UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ARQUITECTURA DE SEGURIDAD PARA REDES CORPORATIVAS

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

HERNAN EDILBERTO TELLO ARBIETO

PROMOCIÓN
2002- I

LIMA – PERÚ
2006

ARQUITECTURA DE SEGURIDAD PARA REDES CORPORATIVAS

Dedico este trabajo a:

Mis padres por su sacrificio y dedicación

A mis hermanos por su apoyo y ejemplo

Mis sobrinos, por la esperanza en el mañana.

SUMARIO

El presente trabajo tiene por finalidad elaborar identificar e implementar políticas de seguridad en redes corporativas en base a estándares internacionales, que permitan construir un entorno de operaciones confiable para la marcha de una organización.

Se desarrolla los sistemas de protección necesarios tanto de políticas estándares y procedimientos de seguridad, auditoria de sistemas de información y sus mejores prácticas, luego se identifican vulnerabilidades y se desarrollan sus correspondientes mecanismos de protección, en cada escala de dimensión de la red.

Como parte final se muestra un caso de estudio el análisis e implementación de las políticas en un entorno real.

INDICE

INDICE DE ILUSTRACIONES

INDICE DE TABLAS

PROLOGO

La evolución vertiginosa de la tecnología, esta provocando que la humanidad interaccione como nunca antes ha sucedido, los avances en los sistemas de comunicaciones permiten el desarrollo de innumerables campos del conocimiento, cubriendo necesidades y creando nuevas formas de comunicación.

Esta creciente integración genera bienestar y nuevas oportunidades de desarrollo, pero también nuevas formas de peligro a las que están amenazadas los sistemas de comunicación, y todo lo que él porta.

Hoy en día con el advenimiento de la era de la información, las sociedad esta girando en torno a los sistemas de información, cada vez la sociedad se digitaliza mas, en diversas áreas como salud, educación, cultura, comercio, banca, investigación, defensa, entretenimiento, entre otras, cambiando la manera en que vivimos, pensamos, y nos desarrollamos.

Sin embargo, los ataques a sistemas informáticos, el robo de información, la pérdida por desastres u otros, son también parte de ese desarrollo y son formas de disrupción en una creciente sociedad digital.

Bajo este escenario se requiere que existan formas de protección de las organizaciones, sobre cualquier forma de amenaza, que permita que estas se sigan desarrollando y cumpliendo los objetivos que cada organización se establezca.

Por lo tanto la seguridad de la información pasa a se un tema crítico, para la nueva sociedad de la información ya emergente.

Actualmente los sistemas de seguridad de la información se están estandarizando globalmente, bajo estándares de seguridad como el ISO 27001, por el cual se rigen las políticas de seguridad de la organización.

Estas políticas deben gobernar sobre los elementos de protección individuales como: Firewalls, sistema de prevención de intrusiones, antivirus, y sobre mecanismos de autenticación, acceso, monitoreo.

Dado esta premisa el presenta trabajo pretende dar una óptica de seguridad de la

información desde la infraestructura de comunicaciones, desarrollando los componentes para su estudio.

En el capitulo I, se describe la necesidad y la naturaleza de la protección, requisito necesario para poder desarrollar un visión de un sistema de seguridad.

En el capitulo II, se engloba las características de un proceso de auditoria de seguridad, el orden del mismo es debido a que muchas organizaciones poseen sistemas de comunicación ya establecidos y no necesariamente sujetos a sistemas de seguridad, una auditoria previa es el paso para determinar el estado en que se encuentra su infraestructura.

Los capítulos III, esta dedicado a la división de las políticas de seguridad, en políticas propiamente, estándares y procedimientos.

Cabe resaltar en esta capitulo se hace hincapié en el estándar actual de seguridad ISO 17799.

Los capítulos IV, y V, están orientados hacia las características particulares de sistema de protección, como son los *firewalls,* y la clasificación de las redes y sus componentes de seguridad de acuerdo a su dimensión.

El en capitulo VI, se desarrollo íntegramente un caso real de una sistema de protección, con diversos componentes que la organización gestiona para la seguridad de la información.

CAPITULO I

IDENTIFICACION DE LA NATURALEZA DE LA PROTECCION

1.1 La necesidad de protección

La creciente integración de redes de datos, y su necesaria ínter operación con entornos diversos, hace que los sistemas de comunicación sean mas complejos y pero también inseguros.

La marcha de la organización cada vez mas depende de una infraestructura tecnológica, y los datos digitalizados que manejan, son de naturaleza crítica.

1.2 Comprendiendo la seguridad

Entendemos la seguridad como un entorno de operación libre de peligro o daño o riego. Pero esta apreciación es ideal, la propia naturaleza de un entorno es desarrollado por humanos y susceptible a error u omisiones de diseño; bajo esta premisa se encuentran fallos que son explotados maliciosamente y/o corregidos; de aquí a que el termino mas real es de un **entorno fiable** [8]

De lo anterior podemos afirmar que la seguridad no es un problema tecnológico sino uno de naturaleza social.

Las 3 cualidades estándares para medir un entorno seguro o fiable se pueden resumir en:

- Confidencialidad
- Integridad
- Disponibilidad

Se puede entender como **confidencialidad**, al entorno en el que los componentes o recursos son accedidos solo por el personal autorizado.

La **integridad** se refiere a cuando los recursos solo son modificados por personal autorizados.

La **disponibilidad** se refiere a que los recursos del sistema se encuentran accesibles a entes autorizados.
De acuerdo al tipo de organización, estos 3 parámetros pueden ser considerados con diversas prioridades, por ejemplo una organización financiera considerará como prioritario a la **integridad** y la **disponibilidad**, pero para una organización diplomática o militar considerará como prioritario la **confidencialidad**.

1.3 Elementos a proteger

Para poder analizar el objeto a proteger es necesario evaluar la naturaleza de nuestra organización y ubicar los elementos susceptibles a riesgo y de necesaria protección. No necesariamente todo ha de ser protegido con igual grado; se debe determinar diversos niveles de seguridad de acuerdo a la naturaleza o exposición del objeto a proteger.
Los elementos a proteger pueden ser clasificados en:

Datos: base de datos de registros, son los sistemas de almacenamiento digital.

Software: códigos fuente de programas, son los códigos fuente de los sistemas informáticos desarrollados o adquiridos por la organización y que necesaria protección.
En organizaciones de desarrollo de software este el elemento fundamental de su negocio.

Hardware: Protección de acceso de equipos estos equipos son ubicados en centros de computo, y generalmente son de altos de costos, su acceso local y mas aun remoto deben ser protegidos.

De todos los elementos señalados indudablemente, la protección de los datos es el de más alta importancia**,** dado que restituir una determinada información almacenada de manda una tarea compleja o es irrecuperable.

Los demás elementos giran como entorno de protección a este elemento. Cabe resaltar que la seguridad depende de la interacción de estos tres elementos, por ejemplo, un elemento de hardware o un código de software mal programado podrían poner en riesgo los datos o la operación de una organización.

1.4 De quien protegernos

Durante el proceso de determinación de nuestras amenazas, estas pueden ser de origen diverso pero debemos evaluar las de mayor riesgo, pueden identificarse como:

Personas

- Personal, son las personas que de alguna manera interaccionan con la organización, ya sea de manera parcial o total, físicamente dentro o de acceso remoto.
- Curiosos, en esta categoría se encuentra los individuos ya sean pertenecientes a la organización o de fuera, pero que indagan e intentan determinar el grado de acceso de los sistemas, su riesgo no es crítico, pero deben ser tomados en cuenta.
- *Crackers*, son los elementos (podrían no ser personas) que intencionalmente participan en un acto de intrusión no autorizado a un sistema informático, con la intención general de robar información o dañar la organización atacando su sistema informático.
- Terroristas, son los elementos con fines violentos que atacan a una organización con el fin de crear el mayor daño o realizar sabotaje.
- Intrusos pagados, son los individuos o elementos a sueldo que intenta acceder a un organización por encargo de un tercero, para múltiples fines.

Amenazas lógicas:

- Software incorrecto: este es el elemento pasivo de vulneración de la seguridad, pues si no es probado correctamente puede poner el riesgo la organización, pasando desapercibido por los sistemas de seguridad.
- Herramientas de seguridad: son los programas de software que permiten controlar los accesos y administrar las políticas de seguridad de una organización.
- Puertas traseras: se les denomina así a los programas que abren conexiones para permitir el acceso de atacantes.
- Bombas lógicas: son código de software que es activado baja ciertas condiciones para realizar algún tipo de daño.
- Virus: es el software diseñado con la intención de dañar los sistemas informáticos
- Gusanos: programas de software que se expanden y se basa en la reproducción e infección en cadena.
- Troyanos: similar a las puertas traseras.

- *Spywares*: programas de software que se alojan en los sistemas con la intención de recolectar información de los usuarios y/o general publicidad.

Catástrofes

- Incendios
- Ataques terroristas
- Accidentes

1.5 Como protegernos

Como parte del proceso de protección de nuestros sistemas debemos determinar el mecanismo de protección, se ha clasificado en general en tres aspectos:

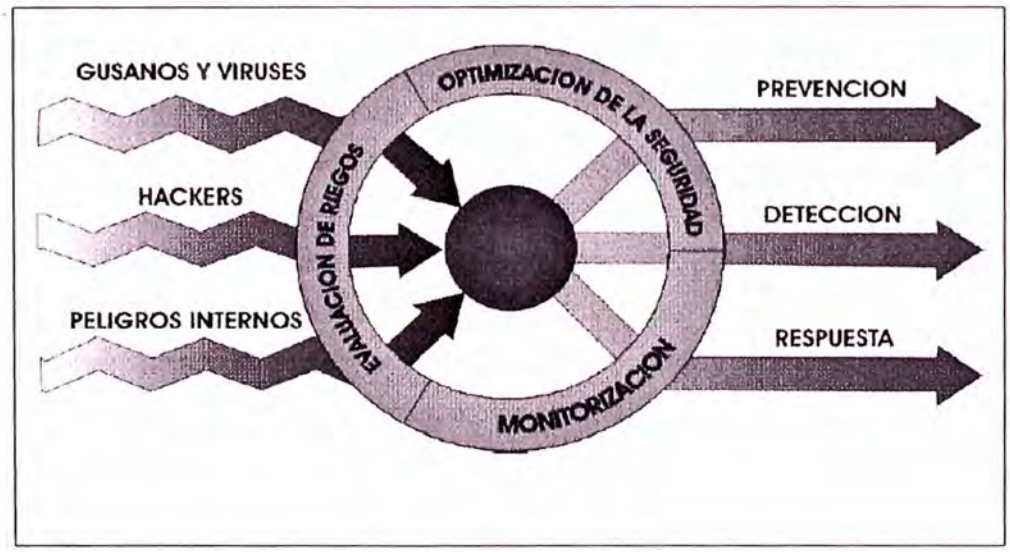

FIG. 1.1 ROLES DE LOS SISTEMAS DE SEGURIDAD

1.5.1 Prevención

Proceso por el cual se implementa mecanismos de seguridad con el objetivo de prevenir y contener ataques y/o determinadas brechas de seguridad, estos mecanismos operan durante los procesos normales de funcionamiento de un sistema.

Recurrentemente se diseñan planes de mantenimiento preventivo para optimizar los sistemas y asegurarlos, aquí también se encuentran los diseños de seguridad de la red, la

implementación de *firewalls*, detectores de intrusiones, sistemas de prevención de intrusiones, antivirus, implementación de las políticas de acceso a los usuarios, entre otras.

1.5.2 Detección

Se ubican aquí elementos de auditoria y los de alerta en tiempo real con el objetivo de detectar violaciones de seguridad.

En este nivel se espera que los sistemas que se han implementado operen satisfactoriamente en ambientes de producción y los sistemas de alerta sean activados oportunamente y cualquier ataque sea bloqueado.

Es importante resaltar aquí sobre los sistemas de detección de intrusiones que estos podrían alertar pero no siempre podrían bloquear los ataques, pues estos sistemas son sistemas pasivos por concepción, requiriéndose sistemas de prevención de intrusiones para fortalecer la reacción en tiempo real.

1.5.3 Recuperación y respuesta

Se refiere a aquellos mecanismos luego de que se ha detectado la violación del sistema; aquí se ponen en funcionamiento planes de contingencia, recuperación, *backups*, etc.

Esos planes se refieren a los mecanismos previstos de incidentes de compromiso en los sistemas.

Regularmente en este nivel, la detección de un ataque o intento de intrusión y si son a sistemas críticos, deben ser bloqueado inmediatamente y luego rastrearse; pero en determinadas condiciones si el sistemas no es critico, puede activarse los mecanismos de rastreo, mas aun si el atacante proviene de la misma organización, dado que es tan importante ubicar a agresor como detener el acceso indebido.

Se puede mencionar un mecanismo *post* investigación, llamado **análisis forense**, procedimiento con el cual se intenta determinar la naturaleza del ataque o vulneración, el nivel de daño o compromiso, y los niveles de responsabilidad de lo producido.

Y por el cual se deben determinar y responder las siguientes interrogantes:

- Quien realizo el ataque.
- Como se realizo el ataque.
- Cual fue el impacto del ataque.

Luego de exponer estos conceptos podemos englobar un esquema completo [8] de sobre la

seguridad informática en la siguiente estructura.

Visión global de la seguridad informática

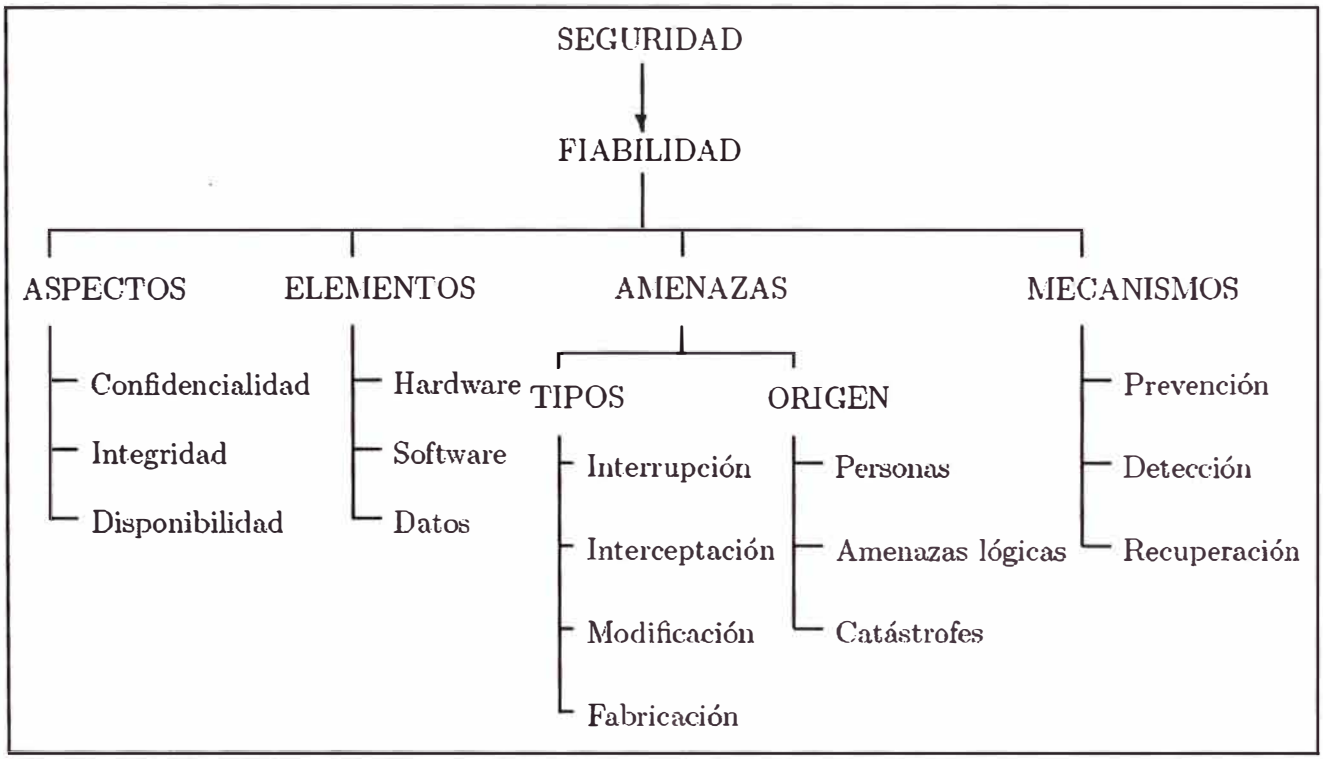

FIG. 1.2 ESTRUCTURA Y ELEMENTOS DE LA SEGURIDAD INFORMÁTICA

1.5 Resumen del capitulo

En este primer capitulo se ha esbozado los conceptos primarios de seguridad informática, conceptos que se han estandarizado, y que definen los campos de acción, los métodos de análisis, clasificación de ataques, y una visión global de la estructura de seguridad informática.

El concepto más importante que se menciona son los 3 tipos de cualidades de niveles para medir un sistema fiable, como son la disponibilidad, confiabilidad e integridad.

CAPITULO II

AUDITORIA INTERNA DE SEGURIDAD

Luego de que se ha obtenido un primer alcance de la visión de seguridad para nuestros sistemas, se debe realizar la primera evaluación del estado actual de nuestra arquitectura de seguridad, un procedimiento regular de evaluación de la seguridad es:

- Evolución de las políticas
- Fecha de implementación
- Periodo de actualización
- Descripción de los procedimientos
- Mecanismos de protección
- Evolución del diseño de la red.
- Evaluación de vulnerabilidades en equipos de red
- Evolución de vulnerabilidades en servidores
- Evolución de vulnerabilidades en estaciones de trabajo
- Descripción de elementos de protección de red – *firewall* , *IDS* etc.-
- Respuesta a emergencias.
- Análisis de tráfico en enlaces remotos.

Las Auditorias se realizan en base a componentes que son distribuidos en cada elemento a monitorear. El flujo de componentes se muestra en la Fig. 1.3

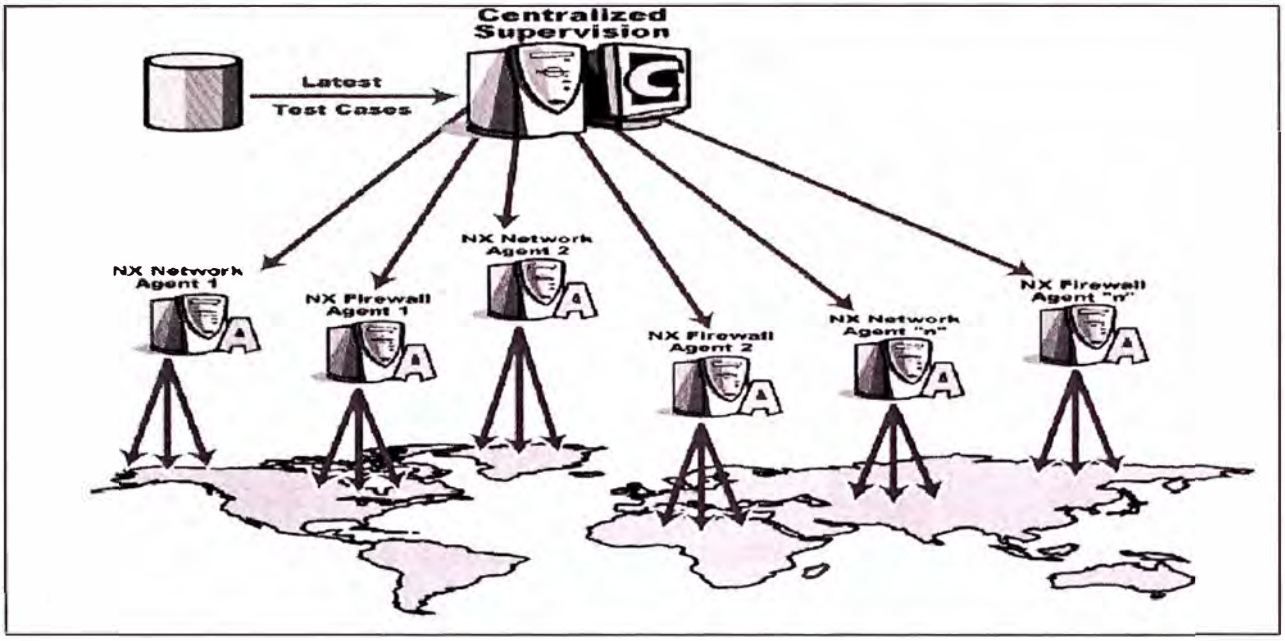

FIG. 2.1 ELEMENTOS EN LOS SISTEMAS DE AUDITORIA DE SEGURIDAD

Debido a que es recurrente la necesidad de auditoria en sistemas de seguridad, esta disciplina cuenta con estándares internacionales, uno de los conocidos es el **OSSTMM** (Open Source Security Testing Methodology Manual)

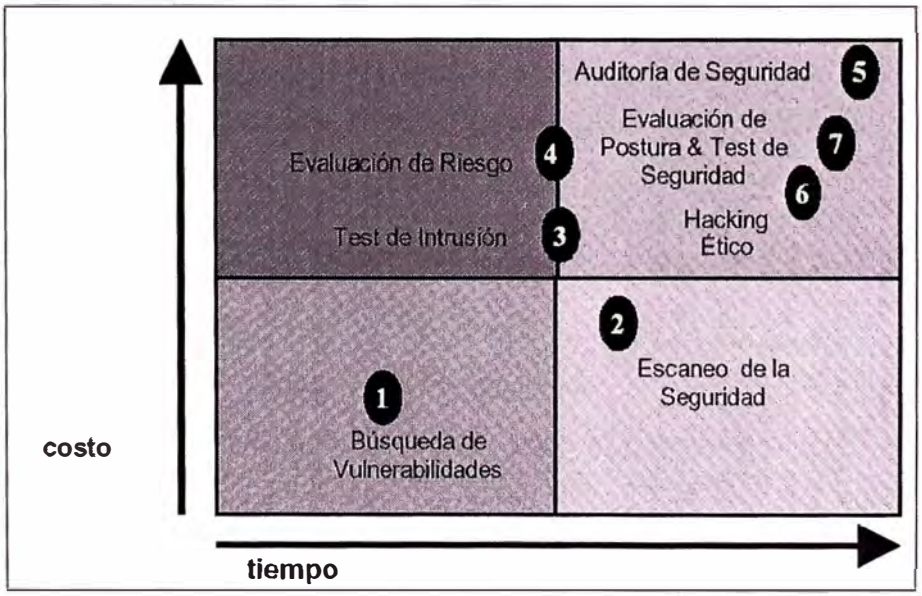

FIG. 2.2 COMPONENTES DE AUDITORIA

Los siguientes los componentes presentes en dicho modelo:

- Búsqueda de vulnerabilidades
- Escaneo de Seguridad
- Prueba de intrusión
- Evolución de riesgo
- Auditoria de seguridad
- *Hacking* ético
- Prueba de seguridad y su equivalente militar.

Como parte de proceso de evaluación de la existencia de seguridad en un determina organización se debe construir un mapa de seguridad de la información constituido por los siguientes elementos:

- Seguridad de la información.
- Seguridad en los procesos.
- Seguridad en las tecnologías de Internet.
- Seguridad en las comunicaciones.
- Seguridad inalámbrica.
- Seguridad física.

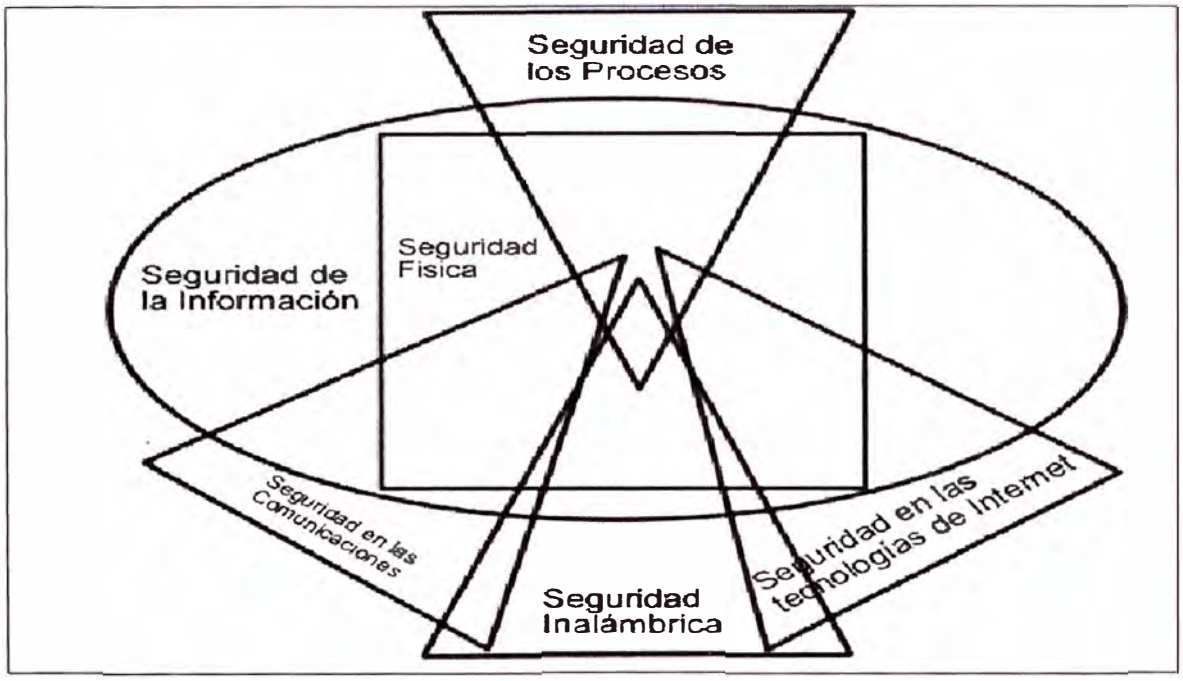

FIG. 2.3 MAPA DE LA SEGURIDAD DE LA INFORMACIÓN

2.1 Seguridad de la información

- Revisión de la inteligencia competitiva.
  Es la recolección de información en un medio como la Internet u otros, para luego ser analizada, este en un método de investigación no invasivo.
- Revisión de la privacidad.
  Es el punto de vista legal y ético sobre la transmisión almacenamiento y control de los datos con respecto a la privacidad del cliente y del empleado.

