comparación de archivos del sistema con medias originales, o *backups* efectuados con anterioridad al incidente. Se deberá revisar comportamientos anormales en los sistemas centralizados de bitácoras que permitan determinar los sistemas

implicados y la duración del incidente. Se verificará los registros de accesos observando minuciosamente patrones que permitan encontrar en que momento ocurrió el problema.

4.9. Manejo del incidente

4.9.1. Tipos de notificación e intercambio de información

Una vez se haya confirmado el incidente deberá notificarse al personal correspondiente. La situación deberá ser descrita con mucho detalle para ayudar a comprender rápidamente el problema. La información técnica del problema deberá ser descrita únicamente y exclusivamente al personal con responsabilidades del manejo de incidentes evitando que salga al exterior de la compañía. Toda notificación deberá ser explícita utilizando llamadas telefónicas o mensajes de correo electrónico en forma clara, concisa, y precisa. No deberá esconderse ni pasar por alto detalles que entorpezcan la solución al incidente. Importante mantener la calma en la comunicación de mensajes escritos y orales.

4.9.2. Protección de evidencia

Todos los detalles de acciones llevas a cabo durante el incidente e información relevante deberán ser documentadas para uso posterior. Independientemente si se llegue a efectuar la investigación legal del hecho, se deberá recopilar lo siguiente:

a. Todos los registros de eventos de sistemas.
b. Todas las acciones tomadas durante el incidente.

c. Registro de conversaciones externas durante el incidente.

La información recopilada deberá ser almacenada en un lugar seguro para garantizar la integridad y confidencialidad.

4.9.3. Contención

El propósito de la contención es evitar la expansión del ataque. Para llevar a cabo lo anterior se podrán tomar medidas como:

a. Apagar el sistema.
b. Desconectar el sistema de la red.
c. Monitorear la actividad del sistema para obtener evidencia del intruso
d. Deshabilitar servicios.
e. Desconectar la conexión a Internet.

La acción que se tomará dependerá del nivel de impacto del ataque y los requerimientos de disponibilidad del sistema. Mientras los sistemas e información están bajo ataque, la integridad deberá tener mayor prioridad sobre la actividad de investigación de la fuente del ataque.

4.9.4. Erradicación

Una vez el incidente haya sido controlado será necesario efectuar la restauración de los sistemas implicados, siendo cuidadoso de recopilar toda la información que permita una posterior investigación. Las siguientes actividades podrán ser llevadas a cabo:

a. Restauración del sistema, formateando y reinstalado el sistema operativo.
b. Utilización de cintas de *backups* consistentes para restaurar datos.
c. Utilización de antivirus para eliminar archivos infectados.
d. Aplicación de parches si el incidente fue causado por alguna vulnerabilidad.

4.9.5. Recuperación

Una vez la causa del incidente haya sido erradicada, la fase de recuperación define el retorno del sistema a su estado normal. Los servicios deberán ser habilitados dependiendo del nivel de disponibilidad requerido para evitar en lo posible inconveniencias a los usuarios.

4.9.6. Análisis de los hechos

Una vez el sistema haya sido restaurado a un estado seguro será necesario continuar un proceso de monitoreo continuo de componentes que pudieran haber sido pasados por alto en el proceso de recuperación. Los administradores deberán certificar la seguridad del sistema apoyándose en herramientas de detección de vulnerabilidades definidas previamente en las políticas de seguridad y en buenas prácticas de administración.

El análisis posterior al incidente deberá dar respuestas como:

a. ¿Exactamente qué sucedió?
b. ¿En qué momento sucedió?
c. ¿Qué tan bien respondió el personal envuelto en el incidente?
d. ¿Qué tipo de información necesitó el personal con prontitud?

e. ¿Cómo pudieron haber obtenido lo antes posible la información?
f. ¿Qué deberá hacer diferente el personal la siguiente vez que ocurra?

Se escribirá un reporte detallado, que describa secuencialmente los eventos del incidente incluyendo:

a. Método utilizado para describir el incidente.
b. Procedimiento de corrección.
c. Procedimiento de monitoreo.
d. Un resumen de la lección aprendida.
e. Recomendación de medidas de seguridad.
f. Costos asociados con pérdida de *software*, archivos, datos, *hardware*
g. Costos de mano de obra para restauración de sistemas afectados.
h. Costos de contratación de servicios efectuados por agencias de seguridad externas.
i. Estimación monetaria total del año causado.

4.9.7. Cierre del incidente

Para cerrar el incidente deberán ser tomadas algunas acciones. Estas acciones permitirán determinar qué aspectos de seguridad mejorar y la manera de prevenir la ocurrencia de nuevos ataques:

a. Realizar un inventario de los recursos de sistemas afectados, examinando cuidadosamente la forma en que fueron afectados.
b. Revisión de las lecciones aprendidas por el incidente, para prevención posterior.
c. Análisis de riesgos tomando como marco de referencia el incidente.

d. Revisión y ajustes en políticas de seguridad y procedimientos establecidos por la compañía.

CONCLUSIONES

1. El riesgo de ataque en Internet en contra de las redes privadas, continúa siendo alto y con tendencia al crecimiento, por lo que es considerado obligatorio el empleo de tecnologías de protección perimetral.

