UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL PARA REDES CORPORATIVAS

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

ALDO ERIK ROMERO TORRES

PROMOCIÓN
1992 - I

LIMA – PERÚ
2006

INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL PARA REDES CORPORATIVAS

A mis padres Alicia y Valeriano por todo su apoyo en los años de estudios en la universidad, sin ellos nunca hubiera podido culminar mis estudios, a mi esposa Giannina por su paciencia y apoyo en esta etapa de la titulación y sobre todo a Dios por los dones derramados en mi vida.

SUMARIO

El presente informe de suficiencia profesional abarca las características de diseño e implementación de una red de comunicaciones de datos perimetral para una corporación considerando la seguridad como factor de primer orden. Se parte de las definiciones de seguridad y comunicaciones que tienen hoy en día las corporaciones, las cuales son básicamente mayores que las empresas de otra envergadura. Una vez establecidas estas necesidades y requerimientos se describe el proceso de diseño de la red de datos perimetral, mencionando la base teórica y estableciendo etapas de implementación, se describen cuales son los servicios disponibles, las consideraciones de seguridad necesarias, así como los equipos y topología de la red en cada una de las etapas. Finalmente y una vez que se tiene montada la red diseñada originalmente se establecen los pautas y procesos que se deben tomar en cuenta para el mantenimiento y actualización de la red de datos perimetral.

INDICE

PROLOGO

En este trabajo se muestran las consideraciones y etapas de diseño de una red de comunicaciones de datos perimetral que tiene la seguridad como un elemento importante. Se ha escogido este tema por considerarse que cada día la seguridad de la información cobra mayor importancia dentro de los parámetros a tomar en cuenta cuando se realiza el diseño y puesta en funcionamiento de cualquier sistema de comunicaciones. El foco es un entorno de gran empresa debido principalmente a que estas son justamente las que mayor relevancia le dan actualmente al tema de seguridad, tanto por los niveles de confidencialidad, disponibilidad e integridad de la información que requieren para su operación normal, como por los aún altos niveles de inversión que se requieren para montar una infraestructura de este tipo. Sin embargo, muchos de los puntos tocados pueden ser fácilmente adaptados a un entorno más pequeño ó reducido, efectuando el correspondiente análisis de riesgos. El presente trabajo se basa principalmente en la experiencia del autor en el diseño e implementación de la red perimetral de datos de TIM PERU y anteriormente como consultor interno para la Corporación CREDICORP. El caso práctico escogido es justamente el primero debido a que es más reciente y aún se encuentra en proceso de evolución. El alcance abarca desde la fijación de los conceptos de comunicaciones, y seguridad necesarios para comprender adecuadamente el presente trabajo y la presentación de las diversas etapas por las que pasó la red de datos desde el inicio de operaciones de la empresa en el año 2000 hasta fines del año 2005, así como las consideraciones necesarias para lograr mantener en niveles óptimos la seguridad de la misma en la operación diaria.

Capítulo I.- Definición de las necesidades de comunicación y seguridad de una corporación.- Se fija el marco general bajo el cual se va a desarrollar el presente trabajo indicando las necesidades de una corporación en materia de comunicaciones e integración con el mundo externo, los riesgos existentes y la medidas de seguridad que es necesario tomar para resguardar la información.

Capítulo II.- Conceptos de Seguridad.- Se definen los principales conceptos de seguridad de la información relacionadas con las redes de comunicaciones, estos son necesarios para fijar y entender los procesos posteriores.

Capítulo III.- Conceptos de Tecnología y Comunicaciones.- Se definen brevemente los principales conceptos de tecnología de cómputo y de comunicaciones asociados a las redes de datos.

Capítulo IV.- Conceptos de Data Networking y Seguridad de Comunicaciones.- Se definen los principales conceptos de data networking, principalmente los elementos de comunicaciones y los protocolos; ya que es necesario tener un conocimiento cabal de ellos para efectuar análisis de seguridad riguroso. Asimismo se definen los principales conceptos de seguridad en las comunicaciones.

Capítulo V.- Consideraciones y etapas de implementación de la red de seguridad perimetral. En este capítulo se describen las diversas etapas que conforman la evolución de la red de datos perimetral de una corporación. Para el caso práctico se ha tomado como ejemplo a TIM PERU, desde sus inicios en el año 2000 hasta fines del año 2005.

Capítulo VI.- Interacción de la red de seguridad perimetral con los sistemas y aplicaciones corporativas que se sostienen en ellas.- En este capítulo se describen las políticas, estándares, procedimientos y líneas base para los sistemas y aplicativos que son soportados por la red de seguridad perimetral, es necesario tener todo esto claramente especificado puesto que la red de datos se complementa con una arquitectura de aplicaciones adecuada para utilizar adecuadamente las facilidades de seguridad y confiabilidad que brinda.

Capítulo VII.- Consideraciones de mantenimiento y actualización de la red de seguridad perimetral.-Se describen los principales procesos se requieren para mantener óptimos niveles de seguridad en la red de seguridad perimétrica.

Observaciones y conclusiones.- Mencionamos los aspectos que es necesario tomar en cuenta para lograr niveles adecuados de seguridad en una red de datos perimetral y como algunos procesos internos de la propia empresa pueden afectar el trabajo netamente de ingeniería que es necesario realizar.

CAPÍTULO I
DEFINICIÓN DE LAS NECESIDADES DE COMUNICACIÓN Y SEGURIDAD DE UNA CORPORACIÓN

1.1.- Situación actual de las redes de comunicaciones.-

En los últimos 20 años y más recientemente en los últimos 10 años hemos visto el crecimiento explosivo de las tecnologías de las redes de computadoras y las comunicaciones en general, pasando de las primeros sistemas Mainframe con arquitectura SNA y las redes token ring a las redes masivas actuales y la Internet; así como del tradicional sistema de telefonía fija a las redes celulares e inalámbricas de transmisión de datos. Estos cambios significativos producidos desde los años 90 con mayor auge, han cambiado prácticamente todo nuestro modo de comunicarnos, de cómo percibimos la comunicación y de las necesidades de comunicación en sí; no solo de nosotros como individuos sino sobre todo de las empresas de toda envergadura, desde las grandes corporaciones , los organismos estatales hasta los pymes y micro empresas, todos en el mundo actual globalizado necesitamos estar comunicados, " conectados" más directamente y en tiempo real.

Estos cambios vertiginosos no solo han traído beneficios a la humanidad en general, sino que también nos han planteado retos, problemas que antes no existían, han requerido de la especialización de los ingenieros, del nacimiento de nuevas profesiones, pero también de la aparición de riesgos nuevos que pueden alterar el funcionamiento de nuestros sistemas de comunicación, de nuestro "establishment" actual. Estos riesgos no solo son producto de la tecnología y la complejidad de la misma, sino que también nacen del mal uso de toda esta nueva tecnología, es así como hemos visto aparecer en los últimos años términos nuevos en nuestro vocabulario, términos para los cuales nuestra lengua española aún no estaba preparada y que han pasado directamente del inglés a nuestro vocabulario, palabras como "hacker", "back up", "phishing", "spoofing", ya se han hecho de uso cotidiano para nosotros.

Es así que con la necesidad que tienen actualmente las empresas de todo tipo y en especial las corporaciones de hacer uso de todas estas facilidades de comunicación que nos brinda la tecnología, nace también la necesidad de protegerse adecuadamente de estos riesgos , apareciendo así los primeros profesionales dedicados a analizar las redes y determinar los niveles adecuados de seguridad, dando poco a poco surgimiento a una nueva especialidad, Seguridad de Información, que si bien engloba dentro de su área de influencia muchos aspectos, tiene como uno de sus pilares el velar por la Seguridad de las telecomunicaciones y redes de datos.

1.2.- Seguridad de redes y Telecomunicaciones.-

Este punto de la ingeniería de redes incluye los siguientes aspectos:

- La Seguridad de la voz, datos, multimedia, y transmisiones de fax en términos de área local (LAN), área extendida (WAN), Internet y acceso remoto.
- Las técnicas necesarias para prevenir, detectar y corregir errores para mantener adecuadamente la integridad, disponibilidad e confidencialidad de la información transmitida a través de las redes de comunicaciones.
- Internet/ Intranet/Extranet en términos de firewalls, routers, gateways y los diversos protocolos de comunicación que se utilizan.
- La correcta gestión de seguridad para lograr los puntos anteriores.

Este dominio de la Seguridad de la Información, incluye las estructuras, métodos de transmisión, formatos de transporte, y medidas de seguridad que son necesarias para proveer integridad, disponibilidad, autenticación, y confidencialidad de la información que es transmitida sobre redes de datos de toda naturaleza, también las medidas de prevención y detección del mal uso ó abuso de los sistemas de comunicaciones.

1.3.- Necesidades de Comunicación y Seguridad de una Corporación

En el mundo actual las telecomunicaciones tienen un papel relevante en todas las áreas de la actividad humana, en los últimos años hemos vivido un cambio radical en nuestra percepción y forma de comunicarnos, tanto a nivel personal como en las empresas. Sino recordemos la ya lejana década de los 80 cuando en nuestro país el acceder a un teléfono era un privilegio de pocos, y era lo principal para que una empresa de tamaño mediano ó corporación pudiese entrar a operar. Las comunicaciones dentro de las empresas se daban a través de anexos y la documentación entre las áreas a través de impresos, los ya recordados memorandums, oficios, ó cartas, ni que decir de las comunicaciones entre empresas, el mensajero era un factor primordial de comunicación. Hoy la situación a cambiado radicalmente, toda empresa necesita para su eficaz

desenvolvimiento tener un buen esquema de comunicaciones tanto al interior como al exterior de la empresa, quizás ya muchos no podamos concebir como era la comunicación sin el e-mail, el acceso a Internet, la interconexión en tiempo real entre las filiales de las empresas ó con empresas proveedoras ó partners, hasta llegar al comercio electrónico. Tanto ha variado este esquema que han surgido nuevos paradigmas comerciales, nuevas formas de enfocar las relaciones empresariales.

1.4.- Necesidades de comunicación de una corporación

El enfoque de estas necesidades de comunicación está circunscrito al ámbito de las comunicaciones al externo de la empresa ya que es en este medio que se crea o define la infraestructura de seguridad perimetral. Dentro de este alcance y partiendo de lo básico a lo complejo tenemos:

- Correo electrónico externo
- Presencia en el World Wide Web, partiendo de la elemental página web, hasta la más compleja de servicios a los clientes y proveedores, comercio electrónico, servicios de valor agregado y otros.
- Acceso desde la empresa a Internet para la búsqueda de información ó contactos con otras empresas.
- Transferencia de información básica con otras empresas ó filiales.
- Acceso a servicios que ofrecen otras empresas ó el estado.
- Interconexión con oficinas remotas de la misma empresa en el ámbito nacional ó internacional.
- Interconexión con empresas socias ó proveedores (Extranet)
- Acceso remoto a los sistemas internos de la empresa para fines de soporte ó Home working.

1.5.- Identificación de riesgos en las comunicaciones

Como habíamos indicado anteriormente, las necesidades actuales de comunicación de una corporación, han traído consigo que se incremente notablemente los riesgos que tienen que enfrentar, y por consiguiente tomar las medidas adecuadas para disminuirlo a niveles aceptables tomando siempre en consideración el análisis costo-beneficio. Todo establecimiento de las medidas de seguridad de un sistema, aplicación, proceso, ó disciplina necesariamente empieza por efectuar un análisis de riesgos profesional que tiene que pasar por las siguientes etapas:

- Clasificación de la información
- Establecimiento de una Infraestructura de Seguridad de la Información

  - Definición de roles y responsabilidades
  - Definición de Políticas, estándares, líneas de guía y procedimientos
- Gestión y análisis de los riesgos
  - Principios del análisis de riesgos
  - Términos y definiciones
  - Tipos
  - Pasos a seguir
- Análisis costo beneficio. Para determinar efectivamente la viabilidad de las medidas de seguridad a implementar.

Una vez realizado este análisis recién se pueden proponer alternativas y opciones diversas que respondan a las necesidades y estén dentro de las expectativas económicas de las empresas.

1.6.- Principales Riesgos

En general los principales riesgos que enfrentan las empresas en sus necesidades de comunicación son las siguientes:

Infección de virus, gusanos y troyanos

Alteración de la información contenida en los servicios web que se dan a los clientes y proveedores

Denegación de los servicios que se brindan a los clientes y proveedores

Pérdida de privacidad de la información que se intercambia con proveedores y clientes.

Pérdida ó robo de información importante para la empresa.

Accesos no autorizados a la red de la empresa ó a los servicios web en general.

Pérdida de información personal de los usuarios de los servicios de comunicación de la empresa.

Mal uso ó uso deshonesto por parte de los usuarios de los servicios de comunicaciones que les brinda la empresa.

1.7.- Necesidades de Seguridad de una empresa

En general las necesidades de seguridad de una empresa van a variar mucho; no hay algún estándar para eso, dependen básicamente de la orientación de la empresa, del rubro de la empresa. No son por ejemplo, iguales las necesidades de un banco que las de una empresa de servicios estatal, ni las de una empresa de servicios postales a las de una netamente e-commerce. Vamos a describir cuales serían las principales necesidades

de seguridad, no se pone un orden de preferencia, el cual puede variar dependiendo del análisis de riesgos:

Prevención de infecciones de virus, gusanos y troyanos.

Prevención y detección de accesos no autorizados a los servicios web que brinda la empresa

Disponibilidad de los servicios web y de comunicación que brinda la empresa

Confidencialidad de la información

Integridad de la información

Evitar el mal uso por parte de los usuarios internos de los servicios de comunicación que brinda la empresa.

Resumen del Capítulo

En este capítulo se han descrito las principales características de una red de comunicaciones de datos de una corporación, no desde el punto de vista técnico sino funcional. Las necesidades de hoy en día, los riesgos que estas necesidades de comunicación conllevan y las medidas de seguridad que son necesarias para garantizar la confiabilidad, disponibilidad y confidencialidad de la información que es por hoy el activo más importante de una empresa.

CAPÍTULO II
CONCEPTOS DE SEGURIDAD

Para el inicio del diseño de la infraestructura de seguridad corporativa es necesario definir adecuadamente los elementos involucrados, tanto elementos físicos (dispositivos y enlaces) como los conceptos necesarios para crear nuestra estructura de seguridad.

Conceptos de Seguridad:

2.1.- Confidencialidad.- Es la prevención de la exposición intencional ó no intencional sin autorización de la información. Es decir la información solo debe ser conocida ó recibida por las personas autorizadas a hacerlo. Algunos de los elementos de comunicaciones utilizados para garantizar la confidencialidad son

- Protocolos de seguridad de redes
- Servicios de autenticación
- Servicios de encripción.

2.2.- Integridad.- Es la garantía que la información recibida es la misma información enviada, que la información no ha sido intencional ó no intencionalmente alterada. La pérdida de integridad puede ocurrir, a través de un ataque intencional para cambiarla (por ejemplo un web site hacking) ó más comúnmente es alterada accidentalmente por algún usuario u operador de la información. La Integridad también contiene el concepto de "No repudiación". Algunos de los elementos de comunicaciones utilizados para garantizar la integridad son:

- Firewalls
- Gestión de la seguridad de las comunicaciones
- Servicios de detección de intrusos

2.3.- Disponibilidad.- Este concepto se refiere a los elementos que crean confiabilidad y estabilidad en las redes y sistemas, lo cual asegura que la conectividad esta accesible cuando se necesite, permitiendo a los usuarios autorizados el acceso a las redes ó sistemas. También garantiza que los servicios y elementos de seguridad estén

disponibles. El concepto de disponibilidad también incluye elementos de otras áreas de Tecnología que muchas veces no son considerados como propiamente de seguridad, tales como garantía del servicio, performance y up –time. Algunos de los elementos de comunicaciones utilizados para garantizar la disponibilidad son:

- Tolerancia a fallas y disponibilidad de la información. Respaldos y sistemas redundantes.
- Registro de accesos y performance de los procesos.
- Procesos de seguridad confiables y mecanismos de seguridad de red.

2.4.- Autorización.- Son los privilegios concedidos a una persona ó a un proceso y que hacen posible el acceso a los recursos de información. Una vez que el usuario ha sido identificado y autenticado, los niveles de autorización determinan la extensión de los derechos concedidos.

2.5.- Auditabilidad.- Se define como la capacidad de un sistema de registrar las acciones y comportamiento individuales de un usuario ó proceso del sistema. Los registros de auditoria y los logs del sistema soportan la auditabilidad.

2.6.- Privacidad.- Es el nivel de confidencialidad y seguridad que un sistema brinda a la información de sus usuarios. Es a menudo un componente importante en el diseño de los controles de seguridad. La privacidad no solo garantiza una adecuada confidencialidad a la información de la empresa sino que también garantiza niveles de privacidad a la información de acuerdo a su importancia.

2.7.- Acceso Remoto.- Es una tecnología que esta enfocada en proveer que un usuario remoto (es decir no ubicado físicamente en el entorno de red) pueda acceder a los recursos y a la red misma pero manteniendo adecuadamente los principios de confidencialidad, disponibilidad e integridad.

El usar esta tecnología nos da muchas ventajas entre las que tenemos:

- Reducir los costos de conexión (networking) al utilizar las facilidades de Internet en reemplazo de los enlaces dedicados.
- Proveer a los empleados la facilidad del teletrabajo.
- Comunicación rápida y efectiva con los clientes, y proveedores.

2.8.- Detección de Intrusos.- (Intrusión Detection Systems- IDS) Son sistemas utilizados para monitorear el tráfico en la red ó para monitorear los registros de auditoria

para poder determinar la existencia de violaciones a las políticas de seguridad de la empresa. Un sistema IDS puede detectar intrusiones que puedan pasar el primer nivel de seguridad del firewall ó que puedan ocurrir dentro de la red interna. Un sistema realmente efectivo de IDS puede detectar ataques comunes en el momento en el que están ocurriendo. La evolución de esta tecnología ha dado origen a los nuevos sistemas de IPS (Intrusión Prevention Systems) ó Sistemas de Prevención de Intrusión. De acuerdo a la forma en que trabajan se pueden dividir en las siguientes categorías:

a) Sistemas de red.- Es un sistema ubicado ya sea en forma paralela ó en serie con la red de comunicaciones de datos y monitorea en tiempo real el tráfico de la red, para ser realmente efectivo no debe consumir recursos de la red. Revisa los paquetes y las cabeceras de los paquetes, por lo que puede detectar ataques de denegación de servicios. Asimismo como esta monitoreando en tiempo real, puede responder al ataque tomando determinadas acciones programadas, tales como el bloqueo de determinados tipos de paquetes ó de determinadas direcciones IP. Su principal desventaja es que no puede detectar un ataque contra un host si un usuario esta efectivamente ya identificado y autorizado en el mismo.

b) Sistemas de host.- Este tipo de sistemas residen en los host y mediante el análisis de los registros de auditoria pueden detectar un ataque ó determinar si el ataque fue exitoso, y también generar respuestas para minimizar el ataque. Estos sistemas tienen menor capacidad de detección de eventos y están limitados muchas veces por las capacidades de registro de eventos de los sistemas en sí.

c) Sistemas basados en firmas.- Son sistemas que guardan una base de datos de los eventos considerados riesgosos, cuando la data pasa a través de ellos, lo analizan y comparar con lo que tienen registrado y de hallar igualdad proceden de acuerdo a las instrucciones programadas. Su principal desventaja es que solo detectan patrones que tienen registrados por lo que tienen que ser constantemente actualizados.

d) Sistemas basados en el comportamiento.- Con este método, los sistemas adquieren data y definen un perfil "normal" para la red ó el host que están protegiendo. Lo complicado justamente reside en programar este perfil normal, el cual debe ser realizado tomando en cuenta las variaciones normales de carga de trabajo por día y hora u otros factores. Con esta información los ataques pueden ser detectados si producen eventos que no corresponde al perfil "normal" ó si

exceden cierto umbral; su principal desventaja es que no van a detectar eventos que no cambien las características de operación del sistema, ó pueden dar falsos si se presentan cargas de trabajo fuera de lo usual.

2.9.- Equipo de Respuesta rápida a incidentes.- Debe ser considerado una parte importante de un sistema de Detección y respuesta, es básicamente tener identificado al personal y las funciones que realizan para poder superar rápidamente un incidente, abarca la coordinación de la notificación y distribución de la información pertinente a los niveles apropiados y con tiempos de escalamiento adecuados. También el mitigar el riesgo para la empresa minimizando los problemas ó cortes de los servicios afectados mientras se recuperan los mismos.

2.10.- Disponibilidad de la red: Se puede definir como la capacidad de una red de comunicaciones de datos de brindar confianza a sus usuarios, de estar siempre disponible para que los usuarios puedan acceder a los recursos de información de una empresa, como una red corporativa es de por si bastante compleja, el concepto de disponibilidad engloba diversos sistemas ó grupos de dispositivos que contienen una red de datos. Nosotros vamos a examinar los siguientes:

2.10.1.-Arreglos de discos.- Proveen disponibilidad a la red al facilitar que la información almacenada en ellos (generalmente bases de datos ó información no estructurada) este siempre disponible; previniendo de una posible falla física ó lógica en los dispositivos de almacenamiento. Dentro de los estándares de dispositivos de almacenamiento de datos que proveen disponibilidad tenemos el RAID (Siglas en inglés de Arreglo redundante de discos normales – Redundant Array of Inexpensive Disks). Su propósito principal es brindar tolerancia a fallas, especialmente a fallas físicas en los discos. Algunas categorías de arreglos RAID mejoran el rendimiento del sistema con el uso de "disk cache" ó la lectura distribuida en los discos que trabajan simultáneamente en la grabación de la data. Básicamente, RAID separa la data en múltiples unidades y la guarda en múltiples discos usando un proceso denominado "striping". Esto puede ser implementado mediante una solución de hardware ó software. Se han definido tres tipos de arreglos RAID: Sistema de discos resistentes a fallas (FRDS); Sistemas de discos tolerantes a fallas y Sistemas de discos tolerantes a desastres. Pero solo el FRDS es un estandar existente y en uso, los otros están aún pendientes. Vamos ahora a describir la implementación de los niveles de FRDS.

a) Sistemas de Discos Resistentes a Fallas (FRDS Failure Resistent Disk System) Tienen como función básica proveer a los servidores de archivos ó bases de datos de la pérdida de los datos ó de la disponibilidad de los mismos por causa de una falla en el disco. Tienen la capacidad de reconstruir el contenido de un disco que presenta fallas en otro que lo reemplaza, brindando adicionalmente protección contra la pérdida de los datos a consecuencia de fallas de hardware en los servidores. Una característica especial de los sistemas FRDS es que tienen la capacidad de monitorear continuamente los posibles puntos de falla y alertar ante cualquier falla. [1]

b) FDRS Plus.- Es una versión mejorada de la anterior. Adicionalmente tiene la capacidad de hacer automáticamente un **hot swap** (reconstruir dinámicamente la data de un disco con falla en otro, mientras el sistema continúa operando normalmente). Monitorea además determinados parámetros ambientales que pueden afectar a los dispositivos magnéticos de almacenamiento (temperatura, rangos de voltaje) y da señales de alerta ante posibles fallas ó variaciones de estos parámetros.

c) Niveles de arreglos tipo RAID

Raid Nivel 0.- Crea un solo gran disco usando varios discos. Este proceso es llamado "striping". Divide y graba la información en todos los discos (por lo tanto no provee redundancia) utilizando toda la capacidad disponible en los discos para crear un solo gran disco virtual incrementando la perfomance de lectura/ escritura al efectuarlo en forma paralela. Un problema que tiene es que la falla de una sola de las unidades de disco que lo conforman afecta a todo el sistema.

Raid Nivel 1.- Es comúnmente denominado de "mirroring" (espejo) debido a que refleja la data de un disco en un set de discos duplicando físicamente la data. Normalmente es utilizado en un arreglo de 1 a 1, es decir la data de un disco es "espejada" en otro, si uno falla el sistema automáticamente consigue la data del disco "espejo". La principal desventaja de este sistema es que es caro, resultado del costo de duplicar

la capacidad real del sistema. Es muy usado para sistema con información crítica en cuanto a su integridad y disponibilidad.

Raid Nivel 2.- Consiste en disgregar la información y guardarla en varios discos (bit-interleaved). Se crea un bit de paridad de información a partir de la data original, este bit de paridad es almacenado en un disco aparte y mediante algoritmos que detectan los errores al momento de leer la data se puede detectar si alguna parte (algún disco del arreglo) presenta fallas. Normalmente define un sistema con 39 discos, 32 discos de data y 7 de bits de recuperación de errores. Este nivel no es utilizado actualmente porque fue rápidamente desplazado por los siguientes niveles de arreglos RAID.

Raid Niveles 3 y 4.- Los estamos considerando juntos debido a que funcionan de la misma manera. La única diferencia que tienen es que el nivel 3 es implementado a un nivel de byte y el nivel 4 a un nivel de bloques de bytes. En este escenario la data es dividida y guardada en múltiples discos y el bit de paridad es guardado en un disco de paridad, tiene las ventajas de la lectura y escritura en paralelo del RAID 0, igualmente crea grandes discos virtuales, pero con la adición de un disco de paridad que provee la redundancia. Si un disco falla, la data puede ser reconstruida usando el bit de paridad. La principal desventaja de este nivel es que la constante escritura del bit de paridad puede disminuir la performance del sistema. En las implementaciones se suelen consideran discos de backups que en línea pueden reemplazar a cualquier disco que presente fallas. [1]

Raid Nivel 5.- Guarda la información y los bits de paridad a nivel de bloques en todos los discos del arreglo. Es similar a RAID 3 y RAID 4, excepto que la información de paridad es guardada en el siguiente disco disponible en lugar de en un disco especialmente dedicado a esa función, esto hace posible tener mayor flexibilidad en la implementación e incrementa la tolerancia a fallas al no tener un punto de falla crítico. El sistema lee y escribe los discos en forma paralela incrementando la performance. Los discos de reemplazo para los discos que presentan fallas normalmente tienen la capacidad de ser habilitados “en caliente” es decir

con el sistema corriendo. Esta es probablemente la implementación más popular de los arreglos RAID.

Raid Nivel 7.- Es una variación del nivel 5 que tiene la capacidad de trabajar sobre el arreglo de discos como si se tratara de un solo disco. A menudo se simula mediante software sobre un arreglo físico de RAID 5. Esto hace posible que el arreglo de discos continúe operando si cualquier disco ó path de cualquier disco falla.

Existen otras implementaciones RAID propias de los diversos proveedores que combinan características de los niveles presentados, pero no están oficialmente definidos. Por ejemplo el nivel 10 es una combinación del nivel 0 (striping) con el nivel 1 (mirroring). El nivel 6 es una combinación del nivel 1 con el nivel 5 (interleave).

2.10.2.-Servidores Redundantes Una implementación de servidores redundantes toma el concepto de RAID 1 (mirroring) y lo aplica a un par de servidores, uno de los cuales toma el rol de primario, siendo el otro el secundario, cuándo el primario presenta alguna falla, pasa las funciones al secundario (rollover) Este cambio de funciones puede ser en caliente (cuando es transparente para el usuario) ó no, esto depende de la implementación y la sensibilidad de la aplicación.

2.10.3.- Server Clustering (Granja de servidores).- Una granja de servidores es un grupo de servidores independientes entre si, los cuales funcionan como si fueran un solo servidor, brindando alta disponibilidad del sistema, fácil administración, y gran escalabilidad. El concepto de Server clustering es similar a la de servidores redundantes excepto que todos los servidores de la granja están siempre en línea y procesando información, es decir actúan como una entidad inteligente que balancea y distribuye la carga de proceso mejorando el rendimiento del sistema. Si cualquiera de los servidores de la granja falla, el proceso continúa transparentemente, sin embargo todo el conjunto sufre una baja en el rendimiento.

2.10.4.- Respaldo de la Información (Backups).- Es la grabación en dispositivos masivos de la información existente en un determinado sistema en un determinado momento, con el fin de guardarla y prevenir cualquier falla en el

sistema en línea que pudiera afectar la disponibilidad e integridad de la información. Existen variados métodos de respaldar la información. Sin embargo los métodos más usados son los siguientes:

a) Full Backup.- Es efectuar una copia de respaldo de cada archivo del servidor cada vez que realice el respaldo. Este es el método primario y es usado como línea base del sistema de respaldo.

b) Backup Incremental.- Este método de respaldo solo copia los archivos que han sido recientemente agregados ó modificados en el día. Reinicia el bit de backup de los archivos luego de haber efectuado la copia. Este método nos ahorra tiempo y espacio pero tiene varias vulnerabilidades.

c) Backup Diferencial.- Este método solo copia los archivos que han sido modificados desde que un full backup, Es un método aditivo porque el tiempo y espacio requerido porque cada copia de respaldo diario es una copia de los archivos cambiados y modificados desde el último full backup. En este escenario el bit de backup no es reiniciado hasta el próximo full backup.

2.11.- Ataques y abusos de la red.- Es muy importante antes de efectuar el diseño de una red de seguridad perimetral conocer los varios tipos de ataques que se pueden dar hoy en día y como trabajan. Estos ataques están en constante evolución, ésta es probablemente el área más dinámica de la Seguridad Informática hoy en día. Las empresas dedican importantes montos de dinero, personal y recursos para prevenir y defenderse de estos ataques. Los estudios y estadísticas al respecto informan que estos ataques son hoy en día más comunes de lo que se cree y pueden tener fuentes internas y externas. Si no se está protegido adecuadamente las empresas pueden sufrir graves daños a la disponibilidad, integridad u confidencialidad de su información y más aún si los efectos son conocidos ó visibles desde Internet pudiendo tener efectos muy profundos y adversos sobre la imagen y confiabilidad de la empresa. Que pasaría si fuera su banco el afectado, ó la tienda virtual donde usted suele hacer compras?

Los crímenes cibernéticos top reportados en el año 2004 son los siguientes:

Principales Crímenes Cibernéticos

- Intrusión 46 %
- Denegación de Servicios 45 %
- Robo de Información 27 %
- Fraude 21 %
- Robo de Identidad 16 %
- Extorsión 4 %
- Otros 18 %

En total, más del 88% de las empresas e instituciones a nivel mundial han sido victimas de algún crimen cibernético. Un total de 368,529 incidentes reportados en el 2004. No se dispone de estadísticas a nivel de personas.