- Recolección de documentos.
  El objetivo es formar un perfil de la organización y de los empleados, así como la red de la organización, adicionalmente se incluyen perfiles sobres los elementos de terceros con los que se interacciona.

2.2 Seguridad de los procesos

- Prueba de solicitud.
  Es el método de obtención de privilegios de accesos a una organización utilizando técnicas comunes de ingeniería social.
- Prueba de sugerencia dirigida.

Es el método en enumeración de puntos de acceso con la intención de recolectar dirección IP internas.

- Prueba de personas confiable.
  Se basa en le obtención de acceso usando posiciones de confianza, como de socios, familiares o otros.

2.3 Seguridad de las tecnologías de Internet

En esta sección se analizan módulos para sistemas que se encuentran directamente conectados a la Internet.

2.3.1 Logística y controles

Esta relacionado con la reducción de falsos positivos y negativos, como por ejemplo paquetes TCP/UDP perdidos, problemas con el enrutamiento, etc.

2.3.2 Sondeo de red

Es el punto de partida del análisis basado en la recolección de datos, obtención de la información y políticas de control.

2.3.3 Identificación de los servicios de sistemas

Es la parte correspondiente a la pruebas invasivas de los sistemas, con la intención de descubrir posibles brechas de seguridad, en este modulo se realizan los escaneo de puertos, se deben entonces aquí recolectar la información sobre:

- Dirección IP de los sistemas activos
- Puertos abierto filtrados o cerrados.
- Protocolos túnelizados y encapsulado.

En esta etapa de deben realizar el siguiente diagnóstico:

- Recoger respuesta de *broadcast*.
- Intentar traspasar los cortafuegos con valores estratégicos de TTLs para todas las direcciones IP.
- Utilizar el protocolo ICMP junto con la resolución inversa de nombres.
- Utilizar paquetes TCP con puertos de origen 80 y con el *bit* ACK en estado activo en los puertos de destino 3100-3150, 1001-10050,33500-33550 y 50 puertos aleatorios por encima de 35000 para todos los *host* de la red.

- Utilizar paquetes TCP fragmentados en orden inverso mediante escaneo FIN, NULL y XMAS en los puertos de destino 21, 20, 25, 80, 443.
- Realizar intentos de conexión a DNS para todos los servicios de la red.
- Realizar conexiones FTP y con conexiones a *proxy* locales, para realizar los *scans* a diversas zonas protegidas, utilizando los puertos 22, 81, 111, 132, 137 y 161.
- Realizar *scans* SYN TCP (Half-Open).
- Realizar *scans* TCP *full connect* para escanear todos los servidores de la red.
- Realizar *scans* TCP fragmentados en orden inverso para enumerar puertos y servicios.
- Realizar *scans* con el protocolo para servicios que utilicen el protocolo UDP.

2.3.4 Búsqueda de información competitiva

Búsqueda de información a partir de la presencia en Internet y que se puede tratar como información sobre el negocio, realizar un mapa de la estructura de directorios de los servidores web y ftp. Así mismo registra posible productos encontrados en redes P2P (*point to point*).

Verifica los contratos que se puedan realizar a través de la Internet utilizando firma digital.

2.3.5 Prueba de aplicaciones de Internet

Es cuando se emplean diversas técnicas de prueba de software con el objetivo de encontrar posibles brechas de seguridad y se consideran los siguientes aspectos:

- Descomponer o reconstruir los códigos binarios, si es posible.
- Reconocer las especificaciones del protocolo en base a los mensajes de error o *debug*.
- Uso de técnicas de acceso por combinación de contraseñas por fuerza bruta.
- Recopilar las limitaciones del control de acceso en las aplicaciones tiempo de uso de las sesiones, tiempo inactivo y permisos.
- Identificar la información sobre el tipo de autenticación, por IP, por roles, por identidades, por *cookies*, por ID de sesión u otro modo de autenticación.
- Determinar las limitaciones de uso de sesión, ocupación del ancho de banda, limitación de transacciones, o descarga de archivos.
- Recolectar información sensible en base a ataques de '*Man-of-Middle*' supervisados.

- Encontrar las limitaciones de variables, protocolos, longitud de datos tipos de datos etc.
- Intentar provocar desbordamiento de memoria usando cadenas de caracteres largas.
- Utilizar técnicas de inyección de comandos SQL en las entradas de cadenas de aplicaciones *web* con conexión a base de datos.
- Utilizar comandos remotos a través de "*Server Side Include*"

2.3.5 Enrutamiento

Se deben revisar sobre este dispositivo que actúa de *gateway* las reglas de control aplicadas las llamadas ACLs, y deberá asegurarse que solo sea permitido expresamente el tráfico y el acceso; dado que este dispositivo es cada vez mas complejo se debe limitar la auditoria a determinar la función de estos equipos dentro de la organización.

Verificar los siguientes parámetros:

- Revisión de ACLs, contrarrestarlas contra las políticas de seguridad
- Verificar si los *routers* están filtrando tráfico de la red local hacia fuera.
- Comprobar que se estén bloqueando y detectando direcciones falsas.
- Cuantificar las capacidades de manejo de paquetes muy pequeños y muy grandes.
- Registrar la capacidad del *router* de manejar fragmentos coincidentes como los usados en ataques TEARDROP.
- Prueba de sistemas de control de acceso.

  En esta sesión se realizan las pruebas a los sistemas de *firewalls* existentes en la organización, los siguientes son las pruebas requeridas:

a) Revisión de las ACLs o reglas de seguridad aplicadas
b) Verificar si el *firewall* esta filtrando el tráfico de la local hasta afuera.
c) Verificación de los reglas de traslación de direcciones ocultas y estáticas.
d) Comprobar que el *firewall* este bloqueando y detectando direcciones falsas.
e) Examinar la factibilidad de identificar el *Firewall* a través de destinos tipos de respuesta.
f) Utilizar técnicas de SYN oculta y verificar su bloqueo.
g) Medir la capacidad del *firewall* de manejar parámetros pequeños.
h) Examinar la respuesta del *firewall* para ataques de inundación de SYN
    a. y de respuesta a paquetes con la bandera de RST activada.

i) Examinar su protección contra ataques usando paquetes ACK, FIN, NULL y ataques midiendo el tamaño de la ventana en el paquete (WIN).
j) Examinar su protección contra paquetes encapsulados, ataques de denegación de servicio con conexiones TCP ininterrumpidas, TCP temporales, datagramas UDP, y contra ataques usando protocolo ICMP.

2.3.6 Prueba de sistemas de detección de intrusos

Aquí se concentra el examen a la configuración de los sistemas de intrusiones las siguiente son las pruebas que se deben realizar:

- Verificar el tipo de IDS con la información recolectada con la inteligencia de la información.
- Determinar las esferas de protección o de influencia.
- Testear los estados de alarmas del IDS.
- Examinar los parámetros de sensibilidad de las firmas pasado 1 minuto, 5 minutos, 60 minutos y 24 horas.
- Examinar la configuración del IDS para reacciones múltiples ataques por inundación variados.
- Examinar la configuración del IDS para ataques con URL manipulada y rutinas de explotación.
- Examinar la configuración del IDS ante cambios de la velocidad y cambios aleatorios de velocidad en el envió de paquetes.
- Examinar la configuración del IDS antes cambios aleatorios de protocolo durante un ataque.

2.3.7 Prueba de medidas de contingencia

Aquí se encuentran las siguientes medidas:

- Medir el mínimo de recursos necesarios que se necesitan en el subsistema para realizar las tareas.
- Verificar los recursos disponibles a este subsistema que necesiten realizar estas tareas, y que recursos están protegidos desde este subsistema.
- Verificar la detección de medidas presentes para la detección de intentos de acceso a los recursos protegidos.
- Verificar recursos innecesarios.
- Verificar las propiedades del sistema de contingencia.

- Verificar la detección de medidas presentes para la detección de accesos "no comunes" a los recursos "necesarios".

2.3.8 Evaluación de las políticas de seguridad

Las políticas de seguridad son el ente rector de la seguridad de la información en una organización, y deben realizar las siguientes funciones para su verificación:

1. Examen del contenido y contrarrestarlo con el estado actual de las conexiones y permisos.
2. Verificar que la política esta dentro de la justificación del negocio, y las normas locales y regionales e internacionales, sobre todo con respecto a las derechos y responsabilidades tanto como del empleados como de los empleados.

2.4 Seguridad de las comunicaciones

Comprende el análisis de los sistemas de comunicaciones de voz

- Prueba de la PBX:

a) Revisar los sistemas de registros para verificar posibles abusos del servicio.
b) Examinar que las cuentas administrativas no tengan contraseñas por defecto.
c) Examinar que el sistema operativo se encuentre actualizado y con los últimos parches aplicados.
d) Verificar el acceso remoto para el mantenimiento del sistema.
e) Comprobar la autenticación de las llamadas entrantes.

2.5 Seguridad inalámbrica

Las redes inalámbricas están en constante expansión, pero también sus posibilidades de intrusión utilizando estos medios están presentes.

- Verificación de la radiación electromagnética (EMR)
- Verificación de las redes inalámbricas (802.11) y *Bluetooh :*
  a) Uso de algoritmos de cifrado basado en flujos RC4.
  b) Verificación de las políticas de seguridad para redes inalámbricas.
  c) Realizar el inventario de dispositivos inalámbricos.
  d) Determinar el nivel de control de acceso físico a los puntos de

2.6 Seguridad física

Entre los componentes principales se tiene:

- Revisión de perímetro
- Revisión de monitoreo
- Evaluación de control de accesos
- Revisión de respuestas de alarmas
- Revisión de ubicación
- Revisión de entorno

Dado el alcance del presente informe no se detallaran estos componentes.

2.7 Resumen del capítulo

En este capitulo se ha tratado sobre la necesidad y la forma en que se deber realizar una auditoria sobres los sistemas informáticos; como ha sido indicado se debe realizar antes y después de la implementación de las políticas de seguridad para evaluar nuestro real estado en materia del protección de la información.

El análisis de auditoria básicamente se ha centrado en los estándares internacionales como el OSSTMM, que define un mapa de la seguridad informática y sobre este mapa, se centra diversas pruebas y exámenes para verificar la configuración de los sistemas de seguridad.

CAPITULO III

POLITICAS, ESTANDARES Y PROCEDIMIENTOS DE SEGURIDAD

Actualmente para una mejor administración de la seguridad de la información, se elaboran un conjunto relacionados de documentos que se pueden subdividir en:

Políticas: Determina la causa de la protección, y aquí se plasma la concepción de la seguridad de la organización, así mismo su alcance, y las consecuencias de su incumplimiento, esta políticas son parte del conjunto de políticas globales de la organización

Estándares: Determina lo que se protege, y estos documentos son aplicados a las diversas dependencias de una organización sobre los controles en diversas objetos, físicos, administrativos o lógicos, que estén relacionados con la protección de la seguridad.

Procedimientos y guías: Determina detalladamente las operaciones a realizar para cumplir los estándares de una actividad especifica.

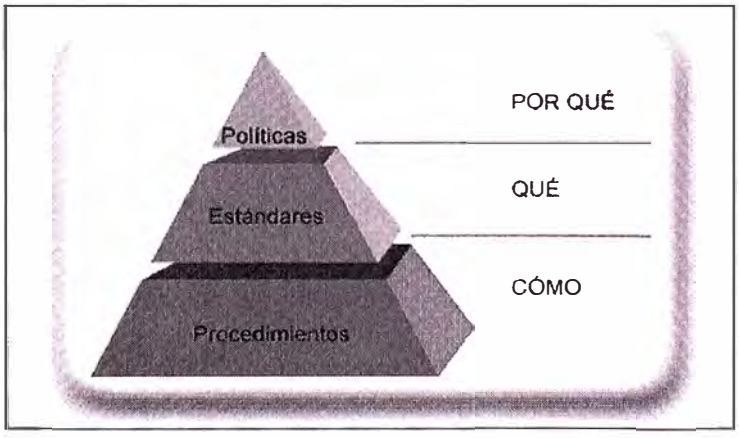

FIG. 3.1 NIVELES Y FUNCIONES DE LOS COMPONENTES DE SEGURIDAD

Formación: Este proceso se puede entender como colateral y cíclico para una mejor formación del personal que organiza la estructura de seguridad de un sistema.

El gráfico a continuación coloca los distintos elementos mostrados:

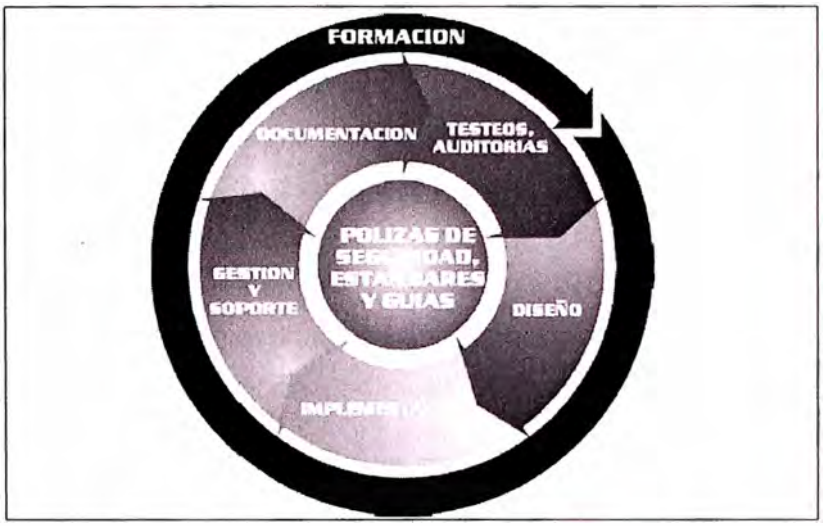

FIG. 3.2 CICLO DE VIDA DE LOS SISTEMAS DE SEGURIDAD

3.1 Construcción de las políticas de seguridad

Las políticas se construyen de manera particular a cada organización, pero algunos criterios son comunes y se desarrollan a continuación.

3.1.1 Identificación de activos

Se deben ubicar aquí a los elementos de la organización a ser protegidos, como: base de datos, software, hardware etc.

3.1.2 Identificación del valor de los activos

Se debe asignar distintos valores o pesos a los elementos a proteger, priorizando los objetos de naturaleza crítica para la marcha de la organización.

3.1.3 Identificación de amenazas

Se debe poder reconocer los potenciales peligros de diversa naturaleza que pueden atentar contra algún sistema de la organización.

- Amenazas externas: se requiere a elementos ajenos a la organización.
- Amenazas internas: se requiere a elementos internos a la organización.

3.1.4 Evaluación de riesgos

La evaluación de riesgos es la probabilidad de ocurrencia de una determinada amenaza, su impacto puede ser clasificado por el nivel de daño que podría causar.

3.1.5 Interrupción de operaciones

Este evento es recurrente ya sea por el tipo de ataque o como medida de protección o evaluación de daños.

3.1.6 Responsabilidad jurídica

Es cuando la organización se ve involucrada en la infracción de algún acuerdo de naturaleza comercial o legal, infringiendo convenios y/o normativas, pudiendo participar como demandado o demandante.

3.1.7 Reducción de competitividad

Las organizaciones que regularmente son afectadas por ataques deben desviar recursos, organización, tiempo, y otros elementos para superar el incidente, este se acrecienta cuando de por medio existe robo de información estratégica de la organización.

3.1.8 Perjuicio de imagen

En organizaciones privadas o comerciales, la imagen corporativa es uno de los activos mejor cuidados, y estos son afectados directamente en pérdida o desconfianza, aun si un determinado ataque es de baja intensidad, el efecto perceptivo es sumamente dañino.

3.1.9 Designación de responsabilidades

Es el equipo encargado de identificar las vulnerabilidades de una organización debe considerar un conjunto de personal multidisciplinario, como: especialistas en seguridad, administradores de red, asesores jurídicos y personal de recursos humanos.

3.2 Características de las políticas de seguridad

Para una mejor implementación de las políticas de seguridad estas deben poseer ciertas características:

- Debe ser de fácil interpretación para su implementación práctica.
- Debe ser concordante con las políticas de la organización.
- Debe definir las responsabilidades de cada persona o dependencia.
- Debe considerarse los aportes de las diversas dependencias y también tomar de base a la experiencia de la organización.
- No debe transgredir las políticas locales o regionales.

3.3 Estándares de Seguridad

De acuerdo a la estructura de organización de políticas, son los estándares de seguridad los que determinan que se debe proteger estableciendo lo que se debe proteger y los controles que se requieren para dicha protección.

3.4 Estándares Internacionales

Para ayudar a que las organizaciones construyan sus políticas de seguridad de manera efectiva, diversos organismos internacionales han emitido documentación que como realizar esta tarea.

Los estándares actuales en materia de seguridad de la información puede nombrarse a:

- BS-7799 , Año 1995, emitido por el Instituto de Estándares Británico
- ISO 15408 Año 1999
- ISO 17799 Año 2000 y basado en el estándares BS-7799
- ISO 27001 Año 2005

3.4.1 ISO 17799

Esta norma ha sido adoptada como base para la emisión de las correspondientes normas nacionales : NTP-17799 dicha norma clasifica y agrupa los sistemas de seguridad informática en controles de seguridad , las características mas importantes son :

1.- Políticas de Seguridad

Se refiere a la responsabilidad de la dirección de la política de seguridad de la información, que debe recaer en la alta gerencia, delimitando y extendiendo las políticas de seguridad a toda la organización.

La concepción de la seguridad de la información debe contener los siguientes elementos básicos :

- Definición de la seguridad de la información y objetivos, alcances e importancia de la misma.
- Trazar el objetivo de la dirección en base a los principios de la seguridad de la información.
- Breve explicación de las políticas, principios, normas y requisitos de conformidad de la organización.
- Identificación de las responsabilidades con respecto a la gestión de la seguridad de la información.
- Indicar las referencias a documentos que puedan sustentar la política.

2.- Organización de la seguridad

a) Infraestructura de la seguridad de la información

Compete la gestión de la información dentro del organización, recomendando que se realicen foros de gestión liderados por niveles gerenciales, con el fin de aprobar políticas de la información, asignar roles y funciones, de ser necesario el caso se deben tomar asesoramiento externo en materia competente.

Así mismo se debe realizar un enfoque multidisciplinario de la seguridad de la información con la participación de: directores, administradores, usuarios, auditores, desarrolladores, gestión de seguros entre otros.

La formación de un comité de gestión que garantice una dirección correcta de la seguridad de la organización:

- Se debe asignar un responsable en materia de seguridad de la información, asignando también propietarios para cada recurso.
- Es responsabilidad de cada gerente identificar y definir los diversos recursos y procesos de seguridad de su respectiva competencia.
- Se deben designar al gerente responsable de cada recurso y se deben documentar los detalles de esa responsabilidad.

b) Seguridad de accesos a terceros

Tiene por meta mantener la seguridad de las instalaciones y de procesamiento de la información a los que acceden terceras partes.

Para dichos accesos se de deben realizar una evaluación de riesgo para identificar los requerimientos de control.

Los requerimientos de seguridad deben estar garantizados dentro de los contratos de

servicios para con terceros, dentro de ellos se deben considerar las cláusulas como:

- Política general de la seguridad de la información.
- Procedimiento de protección de activos, y de comprobación de integridad de los mismos.
- Controles que garantizan la recuperación o destrucción de la información al finalizar el contrato.
- Restricciones de copia y divulgación de información.
- Derecho de auditar responsabilidades contractuales o contratar a un tercero para realizar dichas auditorias.
- Derecho a monitorear, revocar (impedir) la actividad del usuario.

c) Caso de tercerización de los sistemas de información

Cuando los sistemas de información son tercerizados para su administración y control , la garantía de la seguridad de dicha información debe ser contemplada dentro del contrato con los aspectos mas resaltantes

- Cumplimiento de requisitos legales.
- Proceso de comprobación de la integridad y confidencialidad de los activos de la organización.
- Tipos de controles físicos y lógicos para el acceso de usuarios.
- Plan de mantenimiento de la disponibilidad de los servicios ante desastres.
- Derecho de auditoria.

3.- Clasificación y control de activos

Unos de los componentes esenciales en la clasificación de los activos son los inventarios siendo este necesario para la gestión de riesgo. En base a la identificación y su valor se le proporciona los niveles de seguridad. Los activos asociados con sistemas de información son :

- Activos de información, archivos base de datos, documentación de los sistemas, manuales, documentación de formación, procedimientos, planes de continuidad, etc.
- Activos de software: software de aplicación, software del sistema, programas de desarrollo.
- Activos físicos: equipos de cómputo y comunicaciones (unidades centrales de proceso, monitores, portátiles, *módems*, *routers, switches*, sistema de aire acondicionado, sistema de energía.

Se debe evitar las sobre clasificación y/o clasificaciones complejas de la información pues esta tiene su importancia dentro de un tiempo determinado, esto evitara gastos innecesarios.

Los procedimientos para marcar y tratar la información debe estar presentes y de acuerdo con los esquemas de clasificación adoptada por la organización.
El tratamiento de la información debe cubrir las siguientes actividades :

- Copia.
- Almacenamiento.
- Transmisión por correo, fax, correo electrónico.
- Transmisión oral, incluida telefonía móvil, transmisión de voz y sistemas de respuesta automática (IVRs).
- Destrucción.

El movimiento de datos en sistemas que manejen información clasificada como sensible, deben llevar etiquetas de identificación adecuadas, en información electrónica se deben usar medios electrónicos de marcado.

4.- Seguridad del personal

Se refiere a los riesgos en errores humanos, robos fraudes o mal uso de las instalaciones y servicios.

Se deben utilizar controles de selección de personal como:

- Disponibilidad de las referencias satisfactorias sobre actitudes y/o capacidades.
- La comprobación del currículum vite del candidato.
- La confirmación de las certificaciones académicas y profesionales.
- Comprobación independiente de la identificación (pasaportes , carnet de extranjería, etc.)

En puestos de alta responsabilidad se deben realizar comprobaciones del crédito de la persona, sobre todo en materia financiera o de alta confidencialidad.
Para trabajadores procedentes de agencias de empleos el contrato con estas debe estipular sus responsabilidades en la selección así como el proceso de verificación si algún resultado son cuestionables.

Los directivos deben conocer que circunstancias privadas de su personal pueden afectar a su trabajo. Los problemas personales o financieros los cambios de comportamiento o estilo de vida, las ausencias recurrentes y la depresión o el estrés evidentes, podrían llevar a fraudes, robos errores u otras implicancias de seguridad.

Esta información debería manejarse de acuerdo a la legislación correspondiente.

La organización debe requerir la firma de acuerdos de confidencialidad a los recursos humanos externos o de los usuarios de terceros no cubiertos por contratos.

5.- Comunicación y administración de operaciones

Sirve para asegurar la correcta operación de los recursos de tratamiento de la información.

Para la ejecución de cada tarea se deben tener en cuenta las siguientes recomendaciones

- Proceso y utilización correcta del la información.
- Se deben realizar las instrucciones sobre el manejo de errores y otras condiciones excepcionales.
- De deben utilizar instrucciones especiales como por ejemplo para la impresión de resultados confidenciales sobre papeles especiales, con procedimientos de destrucción segura cuando resulte tareas fallidas.
- Procedimientos de re inicio del sistema y los procedimientos de recuperación a utilizar en caso de falla.

Unos de los controles mas importantes es el relacionado con el control de cambios, un control inadecuando y más aun, no documentado, es una falla recurrente de seguridad y del sistema.

Para este escenario considérese las siguientes medidas :

- Identificación y registro de cambios significativos.
- Evaluación del posible impacto de los cambios.
- Existencia del procedimiento formal de aprobación de los cambios que se propone.
- Comunicación de los detalles a las personas involucradas.
- Procedimiento que identifique las responsabilidades de abortar y recuperar los cambios sin existo.

Para los procesos de gestión de incidencias se deben crear los procedimientos necesarios para una respuesta rápida y eficaz y ordenada.
Se deben cubrir aquí los planes de contingencia que se diseñados para recuperar los sistemas tan rápido como sea posible.
De deben también evaluar el uso de evidencias como prueba de posibles incumplimiento de contratos, reglamentos o políticas internas de la organización.
Se recomienda que, se utilicen la segregación de tareas para reducir el riesgo de errores por accidental o negligencia. Para esto se deben separar la gestión de la ejecución de ciertas tareas.
Se deben también realizar las segregación de recursos para las áreas de desarrollo, pruebas (o pre producción) y producción, delimitando así mismo las responsabilidades y los procedimientos de transferencia de aplicativos para su puesta en producción. Para este escenario las recomendaciones son

El software de desarrollo y producción deberían, funcionar en procesadores diferentes o en dominios o directorios diferentes.

- Las labores de desarrollo deberían separarse tanto como sea posible.
- Bloquear el uso de compiladores editores u otros servicios de los sistemas de producción, cuando estos no se requieran.
- Utilizar distintos mecanismo de conexión e información del sistema para que sea plenamente identificado cada entorno de ejecución.
- El equipo de desarrollo debería acceder a las contraseñas de producción solo donde se hallan establecido los controles necesarios, y las mismas ser revocadas luego de ser utilizadas.

Se deben implementar las políticas de protección contra software malicioso se deben tomar las siguiente recomendaciones:

- Política de cumplimiento de licencias de software y la prohibición de uso de software no autorizado.
- Política expresa de protección contra riesgos asociados del uso de archivos, programas o otros elementos que provengan de redes externas.
- Existencia de planes de continuidad de negocio apropiados contra ataques de virus.

Para la recuperación de la información se deben tener las siguientes recomendaciones :

- Almacenamiento de niveles aceptables de información de respaldo a distancias prudentes del local principal.
- Se deben respaldar un mínimo de 3 generaciones o ciclos de la información de respaldo para las más importantes aplicaciones de la organización.
- Se deben probar regularmente la información de respaldo para comprobar su integridad.