2. La tendencia de los últimos cinco años, muestra que el denegado de servicio y vandalismo son los ataques más comunes en Internet, llevando consigo destrucción y daño a la integridad de los sistemas, y como consecuencia el deterioro de la imagen de las compañías y considerables pérdidas financieras.

3. El nuevo enfoque de la seguridad es más permisivo, ya que considera la apertura de accesos de la red hacia proveedores, clientes, socios de negocios y otros, sustituyendo el enfoque cerrado, donde solamente se proporciona accesos a empleados internos.

4. La protección de los recursos de las compañías demanda mayor esfuerzo, ya que la tendencia de modelos de red centralizados se ha desplazado a la distribución de los recursos como aplicaciones, datos, servidores y unidades de negocio en múltiples localidades.

5. La meta de la seguridad no se limita solamente a garantizar la protección de los recursos, sino a hacer posible que las compañías puedan llevar a cabo las estrategias de comercialización en Internet tomando ventaja de las nuevas oportunidades.

6. La arquitectura de Internet presenta debilidades de seguridad, ya que fue diseñada para facilitar la comunicación abierta entre sistemas.

7. La principal debilidad de seguridad no radica en la tecnología sino en la falta de aplicación de políticas de seguridad.

8. Las políticas de seguridad proveen un marco de trabajo general para la implementación de la seguridad de red, normando las conductas de directores, administradores, operadores y usuarios, y definiendo procedimientos, mecanismos y tecnologías que hagan posible los objetivos de las organizaciones.

9. La naturaleza de la seguridad es dinámica y cambiante, motivada por los avances en la investigación de nuevas amenazas tecnológicas, el desarrollo de herramientas de ataque sofisticadas y extensión del conocimiento especializado de redes.

10. Ningún sistema de protección por sí mismo define la arquitectura de seguridad para una red, más bien la arquitectura de seguridad representa un modelo de servicios de protección tecnológicos basados en la definición de las políticas de seguridad de la organización.

11. Las buenas herramientas no sustituyen las buenas prácticas de administración de seguridad.

RECOMENDACIONES

1. Establecer los objetivos de seguridad perimetral con base en los objetivos y requerimientos de negocio de la compañía, considerando las ventajas, oportunidades, amenazas, debilidades y recursos.

2. Aplicar mecanismos y tecnologías de seguridad perimetral en la apertura de la red privada a Internet y otras redes externas, permitiendo el aprovechamiento de las ventajas y oportunidades que ofrecen las tecnologías de comunicación.

3. Formar una unidad de seguridad de sistemas con la responsabilidad de establecer, educar y velar por el cumplimiento de las buenas prácticas de seguridad dentro de la organización.

4. Aplicar en todos los niveles de la organización un plan continuo de políticas de seguridad con la definición de procedimientos periódicos en áreas como auditoría de seguridad, monitoreo de sistemas y reestructuración de seguridad.

5. Implementar procedimientos periódicos de revisión y actualización de políticas de seguridad para garantizar un marco de trabajo de seguridad de sistemas adaptable al cambio.

6. Para el diseño de un esquema de protección perimetral se deberá emplear redes de perímetro con el propósito de limitar el alcance y expansión de un ataque externo.

7. Definir un plan de manejo de incidentes que describa las acciones, responsabilidades y medidas que deberán emplear los miembros de la organización, en caso de que se presente algún incidente de seguridad con el propósito de limitar la extensión del daño, reforzar las barreras de seguridad y prevenir ataques futuros.

BIBLIOGRAFÍA

1. **A Gauntlet *Firewall* Executive White Paper**, http://www.nai.com, 1999.

2. **A guide to Intrusión Detection Technology**, http://www.iss.net, 1998.

3. CISCO Systems, Inc. **Managing Cisco Network Security Student Guide**. Versión 1.0. Estados Unidos de Norte América: Cisco Systems, Inc.,1998.

4. CISCO Systems, Inc. **Security Technologies Document**. Estados Unidos de Norte América: Cisco Systems, Inc.,1999.

5. COMPUTER Security Institute. **2003 CSI/FBI Computer Crime and** Security **Survey**. Estados Unidos de Norte América: Computer Security Institute. 2003.

6. TANENBAUM, Andrew. **Redes de computadoras**. 3er. Ed. Tr. David Morales, México: Prentice hall Hispanoamérica, S.A., 1997. 840 páginas.

7. **DMZ: Isolation and Control**, http://www.infosecuritymag.com/feb2000/dmz.html, 2000

8. FRASER, Barbara. **Site Security Handbook**. RFC: 2196. Estados Unidos de Norte América: *Software* Engineering Institute Carnegie Mellon University, 1997.

9. **Implementación práctica de políticas de seguridad: La S.G.T.I. del** MEC, http://www.rediris.es/rediris/boletin/38/ponencia1.html, 2000.

10. **Mecanismos de Seguridad en Redes: *Firewalls* y Routers de** Selección, http://www.geocities.com/SiliconValley/Cable/3280/index.htm, 2000.

11. **Network Security Filters and *Firewalls*,** http://www.acm.org/crossroads/xrds2-1/security.html, 2000.

12. **Secure E-Business**, http://www.iss.net, 2003.

13. SOKOL, Marc S., **Security Architecture and Incident Management for** E-**business**. Estados Unidos de Norte América: Internet Security Systems, 2000.

14. **Stateful Inspection *Firewall* Technology**, http://www.checkpoint.com/products/technology/stateful1.html, 2000.