Sin embargo en el año 1999 los ataques externos eran solo el 3% del total de incidentes de seguridad en el 2004 son ya el 40%, esto también nos revela que ahora el 60% de los incidentes de seguridad son internos y las fuentes más comunes de estos ataques ó de errores en los sistemas son:

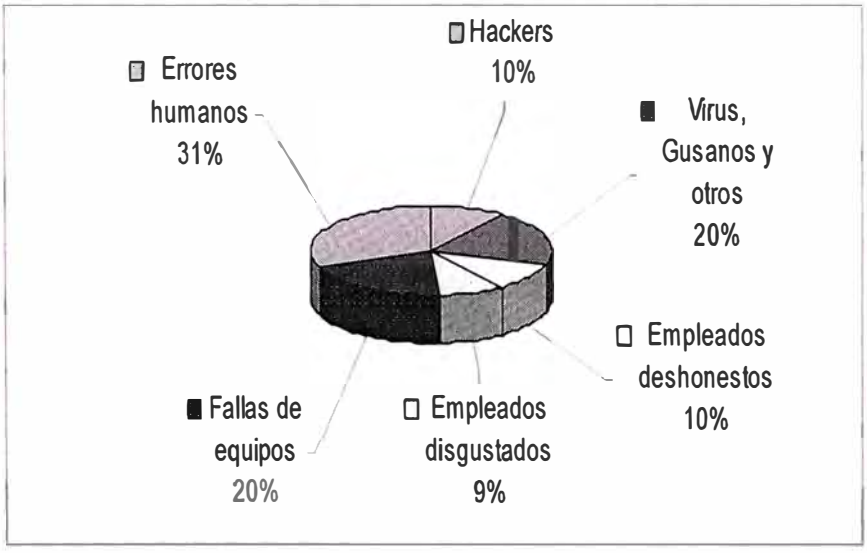


Figura 2.1 Distribución estadística de los principales problemas de seguridad.

Ahora vamos a explicar los diversos tipos de ataques y también los más comunes. Estas clases han sido creadas para explicarlas de un modo ilustrativo y no pretenden listar a todos los tipos de ataques existentes (debido a que cada día surgen nuevos).

a) Clase A.- Acceso no autorizado a servicios de red restringidos.- Este tipo de ataque también es conocido como "logon abuse". Se refiere a usuarios legítimos y autorizados de una red ingresando ó intentando acceder a servicios que están restringidos para ellos, son los usuarios curiosos ó que quieren muchas

veces explorar los servicios existentes en la red, pero también aquellos que saben que tienen restricciones y pretenden saltarlas. Se da el caso de usuarios que pretenden ser otros, (técnica de enmascaramiento). Un ataque de Ingeniería social puede ser un buen ejemplo de esto.

b) Clase B.- Uso no autorizado de la red para fines que no son del negocio.- Esta clase refiere al mal uso que hacer el personal autorizado de las facilidades que la empresa le brinda para cumplir adecuadamente su labor, este uso no es de normalmente de mala intención y esta referido por ejemplo a la navegación en Internet que suelen hacer los empleados distrayendo tiempo valioso de la labor diaria e ingresando a sitios que no tienen nada que ver con el negocio (pornografía, viajes, deportes, chats, foros, etc). De acuerdo al Código de ética del ISC2 y a las recomendaciones del Internet Advisory Board (IAB) el uso de los servicios de red para propósitos ajenos al negocio debe ser considerado un abuso del sistema. Es por eso necesario que las empresas tengan los medios necesarios para filtrar la navegación por Internet para no tener problemas legales ó verse afectados por lo peligros de Internet (cookies, robots, virus y otros).

c) Clase C.- Eavesdrooping.- Este tipo de ataque consiste en la intercepción no autorizada del tráfico de red. Ciertos medios de transmisión de información tales como las comunicaciones satelitales, las inalámbricas, las comunicaciones móviles son vulnerables a este tipo de ataques. Ahora bien la intercepción física de un medio de transmisión se denomina tapping (puede ser derivación de un medio alterno, tipo anexo en las comunicaciones telefónicas ó por equipos que mediante la inducción electromagnética pueden por variación de campos electromagnéticos reconstruir la información que pasa por el medio físico, como por ejemplo el alambre de cobre) Existen dos variaciones:

- Eavesdroping Pasivo.- Monitorea y escucha las transmisiones sin conocimiento ni del transmisor ni del receptor.
- Eavesdroping Activo.- Consiste en establecer un canal encubierto de transmisión a través de otro canal oficial para transmitir información no autorizada, puede ser por división de frecuencia ó de tiempo.

El eavesdroping y el probing son a menudo los pasos preliminares para efectuar un secuestro de la sesión (hijacking) y otros tipos de intrusión.

d) Clase D.- Denegación de Servicios.- Estos tipos de ataques crean una situación que satura los recursos de la red, se denominan comúnmente ataques DoS (Denial of Service) por sus siglas en inglés. La saturación puede ocasionar que los dispositivos de red, servidores, ó ancho de banda de la infraestructura de red puede ser seriamente afectada por el gran volumen de tráfico generado y degradar la performance del sistema en su conjunto.

Los ataques DoS pueden usar las siguientes técnicas para saturar a sus blancos:

- Llenar el disco duro del blanco por el envío de correos electrónicos ó transferencias de grandes volúmenes de datos.
- Abrir simultáneamente múltiples sesiones ó conexiones de red, ocasionando que los siguientes intentos de conexiones sean rechazados.

Los tipos de ataques DoS más comunes son las siguientes:

- **Buffer Overflow.-** Ocurre cuando un proceso ó recurso recibe una mayor cantidad de datos de lo esperado. Si el proceso ó recurso no tiene la capacidad de procesar ó rechazar esta gran cantidad de información puede actuar de modo inesperado lo cual puede ser aprovechado por un atacante. Entre los muchos tipos de ataques DoS de este tipo el más común es el llamado "Ping of death" (un ataque con paquetes ping más grandes de lo usual) y también el que utiliza nombres de archivos adjuntos al correo electrónico mayores de 256 caracteres. Un ataque con el comando PING utiliza el protocolo ICMP con la señalización ping, y consiste en enviar comandos "ping" con una trama modificada y más grande de lo usual, esto llena el buffer del sistema receptor y puede causar el reboot del equipo ó que este se cuelgue.
- **SYN Attack.-** Ocurre cuando el atacante intenta explotar el uso del espacio de buffer durante la transmisión de información con el protocolo TCP, el cual para iniciar una comunicación utiliza una técnica de handshaking. El atacante envía hacia el blanco una serie de mensajes de inicio de conexión, pero no responde cuando el blanco responde a ese requerimiento. Esto causa que el sistema blanco del ataque quede en espera de la respuesta, pero como son muchas conexiones simultáneas el sistema se inhibe ó colapsa.
- **Teardrop Attack.-** Consiste en modificar la longitud y los campos de fragmentación de la secuencia de los paquetes IP. El sistema blanco del ataque no puede procesar esa información, se "confunde" ante requerimientos extraños y contradictorios, ocasionando que el sistema se inhiba ó colapse.

- **Smurf.-** Un ataque smurf ó "pitufo" usa una combinación de ICMP e IP spoofing para saturar al sistema blanco del ataque con tráfico de red. El atacante envía un paquete PING con dirección IP cambiada a toda la red blanco. El paquete modificado contiene la dirección del sitio atacado, esto causa que el sitio afectado envíe mensajes tipo broadcast a toda su red. Entonces todos los dispositivos de la red responden al sistema blanco el cual se satura el ser este evento reiterativo.
- **IP Spoofing.-** Es utilizado para convencer al sistema blanco que se está comunicando con una entidad conocida ó autorizada en lugar de con el atacante. Utiliza una alteración del paquete a nivel del protocolo TCP, es utilizado para atacar a sistemas conectados a Internet . El atacante oculta su verdadera dirección IP y utiliza una dirección IP confiable para el blanco.
- **TCP Secuence Number.-** Este ataque explota la sesión de comunicaciones ya establecida entre el sistema blanco y otro sistema confiable. El atacante engaña al sistema blanco para hacerle creer que sigue conectada con el sistema confiable y "secuestra" la sesión, esto lo logra prediciendo ó reemplazando el número inicial de la secuencia de paquetes TCP.
- **Fragmento TCP desmenuzado.-** Ocurre cuando un atacante envía un paquete TCP muy pequeño que fuerza que el campo de cabecera sea enviado en un segundo paquete. Si el sistema blanco no puede procesar el pequeño primer paquete este puede contener otra información que puede aprovechar las vulnerabilidades del sistema operativo.

e) Clase E.- Intrusión.- Este tipo de ataque se refiere al uso de accesos no autorizados para romper la seguridad de la red externa desde una fuente externa. Normalmente el intruso no es conocido en la red. La mayor parte de los ataques pueden caer en esta clase, es también conocido como ataque de penetración y trata de explotar las vulnerabilidades del perímetro de seguridad. Tenemos las siguientes variaciones:

- **Spoofing.-** Esta referido a que un atacante deliberadamente induce a un usuario ó dispositivo a efectuar una acción incorrecta.
- **Piggy-backing.-** Esta referido a que un atacante logre acceso no autorizado a un sistema con el uso de una conexión ó sesión de un usuario legítimo. Si un usuario no cierra adecuadamente su sesión posibilita que el atacante pueda capturar esta sesión.

- **Back Doors.-** Comúnmente referidos a intrusiones via dial-up ó conexiones asíncronas, que abren conexiones no autorizadas desde el sistema blanco hacia el sistema atacante.

f) Clase F.- Probing.- Es una variación del eavesdropping activo. Es usualmente utilizado por el atacante para obtener información de la red del sistema blanco en preparación a un ataque tipo DoS. Permite al atacante mapear la red y los servicios disponibles. El análisis del tráfico a través de un "sniffer" es una forma de "probing". El "probing" puede ser manual ó automático. La forma manual es mediante el uso de herramientas tales como el Telnet, el cual es usado para conectarse a un sistema remoto y comprobar que esta escuchando y listo a permitir conexiones. Los scanners de vulnerabilidades son softwares que automáticamente intentan las conexiones a los sistemas blancos a través de una amplia gama de puertos TCP y luego lo reportan al atacante.

Resumen del Capítulo

En este capítulo se ha revisado los principales conceptos de seguridad asociados con la seguridad de redes y de la información, hemos podido conocer las principales técnicas de prevención, así como lo principales ataques que pueden sufrir las redes de comunicaciones y sistemas de datos.

CAPÍTULO III
CONCEPTOS DE TECNOLOGÍA Y COMUNICACIONES

En este capítulo se tratará de entender y conocer:

- Que la seguridad de la red y las comunicaciones abarca toda comunicación de voz, data, multimedia, y otras limitadas a una red LAN, WAN y medios de acceso remoto.
- Las técnicas de seguridad informática sirven para prevenir, detectar, y corregir errores de integridad, disponibilidad y confidencialidad de las redes de comunicaciones.
- Los tipos de redes Internet/Extranet/Intranet y los dispositivos que las protegen e interrelacionan tales como firewalls, routers, gateways y los protocolos de comunicaciones.
- La gestión de seguridad de las comunicaciones y las técnicas empleadas para prevenir, detectar y corregir problemas que atenten contra la integridad, disponibilidad y confidencialidad de las comunicaciones.

3.1 Protocolos.- Son la base sobre la que construyen los conceptos de comunicaciones y seguridad. Un protocolo es una serie de reglas ó estándares que rigen la forma en como los dispositivos de una red se comunican unos a otros a través de la red misma. Cuando una computadora se comunica con otra intercambia una serie de mensajes. Un protocolo describe el formato que ese mensaje debe tener para poder ser entendido por la entidad receptora. Así se hace posible que distintos tipos de equipos tales como Pc´s , Unix ó Apple se puedan comunicar entre sí a pesar de sus diferencias. Este formato de comunicaciones obedece a un modelo de arquitectura que toma en consideración varios niveles ó capas. Hay muchas razones para utilizar una arquitectura de niveles ó capas:

Facilita la comprensión de los procesos de comunicaciones al poner el foco en lo que específicamente hace.

Divide el complejo proceso de comunicaciones en niveles más fáciles de entender y manejar.

Al definir estándares por niveles permite la interoperatividad de las distintas plataformas.

Permite cambiar las características de un nivel de un determinado proceso ó aplicación sin afectar el funcionamiento de los demás niveles.
Facilita la detección de problemas.

¿Cómo la data se mueve a través de una arquitectura de niveles?
La data es enviada desde la computadora fuente hacia la computadora destino. En el modelo de niveles, la data pasa a través de las distintas capas desde los niveles superiores (Nivel 7 en el modelo OSI) hacia los niveles inferiores (Nivel 1 ó físico en OSI) en la computadora fuente, luego es transmitida por el medio de transmisión y es recibido por la computadora destino donde pasa nuevamente por los niveles pero en sentido inverso, desde el más bajo (Nivel 1) hasta el más alto (Nivel 7).

Cada uno de los diversos protocolos opera en una capa ó nivel específico. Cada protocolo en la computadora fuente tiene una labor que cumplir, desde empaquetar la data, ensamblarla en paquetes poniéndole un código único de identificación, hasta formas las tramas con las direcciones de destino estableciendo la ruta que la comunicación debe seguir. Igualmente en la computadora destino cada protocolo tiene su labor, generalmente en sentido inverso a lo hecho anteriormente.

3.2.- Modelo de Referencia OSI (Open Systems Interconnect) .- A los inicios de los años 80 este modelo de referencia fue creado por la International Standards Organization (ISO) para ayudar a las empresas fabricantes de dispositivos de comunicaciones a crear dispositivos interoperables. El modelo de referencia OSI describe como la data y las comunicaciones en la red deben darse para lograr la comunicación con otros equipos. Para hacerlo establece 7 niveles ó capas, cada capa tiene un único conjunto de propiedades que directamente interactúa con las capas adyacentes. Se esperaba que este modelo se convirtiera en un estándar único sin embargo no ha logrado prevalecer sobre el TCP/IP.
Los 7 niveles del modelo OSI son:

Nivel 1	Físico
Nivel 2	Enlace de datos
Nivel 3	Red
Nivel 4.	Transporte
Nivel 5	Sesión
Nivel 6	Presentación
Nivel 7	Aplicación

No vamos a entrar en el detalle de los mismos por no ser el cauce de este informe.

3.3.- Servicios y Mecanismos de Seguridad OSI.- El modelo OSI define seis servicios de seguridad básicos. Un servicio de seguridad es un grupo de mecanismos de seguridad, archivos y procedimientos que protegen a la red.

Estos son los seis servicios básicos:

Autenticación
Control de acceso
Confidencialidad de la data
Integridad de la data
No repudio
Monitoreo y registro de eventos (logging)

Además el modelo OSI también define ocho mecanismos de seguridad. Un mecanismo de seguridad es un control que se implementa para lograr los seis servicios básicos de seguridad.

Los mecanismos de seguridad son:

Cifrado ó encriptación
Firmas digitales
Control de acceso
Integridad de la data
Autenticación
Control de tráfico no autorizado
Control de ruteo
Notarización.

3.4.- Modelo TCP/IP.- TCP/IP es el nombre común de una suite de protocolos desarrollada por el Departamento de Defensa de los Estados Unidos y cuyo nombre completo es Transmisión Control Protocol/Internet Protocol, fue diseñado en los años 70 para soportar el desarrollo de la Internet. Internet esta basado en el TCP/IP.

El modelo del protocolo TCP/IP es similar el modelo OSI, también define niveles pero solo cuatro:

- **Nivel de Aplicación.-** Consiste en las aplicaciones y procesos que son utilizadas en la red. Es muy semejante al Nivel de Aplicación OSI, y tiene las mismas funciones.
- **Nivel de transporte Host to Host.-** Provee el servicio de entrega de la data al nivel de aplicación. Brinda confiabilidad en la transmisión end-to-end, asegura la

entrega de la data sin errores, maneja la secuencia de paquetes y mantiene la integridad de la data.

- **Nivel Internet.-** Define el datagrama IP y maneja el routing de la data a través de la red. Corresponde al nivel de Red de la OSI. Designa los protocolos que se encargan de la transmisión de los paquetes de datos sobre la red. Este nivel maneja los nodos y las direcciones IP permitiendo el ruteo de los paquetes a través de diferentes redes. Controla también el flujo de comunicación entre los equipos terminales.
- **Nivel de enlace.-** Consiste en la rutinas de accesos físico al medio de transmisión. Monitorea el flujo de información entre el host y la red. Es el equivalente a los niveles de Enlace de datos y Físico del modelo OSI, maneja el direccionamiento físico y los protocolos para la transmisión física de la data.

Los protocolos funcionales pueden ser agrupados de acuerdo al nivel TCP/IP en el cual trabajan. Los principales protocolos utilizados en las comunicaciones de datos son:
Protocolos del nivel de transporte Host-to-Host

Transmisión Control Protocol (TCP).- Provee comunicación orientada a la conexión, confiable, establece un circuito virtual. Los paquetes TCP son secuenciales a un número establecido aleatoriamente durante el establecimiento de la conexión. Dado que los paquetes perdidos ó que llegan con errores son retransmitidos, el TCP es más costoso en términos de ancho de banda y velocidad de transmisión que el protocolo UDP.

- Un mensaje de conformidad (acknowlegment - ACK) es enviado por el equipo receptor al equipo transmisor cada vez que recibe un paquete de datos.
- Si no se recibe el mensaje de ACK por cada paquete enviado, se vuelve a transmitir el paquete.
- Los paquetes son ensamblados en el orden correcto en el equipo receptor.
- Se manejan controles de flujo en la comunicación para evitar la congestión, la sobrecarga y la pérdida de data.

TCP y UDP deben utilizar “puertos” para comunicarse con los niveles superiores. Los “números de puerto” son utilizados para separar diferentes canales de comunicación (conversaciones) que simultáneamente se pasan por la red.

Originalmente los puertos origen son asignados dinámicamente por el equipo transmisor y pueden variar, pero generalmente son mayores al 1023.

User Datagram Protocol (UDP).- Es una versión más "light" del TCP. Es utilizado como el TCP solo que no ofrece corrección de errores, no está orientado a la conexión, no secuencia los paquetes de datos y no tiene cuidado del orden en el cual los paquetes de datos llegan al destino. Es un protocolo "no confiable". UDP no crea un circuito virtual y no establece contacto con el equipo destino antes de enviar la información. Es por eso considerado un protocolo no orientado a la conexión (connecctionless) . Es más rápido que el TCP.

Protocolos de Internet.- Internet Protocol (IP) es el origen de todos los protocolos. Todos los equipos en una red tienen una dirección lógica llamada "Dirección IP" Esta dirección contiene la información necesaria para simplificar el ruteo de los mensajes. Cada paquete a ser enviado por el equipo transmisor es asociado a una "Dirección IP" (que es la "Dirección IP" del equipo receptor) antes de ser transmitido por la red. Cada dispositivo de la red recibe el paquete y toma la decisión de ruteo basado en la "Dirección IP" de destino del paquete enviado.

Address Resolution Protocol (ARP).- El IP necesita conocer la dirección física del paquete de destino antes de poder enviarlo. ARP proporciona esta información al poder correlacionar la dirección IP con la dirección real de la tarjeta de comunicaciones. Esta es una dirección de 48 bits que es colocada por el fabricante en la tarjeta (NIC). ARP logra correlacionar esta dirección con la dirección IP de 32 bits con una técnica conocida como Media Control Access (MAC) Address. ARP interroga a la red enviando un broadcast buscando al nodo que tiene la dirección IP buscada, y este replica enviando su dirección física. ARP mantiene una tabla dinámica con la información que correlaciona direcciones físicas con direcciones IP y solo envía un broadcast cada que requiere comunicarse con un nodo de la red por primera vez.

Reverse Address Resolution Protocol (RARP).- A veces se presenta el caso inverso al anterior es decir conociendo una dirección física se necesita conocer la dirección IP. Este es el caso, a menudo, de equipos sin disco de boot en la red, ó la utilización de direcciones IP variables. El protocolo RARP envía un paquete en el cual incluye su dirección física y un requerimiento para que le indiquen cual

será la dirección IP que le será asignada, luego el servidor de RARP le responderá asignándole una dirección IP.

Internet Control Message Protocol (ICMP).- Es un protocolo de administración y mensajería de la suite IP. Su función primaria es enviar mensajes a través de la red para preguntar el estado de la misma. También informa a los host cual es la mejor ruta hacia el destino ó si hay un problema en la ruta actual, pudiendo también ayudar a identificar el problema. El programa utilitario PING utiliza mensajes ICMP para revisar la conexión física de los equipos a la red.

Telnet.- Es una función que emula un Terminal. Posibilita que un usuario en una máquina remota pueda acceder a los recursos de otra máquina. Las capacidades del Telnet están limitadas por las mismas aplicaciones y no puede ser utilizada por ejemplo para bajar archivos. Utiliza el puerto 23.

File Transfer Protocol (FTP).- Es un protocolo utilizado para la transferencia de archivos entre dos equipos, y para ciertas tareas de administración de archivos, posibilita el acceso a directorios y archivos, sin embargo no puede ejecutar programas. Utiliza los puertos 20 y 21.

Trivial File Transfer Protocol (TFTP).- Es una versión más ligera del FTP. No tiene la capacidad de navegación ó browsing que tiene el FTP, es básicamente para el envío y recepción de archivos. No tiene mecanismos de autenticación por lo tanto es inseguro, por lo que no es muy utilizado.

Network File System (NFS).- Es un protocolo que soporta el intercambio y compartir de archivos. Hace posible que dos equipos con distintos tipos de sistemas operativos puedan intercambiar archivos.

Simple Mail Transfer Protocol (SMTP) Es un protocolo muy usado hoy en día para enviar y recibir correo por Internet. Cuando un mensaje es enviado, se coloca a una cola de correo, el SMTP regularmente revisa la cola de correo para buscar los nuevos mensajes y cuando los detecta los envía. Utiliza el puerto 25.

Line Printer Daemon (LDP).- Posibilita el uso de impresoras en la red para ser compartidas por diversos equipos; estas envían sus requerimientos de impresión a una cola de la impresora de red.

Simple Network Management Protocol (SNMP).- Es un protocolo que recopila información del estado de la red preguntado sucesivamente (polling) a todos los dispositivos de la red. También puede notificar a los administradores de la red de los eventos considerados sensibles a través del envío de alertas a la estación base.

Hyper Text Transfer Protocol (HTTP – Protocolo de transferencia de hipertexto) es el más usado en la Internet y posibilita que los datos de las páginas web residentes en servidores de servicios web sea transferida de manera rápida hacia la estación "cliente" que en este caso es la que hace la petición. Estos datos normalmente están escritos en formato HTML (Hyper Text Markup Text) y trabajan de manera eficiente a las peticiones hechas por el http.

3.5.- Protocolos y tecnologías de Seguridad.- Los protocolos de seguridad son en algunos casos variaciones de otros protocolos con funciones agregadas de seguridad tales como facilidades de encriptación, autenticación. En otros casos son tecnología y protocolos diseñados exclusivamente para funciones específicas que requieren altos niveles de seguridad. Ahora mostraremos los más utilizados.

Simple Key Management for Internet Protocols (SKIP).- Es una tecnología de seguridad que brinda alta disponibilidad y encriptación de las sesiones. Es similar al protocolo SSL, excepto que no requiere una comunicación preliminar para el intercambio de llaves y no genera continuamente nuevos valores de llave de encriptación.

Secure Sockets Layer (SSL).- Es una tecnología de encriptación que se utiliza para efectuar intercambios de información sensible entre dos equipos que se comunican a través de una red. Es un protocolo de dos niveles, SSL Record Protocol y el SSL Handshake Protocol, este último se encarga de establecer la comunicación inicial y generar un intercambio de llaves de encriptación que son luego utilizadas para generar la llave de encriptación de la comunicación. Esta última es una llave

simétrica. También utiliza el Message Autentication Code para revisar la integridad de los mensajes.

Secure Shell (SSH2).- Es un método fuerte de autenticación de clientes remotos, soporta además compresión de datos, y mecanismos de confidencialidad e integridad. Es utilizado frecuentemente a través de Internet, tiene dos importantes componentes: intercambio de llaves asimétricas mediante el método de RSA y Triple DES (3DES) para encriptación.

3.6.- Arquitectura y tipos de Firewalls.- [2] Los firewalls ó cortafuegos, (traducción castellana solo utilizada en España), son dispositivos de seguridad que aíslan las redes unas de otras. Generalmente son utilizados como "guardas de frontera" entre las redes internas y las redes públicas revisando el tráfico de datos que fluye entre ellas y dejando pasar solo el tráfico autorizado. Son dispositivos fundamentales de cualquier esquema de seguridad perimetral hoy en día y en caso de redes pequeñas y con pocos servicios hacia el mundo exterior correctamente configurados y sobre una plataforma idónea pueden ser suficientes como plataforma de seguridad. Existen diversos tipos de firewalls. A continuación los describimos ordenados por generación, es decir en el orden en el cual fueron desarrollados.

3.6.1.- Tipos de firewalls

a) Packet Filtering (De filtrado de paquetes).- También llamado "screening router" este tipo de firewall examina la dirección fuente y el destino, así como al paquete de datos, luego de esta revisión bloquea ó deja pasar el paquete. Para efectuar este análisis y denegar el acceso a destinos específicos ó servicios se basa en "Listas de Control de Acceso" (Access Control Lists – ACL), que son archivos de configuración almacenados en el firewall y que son gestionados por el administrador del firewall y que le indican al firewall que tipo de paquetes debe dejar pasar y a que direcciones específicas. Un firewall de filtrado de paquetes mira en ele paquete entrante para conseguir información sobre las direcciones de origen y destino , así como el tipo de sesión de comunicación que va a utilizar la comunicación (TCP, UDP ó ICMP) , y los puertos de aplicación destino y origen que van a ser utilizados. Este tipo de sistema de firewalls son considerados la "primera generación" de firewalls, y pueden operar en los capas de Red ó Transporte del modelo OSI.

b) Aplication Level .- Este tipo de firewall es a menudo un equipo de computo (host computer) que corre algún tipo de software de proxy Server, lo cual lo convierte en un "proxy server". Este firewall trabaja transfiriendo una copia de paquete de datos aceptado desde una red hacia otra, enmascarando la dirección IP de origen del paquete. Entonces puede controlar que servicios son utilizados por cada estación a la vez que protege la red interna de agentes externos que traten de conseguir información sobre ella.

Este tipo de firewall es considerado la "Segunda generación" de firewall. Es también llamado "Gateway de nivel aplicación" (Application Layer Gateway). Opera en el nivel de "Aplicación" del modelo OSI. Un problema de este tipo de firewall es que reduce el rendimiento de la red al analizar cada paquete y decidir que hacer con él.

Una variación de este tipo de firewall en el llamado "Firewall de nivel de circuito" (Circuit Level Firewall), que crea un circuito virtual entre la estación cliente y el servidor.

c) Stateful Inspection (De Inspección de Estado).- En este tipo de firewalls los paquetes entrantes son capturados por un motor de inspección que opera a nivel de la capa de "RED". Los paquetes son puestos en una cola y analizados en todos los niveles OSI. Si bien puede bajar la performance sobre la comunicación brinda una completa inspección de los datos. Examinando el "estado" y el "contexto" de los paquetes de datos entrantes, puede revisar adecuadamente a los mensajes de protocolo son orientados a la conexión tales como los UDP y las aplicaciones que utilizan RPC (Remote Call Procedures). Este tipo de firewalls son conocidos como la "Tercera Generación de firewalls".

d) Dynamic Packet Filtering.- (De filtrado dinámico de paquetes) Este tipo se firewalls es considerado la "Cuarta generación" e las tecnologías de firewalls, y tiene como principal ventaje la modificación dinámica de la reglas de filtrado. Por un corto periodo de tiempo este firewall recuerda todos los paquetes UDP que han pasado por él y decide en base a esta "memoria" si permite ó no el paso de los siguientes paquetes.

3.6.2.- Arquitecturas de firewalls.- En este parte vamos a hablar de las cuatro más comunes arquitecturas de firewalls. Algunas están específicamente

asociadas a los tipos de firewalls que se han descrito anteriormente, mientras que otras arquitecturas pueden ser consideradas una combinación de firewalls de varias generaciones. La forma como se usan depende del tipo de redes que protegen y las demandas de seguridad y flexibilidad que dicta el negocio.

a) Packet filtering Routers.- Es la más común y más antigua arquitectura de firewalls. Algunos autores no lo consideran un tipo ó arquitectura de firewalls. Un router de filtrado de paquetes se sitúa entre la red interna y confiable y la red externa no confiable, también se le llama router de borde (boundary router). Utiliza una Lista de Control de Acceso (ACL). Este firewall protege contra ataques externos genéricos. El principal problema que tienen es el mantenimiento de los ACLs. Otros problemas son que no brinda facilidades de autenticación fuerte, tiene mínimos niveles de auditoria y si los ACLs son bastante grandes y complejos pueden dar problemas de performance y rendimiento en el sistema. Esta arquitectura puede ser utilizada para manejar el acceso desde el segmento externo hacia la zona "Desmilitarizada" (DMZ) en redes que no requieran altos niveles de seguridad ó no dispongan de los recursos necesarios para altas inversiones en tecnología de firewalls especializados.

b) Screening Host (Servidor de pantalla).-Esta arquitectura de firewalls emplea un router de filtrado de paquetes y un servidor conocido como " bastion host" ,es un poco más complicada que otras arquitecturas porque ofrece un mayor nivel de seguridad al proporcionar dos características importantes de seguridad a nivel de red (filtrado de paquetes) y de aplicación (servicios de Proxy). Esta arquitectura es considerada más segura porque un intruso requeriría penetrar dos sistemas separados antes de comprometer la red interna ó privada. El servidor que actúa como "bastion host" debe estar ubicado en la red interna y todo el tráfico que el router de filtrado de paquetes deje pasar debe ser diseccionado hacia él antes de pasar a la red interna en sí. Debido a que el "bastion host" es a menudo blanco de muchos ataques externos es a menudo llamado "host de sacrificio".