Cuando se realicen intercambio de datos entre organizaciones deben estar basadas en acuerdos formales incluyendo los de custodia de software.
Se deben tener presente las siguientes consideraciones:

- Responsabilidad de administrar el control y notificación de la transmisión su despacho y recepción.
- Deben existir procedimientos de notificación de envíos, transmisión despacho y recepción.
- Se deben cumplir las mínimas normas técnicas de empaquetado y transmisión.
- Verificación de la identidad del mensajero.
- Definirse las responsabilidades y obligaciones en caso de perdida de datos.
- Uso de medidas especiales requeridas para proteger los elementos sensibles como contraseñas y claves criptográficas.

Para sistemas de comercio electrónico, donde el medio es no confiable se deben realizar las siguientes consideraciones de control:

- Determinar el nivel de confianza que deberían requerir el vendedor y el comprador en la identidad que afirma el otro.
- Determinación de la responsabilidad de fijación de precios redacción de documentos claves.
- Información de precios y la garantía respecto a la lista de precios contra los acuerdos secretos sobre descuentos.
- Lograr la confidencialidad e integridad de los detalles de los pedidos.
- Protección del riesgo frente a transacciones fraudulentas.

En cuando a políticas de uso de sistemas de correo electrónico se deben tener en consideración los siguientes aspectos

- Protección contra ataques de virus.
- Protección de los archivos adjuntos de posible filtración de información sensible.
- Responsabilidad del empleado del uso correcto del correo, no realizando difamaciones, hostigamientos, compras, suscripciones de servicios online entre otros.
- Uso de técnicas de cifrado para la protección del contenido e integridad de los mensajes electrónicos.

6.- Control de accesos

Durante la política para el control de accesos se debe tener en consideración:

- Distinción entre reglas a cumplir siempre y las opcionales
- Se debe establecer como premisa la regla : "**esta prohibido todo lo que no esta permitido explícitamente**"
- Se deben formalizar los procedimientos de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios.
- Entrega a los usuarios de una relación escrita de sus derechos de acceso.
- Petición a los usuario para que reconozcan con su firma la compresión de las condiciones de acceso.
- Revisar con frecuencia los derechos de acceso de los usuarios, cada 6 meses por ejemplo y a intervalos menores para usuarios con accesos especiales, (3 meses).

Para el uso de contraseñas se recomienda lo siguiente :

- Mantener en confidencialidad las contraseñas.
- Evitar la escritura en papel, salvo que existan formas seguras de almacenamiento.
- Seleccionar contraseñas de buena calidad con longitud mínima de 6 caracteres que sean fáciles de recordar, no basado en diccionario.
- Habilitar la política de cambio necesario de contraseñas a intervalos regulares de tiempo.

Para usuarios de servicios múltiples o plataformas son aconsejables mantener una sola contraseña de calidad que brinde un nivel razonable de protección.

Para el acceso a la red se requiere el uso de 'rutas forzosas' esto se refiere a

implantar mecanismos de protección en distintos puntos de la red para que un usuario no puede acceder directamente a los recursos a proteger , se pueden tomar en cuenta las siguientes consideraciones :

Limitar las opciones de menús para usuarios particulares:

- Evitar recorridos cíclicos ilimitados en la red.
- Forzar el uso de sistemas de seguridad para accesos de usuarios externos.
- Restringir el acceso a la red estableciendo dominios lógicos separados, como VLANs.

Sobre el control de acceso a sistemas operativos se debe tener en consideración los siguiente aspectos

- Identificación y verificación de cada usuario autorizado y terminal de acceso.
- Cuando sea el caso, restringir los tiempos de conexión.
- Registro de intentos fallidos de conexión.
- Tiempo forzoso de espera antes de permitir un nuevo intento.

Los mecanismos de acceso de emergencia o *recovery password* deben ser fuertemente controlados y restringidos mediante claras políticas de seguridad.

Deben también implementarse mecanismos de protección contra coacción y que los usuarios tengan facultad de lo activación y alarma, estos deben ser definidos con procedimientos y acciones de respuesta ante este evento.

Se deben crear políticas de desactivación de terminales en ambientes de riesgos.

Para efectos de realizar auditorias y seguimiento correcto de eventos es necesarios que exista sincronización de los relojes de los procesadores.

Se deben implementar políticas de control para equipos o accesos móviles, que deben incluir, protección física, técnicas de criptografía, respaldos, así mismo diversas recomendaciones y precauciones para su conexión en lugares públicos.

Para el caso de escenarios como la necesidad del tele trabajo, deben tener en consideración lo siguiente :

- Seguridad física real del lugar de donde proviene.
- Que se cumplan los requisitos de seguridad de la comunicación, de acuerdo a la necesidad del acceso, el valor del activo y su criticidad.
- Definición del trabajo permitido, el tiempo de acceso.
- Reglas y guías sobre la familia y el acceso de visitas al equipo y la información.

7.- Desarrollo y mantenimiento de los sistemas

El objetivo de este control es incorporar la seguridad a los diversos sistemas de información, realizando requerimientos de seguridad antes del desarrollo de los sistemas.

Los controles que son implementados en las etapas de diseño son muchos menos oneroso que su implementación luego de la puesta en producción de los sistemas.

Uno de los controles necesarios a aplicarse son relacionados con la validación de los datos de entrada, estos deben ser aplicados a las entradas de las transacciones de negocios se pueden mencionar las siguientes consideraciones

- valores fuera de rango, caracteres inválidos, datos incompletos, volúmenes de datos en exceso.
- Revisión periódica de los contenidos de campos clave o archivos de datos para confirmar su valides e integridad.
- Procedimiento para responder frente a errores de validación
- Determinación de responsabilidades

Para los controles de verificación se deben tener en consideración los siguientes aspectos:

- Control de sesión o lotes para contrarrestar los archivos de datos luego de las actualizaciones transaccionales.
- Control de balance para la comprobación entre los cierres y apertura
- Totalidad de registros y archivos.
- Verificación de la ejecución de las tareas en el momento y orden correcto, de producirse fallas que se detenga el procesamiento posterior y se genere alarma.

Se deben aplicar también los controles a los datos de salida, y asegurar que los datos a almacenar seas los correctos, las consideraciones son:

- Comprobar la plausibilidad de los datos que se obtienen.
- Realizar control de conciliación de cuentas.
- Proveer información suficiente para que el sistema siguiente puede realizar los controles respectivos.
- Procedimiento para responder a las pruebas de validación de salidas.
- Delimitación de responsabilidades de todo el personal involucrado en el proceso de salida de datos.

Para efectos de proteger la confidencialidad autenticidad e integridad de la información pueden utilizar diversas técnicas de cifrado de la información para los cual se deben tener presentes :

- Enfoque gerencial respecto al uso de controles cifrados en toda la organización
- Políticas de administración de claves, junto con el uso de métodos para la recuperación de la información
- Funciones y responsabilidades de quienes implementan la política y administran las claves.
- Determinación del nivel apropiado del cifrado.
- Descripción del estándar que se ha adoptarse para la correcta implementación de la solución en la organización.

Para el uso del técnicas de cifrado también de debe tener en consideración las normas y restricciones nacionales y las cuestiones relativas al flujo de la información cifrada a través de las fronteras. También se deben tener en consideración los controles aplicados a la exportación e importación de tecnologías de cifrado.

Se deben implementar mecanismos como la forma digital que garanticen la autenticidad e integridad de los documentos electrónicos como transferencia de fondos, contratos, y convenios electrónicos.

Se deben implementar a bases de técnicas de cifrado de dupla de llaves relacionadas, donde una de ellas se utiliza para crear firmas (clave privada) y la otra se utiliza para verificarla (la clave pública). Se debe tener presenta la calidad del algoritmo, la longitud de las claves, así como también la situación jurídica de las firmas. De ser necesario establecer contratos de cumplimiento obligatorio que respalden su uso.

Para efectos de administración de las claves se deben tener en cuenta las siguientes recomendaciones

- General claves distintas para distintos sistemas cifrados y diferentes aplicaciones.
- Generar y obtener certificados de claves publicas.
- Garantizar la correcta entrega de claves incluyendo el procedimiento de su activación.
- Generar el procedimiento de cambio, destrucción y registro de claves y claves comprometidas.

Las claves que se manejan deben tener un tiempo de vigencia, y este periodo será determinado según el riesgo percibido.
La protección de las claves públicas también es esencial para evitar la falsificación de una firma digital, un posible atacante podría reemplazar una clave pública por la suya, contra este mecanismo se requieren el uso de certificados de clave pública. El importante que el proceso que genera estos certificados debe sea confiable, debiendo estas alojado en una organización reconocida con los controles y procedimientos de seguridad necesarios.
Para el caso de software que se opera se deben tener en consideración los siguientes aspectos :

- Las actualización de módulos solo debe ser realizada por el responsable designado.
- De ser posible los sistemas en operación solo deben almacenar códigos ejecutables.
- Estos códigos no deben ser implementados en los sistemas hasta que no se hallan realizado las pruebas necesarias de calidad y aceptación del usuario.
- Deben mantenerse un registro de auditoria de cada actualización o modificación de los programas.
- Se deben conservar las versiones previas de software como medida de contingencia

Se debe permitir el acceso lógico o físico a los proveedores con fines de soporte si resulta necesario, previa autorización de la gerencia.
Par el caso de modificación de códigos fuentes de programas se deben tener en cuenta las siguiente recomendaciones

- Se debe evitar el almacenamiento de códigos fuentes de programas en los sistemas que se encuentran en estado de producción.
- Se debe asignar un responsable de programas para cada aplicación.
- No se debe permitir el acceso irrestricto de personal de TI a los sistemas de almacenamiento de códigos fuentes.
- Deben mantenerse un registro de auditoria de todos los accesos.
- Se deben conservar las versiones de código antiguas, con los respectivos controles de fecha y hora exacta.

Para el caso de desarrollo de software por externos se deben tener en consideración los siguientes aspectos

- Acuerdos de licencias, propiedad de códigos y derechos de propiedad intelectual
- Certificaciones de calidad y precisión del trabajo efectuado.

- Acuerdos de custodia en caso de quiebra de tercera partes.
- Derechos de auditoria de la calidad y precisión del trabajo realizado.
- Requerimientos contractuales con respecto a la calidad del código.
- Realización de prueba previa para la detección de códigos troyanos.

8.- Administración de la continuidad de la organización

Se recomienda implementar el proceso de gestión de continuidad del negocio ante eventos como desastres naturales, accidentes fallas de equipo o acciones intencionadas.

Se deben tener en cuenta las siguientes recomendaciones:

- Identificar los riesgos que afronta la organización midiendo su impacto incluyendo la identificación y priorización de los procesos críticos.
- Tener presente la adquisición de los seguros como parte del proceso de continuidad del negocio.
- Probar y actualizar planes de continuidad del negocio.
- Incorporar la gestión de la continuidad del negocio a los procesos y estructuras de la organización.

Para efectos de garantizar seguridad a los planes de contingencia se deben tomar en cuenta los siguientes aspectos

- Análisis de varios posibles escenarios de eventos.
- Simulaciones, para entrenar al personal involucrado.
- Pruebas de recuperación técnica.
- Pruebas de recuperación en lugar alternativo.
- Prueba de recursos y servicios del proveedor.
- Ensayos completos.

9.- Cumplimiento de requisitos

Este control esta diseñado para el evitar el incumplimiento de la legislación existente en materia civil, penal o contractual.

Se deben identificar de forma explicita la regulación que se aplicable para los distintos mecanismos de control y responsabilidades.

Para el caso de productores de software se deben tener las siguientes consideraciones legales:

- Divulgar una política de conformidad de los derechos de autor de software que rija el uso legal de los mismos.
- Divulgar la norma para los procesos de adquisición de productos de software.
- Proteger los documentos de acreditación de licencias.
- Implementar controles para no sobrepasar del numero máximo uso de usuarios permitidos.
- Implementar el control para el uso de solo software autorizado y bajo licencia.
- Utilizar herramientas adecuadas de auditoria.

Para la protección de los registros de la organización de deben implementar controles para asegurar la protección de la documentación sensible, y contrarrestar posibles destrucción o falsificación.

Se deben tener en cuenta la posibilidad de degradación de los medios utilizados para el almacenamiento de registros, y como consecuencia implantar los mecanismos para el almacenamiento y bajo recomendación del fabricante de los medios mencionados.

En el caso de medios electrónicos de almacenamiento se deben asegurar la accesibilidad de los mismos tanto del formato como del medio, para cambios producto de la actualización tecnológica.

Sobre las pruebas, están son necesarias para apoyar cualquier sistema de control interno o acción disciplinaria, a su vez estos deben estar dentro de los procedimientos internos.

Para la aceptación de la pruebas, la organización debe asegurar que sus sistemas de información se rigen y cumplen normas, códigos y buenas practicas, para producir pruebas admisibles.

Con respecto a la calidad de las pruebas se requiere un rastro convincente de ella, se pueden tener en cuenta los siguientes aspectos:

- En el caso de documentación en papel, el documento original debe estar resguardado de forma segura, y con registro de quien, donde, cuando se encontró y quien atestiguo su descubrimiento.
- En el caso de la información en medio electrónico, se debe asegurar su disponibilidad realizando copias de los medios removibles, así mismo se deben registrar todas las acciones realizadas durante el proceso de copia.

Sobre la conformidad técnica, se deben realizar revisión periódica de los sistemas operativos, con el fin de asegurar la correcta implementación de las medida de control de

hardware y software, el mismo debe ser realizado por un personal especializado, ya sea por medio manual o utilizando herramientas automáticas que generen reportes, los mismos que luego pueden ser interpretado por un especialista técnico.
La prueba de conformidad mencionada también incluyen pruebas de intrusión, a cargo de especialistas independientes; si es que estas resultan exitosas se deberán tener la consideración entre la seguridad del sistema y la explotación inadvertida de otras vulnerabilidades.
Sobre el control para auditoria de sistemas se deben tener las siguiente consideraciones:

- Establecer los requisitos de la auditoria con en área responsable.
- Establecer el alcance del mismo.
- Permisos de solo lectura, al software y los datos.
- Se deben identificar explícitamente los recursos a ser accedidos
- Todos los accesos deberán ser registrados y supervisados para producir los controles de referencia.
- Todos los procedimientos , requisitos y responsabilidades deben estar documentados

3.5 Procedimientos

Como se menciono en capítulos previos, los procedimientos son los encargados finales de definir la manera y como se protegen los diversos sistemas. Estos procedimientos deben mantener estrecha concordancia con los estándares para garantizar una adecuada administración de las políticas de seguridad globales.

Si bien es cierto que los procedimientos son los que se deben cumplir en la labor cotidiana, estos no pueden ser inflexibles, se debe permitir cierto grado de excepciones.
Estas excepciones bajo circunstancias preestablecidas, pueden no cumplir con procedimientos puntuales, por supuesto estas excepciones deberán ser controladas, supervisadas y limitadas en el tiempo.

Los procedimientos para una compresión mas detallada por las diversas dependencias deberán tener un formato estándar evitando así confusión y simplificando su ejecución; así mismo, debido que los procedimientos pueden ser susceptibles a ser modificados, deber mantenerse un control de versiones de los mismos.

Para los casos de información sensible los procedimientos de control también deberán ser de acceso controlado para evitar cualquier información que sirva a un posible atacante.

3.6 Etapas en la elaboración de una política

Todo ciclo [5] de desarrollo para la elaboración de las políticas se puede clasificar en 11 módulos que corresponden a su ciclo de vida y estos a su vez se organizan en 4 fases.
La figura 3.3 muestra el esquema de organización.

3.6.1 Fase de desarrollo

Esta fase le compete la creación revisión y aprobación de la política.

- Creación: es la etapa donde se planifica investiga, y redacta la política. aquí se determina los requerimientos organizacionales, investigación de las mejores prácticas, y su aplicabilidad.
- Revisión: en esta segunda etapas de toma la documentación creada y debe ser remitida a un grupo independiente para su evaluación. En esta etapa se requiere que el creador de la política utilice las recomendaciones y se realicen los cambios necesarios.
- Aprobación: es la etapa final en la etapa de desarrollo de la política. Mediante este proceso se puede iniciar la implementación de la política.

3.6.2 Fase de Implementación

En esta fase la política es comunicada y acatada.

- Comunicación: Es la etapa de la difusión de la política, y forma parte de la fase de implementación, aquí se determina el alcance y el método inicial de distribución de las políticas, como distribución geográfica, cultura, idioma, entre otros, previendo recursos necesarios.
- Cumplimiento: compete a esta etapa la ejecución de la política, interaccionando con distintos niveles organizacionales para la mejor implantación de las políticas
  En cada situación, asegurando que dicha política es entendida.
- Excepciones: esta etapa es necesaria debido a situaciones operaciones, deberán ser identificadas, registradas y evaluadas, también es posible excepciones permanentes a la política justificando la no aplicación temporal.

3.6.3 Fase de Mantenimiento

Se refiere a la concienciación de la importancia de la política, su cumplimiento debe ser monitoreado garantizando su cumplimiento.

- Concienciación: es la etapa donde se realizaran los esfuerzos continuos para garantizar que las personas estén concientes de las políticas aplicadas.
- Monitoreo: es la etapa correspondiente donde se realiza los seguimientos y reportes del cumplimiento de la política, aquí se realizan evaluaciones de la efectividad de la política, como también las observaciones de diverso personal.
- Garantía de cumplimiento: en esta etapa incluye la garantía de cumplimiento de las políticas, es esta etapa también se consideran las contravenciones de la política, a fin de prevenir que sigan ocurriendo.
- Mantenimiento: en esta etapa esta contempla el proceso de garantizar la vigencia e integridad de las políticas, el seguimiento y las tendencias de cambios, tanto tecnológicos como de procesos.

3.6.3 Fase de Eliminación

Es a fase de retiro de la política cuando no caduque su aplicación.

- Retiro: luego de que las políticas han cumplido su finalidad y ya es prescindible entonces esta puede ser retirada, esta etapa corresponde a la fase de eliminación del ciclo de vida de la política.

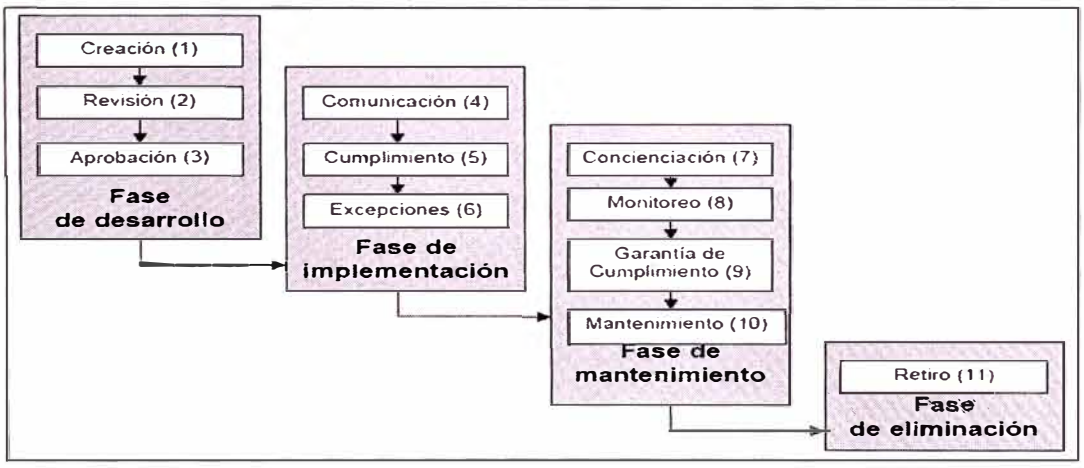

Fig. 3.3 FASES DEL CICLO DE VIDA DE LAS POLITICAS DE SEGURIDAD

3.7 Resumen del capítulo

En esta capitulo se ha estudiado los estándares presentes en materia de seguridad informática, las diferencias entre políticas de seguridad, estándares y procedimientos; conceptos resaltantes, pues permite manejar el ciclo de vida de un sistema de seguridad.
Se desarrolla tan bien el los aspectos mas resaltantes de la norma de seguridad ISO 17799 que es aplicable actualmente en el país.

CAPITULO IV

SEGURIDAD PERIMETRAL

Se entiende aquí los diversos elementos de diseño y de protección a los que son sometidas las redes para mitigar ataques a las redes.

Antes que nombrar las topologías mas conocidas mencionaremos algunos conceptos necesarios:

- **Intranet:** Se denota así a las redes internas de una organización o las que tienen control.
- **Extranet:** Son las redes de acceso externo para organizaciones asociadas que acceden a determinados servicios.
- **Internet:** Es el término general para denotar a las múltiples redes autónomas, interconectadas con el propósito de proporcionar una conectividad colectiva.
- **Host Bastión:** Se denomina así a la parte más expuesta de la red y de necesario fortificación.
- **Zona Desmilitarizada:** Se denomina así a la parte de la red interna que se encuentra destinada a una mayor protección.

4.1 Seguridad en Redes Básicas

Una red de este tipo cuenta generalmente con 2 módulos: el modulo de Internet y el modulo de la red de *campus*, [4] en la primera se puede observar los servicios de acceso como terminales VPN y servicios públicos: DNS, HTTP, FTP SMTP, etc. El segundo modulo están ubicados todos los usuarios finales. Ambos módulos son mostrados en la Fig. 4.1.

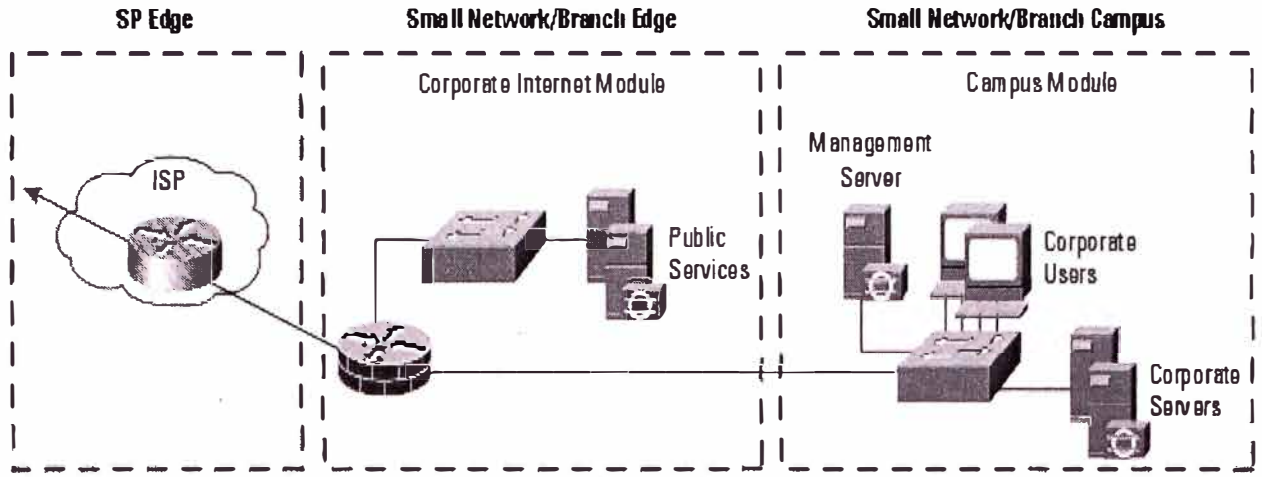

FIG. 4.1 ELEMENTOS DE UNA RED BÁSICA

Bajo este escenario se puede contemplar las siguientes características de mitigación de ataques:

- Accesos desautorizados: mitigación a través de filtros y *firewall.*
- Ataques a nivel de aplicación: mitigación a través de HIDS en los servidores públicos.
- Virus y troyanos: mitigación a través de escaneo de virus en el nivel de *host.*
- Ataques de *password*: Limitar los servicios disponibles a ataques de fuerza bruta.
- *Denial of Service*: Filtrar la taza de acceso (CAR) en coordinación con el ISP.
- IP *spoofing*: Solicitar filtro de protección en el ISP, y configurar el *firewall* local.
- *Sniffing* de Paquetes: Infraestructura de *switches* y protección a nivel de capa 2.

4.2 Seguridad en redes medianas

En este tipo de topologías se observa 3 módulos: el modulo de Internet, el modulo de *campus* y el modulo WAN, que son las conexiones hacia sedes remotas.

La red de *campus* o corporativa, posee *switches* de capa dos y capa tres, (capas referentes a los niveles OSI) sistemas de detección de intrusiones y sistemas de filtrado de paquetes.

Bajo este escenario se puede contemplar las siguientes características de mitigación de ataques:

- Accesos desautorizados: mitigación a través de filtros y *firewall.*
- Ataques a nivel de aplicación: mitigación a través de HIDS en los servidores públicos.
- Virus y Troyanos: mitigación a través de escaneo de virus en el nivel de *host.*

- Ataques de *password*: limitar los servicios disponibles a ataques de fuerza bruta.
- *Denial of Service*: filtrar la taza de acceso (CAR) en coordinación con el ISP.
- IP *spoofing*: solicitar filtro de protección en el ISP, y configurar el *firewall* local.
- *Sniffing* de paquetes: infraestructura de *switches* y protección L2.
- Topología de descubrimiento de la red:
- Ataques de *password*: mitigación con tiempo de intento
- Ataques de captura de password: son mitigados a través de conexiones remotas cifradas.