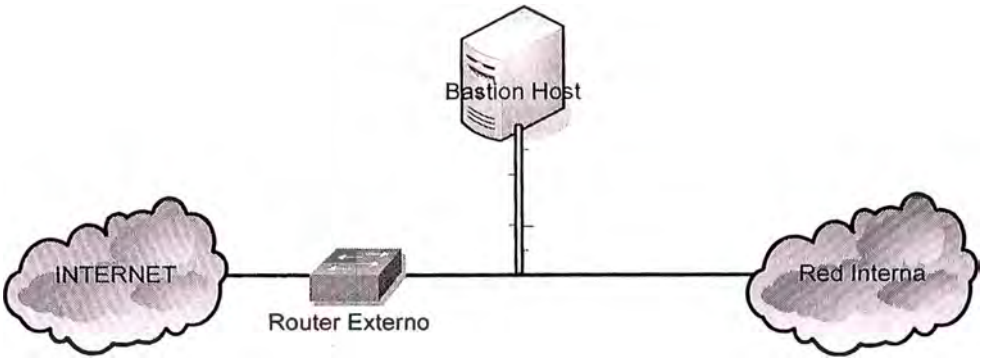


Figura 3.1 Firewall de servidor de pantalla

c) Dual – Home Host.- Otra arquitectura muy común de firewalls es la llamada "Dual Home Host" ó "Multi Bastion Host". Esta arquitectura es una simple configuración que consiste en un "bastion host" con dos tarjetas de comunicación (tarjetas de red). Una de ellas conectada hacia la red interna y la otra hacia la red externa no confiable. Actúa como un filtro del tráfico que intenta circular entre ambas redes, todo el tráfico es sometido a algún tipo de revisión. Esta arquitectura permite pasar tráfico entre redes de distinta características a nivel de "RED" tales como ethernet ó token ring.

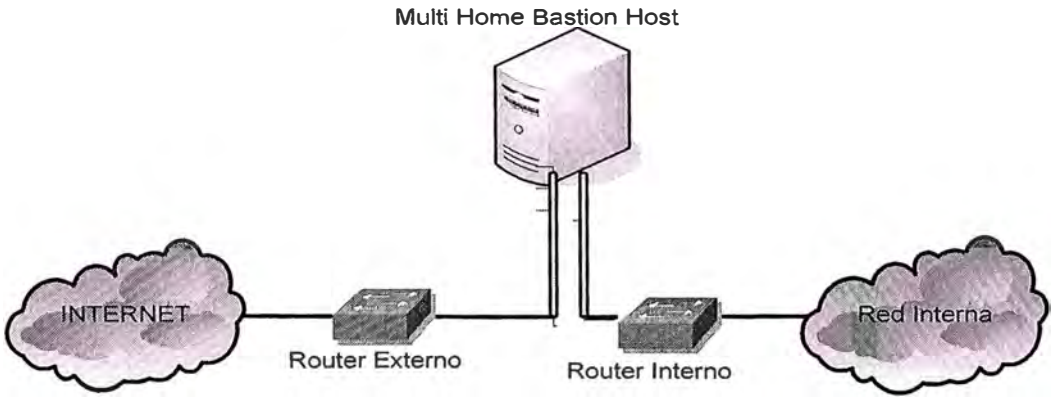


FIGURA 3.2 Firewall de Servidor con doble tarjeta

Una consideración de diseño en esta arquitectura es que las capacidades de ruteo del "bastion host" deben ser deshabilitados para no permitir ningún ruteo de tráfico no autorizado y que puede conectar las dos redes haciendo un bypass del firewall.

d) Screening – Subset Firewall.- Es una de las seguras implementaciones de arquitecturas de firewalls. Utiliza dos router de filtrado de paquetes y un

bastion host. Soporta filtrado de paquetes y servicios de Proxy y también define una zona desmilitarizada (DMZ) como un segmento de red que está aislado tanto de la red interna como de la red externa y en donde suelen ponerse los servidores que brindan los servicios de Internet y el bastion host. El router externo provee defensa contra ataques externos mientras que el interno maneja el acceso de la red interna hacia la red desmilitarizada a través del bastion host. Una consideración de esta arquitectura es que es compleja en su configuración y difícil de mantener.

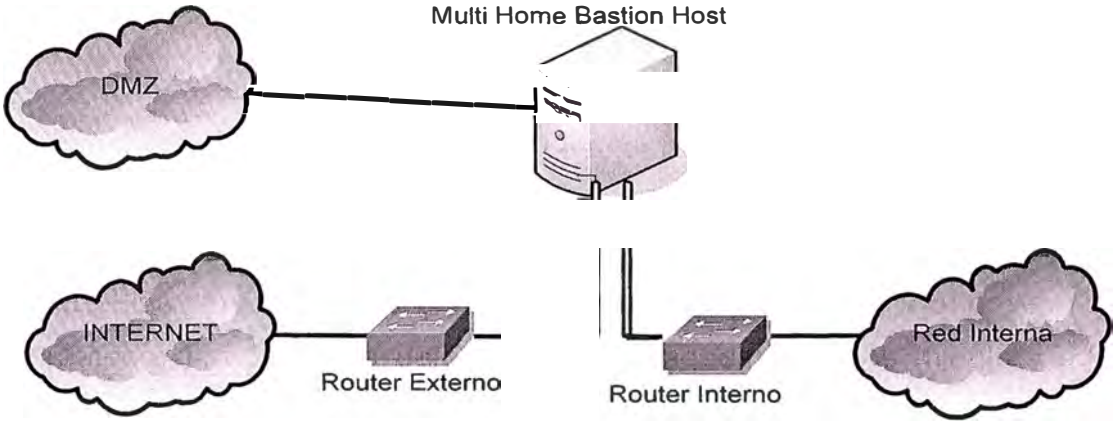


FIGURA 3.3 Firewall con red desmilitarizada DMZ(Screening Subset)

e) Socks Servers.- Otra variación de arquitecturas de firewalls es la llamada de SOCKS SERVERS. Consiste en un Proxy a nivel de circuito que no requiere de un servidor convencional, sin embargo requiere tecnología propietaria y la instalación de un cliente en cada estación de trabajo que va a utilizar esta facilidad, es a menudo utilizada como filtro de los servicios de Internet permitidos al interno de una organización. Como un claro ejemplo de esta tecnología tenemos al Proxy Server- Firewall de Microsoft.

3.7.-Redes Privadas Virtuales.- Una red privada virtual (Private Virtual Network VPN) es un circuito de comunicaciones seguro creado dinámicamente entre dos nodos que se comunican, este enlace es como un túnel seguro encriptado, aunque la encripción no un requisito indispensable. Puede ser creado utilizando algunos de los métodos que a continuación se describen:

Instalando agentes de software ó hardware dedicados en cada nodo cliente y en el gateway de red.

Utilizando varios nodos de autenticación de los usuarios.

Implementando sistemas de intercambio de llaves y certificados digitales.

3.7.1.- Estándar de protocolos VPN.- Existen tres protocolos de comunicación VPN que son los más usados:

a) Point to Point Tunneling Protocol (PPTP).- Este protocolo trabaja en el nivel de Enlace de datos del modelo OSI. Esta diseñado para conexiones individuales de los clientes con el servidor. Es un estándar muy común en conexiones asíncronas que usan clientes de tecnología Microsoft. PPTP usa los servicios de autenticación y encriptación nativos del protocolo Point-to-Point (PPP)

b) Layer 2 Tunneling Protocol (L2TP).- Es una combinación del PPTP y del L2F (Layer 2 forwarding protocol) que trabaja también en el nivel de enlace de datos. Ha llegado a ser un estándar de facto entre los fabricantes de tecnología VPN. Es también para conexiones punto a punto entre clientes y un servidor y puede encapsular múltiples protocolos dentro del túnel L2TP.

c) IPSEC.- Opera en el nivel de Red y hace posible tener múltiples y simultáneas sesiones de VPN. Tiene también la funcionalidad de encriptar y autenticar los datos IP. Está construido sobre el estándar IPv6 y es usado como un extra sobre la versión actual IPv4. Mientras PPTP y L2TP son utilizadas mayormente en conexiones dial up, IPSec esta enfocado en conexión de red a red.

3.7.2.- Dispositivos VPN.- Los dispositivos VPN son elementos de software ó hardware que utilizan los estándares de VPN ya explicados para crear un canal seguro de una conexión VPN.

a) IPsec Compatibles.- Los dispositivos VPN de este tipo están instalados en la red perimetral y encriptan el tráfico entre redes ó entre nodos creando un túnel seguro a través de una red insegura. Debido a que emplean encriptación por IPSec solo pueden trabajar con el protocolo IP. Estos dispositivos operan en el nivel de Red (Nivel Tres OSI). Tienen dos modos operacionales:

- **Modo Túnel.-** Todos los paquetes de datos son encapsulados y encriptados en un paquete IPSec.
- **Modo transporte.-** Solo los datagramas son encriptados, dejando la dirección IP visible.

b) IPSec No Compatibles.- Comúnmente los dispositivos VPN que no son compatibles con IPSec incluyen algún Proxy Server basado en sockets, dispositivos compatibles PPTP ó dispositivos que utilizan SSH.

Los Proxy Servers basados en sockets pueden ser utilizados en una configuración VPN como un sistema de firewall. En esta configuración ellos habilitan el acceso a la red interna desde el exterior a la vez que permiten que las estaciones de la red interna puedan salir a Internet a través del firewall de Proxy. Estos sistemas basados en sockets contienen funciones de autenticación y encriptación, y operan normalmente en el nivel siete del ISO. Es un sistema multiprotocolo y utilizan PAP ó CHAP para autenticación comprimiendo la data para optimización empleando encriptación punto a punto. Los servidores de acceso remoto de las LANs utilizan servicios VPN multiprotocolos a través del PPTP. Son a menudo utilizados por los proveedores de acceso a Internet (ISPs).

Secure Shell (SSH-2) no es estrictamente un producto de VPN pero puede ser utilizado como si lo fuera. SSH abre una sesión segura, encriptada de líneas de comando. Después de ser establecida puede ser utilizada como una sesión de Terminal remoto ó para hacer un túnel a través del cual circulen otros protocolos.

c) Basados en Firewalls.- Este tipo de dispositivos VPN están disponibles desde los firewalls de tercera generación.. Estos equipos emplean un sistema VPN el cual está integrado en el firewall y a menudo utilizan protocolos propietarios. Estos VPNs operan a nivel de la capa de aplicación en modo túnel. Debido a que utilizan autenticación basada en el usuario y encriptación end-to-end, pueden ocasionar problemas de performance.

d) SSL VPN.- Son sistemas relativamente nuevos que facilitan el acceso remoto a través de Internet, se basan en la creación de una conexión tipo VPN pero utilizando el protocolo SSL lo cual posibilita que no sea necesario utilizar clientes en los terminales remotos para levantar la conexión VPN.

3.8.- Aplicaciones de Seguridad en Internet.- Con el crecimiento del uso de Internet para transacciones comerciales se ha hecho muy necesario contar con “herramientas que nos provean de confidencialidad, disponibilidad e integridad de la información” Esta

sección describe y refuerza algunos conceptos sobre los mecanismos que hacen seguro el comercio electrónico.

3.8.1.- Message Authentication Code (MAC).- Fue desarrollado para brindar protección contra fraudes en las transferencias de fondos, es una norma ANSI X9.9.El MAC es un valor de revisión (check value) el cual es derivado del contenido del mensaje en sí, es muy sensitivo a cualquier cambio en el mensaje. Es muy similar al CRC (Cyclic Redundancy Check). El código MAC generado es agregado al mensaje original antes de ser enviado. En el equipo receptor, el MAC es nuevamente generado a partir del mensaje recibido y comparado con el MAC del mensaje original. Si son iguales significa que el mensaje fue recibido sin ninguna modificación efectuada en el camino.
Este algoritmo requiere de una llave, la cual puede ser generada utilizando una llave simétrica como puede ser el DES. Típicamente es una función OR Exclusiva de la llave DES sobre el texto del mensaje.

3.8.2.- Secure Electronic Transaction (SET).- Creado en el año 1997 por un consorcio formado por VISA y MasterCard para prevenir el fraude en los pagos electrónicos. SET brinda confidencialidad para las compras encriptando los datos referentes al pago, de esta manera la entidad vendedora no puede leer estos datos. Utiliza un sistema de llave simétrica DES para la encriptación y llaves RSA para el intercambio de llaves y firmas digitales. SET es todo un protocolo bastante complejo que involucra a las entidades administradoras de tarjetas, a los bancos asociados, a las entidades vendedores y a los usuarios finales cubriendo todo el proceso de compra y pago.

3.8.3.- Secure Socket Layer (SSL).- Aunque ya hemos hablado de él anteriormente es necesario precisar algunos detalles adicionales, este protocolo fue desarrollado por Netscape en el año 1994 para seguridad de las transacciones cliente-servidor sobre Internet. Autentica en el servidor al cliente usando criptografía de llave pública y certificados digitales. También autenticación adicional del cliente en el servidor, soporta el uso del algoritmo de llave pública RSA, y de llave privada IDEA, DES y 3DES, así como el MD5 como función de hash. Las páginas web que utilizan SSL utilizan como protocolo el HTTPS.

3.8.4.- Internet Open Trading Protocol (IOTP).- Es un protocolo diseñado para las transacciones consumer-to-business. Es muy similar al mundo real porque permite al comprador elegir su método de pago. Soporta algoritmos de encriptación de llaves pública y privada, puede utilizar certificados digitales. IOTP está diseñado para ser flexible y acomodar otros modelos de pago electrónico que pudieran surgir en el futuro.

3.9.- Mecanismos de Protección de Equipos de Procesamiento.- En un equipo de procesamiento múltiples procesos pueden estar corriendo simultáneamente. Cada proceso tiene la capacidad de acceder a ciertas direcciones de memoria y ejecutar ciertos sets de instrucciones. La ejecución y el espacio de memoria asignando a cada proceso se llama "Dominio de protección" (Protection Domain) Este dominio puede ser extendido a la memoria virtual, la cual incrementa el tamaño real de la memoria física usando espacio en disco en un proceso denominado "paginación". El propósito de establecer un dominio de protección es proteger los programas de modificaciones no autorizadas ó interferencia en su ejecución.

En seguridad existe un concepto denominado "Trusted Computing Base" (TCB) el cual es una combinación de mecanismos de protección de un sistema de cómputo, el cual incluye hardware, software y firmware. El perímetro de seguridad es la frontera que separa el TCB de los otros componentes del sistema. Un "trusted path" (camino confiable) .debe existir para permitir que un usuario autorizado pueda acceder al TCB sin ser comprometido por otros procesos ó usuarios. Este sistema de seguridad requiere el establecimiento de múltiples niveles de proceso y de clasificación de la información sensitiva. Se requiere conocer los requerimientos específicos de confiabilidad y seguridad.

Los recursos pueden ser protegidos a través del principio de "abstracción", este principio consiste en ver los componentes de un sistema a un nivel alto considerándolo como un todo e ignorando los detalles específicos. Requiere la habilidad de entender sistemas complejos y enfocarse en los problemas críticos. En la programación orientada a objetos, por ejemplo, los programas y la data son encapsulados en un objeto que puede ser visto como una abstracción. El concepto es denominado "information hiding" porque los detalles funcionales están ocultos. La comunicación con este objeto se realiza a través de mensajes a los cuales el objeto responde de una manera definida.

3.9.1.- Rings.- Un esquema que soporta múltiples dominios de protección es el uso de anillos de protección (protection rings). Estos anillos están organizados desde el dominio con mayores privilegios localizado en el centro del anillo, hasta el de menos privilegios localizado en el anillo más externo.

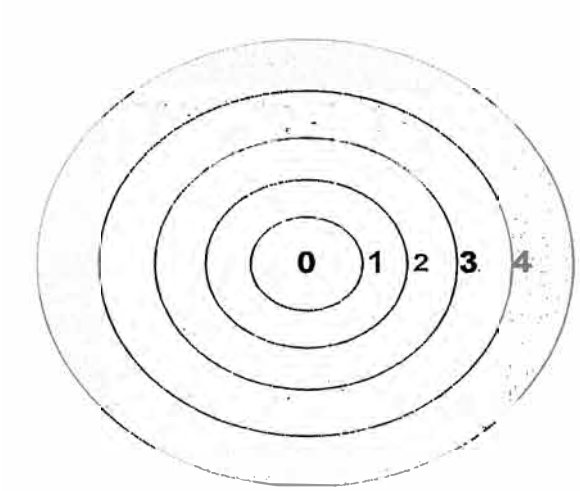


FIGURA 3.4 Anillos de Protección - RINGS

El kernel del sistema operativo es usualmente colocado en el anillo 0 y tiene derechos de acceso a todos los anillos del sistema.

3.9.2.- Security Labels.- Es asignar a un recurso una etiqueta que denota un tipo de clasificación ó designación. La etiqueta puede indicar un manejo especial de seguridad ó puede ser utilizada para control de acceso. Una vez que ha sido asignada no puede ser cambiada y es un efectivo mecanismo de control de acceso. Las etiquetas deben ser periódicamente revisadas y evaluadas para verificar que cumplen con las políticas de seguridad vigentes.

3.9.3.- Security Modes.- Un sistema de información opera en diferentes modos que son determinados por el nivel de clasificación de la información que contiene y por los privilegios de los usuarios. En el modo alto de operación, el sistema opera con información de un alto nivel de clasificación en materia de seguridad y todos los usuarios deben tener permisos para utilizar esa información. En el modo de operación multinivel existen usuarios con distintos niveles de accesos e información con distintos niveles de clasificación. Sin embargo los modos de operación más comunes son los siguientes:

a) Dedicado.- El sistema maneja múltiples niveles de clasificación de información y los usuarios tienen permisos sobre toda la información que es procesada por el sistema.

b) Compartido.- Todos los usuarios tienen autorización para el más alto nivel de información, pero no necesariamente tiene autorización para conocer toda la información que es manejada por el sistema.

c) Controlado.- Es un tipo de seguridad multinivel donde se da un determinado nivel de confianza a un sistema ó aplicación (hardware y software) basado en las restricciones de la información que va a procesar, es decir en la clasificación del nivel de seguridad de la información residente en el sistema.

d) De Acceso Limitado.- Es un tipo de acceso a la información donde el mínimo nivel de acceso de un usuario no está definido, y el máximo nivel de clasificación de la información es "No clasificado" pero sensible.

3.9.4.- Otras consideraciones adicionales de Seguridad.- Las vulnerabilidades en la arquitectura de seguridad de un sistema pueden conducir a violaciones de la política de seguridad. Las vulnerabilidades típicas de la arquitectura de un sistema incluyen a las siguientes:

a) Canal Encubierto.- Es un canal de comunicaciones ni autorizado entre dos ó más sujetos que comparten un recurso del sistema y permite la transferencia de información de una manera tal que viola la política de seguridad del sistema. La transferencia de información usualmente se da a través de las áreas de storage comunes ó de un medio de comunicación usando multiplexación de tiempo.

b) Revisión de parámetros.- Es común que se obvie la revisión del tamaño de los paquetes de entrada, estos deben estar especificados por parámetros configurables. Los ataques de "buffer overflow" explotan esta vulnerabilidad en ciertos sistemas operativos y programas.

c) Mantenimiento.- Se debe revisar todos los mecanismos de hardware y software instalados en el sistema y que permitan opciones de mantenimiento, ya que usualmente permiten efectuar un by pass de los mecanismos de seguridad del sistema. Esta vulnerabilidad es comúnmente denominada como "trapdoor" (puerta trasera)

d) Ataque del Tiempo de Uso.- Este ataque explota la diferencia entre el tiempo de aplicación de los controles de seguridad y el tiempo en el que se ha utilizado un servicio no autorizado.

3.9.5.- Procedimientos de Recuperación.- Todos los componentes de un sistema, sean estos de hardware ó software tarde o temprano son susceptibles de fallar aún en el sistema más confiable. Lo importante es que estas fallas no comprometan la seguridad del sistema (confidencialidad, disponibilidad, confiabilidad). Además los procedimientos de recuperación no deben dar pie a violaciones de la política de seguridad del sistema. Si se requiere efectuar por ejemplo un reinicio del sistema, el sistema debe reiniciar en un modo seguro. El start-up debe ocurrir solo en "modo de mantenimiento" para permitir el acceso solo a usuarios privilegiados ó desde terminales autorizados. Este modo permite restaurar la seguridad del sistema.

Si tenemos un sistema en el cual falla alguno de sus nodos ó componente de red y le sistema continua trabajando sin problemas, podemos decir que tenemos un sistemas "tolerante a fallas" (fault tolerance). Estos sistemas son capaces de detectar cuando una falla se ha presentado y también debe tener la capacidad de corregir la falla ó poner en funcionamiento determinados mecanismos que le permitan seguir operando. En seguridad también se habla de sistemas "de falla segura" (fault safe) en los cuales ante una falla de software ó hardware terminan la ejecución de los programas, y el sistema en general restringe los accesos y se coloca en un modo "seguro" hasta que el problema halla sido solucionado. Igualmente tenemos los sistemas "resilentes" los cuales terminan los procesos no críticos cuando se detecta una falla de hardware ó software, luego el sistema sigue operando pero en modo restringido y con funcionalidades restringidas ó degradadas.

Existen además otras formas de recuperación, tenemos los sistemas con "failover" que son los sistemas que ante una falla efectuar un switch hacia otro sistema duplicado (de backup) en tiempo real, por lo tanto el sistema en conjunto continua operando.

3.9.6.- Certificación y Acreditación.- Estos términos están referidos a los métodos formales que deben ser aplicados en los sistemas para asegurarnos que

los requerimientos y líneas base de seguridad han sido implementadas y están funcionando de acuerdo a las especificaciones. Esta es una responsabilidad de la autoridad (área ó unidad encargada, normalmente Quality Assurance) antes de la puesta en operación (en producción) del sistema. Formalmente las definiciones son las siguientes:

a) Certificación.- Es la evaluación de las características de seguridad técnica y no técnicas de un sistema de información, las cuales han sido establecidas para cumplir con determinadas especificaciones de seguridad.

b) Acreditación.- Es una declaración formal de que el sistema de información revisado esta apto para operar en un modo de seguridad particular, bajo determinadas condiciones y con un nivel aceptable de riesgo.

Tanto la certificación como la acreditación, de un sistema deben ser revisadas después de un periodo determinado de tiempo ó cuando se han efectuado cambios en los sistemas ó los ambientes que los contienen, este proceso se denomina re-certificación y re-acreditación.

Resumen del capítulo

En este capítulo hemos explicado los conceptos de tecnología y comunicaciones involucradós en el desarrollo de sistemas que involucran la seguridad como uno de sus elementos principales a la vez que han explicado las principales tecnologías de seguridad propiamente dichas y los tipos de redes Internet/Extranet/Intranet y los dispositivos que las protegen e interrelacionan tales como firewalls, routers, gateways y los protocolos de comunicaciones.

CAPÍTULO IV
CONCEPTOS DE DATANETWORKING Y SEGURIDAD DE COMUNICACIONES

4.1.- Conceptos de Data Networking .- El término Data Networking hace referencia a las redes de computadoras, las cuales consisten en dos ó más computadoras que están conectadas entre sí con el propósito de compartir archivos, impresoras, intercambiar información, y recursos en general. Para poder comunicarse en una red cada computadora debe tener una tarjeta de comunicaciones (NIC- Network Interface Card), insertada en ella y conectada a un medio de transmisión, un sistema operativo, y dispositivos de red (como router ó switches). Estos temas ya han sido tratados con amplitud en los cursos de actualización profesional razón por la cual no vamos a ampliar en ellos y solo vamos a fijar algunos términos que nos serán útiles en el desarrollo del presente informe.

4.1.1.- LAN.- (Local Area Network) Red de área local, es una red discreta diseñada para operar en un área geográfica específica, tal como un edificio. Las LANs conectan computadoras con servidores de archivos, impresoras, servicios de e-mail. Los dispositivos de una LAN están conectados por un medio físico y utilizan protocolos y métodos de acceso de acuerdo a su topología para comunicarse. También pueden estar conectadas a redes públicas ó privada mayores.

Los dos tipos más comunes de redes LAN son:

Campus Area Network.- Que conecta diversos edificios dentro de una misma área geográfica, brinda alta perfomance y un backbone para las redes locales.

Metropolitan Area network (MAN).- Es una LAN extendida al área de una ciudad, ó un área metropolitana.

4.1.2.- Wide Area Networks (WAN).- Una WAN puede ser considerada una gran red formada por varias subredes LAN que están física ó lógicamente interconectadas sobre una gran área geográfica. Una WAN puede se operada por una comunidad específica de usuarios ó una gran corporación ó puede ser pública

como la INTERNET, puede soportar múltiples protocolos de comunicaciones y diversos servicios de red entre todos sus segmentos ó subredes.

4.1.3.- Internet- Intranet- Extranet .- Más que tipos de redes se podrían decir que son conceptos asociados a las redes WAN y hacen referencia a lo que está dentro, fuera ó es público tomado desde la perspectiva de la LAN privada en particular. Pero vayamos a las definiciones:

a) Internet.- Es una WAN que fue fundada originalmente por el Departamento de Defensa de los Estados Unidos, la cual usa TCP/IP para el intercambio de datos. Se refiere específicamente a la gran red global y pública a través de todo nuestro planeta. Se tiene acceso a ella a través de los Internet Service Providers (ISPs).

b) Intranet.- Una Intranet es una red privada circunscrita a una determinada área ó estructura organizativa, pero que es como la Internet en cuando a estructura lógica y física. Porque también utiliza el protocolo TCP/IP y los estándares http, puede utilizar los productos de bajo costo diseñados para Internet, tales como los navegadores web (web browsers). Una Intranet brinda mayor seguridad y control que una red pública como Internet. Actualmente el término se ha generalizado y se utilizada para designar a cualquier tipo de red privada.

c) Extranet.- Como la Intranet, la Extranet es una red privada que utiliza los protocolos de Internet, una Extranet puede ser accesada por usuarios externos a la entidad que la mantiene (socios, proveedores, etc.) pero no puede accesada por el público en general.

4.1.4.- Topologías de redes LAN.- Este punto también va ser tratado muy brevemente debido a que ya es un tema hartamente tratado y conocido en la gran mayoría de libros sobre tecnologías de redes, sin embargo debido a que utilizaremos muchos de estos términos en los capítulos subsiguientes se hace necesario precisar algunos detalles.

Una topología de red define la manera en la cual los dispositivos de red están organizados para facilitar las comunicaciones entre ellos. Una topología de red LAN define la manera de transmisión de datos través de una red LAN. Hay

topologías de red LAN que son las más comunes y solo las vamos a mencionar: Bus, Estrella, Anillo, Árbol y Mesh.

4.1.5.-Protocolos de transmisión en redes LAN.- Son las reglas de comunicación entre dispositivos en una red LAN. Estos protocolos integran los diversos pasos en las comunicaciones, tales como el formateo del paquete de datos, el tiempo y la secuencia de envío de paquetes y la resolución de errores de estado.

a) Carrier Sense Multiple Access (CSMA). Tiene dos variaciones funcionales: CSMA/CA y CSMA/CD, el cual es un estándar ethernet. En CSMA la estación continuamente monitorea la línea mientras espera enviar un paquete de datos, entonces envía el paquete cuando piensa que la línea está libre, si no recibe el acknowledgment de la estación de destino, asume que una colisión ha ocurrido y reenvía el paquete. A este se define como monitoreo de portadora permanente. Otra versión de CSMA la cual no monitorea persistentemente la portadora se caracteriza porque la estación espera un tiempo aleatorio antes de reenviar el paquete de datos.

b) Polling.- La traducción más adecuada podría ser muestreo, es este método de transmisión, la estación primaria se conecta la secundaria cada cierto intervalo de tiempo predeterminado para ver si tiene alguna información que transmitir. La estación secundaria no está autorizada a transmitir hasta que no tenga el permiso de la estación primaria. Este método era mayormente utilizado por las grandes redes basadas en mainframe, donde justamente el mainframe preguntaba a sus estaciones si tenían algo que transmitirle.

c) Token-Passing.- Usado en las redes Token Ring, FDDI, y ARCNet, las estaciones en una red token passing no pueden transmitir hasta que reciban una trama especial denominada token. Este arreglo previene de los problemas de colisión que se dan en el CSMA. Sin embargo no trabaja bien en redes con muchos nodos.

4.1.6.- Tecnologías de Acceso Remoto.- Estas tecnologías pueden ser definidas como aquellas tecnologías de red que tiene como foco proveer a los usuarios remotos (alejados físicamente, no conectados físicamente) acceso a una

red de datos. Pero manteniendo siempre los principios básicos de Confidencialidad, Integridad y Disponibilidad. Existen numerosas ventajas al emplear métodos de acceso remotos seguros, entre ellos tenemos:

- Reducir costos de red al usar Internet en reemplazo de líneas dedicadas.
- Permitir a los empleados de una empresa estilos flexibles de trabajo tales como el teletrabajo.
- Construir lazos ó sinergias con consumidores, proveedores y empleados.

Tipos de acceso remoto: Existen muchos tipos de métodos de acceso remoto, los cuales comparten los mismos protocolos WAN, vamos a nombrar algunos de los más usados:

a) Dial –up Asíncrono.- Es el método más común de acceso remoto para usuarios personales remotos porque utiliza la red pública conmutada de servicio telefónico, se basa en el usuario a conectarse efectúa una llamada telefónica a un número convenido y establece una conexión via MODEM para la transmisión de datos.

b) ISDN.- Es una tecnología WAN, el ISDN es un protocolo de comunicaciones ofrecido por las empresas de telefonía que permite a las redes de telefonía enviar datos y voz. ISDN tiene dos interfases típicas: Basic Rate Interface (BRI), el cual esta compuesto de dos canales B y un canal D; y el Primary Rate Interface (PRI) el cual consiste en un canal D de 64 Kbps más 23 (T1) ó 30 (E1) canales de voz ó datos.

c) xDSL.- Se les describe como una tecnología WAN, la cual utiliza las líneas regulares de telefonía para un acceso digital a alta velocidad.

d) Cable Modems.- Provee acceso de alta velocidad a Internet a través de las empresas de servicio de televisión por cable. Comparte el ancho de banda del cable coaxial para la transmisión de datos. Es considerado una de los métodos más inseguros porque los “segmentos locales” (compartidos por varios usuarios) no tienen ningún tipo de protección ó filtrado.

e) Wireless.- Esta tecnología es la de más rápido desarrollo y expansión en la actualidad. Los expertos predicen que el número de usuarios conectados a la red a través de dispositivos portátiles (como Laptops, PDAs) eclipsarán el número de computadoras personales conectadas a las mismas redes en un corto número de años. La seguridad es aquí un factor muy importante, porque la tecnología wireless es especialmente susceptible de intercepción y eavesdrooping. Debido a esto los estándares de encriptación y autenticación también se están desarrollando rápidamente. Esta tecnología permite al acceso a las redes LAN ó WAN de dispositivos portátiles que se conectan a través de puntos de acceso (Access Points) estableciendo un enlace por ondas electromagnéticas que viajan a través del aire, se utiliza una amplio rango de frecuencias dependiendo del alcance que se requiera tener.

4.2.- Conceptos de Seguridad de Comunicaciones.- Conforme se iban desarrollando las tecnologías de comunicaciones los requerimientos de seguridad para las transmisiones de información se hacían cada vez mayores, esto trajo como resultado que se desarrollaran diversas tecnologías y protocolos de seguridad, vamos a continuación a revisar varios de los más utilizados.

4.2.1.- Seguridad en los métodos de Acceso Remoto.- Para hacer posible todas estas opciones de conexión remota se han desarrollado diversos métodos de seguridad que nos permiten utilizar todas las facilidades del acceso remoto con la confianza que nuestra comunicación es segura.

a) Dirección restringida.- Este procedimiento filtra a los usuarios no autorizados basándose en la dirección de origen del protocolo (IP ú otro de LAN). Permite solo las llamadas provenientes de las direcciones autorizadas en una lista de acceso. Este procedimiento sin embargo autentica al nodo de comunicaciones pero no al usuario.

b) Caller ID.- Este método, utilizada para filtrar el acceso vía dial up, revisa el número telefónico que origina la llamada, contra una lista aprobada. Este también es uno de los métodos más utilizados porque es muy difícil de evadir. Su mayor desventaja es que muy difícil de administrar cuando se tiene usuarios viajeros, que pueden acceder desde distintos números telefónicos.

c) Callback.- En un escenario callback, cuando un usuario intenta iniciar una sesión se identifica en el sistema con un código de usuario y un password, luego el servidor de acceso da por terminada la llamada y procede a discar al número telefónico registrado para ese usuario. Al igual que los anteriores este método autentica al nodo no al usuario y es muy difícil de administrar para usuarios viajeros.

4.2.2.- Tecnologías para la Autenticación e Identificación de los accesos remotos.- Son tecnologías que son muy necesarias en seguridad para verificar quien se está comunicando remotamente. Debido a que el acceso remoto presenta innumerables desafíos a la seguridad, se han desarrollado una amplia gama de tecnologías que presentan soluciones a esos desafíos. La identificación se refiere a conocer quien está intentando la conexión (está asociado al concepto de código de usuario), y la autenticación a estar seguros de que efectivamente quien está intentando acceder es quien dice ser (está asociado al concepto de password ó contraseña), de esta manera se pueden establecer niveles de acceso, asociado a estos conceptos tenemos también el de no repudiación que implica que cada usuario debe ser asumir la responsabilidad de sus acciones.

Protocolos de seguridad para los nodos remotos.- Los siguientes son los más usados:

a) Password Authentication Protocol (PAP).- Es un protocolo de seguridad para acceso remoto que brinda autenticación e identificación a un nodo que está intentando establecer una conexión. Utiliza un password "reusable" (lo cual actualmente se considera una vulnerabilidad) para la autenticación, tampoco encripta el user-id ni el password durante la comunicación.

b) Challenge Handshake Authentication Protocol (CHAP).- Es considerado una evolución del PAP, utiliza un proceso de autenticación más seguro que el PAP, basado en un proceso de dialogo desafío/respuesta no reusable para identificar al nodo que está intentando establecer una conexión remota. El protocolo CHAP es a menudo utilizado para establecer una conexión de red a red y en las redes de tipo xDSL, ISDN y Cable Modems.

4.2.3.- Sistemas de Autenticación de acceso remoto.- Cuando la demanda de acceso remoto a las redes aumentaba, hicieron su aparición dos sistemas de de

administración de estos accesos, TACACS y RADIUS, los cuales surgieron para una base de datos centralizada, la cual contuviera las listas de usuarios, passwords y perfiles de usuarios. Estos sistemas son "estándares base" lo cual significa que pueden interoperar con otros sistemas del mismo tipo. A continuación los describiremos brevemente.

a) Terminal Access Controller Access Control System (TACACS).- Es un protocolo de que brinda autenticación para acceso remoto y servicios adicionales tales como el registro de acciones (auditoria ó logging). En un sistema TACACS los passwords de usuarios son administrados en una base de datos central en lugar de cada uno de los nodos de acceso. Un dispositivo que trabaja dentro de un arquitectura que utiliza TACACS pregunta al usuario remoto por su código de identificación de usuario y su password, luego este dispositivo pregunta al servidor TACACS para verificar estos datos. TACACS no soporta el cambio de password ni el uso de passwords dinámicos.

b) TACACS + .- Es la evolución del TACACS desarrollado por CISCO (lo cual lo hace propietario) que adicionalmente provee de las siguientes mejoras:

El uso de una autenticación de dos factores
La posibilidad para el usuario de cambiar de password
La posibilidad de usar password dinámicos
Mejores registros de auditoria (Audit Trails) y registro de las acciones de los usuarios.

c) Remote Authentication Dial-Up User Service (RADIUS).- Fue adoptado como un protocolo estándar por el Internet Engineering Task Force (IETF). Provee similares facilidades de autenticación de usuarios (incluyendo el uso de password dinámicos) y administración que el TACACS+. Es un sistema distribuido cliente/servidor en el cual los nodos de acceso (clientes) envían sus requerimientos de autenticación hacia un servidor central de RADIUS el cual contiene los datos de los usuarios y los servicios asociados (basados en listas de control de accesos ACLs). RADIUS es un protocolo totalmente abierto, su código fuente es distribuido y puede ser modificado para trabajar con cualquier sistema disponible en el

mercado. Puede ser usado con TACACS + y Kerberos , brindando además autenticación con CHAP.

RADIUS sin embargo no soporta los siguientes protocolos:

AppleTalk Remote Access Protocol (ARAP)
NetBIOS Frame Protocol Control Protocol (NBFCP)
Netware Asynchronous Service Interface (NASI).

4.2.4.- Sistemas de Password Dinámico.- También llamados sistema OTP (One time password) estos sistemas obligan al usuario a utilizar un password ó contraseña diferente cada vez que requieran autenticarse, para lograr esto se tienen varios estándares ó sistemas que generan a la vez passwords diferentes para los usuarios y están sincronizados con los mecanismos de autenticación, esta sincronización puede ser función de una secuencia ó del tiempo.

4.2.5.- Criptografía.- La criptografía es la disciplina que tiene objeto proteger la transmisión de la información de modo que solo pueda ser leída y entendida por el destinatario, para esto se suele utilizar modelos matemáticos de diversos tipos, ó equipos mecánicos (forma ya en desuso). La criptografía es una ciencia bastante antigua los primeros datos de su uso se remontan a 3000 años atrás por los egipcios, pero las primeras técnicas militares se remonta a unos 2500 años en Esparta con el sistema de cifrado llamado "Scytale". Actualmente la criptografía alcance el nivel de una ciencia con muchos elementos de alta matemática y alta tecnología involucrados en su desarrollo.

a) Métodos de encriptación.- Hay innumerables métodos de encriptación, muchos surgen cada día y otros caen en desuso por el constante avance del poder computacional, los cuales tornan en simples y rápidos los modelos matemáticos que eran considerados complejos y difíciles. Las dos principales tecnologías criptográficas son las de llave simétrica y la de llave asimétrica.

i) Encriptación Simétrica (Secret Key).- Es el tipo de encriptación que es familiar para la mayoría de personas. En este tipo de criptografía, el remitente y el receptor de la información comparten el conocimiento de una llave de encriptación (llave secreta). El

remitente encripta el texto plano del mensaje con la llave secreta y el receptor descencripta el mensaje con la misma llave secreta. Obviamente el desafío es mantener el secreto de la llave de encripción. Para incrementar la seguridad la llave secreta puede ser cambiada frecuentemente. Idealmente solo debe ser usada una vez. Debido a las nuevas tecnologías de computación cada vez se hacen más necesarias utilizar llaves de mayor longitud (> a 128 bits) La principal desventaja de esta tecnología es que no brinda autenticación ni no repudiación. Entre los más métodos más usados de encripción por llave simétrica tenemos:

Data Encryption Estándar (DES) .- Es quizá el más popular y conocido fue desarrollado en el año 1972 a partir del algoritmo Lucifer desarrollado por IBM. Utiliza el Data Encryption Algorithm (DEA), que fracciona la información en bloques de una longitud estándar y sobre esos bloques aplica el algoritmo utilizando una llave de 128 bits (actualmente), es un método recursivo desarrollado inicialmente para ser aplicado por hardware y que nos da 2 elevado a la 128 posibilidades de llaves de encripción, lo cual si bien hasta hace unos años era muy difícil de romper por ataques tipo fuerza bruta, actualmente ya no lo es por lo que ya prácticamente está en desuso, y solo se utiliza en implementaciones comerciales de media y baja criticidad. [2]
El DES opera en 4 modos:

- **Cipher Block Chaining (CBC).-** Opera con bloques de datos de 64 bits. Utiliza un vector de inicialización aleatorio de 64 bits para el primer bloque a encriptar el cual es unido al segundo bloque con un simple XOR evitando de esta manera hacer predecible los datos, y luego el segundo bloque lo une al tercero y así sucesivamente.[2]
- **Electronic Code Book (ECB).-** Es el modo nativo del DES y un cifrador en bloques, es usualmente aplicado para encriptar los vectores de inicialización ó las llaves de encripción, se aplica a bloques de datos de 64 bits,

los cuales son separados en dos vectores de 32 bits cada uno, los cuales son mezclados para producir dos bloques de 48 bits cada uno, los cuales son encriptados con una llave de 48 bits.[2]

- **Cipher Feedback Mode (CFB).-** En esta forma el texto cifrado de un bloque es usado como un parámetro de entrada junto con la llave del siguiente texto a cifrar.[2]
- **Output Feedback (OFB).-** Es parecido al anterior pero no utilizada el primer texto cifrado en combinación con la llave sino con el nuevo texto encriptado en una suma tipo XOR. [2]

3DES.- Es el sucesor natural del DES debido al avance de las facilidades de procesamiento de datos. Es básicamente aplicar al texto a cifrar tres veces consecutivas el estándar DES con algunas variaciones, ó cambios de llaves en cada una de las etapas de encriptación.

Advance Encryption Standar (AES).- Es el sucesor real del DES y fue desarrollado a partir de una convocatoria que hizo en el año 1997 el National Institute of Standards and Tecnology (NIST) para lograr un método fuerte de encriptación que reemplazara al DES y fuera aceptado como un estándar para las diversas organizaciones dentro de los EEUU. En Marzo del año 2000 el NIST anunció al ganador el cual fue el Rijndael desarrollado por los belgas Joan Daemen y Vincent Rijmen.

Este algoritmo fue diseñado para tener las siguientes propiedades:

- Resistencia contra todos los ataques conocidos
- Diseño Simple
- Código compacto y velocidad sobre una amplia variedad de plataformas.

El Rijndael puede ser catalogado con un cifrador iterativo sobre un bloque de datos de longitud variable con una llave variable los cuales son independientes entre sí y pueden ser

de 128, 192 ó 256 bits. En términos decimales existen aproximadamente 3.4x10^38 llaves posibles de 128 bits y 1.1x10^77 llaves posibles de 256 bits.

International Data Encryption Standar (IDEA).- Es un algoritmo considerado seguro , cifra en bloques de 64 bits con una llave de 128 bits, el cual fue desarrollado por James Massey y Xuelia Lai en 1992. Y que aún es ampliamente utilizado especialmente en sistemas comerciales y el muy conocido PGP del correo electrónico.

ii) Encriptación Asimétrica (Public Key).- Esta tecnología de encriptación utiliza dos llaves, una llave pública y una llave privada. La llave pública es conocida por todas las entidades que necesiten encriptar y enviar un mensaje. La llave privada es utilizada para desencriptar el mensaje, la principal ventaja que tiene es que elimina la necesidad del intercambio de llaves. Hay que tener en consideración que:

- La llave pública no puede desencriptar el mensaje que está encriptado.
- Idealmente la llave privada no puede ser derivada de la llave pública.
- La llave privada debe mantenerse privada.

La criptografía de llave pública se basa en las funciones de un sentido, estas funciones son fáciles de calcular en un sentido pero muy difíciles de hacerlo en sentido inverso. Por ejemplo si tenemos y = f(x) debe ser fácil obtener y si se tiene x, pero muy difícil obtener x a partir de y.

Se han desarrollado un gran número de algoritmos de llave pública, algunos son aplicables a firmas digitales otras a encriptación de mensajes ó a ambos. Estos sistemas por su complejidad matemática son muchos más lentos que los sistemas de llave secreta. Sin embargo se han desarrollado sistemas híbridos que utilizan la criptografía de llave pública para distribuir seguramente

las llaves secretas de un sistema de criptografía simétrica. A continuación nombraremos a algunos de los más importantes:

RSA.- Es un algoritmo derivado de los apellidos de los inventores (Rivest, Shamir, Addleman), se basa en la dificultad de factorizar un número N, el cual es producto de dos número primos grandes (de 200 dígitos cada uno) Luego la dificultad de obtener la llave privada de la llave pública es muy grande ya que equivale a la dificultad de encontrar los factores primos del número N. Se usa para encriptación, intercambio de llaves y firmas digitales.

Diffie- Hellman.- Es un método de intercambio de llaves sobre un medio no seguro sin exponer las llaves y mediante la utilización de una llave adicional denominada llave de sesión. De manera similar al RSA utiliza número primos grandes.

El Gamal.- Es una versión extendida del Diffie-Helman que se ha difundido ampliamente ya que nunca estuvo patentada, se basa en la utilización de logaritmos discretos.

b) Firmas Digitales.- El propósito de las firmas digitales es detectar modificaciones no autorizadas de data así como autenticar la identidad de los participantes en la comunicación asegurando mecanismos de no repudiación. Las firmas digitales se basan en la generación de un bloque de datos más pequeño que el mensaje original y es originado a partir de este. Para generar la firma digital, el sistema pasa el archivo a ser enviado a través de una función hash de un sola vía. Esta función hash produce un bloque de salida de una longitud fija (message digest) sin importar la longitud del mensaje de entrada, este mensaje de salida tiene las siguientes características:

La función hash es considerada de una sola vía porque el mensaje original no puede ser recreado a partir del mensaje de salida.

Dos archivos no pueden originar el mismo mensaje de salida ya que es función del contenido del archivo.

El mensaje de salida puede ser nuevamente calculado a partir del mensaje original.

Luego de la generación del mensaje de salida, este es encriptado con la llave privada del remitente, luego es adjuntado al mensaje original y enviado al receptor. El receptor luego desencripta el mensaje generado por la función hash utilizando la llave pública del remitente, si esta operación es satisfactoria, se ha comprobado la identidad del remitente. A continuación el receptor procede a calcular a partir del mensaje original y mediante la función hash el message digest, si este es idéntico al enviado como parte del mensaje total se comprueba que el mensaje no ha sido modificado.

Los dos algoritmos de firma digital más utilizados son los siguientes:

SHA-1.- Utiliza el Digital Signature Algorithm (DSA) basado en una modificación del El Gamal. Produce un message digest de 160 bits para cualquier mensaje menor a 2^64 bits.

Tiene las siguientes propiedades:

- Es computacionalmente imposible encontrar el mensaje original a partir del message digest.
- Es computacionalmente imposible encontrar dos mensajes que produzcan el mismo message digest. [3]

MD5.- Es un algoritmo de message digest que fue desarrollado por Ronald Rivest en 1991. Genera un message digest de 128 bits a partir de un texto de cualquier longitud, para el proceso divide la data en bloques de 512 bits y los procesa en cuatro distintas formas. [3]

4.2.6.- Certificados digitales .- Los certificados digitales son el equivalente digital del DNI, en lo que a la autentificación de individuos se refiere, ya que permiten que un individuo demuestre que es quien dice ser, es decir, que está en posesión de la llave privada asociada a su certificado.

Para los usuarios proporciona un mecanismo para verificar la autenticidad de programas y documentos obtenidos a través de la red, el envío de correo encriptado y/o firmado digitalmente, el control de acceso a recursos, etc.

Un "certificado de llave pública" es un punto de unión entre la llave pública de una entidad y uno o más atributos referidos a su identidad. El certificado garantiza que la llave pública pertenece a la entidad identificada y que la entidad posee la correspondiente llave privada.

Los certificados de llave pública se denominan comúnmente Certificado Digital, ID Digital o simplemente certificado. La entidad identificada se denomina sujeto del certificado o subscriptor (si es una entidad legal como, por ejemplo, una persona).Los certificados digitales sólo son útiles si existe alguna Autoridad Certificadora (Certification Authority o *CA*) que los valide, ya que si uno se certifica a sí mismo no hay ninguna garantía de que su identidad sea la que anuncia, y por lo tanto, no debe ser aceptada por un tercero que no lo conozca. Es importante verificar que una autoridad certificadora ha emitido un certificado y detectar si un certificado no es válido. Para evitar la falsificación de certificados, la entidad certificadora después de autentificar la identidad de un sujeto, firma el certificado digitalmente.

Los certificados digitales proporcionan un mecanismo criptográfico para implementar la autentificación; también proporcionan un mecanismo seguro y escalable para distribuir claves públicas en comunidades grandes.[4]

4.2.7.- Infraestructura de llave Pública (PKI).- Es la integración de las firmas digitales y de los certificados, así como de los otros servicios requeridos por el Comercio electrónico. Estos servicios proveen integridad, control de acceso, confidencialidad, autenticación, y no repudiación para las transacciones electrónicas. Incluye los siguientes elementos:

Certificados digitales
Autoridad Certificadora (CA)
Registros de autorización
Políticas y procedimientos
Revocación de certificados
Soporte a la no repudiación

4.2.8- Protección y Controles.- Este dominio de la seguridad se refiere a los controles que son necesarios para proteger los recursos de una red ó sistema de datos (hardware, software) de las siguientes amenazas:

- Vulnerabilidades en los ambientes operativos
- Intrusos internos ó externos.
- Usuarios autorizados que hagan uso inapropiado de sus privilegios.

Categorías de Controles.- Las siguientes son los principales categorías de controles de seguridad operativos.

Preventivos.- Están diseñados para disminuir el impacto de un error no intencionado en el sistema y para prevenir el acceso no autorizado interno ó externo al sistema.

Detectivos.- Se utilizan para detectar un problema una vez que este se ha producido. A diferencia de los controles preventivos operan luego de la ocurrencia y sirven para el rastreo de acciones ó para minimizar el impacto mediante la identificación rápida. Un ejemplo de este tipo de control son los logs de auditoria.

Correctivos.- También llamados de recuperación, son diseñados para minimizar el impacto de una pérdida a través de procedimientos de recuperación.

Controles Directivos (Deterrent Controls).- Son utilizados para asegurar el cumplimiento de normas externas (reguladoras). Estos controles complementan a otros tales como los preventivos y los detectivos.

Controles de Aplicación.- Son controles diseñados dentro de una aplicación de software para minimizar y detectar problemas operativos del mismo software, entre los controles de este tipo tenemos a los "Controles de Transacción" que se utilizan para lograr control sobre las varias etapas de una transacción y son los siguientes: Entrada, proceso, salida, cambio, prueba.

4.2.9.- Recomendaciones del Orange Book.- [4] Este criterio desarrollado y utilizado por el Departamento de Estado de los Estados Unidos, recomienda determinados mecanismos de control sobre los procesos operativos de un sistema de procesamiento de datos, y se refiere no solo al tipo de arquitectura de los sistemas a utilizar sino sobre todo a procesos ó procedimientos administrativos que deben ser tomados en cuenta para mantener la seguridad de una red de comunicaciones de datos, vamos a tomar los siguientes como los más relevantes para el desarrollo de este trabajo.

a) Administración Segura y Confiable.- Se puede definir como la asignación segura de las tareas necesarias para la gestión de un sistema de información. Estas recomendaciones varían de acuerdo al nivel de seguridad del sistema (B2, B3, ó A1). Para este trabajo vamos a tomar las que deben tenerse en cuenta para mantener los niveles de seguridad de una red corporativa.

Separación de Funciones.- Asigna partes diferentes de las labores a personas diferentes, estas labores deben ser complementarias, de este modo se asegura que una sola persona no pueda comprometer todo el sistema. Se relaciona con el concepto de menor privilegio en el sentido que la persona solo debe tener los accesos necesarios para realizar la labor asignada. Lo principal es mantener las funciones de administrador del sistema de las de administrador de seguridad, y donde el sistema no lo permite efectivamente se deben tener procedimientos de control y registro para asegurarse esta separación de funciones.

Rotación de Funciones.- Considera que las personas asignadas a determinadas tareas deben ser cambiadas de función luego de un tiempo determinado para evitar que las personas que cumplen tareas complementarias puedan ponerse de cuerdo para eventos fraudulentos.

b) Restauración Confiable.- Este recomendación busca asegurar que no se den brechas de seguridad en el proceso de restauración de un sistema que hubiera tenido problemas. El reinicio de un sistema no debe comprometer el esquema de seguridad adoptado. Tiene dos actividades primarias que son mandatarias y son las siguientes:

- Anticipo de fallas.- Implica estar preparado para una falla del sistema, y puede consistir en tener respaldos periódicos de la información crítica, y procedimientos que aseguren la recuperación del sistema luego de una falla, asimismo que se tienen los elementos necesarios para una vuelta a operación normal del sistema.

-Recuperación del Sistema.- Generalmente dependen de los requerimientos del sistema e incluyen lo siguiente:

- Reinicio del sistema en Single User Mode para no permitir otros accesos hasta estar seguros del funcionamiento total y real del sistema.
- Recuperación de todos los file systems que se encontraban activos al momento de la falla.
- Recuperación de las características de seguridad propias del sistema.
- Revisión de todos los archivos críticos para asegurar que el nivel de acceso a ellos es el adecuado.

c) Administración del Control de Cambios.- Es el proceso para asegurar que en el sistema se realizan los cambios debidamente autorizados y probados. Este implica identificar, controlar y auditar todos los cambios hechos al sistema tanto de hardware como de software, de comunicaciones, y cualquier otro cambio. El control de cambios también puede ser utilizado para proteger un sistema crítico mientras este es desarrollado. Los procesos principales de esta función son:

- Asegurar que el cambio será implementado de una manera adecuada y luego de haber aprobado las pruebas necesarias.
- Asegurar que las instancias adecuadas están notificadas y enteradas del cambio que se va a realizar.
- Analizar el impacto del cambio en el sistema luego de su implementación.
- Reducir el impacto negativo que pueda tener el cambio en los servicios y recursos del sistema.

4.2.10.- Controles de Operación.- Los controles de operación involucran los procedimientos diarios de protección a los recursos de un sistema de información.

a) Protección de Recursos.- Este concepto tal como su nombre lo indica, protege los recursos de un sistema de información de pérdidas ó compromisos. Los recursos de un sistema de información involucran el hardware, software y la data que es utilizada ó de la que es dueña la organización. A través de la protección de recursos se trata de reducir las posibilidades de daño de la información que pueda ocasionar un acceso no

autorizado ó alteración de la data. Los recursos que requieren protección son los siguientes:

- Recursos de Hardware.-

- Comunicaciones, lo cual incluye routers, firewalls, gateways, switches, modems y servidores de acceso.
- Medios de almacenamiento, sistemas de storage, discos fijos y discos removibles, tapes.
- Sistemas de procesamiento, lo que incluye servidores de archivos, de correo, de Proxy, de backup.
- Estaciones de trabajo y sus periféricos.
- Impresoras y fax.

- Recursos de Software

- Código fuente y librerías.
- Software propietario y paquetes.
- Sistemas operativos y utilitarios.

- Recursos de Información

- Archivos de backup
- Archivos de los usuarios
- Archivos de seguridad
- Directorios de sistema operativo
- Sistemas de registro de eventos y auditoria.

b) Controles de Hardware.- Son los controles que se deben tener asociados a los recursos de hardware y son:

- **Mantenimiento del Hardware.-** El mantenimiento de los sistemas requieren de acceso físico ó lógico al sistema por parte del personal de soporte y operaciones, proveedores y otros. Es por eso necesario conocer el background del personal que tendrá acceso y supervisar y tener conocimiento de cada intervención, activando los registros de auditoria necesarios.
- **Cuentas de usuarios mantenimiento.-** Muchos sistemas traen por default cuentas de usuarios de mantenimiento con altos niveles de privilegios sobre el sistema, estas cuentas a menudo vienen por password también default que ya son muy conocidos. Es crítico realizar el cambio de estos password

default y deshabilitar las cuentas de mantenimiento hasta que sean necesarias.

- **Control de los Puertos de Diagnóstico.-** Muchos dispositivos de hardware traen consigo puertos de diagnostico, generalmente son puertos asíncronos ó de consola a través de los cuales se puede acceder directamente al hardware del equipo. El acceso a estos puertos debe ser restringido solo permitido al personal debidamente autorizado.
- **Control Físico del Hardware.-** Se deben implementar ambientes seguros en los cuales se instale el hardware , esto es usual en una empresa grande que por lo general cuentan con un Datacenter, gabinetes y racks para proteger sus equipos.

c) Controles de Software.- Son un elemento importante de de la seguridad operativa y están referidos al control del software que va a ser utilizado en el sistema. Elementos de control de software son los siguientes:

- **Administración Antivirus.-** Si el personal puede cargar ó ejecutar cualquier tipo de software en el sistema este estará más expuesto a problemas de virus, gusanos, troyanos y a software no autorizado, por lo que se debe tener un buen sistema de gestión al respecto.
- **Prueba y revisión del Software.-** Debe existir un proceso formal de prueba del software para determinar la compatibilidad de las aplicaciones existentes y de las nuevas aplicaciones ó modificaciones requeridas por el sistema (software upgrade)
- **Utilitarios del Software.-** Los utilitarios pueden comprometer la integridad de los sistemas y los controles de accesos lógicos. La utilización de los mismos debe estar regulada por política.
- **Protección de fuentes y data.-** Se debe implementar una combinación de controles de acceso físico y lógico para asegurarse que el software y las copias de seguridad no pueden ser modificadas sin autorización.

d) Controles de Privilegios Especiales.- Los privilegios especiales están referidos a los accesos especiales que por la naturaleza de su función

deben mantener los operadores y administradores. Entre estos tenemos el acceso a comandos del sistema, a configuración de parámetros. Estos controles deben estar dirigidos a minimizar la cantidad de usuarios con este tipo de acceso y a controlar el uso de los mismos, esto puede hacerse por procedimiento ó registros de auditoria si el sistema no lo permite.

4.2.11.- Monitoreo y Auditoria de la Seguridad.- El monitoreo y la auditoria son dos conceptos de mucha utilidad para la seguridad, nos permiten identificar los problemas y poder hacerles un seguimiento adecuado para lograr solucionarles y tomar medidas concretas para evitar ó minimizar su posterior ocurrencia.
El monitoreo contiene los mecanismos, herramientas y técnicas que nos van a permitir la identificación de los eventos de seguridad y cual puede ser su impacto en el sistema. También incluye las acciones para identificar los elementos de importancia y poder hacer un reporte adecuado del problema.

a) Técnicas de Monitoreo.- Son varias las que usan en la actualidad, y tienen un uso y tecnología específicas para cada necesidad. Entre ellas tenemos:

Detección de Intrusos.- Es una técnica que nos da gran ayuda para el análisis detectivo de los eventos de intentos de intrusión. Puede ser usado no solo para la identificación de los intrusos sino también para crear ó determinar patrones de tráfico. Mediante el análisis de las actividades ocurridas fuera de lo que es usual un analista de seguridad puede encontrar evidencia de eventos no autorizados.

Pruebas de Penetración.- Es un proceso para probar las defensas de una red intentando accesar al sistema desde el exterior utilizando las mismas técnicas que un hacker puede utilizar, a este tipo de pruebas también se le denomina “ethical hacking”. Mediante este prueba se puede tomar una foto exacta del estado de la seguridad de un sistema en un momento particular. Algunas de las técnicas empleadas en esta prueba son las siguientes:

- **Scanning y Probing.-** Normalmente requiere la utilización de una herramienta denomina scanner que prueba por que puertos

es probable realizar una conexión y de esta manera obtener información acerca de la estructura de la red y posiblemente lograr accesar a recursos que tiene puertos IP abiertos.

- **Demon Dialing.-** Es una técnica para probar las conexiones remotas dial up, se basa en el discado de todas las líneas telefónicas de la empresa para encontrar modems dispuestos a aceptar una conexión.
- **Sniffing.-** Es el análisis del tráfico de un segmento de red al cual es capturado mediante un analizador de protocolos, a través de la captura de estos paquetes de datos se espera recolectar información sobre usuarios y password, sobre la arquitectura de la red ó información en general.
- **Dumpster Diving.-** Es la revisión de la información escrita desechada por los usuarios en los escritorios ó basureros, a través de ellos se pueden conseguir información relevante sobre la empresa.
- **Ingeniería Social.-** Es quizá la técnica más utilizada y muchas veces la más efectiva y consiste en conseguir la información directamente de quienes la poseen mediante artimañas de tipo psicológico (preguntas y situaciones ficticios ó suplantando a otros usuarios) a modo de una estafa ó fraude normal.

b) Análisis de Violación.- Una de las técnicas mas utilizadas para detectar anomalías en las actividades normales de los usuarios es el registro de acciones, violaciones e intentos por parte de los usuarios y su posterior análisis. Para un correcto análisis es necesario fijar umbrales de uso normal o rutinario cuando estos umbrales son excedidos entonces se debe producir una alarma ú alerta. Estos niveles de umbral también son utilizados para detectar variaciones de comportamiento. Los siguientes son algunos tipos de violaciones que deben ser registradas, procesadas y analizadas:

- Errores repetitivos que excedan los niveles umbrales.
- Individuos que intentan exceder sus niveles de autorización.
- Cantidad de usuarios por encima del umbral intentando acceder a recursos del sistema.
- Patrones que indiquen intentos serios de intrusión.

c) Auditoria de la Seguridad.- Toda implementación de seguridad en un sistema debe necesariamente con un sistema de auditoria que permita registrar, controlar y monitorear los eventos y acciones de los usuarios y los procesos del sistema. Los sistemas de auditoria se basan principalmente en la generación de registros de auditoria (audit trails) que registren todas los eventos relevantes de los usuarios y que permitan tener hacer un seguimiento a modo de historia de las acciones (trace). Se consideran elementos relevantes las adiciones, eliminaciones, ó modificaciones de información relevantes del sistema, para hacer posible esto cada usuario debe estar debidamente identificado en el sistema mediante un user-id único que permite la individualización de responsabilidades. Asimismo y de igual modo que el monitoreo, permite la identificación de problemas ayudando a su resolución.