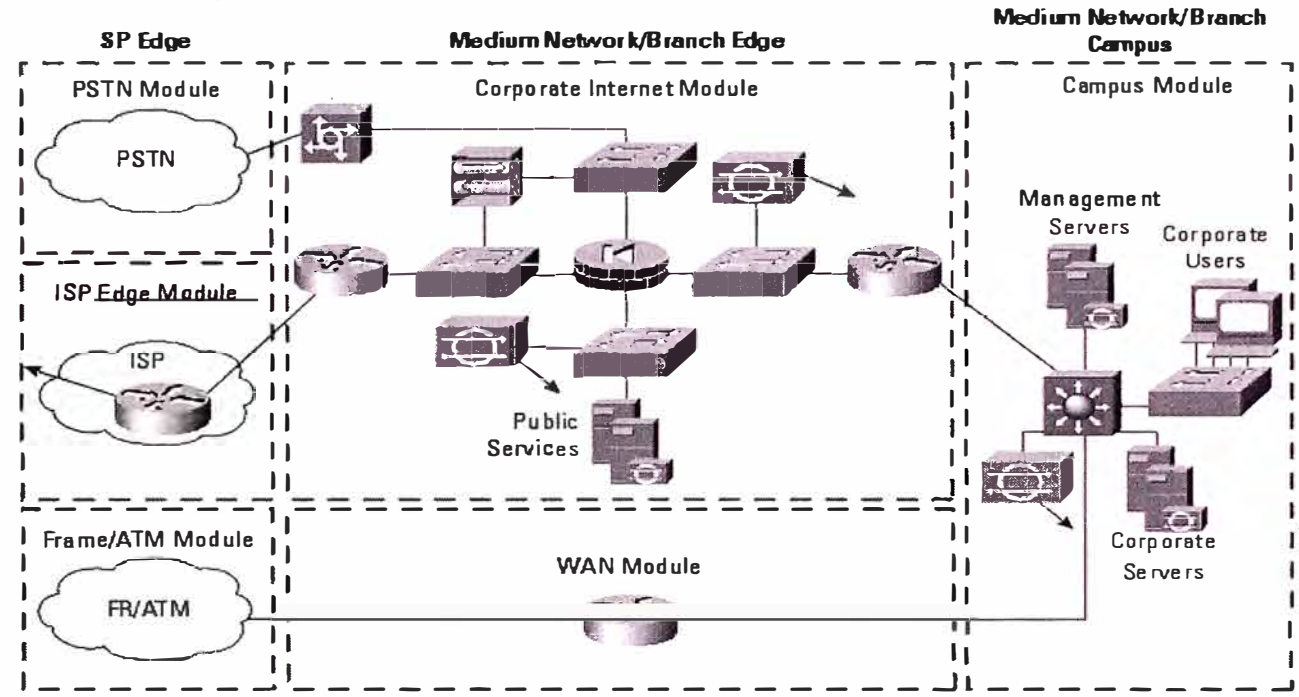

FIG. 4.2 ELEMENTOS DE PROTECCIÓN EN REDES MEDIANAS

En este tipo de redes se puede observar la presencia de elementos necesarios para la seguridad de una red, como son:

- *Firewall* Perimetral
- Sistema de detección de intrusiones
- Soporte de filtro de contención para ataques de *denial of service*
- Sistemas de autenticación para usuarios VPN.
- VLAN privadas
- Contenido de Inspección de trafico SMTP

Las distintas funciones de mitigación de cada componente son mostradas en la figura 4.3.

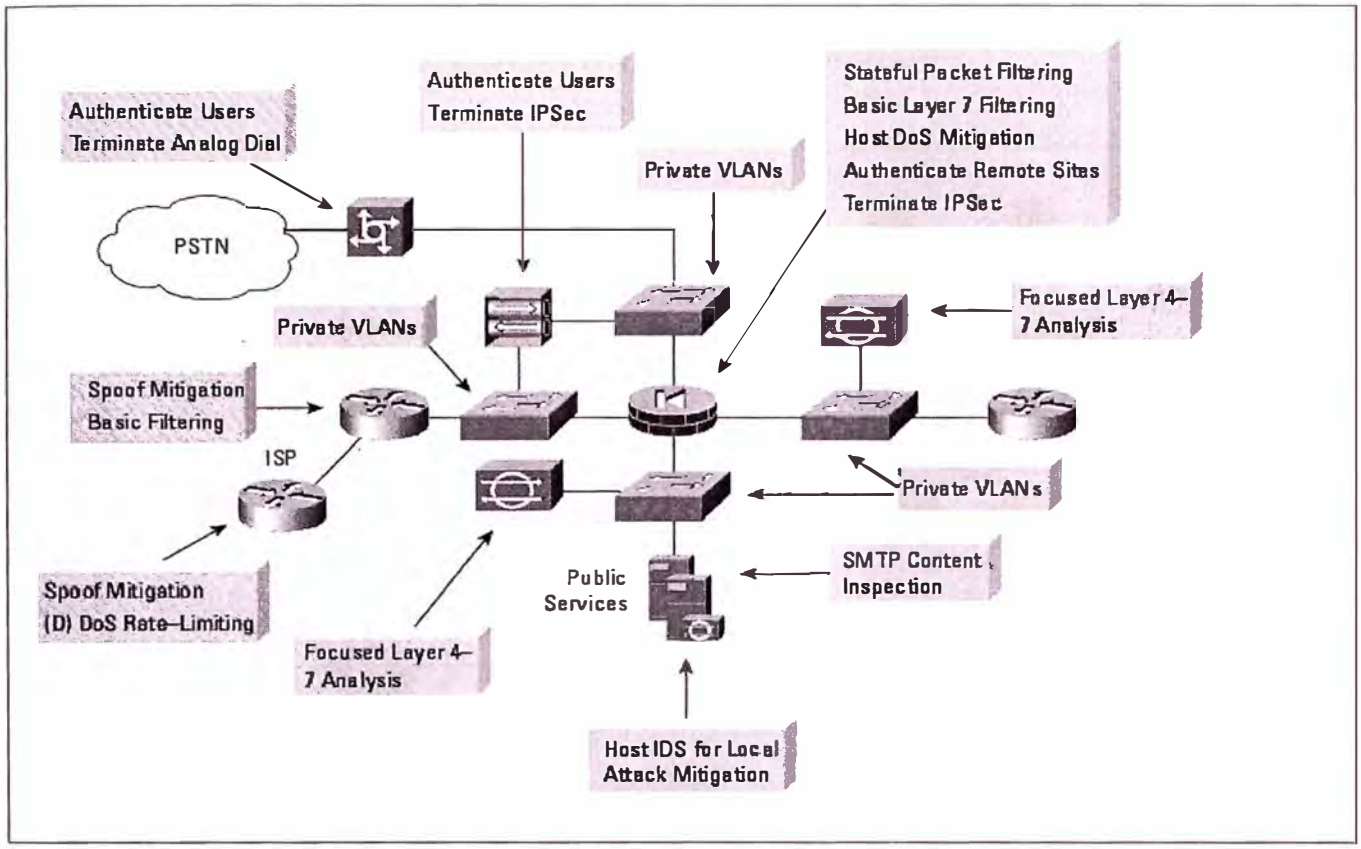

FIG. 4.3 ROLES DE MITIGACIÓN DENTRO PARA REDES MEDIANAS

Se pueden mencionar los siguientes aspectos de mitigación:

- Autenticación de usuarios en terminales de conexión analógica.
- Autenticación de usuarios en conexiones VPN.
- Mitigación de *spoofing* en *routers* de la organización y el ISP.
- Análisis focalizado de tráfico en capas 4-7 utilizando IDS
- Mitigación de Ataques utilizando IDS de *host*.
- Filtrado de paquetes, filtrado básico a nivel de capa 7, mitigación de DoS en el *Firewall* principal.
- Inspección de contenido en SMTP.
- VLAN privadas en *switches* de *core*.

4.3 Seguridad en redes de e-commerce

El escenario de rede de comercio electrónico [4] posee múltiples aspectos, y capas de protección, servicio de renuncia, *performance*, confiabilidad. Con el propósito de esto es producir un ambiente seguro para las transacciones electrónicas

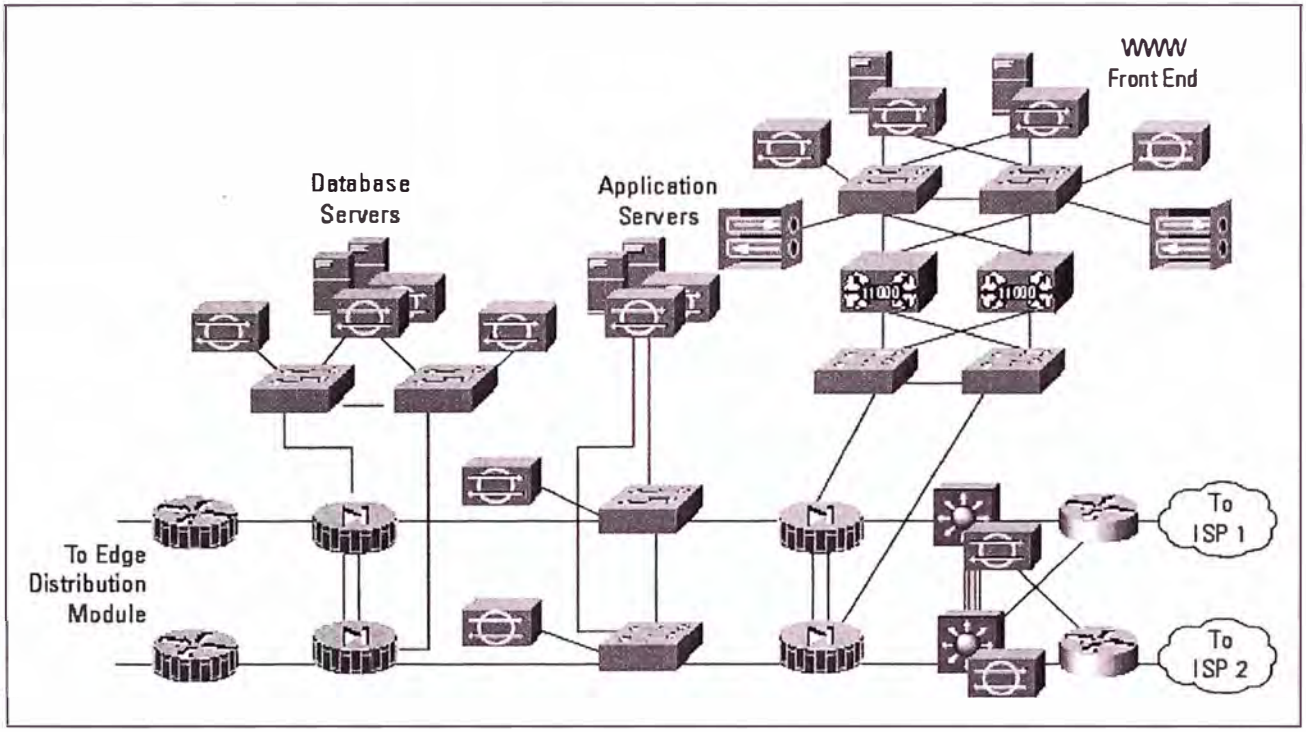

FIG. 4.4 ELEMENTOS DE PROTECCIÓN EN REDES DE E-COMMERCE

La redundancia completa, provee un mínimo de tiempo de caída e interrupción del servicio.
El diseño de 3 frentes (three tier) para el *data center* permite a la organización separar y asegurar los servicios críticos. El primer frente o tier, es llamado el Web tier y es el alojamiento de los servidores Web y terminaciones SSL. El segundo frente es llamado el frente de aplicación o *aplication tier*, y alojan a los servidores de Aplicaciones en *back-end*. El tercer frente es llamado frente de fondo, o simplemente *back-end*, es el frente de base de datos, y es donde se alojan los servidores de base de datos, los cuales ofrecen son almacenamientos de misión critica.
La figura 4.5 muestra la distribución de estos:

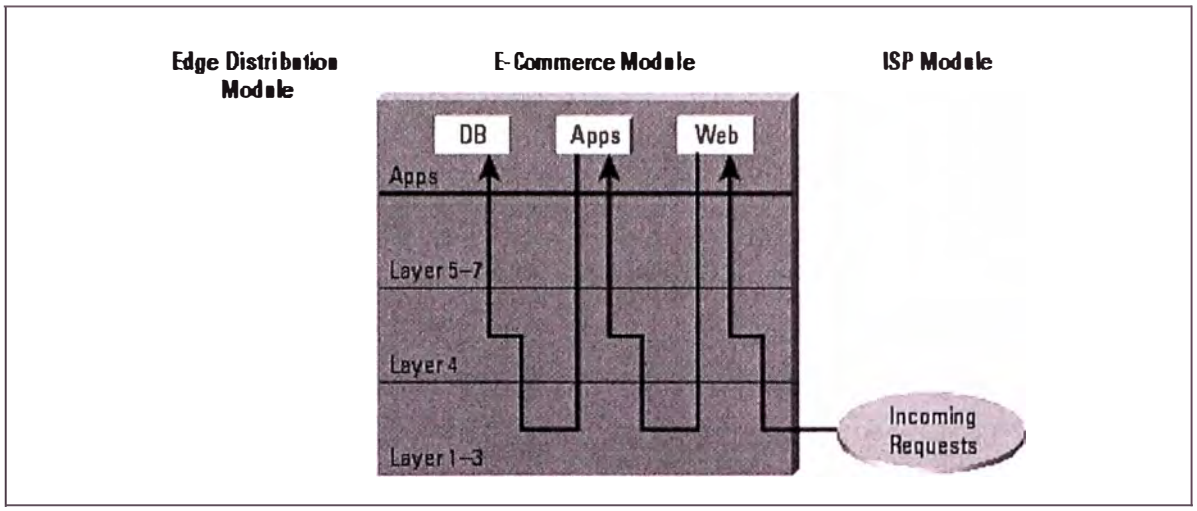

FIG. 4.5 CAPAS DE ACCESO PARA REDES DE E-COMMERCE

Escenario de mitigación:

- Accesos no autorizados, control de estado en *firewall*, y listas de protección ACL.
- Ataques en capas de aplicación, son mitigados a través de los IDS.
- Ataques DoS, son mitigados en el ISP, en los *routers* de borde y en el *firewall*.
- Reconocimiento de puertos, estos son mitigados limitando solo los necesarios, el protocolo ICMP es restringido.
- Código malicioso: son mitigados en los sistemas de prevención.
- Ataques de URL, estos pueden ser mitigados en los sistemas de balanceo de carga o en los proxy de la organización.

Estos aspectos de mitigación son mostrados en la figura 4.6:

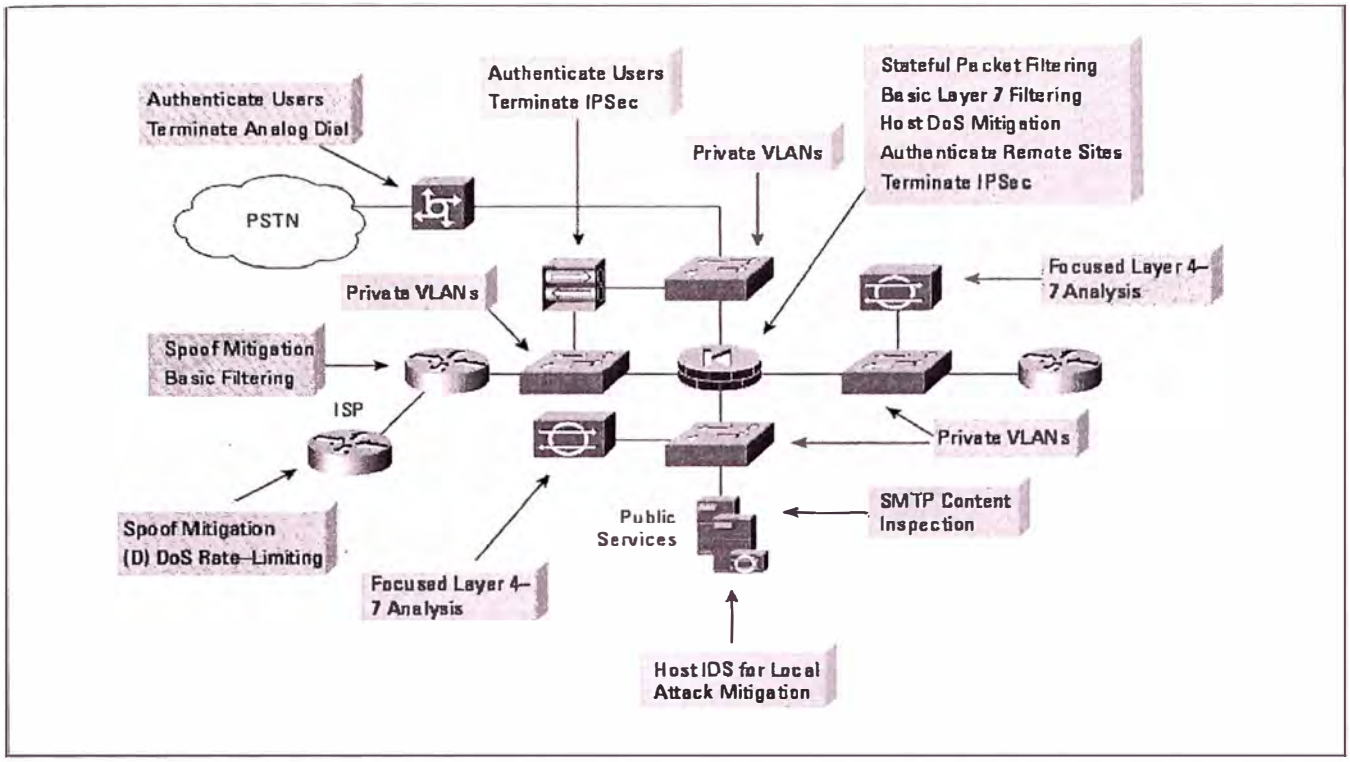

FIG. 4.6 ROLES DE MITIGACIÓN CONTRA ATAQUES

4.4 Seguridad interna

Durante los diseños para seguridad de redes erróneamente se le poca importancia a la protección interna de la red, solo concentrándose principalmente ataques y protección de intrusiones externas, de acuerdo a las estadísticas recientes la mayoría de ataques perpetrados son en su mayoría desde la misma red corporativa, de ahí la necesidad de implementar controles de seguridad interna que protejan los activos de la organización desde todos los frentes, su papel es mostrado en la figura 4.7.

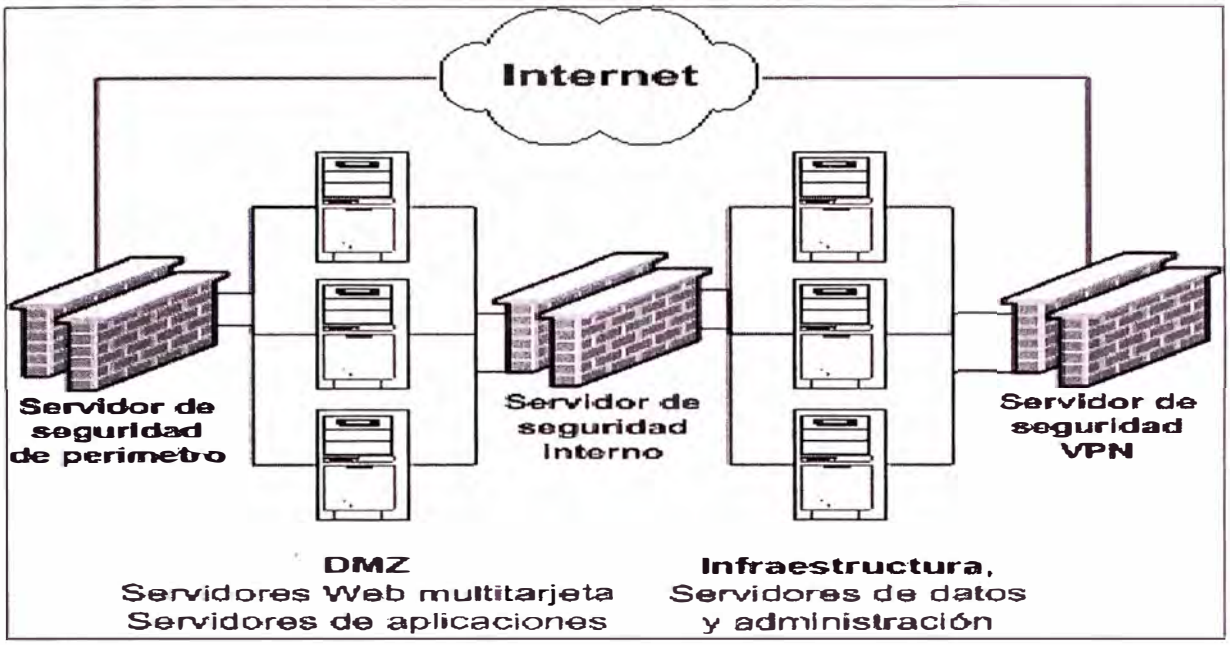

FIG. 4.7 COMPONENTES DE PROTECCIÓN INTERNA

Se requiere la habilitación de puertos TCP y UDP específicos para la comunicación entre los servidores de la DMZ y la red interna.

Si se esta utilizando controladores de dominio estos deben estar ubicados en la red interna.

TABLA Nº 4.1 SERVICIOS Y PUERTOS DE USO EN SEGURIDAD INTERNA

Definición del protocolo	Puerto	Protocolo	Notas
Administración (agente de administración de aplicaciones)	9979 9998 9999 +RPC	TCP	Necesario si los servidores del Web de aplicaciones para el usuario tienen instalado el agente de AppManager y reenvían la información a un servidor de administración interno.
Administración (agente de	1270	TCP	Necesario si los servidores del Web de aplicaciones para

Definición del protocolo	Puerto	Protocolo	Notas
administración de operaciones)			el usuario tienen instalado el agente de administración de operaciones y reenvían la información a los servidores de administración internos.
Administración (Application Center)	4243 4244	TCP	Necesario si se utiliza un servidor Application Center para administrar el contenido de cada matriz Web.
Administración (Servicios de Terminal Server)	3389	TCP	Permite a los administradores de la VPN de administración tener acceso a los Servicios de Terminal Server de todos los servidores de la Web de aplicaciones para el usuario.
Aplicación (SQL Server)	1433	TCP	Todos los servidores IIS tienen entradas DNS que apuntan a los clústeres virtuales de SQL Server en la red VLAN 12.
Aplicación (Message Queuing)	1801	TCP	Todos los equipos IIS tienen instalado Message Queuing y reenvían la información al servidor de clústeres interno Message Queueing, en la VLAN 13.
Infraestructura (Dominio: Kerberos)	88	UDP	Servidores DMZ miembros del dominio interno.
Infraestructura (Dominio: NTP)	123	UDP	Servidores DMZ miembros del dominio interno.

Definición del protocolo	Puerto	Protocolo	Notas
Infraestructura (Dominio: asignador de extremos de RPC)	135	TCP	Servidores DMZ miembros del dominio interno.
Infraestructura (Dominio: LDAP)	389	TCP UDP	Servidores DMZ miembros del dominio interno.
Infraestructura (Dominio: host directo SMB)	445	TCP	Servidores DMZ miembros del dominio interno.
Infraestructura (Dominio: NTDS)	1026	TCP	Servidores DMZ miembros del dominio interno.

Para el caso de servicios DCOM/RPC se deberán habilitar rangos de puertos específicos, tanto en el servidor de seguridad interno como en los servidores a comunicar.
Se deben también crear sub. Redes para que el acceso entre ellas sea controlado.
Se deben definir los puertos TCP y UDP necesarios para la autenticación, como kerberos, LDAP, aquí se especifica el numero de puerto, el protocolo IP utilizado (TCP, o UDP) así mismo la dirección de tráfico en caso de TCP, de acuerdo a las opciones de la Tabla 4.2.

TABLA Nº 4.2 CARACTERÍSTICA DE LOS PAQUETES A PERMITIR

	solo enviar	solo enviar	enviar y recibir
TCP	X	X	X
UDP			X

Luego de esto se pueden utilizar el filtrado de paquetes las reglas de protocolo y las reglas de publicación de los servidores.
El servidor de protección interno atiende las solicitudes en su interfaz externa en nombre de un servidor interno, creando una sesión entre si mismo y el servidor de destino interno.

Para el tráfico de controladores de dominio de la familia Microsoft, se deben deshabilitar el servicio de *Netbios* en el servidor de protección interno.

Para el diseño de esquema distribuido de servidores DNS se deben considerar los siguientes aspectos:

- Se deben configurar las transferencias de zonas solo desde interfaces internas
- No se deben permitir la transferencia de zonas entre servidores de DNS externos e internos.
- Tampoco debe permitirse las consultas desde la Internet hace el servidor de DNS interno. .
- Se puede considerar transferir las zonas DNS externa al servidor DNS del ISP para lograr una mayor redundancia.
- El caso de servidores DNS interno estos por razones de simplicidad se pueden ubicar dentro de los servidores con directorio activo, y utilizar su sistema de replicación para las actualizaciones necesarias.
- Así mismos para cuando se necesiten resoluciones de nombres desde Internet, los servidores de DNS interno son configuradotas para que reenvíen las peticiones hacia los DNS externos.

La separación de las funciones de los servicios de DNS se realiza sobre 2 componentes:

- DNS anunciante: controlan las consultas desde la Internet para las zonas que cuenta con autoridad.
- DNS de resolución: estos controlan las consultas reenviadas desde los DNS internos y las resuelven en su lugar.

Este tipo de configuración provee protección contra ataques de contaminación de *cache*.

Cuando se activa el sistema de seguridad, una consulta al DNS, es enviada a un servidor DNS de Internet referida a una zona que no se tiene autoridad, este mecanismos evita que la opción de recursidad del DNS envíe consultas a un servidor DNS con autoridad, que podría en un respuesta contener una tipo de ataque de contaminación de *cache*. Su distribución es mostrada en la Fig. 4.3

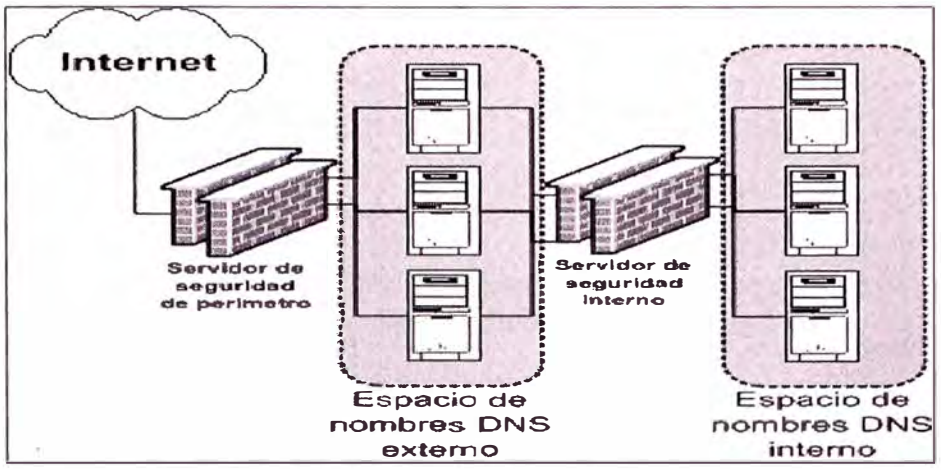

FIG. 4.8 SISTEMA DE DOBLE DNS

4.5 Resumen del capítulo

En este capitulo se ha tratado sobre los diversos tipos de estructura de redes presentes, clasificados por su tamaño, básicas, medianas redes de *e-commerce,* así como las características de protección interna. Se ha mencionado los mecanismos de protección que deben estar presentes, los lugares a proteger, y los tipos de factores que son susceptibles a ser atacados.