Los registros de auditoria deben registrar lo siguiente:

- La hora y fecha del evento
- Quien generó el evento
- Desde que Terminal fue generado el evento (dirección IP y hostname)
- Información relevante con el evento en sí.

Otras características a tomar en cuenta en los audit logs son:

- Retención y protección de los registros de auditoria por un tiempo adecuado. Si existen normas regulatorias estas son mandatarias.
- Protección adecuada contra la alteración de los registros de auditoria.
- Protección contra la indisponibilidad del sistema de auditoria durante un evento.

Resumen del capítulo

Hemos podido revisar brevemente los términos de datanetworking más importantes para este trabajo y hemos podido conocer las diversas tecnologías de acceso remoto y la seguridad asociada a esas tecnologías, asimismo las técnicas más usadas de encriptación, los controles necesarios para minimizar los riesgos en las redes de datos y los métodos de prueba de seguridad de las redes. Finalmente se describe la importancia y forma que debe tener un sistema de registro de auditoria de eventos que nos permitirá detectar incidencias y tomar las medidas correctivas necesarias.

CAPÍTULO V
CONSIDERACIONES Y ETAPAS DE IMPLEMENTACION DE LA RED DE SEGURIDAD PERIMETRAL - CASO TIM PERU

Partiendo de las consideraciones de diseño definidas en el capítulo anterior, se va ahora a definir las etapas de implementación de esta estructura de seguridad perimetral, la definición de etapas se hace necesaria ya que para montar la solución completa no solo requiere de una gran inversión sino de la maduración de las necesidades de comunicación de una empresa la cual conforme la empresa se va asentando y manteniendo una presencia en el mundo virtual y real son cada vez mayores, esto también puede variar de acuerdo al rubro de negocio de la empresa ó de la orientación de servicios que quiera ofrecer, así hoy en día, tenemos empresas que no tienen oficinas reales sino virtuales y todos los servicios que ofrecen están dados por ese medio, para tipo de empresas dedicadas el e-business sus prioridades son muy distintas.

En el caso de TIM PERU se tiene un presupuesto anual de Gastos de Inversión, el cual se presentaba a mediados del año precedente por lo que se consideró que la red perimetral tendría un crecimiento marcado por los presupuestos aprobados año tras año en un periodo de 4 años que era el que la empresa consideraba como periodo de inversión y se podía contar con un presupuesto adecuado para lograr una buena estructura de seguridad perimetral.

La empresa inició operaciones en el mes de Agosto del año 2000 pero el lanzamiento comercial se realizó en Enero del año 2001, para el lanzamiento comercial ya se tenía la estructura básica y fundamental de servicios hacia Internet, los servicios considerados eran los de correo electrónico y navegación web, por lo que el esquema de funcionamiento era muy básico.

A continuación describiremos etapa por etapa el crecimiento de la red de datos perimetral, lo cual estuvo muy marcado por los requerimientos comerciales:

5.1.- Inicio de Operación – 2000 – 2001.- Al inicio de operaciones de la empresa se planteó como necesidad básica contar con dos servicios esenciales de Internet, el de correo electrónico y el navegación por Internet, dado que ese momento las prioridades principales de la empresa estaban enfocadas en montar la infraestructura de red celular en Lima y las principales ciudades del país, se optó por un esquema básico que diera las facilidades requeridos, para esto se instalaron dos servidores de correo electrónico en la red interna de la empresa con sistema operativo Windows NT y Exchange y un servidor con sistema operativo Sun Solaris en un equipo Sun Ultra 450 y con software de firewall Checkpoint 4.1 . No se implementan aún reglas de seguridad avanzada solo se protege el perímetro, se permiten la salida solo a través del puerto 80 y se autorizan las Ip's de los usuarios autorizados a navegar, no existen filtros de navegación, se autoriza el envío y recepción de correos a través del puerto 25. Este esquema se detalla a continuación:

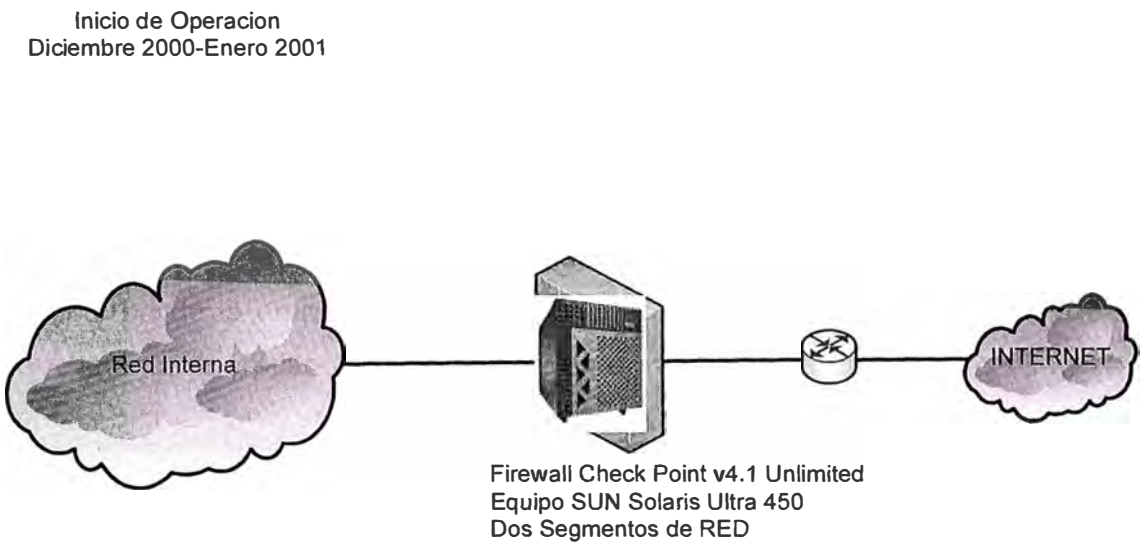


Figura 5.1.- Esquema inicial de la red de seguridad perimetral.

5.2.- Segundo Semestre del Año 2001 .- Posteriormente este esquema básico se vió reforzado con la inclusión de un servidor de Proxy para permitir la navegación Internet a un mayor número de usuarios a la vez que se mantenía el esquema inicial de tener la red con DHCP, este servidor de Proxy fue el primero en la empresa con Sistema operativo Windows 2000 sobre el que corría el Windows Proxy Server, adicionalmente se montó sobre este mismo servidor el software de filtrado de acceso a Internet, de la empresa Websense que permitía fijar reglas de navegación a los usuarios sobre Internet, se establecieron perfiles de acceso de acuerdo a la función (8 perfiles) y se prohibió el acceso a páginas de correos electrónicos gratuitos y categorías no relacionadas con el negocio.

También se crearon dos segmentos en la red perimetral, denominados como es usual DMZ (Red desmilitarizada), en este caso las redes DMZ1 y DMZ2 en las cuales se instalaron los primeros servidores de servicios en Internet, desde un inicio se optó por establecer una arquitectura de tres capas en los servidores de servicios Internet, en la red DMZ1 que es la que "da la cara" hacia Internet solo se deben poner las páginas estáticas, en la DMZ2 los servidores que tienen la lógica de la aplicación y en la red interna las Bases de datos ó información en general. Se optó por utilizar para estos servidores el sistema operativo Linux en su versión Red Hat debido a su flexibilidad en cuanto a la configuración, es decir nos permite instalar solo los componentes que son necesarios en cada servidor de acuerdo a la función especializada que cumplen adicionalmente por presentar menor cantidad de vulnerabilidades que otros sistemas operativos, y sobre todo por presentar facilidad en el cambio de versión y aplicación de parches de actualización. (Service packs) El software de presentación web adoptado fue el Apache, por presentar facilidad de actualización, configuración y compatibilidad con el Red Hat, no detallamos las versiones porque estas fueron mudando a lo largo del año de acuerdo a las necesidades de seguridad.

Simultáneamente ese año se cambió el esquema de correo electrónico de la empresa en cuanto a arquitectura, estableciéndose 4 servidores de correo interno que efectúan un relay hacia un quinto servidor los correos dirigidos hacia Internet (correos externos) siendo este servidor el único autorizado a enviar y recibir correos externos. Este servidor se hallaba aún en la red Interna.

Finalmente se estableció que la base de datos de autorización de usuarios para los servicios de red fuera la Microsoft ya que conformaba la mayor parte de los servicios de red interna (los servicios de red interna Intranet) y las aplicaciones desarrolladas in-house, se estableció un sistema de autorización de acceso y auditoria denominado TIM Accesos que controla el acceso a todos los desarrollos locales. Asimismo se fijaron políticas de seguridad a los usuarios restringiendo el uso de los puertos USB, disketeras y quemadores de CD, de igual modo se restringieron los privilegios administrativos sobre los equipos para evitar la instalación de software no autorizado.

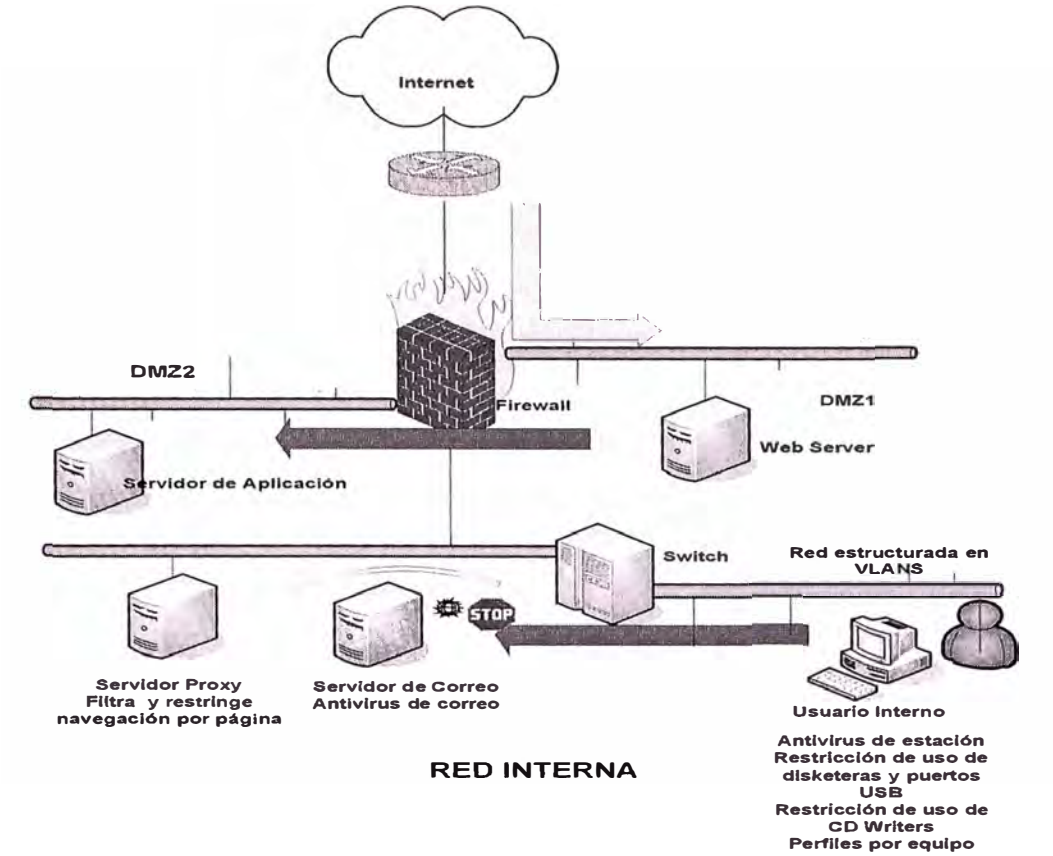


Figura 5.2 Diagrama de la red perimetral para finales del año 2001

5.3.- Primer Semestre del año 2002.- A partir del año 2002 se inició un proceso de mejora continua en la arquitectura de la red perimetral, lo primero que se consideró prioritario fue darla alta disponibilidad a los sistema de firewall y para esto se estimó necesario cambiar el equipamiento presente hasta ese momento, se hizo al análisis respectivo se optó por mantener como elemento de firewall al sistema de Checkpoint pero basado en un hardware de alta disponibilidad y rendimiento, por esto se compraron dos equipos Nokia IP440 que trabajan compartiendo la carga y en caso de fallas uno solo de los equipos puede mantener la carga presente. Se continuó manteniendo el Checkpoint 4.1

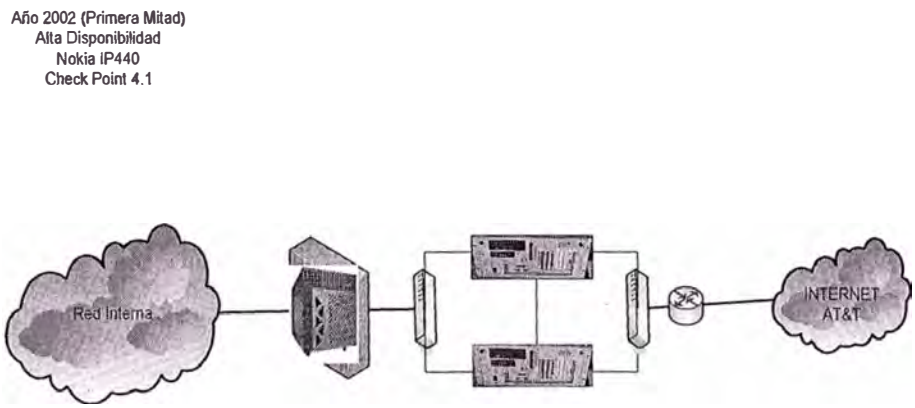


Figura 5.3 Esquema de la red perimetral en el primer trimestre del 2002

5.4.-Segundo Semestre del 2002.- Se implementan los primeros sistemas de Detección de Intrusos, luego del análisis se instaló el sistema Real Secure versión 6.0 de la empresa Internet Security Systems, se utiliza como plataforma servidores HP con procesador Intel DL380 y con sistema operativo Windows 2000, se compran tres licencias, se instala uno en la red externa, entre el firewall y el router, el segundo en la DMZ1 donde están los equipos que son la cara hacia Internet y el tercero en la red Interna en el enlace central de las Tiendas propias (Mundos TIM) con los servidores centrales, debido principalmente a problemas con virus informáticos. Junto a estos equipos se instalan sus consolas de administración y monitoreo y se instala un servidor de syslogs para los IDS y los firewalls, este servidor es un Windows 2000.

Paralelamente y por estrategia corporativa se separan la red de transmisión de datos corporativa de la red de transmisión de datos de los equipos que conforman la plataforma de servicios celulares, quedando está última bajo la responsabilidad del área de RED. Por lo que se tiende un enlace (como si fuera hacia un tercero) hacia la red de datos de la RED.

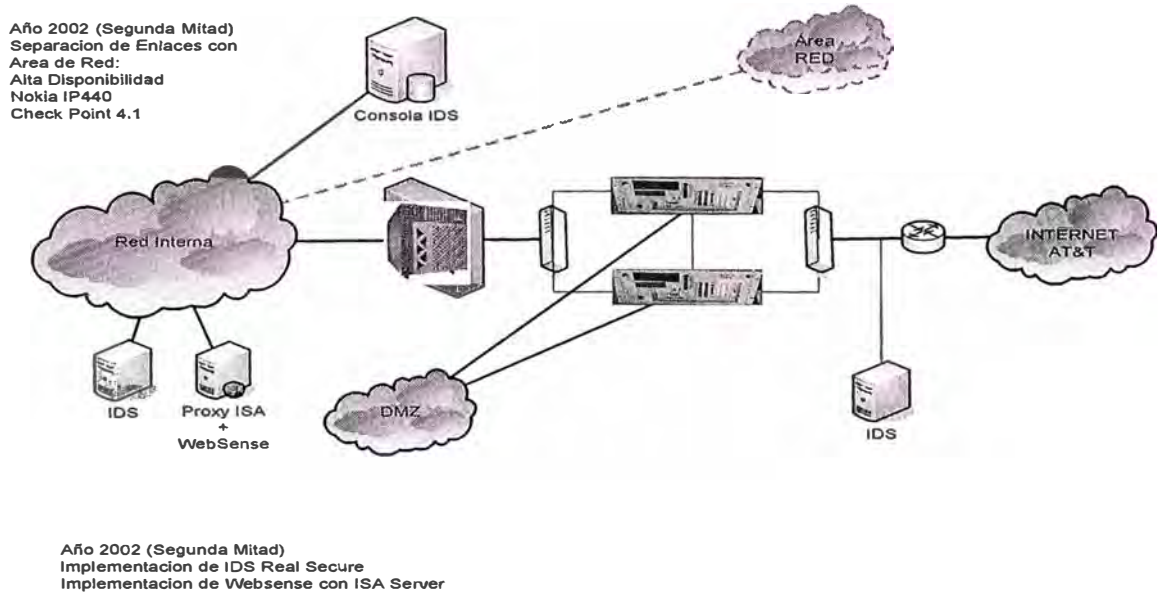


Figura 5.4 Diagrama de la red hacia la segunda mitad del año 2002

Incluso antes de finalizar el año 2002 se efectuaron algunos cambios adicionales ya que el servidor de Proxy que controla los servicios que los usuarios obtienen de Internet fue migrado hacia el nuevo Sistema Microsoft ISA Server, este sistema no solo es un Proxy sino que tiene funciones de firewall (algunas empresas pequeñas lo utilizan de este modo) por lo que podían brindar mayores facilidades a lo usuarios internos en cuanto a la

utilización de servicios adicionales tales como ftp, webcasts, conexiones a servicios que utilizan puertos especiales (Infocorp, Reniec, Ransa) dejando de lado los enlaces dedicados configurados para algunos de ellos inicialmente. Paralelamente a todo estos cambios se efectuó la migración de la arquitectura de servicios internos para montar una red Windows 2000 con la implementación de Directorio Activo, que nos brinda muchas mayores facilidades de autenticación y autorización de usuarios a los servicios de red, todos los servidores fueron migrados hacia este nuevo sistema operativo.

En detalle el nuevo esquema es el siguiente:

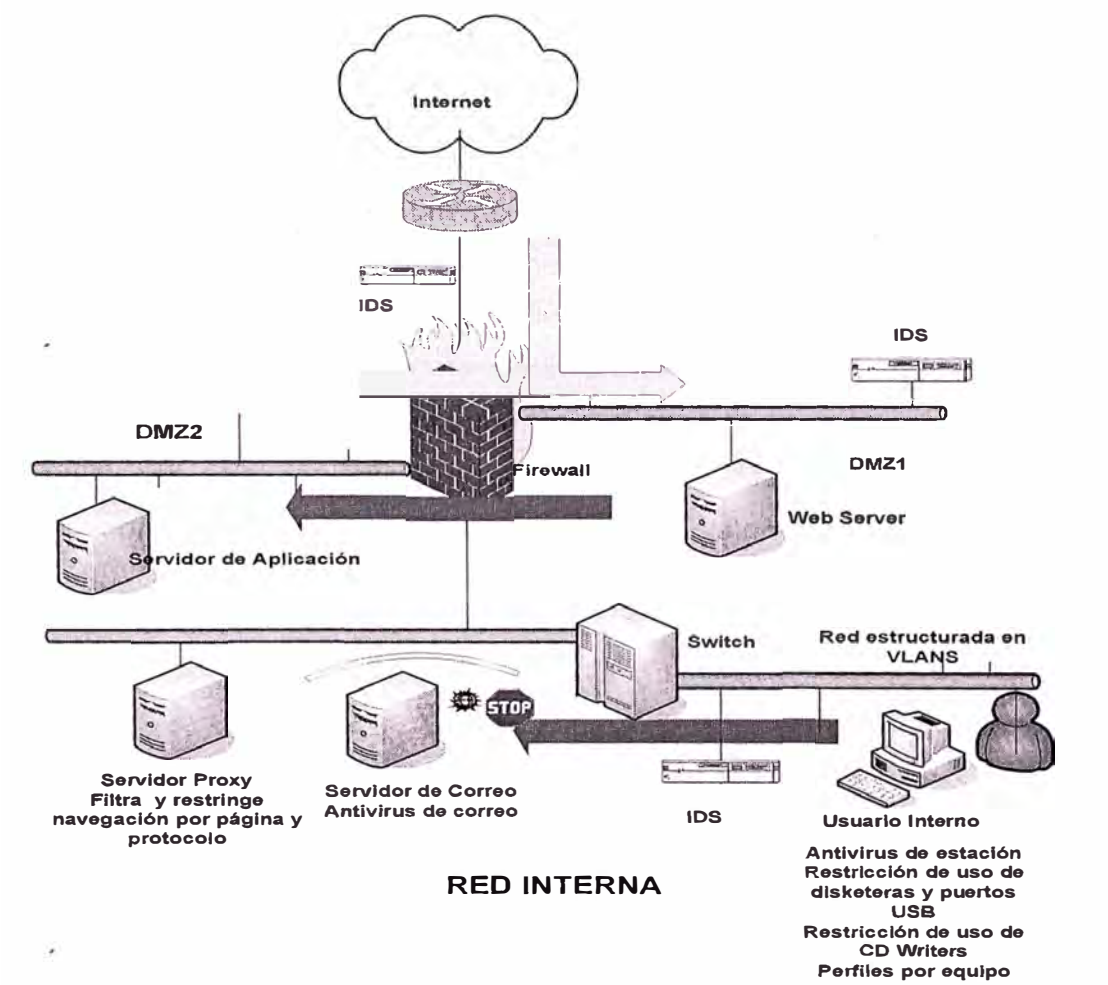


Figura 5.5 Esquema de la red para finales del año 2002

5.5.- Arquitectura de la red de datos para el año 2003.- El primer cambio que se consideró fue el de ampliar la capacidad de hardware de los firewalls dado el incremento del tráfico de Internet hacia el sitio web de TIM, para eso migró la plataforma de los equipos Nokia IP440 a equipos Nokia IP710 manteniendo la misma configuración de alta redundancia. Ahora bien el incremento de tráfico se debía principalmente a la gran demanda de clientes y no clientes para enviar mensajes SMS gratuitos desde la página web de TIM (www.tim.com.pe) hacia los teléfonos celulares de la empresa. Esto implicó

que también se tuviera que pasar a un esquema de granja de servidores, asimismo para aprovechar la gran cantidad de personas que accedían a los servicios informativos web se monta una Tienda Virtual donde se venden equipos y tarjetas virtuales de recarga, (para el pago se redirecciona el pedido a los bancos y entidades emisoras de tarjetas y través de un enlace SSL, y se recibe la respuesta a través del enlace que se instaló con BancaRed) Para los servidores web si bien se mantuvo la plataforma de servidores HP con procesador Intel y sistema operativo Red Hat se pasó del servidor web Apache a uno proporcionado por la empresa BEA y denominado WebLogic que en el futuro nos permitiría montar con mayor rapidez nuevos servicios web para nuestros clientes, esta migración se hace respetando la arquitectura de tres capas propuesta en un inicio.

Finalmente se monta un nuevo sensor IDS en el enlace que la RED va a mantener hacia Internet y que servirá temporalmente como enlace alterno a la falla del principal, hacia este enlace se destinan los equipos IP440 de Nokia sobre los cuales se pone Checkpoint 4.1.

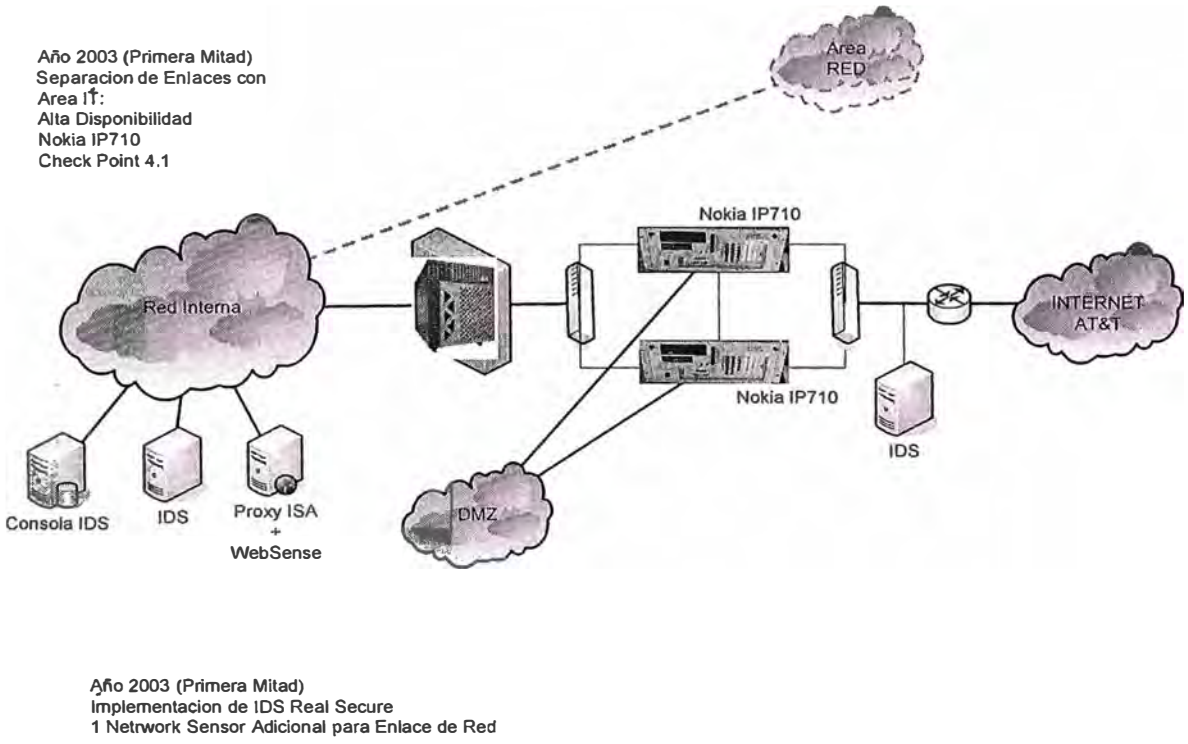


Figura 5.6 Diagrama de la red perimetral para la primera mitad del año 2003

Paralelamente a estos se cambios implementó un sistema de seguridad para el correo electrónico que a la vez es antivirus, antispam y de gestión de correo, el sistema que se eligió es el IMSS (Internet Messaging Security Suite) de la empresa TrendMicro que es la

empresa lider en este rubro a nivel mundial. Para esto fue necesario colocar un nuevo servidor de correo en la DMZ1 el cual es un servidor HP con procesador Intel y sistema operativo Linux Red Hat, asimismo se cambió la configuración que el servidor Exchange que anteriormente redireccionaba los correos hacia Internet solo los pueda reenviar hacia este nuevo servidor. Finalmente cuenta con un elemento que puesto sobre el servidor de Proxy nos permite filtrar los posibles virus y gusanos que puedan descargarse desde páginas webs. (Interscan Web Security Suite)

Se crearon nuevos segmentos DMZ para atender las necesidades de establecer enlaces con la red de Bancos (BancaRed) ya que se establecieron convenios con los principales bancos tanto para facilitar el pago de servicios a nuestros clientes como para posibilitar la venta de Pines de recarga virtual en todas las ventanillas y cajeros automáticos de los principales bancos, este enlace llega a la DMZ2. Los servidores de lógica de negocios de los web servers fueron migrados hacia la nueva DMZ5 (básicamente por un tema de capacidad de los switches).

Igualmente durante ese año se inaugura la red de acceso remoto para los usuarios móviles y los establecimientos de ventas de terceros (partners de negocio de TIM) la forma principal de acceso es vía dial up a través de la red conmutada local de telefonía fija ó a través de la red propia de telefonía GSM, para este servicio se contó con un hunting de 60 líneas de las cuales 20 son para la red conmutada de telefonía fija y 40 para la red celular GSM. Para controlar el acceso se montó un servidor RADIUS de Cisco, (Ciscosecure versión 2.6) y a través de Listas de acceso se manejaban los servicios a los que tenían acceso, para darle un mejor nivel de seguridad se montó un sistema basado en passwords dinámicos (OTP) se eligió la de la empresa RSA y el sistema Secure-ID, este sistema trabajo con pequeños dispositivos electrónicos denominados Tokens los cuales en una pantalla van mostrando una serie de 6 números los cuales cambian cada 60 segundos, estos números son función del número de serie del Token, de la fecha, hora y una semilla propia para cada empresa y debe encontrarse sincronizado con el servidor central, el password de acceso lo conforman este número cambiando más un código fijado por el usuario y de valor entre 4 y 6 digitos por lo que la longitud total del password es de mínimo 10 y máximo 12 caracteres. Este sistema de control del acceso remoto se montó sobre servidores HP con procesadores Intel y sistema Windows 2000.

A continuación el esquema final para el año 2003

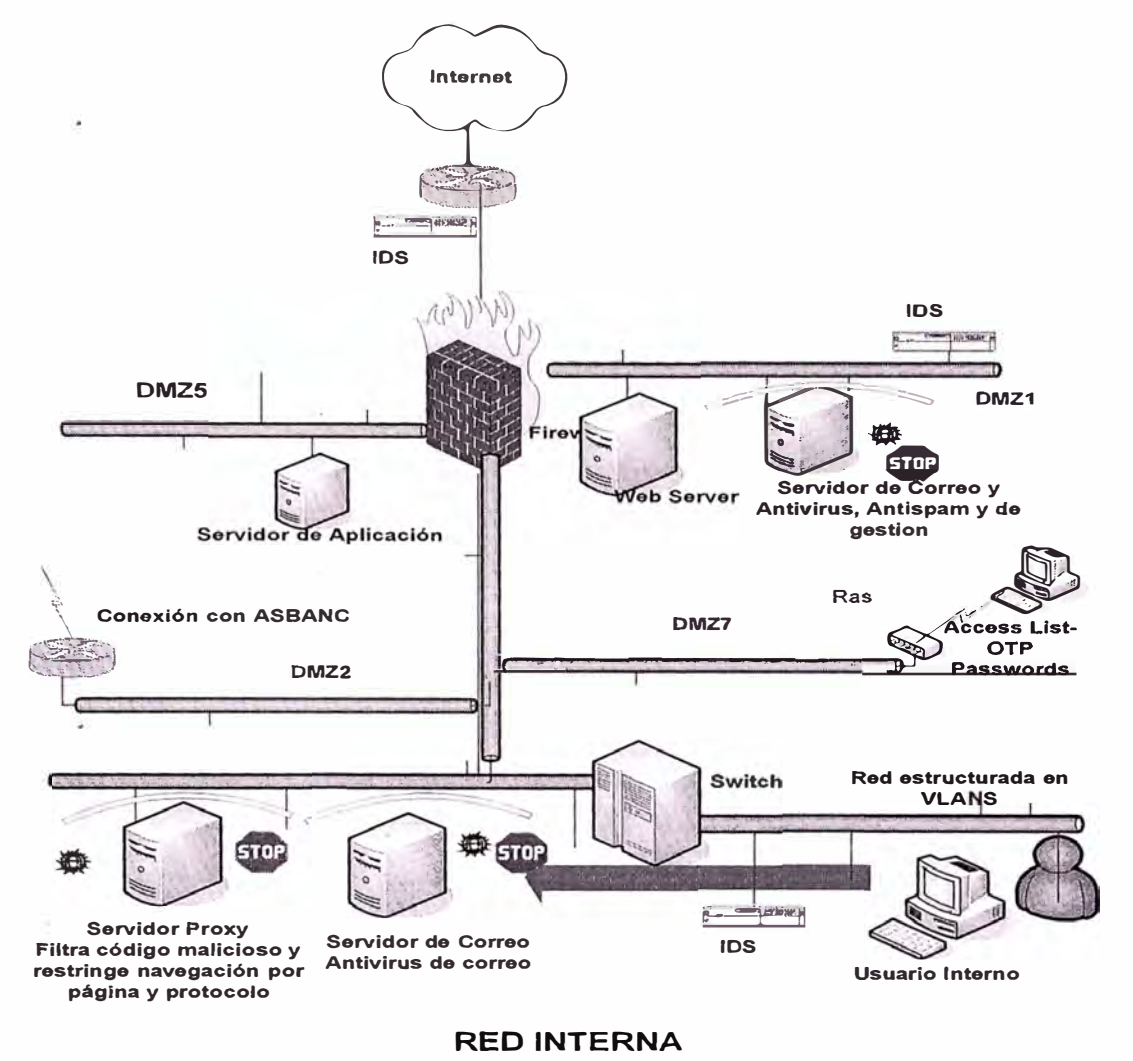


Figura 5.7 Diagrama de la red perimétrica final para el año 2003

5.6.- Arquitectura de la red de datos perimetral para el año 2004.- Ese año no se tuvieron muchos cambios ya fue un año clave para la organización de TIM a nivel de América Latina, el grupo empresarial TIM (Telecom Italia Mobile) es parte del grupo Telecom Italia que agrupa a más de 200 empresas de todas las ramas de las telecomunicaciones, es el 5 operador de telefonía celular en el mundo y tiene empresas en Europa, América, África y Asia, ese año se empezaron a dar cambios organizacionales importantes derivados principalmente del cambio de dueños del conglomerado Telecom Italia producido el año anterior, lo primero fue relacionar a las empresas del grupo con el fin de obtener sinergias entre ellas y empezar con el establecimiento de políticas y estándares corporativos. Uno de los primeros pasos fue la creación de la organización TIM LATAM y de una red corporativa dedicada que uniera a todas las empresas del grupo en América Latina (similar determinación se tomó a nivel de los continentes) este fue el objetivo prioritario de ese año a nivel de redes de comunicaciones. Es así que para poder enlazarnos con las otras empresas de grupo se

establecieron enlaces dedicados con TIM LATAM (con sede en Brasil) para este enlace se creó una nueva DMZ denominada DMZ6 y se montaron nuevos firewalls Checkpoint NG FP3 sobre hardware Nokia IP530, la gestión de estos firewalls estaría bajo nuestra responsabilidad si bien los políticas serían fijadas de modo corporativo.

Por nuestra parte y en paralelo a lo anterior ese año se había programada la migración de la versión del software de firewall Checkpoint de la versión 4.1 a la versión NG FP3 (New Generation FP3) este trabajo se realizó durante el 2 trimestre de ese año. Finalmente se cambió el sistema de IDS Real Secure 6.0 sobre hardware HP con procesador Intel y Sistema Operativo Windows a los nuevos dispositivos de hardware propietario y especialmente diseñados para la función de IDS y que trabajaban en la versión 7.0 del Real Secure.

Paralelamente se empezó a utilizar un sistema de acceso remoto para nuestros principales distribuidores autorizados a través de Internet y utilizando servidores de VPN Linux (distribución libre) y con el apoyo del sistema Metaframe. Por último para la optimización del ancho de banda se instaló un equipo de monitoreo y división de ancho de banda de acceso a Internet de la empresa Packteer.

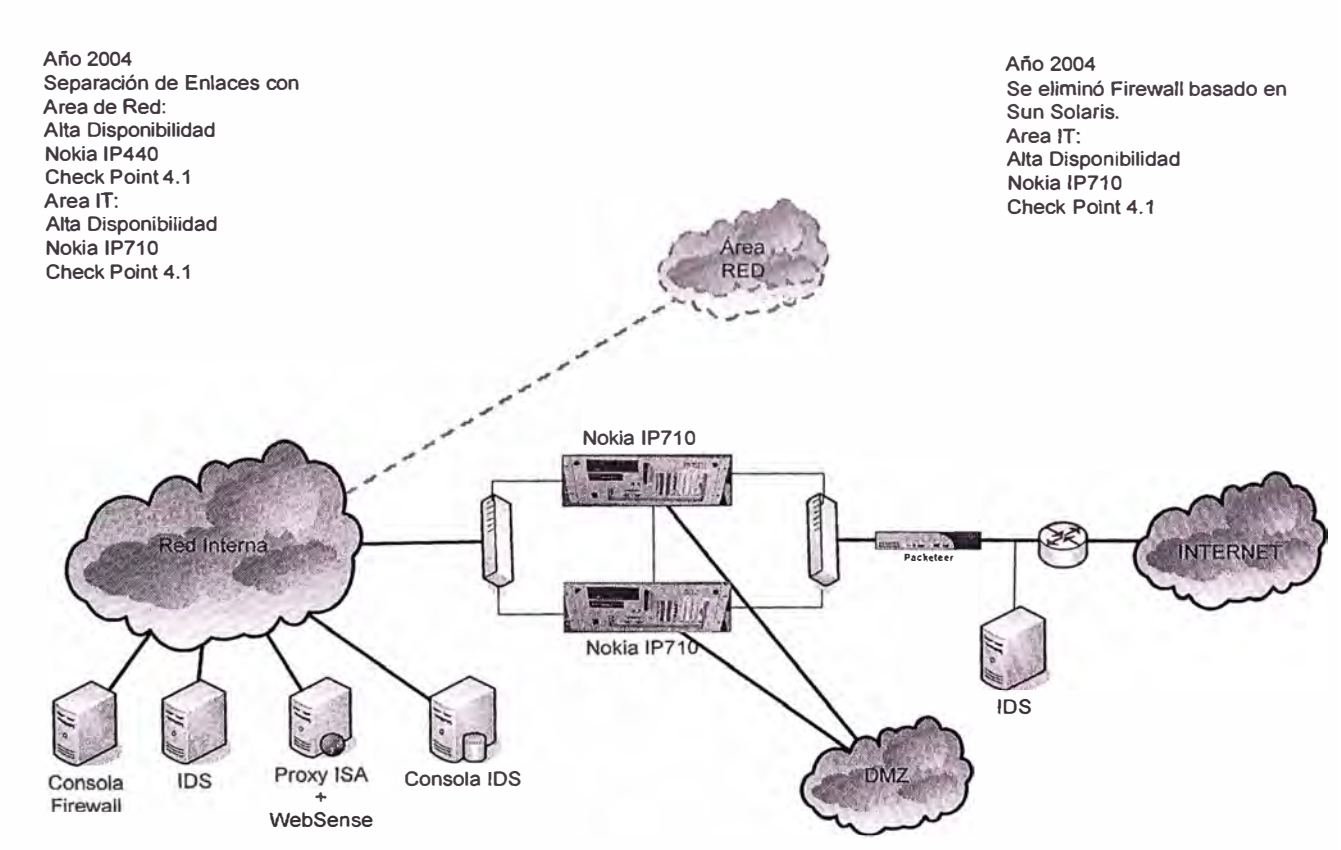


Figura 5.8 Diagrama de la red para el año 2004

5.7.- Primer Semestre del año 2005.- Las necesidades de negocio forzaron a diversos cambios en las redes de comunicaciones entre ellos se tuvo la necesidad de habilitar nuevas redes DMZ para los enlaces con nuestros proveedores se servicios de desarrollo y soporte de usuarios (DMZ3). Así como la DMZ7 para los nuevos servicios de acceso remoto VPN, RAS, GSM y GPRS (una funcionalidad de la telefonía celular GSM que transmite los datos de manera digital directamente).

Durante la primera mitad del año se procedió a instalar 7 IPS (Intrusion Prevention System) destinados a proteger 7 puntos estratégicos dentro de la red de América Móvil Perú, estos equipos IPS son la evolución de los anteriores sistemas IDS, es un plataforma de hardware propietario nuevo del mismo fabricante Internet Security Systems (ISS) con el software Real Secure 8.0 (Site Protector)

Segmento Internet (1 IPS): Tiene la función de proteger contra las principales amenazas (tráfico malicioso) provenientes de Internet, tales como hackers, virus, gusanos, troyanos, spyware, malware y amenazas híbridas (ataque sobre vulnerabilidades), para mantener la data segura de intrusos. Desde entonces el tráfico malicioso hacia la red interna se ha visto reducido en gran manera.

En la DMZ-1 (1 IPS): Para proteger contra todo el tráfico malicioso que esté dirigido hacia los servidores de acceso público existentes este segmento (Servidores Web, Correo, etc). Cabe recordar que gran parte de los ataques de seguridad a los sistemas dentro de una organización provienen en más de un 70% desde la misma red interna (ISS).

En la DMZ-2 (1 IPS): Para proteger contra todo el tráfico malicioso proveniente de la Red de Bancos (BANCA RED – RED ASBANC) tanto de entrada como de salida.

En la DMS-3 (1 IPS): Para proteger contra todo el tráfico malicioso que pueda provenir desde el enlace con las redes de los Partners (IBM, Siemens, Novatronic, TeamSoft, etc) y viceversa.

En la DMZ-6 (1 IPS): Para proteger contra todo el tráfico malicioso que pueda provenir desde la red de LATAM (Italia) y viceversa.

En la DMZ-7 (1 IPS): Para proteger contra todo el tráfico malicioso proveniente de las conexiones entrantes por GPRS, RAS, VPN, etc y viceversa. Recordar que estas conexiones provienen de cualquier punto de Internet

Segmento Internet del Área de Red (1 IDS): Para proteger contra todo el tráfico malicioso proveniente del segmento externo del Área de Red (Internet IMPSAT).

Adicionalmente, como parte del proyecto de implementación de los 7 IPS arriba mencionados, fue necesaria la instalación de la consola de administración de los IPS. Mediante esta consola se llevará a cabo la administración y monitoreo de los equipos IPS, así como también la aplicación de las políticas de seguridad para ellos.

También se procedió a la instalación del servidor WebTrends Firewall Suite. Éste es un reporteador de los logs del firewall y que sirve para analizas los registros de todos los paquetes que pasan a través del firewall.

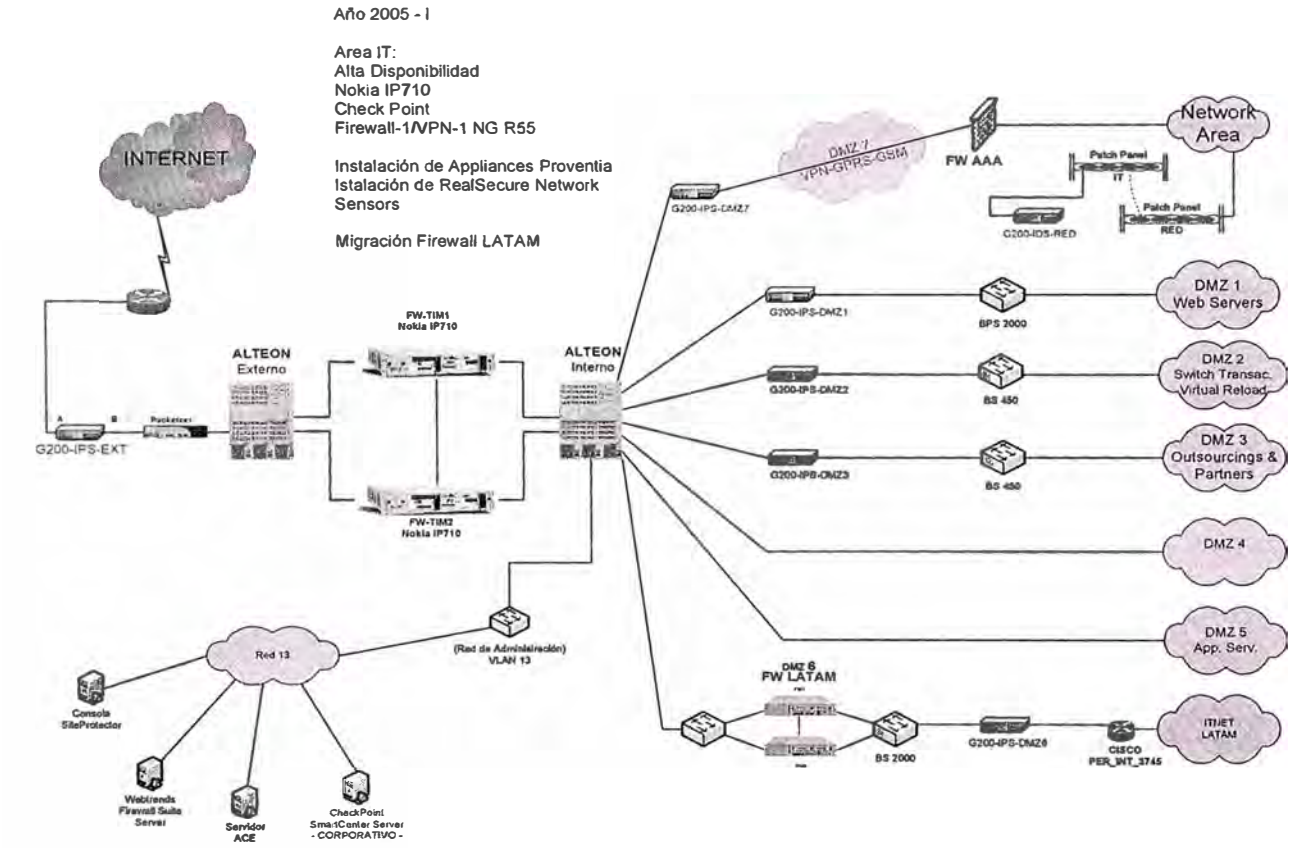


Figura 5.9 Diagrama de red para el primer semestre del año 2005

5.8.- Segundo Semestre del año 2005.- Este fue una etapa muy atípica ya que algunos de los proyectos que se tenían fueron detenidos por la venta de la empresa hacia el grupo América Móvil, el cual y como es obvio antes de aprobar inversiones grandes prefería conocer la real situación de la empresa, es por eso que solo se pudieron continuar con los proyectos que ya se habían iniciado en el primer semestre del año 2005 y que ya tenían presupuesto comprometido.

Durante la segunda mitad del año, por motivo de la Implementación de los Switches Alteon en Redundancia, se procedió a reubicar los 7 IPS (Intrusion Prevention System) por lo que a partir de entonces se tenían 2 conexiones físicas a cada DMZ, quedando de la siguiente manera:
DMZ-1: 2 IPS
DMZ-2: 2 IPS
DMZ-3: 2 IPS
Segmento Internet TELMEX: 1 IPS

Para las conexiones VPN de los Dealers (Franquicias y Corners) se implementó un Cluster de Firewall-VPN con Check Point completamente dedicado a estas conexiones. De esta manera se busca liberar de la carga y responsabilidad de dichas conexiones al Firewall Corporativo.

Se implementó un IDS dentro de la red interna de América Móvil Perú, detrás del Firewall Corporativo con el objetivo de filtrar todo el tráfico malicioso proveniente de las conexiones VPN remotas y que escapaban a la protección del IPS externo y adicionalmente se implementó un segundo IDS detrás del Cluster de Firewall-VPN con el mismo objetivo del IDS ubicado detrás del Firewall Corporativo, filtrar todo el tráfico malicioso proveniente de las conexiones VPN. También se implementó un tercer IDS que se colocó en lugar del IPS de la DMZ-7 (que fue reubicado en la DMZ-3) para proteger contra todo el tráfico malicioso proveniente de las conexiones GPRS, RAS, VPN, etc.

Cabe mencionar que si bien los IDS (Intrusión Detection System) pueden monitorear todos lo eventos de naturaleza maliciosa en la red, su capacidad en cuanto al bloqueo de dichos eventos es limitada en comparación a los IPS (Intrusión Prevention System) quienes por su ubicación en la red (In Line) son mucho mas eficientes ante respuestas a ataques de un solo paquete. Se optó por poner estos equipos debido a que los nuevos requerimientos comerciales requerían de mayor cantidad de enlaces remotos por parte de los distribuidores autorizados y para tener mejor rendimiento se optó que estos accesos remotos fueran a través de Internet, este es un esquema temporal que se apoya en el uso del sistema Metaframe Citrix para optimizar el uso del ancho de banda y a la vez nos da un nivel adicional de seguridad ya que los usuarios que acceden por Internet no accedan directamente a los servidores corporativos sino solo a los servidores Metaframe los cuales manejan la petición y establecen los enlaces con los servidores corporativos.

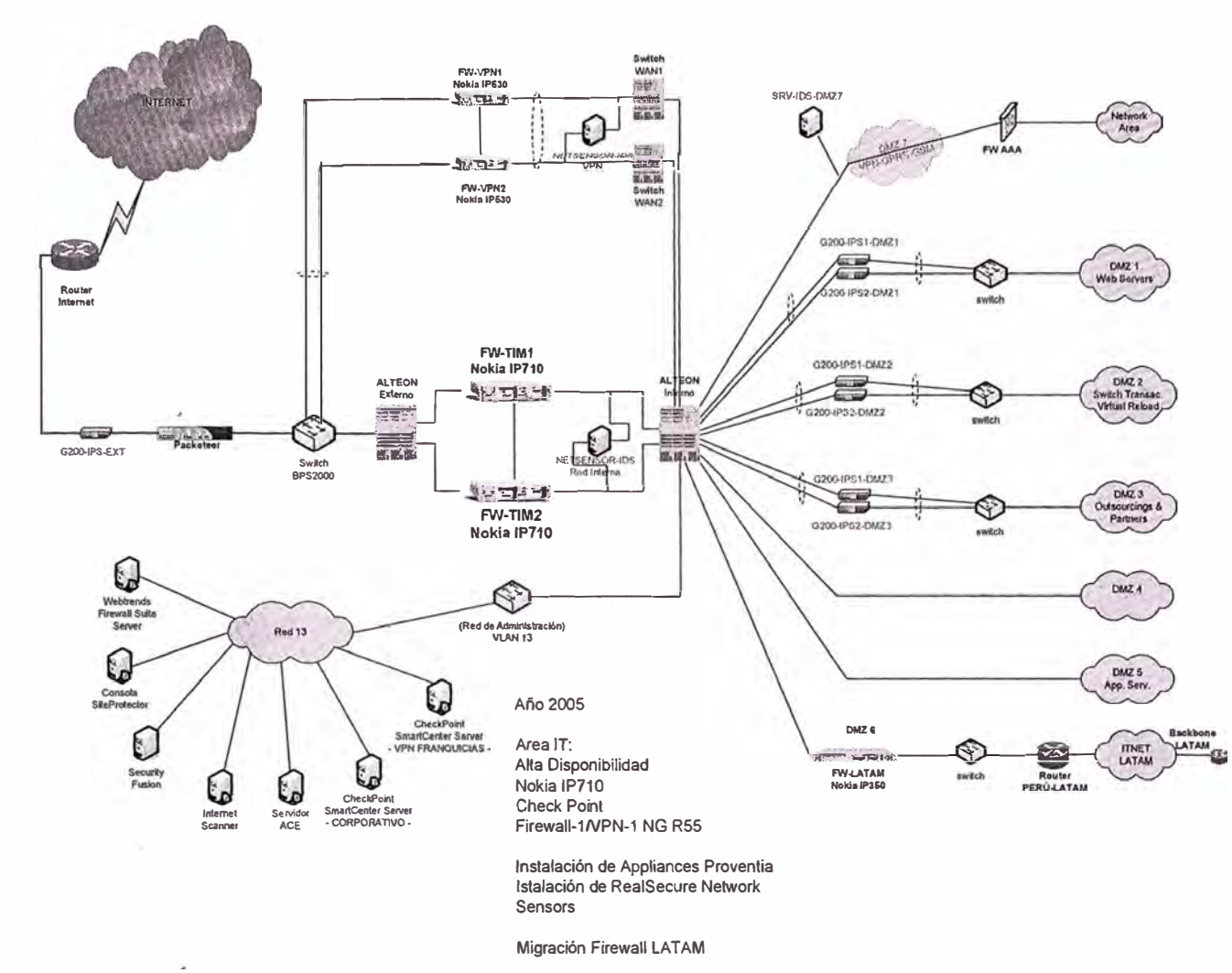
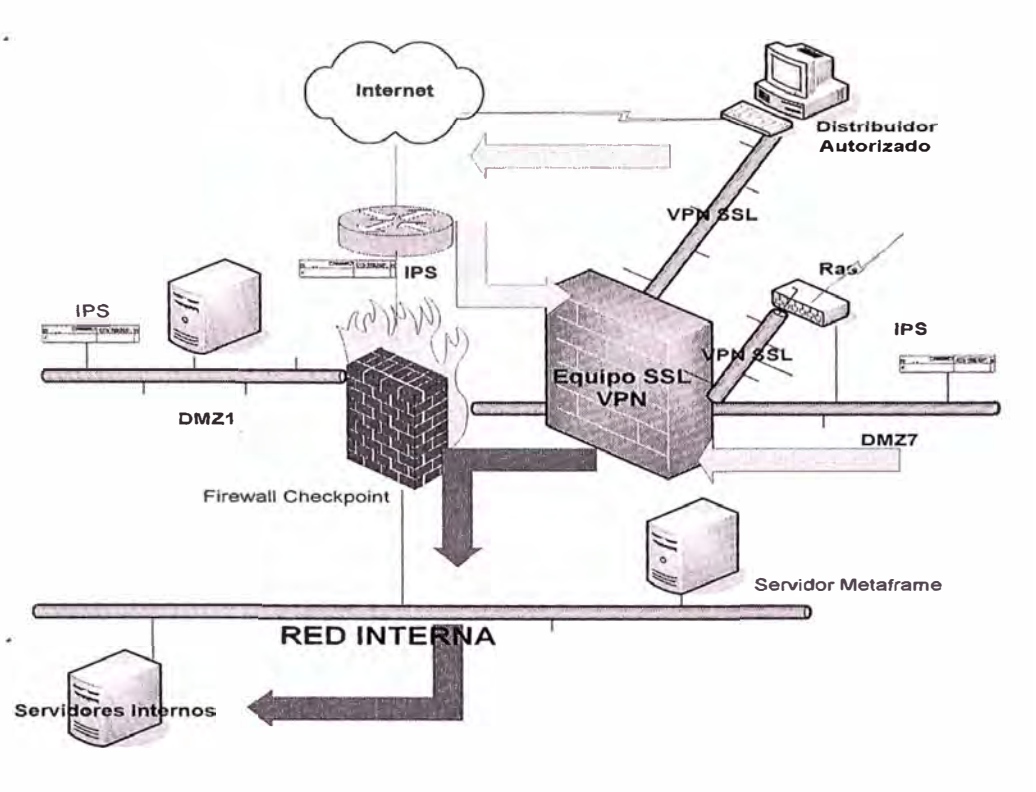


Figura 5.10 Diagrama de la red de seguridad perimetral para el 2005

5.9.- Proyectos Futuros .- Definitivamente se tienen varios proyectos para potenciar y adecuar la red de seguridad perimetral, entre ellos se tienen el de instalar servidores de acceso VPN para nuestros distribuidores autorizados basado en la tecnología VPN sobre SSL la cual ha evolucionado bastante en los dos últimos años, estos sistemas de los cuales tuvimos oportunidad de probar varios (Citrix, F5, Juniper, Nortel) tienen muchas funcionalidades y a la vez garantizan el acceso seguro y confiable a través de Internet, el esquema definitivo que se quiere para la red de seguridad perimetral en el corto plazo es la siguiente:



5.11 Diagrama de la red esperada para la primera mitad de este año.

También se necesita potenciar el parque de equipos IPS para poder cubrir los vacíos dejados por la puesta en funcionamiento de los enlaces redundantes. Y finalmente un sistema correlacionador de eventos mediante el análisis de los registros de auditoria tanto del firewall como de los IPS y los sistemas de seguridad perimetral (IMSS, Proxy, router, etc.) Este fue un proyecto que estaba en marcha de la mano de Telecom Italia quienes ya habían montado un Security Operation Center (SOC) en la ciudad de Milán Italia y el Perú era el primer país a nivel de América Latina que iba a utilizar sus servicios en el sentido de enviarles todos nuestros registros de auditoria y ellos mediante herramientas adecuadas efectuar la correlación para detectar posibles problemas.

Resumen del Capítulo

A través de este capítulo hemos podido apreciar de un modo esquemático el crecimiento y evolución de la estructura de seguridad perimetral de TIM Perú desde sus inicios en el año 2001 hasta los últimos cambios realizados a finales del año pasado. Se puede apreciar el paso desde un esquema simple y sencillo hasta uno bastante complicado y que responde tanto a las necesidades del negocio de la empresa como seguridad ya que para TIM Perú la seguridad siempre fue un elemento de importancia al momento de considerar cualquier proyecto es por eso que la evolución de la red está muy marcada por la evolución de la seguridad en sí.

CAPÍTULO VI
INTERACCIÓN DE LA RED DE SEGURIDAD PERIMETRAL CON LOS SISTEMAS Y APLICATIVOS CORPORATIVOS - CASO TIM PERU

En este capítulo se describen las políticas, estándares, procedimientos y líneas base para los sistemas y aplicativos que son soportados por la red de seguridad perimetral, es necesario tener todo esto claramente especificado puesto que la red de datos se complementa con una arquitectura de aplicaciones adecuada para utilizar adecuadamente las facilidades de seguridad y confiabilidad que brinda.

6.1.- Estándares de desarrollo de aplicaciones.- Una vez fijada la arquitectura de seguridad de la empresa y desplegada la red de comunicaciones perimetral, se hace necesario que las aplicaciones que van a ser soportadas por esta estructura de comunicaciones y seguridad cumplan con determinados estándares de desarrollo para poder realmente utilizar las ventajas de esta red y no debilitar el esquema de seguridad. Como parte de la arquitectura de comunicaciones de la empresa se ha determinada la existencia de varias redes desmilitarizadas (DMZ) cada una de las cuales esta destinada a una función especifica. (Detallado en el capítulo anterior).

Las aplicaciones desarrolladas para dar servicios en la Internet a los usuarios deben cumplir con las siguientes condiciones:

Deben estar desarrolladas en una arquitectura de 3 capas (presentación, lógica de negocio e información) cada una de las cuales estará en una DMZ distinta. Así la primera capa (presentación, páginas estáticas) que es la que interactúa con el usuario estará sobre la DMZ1, la segunda capa (lógica de negocio ó aplicación en sí) estará en la DMZ5 y la capa de información ó bases de datos dependiendo de si la información es también de uso interno ó solo para el uso de la aplicación con cara Internet estará ó en la red interna ó en la misma DMZ5.

La comunicación se realizará entre las tres capas (ubicadas en 3 servidores distintos) solo a través de los puertos expresamente definidos para tal fin.

Los servidores que se utilizarán en los desarrollos de servicios para Internet pueden ser de cualquier arquitectura de procesador pero necesariamente tendrán como sistema operativo Linux en su versión RED HAT y actualizándose constantemente, debiéndose instalar solo los módulos que sean necesarios (actualmente estamos utilizando el Advanced Server).

El desarrollo de los servicios web se hace sobre plataformas Apache salvo para la plataforma central de servicios web para los usuarios la cual será BEA WebLogic Portal. Se ha decidido utilizar estas plataformas por presentar menores vulnerabilidades a incidencias de seguridad lo que mejora grandemente la gestión de seguridad de la misma.

La información sensible de los usuarios, tales como datos de identificación y passwords de acceso deben ser protegidos mediante certificados digitales que encripten la información, se protegen mediante túneles SSL.

Las aplicaciones deben cumplir con los estándares de seguridad para el desarrollo de todas las aplicaciones de TIM Perú.

Estos estándares son los siguientes:

Para las aplicaciones de Internet

Generalidades.-La topología de red de TIM considera la existencia de 3 áreas de red:

- Red Externa
- Red Desmilitarizada
- Red Interna

Entre cada una de las redes se ubicara un firewall que solo permitirá el flujo de la información autorizada y solo por los puertos expresamente permitidos, todos los demás servicios que no sean necesarios serán desactivados. (rige también para el tráfico entre las distintas DMZ)

Para el desarrollo de servicios a través del Internet debe considerarse lo consiguiente:

a) Los servidores que administren páginas web (Information Servers) deben estar ubicados en la red DMZ1, no contener información relevante y tener como sistema operativo Linux de acuerdo a la versión que indique el área de Soporte Técnico que debe ser la más actual. La lógica de la aplicación debe estar en servidores de la DMZ5

b) La información que utilicen estos sistemas sean archivos planos ó bases de datos se ubicaran en un servidor distinto del primero y que necesariamente estará ubicado en la Zona DMZ5 ó en la Interna. El sistema operativo de estos servidores también deberá ser preferentemente Linux y la base de datos Oracle.

c) Los usuarios que ingresan desde Internet solo deben ver el servidor ubicado en la Zona DMZ1, este servidor es el único que puede comunicarse con el servidor de aplicación de la DMZ5 y este a su vez con el servidor de información o Base de datos.
d) Los servidores ubicados en la red DMZ5 solo deben comunicarse con el servidor propio de cada aplicación en la red DMZ5. El acceso a estos servidores desde la red interna estará restringido, sólo estará permitido para los backups, procesos batch de transferencia de información y usuarios administradores.
e) En la configuración de estos servidores se debe tener presente que solo deben estar configurados los servicios estrictamente necesarios para el correcto funcionamiento del sistema. De igual modo deben estar cerrados los puertos TCP/IP que no se utilicen
f) Para las aplicaciones web públicas que requieran la transmisión de información sensible se requiere siempre la utilización de un Certificado Digital expedido por un ente válido y reconocido y la utilización del protocolo https (puerto 443)
g) La comunicación entre los servidores debe ser solo a través de un rango acotado de puertos TCP /IP.