CAPITULO V

SEGURIDAD EN SWITCHES Y ROUTERS

Unos de los aspectos también importantes en un sistemas de protección es la protección a nuestros equipos de conexión, como son *switches* y *routers*.

Estos dispositivos de interconexión están siendo cada vez mas atacados por diversas vulnerabilidades, y su análisis de protección es necesario para asegurar la operatividad de la red.

Se tomara de ejemplo de configuración a los *routers y swtches* [10] del fabricante Cisco Systems, dado que posee mayor presencia en las redes de comunicaciones, sin embargo los conceptos son aplicables a cualquier otro proveedor de equipos de comunicaciones.

5.1 Protección en *routers*

Existe un conjunto de razones por las cuales es necesario proteger los *routers*, dado que dichos dispositivos son elementos de interconexión entre redes y su vulneración o sabotaje pondría en riesgo las operaciones de una organización, una alteración en la tabla de ruteo comprometida puede reflejarse en una pérdida de *performance*, o un ataque de *denial of services* podría dejar sin servicio vitales; en el caso de listas de acceso comprometidas, puede resultar en exponer los detalles de la configuración de red, y facilitar ataques contra otros componentes de la misma.

5.1.1 Seguridad en el router, principios y objetivos

Conceptualmente un *router* opera en tres distintos dominios o planos:

Plano de administración, es donde realizar la administración, configuración y el estado del *router.*

Plano de control: en este plano se realiza el monitoreo, actualización de tablas de ruteo, y en general la operación dinámica del *router.*

Plano de reenvió o data: este plano maneja la transición de paquetes entre la red y los servicios que sirve.

Estos planos y sus componentes se encuentran graficados en la figura 5.1.

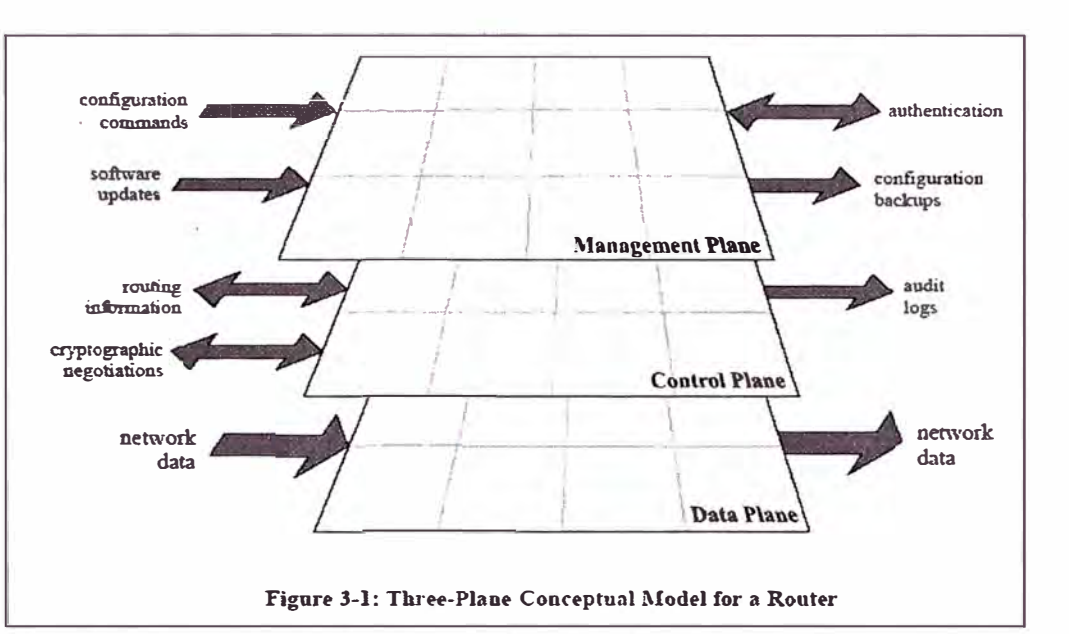

FIG. 5.1 MODELO CONCEPTUAL DE PLANOS DE OPERACIÓN DE UN ROUTER

5.1.2 Componentes de protección

a.- Protección Física

Se debe tener en consideración lo siguiente:

- Habitación libre de interferencia electrostática o magnética.
- Se debería tener control de temperatura y humedad.
- De ser necesario se debe poseer un sistema de energía ininterrumpido (UPS)
- Sistema de control de acceso perimetral, para personal autorizado.

b.- Protección en el sistema operativo

Dado que es un componente crucial deberían tenerse las siguientes consideraciones:

- Utilizar la última versión estable

c.- Configuración Hardening

Un *router* como las computadoras, tiene múltiples servicios habilitados por defecto, muchos de estos no son necesarios, y podrían ser usados y/o explotados por posibles atacantes.

5.1.3.- Protección de redes con routers

Antes de describir los métodos de protección se debe realizar una breve clasificación:

Tipos de Routers

- *Routers* interiores: son aquellos que redirigen el tráfico entre dos o más redes locales dentro de una misma organización. Estas pueden compartir las mismas políticas de seguridad y regularmente poseen un alto nivel de confianza.
- *Routers* de *backbone:* estos dispositivos reenvían el tráfico entre distintas organizaciones que son también conocidos como 'sistemas autónomos'. Entre dichos sistemas el nivel existe un bajo nivel de confianza.
- *Routers* de borde: son aquellos que reenvían el tráfico entre una organización y una red externa o también entre una red de confianza contra una de no confianza, dado su posición, las organizaciones pueden emplearlo como un medio de protección de red para forzar una política de seguridad granulada.

Entre mecanismos de protección de redes en los *routers* podemos mencionar:

a .- Filtro de Paquetes

Los filtros de paquetes dentro del pila de protocolos TCP/IP brindan un mecanismos de control de tráfico basado en direcciones y protocolos, para realizar dichos filtros se deben tener algunas consideraciones, como la dirección del trafico, la longitud del filtro, y sobre todo el orden, este ultimo factor es el mas crítico, pues el sistema de filtrado compara el tráfico con cada una de la reglas aplicadas, hasta que encuentre una coincidencia, y dejará de buscar las siguientes reglas, solo en caso de que no encuentre ninguna aplica la regla por defecto.

Bajo este escenario se pueden aplicar 2 tipos de políticas:

- **Aplicar filtrado de paquetes permitiendo solo protocolos y servicios requeridos**
  Los servicios que no son explícitamente permitidos son prohibidos; se aplica

regularmente a los *routers* de borde.

- **Aplicar filtro de paquetes rechazando protocolos y servicio con riesgo**
  En algunos casos donde no se puedan aplicar las políticas estrictas de seguridad, se deben prohibir servicios que son comúnmente no necesarios o que poseen historial de compromiso de seguridad, la Tabla 5.1 muestra la relación de de servicios a deshabilitar para el caso de conexiones externas.

TABLA Nº 5.1 RELACIÓN DE SERVICIOS VULNERABLES

Puerto	Protocolo	Servicio
79	TCP	Finger
161	TCP & UDP	Snmp
162	TCP & UDP	snmp trap
513	TCP	rlogin
513	UDP	Who
514	TCP	rsh,rcp,rdist,rdump
550	TCP & UDP	New who

b.- Filtro de direcciones

Los principios que deben aplicarse para el filtrado de direcciones son los siguientes:

- Rechazar todo el tráfico desde las redes internas con dirección de origen que no pertenezcan las direcciones de redes internas de la organización.
- Rechazar todo el tráfico desde las redes externas que contengan direcciones de origen utilizadas por las redes internas de la organización, el tráfico de esta naturaleza es considerado tráfico *spoofed* es usualmente una forma de ataque de red y debe ser siempre filtrado en los *routers* de borde.
- Rechazar todo el tráfico (tanto dirección origen como destino) que contengan direcciones reservadas, no ruteables o direcciones de rangos ilegales.

c.- Mitigación de ataques de denegación de servicio

Las formas de ataques recurrentes en la actualidad también incluyen saturación de los enlaces y servicios que se brindan, conocidos también como *denial of service,* no hay soluciones completas frente a este problema, debido a que los recursos de red son limitados

y los servicios requieren están disponibles, sin embargo se pueden tomar medidas que disminuyan los efectos de estas formas de ataques, estas requieren de coordinación entre los administradores de red de la organización y los proveedores de servicios debiéndose planificar y tomar las medidas antes de que estos ocurran.

Se pueden tomar las siguientes estrategias para mitigar estas formas de ataque:

- Filtro para direcciones IP incorrectas.
- Utilizar *black hole routing.,*
- Configurar el mecanismo llamado *Unicast Reverse-Path Forwarding Verificación* , que utilizar una tabla de ruteo para detectar y descartar paquetes con direcciones incorrectas.
- Registrar las ocurrencias, sobre todo de tráfico considerado incorrecto.
- Habilitar las opciones de mitigación contra ataques *TCP SYN flood.*
- Habilitar la opción de *TCP intercept.*

En el caso de routers de borde, no pueden controlarse todo el tipo de tráfico dado la cantidad del mismo que se envía o recibe, de ahí que se deben usar métodos estadísticos para discriminar un posible ataque, como exceso de conexiones a un determinado puerto, flujo no usual de trafico ICMP, o protocolos no comunes.

f.- Mecanismos de administración en *routers*

Controlar el sistema de acceso a la administración de un *router* es una de los mecanismos necesarios para asegurar su protección, estos accesos en sus dos formas:

- Acceso local: aquí se involucran las conexiones directas al puerto de consola utilizando el algún software de terminal de acceso.
- Acceso remoto: son las conexiones no locales, usando protocolos como *telnet*, *ssh*, *http, https, snmp , tftp* entre otros.

Es recomendable que solo algunas direcciones locales puedan acceder a los *routers*, debido a que credenciales son enviadas en texto plano, también bajo este esquema se pueden implementar mecanismos de conexión cifrada, como *ipsec, ssh o https*.

Otra de las opciones aplicables es el uso de una red administrativa paralela, que permita aislar las conexiones que se realicen a los equipos de comunicaciones, los mismos que tendrán una red independiente de administración.

Se deben habilitar como mínimo dos niveles de acceso, operador y administrador, ambos con funciones especificas de monitoreo o cambio de configuración respectivamente.

g.- Actualización del router

Periódicamente también se requiere la actualización del sistema operativo, por las siguientes razones:

- Los parches reparan problemas potenciales de seguridad.
- Mejora la *performance* y habilita nuevas características.

Durante el proceso de actualización, es recomendable que se realice el siguiente procedimiento:

- Apagar y desconectar las interfaces del *router*.
- Realizar copia de seguridad del actual sistema operativo y de la actual configuración.
- Cargar el actualizador y el archivo de configuración.
- Realizar las pruebas de *performance* y nuevas características para validar que la actualización ha sido correcta.
- Si es que las pruebas fallan, realizar la restauración de la anterior configuración.

5.1.4 Implementación de políticas de seguridad

En *routers* el proceso de aseguramiento del sistema (también llamado *hardening*) se debe realizar prioritariamente en los lugares que hayan sido ubicados como blancos de posibles ataques, por ejemplo en *routers* de acceso a Internet y *routers* cabecera de tráfico.

Las siguientes son las recomendaciones para una mejor protección para dichos equipos.

- Remover configuración y servicios de red innecesarios como:
  Cree una interfaz virtual interna (*Lookback interface*) para que sea designado como origen del tráfico que se genera:
  Router# config t
  Enter configuration commands, one per line. End with CNTL/Z.
  Router(config)# interface loopback0
  Router (config-if)# description Main loopback interface
  Router(config-if)# ip address 14.2.11.250 255.255.255.255

- Forzar la desconexión en las consolas por tiempo de exceso (*timeout*), de esta manera se garantiza que no quedan abiertas sesiones para usuarios no autorizados.
  El siguiente ejemplo muestra la desactivación del acceso a consola luego de 5 minutos de inactividad:
  Router(config)# line con 0
  Router(config-line)# transport input none
  Router(config-line)# exec-timeout 5 0

a.- Privilegios :

El sistema operativo que provee Cisco (IOS) tiene 16 niveles de privilegios. El modo usuario EXEC, se ejecuta con el nivel 1, y el modo privilegiado *enabled* se ejecuta con el nivel 15. Cada uno de los comandos del sistema operativo tiene preasignado uno de los niveles.
Un ejemplo de configuración de cambio al nivel más alto de algunos comandos se muestra a continuación:

Router(config)# privilege exec level 15 connect
Router(config)# privilege exec level 15 telnet
Router(config)# privilege exec level 15 rlogin
Router(config)# privilege exec level 15 show ip access-lists

b.- Deshabilite los servicios innecesarios:

1. TCP y UDP *small servers*
2. *Finger server*: Son los servicios heredados que realizan consultas sobres *host* de los usuarios conectados.
3. HTTP *server* : es la servicio web para administración del dispositivo.
4. Bootp server : es el protocolo que es usado para cargar sistemas operativos desde sobre la red.
5. PAD *service* : es un ensamblador/desensamblador de paquetes para servicios que soporten enlaces X.25.
6. IP *source routing*: es una característica por el cual paquetes individuales pueden ser ruteados. Es también usada par varias formas de ataques.
7. Proxy ARP : El es servicio que permite realizar transacciones de protocolo ARP, entre

2 segmentos de red .

8. IP *directeted broadcast*: Permite a un *host* de un segmento de red iniciar un *broadcast* físico en diferentes segmentos de red. Esta técnica fue aprovechada por las iniciales formas de ataques de denegación de servicio.
9. IP *unreachables* , *redirects* , *mask replies* : estas condiciones de mensaje dentro del protocolo ICMP pueden ser utilizadas por atacantes para conocer el estado de la red

10. MOP: (*maintenance operations protocol*) fue usado para servicios para servicios para los protocolos de red *DECnet.*
11. NTP *service*: este protocolo es utilizado para mantener la sincronía en los en los relojes de los equipos de comunicación. Se debe configurar los routers dentro de un sistema de jerarquía NTP, si este servicio no esta disponible se puede deshabilitar el servicio NTP.
12. SNMP *services*: es un protocolo estándar para automatizar monitoreo y administración remota. Todos los *routers* deberían pertenecer a una infraestructura de gestión SNMP configurado adecuadamente con los mecanismos de seguridad que posee. Si es que no existe dicha infraestructura, se puede deshabilitar dicho servicio.
13. *Router name and* DNS *resolution* : Por defecto Cisco envía consultas de nombres a la dirección de *broadcast* : 255.255.255.255. Se puede deshabilitar este envió para una mejor *performance*.

    Los comandos a emplear son
    Router(config)# no service tcp-small-servers
    Router(config)# no service udp-small-servers
    Router(config)# no ip bootp server
    Router(config)# no service finger
    Router(config)# no ip http server
    Router(config)# no ip identd
    Router(config)# no snmp-server community name_community
    Router(config)# no snmp-server community private

14. Si es necesario utilizar el protocolo SNMP, habilite solo con la opción *read only* RO y utilice nombres del parámetro comunidad no comunes, como se muestra a continuación:

Router(config)# snmp-server community S3cr3t-str1n9 ro 10

15. Deshabilitar los servicios de *Cisco Discovery Protocol,* (CDP), configuración remota, *source routing*, y *zero subset* :

Router(config)# no cdp run
Router(config)# no service config
Router(config)# no ip source-route
Router(config)# no ip subnet-zero
Router(config)# no ip mroute-cache
Router(config)# no ip proxy-arp

16. Deshabilite las interfaces no usadas:

Router(config-if)# shutdown

17. Habilite la protección de ataques *smurf*, *ad-hoc* , y consultas de *access-list*:

Router(config-if)# no ip directed-broadcast
Router(config-if)# no ip proxy-arp
Router(config-if)# no ip unreachables

18. Configure la línea de consola, los terminales virtuales, tiempo de expiración y desactivar la línea auxiliar de no ser necesaria:

Router(config)# line con 0
Router(config-line)# exec-timeout 5 0
Router(config-line)# login
Router(config-line)# transport input telnet
Router(config)# line aux 0
Router(config-line)# no exec
Router(config-line)# exec-timeout 0 5
Router(config-line)# no login
Router(config-line)# transport input none
Router(config)# line vty 0 4

Router(config-line)# exec-timeout 5 0
Router(config-line)# login
Router(config-line)# transport input telnet

19. Configure el *enable password* con protección en base al algoritmo MD5 y configure distintas contraseñas en la línea de consola, auxiliar y terminales virtuales:

Router(config)# enable secret 0 45betk3_h
Router(config)# line con 0
Router(config-line)# password dmery89
Router(config)# line aux 0
Router(config-line)# password crep_45_7
Router(config)# line vty 0 4
Router(config-line)# password calip_x_5
Provide a basic protection for the line passwords by using the following global configuration command.
Router(config)# service password-encryption

c.- Listas de control de accesos

Este es un mecanismo de protección y filtro de paquetes que permite autorizar tráfico y proteger las redes que se interconectan.

Para los tráficos IP, hay 2 tipos de listas: estándar y extendida. Las primeras solo permiten filtrar por dirección IP de origen. Las extendidas pueden permitir o denegar tráfico basadas en sus protocolos, direcciones destino y origen, puertos de origen y destino TCP/UDP o protocolos ICMP, IGMP, entre otros. Ambas formar de lista pueden aplicarse a las interfaces *vty lines*, IPSec, protocolo de ruteo.

A continuación se muestra un ejemplo de aplicación de una lista extendida para el control de *anti spoffing*.

Se deben configurar las listas de acceso para protección *anti-spoffing* y habilitando la estricción del uso de las direcciones privadas:

Router(config)# access-list 100 deny ip 14.211.150.0 0.0.0.255 any log
Router(config)# access-list 100 deny ip 127.0.0.0 0.255.255.255 any log
Router(config)# access-list 100 deny ip 10.0.0.0 0.255.255.255 any log

```
Router(config)# access-list 100 deny ip 172.16.0.0 0.15.255.255 any log
Router(config)# access-list 100 deny ip 192.168.0.0 0.0.255.255 any log
Router(config)# access-list 100 deny ip 224.0.0.0 15.255.255.255 any log
Router(config)# access-list 100 permit ip any 14.211.150.0 0.0.0.255
Router(config)# interface Ethernet1/2
```

d.- Control de Atagues

1.- Ataques SYN : Los ataques SYN involucran un volumen de conexiones que nopueden completarse al destino. El ataque causa un tráfico de encolamiento que puede denegar el servicio de usuarios TCP legítimos.

```
Router(config)# access-list 106 permit tcp any 14.2.6.0 0.0.0.255established
Router(config)# access-list 106 deny ip any any log
Router(config)# interface eth 0/0
Router(config-if)# description External interface
Router(config-if)# ip access-group 106 in
```

2.- *Limit External Access* con TCP *Intercept* : Las listas de acceso mostradas bloquearan los paquetes desde *hosts unreachable*, usando la característica de TCP *intercept*. Esta característica bloquea el inicio de conexiones desde redes externas hacia redes internas. El mecanismo de TCP *intercept*, es un mecanismos efectivo de protección de *hosts*, para ataques TCP SYN, sin embargo deber supervisarse los parámetros de rendimiento, ya que este mecanismo requiere una operación extra de recursos del *router.*

```
Router(config)# ip tcp intercept list 107
Router(config)# access-list 107 permit tcp any 14.2.6.0 0.0.0.255
Router(config)# access-list 107 deny ip any any log
Router(config)# interface eth0
Router(config-if)# description External ethernet interface to 14.1.0.0 net
Router(config-if)# ip access-group 107 in
Router(config-if)# exit
```

3.- Ataques tipo lan : estos ataques tienen por característica el envió de paquetes hacia el *router* con la misma dirección IP de origen y destino, y con el mismo número de puerto de origen y destino.

Estas formar de ataques podría causar una forma de denegación de servicio o degradar las

prestaciones que el *router* ofrece.

```
Router(config)# access-list 103 deny ip host 14.1.1.20 host 14.1.1.20 log
Router(config)# access-list 103 permit ip any any
Router(config)# interface eth0
Router(config-if)# description External interface to 14.1.0.0/16
Router(config-if)# ip address 14.1.1.20 255.255.0.0
Router(config-if)# ip access-group 103 in
Router(config-if)# exit
```

4.- Ataques *Smurf* : este tipo de ataques tipo por comportamiento el envió masivo de paquetes del tipo ICMP a direcciones *broadcast* con la dirección origen *spoofed* de una subred.

El siguiente ejemplo muestra la forma de bloqueo:

```
Router(config)# access-list 110 deny ip any host 14.2.6.255 log
Router(config)# access-list 110 deny ip any host 14.2.6.0 log
Router(config)# interface interface eth0
Router(config-if)# ip access-group 110 in
Router(config-if)# exit
```

5.- Tipos de Mensajes ICMP y Traceroute: de las múltiples variedad de mensajes ICMP, se deben bloquear la entrada de algunas como: *echo* y *redirect.* Con los primeros un atacante podría crear mapas de la redes detrás de un *router* y activar un ataque de denegación con paquetes *echo* contra estas redes internas. Con paquetes *redirect,* una atacante podría provocar el cambio en la tabla de ruteo de un *router.*

Se muestra a continuación la forma de filtrado:

```
Router(config)# access-list 100 deny icmp any any echo log
Router(config)# access-list 100 deny icmp any any redirect log
Router(config)# access-list 100 deny icmp any any mask-request log
Router(config)# access-list 100 permit icmp any 14.2.6.0 0.0.0.255
```

En el caso de tráfico saliente se podrían permitir los tipos de paquetes ICMP: *echo,*

parameter problem, packet, too big y *source quench* permaneciendo el resto de tipos bloqueados. Los paquetes *echo* son usados para realizar *pings* hacia el exterior. El Paquete *parameter problem* y *source quench* mejoran las conexiones con la información de los problemas de red. Los paquetes *too big* es necesario para el la ruta de descubrimiento de MTU.

Se pueden utilizar el siguiente ejemplo para su aplicación:
Router(config)# access-list 102 permit icmp any any echo
Router(config)# access-list 102 permit icmp any any parameter-problem
Router(config)# access-list 102 permit icmp any any packet-too-big
Router(config)# access-list 102 permit icmp any any source-quench
Router(config)# access-list 102 deny icmp any any log

Para el caso del *traceroute* este muestra las direcciones IPs de los *routers* así como la cantidad de saltos que se realizan debe el origen hasta el destino. En algunos sistemas operativos, el *traceoroute* utilizar paquetes UDP que causan que por la cantidad de rutas se generen mensajes ICMP de *time exceded* y *unreachable.* En base a esta información un atacante podría crear un mapa de subredes y *host* detrás de un *router.*
Un ejemplo de como filtrar una de las formas de traceroute que usualmente usa los puertos 33400 hasta el 34400 dentro del protocolo UDP es:
Router (config)# access-list 100 deny udp any any range 33400 34400 log

6.- Ataques distribuidos de denegación de servicios: existen muchas formas de ataques que se encuentran en Internet, los *router* no pueden prevenir todas las formas de ataques, sin embargo se pueden aplicar medidas de atenuación contra las formas mas conocidas de ataques añadiendo listas de acceso para bloquear puertos específicos. Este tipo de configuración puede tener algún impacto en los usuarios, dado que el bloqueo de puertos puede coincidir con el puerto que aleatoriamente se asigna a una comunicación. Se pueden aplicar estas reglas cuando un ataque ha sido detectado.

! the TRINOO DDoS systems
access-list 170 deny tcp any any eq 27665 log
access-list 170 deny udp any any eq 31335 log
access-list 170 deny udp any any eq 27444 log

```
! the Stacheldraht DDoS system
access-list 170 deny tcp any any eq 16660 log
access-list 170 deny tcp any any eq 65000 log
! the TrinityV3 system access-list 170 deny tcp any any eq 33270 log
access-list 170 deny tcp any any eq 39168 log
! the Subseven DDoS system and some variants
access-list 170 deny tcp any any range 6711 6712 log
access-list 170 deny tcp any any eq 6776 log
access-list 170 deny tcp any any eq 6669 log
access-list 170 deny tcp any any eq 2222 log
access-list 170 deny tcp any any eq 7000 log
```

7.- Configure el acceso vía ssh (Secure Shell) : esta habilitación permite implementar el servicio ssh , para la gestión del dispositivo, dado que este protocolo provee comunicación segura , su uso es necesario en redes con confiables. Los comandos para habilitar dicho servicio son:

```
Router(config)#username user1 password 0 sad
Router(config)# Crypto key generate rsa
Router(config)# Ip ssh time-out
```

Configurar la configuración del terminal virtual a :

```
line vty 0 4
access-class 1 in
login local
transport input ssh
```

5.2 Protección en *switches*

Los equipos de comunicación de capa dos, controlan considerables volúmenes de tráfico en redes de computadora y cada vez están abundando los ataques a nivel de capa de enlace de datos del nivel OSI, es imprescindible por lo tanto prestar cuidado a la configuración que se realice en este nivel. Los administradores pueden configurar el control de accesos el control de ataques y así proteger la integridad y confidencialidad de la red.

Pero antes partiremos de algunas premisas incorrectas:

- Las direcciones MAC, son únicas
- Los switches protegen contra *sniffers*.
- Las *vlan* proporcionan aislamiento

5.2.1 Tipos de ataques en redes basadas en *switches* y protección.

a.- Ataques MAC: Esto se produce por la inundación de las Tablas CAM (Content Addressable Memory), esta tabla dado su tamaño fijo, es susceptible a ser saturado.
Un tipo programa de saturación de tablas CAM es conocido como *macof.*
La figura 5.2 muestra el modo de operación de la Tabla CAM.

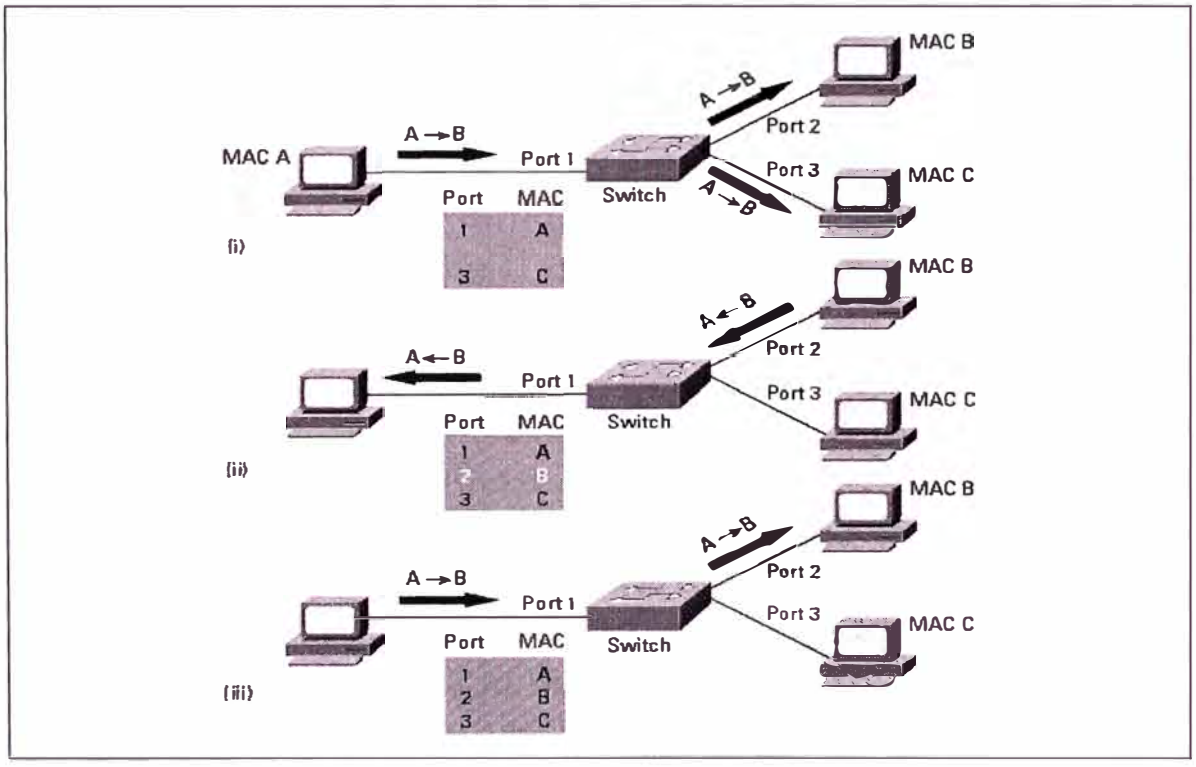

FIG. 5.2 ESQUEMA DE OPERACIÓN DE LA TABLA CAM EN *SWITCHES*

Para la protección de ataques tipo MAC es necesario limitar el número de MAC que se pueden esperar de los puertos, esta opción conocida como *port security* de acuerdo a la acción que se desea realizar, se puede realizar los siguientes eventos:

- Que el *switch* bloquee a la MAC detectada
- Que el *switch* bloquee el puerto.

Un ejemplo de protección evitar ataques tipo MAC sería:
Switch# configure terminal
Switch(config)# interface fastethernet 4/12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 4

b.- Ataques al Protocolo ARP (*Adress Resolution Protocol*): El ARP request se utiliza para averiguar cual maquina tiene cierta dirección IP y se implementa con un broadcast en la red. El modo de ataque es cuando se publica repetidamente una determina dirección MAC, al segmento haciendo suponer que es una dirección que no es, este a su vez envía el tráfico al verdadero propietario, pero él se comportará como un puente, capturando el tráfico de la red.
Para mitigar ataques tipo ARP, se requiere configurar redes virtuales privadas, aislando el tráfico en grupos específicos para crear redes distintas en una misma red local.

c .-Ataques de *Spanning Tree* : El *Spaning Tree* es el protocolo utilizado para mantener una topología libre de ciclos en una red de nivel 2, proporciona a su vez servicios de redundancia.
El ataque se produce cuando se envían mensajes BDPU con el objeto de forzar el recalculo de *spanning tree* y transformarse en *root bridge*, produciéndose así denegación de servicio porque durante el recalculo, el *switch* no hace reenvió de datos.

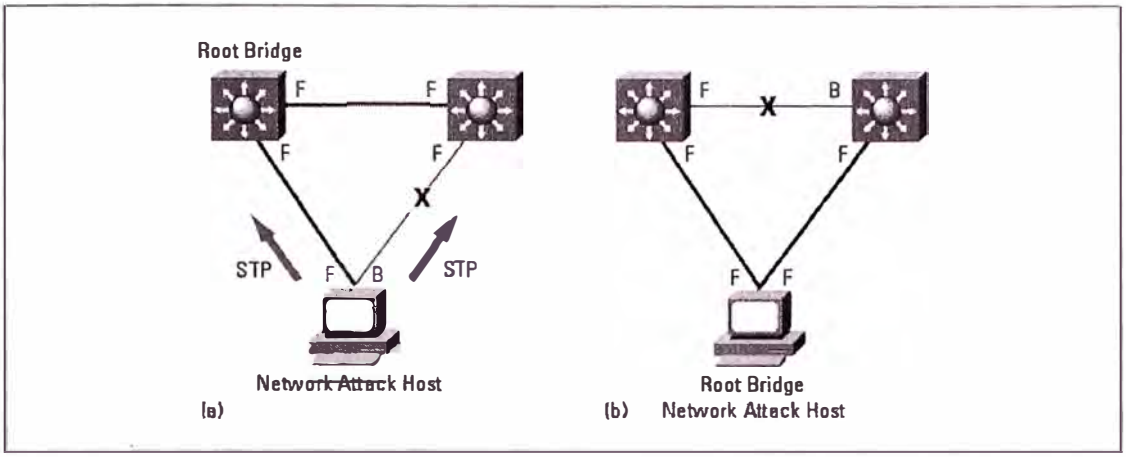

FIG. 5.3 ESQUEMA ATAQUE VÍA SPANNING TREE

Para mitigar ataques vía el protocolo *spanning tree* se debe realizar:
BPDU *Guard*: deshabilitar el puerto de *switch* si se recibe un mensaje BPDU habilitado en todos los puertos de un *switch catalyst*. Se tiene habilita la función de *port fast*
Ejemplo:
CatOS(enable) set spantree port fase bpdu-guard enable
IOS (config)# spanning-tree portfast bpduguard

Root Guard: anula los puertos por los que se recibe anuncios de candidatos a *Root Bridge*:

CatOS (enable) set spantree guard root 1/1
IOS (config)# spanning-tree guard root

La configuración de defecto de un *switch*, posee servicios que no son regularmente usados y estos podrían ser blanco de vulneración es preferible deshabilitarlos.
Dado que corresponden al mismo IOS, los servicios a deshabilitar son los que se mostraron para el caso de *routers* en el punto 5.1.4 , sección b.

d.- Port Security: el *port security* es un mecanismo de seguridad que permite limitar el número de MACs *address* permitidas en un determinado puerto del *switch*. Esta característica puede ser utilizada para servidores y equipos de comunicaciones que estén en puertos físicos en el *switch.*

Existen 3 tipos de accesiones cuando se registra una violación de acceso :

- Eliminar el paquete.
- Eliminar el paquete y enviar un mensaje.
- Inhabilitar el puerto.

Otras características que se pueden habilitar son :
Máximo número de direcciones MACs en un determinado puerto.
Tiempo máximo de inactividad para el dirección MAC configurada en el puerto.

Un ejemplo de implementación de estas características son :

Switch(config-if)#
switchport port-security
Switch(config-if)# switchport port-security violation shutdown
Switch(config-if)# switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address 0000.0200.0088
Switch(config-if)# switchport port-security aging time 10
Switch(config-if)# switchport port-security aging type inactivity

e.- Undireccional Links Detección **(UDLD)** mediante este protocolo, se puede determinar si es que un enlace indirecto existe entre ellos, si es que es detectado el enlace es deshabilitado hasta que manualmente sea habilitado. Este protocolo podría ser utilizado para ataques de denegación de servicio.

Se pueden tomar adicionalmente las siguientes medidas para mitigar algunas formas de ataque :

- Para prevenir los ataques de *fast flooding,* se puede utilizar el comando *scheduler interval* para que aun los procesos de mas baja prioridad obtengan un tiempo de uso del procesador.
- Deshabilitar en las interfaces el control de flujo mediante el comando *flowcontrol receive off.*
- Para prevenir ataques SYN Flood, se puede configurar un parámetro de tiempo de espera para el intento de conexiones TCP usando el comando : *ip tcp synwait-time* .

5.3 Resumen del capítulo

En este capítulo se ha tratado sobre la protección en sistemas de comunicaciones como son *routers* y *switches*, ya que ataques recientes han tenido como blanco estos dispositivos. Por lo tanto es necesario proteger nuestra infraestructura de comunicaciones contra posibles *sniffers* en la red, duplicidad de direcciones MAC, o ataques a protocolos como *spanning tree* entre otros.

Esta configuración si bien han sido aplicados a productos del fabricante de dispositivos Cisco Systems , sin embargo los conceptos son también aplicables a otros fabricantes.

CAPITULO VI

IMPLEMENTACION DE LAS POLITICAS DE SEGURIDAD EN UNA ORGANIZACIÓN GUBERNAMENTAL

6.1 Descripción del escenario

El caso a estudiarse corresponde a una institución gubernamental, que administra importantes recursos público de información, y a su vez brinda servicios a terceras instituciones.

Dicha institución posee una considerable infraestructura tanto de comunicaciones, *data centers*, software y recursos que se mencionan a continuación:

- 30 líneas dedicadas para la comunicación con sus diversas oficinas ubicadas a los largo de todo el territorio nacional.
- 2 *data centers*, para el procesamiento de la información y contingencia de las operaciones.
- Servicios de acceso a información a instituciones financieras, de telecomunicaciones y gubernamentales.
- 79 accesos vía conexiones conmutadas para oficinas en lugares remotos.
- Servicios de acceso a información vía aplicaciones Web.
- 35 servidores de diversa arquitectura (RS 6000, Alpha Systems, Intel) de rango alto y medio.
- Servicio de Internet
- Servicios de correo electrónico
- 1535 estaciones de trabajo.
- Servicio de telefonía IP.

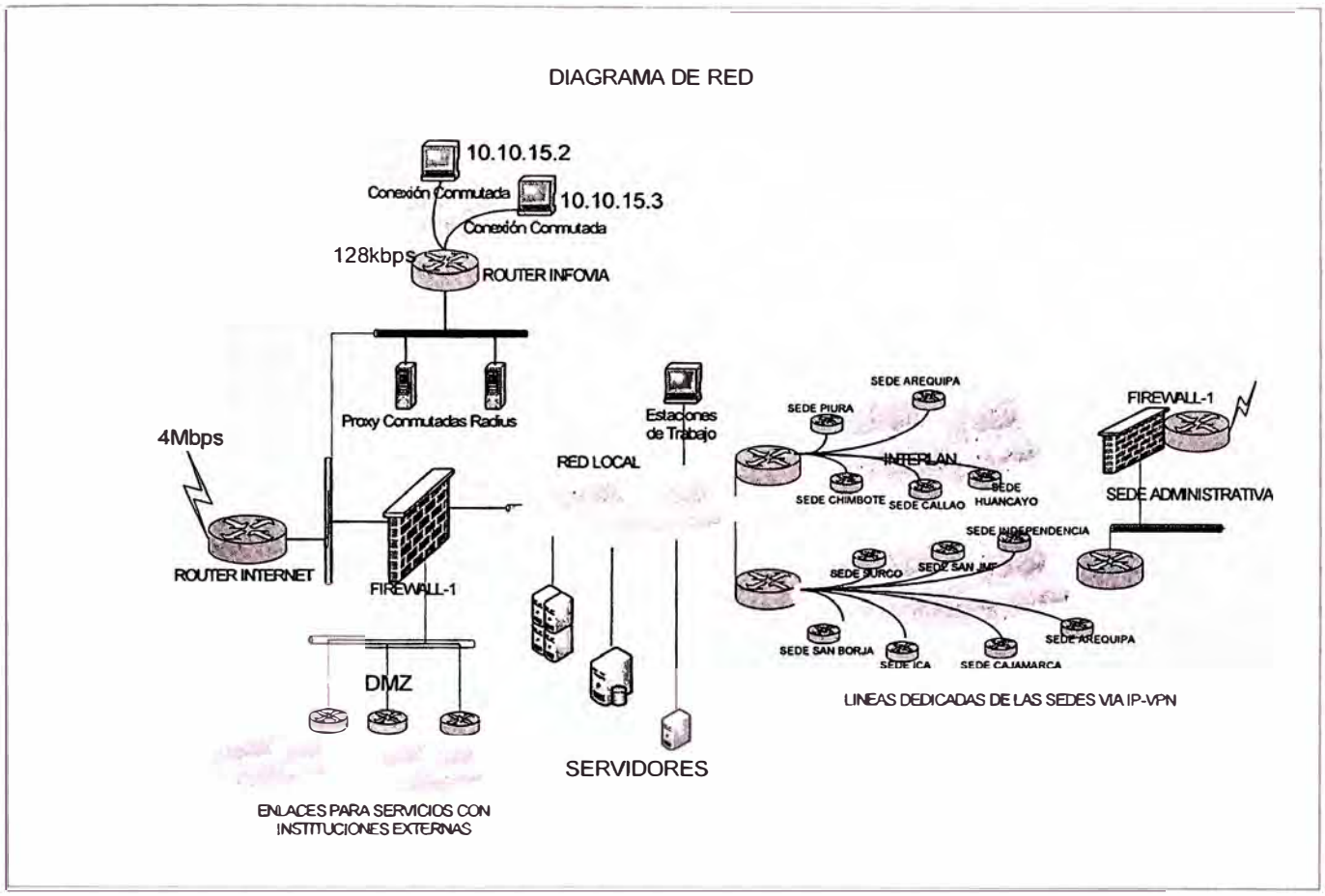

FIG. 6.1 DIAGRAMA DE RED DEL CASO DE ESTUDIO

6.2 Identificación de elementos a proteger

Aquí se encuentran clasificados los distintos sistemas de almacenamiento de información, tener en cuenta que este rubro a proteger es el mas importante debido a su dificultad en recuperarlo.

Se posee los siguientes sistemas lógicos de datos a protegerse:

- Sistema Nacional de Información
- SIGA
- PADRONES
- BACKUPS
- Código fuente de programas
- Correos y perfiles

- Configuración de servidores
- Sistemas de tramite documentario

TABLA Nº 6.1 RECURSOS A PROTEGER

Servidores
Superdome
RS6000
GS 160
Consultas Masivas
Servicio de correo y dominio
Servidor Web
Servidor SIGA
Servidor FTP
Firewall
Servidor RADIUS
Storage Works
Storage IBM
Servidor Intranet
CallManger
Routers
Switches

6.3 Valoración de los factores de seguridad

En capítulos anteriores hemos analizado que en toda organizacion existen 3 factores a cuantificar y priorizar, estos son : confidencialidad, integridad, disponibilidad y son analizados a continuación:

- Integridad: dado la naturaleza de la organización, y que tiene como garantía preservar y garantizar la veracidad de los datos, se condicionará este factor como prioritario.

- Disponibilidad: la organización en estudio provee también diversos servicios críticos de verificación de datos, ahora si bien es cierto este mismo servicio es crítico, no lo es mas que la integridad, por lo tanto daremos prioridad 2.

- Confidencialidad: La información presente dentro del estado es protegida (protegida principalmente de alteración no autorizada), pero también es pública, aspectos que no son contradictorios, y le daremos a este factor prioridad 3.

TABLA Nº 6.2 FACTORES DE VALORACIÓN DE RIESGOS

Factor	Prioridad	Peso(100)	Característica
Integridad	1	60	Preservar la Información
Disponibilidad	2	25	Brinda servicios críticos, pero requiere veracidad
Confidencialidad	3	15	Información protegida pero pública

6.3 Implementación de políticas de seguridad

Para los sistemas de protección de red se ha considerado los siguientes elementos:

- Firewall externo: este elemento protegerá contra posibles ataques desde fuera de la organización.
- Firewall interno: este sistema pretejerá contra posibles ataques desde dentro de la organización.
- Sistema de detección de intrusiones.
- Filtro de contenidos para acceso Internet.

Para esta implementación se ha considerado el esquema de 3 frentes, frente de servidores web, frente de aplicaciones y frente de servidores de base de datos.
La figura 6.2 se muestra el diagrama de implementación, de las diversas zonas protegidas.

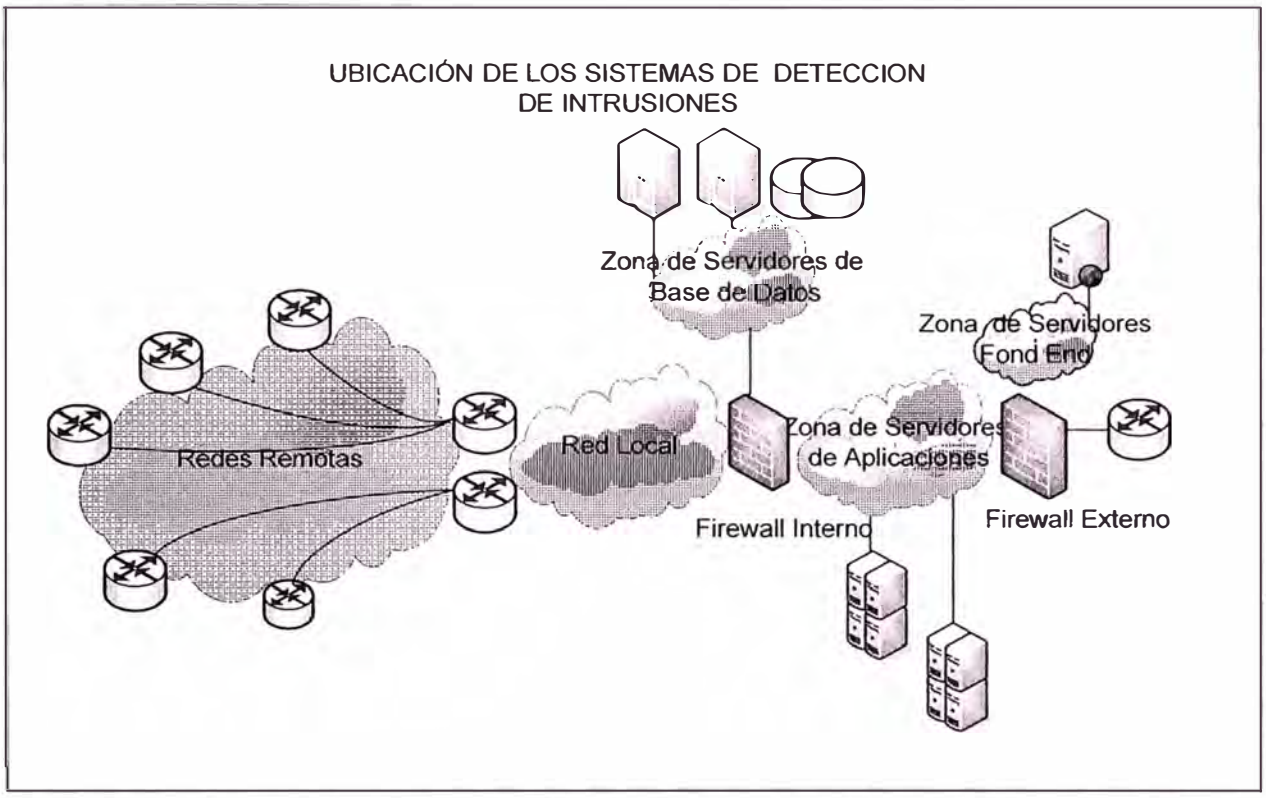

FIG. 6.2 SISTEMA DE PROTECCIÓN PERIMETRAL

Debido a las características de las aplicaciones, en las distintas zonas de aplicación, se puede hacer una comparación de requisitos para los escenarios de protección interna y externa. Estos son resumidos en la tabla 6.3

TABLA Nº 6.3 COMPARACION DE FUNCIONES FIREWALL INTERNO Y EXTERNO

	FIREWALL EXTERNO	FIREWALL INTERNO
APLICACIONES	Protocolos estándares	Aplicaciones internas.
	Client-to-Server	aplicaciones client-client, client-to-server
	Cumplimiento de los protocolos	Poca cumplimiento de los protocolos
	Seguridad centralizada	Seguridad no centralizada

POLITICA	Permitir solo trafico explícitamente	Permitir todo el trafico y bloquear solo
	Autorizado bloqueando el resto.	el que sea explícitamente denegado.
PRIORIDAD	1.- Seguridad	1.- Ininterrupción del tráfico
	2.- Ininterrupción del tráfico	2.- Seguridad
PROTOCOLOS LAN	Generalmente bloqueados	Deben ser permitidos
IMPLEMENTACION	Pocos servicios activos , y pocos	Acceso general, segmentación de red
	usuarios con acceso remoto	

6.4.1 Implementación Firewall Externo

a. - Las funciones de las zonas desmilitarizadas son:

- **Zona pública**, es la parte de la red que esta directamente conectada a Internet y en esta zona se encuentran los primeros sistemas de protección, *Firewall,* detector de intrusos externos o sistemas de prevención y router principal de conexión, filtro de inspección y controles primarios de ataques.

- **Zona de para convenios interinstitucionales**, aquí se encuentran los enlaces de terceras instituciones que les brinda servicio, vía líneas dedicadas o canales cifrados. Dado que las instituciones con convenio alquilan circuitos de datos para la interconexión con la institución del caso de estudio, estos serán ubicados en esta zona.

  Los elementos presentes son:

  - *Router* de Comunicaciones de Telmex
  - *Router* de Comunicaciones de Telefónica
  - *Router* de Comunicaciones de Millicom del Perú

- **Zona de conexiones conmutadas**, en este segmento se encuentran las conexiones a los servicios de la institución que acceden vía conexiones circuitos de comunicación conmutados.
  Este tipo de conexiones son requeridas en lugares remotos.

- **Zona de servicios a Internet,** en esta zona de protección de colocaran los servicios brindados a Internet y los servicios relacionados con convenios interinstitucional :
  - Servidores Web de contenidos estático.
  - Servidor Anti-SPAM.
  - Servidor de envío de correo electrónico.
  - Servidor FTP de acceso vía RAS.
  - Servicio de Web mail.
  - Servidor transaccional para convenios interinstitucionales.

b.- Las política de protección externa a aplicarse son :

- Toda conexión deberá ser registrada y permitida explícitamente.
- Deberá esta activo los filtros *antispofing.*
- Activar los filtros de protección de inspección de protocolo.
- Controlar y reservar el ancho de banda para cada aplicación y/o servicio a brindarse.

TABLA Nº 6.4 IMPLEMENTACIÓN DE POLÍTICAS EN LISTAS DE ACCESO

Origen	Servidores	Servicios	Acción
Cualquier Origen	Servidor Web 1	http, https	ACEPTADO
Cualquier Origen	Servidor Web 2	http, https	ACEPTADO
Cualquier Origen	Servidor Antispam/Mail	smtp	ACEPTADO
Conexiones RAS	Servidor FTP	ftp	ACEPTADO
Grupo dedicadas de terceros	Servidor Transaccional	Transac. port	ACEPTADO
Acceso Irrestrictos	Cualquier Destino	todos	ACEPTADO
Accesos ftp	Cualquier Destino	ftp	ACEPTADO
Servidor Proxy	Cualquier Destino	http, https	ACEPTADO
Cualquier Origen	Cualquier Destino	todos	DENEGADO

Para este esquema se ha habilitado [3] y configurado la siguiente plataforma de seguridad perimetral: *Firewall-1 NGX* sobre el sistema hardening Secure Platform . Las características del mismo son mostradas en el ANEXO B. Las opciones de IPS habilitadas se muestran en el ANEXO C .

c .- Clasificación de las políticas de ancho de banda:

Debemos garantizar que los servicios de mayor importancia, descritos en la tabla 6.4, tengan mayores recursos de tráfico. Este se consigue implementando políticas de calidad de servicio de alto nivel, por pesos y limites.

TABLA Nº 6.5 DISTRIBUCIÓN DE ANCHOS DE BANDA USADOS

Clasificación	Ancho de Banda Garantizado
Servicios en Línea	40%
Portal Institucional	35%
Acceso a Internet	10%
Correo	10%
Otros	5%

Las políticas a aplicarse se reflejan en el correspondiente herramienta de gestión se muestran en la figura 6.3.