Para las aplicaciones en general

a) No deben existir usuarios ni passwords en plano en archivos de configuración o de otro tipo, no deben utilizarse archivos tipo "ini" en los equipos, en el caso de los servidores con IIS de Microsoft deben referenciar a entradas de registry y no tener los usuarios y passwords en texto.
b) Las conexiones de los sistemas a las Bases de datos se efectuaran mediante un único usuario de conexión, no esta permitida la creación de logins por cada usuario.
c) Los usuarios y password de conexión para el caso de servidores Windows se encontrarán en entradas independientes en el registry y estarán encriptadas.
d) Los usuarios y passwords de conexión para el caso de servidores con sistema operativo UNÍX deberán almacenarse encriptados y el archivo que los contenga solo debe poder ser leído y modificado por el root y el usuario de la aplicación.
e) Los algoritmos válidos de encriptación son los siguientes: DES de 128 bits, rijndael, DES de 64 bits y skipjack, siendo altamente recomendable la utilización solo de los dos primeros. La llave de encriptación debe ser diferente para cada sistema ó servidor y solo de conocimiento del área de IT Security quién la ingresará al sistema para generar el archivo de desencriptación.

f) Todos los desarrollos propios deben trabajar los controles de acceso a través del sistema de TIM ACCESOS, y trabajar los permisos de usuarios y grupos de acuerdo a los estándares de esa aplicación.
g) No se deben utilizar en procesos los usuarios que vienen por default con los sistemas y tienen altos privilegios(sa, administrador, root, etc) se deben crear usuarios propios con características especiales y sólo con los privilegios necesarios.
h) Los sistemas que sean comprados deben contemplar al menos los estándares mínimos de seguridad en cuanto a la autenticación de usuarios y confidencialidad del password de acuerdo a la **"Política de Autenticación de Usuarios"**
i) Para los desarrollos de transacciones en SAP, cada nueva transacción debe incluir sus propios objetos de autorización, y la documentación de los mismos y de las transacciones que invocan si las hubiesen.
j) Todos los sistemas por desarrollarse ó instalarse en TIM deben desde la etapa inicial del proyecto ser analizadas por el área de IT Security.

6.2.- Estándares de configuración de servidores y líneas base de aseguramiento de servidores.- Como ya se mencionó líneas arriba, para reforzar la seguridad se optó por utilizar el sistema operativo Linux en la versión Red Hat como estándar único en los servidores que conforman la red de seguridad perimetral de acceso, esta decisión se basa en la fortaleza que ha demostrado este sistema operativo así como en la facilidad de configuración que posee, no solo en la configuración de parámetros sino en que permite instalar solo aquellas funciones que son requeridas por el sistema ó aplicación a la que va a dar soporte, con lo se minimiza aún más el riesgo de vulnerabilidades propias del sistema operativo.

6.3.- Políticas de seguridad para el intercambio de información.- Igualmente para reforzar la seguridad de la red de seguridad perimetral se ha determinado cuales son las políticas y procedimientos de la empresa para las transferencias de información con otras empresas del grupo, con empresas proveedores ó de servicio, estas transferencias normalmente se dan por la utilización del protocolo ftp ó del ssh (que es la forma segura). Como política se definió que TIM Perú no ofrecía el servicio de recepción de información vía ftp ú otro protocolo, sino que en caso se requiriera efectuar una transferencia de información, sería TIM Perú, la que saldría a "enviar" ó "recoger" la información, según sea el caso. Adicionalmente todas las transferencias de información se realizan previa verificación del área de IT Security.

6.4.- Análisis de Seguridad de Información de los cambios y nuevos servicios. Para mantener los niveles de seguridad para la plataforma de seguridad es necesario que dentro de la metodología adoptada por la empresa, sea propia ó basada en algún estándar del mercado se establezcan niveles de revisión de seguridad para los cambios y nuevos servicios. Nuestra experiencia nos ha señalado que los puntos de revisión de seguridad son en las siguientes etapas de un proyecto:

a) Una vez establecido el documento de especificaciones funcionales, es decir el documento donde se especifica cuales son los requerimientos del negocio ó de soporte para el cambio ó los nuevos servicios. La Unidad responsable de IT Security debe revisar el proceso para verificar que se cumplen las best practices y se va a mantener la seguridad alcanzada como un conjunto de todos los sistemas, los puntos a revisar son principalmente de Seguridad de procesos, (separación de funciones, puntos de control , niveles de auditoria, conformidad del líder usuario de la aplicación).
b) En las etapas del desarrollo ó configuración de la solución a implementar para evitar que se den back doors, ó se incumplan los estándares.
c) En las pruebas funcionales y de carga para verificar que no se tienen problemas en la integridad de la información ó en la confidencialidad de la misma.

Como se ve es todo el proceso debe estar siempre implicada la Unidad de IT Security para lograr niveles adecuados de seguridad de acuerdo a las necesidades de negocio de la empresa. Es un hecho que en toda revisión de seguridad siempre se va a tener riesgos detectados y no todos los riesgos detectados en estas etapas es posible mitigarlos antes del proceso de pase a Producción, por lo que se hace necesario incluir un nivel de administración del riesgo.

6.4.1.- Procedimiento de Análisis de Riesgos de tecnología .- A continuación vamos a exponer el procedimiento para este diagrama de flujo:

a.- Identificar riesgos informáticos

- Identificar los riesgos informáticos a los cuales están sometidos no sólo los procesos y actividades de la Dirección IT sino toda la empresa, es decir todos los componentes de un sistema susceptibles de ser dañados, dando lugar a la pérdida de conectividad, computadoras o datos.
- Para poder identificar los riesgos, debemos tener en claro las consideraciones de seguridad definidas en las políticas: :Políticas de IT Security y de Organización de IT Security

Responsable IT Security

b.- Evaluar el nivel de riesgo

- Clasificar los riesgos identificados de acuerdo a su naturaleza, los cuales pueden ser cualitativos ó cuantitativos. Evaluar el nivel de los riesgos, para lo cual se deberá determinar lo siguiente:
    - Determinar el costo que significa para la empresa sufrir un desastre que afecte su actividad.
    - Determinar la probabilidad de ocurrencia. Esta probabilidad se encuentra dentro del rango del cero al uno (0-1), donde cero es la probabilidad que no ocurra y uno que ocurra.
- Determinar el impacto que tendría en la operatividad de la empresa si se diera. El impacto se califica del uno al diez (1-10), donde uno es la calificación más baja y con diez la empresa dejaría de funcionar.

Responsable IT Security

c.- Asignar prioridades

- Determinar cuáles son los sistemas y/o aplicaciones fundamentales de la empresa, para poder definir que sistemas priorizar para minimizar riesgos.

Responsable IT Security

d.- Elaborar Plan de Riesgos

- Elaborar el Plan de Riesgos de acuerdo a la evaluación y a la asignación de prioridades.
- Ingresar los riesgos identificados en el sistema Matriz de Riesgos.

Responsable IT Security

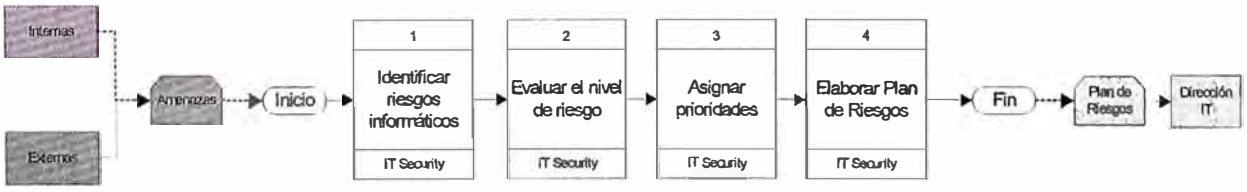


Figura 6.1 Diagrama de flujo del proceso de análisis de riesgos de tecnología.

De igual manera se tiene un procedimiento de Control de cambios, que partiendo de la premisa que todo cambio debe estar debidamente sustentado y aprobado por las instancias respectivas de IT Security y Operaciones IT.

Junto con este procedimiento de Gestión del Riesgo se tiene la de Garantizar la Seguridad de la Información que abarca un concepto más amplio y verifica los controles de cambio, el control de software y versiones, es el que se detalla a continuación:
Diagrama de Flujo:

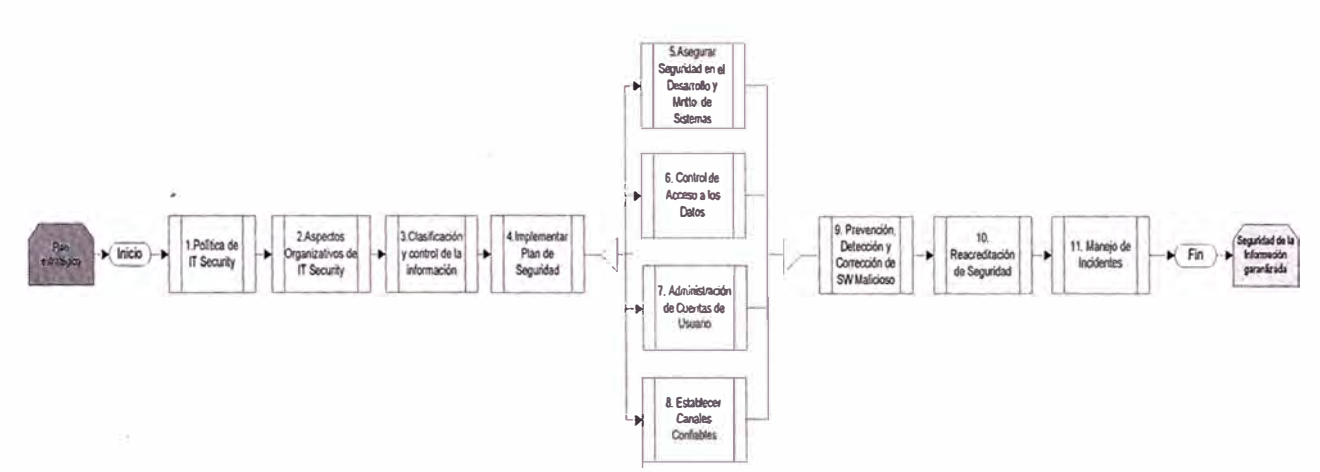


Figura 6.2 Diagrama de flujo del proceso de seguridad de aplicaciones realizada por el área de IT Security.

6.4.2 Procedimiento de Seguridad de aplicaciones .- El procedimiento a seguir se describe a acontinuación:

a.- Política de IT Security

Definir la política de seguridad en la organización que brinde los lineamientos a seguir para dirigir, administrar y dar soporte a la gestión de IT Security. Para ello se debe:

- Definir una política de IT Security que se encuentre en línea con los requerimientos del negocio y refleje las líneas directrices de la organización.
- Solicitar la aprobación de la Dirección IT.
- Con la aprobación y compromiso de la Dirección IT, desplegar un plan de difusión y publicar esta política.

Es importante que la alta dirección apoye visiblemente la seguridad de la información en la organización.

Responsables: Dirección IT, IT Security

b.- ASPECTOS ORGANIZATIVOS DE IT SECURITY

Gestionar la seguridad de tecnologías de información dentro de la organización implica tener claro las entidades involucradas en este proceso. Para ello se debe:

- Diseñar una estructura organizativa que defina las responsabilidades que tiene cada usuario o área de trabajo en materia de IT Security. Esta estructura organizativa debe poseer un enfoque multidisciplinar ya que los problemas de seguridad no son exclusivamente técnicos.
- Mantener la seguridad de los activos de información de la organización que son accedidos por terceros.

Responsable: IT Security

c.- CLASIFICACIÓN Y CONTROL DE LA INFORMACIÓN

Para mantener una protección adecuada sobre la información de la organización y asegurar un nivel de protección adecuado, se debe:

- Definir quién es el dueño de la información, generalmente son los Líderes Usuarios.
- Determinar la criticidad de la información. Esto se puede realizar mediante entrevistas cruzadas con diferentes tipos de usuarios.
- Clasificar la información relacionada con los sistemas de información. La clasificación de la información es responsabilidad de los líderes usuarios.

Documentos normativos relacionados: Políticas de IT Security

Responsable: IT Security

d.- IMPLEMENTAR PLAN DE SEGURIDAD

- Definir el plan de seguridad en base a la política definida de seguridad de tecnologías de información, a la información sobre evaluación de riesgos, a las entidades involucradas y a la clasificación de la información. El plan de seguridad debe incluir acciones
- Enviar este plan para la aprobación de la Dirección.
- Implementar el plan de seguridad. Es responsabilidad de los líderes usuarios la implementación de este plan de seguridad.
- Monitorear la implementación del plan de seguridad.

Responsable: IT Security

e.- ASEGURAR SEGURIDAD EN EL DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Debe completarse la seguridad de la información en todas las etapas del ciclo de vida de los sistemas: especificaciones de requisitos, desarrollo, explotación, mantenimiento, etc.

- Asegurar que la seguridad esté incluida dentro de los sistemas de información para lo cual se debe solicitar y verificar que todos los sistemas cuenten con logs habilitados que permitan registrar las actividades realizadas por los usuarios.
- Evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones.
- Proteger la confidencialidad, autenticidad e integridad de la información.
- Asegurar que los proyectos IT y las actividades complementarias sean llevadas a cabo de una forma segura.
- Establecer mecanismos que controlen las actividades no autorizadas.

Responsable: IT Security

f.- CONTROL DE ACCESO A LOS DATOS

Se deben establecer los controles de acceso adecuados para proteger los sistemas de información críticos para el negocio a diferentes niveles: sistema operativo, aplicaciones, redes, etc. Es necesario:

- Controlar los accesos a la información.
- Establecer mecanismos de autenticidad.
- Evitar accesos no autorizados a los sistemas de información. Cada empleado debe tener una identificación y password únicos.
- Protección de los servicios de red.
- Detectar actividades no autorizadas.
- Garantizar la seguridad de la información cuando se usan dispositivos de acceso remoto.

Es responsabilidad de los Líderes Usuarios decidir quiénes deben tener acceso a la información.

Documentos normativos relacionados:

- Políticas de IT Security
- Política de Control de Accesos
- Política de Identificación de Usuarios
- Política de Autenticación de usuarios
- Política de Accesos a Sistemas y Aplicativos de Personal de Tecnología de Información
- Procedimiento Operativo readministración de Autorizaciones de Acceso a los Sistemas

- Procedimiento Operativo de Mantenimiento de Accesos de Red y Accesos Remotos
- Procedimiento Operativo: Atención de Solicitudes de Accesos IT

Responsable: IT Security

g.- ADMINISTRACIÓN DE CUENTAS DE USUARIO

- Establecer procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión y suspensión de cuentas de usuario.
- Controlar periódicamente los derechos de acceso.
- Establecer mecanismos de información que permitan a los usuarios la actividad normal, así como alertarlos de actividades inusuales.

Documentos normativos relacionados:

- Procedimiento Operativo de Administración de Autorizaciones de Acceso a los Sistemas.
- Procedimiento Operativo: Atención de Desbloqueo de Usuarios
- Procedimiento Operativo: Atención de Reinicialización de Passwords de Red

Responsable: IT Security

h.- ESTABLECER CANALES CONFIABLES

- Asegurar que la información de transacciones sensitivas sea enviada y recibida a través de canales seguros. La información sensitiva incluye: información sobre administración de seguridad, datos de transacciones sensitivas, passwords y llaves criptográficas.
- Asegurar la confidencialidad de canales de comunicación a través de la encriptación entre usuarios, entre usuarios y sistemas y entre sistemas, lo que garantiza que no exista acceso de usuarios no autorizados.

Responsable IT Security

i.- PREVENCIÓN, DETECCIÓN Y CORRECCIÓN DE SOFTWARE MALICIOSO

Establecer un marco de referencia de adecuadas medidas de control preventivas, detectivas y correctivas. Para ello se deben realizar las siguientes actividades:

- Revisar el código de los sistemas previo al pase a producción.
- Actualizar las herramientas de protección de virus.
- Definir alarmas ante una alerta de detección de virus.
- Dar seguridad a la red corporativa a través de sistemas FireWall para proteger en contra de negación de servicios y cualquier acceso no autorizado a los recursos internos.

Documentos normativos relacionados:

- Procedimiento Operativo de Gestión de Seguridad Antivirus

- Procedimientos Operativos de Gestión de Seguridad de Red Corporativa.

Responsables: IT Security, Administrador de la red Corporativa

j.- REACREDITACIÓN DE SEGURIDAD

Asegurar que se lleve a cabo periódicamente una reacreditación de seguridad, con el fin de conservar al día el nivel de seguridad.

Realizar pruebas de seguridad interna y verificar que los sistemas, aplicaciones y conexiones se encuentren protegidos contra intromisiones.

Responsable: IT Security

k.- MANEJO DE INCIDENTES

Establecer las responsabilidades y los procedimientos de manejo de incidentes para asegurar una respuesta apropiada, efectiva y oportuna a los incidentes de seguridad.

Documentos normativos relacionados:

Procedimientos para Reportar y Dar Respuesta a Incidentes de Seguridad

Responsable : IT Security

Resumen del Capítulo

En este capítulo se describen las principales procesos relacionados con la gestión de la red de seguridad perimetral, estos procesos son especificados y normados ya que se debe entender la seguridad como un proceso integral en el cual si no se toman en cuenta todos estos procesos, así tengamos los mejores equipos y sistemas de seguridad, estos no asegurarían por si solos los niveles adecuados de seguridad.

CAPÍTULO VII
CONSIDERACIONES DE MANTENIMIENTO Y ACTUALIZACIÓN DE LA RED DE SEGURIDAD PERIMETRAL

Para mantener óptimos niveles de seguridad en la red de seguridad perimétrica se hace necesario contar con procesos de revisión de seguridad adecuados que garanticen que los continuos cambios de configuración, sea por nuevos servicios, como por la necesidad de aplicar continuos parches de seguridad no ha afectado la seguridad.

7.1.- Procedimiento de actualización de parches de sistema operativo y software de aplicación. .- Es lo que comúnmente se llama "Patch Management", Hubo un tiempo en que las actualizaciones eran opcionales, hoy día es un asunto complejo que merece dedicación y que en muchos casos afecta el desempeño de la Gerencia de TI. Ante este escenario muchas corporaciones están agudizando sus estructuras para optimizar y controlar la identificación, evaluación y aplicación de los necesarios "parches". Una de las principales labores para mantener en niveles adecuados la seguridad de una red es verificar si se ha dado un mantenimiento adecuado al software y hardware que lo componen.

Este fenómeno es sólo uno de los últimos capítulos de lo que se está convirtiendo familiar en el mercado del software: una carrera constante de los proveedores y sus clientes para contrarrestar el impacto de gusanos, virus y brechas de seguridad en su tecnología de información. Haciendo retrospectiva sobre la evolución del uso de "parches" en las empresas, es fácil entender el impacto que hoy día representa: En un pasado reciente, las actualizaciones representaban una actividad que se ejecutaba normalmente ante la identificación de un problema por parte del administrador o como una de las actividades realizadas por el personal de soporte técnico del proveedor cuando realizaba una visita. Este tipo de actualizaciones se limitaba generalmente a los servidores principales y con frecuencia únicamente se relacionaba con el sistema operativo.

Lejos está aquella época de actualizaciones opcionales. Hoy, la problemática de las actualizaciones es un asunto de complejidad y dedicación, que en muchos casos afecta el desempeño de la Gerencia de TI. Ante este escenario, muchas compañías están invirtiendo en la definición de estructuras para optimizar y controlar la identificación, evaluación y aplicación de "parches". Los proveedores por su parte están haciendo cambios en sus procesos de distribución de actualizaciones. Oracle, por ejemplo, adoptó un plan de emisión mensual de actualizaciones para su plataforma, argumentando que, bajo este esquema ayudará en la gestión de parches. Microsoft ha sustentado un esquema similar desde el año pasado, en tanto que Computer Associates y SAP han mantenido esta práctica por algún tiempo.

Por otro lado, se presentan soluciones para la automatización del proceso de dispersión de actualizaciones en la granja de servidores y estaciones de trabajo de las compañías, en respuesta a la demanda del mercado de optimizar esta labor. Según cifras publicadas de la firma Yankee Group, una compañía con más de 500 computadores en su red, debe invertir 120 horas hombre en la prueba e instalación de cada parche; y pese a los esfuerzos en la utilización de herramientas automatizadas, estima que la actualización de cada computador representa US$ 150 de erogación para la empresa.

- **Enfocando la gestión de actualizaciones desde la perspectiva de seguridad**
  Ante la evidente necesidad de responder rápida y eficientemente a la instalación de parches, es importante conocer los factores claves que afectan esta labor. En tal sentido, es importante entender, que la gestión de actualizaciones puede fallar si:

  - No se realizan procesos de identificación de vulnerabilidades en la plataforma tecnológica y se establece un procedimiento regular de catalogación y selección de parches emitidos por los proveedores de tecnología de información.
  - Pruebas de cumplimiento sobre los procedimientos de actualización no son realizados regularmente.
  - La organización carece de un inventario completo de activos de información, que incluya una clasificación de los mismos, estableciendo prioridades según su importancia para la organización.
  - No se ha establecido procedimientos formales de implantación y seguimiento para los parches en la totalidad de los componentes sujetos a actualizaciones.

El establecimiento de un proceso de actualización de seguridad es sin duda un proceso crítico para la Gerencia de TI, sin embargo no es complicado, y una vez que se ha

establecido, se convierte en una actividad cotidiana. Lo que convierte esta tarea en un reto, especialmente en grandes corporaciones, es la descoordinación de los esfuerzos para alcanzar el objetivo, observándose en muchas ocasiones que las iniciativas individuales culminan incrementando el esfuerzo financiero para la empresa y reduciendo la efectividad del proceso.

Para entender mejor la problemática detrás de la gestión de actualizaciones, es necesario entender el origen de las actualizaciones.
Un parche puede:

- resolver una falla en la aplicación,
- alterar una funcionalidad y
- modificar la configuración del software para resolver una deficiencia de seguridad.

Bajo cada una de estas perspectivas, el "leit motiv" surge de diferentes unidades de la organización, quienes son responsables o afectados por la deficiencia. Es por ello que usualmente el proceso de actualización se lleva a cabo de manera independiente. Otro tipo de prácticas incorrectas que se perciben en esta actividad son:

- Aplicación inoportuna de parches
- Ausencia de un enfoque de prioridades
- Poca o ninguna comunicación entre las unidades de negocios y el personal de TI responsable de las actualizaciones
- Solapamiento de funciones en la actualización de plataformas similares (servidores, estaciones de trabajo, entre otros)
- Actitud reactiva: "Actualizo cuando ocurre la falla"…
- Ausencia de estrategias enérgicas claramente establecidas y apoyadas por la alta gerencia
- Alto volumen de procedimientos manuales costosos y susceptibles de error humano
- Falta de documentación suficiente sobre los procedimientos y la tecnología, que permitan coordinar los esfuerzos de mantenimiento y respuesta ante fallas en la aplicación de parches.
- Pruebas insuficientes de los parches a ser instalados o cambios en la plataforma
- Ausencia o pobre definición de las ventanas de cambio para la aplicación de los parches.
- Permanencia de arquitecturas sin soporte por parte del proveedor

Todo lo antes mencionado, representan aspectos que afectan la efectividad en el proceso de actualización de la Compañía. Tal como se muestra en la siguiente figura, el proceso de generación de código malicioso a partir de una vulnerabilidad identificada, se ha reducido notablemente en el tiempo, por lo cual es necesario incrementar la habilidad de la empresa para actuar oportunamente en la remediación de las fallas.

Figura 7.1 Tiempo requerido para que aparezca software que explote vulnerabilidades detectadas.

La automatización como una respuesta parcial a la solución

Existe un conjunto de productos que actualmente automatizan parcialmente esta actividad, manteniendo incluso un registro de los parches, actualizaciones y alertas emitidas por los proveedores de TI, en función de proveer un inventario de parches necesarios para su implantación y colaborando en el proceso de planificación. Esto sin duda facilita buena parte de la problemática que esta actividad representa; sin embargo no reduce el riesgo de compatibilidad de las actualizaciones, particularmente de desarrollos locales. En consecuencia, la automatización es sólo un componente de una solución de gestión de actualizaciones que debe estar conformado por:

- Gestión del inventario de activos de información
- Herramientas de aplicación automática de parches.
- Procedimientos que definan las actividades de identificación, evaluación de compatibilidad y aprobación de las actualizaciones.
- Personal y estructura organizacional especializada para la función.

Beneficios de una gestión de actualizaciones

Como proceso crítico del negocio, una gestión de actualizaciones bien estructurada puede proveer beneficios de carácter cuantitativo y cualitativo para la organización:

- Reducción de costos asociados con la disminución de los períodos de falla y la reducción de incidentes que afecten la operatividad del negocio. También la disminución del impacto de fallas ocasionadas por virus y la reducción de los tiempos de recuperación se reflejan en reducción de costos para la organización.
- Reforzamiento de la calidad e integridad de la información como consecuencia de la reducción de eventos que puedan afectar el almacenamiento o procesamiento de la información.
- Mejoramiento de la imagen corporativa mediante la reducción de fallas que puedan afectar la calidad del servicio, que evidencien públicamente la presencia de brechas de seguridad en la organización o que la expongan en acciones legales o incumplimiento de regulaciones y convenios.

Para poder cumplir adecuadamente con las exigencias del Patch Management en TIM se adoptaron dos medidas de control y administración que facilitan el mantener un adecuado nivel de gestión en esta importante parte de la seguridad.

La primera es la adopción del sistema SUS de Microsoft que es toda una estrategia para actualizar los parches de sistema operativo Windows en estaciones de trabajo y servidores desde una consola central y permitiéndonos discriminar cuales son los parches necesarios de aplicar, sean estos de Sistema Operativo ó de otras softwares de tecnología Microsoft que administremos en la empresa.

La segunda esta relacionada en la forma de tener alertas adecuadas de las vulnerabilidades descubiertas en los diversos sistemas operativos, equipos y softwares de aplicación que poseemos en nuestra red. Como hacer para tener las alertas adecuadas, hay diversas empresas a nivel internacional que periódicamente envían boletines e información sobre los problemas reportados sean estos sobre issues en los sistemas ó la aparición de nuevos virus ó amenazas sobre los sistemas, de las existentes una de las más confiables es el provee SANS Institute (Sysadmin, Audit, Network, Security) sin embargo a nivel de grupo empresarial el Grupo Telecom Italia del cual es subsidiaria Telecom Italia Mobile decidió en el año 2003 montar un Security Operation Center con base en la ciudad de Milán Italia y cuya labor sería brindar esta información de seguridad a todas las empresas del Grupo Telecom Italia (más de 200 empresas) de

un modo personalizado y en tiempo real , con niveles de alerta de acuerdo a la criticidad del problema reportado. Este SOC comenzó a brindar servicios a las empresas del grupo de América Latina a partir de Abril del año 2004 bajo la responsabilidad del Sr. Rocco Mamolitti y luego del inicio del proceso de montar una estructura de seguridad corporativa que resumiera las mejores prácticas de las empresas del grupo. Dado que TIM Perú fue una de las empresas del grupo con menor incidencia de eventos de seguridad desde el inicio de operaciones fue escogida como la primera subsidiaria de América Latina en recibir este servicio y contar con asesoría desde Italia. Es así que desde el 24 de Abril del 2004 se reciben estos mensajes de alertas personalizados para los sistemas operativos, aplicativos y dispositivos que poseemos en nuestra red con lo que la gestión de seguridad de vulnerabilidades propias de los sistemas se ha reducido grandemente. Estos avisos llegan por correo electrónico normalmente pero de ser críticos por un mensaje SMS a los teléfonos celulares de los responsables de IT Security

7.2.- Ethical Hacking Externo. Como parte de los proyectos de seguridad y para medir realmente los niveles de seguridad alcanzados en nuestra red , en el año 2004, cuando se contaba con un 70% de la estructura de seguridad perimetral montada se decidió someter a evaluación de una entidad externa a la empresa, la seguridad de nuestra infraestructura de seguridad perimetral, a la vez que se sometía a pruebas las políticas adoptadas y la capacitación del personal usuario de los sistemas y del personal técnico a cargo de la gestión de los recursos y servicios que TIM Perú ponía a disposición de sus clientes en la plataforma Internet. Este servicio se manejó con total confidencialidad ya que lo se quería es simular un ambiente de un ataque real a los sistemas utilizando todas las metodologías vigentes de hacking, inclusive la Ingeniería Social, el servicio que se convocó a licitación por invitación fue un servicio de Ethical Hacking (hackeo ético). Las bases sobre las que calificó a la empresa que realizaría este servicio son los siguientes:

7.2.1.- Generalidades.- TIM Perú SAC, ofrece a sus principales clientes servicios de Internet públicos tales como páginas web informativas, de envío de mensajes de texto (SMS) a teléfonos TIM, Tienda virtual y también acceso a aplicaciones corporativas usando la tecnología de Intranets y brinda este servicio a través de acceso vía dial up, vía Internet y vía enlaces dedicados, siendo el de mayor porcentaje los accesos vía dial up e Internet. El acceso a las aplicaciones se realiza a través de Web servers que se encuentran conectados a Servidores de aplicaciones, permitiendo los servicios de consulta de páginas, compra en línea,

consulta de información, y transferencia de información con nuestros socios y proveedores, etc. Para garantizar la seguridad de este sistema se ha montado un sistema de acceso con autenticación basado en passwords dinámicos y un sistema de firewalls que garantizan zonas seguras, transaccionales e internas. Por lo que es necesario convocar a especialistas en Ethical Hacking que emitan un diagnóstico de los niveles de seguridad y sugieran cambios o mejoras al sistema de seguridad para garantizar la disponibilidad y seguridad de los servicios, asimismo se pueda contar con un documento de procedimientos en casos de sufrir ataques de diversos orígenes.

7.2.2- Objetivos

- Análisis de la plataforma de seguridad del sistema de Acceso y conexión a Internet.
- Análisis de la plataforma de seguridad de las aplicaciones Internet / Extranet.
- Documentación de Estado de Seguridad de los sistemas de acceso que TIM Perú SAC brinda a sus usuarios.
- Documento de procedimientos de contingencia en casos de ataques.

7.2.3.- Descripción de la Topologia

El sistema está estructurado de la siguiente manera:

- **RED DE ACCESO**
- **SISTEMA DE SEGURIDAD**

El acceso de los usuarios a la red de TIM Perú SAC, es controlado por un sistema de autenticación, autorización y registro de acceso, basado en un sistema RADIUS con interfaces a un sistema basado en tokens para una mejor autenticación que generan passwords dinámicos.