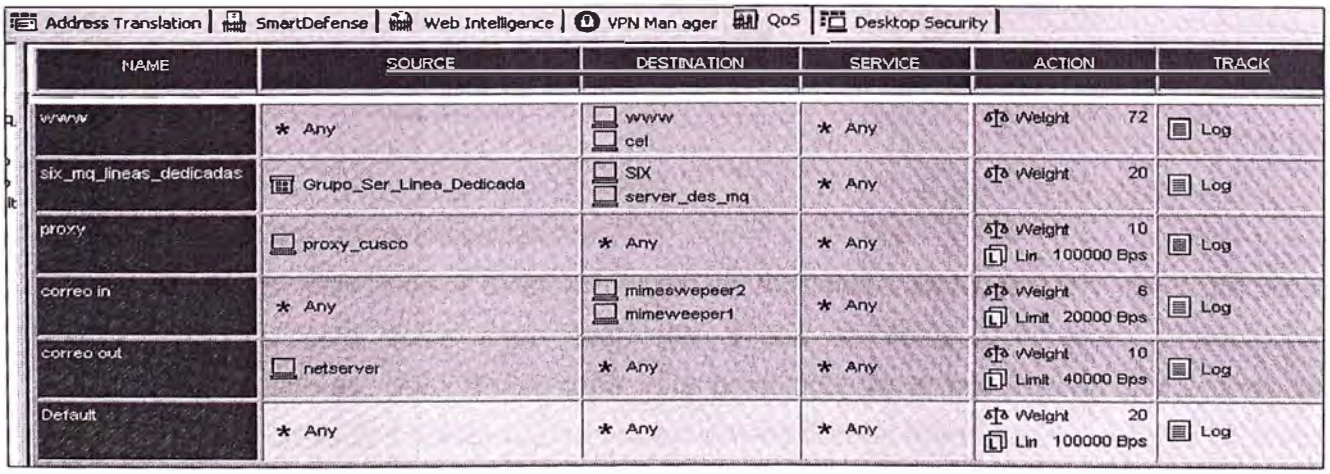

FIG. 6.3 CONFIGURACIÓN DE LAS POLÍTICAS DE ANCHO DE BANDA

6.4.1 Implementación Firewall Interno

De acuerdo a las estadísticas el 80% de las intrusiones son de origen interno, por lo tanto la protección interna de nuestra red es de alta importancia. Consideramos en la implementación y sistema de protección interna tipo arquitectura de tipo *appliance*, se le denomina así a los equipos de fabricación dedicada para una determinada función, con el hardware y software optimizado, se requieren dispositivos de esta naturaleza dado el alto tráfico interno de datos.

a.- Características necesarias para este dispositivo la mencionaremos a continuación:

TABLA 6.6 CARACTERÍSTICAS REQUERIDAS PARA EL *FIREWALL* INTERNO

Características	Valor
Throughput (Mbps)	500
Máximo Número de Conexiones	280,000
Número de Puertos	86
Firewall Transparente de Capa 2	SI
Soporte de Alta Disponibilidad	SI
Soporte de Protocolos de Encriptación	3DES /AES
Memoria de Aceleración para conexiones VPN	256 M
Sistema de Prevención de Intrusiones	SI
Gestión de Ancho de Banda	SI

b.- Descripción de las zonas de protección:

- **Zona de servicios a internet,** como se menciono en la sección de protección externa, esta zona esta destinada a los servicios a Internet y servicios institucionales, pero dicha zona esta protegida de la red interna por el *firewall* interno creando un sistema de protección en ambos frentes.
- **Zona de servidores de aplicación**, zona destina a los servidores de aplicación dado la programación en 3 capas presente en los aplicativos se requiere separar

los servicios de contenido estático de los sistemas donde se encuentren la lógica de negocio
en los servidores de aplicación, estos serán ubicados en esta zona de protección aislada creando una zona de protección de 2 frentes y doble nivel desde la Internet

- **Zona red local**: red interna de usuarios.
- **Zona de base de datos**: zona destinada al alojamiento del servidores de base de batos, y sistema de almacenamiento de datos.

c.- Dado que el esquema de filtrado interno es de prestación critica, se consideran los siguientes factores en su diseño:

- **Alta disponibilidad**: esta característica esta presente en las soluciones de protección existentes, y deberá ser activada y probada frente a algún fallo del equipo.
- **Sistema de conexión de emergencia**: esta configuración permite que todas las zonas de protección creadas puedan ser interconectadas aun en caso de falla de la configuración de alta disponibilidad, y no se encuentre operativo el sistema de protección interna, este escenario es presentado en caso de emergencia, y de acuerdo a la sistema de priorización mencionado, para el caso de estudio, la disponibilidad tiene rango 2, y será necesario mantener la operatividad de las comunicaciones internas, aun en caso de emergencia que será activado bajo el siguiente escenario
- **Tiempo de estado de emergencia**: será determinado y estimado como característica de la solución implementada en el tiempo de respuesta del proveedor frente a falla critica.

d.- Para el diseño de redes de las subredes a utilizarse, se considera el calculo del número de segmentos a utilizarse, estos se calculan en función al número de *host* .
Del número de servidores a utilizarse y el numero de segmentos, se estima un promedio máximo de 32 dirección por segmento, por lo tanto nos ser suficiente subdividir una red de clase C.
Si para nuestras zonas protegidas de nuestro *Firewall* interno elegimos la siguiente red de clase C: 192.168.100.0 /255.255.255.0, las sub redes a formarse se describen en la tabla 6.7.

TABLA Nº 6.7 DIRECCIONES IP PARA LAS REDES DE LAS ZONAS PROTEGIDAS

Dirección de Red	Mascara	Red	Rango de Direcciones	Hosts
192.168.100.0	/27	Servicios a Internet	192.168.100.0-31	32
192.168.100.32	/27	Servidores de Aplicación	192.168.100.32-63	32
192.168.100.64	/27	Servidores de Base de Datos	192.168.100.64-95	32
192.168.100.96	/27	Servicios Externos	192.168.100.96-127	32
192.168.100.128	/27	Servicios de Accesos Conmutados	192.168.100.128-159	32
192.168.100.160	/27	Sub. Red Reserva	192.168.100.160-191	32
192.168.100.192	/27	Sub. Red Reserva	192.168.100.192-223	32
192.168.100.224	/27	Sub. Red Reserva	192.168.100.224-255	32

e.- Políticas de protección:

TABLA Nº 6.8 ACCESO PARA EL *FIREWALL* INTERNO

Origen	Destino	Serv. Permitidos
Rede Local o de Usuarios	Zona de Servicios a Internet	http, https
Rede Local o de Usuarios	Zona de Servidores de Aplicación	http, https
Zona de Servidores de Aplicación	Zona de Base de Datos	nfs, sql
Administradores de Sistemas	Zona de Base de Datos	Sql ssh
Administradores de Sistemas	Zona de Servicios a Internet	ssh
Administradores de Sistemas	Zona de Aplicaciones Internas	ssh
Cualquiera	cualquiera	icmp

f.- Se han activado también las siguientes opciones de seguridad para evitar ataques o desbordamientos internos.

- Aplicación de Políticas de QoS
- Aplicación de Limites de Conexión y TCP Normalización
- Habilitar la Inspección avanzada de HTTP.
- El motor de inspección de ESMTP.
- Habilitar el motor de inspección de ICMP.
- Habilitar el motor de inspección del protocolo SIP.

Para la habilitación de las políticas se ha utilizado la plataforma de seguridad PIX de Cisco Systems cuyas características se mencionan en el ANEXO D.
Sin embargo se tiene en evaluación el sistema de protección interna **Interspect** cuyas características se mencionan en el ANEXO E.

6.4.3 Implementación del IDS distribuido

Como complemento a los sistemas de prevención de intrusiones se implementara IDS.
El primer paso antes de configurar un sistema de detección de intrusiones, debemos habilitar la capacidad de monitorear el tráfico de red, reflejando el puerto de conexión de los *switches*.
En modelos como el switch Cisco de las series 2700 o superior en los comandos son:

```
swdmz#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
swdmz(config)#int Fa0/9
swdmz(config-if)#port monitor
```

Con de la denominación Fa0/9 se refiere al puerto del *switch* que habilitará en modo de análisis de tráfico.
Dado los zonas de protección descritas se colocarán sistemas de detección en cada segmento como se muestra la figura 6.3, cada IDS tendrá como función monitorear cada segmento de la red y todo esta información será centralizada en una sistema de almacenamiento con una base de datos relacional, al cual se conectara una sistema de gestión y mostrara reportes vía una interfaz Web.

El siguiente diagrama muestra el esquema planteado:

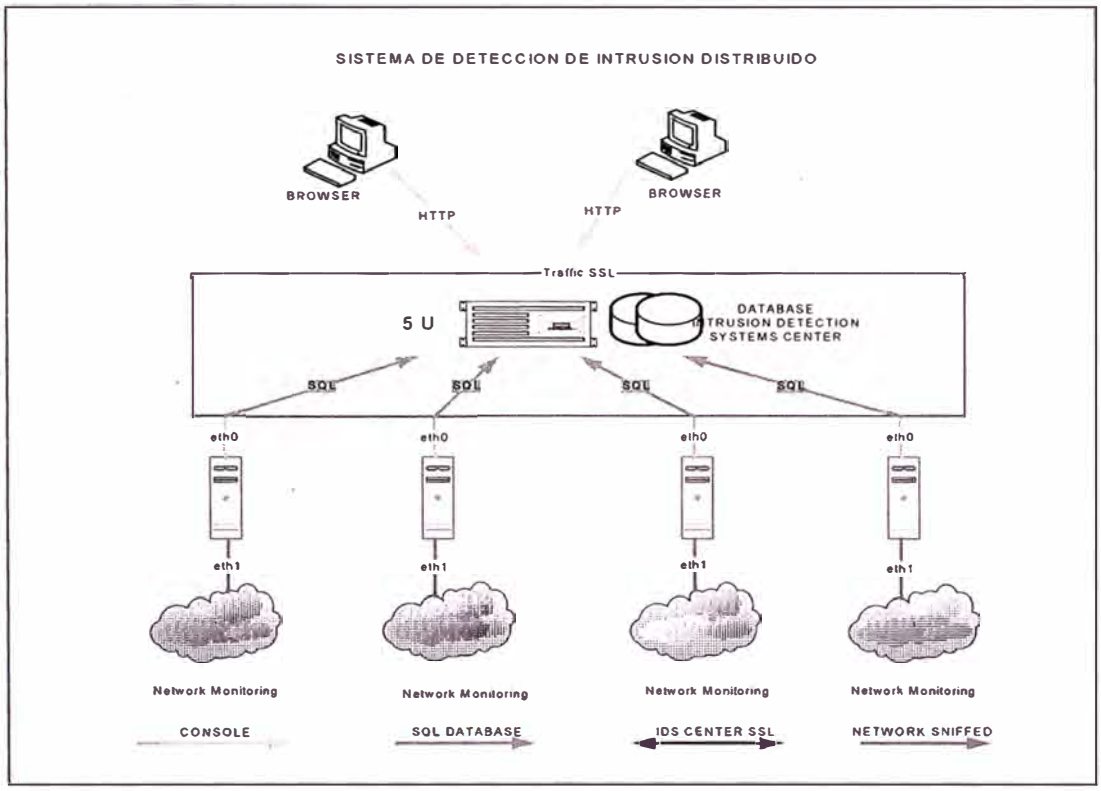

FIG. 6.4 COMPONENTES DEL IDS DISTRIBUIDO

Para este sistema se contempla el uso del sistema de intrusiones: **SNORT,** un proyecto **open source** de desarrollo avanzado flexible y escalable.

Requerimientos de Software:

a. **Snort :** sistema de detección de intrusiones con capacidad de análisis de tiempo real y registro de paquetes de red.
b. **Mysql Server:** es un motor de base de datos relacional, para el almacenamiento de los registros y eventos, que permite ejecutarse en variedad de plataformas.
c. **ACID:** es una aplicación basada en web que permite mostrar y reportar los eventos centralizadas en la base de datos.
d. **Snort center:** es un software que centraliza y administra las firmas, patrones de ataques y archivos de configuración.
e. **Apache Web Server:** es el motor de contenido estático de mayor uso en la Internet debido a sus características avanzadas en el manejo de paginas Webs.

Como lo muestra la figura superior los siguientes son los módulos:

Como lo muestra la figura superior los siguientes son los módulos:
- Sistemas sensores, correspondiente a una igual numero de segmentos protegidos.
- Base de datos relacional.
- Sistema de correlación de eventos.
- Sistema de aplicación gestión Web.

Los detalles de la implementación son mostrados en el Anexo A.

6.4.4 Implementación de las políticas de acceso de Internet

De acuerdo a las políticas implementadas, el acceso a Internet es un recurso a controlarse, tomándose las siguientes medidas de protección

a .- Políticas de Seguridad

- A nivel de usuario , no están permitidos las conexión directas al *firewall*
- Cada acceso deberá ser autenticado y registrado.
- Se debe poseer un filtro de contenidos.
- Se debe contar con un *proxy cache*.
- El uso de los protocolos SSL es restringido a destinos autorizados.

Se ha clasificado entonces, 6 niveles de permisos, de acuerdo a las funciones y cargos que se desempeñan, los cuales están mencionados en la tabla 6.9.

b.- Esquema de acceso

Para la implementación se ha considerado las siguientes esquema de conexión :

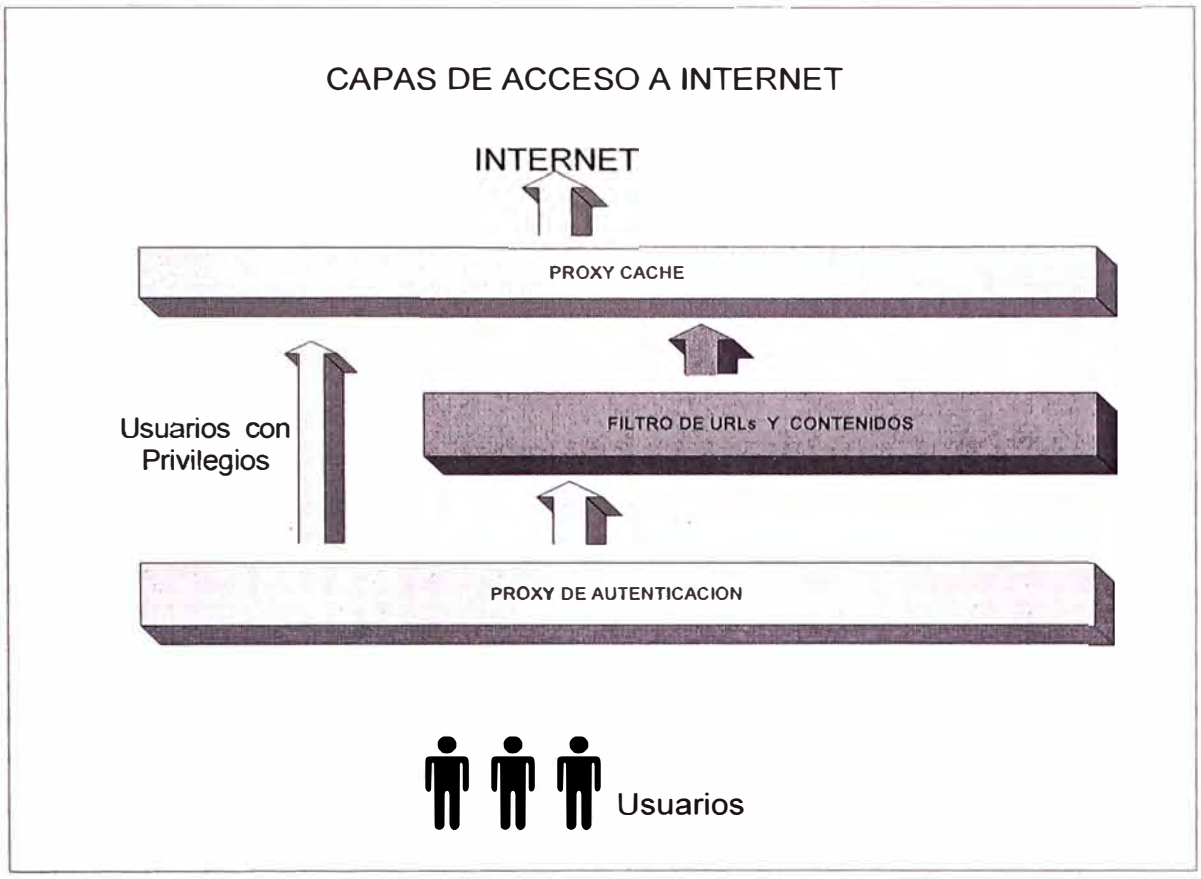

FIG. 6.5 NIVELES DE ACCESO A INTERNET

c.- Componentes del sistema

Para la implementación de cada modulo se usará los siguientes recursos de software:

- Squid-Cache *Proxy cache* y *proxy* de autenticación.
- Samba Plataforma de conexión para los servidores de políticas de dominio.
- Dansguardian : Filtro de contenidos.

Cada componente tiene las siguientes características:

- **Proxy de Autenticación**: permite validar las cuentas de acceso, este módulo se valida a su vez con el controlador de dominio principal usando el modulo LDAP.

  Configurar el soporte de parámetro *cache_peer* direccionándose hacia el filtro de contenidos.

  No almacenar *cache*.

Las siguientes son las opciones necesarias:

```
cache_peer access 127.0.0.1 parent 3120 0  proxy-only no-query default
cache_peer acess 127.0.0.1 allow
no_cache deny all
never_direct allow all
```

Perfiles La configuración de las reglas de acceso se muestra en la tabla siguiente:

TABLA Nº 6.9 PERFILES DE ACCESO A INTERNET

GRUPOS	EXTENSION	HORAS	DIAS	ANCHO DE BANDA
vip 1	Irrestricto	irrestricto	irrestricto	NO
vip 2		irrestricto	irrestricto	
Inter1	.doc .xls .ppt .pdf .zip .exe .rar	8:30-17:30	L-V	SI
Inter 2				SI
básico 1	.doc .xls .pdf .ppt	8:30 15:30	L-V	SI
básico 2	Ninguno	8:30 17:30	L-V	SI

- Filtro de contenidos: este modulo permite bloquear los contenidos de acceso regular para el personal con el servicio de Internet, permitiendo el bloqueo por contenido, URL completo parcial, extensión, *mime*, entre otros formatos.
  filter_port =3120
  proxyip=127.0.0.1
  proxyport=3128
  forwardedfor=on
  usexforwardedfor = on

- Proxy cache: Es la capa externa el cual aloja los diversos objetos de tráfico a Internet, con la intención de optimizar el tráfico, y sirviendo de repositorio para nuevas transacciones.
  http_port = 3128
  cache_dir = ufs /tmp/cache 6000 16 256

cache_access_log /dev/null
cache_log /dev/null

Como se especifico dentro de las políticas de acceso a Internet, el acceso usando el protocolo SSL es restringido, debido a su uso recurrente en sistemas de mensajería instantánea, que no es permitido dentro de la organización. El acceso vía este protocolo será solo permitido para portales de banca, gobiernos, servicios públicos, correo electrónico externos autorizados, y extranet autorizadas.

En el anexo 2 se adjuntan la relación de portales de confianza para la institución.

- Filtro para accesos SSL:
  Mediante este mecanismos se restringe el uso del protocolo SSL a cualquier destino, un ejemplo de filtro es mostrado a continuación:

  Los archivos basico1.txt, intermedio1.txt y vip1.txt contienen los usurarios permitidos.
  Y utilizando la característica de filtrado de paquetes de Netfilter, permitimos solo a algunos y denegamos al resto :

```
#Filtro de https
DIRBASE=/usr/local/squid-auth/etc
num_shost=$(cat "$DIRBASE"/basico1.txt "$DIRBASE"/intermedio1.txt "$DIRBASE"/vip1.txt
| grep -v '#' | wc | cut -c5-8)
contador1=1
echo hay $num_shost registros
while [ $contador1 -le $num_shost ] ; do
ips=$(cat "$DIRBASE"/basico1.txt "$DIRBASE"/intermedio1.txt "$DIRBASE"/vip1.txt | grep
-v '#' | head -$contador1 | tail -1)
#echo contador en $contador1
iptables -t nat -A PREROUTING -i eth0 -s $ips -d 0.0.0.0/0 -p tcp --dport 443 -j ACCEPT
let contador1=contador1+1
done
num_dhost=$(cat /root/dip.txt | grep -v '#' | wc | cut -c5-9)
contador2=1
```

```
echo hay $num_dhost servers https permit
echo permitidos a cualquier destino https para users con permiso
while [ $contador2 -le $num_dhost ] ; do
ipd=$(cat /root/dip.txt | grep -v '#' | head -$contador2 | tail -1 |cut -c1-15)
echo contador2 en $contador2
iptables -t nat -A POSTROUTING -o eth1 -d $ipd -p tcp --dport 443 -j SNAT --to
200.121.68.166
let contador2=contador2+1
done
iptables -t nat -A POSTROUTING -o eth1 -d 0.0.0.0/0 -p tcp --dport 443 -j DROP
```

Los sites de confianza para el uso del protocolo SSL, se muestran en el ANEXO G.

6.4.5 Seguridad en acceso equipos de redes

Políticas de acceso

- Los dispositivos de la infraestructura de telecomunicaciones, son parte importante en la garantía de conectividad de la red, por lo tanto su acceso y configuración es restringida.
- Cada acceso deberá ser autenticado y registrado.
- De deberá contar con un sistema de gestión de cuentas para los equipos de redes

Los dispositivos a gestionarse son:

98 Switches

30 Routers

El esquema contempla la configuración de un servidor TACACS, para autenticar cada usuario que administre los equipos de comunicaciones.

La figura 6.5 muestra el esquema lógico de acceso a los equipos de comunicaciones:

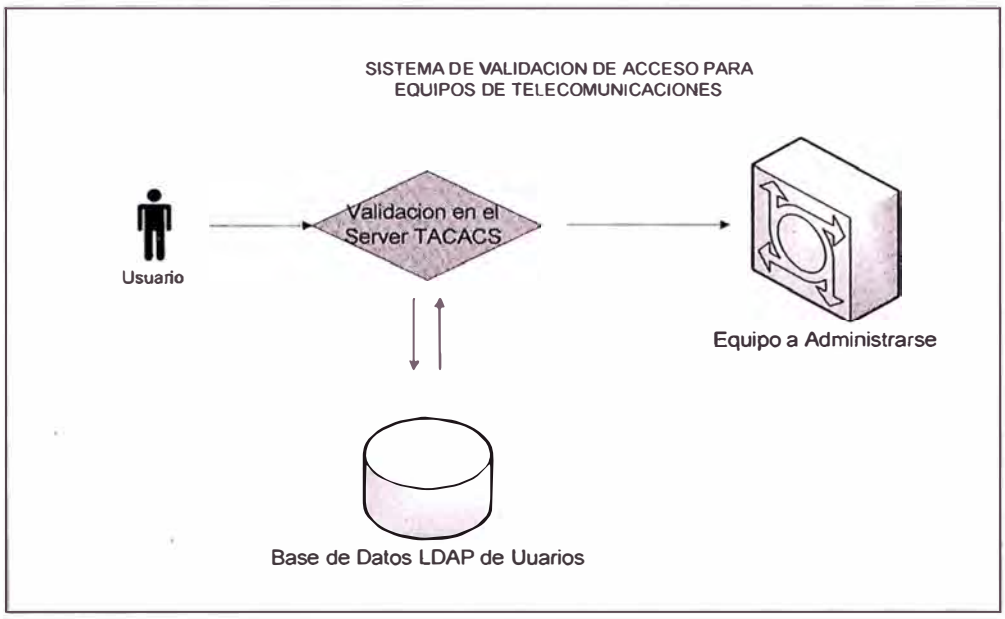

FIG. 6.6 SISTEMA DE AUTENTICACIÓN DE USUARIOS VÍA TACACS

6.4.6 Implementación de accesos VPN

La habilitación de este servicio tiene por finalidad extender los sistemas de comunicación y gestión, de manera segura y transparente, permitiendo que el personal autorizado pueda acceder a recursos informáticos de la organización, desde ubicaciones remotas hacia recursos controlados y protegidos.

a.- Alcance

- Personal ejecutivo que requiera acceder a los servicios Internos desde fuera de la organización.
- Personal de informática de sea responsable de servicios informáticos en la organización.

b.- Análisis de Necesidad

La organización cuentas con diversos sistemas informáticos, que son administrados a su vez por diverso personal especializado, estos cumplen regularmente sus laborares físicamente dentro de la organización, pero a su vez los sistemas informáticos de la organización están activos bajo el servicio 24x7, y si bien estos son monitoreados por el personal de operadores de centro de computo, en diversas ocasiones se requiere que el o los responsables de los servicios configure los sistemas con el menor tiempo posible.

El servicio VPN, permite que el personal autorizado se conecte a los sistemas informáticos que le son asignado, desde canales remotos usando de medio de conexión la Internet, para esto se configuran diversos mecanismos de cifrado y protección de la comunicación, que garantizan la confidencialidad del mismo.

c.-Tipos de seguridad permitidas

El servicio de VPN puede soportar los siguientes sistemas cifrados:

- Algoritmos de Encriptación : 3DES , AES -128, AES-256
- Integridad de Datos : MD5 , SHA1
- IKE Security Associations : Diffie-Hellman 1024 bits

d.- Políticas de seguridad para usuarios VPN

- Los usuarios del servicio deberán contar con la debida autorización de su responsable, indicando servidores a conectarse, niveles de acceso poseídos.
- Sobre los niveles de acceso

  Se especificaron 2 niveles de acceso:

TABLA Nº 6.10 GRUPO DE USUARIOS VPN Y TIPO DE AUTORIZACIÓN

Niveles	Servicios Disponibles	Autorización Manual*
Ejecutivo	Aplicativos internos: correo, tramite Documentario, etc.	No
Administración de Sistemas	Acceso a Recursos que se encuentran bajo su responsabilidad.	Si

- Para el caso de los responsables de la administración de sistemas. Deberán realizar un procedimiento de validación antes del inicio de sesión.
- Para el caso del nivel ejecutivo este procedimiento previo no es necesario dado que solo accederán a los servicios Internos públicos, y no a configuración de recursos informáticos.

- Los usuarios de administración de servicios informáticos no estarán permitido de acceder a recursos que no formen parte de su labor dentro de la organización.
- Solo esta permitido la conexión directa a recursos, vale decir, la conexión a un tercer recurso valiéndose de un conexión ya utilizada no esta permitido.

e.- Implementación y pruebas

A continuación se muestra el cuadro de evolución y duración de implementación del sistema:

TABLA Nº 6.11 ACTIVIDADES PARA LA IMPLEMENTACIÓN VPN

Fases	Estado	Numero de Días
Instalación del servicio	Completado	1
Pruebas de *performance*	Completado	4
Revisión de políticas de seguridad	Completado	5
Creación de usuarios y configuración de equipos		

f.- El diagrama de interconexión se muestra en la Figura 6.6.

Aquí se puede observar los 2 grupos de usuarios que serán permitidos y los recursos a los que podrán acceder.