Todos los servidores de acceso están conectados a la red de TIM Perú SAC y conforman la DMZ junto con los sistemas de autenticación descritos. Para mantener la seguridad, los servidores WEB están conectados a una DMZ. La red pública, la DMZ1 Servicios Web, la DMZ2 Proveedores y la DMZ Transaccional se comunicarán a través de un esquema de firewalls en cluster que garantizan la seguridad entre las diferentes zonas. Estos firewalls están instalados en el enlace corporativo y de servicios

7.2.4 .-Descripción de los enlaces

Enlace Corporativo

Este enlace tiene las siguientes características:

- Ancho de Banda: 2Mb clear channel,
- Proveedor: TIM
- Puertos: 16 Seriales

Enlace de Servicios

Este enlace tiene las siguientes características:

- Ancho de Banda: Internet 2Mb
- Proveedor: AT&T
- Puerto: 01 Ethernet

Enlace Dial -UP

Este enlace tiene las siguientes características:

- 2 E1 con Telefonica
- 1 E1 con TIM
- RAS

7.2.5 Requerimientos Técnicos.- El proveedor debe realizar una evaluación de los diferentes niveles de riesgo de seguridad, estudio de las políticas de seguridad implantadas, Identificación de la vulnerabilidad de la seguridad, análisis de la capacidad de recuperación y prevención de problemas de seguridad, revisión de los reportes de los sistemas de seguridad y una evaluación de la vulnerabilidad de las aplicaciones ofrecidas a los clientes a través de estos medios. Al finalizar la evaluación de estos sistemas deberá emitir los siguientes informes:

Informe de los diferentes niveles de vulnerabilidad de la plataforma de seguridad de la RED y de servidores con aplicaciones posibles.

Reporte final escrito con detalle de las vulnerabilidades encontradas y las respectivas recomendaciones de cómo superarlas.

Certificación del nivel de seguridad de los sistemas instalados.

El estudio debe considerar diferentes estados de evaluación:

- Como cualquier individuo externo a la institución.
- Como cliente del servicio.
- Como usuario de la RED interna de TIM Perú SAC.

Recomendaciones de Procedimientos de Recuperación en casos de ataques.

Recomendación ante eventos del tipo DDoS.

7.2.6. Requerimientos de las pruebas a realizar.- Entre las pruebas que se deben realizar al evaluar estos ambientes, podemos citar entre los principales:

1. Análisis de políticas, estándares y procedimientos.
2. Análisis y certificación de los niveles de seguridad de los servidores de acceso
3. Análisis y certificación de los niveles de seguridad de Firewalls.
4. Análisis y certificación de los niveles de seguridad de la configuración de los ruteadores.
5. Análisis y certificación de los servidores Web.
6. Análisis y certificación de las aplicaciones Web
7. Análisis y certificación de las aplicaciones de Password Dinámico.
8. Análisis y certificación de los módulos de programas de las interfaces a aplicaciones de Host y Cliente-Servidor.
9. Análisis y certificación de los módulos de programación de páginas y aplicaciones ActiveX.
10. Realizar intentos de hacking al sistema en conjunto. Con las siguientes opciones :
    - Tests basados sobre un conocimiento cero, usando información pública ó identificando la información expuesta en Internet.
    - Ingeniería Social
    - Análisis de alto nivel desde Internet para identificar los riesgos y vulnerabilidades de nuestra red.
    - Pruebas al aislamiento a la red interna
    - Pruebas a los accesos dial-up para encontrar vulnerabilidades
    - Pruebas a los servidores críticos.
    - Passwords Cracking

Para estas opciones las herramientas a utilizarse deberán ser de conocimiento de TIM, el tipo de ataque debe validarse para la prevención y evitar falsos negativos, así evitar el filtrado a nivel de firewall y routers.

7.2.7- Requerimientos Generales:

El proveedor debe incorporar en su propuesta el número de especialistas que intervienen en el análisis, incluir el perfil de cada uno de ellos y el grado de experiencia en análisis de seguridad.

El Proveedor deberá indicar las herramientas de análisis que utilizará durante el desarrollo del Ethical Hacking.

- Se debe incluir en el entregable el detalle de los casos de pruebas y un plan detallado de las mismas que no excedan los 15 días.

- Debe garantizarse total confidencialidad y compromiso ético-profesional. Se firmará un contrato de confidencialidad.
- Al finalizar el diagnóstico de seguridad deberá emitir los informes solicitados (4 copias) en un plazo no mayor a 1 semana.
- Debe considerarse la transferencia del KnowHow al personal de Seguridad de Información y Arquitectura IT

7.2.8.- Consideraciones Adicionales

- Compromiso de cumplimiento por escrito de los plazos establecidos
- Carta de garantía de la certificación de los niveles de seguridad por un lapso no menor a 1 año.

Finalmente y luego de un exhaustiva revisión de los perfiles de las empresas concursantes resultó ganadora la empresa Orión de Chile con amplia experiencia en estos trabajos a nivel de América Latina y porque los precios de los postores Europeos y Americanos estaban muy por encima de los presupuestado.

La revisión a nuestras redes se realizó en dos etapas:

- La primera de recopilación de información y del Ethical hacking en sí. Luego de la cual se emitiría un informe con el listado de las vulnerabilidades encontradas y las evidencias de haber podido ingresar a nuestra red ó retirar información de ser el caso.
- La segunda luego de haber tomado las medidas de control y mejoras a partir de los hallazgos presentados en el informe para comprobar que estos ya han sido superados y que se ha mejorado el nivel de seguridad de la red perimetral.

La realización de esta prueba se llevó a cabo entre los meses de Junio – Julio del 2004 (primera etapa) y Setiembre- Octubre del mismo año (segunda etapa).

Los hallazgos reportados en el primer informe no fueron relevantes, verificándose que aún con conocimiento de la estructura de nuestra red y con password de usuarios válidos (para los servicios que se brindan a través de Internet) no se pudo ingresar a la red interna de la empresa ni sacar algún tipo de información, los hallazgos principalmente estuvieron referidos a parches de sistemas operativos en algunos servidores Linux no debidamente actualizados ó a servicios que deberían desactivarse en estos equipos. A partir de esa fecha y luego de solucionar las observaciones acotadas se tiene un proceso mensual de escaneo de vulnerabilidades desde Internet de nuestros servicios de red en forma mensual y un ethical hacking a nuestros servidores web en forma trimestral, esto nos ayuda a mantener en niveles óptimos la calidad y la seguridad de nuestra red de seguridad perimetral.

7.3.- Gestión de Seguridad de la Red Corporativa.- Comprende específicamente la gestión de seguridad de la red corporativa y los procesos y procedimientos que se llevan a cabo para mantener adecuados niveles de seguridad, el proceso en sí se detalla a continuación:

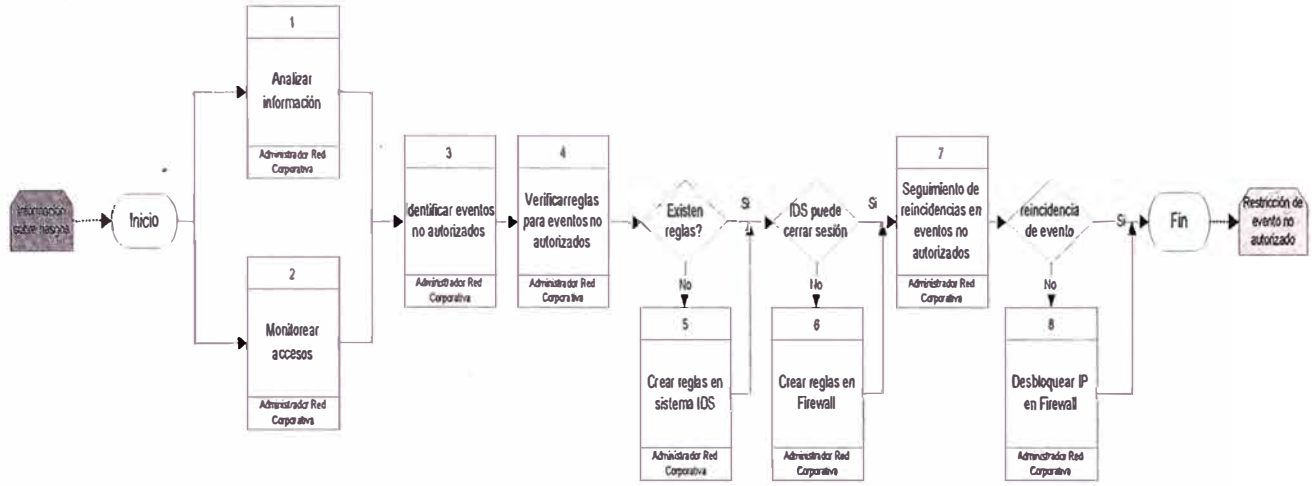


Figura 7.1 Diagrama del proceso de Gestión de la red corporativa.

A continuación se describe el proceso en sí:

a.- Analizar Información

- Recibir de IT Security información sobre los productos que presentan ciertos riesgos de vulnerabilidad en los accesos a la red.
- Determinar si la empresa cuenta con estos productos

Responsable: Administrador de la Red Corporativa – Forma Manual

b.- Monitorear Accesos

- Monitorear periódicamente la información referente a los intentos de accesos no autorizados a la red mediante el "Sistema Detector de Intrusos".

Responsable: Administrador de la Red Corporativa – En el sistema de Prevención de Intrusión.

c.- Identificar eventos no autorizados

- Determinar el tipo de evento no autorizado detectado mediante el monitoreo periódico de accesos.
- Identificar posibles riesgos de eventos no autorizados según la información recibida de IT Security.

Responsable: Administrador de la Red Corporativa – En el sistema de Prevención de Intrusión.

d.- Verificar reglas para eventos no autorizados

- Verificar si existen reglas y políticas definidas en el "Sistema Detector de Intrusos (IDS) para el tipo de evento no autorizado, de ser así la sesión de acceso será cancelada automáticamente.

Responsable: Administrador de la Red Corporativa - En el sistema de Prevención de Intrusión.

e.- Crear reglas en los IPS

- Crear las reglas en el "Sistema Detector de Intrusos" (IDS), en caso de que éstas no estén definidas en el IDS.
- Verificar si el "Sistema Detector de Intrusos" una vez creada las reglas está en capacidad de cerrar la sesión en forma automática.

Responsable: Administrador de la Red Corporativa - En el sistema de Prevención de Intrusión.

f.- Crear reglas en el Firewall

- Crear las reglas y políticas en el Firewall, con la finalidad de no permitir establecer sesiones desde la dirección de origen del evento no autorizado. Estas reglas son creadas cuando IDS no puede cerrar las sesiones.

Responsable: Administrador de la Red Corporativa – En el firewall.

g.- Seguimiento de Reincidencias en eventos no autorizados

- Efectuar periódicamente un análisis de la base de datos del "Sistema Detector de Intrusos", a fin de determinar si ha habido reincidencia en el evento no autorizado identificado inicialmente.

Responsable: Administrador de la Red Corporativa - En el sistema de Prevención de Intrusión.

h.- Desbloquear dirección IP en el firewall

- Desbloquear la dirección IP desde donde se originó el evento no autorizado, en caso de determinar que no ha habido reincidencia en el intento de acceso a la red.

Responsable: Administrador de la Red Corporativa – En el firewall.

7.4.- Gestión de Seguridad Antivirus.- Adicionalmente a estos procedimientos y como refuerzo a las herramientas de control descritos se tiene un procedimiento de control de virus que nos ha ayudado a mantener nuestra red libre de problemas derivados de las infecciones de virus informáticos , estas herramientas y procedimientos han permitido que TIM Perú sea dentro del grupo Telecom Italia la empresa con menor cantidad de virus informáticos en un ratio que mide números de equipos informáticos en la red , versus cantidad de infecciones y la criticidad de los mismos, no fuimos afectados por ninguno de los virus que en los últimos año afectaron a numerosas empresas, el procedimiento de Gestión desarrollado es el siguiente:

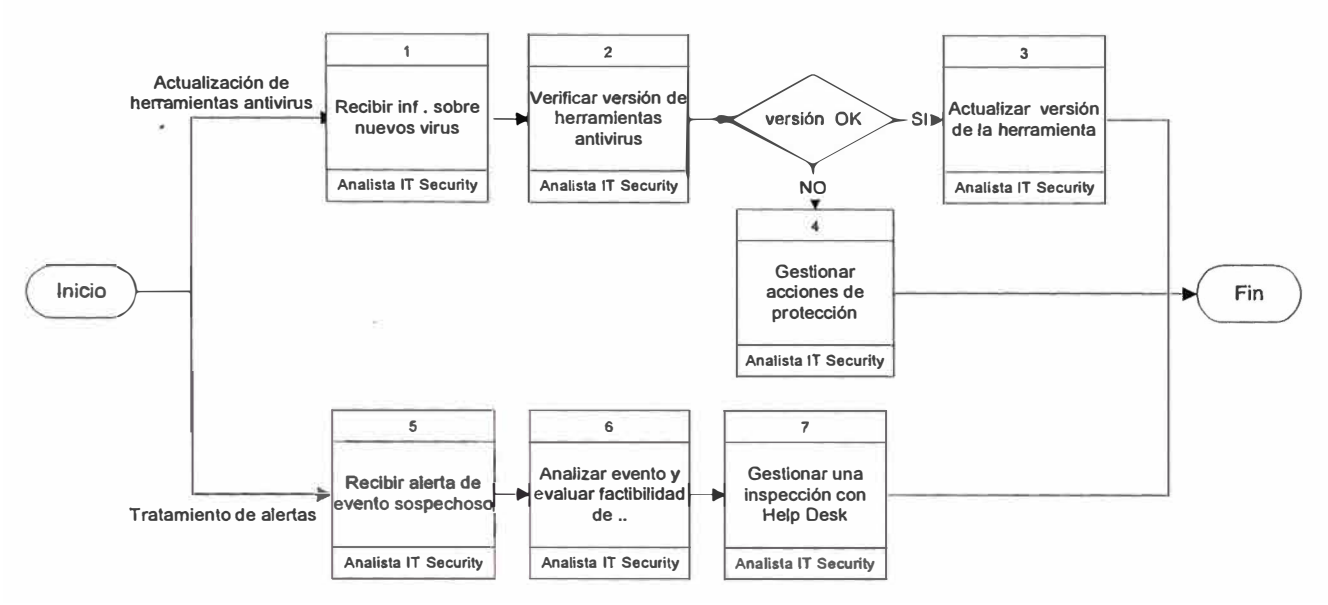


Figura 7.3 Diagrama del proceso de Gestión Antivirus

A continuación se describe el proceso de gestión antivirus en sí:

Actualización de Herramientas Antivirus

a.- Recibir información sobre nuevos virus

- Recibir diariamente de las empresas especializadas información sobre nuevos virus y mutaciones. Cabe señalar que la empresa está suscrita al servicio de "Lista de Alertas" como medida de protección de nuevos virus.

Responsable: Analista de IT Security

b.- Verificar versión de las herramientas antivirus

- Verificar si TIM cuenta con la versión de la herramienta de protección contra el virus o mutación informada.

Responsable: Analista de IT Security

c.- Actualizar versión de la herramienta de protección

- Ejecutar en el sistema la actualización de la versión, en caso de determinar que se cuenta con ella y el sistema por alguna razón no actualizó en forma automática.

Responsable: Analista de IT Security

d.- Gestionar acciones de Protección

- Establecer filtros en el sistema de antivirus teniendo en cuenta la información recibida de la forma cómo actúa el virus.

- En caso de no poder establecer filtros comunicará masivamente al personal de la empresa sobre el peligro del virus y dar las reglas para la protección

Responsable: Analista de IT Security

e.- Tratamiento de Alertas

Recibir alerta de evento sospechoso

- Recibir un correo ante un evento de sospecha de virus, dicho correo es generado en forma automática por los sistemas que monitorean la existencia de virus.

Responsable: Analista de IT Security

f.- Analizar Evento y Determinar Factibilidad de Investigación

- Verificar en el Log si el evento reportado se trata de una inconsistencia del sistema o es un evento sospecho que amerita ser investigado.
- Tener en cuenta que los aspectos a considerar para definir la validez de la investigación son:
    - Tipo de archivo
    - Tipo de problema reportado (ej: no se pudo leer archivo)
    - Archivo corrupto: El archivo que origina el reporte tienen inconsistencias, es decir fue mal generado.
- Determinar si procede o no la investigación

Responsable: Analista de IT Security

g.- Generar una Inspección con Service Desk

- Coordinar con Service Desk la revisión de la máquina, para ello se utilizarán otras herramientas antivirus para determinar si el problema realmente trata de la existencia de un virus o es un problema de archivo.

7.5.- Procedimiento de respuestas a Incidentes.- Un buen plan de seguridad nunca estaría completo sin un adecuado procedimiento de respuesta a incidentes, es decir ante la ocurrencia de un evento de seguridad informática de cualquier índole , por ejemplo una infección masiva de virus, alertas en el sistema de detección de intrusos, la caída de los servicios corporativos hacia Internet ó un intento de DoS, que es lo que se debe hacer , que pasos tomar, a quienes de debe comunicar, recordemos siempre que la Seguridad no es cuestión de equipos ni de sistemas sino de personas y si las personas no reaccionan adecuadamente aún contando con los sistemas más eficaces y modernos no obtendremos un adecuado nivel de seguridad, es por estos motivos que es TIM Perú a comienzos del año 2004 se consideró oportuno crear un equipo CIRT (Computer

Incidence Response Team) que liderara y pudiera dar rápida respuesta a eventos de Seguridad Informática, a continuación se detalla el procedimiento creado para tal fin.

En esquema adjunto, se puede observar que el Equipo de Respuesta a Incidentes de Seguridad (ERIS)- TIM PERÚ S.A.C., opera en función de dos grandes etapas, las cuales se detallan a continuación:

Etapa 1: Recepción de Reportes de Incidentes de Seguridad.

Etapa 2: Respuesta a Incidentes de Seguridad.

Etapa 1: Recepción de Reportes de Incidentes de Seguridad

Los usuarios con problemas reportan directamente a la Mesa de Ayuda, en donde se toman algunos antecedentes de modo de registrar y foliar el reporte, para posteriormente hacer un seguimiento. Así internamente y en forma inmediata, se da aviso al Coordinador de Seguridad de la Información.

El Coordinador de Seguridad de la Información también recibe reportes desde otras fuentes, por ejemplo, a través de notificación externa (Correo Electrónico), Notificación Interna Reporte "Security Alert", mediante Detección IDS y vía Consolas Antivirus.

Todos estos reportes de Incidentes de Seguridad, son recepcionados por el Coordinador de Seguridad de la Información, quien se encarga de evaluar la categoría del incidente, impacto del problema, y clasificar según su potencial daño, en un tiempo máximo de 30 minutos.

Luego el Coordinador de Seguridad, según la evaluación, asigna prioridad y toma acción si es necesario.

Dependiendo de la categoría del Incidente, se clasifican en:

- No-Crítico, Falso, o Incidente resuelto
- Crítico

Etapa 2: Respuesta de Incidentes de Seguridad

Si el Coordinador de Seguridad de la Información, determina que el problema reportado es ***No-Crítico***, se activan los procedimientos de soporte interno normal. Si determinan que el problema reportado es ***Falso***, o ***Incidente Resuelto***, se procede a crear un nuevo Registro independiente del incidente Reportado en el Help Desk. El Coordinador de Seguridad de la Información cierra el caso y luego en el Help Desk procede él, a actualizar el estado del Folio para una investigación posterior. El Coordinador de Seguridad de la Información informa vía mail al Usuario que reportó el incidente.

Por otra parte, si se determina que el problema reportado es **Crítico**, el Departamento de Seguridad reporta directamente al Help Desk, y tiene 30 minutos, desde el inicio para evaluar el ataque antes de escalarlo a ERIS.

El Coordinador de Seguridad de la Información registra cada reporte de incidente, e informa inmediatamente al Equipo de Respuesta a Incidente de Seguridad (ERIS), aportándoles antecedentes que puedan ayudar a la solución del incidente reportado.

Todos los reportes de incidentes de seguridad son identificados y registrados de manera independiente, manteniéndose éstos en una base de datos por un tiempo no menor a tres años.

Se activa el ERIS (Gerente de Arquitectura, Gerente de Operaciones y Jefe de IT Security), estudian la situación, toman las acciones pertinentes para su corrección y, si el incidente tiene impacto sobre Servicios Críticos de Negocio de TIM PERÚ S.A.C., informa a la Gerencia General (o inmediatamente superior) de TIM PERÚ S.A.C., proponiendo las medidas correctivas. Se evalúa si se requiere apoyo externo especializado o apoyo por parte de algún distribuidor.

La Gerencia General de IT de TIM PERÚ S.A.C., procede a autorizar o reprobar las acciones sugeridas por ERIS. Evalúa si el incidente requiere incluir organismos legales en la investigación o respuesta.

En el caso de requerir apoyo externo, se procede a consultar el listado de proveedores y contactar al indicado para el apoyo. Todas las empresas listadas, deben tener firmado un acuerdo de no divulgación y confidencialidad con TIM PERÚ S.A.C..

ERIS, en función de las decisiones tomadas por la Administración de IT de TIM PERÚ S.A.C., toma las acciones correspondientes para terminar de resolver el incidente, para luego cerrar el caso, reportando directamente al Help Desk. Luego de esto, Help Desk procede a actualizar el estado del Folio, para mantener un Feedback hacia el Usuario que reportó el incidente.

El siguiente diagrama de flujo muestra en forma gráfica el procedimiento descrito anteriormente:

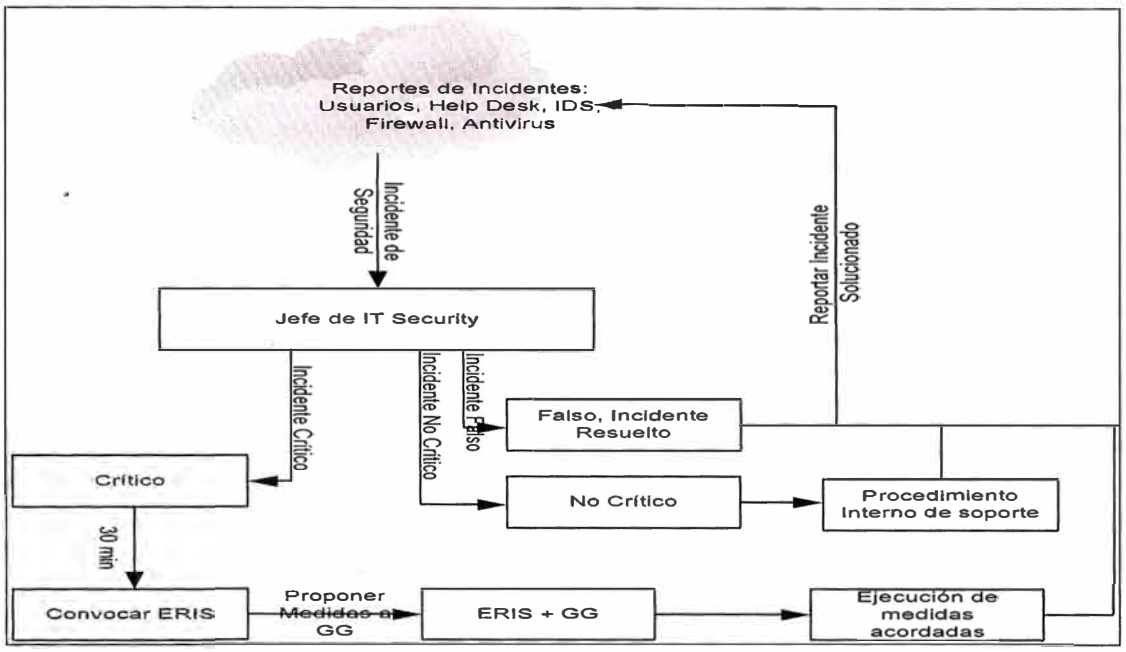


Figura 7.4 Diagrama del proceso de respuesta a Incidentes de Seguridad.

Etapa 2.1: Incidentes de Seguridad v/s Involucrados

Cuando el o los Incidentes de Seguridad involucran a un Cliente de TIM PERÚ S.A.C., o información privada relacionada con un Cliente de TIM PERÚ S.A.C., se debe reportar de inmediato al Departamento Legal de TIM PERÚ S.A.C.

Cuando el o los incidentes de seguridad involucran a un Socio Proveedor de Servicios TIM PERÚ S.A.C. o Socio Comercial, se actúa sobre la base que, los contratos con éstos incluyen la cooperación con la investigación de Incidentes de Seguridad que los relacionan a TIM PERÚ S.A.C. El Incidente deberá ser reportado al Departamento Legal de TIM PERÚ S.A.C.

Cuando el o los Incidentes de Seguridad involucran Conexiones Externas, se debe reportar de inmediato al Proveedor Local de Conexión para coordinar las acciones correctivas.

Etapa 2.2: Después de la Solución de Incidentes de Seguridad

Una vez resuelto los problemas reportados, creados los registros, evaluado la categoría del Incidente, etc., se hace un análisis de pérdidas. Esto es importante para reportar valores cuantitativos entendibles por la Gerencia inmediatamente superior, lo cual permitirá tomar decisiones con mayor conocimiento en otras ocasiones.

Además, muchos de los incidentes podrían requerir la activación de Planes de Contingencia o Recuperación de Desastres. Estos planes deben estar disponibles y actualizados al momento de ser requeridos, y deben ser mantenidos y actualizados por la Gerencia de Operaciones.

Resumen del capítulo

En este capítulo final hemos podido conocer en detalle los procesos relacionados al mantenimiento adecuado de la seguridad de la red de seguridad perimetral de TIM Perú, la seguridad es un proceso continuo que involucra todos las aspectos de un sistema en este caso la red perimetral es por eso que a través de estos procesos, ethical hacking, gestión de seguridad, gestión antivirus, etc. Garantizamos que los niveles óptimos alcanzados en la etapa de diseño e implementación se mantengan a lo largo del tiempo.

CONCLUSIONES

1. En un mundo altamente competitivo como el actual, la información tiene un papel muy importante, y en un gran empresa el 100% de la información relevante se encuentra en medios magnéticos y es transmitida a través de redes de comunicaciones de datos, es dentro de este contexto que la seguridad de redes cobra cada día más importancia, en mi experiencia profesional he podido ver la evolución no solo de los equipos y dispositivos de seguridad cada vez más sofisticados sino la evolución de la seguridad como una disciplina cada día más independiente pero que requiere de una gran base técnica, de tener los conceptos de comunicaciones de datos claros.

2. Si bien el presente trabajo ha estado enfocado en el diseño de una red de comunicaciones perimetral con la seguridad como factor principal para una corporación que tiene muchas y muy complejas necesidades de comunicación y estándares de seguridad igualmente altos, lo explicado en este informe puede ser utilizado para redes de menor envergadura siempre y cuando se realice el análisis de seguridad respectivo y se determinen las reales necesidades de seguridad y comunicaciones.

3. Es necesario tener en cuenta que tanto el diseño de la red de datos como de los elementos de seguridad no los puede determinar el responsable de manera teórica y fija en el tiempo, sino que necesariamente debe estar confrontada regularmente con las necesidades del negocio, es decir una empresa cuya presencia en Internet se restringe a un sitio web con solo elementos informativos es muy diferente a una empresa cuyo primer foco de negocios es el e-business. De igual modo los requerimientos de seguridad de una empresa de logística no son similares a los requerimientos de seguridad de una institución financiera.

4. Para el caso presentado específicamente en este informe que es el de la red de datos perimetral de TIM Perú, se tuvo que al ser una empresa que recién se iniciaba en el Perú y al ser parte de una gran corporación mundial, los estándares solicitados de facilidades de comunicaciones y seguridad eran muy diferentes de los de las empresas locales en general, para lograr imponerlos en la empresa se requirió del apoyo de la alta Dirección de la empresa tanto en la parte administrativa de contar

con los medios y facilidades de publicar las políticas necesarias, como de la parte financiera ya que estos equipos de seguridad generalmente y por ser de última generación tienen un costo bastante alto.

5. Dentro del presente informe no se han detallado los costos de los equipos ni de la implantación debido a que según el esquema de TIM Perú esta es información restringida y sensible, adicionalmente la parte financiera de las adquisiciones de los equipos y su instalación y soporte es negociada por otro departamento de la empresa independiente del área de Tecnología de la Información, nosotros como parte técnica solo intervenimos en la parte técnica de las licitaciones y adquisiciones. Asimismo muchos de estos equipos fueron negociados directamente por la casa Matriz debido a que por volúmenes se manejaban costos especiales (caso de los servidores HP, firewalls, sistemas antivirus) Sin embargo de acuerdo a valores estándar del mercado se asume que en total desde el inicio de operaciones de la empresa, la inversión total en compra de equipos, instalación y costos anuales de mantenimiento está cerca de los cuatro millones de dólares americanos.

6. Actualmente y debido a la venta de TIM Perú al conglomerado de comunicaciones América Móvil se han detenido los proyectos mientras la nueva administración toma real conocimiento de la situación de la empresa. Sin embargo las perspectivas son bastante buenas, sin embargo al ser esta corporación de reciente creación no tiene aún establecidas políticas ni estándares corporativos, sin embargo por conversaciones sostenidas con responsables de IT Security de otras operadores del grupo se sabe que el nivel de la red seguridad perimetral de nuestra red es muy superior al de otras.

7. Finalmente quería resaltar que la Seguridad es un asunto de personas y no de equipos ó sistemas, así poseamos los mejores equipos y dispositivos de seguridad, si no contamos con el personal idóneo para gestionarlos no se podrán lograr reales y efectivos resultados.

BIBLIOGRAFÍA

[1] MASTERING THE TEN DOMAINS OF COMPUTER SECURITY.- Ronald Krutz, Rusell Dean Vines. Editorial Wiley 2001

[2] FIREWALLS Y LA SEGURIDAD EN INTERNET.- Karanjit Siyan , Chris Hare. Prentice Hall Hispanoamericana 3era Edición 2002.

[3] WEB SECURITY.- Lincoln Stein Editorial Addison Wesley Longman Inc. 2003

[4] HACKERS.- SECRETOS Y SOLUCIONES PARA LA SEGURIDAD DE REDES.- Joel
Scambray, Stuart MC Clure, George Kurtz. Editorial Osborne McGraw Hill 2002