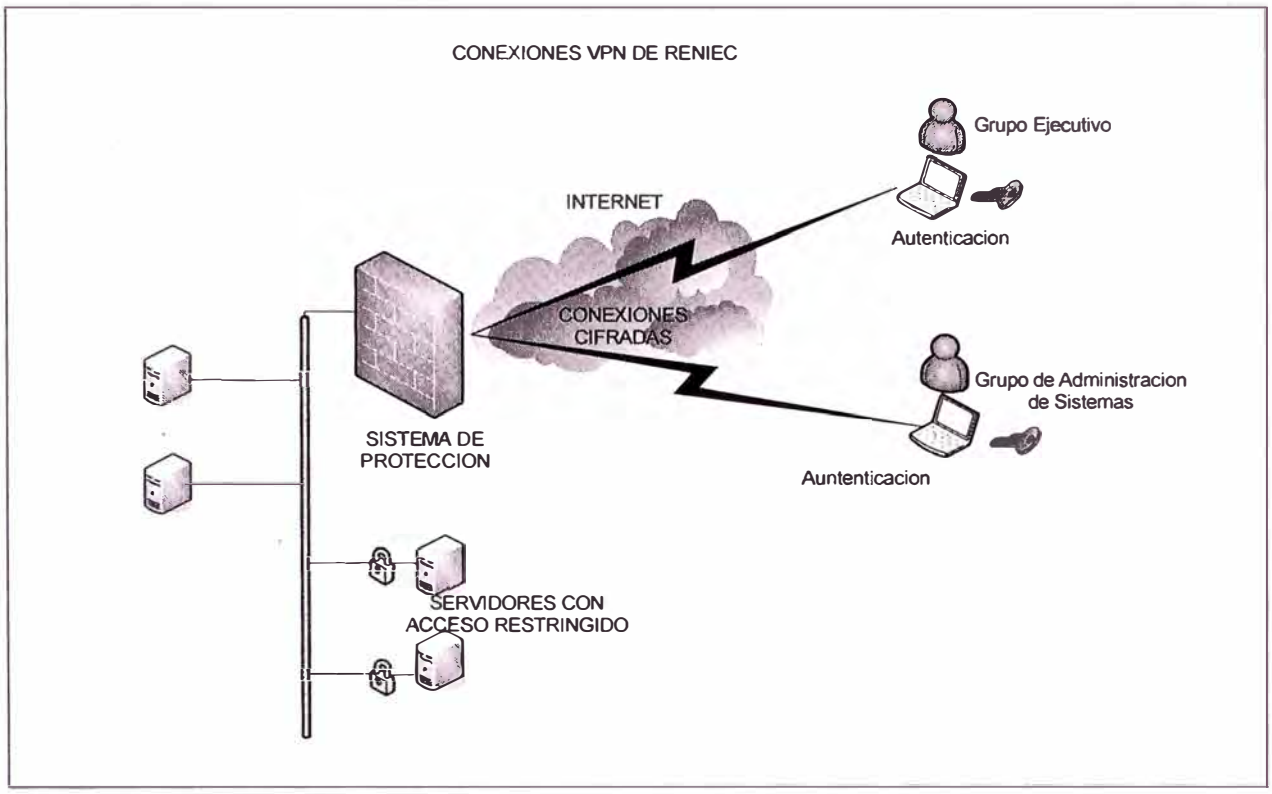

FIG. 6.7 ELEMENTOS DE CONEXIÓN VPN

g.- Seguridad y políticas

Como parte de la puesta en ejecución de estos sistemas, se requiere la implementación de políticas de seguridad, que usuarios las entiendan, las acepten
y las cumplan

- a.- Los accesos son personales e intransferibles, y son uso exclusivo para las labores que la institución requiera.
- b.- Están solo permitidos los accesos a los recursos autorizados por su respectivo jefe inmediato y supervisado por los sistemas de seguridad de la institución.
- c.- Solo son permitidos de acceder los equipos móviles de la instrucción, con la debida configuración por parte del personal competente, los equipos móviles personales, las computadoras personales.
- d.- No son permitidos los accesos desde equipos compartidos, como cabinas de Internet, redes de terceros, etc.

- e.- Todas las estaciones de trabajo deberán aceptar las políticas de protección que les serán transmitas una vez sean iniciadas la sesión de VPN.
- f.- El personal autorizado para realizar dichas conexiones deberá firmar los documentos de las políticas de seguridad estipulando que ha comprendido y que cumplirá el establecido en dichas políticas bajo pena de acción judicial.

h.- Implementación

Para la solución se han consideración los siguientes elementos software:

- *Firewall-1 with VPN1* , como equipo de terminar de los tuneles y autenticación
- *Secure Client*, como cliente de conexión VPN, para los equipos de los usuarios.

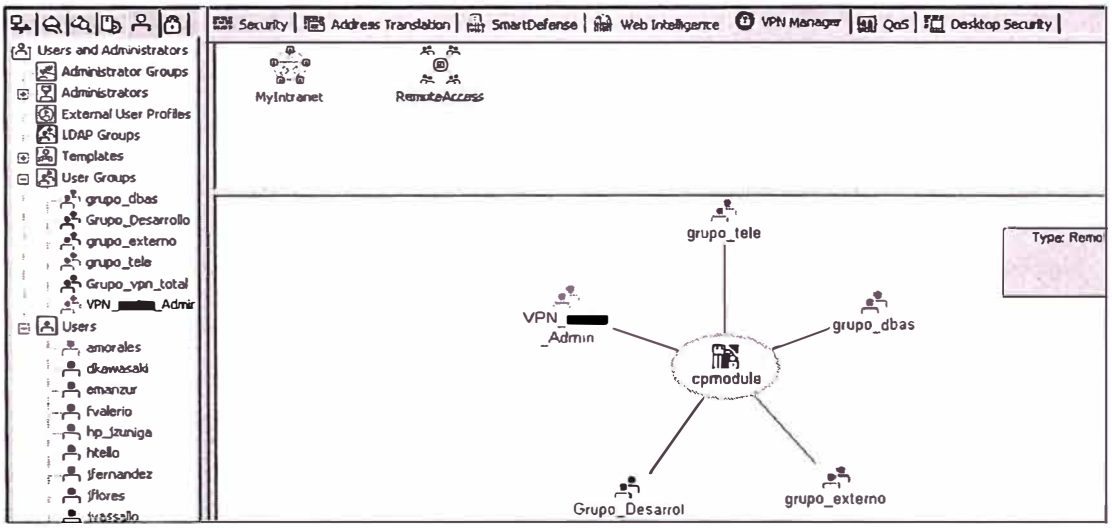

FIG. 6.8 VISTA DE LA CONFIGURACIÓN DE VPN

6.5 Resumen del capítulo

En este capitulo se trata sobre un caso real de implantación de un sistemas de seguridad informática. Se ha analizado, diseñado e implementado los diversos elementos de protección que permiten de manera adecuada fiabilizar nuestros sistemas, mitigando ataques de red que podrían presentarse.

Las soluciones implementadas contemplan también sistemas de seguridad propietario, como de código abierto, permitiendo una mejor flexibilidad para su crecimiento.

CONCLUSIONES

1. De acuerdo a lo mencionado en la sección correspondiente, la seguridad es un término relativo, se trata entonces de construir un entorno fiable.

2. La seguridad informática es naturalmente evolutiva, y dinámica, luego es necesario construir entornos escalables, para que puedan ser adaptados a las nuevas necesidades de la organización.

3. De lo analizado se entienda claramente que la seguridad informática pasa necesariamente por realizar buena práctica en políticas de seguridad, no son adecuados los sistemas de seguridad sin sus respectivas políticas que las gobiernen.

4. Sobre los casos particulares en la etapa de implementación, es necesario que los sistemas de protección sean de fabricantes o de arquitectura distinta, esto debido a que es común que aparezcan vulnerabilidades que afectan a una determina familia de productos.

5. La seguridad de los sistemas informáticas posee muchas formas y alcances; es necesario formar un equipo con el concurso de diversas áreas, incluso área legal y de recursos humanos, para las políticas a implementar se gestionen adecuadamente.

6. Sin bien es cierto que el alcance del presente documento es sobre redes corporativas, existen casos en el cual las redes son más complejas, como redes de e-commerce, redes de proveedores de Internet, que debido a su particular

infraestructura requiere una organización dedicada a la implementación de dicho sistema de seguridad.

7. Otras de las consideraciones que se debe tener en cuenta en las actuales redes de comunicaciones, son los dispositivos de almacenamiento móvil, estos son potenciales mecanismo de extracción de información, las políticas de seguridad también deben ser aplicadas a estos para que su uso se solo permitido bajo supervisión y autorización.

8. Otro de los mecanismos adicionales de protección para las redes internas son las VLANs.

ANEXO A

CUADRO DE SERVICIOS PARA RESTRINGIR EN UN ROUTER

TABLA Nº F.1 CUADRO DE SERVICIO A RESTRINGIR

Puerto	Protocolo	Servicio
1	(TCP&UDP)	tcpmux
7	(TCP&UDP)	echo
9	(TCP&UDP)	discard
11	(TCP)systat	systat
13	(TCP&UDP)	daytime
15	(TCP)netstat	netstat
19	(TCP&UDP)	chargen
37	(TCP&UDP)	time
43	(TCP)whois	whois
67	(UDP)bootp	bootp
69	(UDP)tftp	tftp
93	(TCP)supdup	supdup
111	(TCP&UDP)	sunrpc
135	(TCP&UDP)	loc-srv
137	(TCP&UDP)	netbios-ns
138	(TCP&UDP)	netbios-dgm
139	(TCP&UDP)	netbios-ssn
177	(UDP)xdmcp	xdmcp
445	(TCP)netbios(ds)	Netbios
512	(TCP)rexec	Rexec
515	(TCP)lpr	Lpr
517	(UDP)talk	Talk
518	(UDP)ntalk	Ntalk

540	(TCP)uucp	Uucp
1900-5000	(TCP&UDP)	Microsoft
2049	(UDP)nfs	Nfs
6000-6063	(TCP)XWindow	System
6667	(TCP)irc	Irc
12345	(TCP)NetBus	NetBus
12346	(TCP)NetBus	NetBus
31337	(TCP&UDP)	Back

ANEXO B

CARACTERISTICAS TECNICAS DE FIREWALL -1

Check Point Firewall-1 es una solución de gateway de seguridad que provee protección contra múltiples formas de ataque.
Usa la tecnología INSPECT y Application Intelligence, integrando protección de red y de aplicaciones.
Sus diversos mecanismos de protección de control de accesos, protección de ataques, aplicaciones de seguridad, prevención de intrusiones, seguridad de contenido, autenticación, calidad de servicio, traslación de direcciones (NAT), Open Platform for Security (OPSEC) se adicionan con la compatibilidad para interaccionar con productos de terceros.
Posee las siguientes características:

- Amplia presencia en el mercado
- Extenso soporte de aplicaciones
- Protección contra ataques de red y de aplicación
- Seguridad para aplicaciones Web
- Seguridad de VoIP
- Granularidad en la seguridad del contenido
- Autenticación Flexible
- Traslación de Direcciones integradas
- Consola de Administración central
- Interfaz de usuario para gestión, estado y auditoria
- Alta disponibilidad
- VPN segura

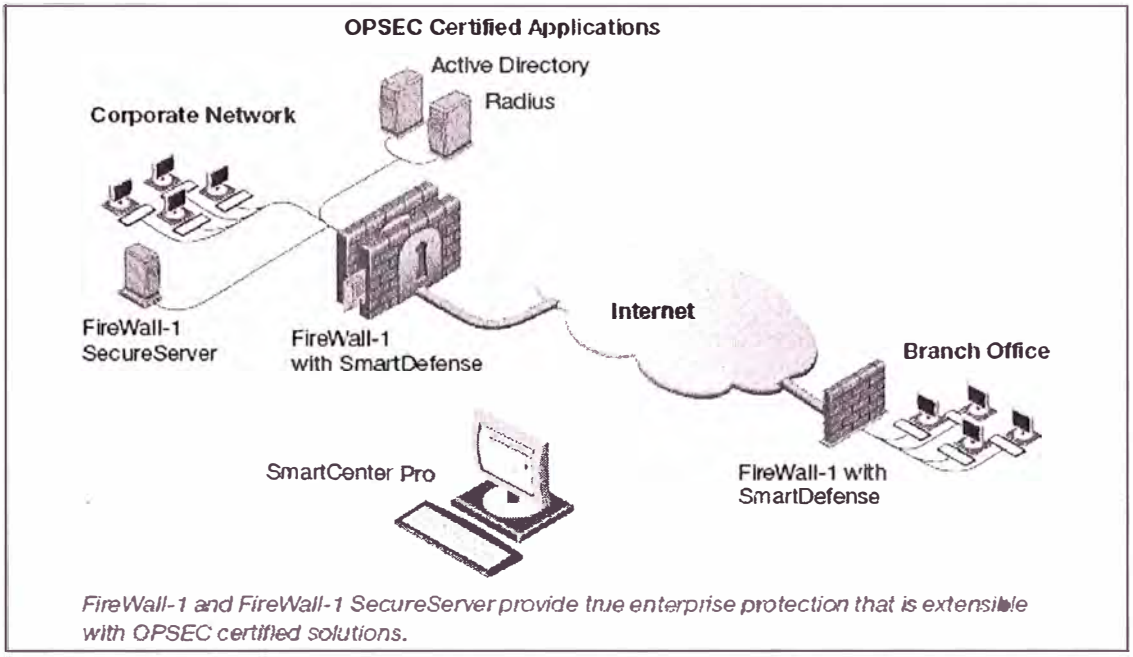

Fig B.1 Esquema de conexión del Firewall -1

ANEXO C

ACTIVACION DE MECANISMOS SISTEMA DE PREVENSION DE INTRUSIONES DEL FIREWALL-1

- *Network Security*

1. *Teardrop*
2. *Ping of death.*
3. *LAND.*

- *IP and TCP*
    1. *Packet sanity*
    2. *Max ping size.*
    3. *IP fragments.*
    4. *Network quota.*
    5. *SYN attack configuration.*
    6. *Small PMTU.*
    7. *Sequence verifier.*
- *Fingerprint Scrambling ISN*

1. *Spoofing.*
2. *TTL.*
3. *IP ID.*

- *Successive Events*
    1. *Address spoofing.*
    2. *Local interface spoofing.*
    3. *Port scanning.*
    4. *Succesive alerts.*
    5. *Sucessive multiples connections.*

- *Web General HTTP Word Catcher*
    1. *Cross Site Scripting.*
- *HTTP Protocol Inspection*
    2. *HTTP Format Sizes*
    3. *ASCII Only Request Headers.*

4. ASCII Only Response Headers.

- *Mail SMTP Content*
- *Mail and Recipient Content*
- *FTP FTP Bounce*
- *VoIP Verify SIP header content*

ANEXO D

CARACTERISTICAS DE SISTEMA DE PROTECCION PIX

Mediante la Familia de equipos ASA, Cisco ha integrado una combinación de tecnologías para la protección proactiva contra amenazas y ataques.

Las características más relevantes son:

Posee completas características y alta capacidad de performance, sistema de prevención de intrusiones, control Anti –X, soporta aplicaciones protocolo de seguridad como IPsec, SSL, sistemas de control de acceso, mitigación de gusanos, protección malware, filtro de contenidos y conectividad remota.

La Arquitectura de identificación y mitigación (AIM), posee un procesamiento de servicios modular y una plataforma de políticas de seguridad, entregando una gran granularidad de control de políticas

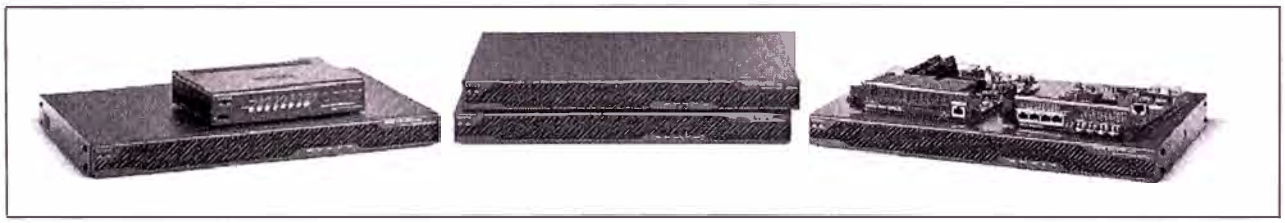

Fig D.1 Diversos modelos de equipos de seguridad de Cisco Systems

Se puede mencionar que también posee las siguientes características:

- Servicios Avanzados de Firewall
- Firewall Transparente (Layer 2 Firewall)

- Seguridad por Contexto (Virtual Firewall)
- Listas de acceso en base a tiempo
- Habilitación/Desabilitación de entradas ACL
- Arquitectura de políticas modular

- Motor de inspección avanzada de HTTP
- Motor de inspección ESMTP
- Motor de inspección SunRPC/NIS+
- Motor de inspección ICMP
- Motor de inspección para redes wireless
- Motor de inspección de H.323
- Motor de inspección SIP

- Soporte de Redes privadas virtuales
- Ruteo dinámico OSPF sobre VPN
- Soporte de certificados digitales X.509

- Inspección IPV6
- Soporte mejorado de multicast
- Sistema de encolamiento y baja latencia (LLQ)
- Sistema Activo/Activo con soporte de routeo asimétrico
- Características de Stateful Failover
- Software de actualización, con características de Zero Downtime
- Soporte de SSHv2, SCP, FTP y SNMP
- Reinicio del sistema por programación de tiempo.

ANEXO E

CARACTERISTICAS DE SISTEMAS DE PROTECCION INTERNA: INTERCEPT

Las siguientes son las características descritas por el fabricante Check Point
Check Point InterSpect es una pasarela interna de seguridad que bloquea la propagación de gusanos y ataques dentro de la red y permite segmentar la red en zonas. InterSpect, basado en las probadas tecnologías de seguridad de Check Point (INSPEC, Stateful Inspection, Application Intelligence y Security Management Architecture), está diseñado específicamente para la seguridad de redes internas. InterSpect ofrece:

• Intelligent Worm Defender
Bloquea la propagación de gusanos y ataques dentro de la red
• Segmentación de la red en zonas
Segmenta la red interna en zonas organizativas de seguridad
• Puesta en cuarentena de los ordenadores sospechosos
Aísla los ataques y los dispositivos infectados
• Protección de protocolos LAN
Ofrece la compatibilidad más extensa y completa con los protocolos de Microsoft y otros protocolos LAN
• Protección preventiva contra ataques
Ofrece defensa proactiva frente a los riesgos de las vulnerabilidades y ataques antes de su explotación.

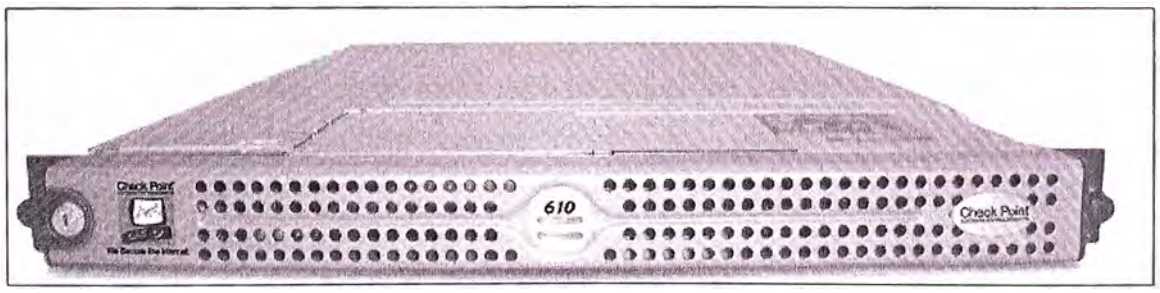

Fig. C.1 Vista frontal del dispositivos de seguridad interna Interspect

Administración adaptada a la seguridad interna:
La administración de InterSpect se ve facilitada por el uso de una interfaz de administración diseñada específicamente para la seguridad interna. Esta interfaz, basada en la arquitectura SMART de Check Point, ofrece un medio potente y de fácil uso para responder a los problemas de configuración y administración de políticas propios de la seguridad interna.
Por regla general, los firewalls de nivel de red se configuran de forma que rechacen todo el tráfico que no esté explícitamente autorizado. Esto puede ser muy complicado de configurar en el caso de instalaciones internas.

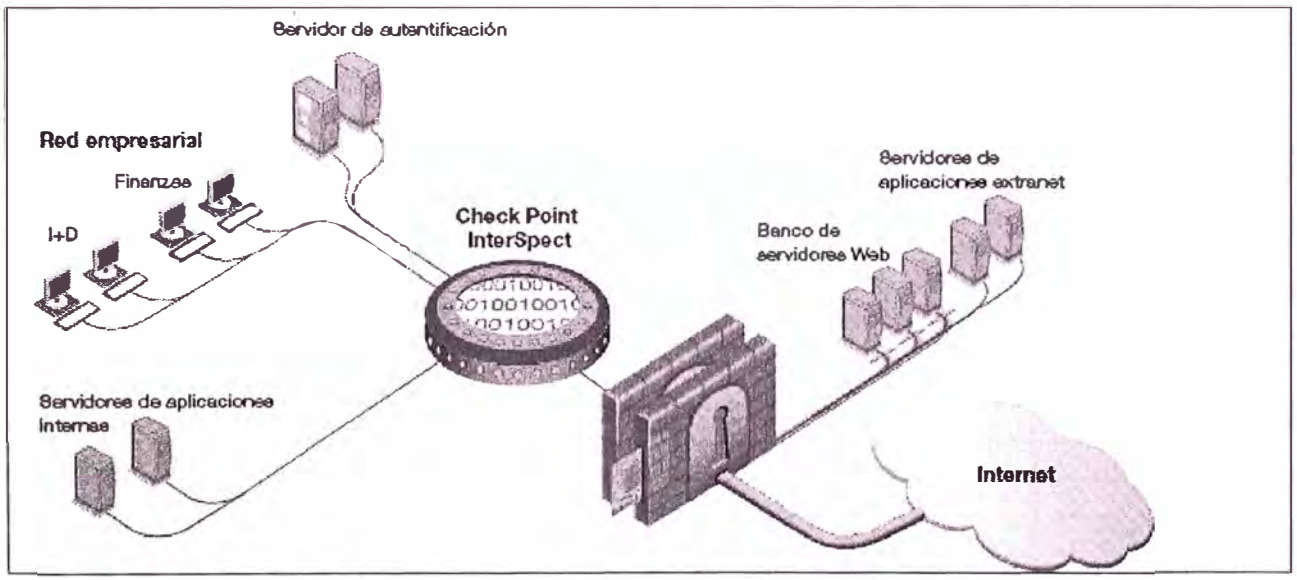

Fig C.2 Esquema de interconexión del Firewall Interspect

Pero, con Check Point, la segmentación de la seguridad es muy sencilla: basta instalar InterSpect en la red y definir las zonas de seguridad de la misma. InterSpect empieza inmediatamente a inspeccionar el tráfico y a rechazar los contenidos maliciosos a la vez que permite el tráfico normal de la LAN. Los administradores pueden desautorizar explícitamente determinados patrones de tráfico y configurar zonas internas de seguridad mediante una sencilla interfaz de segmentación.

RENDIMIENTO

RENDIMIENTO

InterSpect es un dispositivo diseñado para satisfacer las exigencias de rendimiento de la seguridad interna. InterSpect se basa en Secure Platform, el sistema operativo de seguridad reforzado de Check Point. Para garantizar un nivel óptimo
de rendimiento, InterSpect incluye asimismo la tecnología patentada de aceleración de seguridad SecureXL™ de Check Point.

ESPECIFICACIONES

Tabla C.1 Comparaciones técnicas de los modelos de Interspect

	InterSpect 210	InterSpect 410	InterSpect 610	InterSpect 610F
Objetivo	Protección de un grupo de trabajo	Protección múltiple de grupos de trabajo	Protección de red Gigabit	Protección de red Gigabit
Entorno operativo	SecurePlatform de Check Point	SecurePlatform de Check Point	SecurePlatform de Check Point	SecurePlatform de Check Point
Rendimiento	200 Mbps	500 Mbps	1000 Mbps	1000 Mbps
Interfaces de fibra	N/A	Disponibles como complemento	Disponibles como complemento	Incluidas
Ranuras de expansión	N/A	1	1	1
Puertos de inspección	2	3-10	3-10	3-10
Puertos de administración	1	1	1	1
Núm. máximo de puertos	3	10	10	10
Velocidad de la interfaz	10/100 Mbps	10/100/1000 Mbps	10/100/1000 Mbps	10/100/1000 Mbps
VLAN admitidas	8 VLANs	128 VLANs	Ilimitadas	Ilimitadas
Alimentación redundante	No	Opcional	Incluidas	Incluidas
Suscripción a SmartDefense	Incluida el primer año	Incluida el primer año	Incluida el primer año	Incluida el primer año
Ancho	16,7"/42,5 cm	17,61"/44,7 cm	17,61"/44,7 cm	17,61"/44,7 cm
Altura	1,68"/4,2 cm (1U)	1,68"/4,2 cm (1U)	1,68"/4,2 cm (1U)	1,68"/4,2 cm (1U)
Fondo	21,9"/55,5 cm	27"/68,3 cm	27"/68,3 cm	27"/68,3 cm
Peso	27 lbs/12,25 kg	35 lbs/15,9 kg	35 lbs/15,9 kg	35 lbs/15,9 kg
Alimentación	100-220 V 50/60 Hz	100-220 V 50/60 Hz	100-220 V 50/60 Hz	100-220 V 50/60 Hz

ANEXO F

IMPLEMENTACION DE LA SOLUCION DE DETECCION DE INTRUCIONES DISTRIBUIDO

1.- ALCANCES

Con este sistema se pretende habilitar diversos sensores de detección de intrusiones en distintos segmentos de red y gestionar y centralizar la administración.

2.- COMPONENTES

Se requieren el siguiente software para la implementación del sistema:

Sistema Operativo Linux

- Snort
- Mysql
- Mysql-client
- Mysql-shared
- Mysql-devel
- ACID
- PHP
- Php-mysql
- ADODB
- JPgraph
- GD
- Snort Center,
- Snort Center-Agent
- NetSSLay
- Apache

3.- INSTALACION

Instalación de Apache Web Server:

```
# rpm -ivh httpd-last-version.i386.rpm
# chkconfig --level 2345 httpd on
# /etc/rc.d/init.d/httpd start
```

Instalación de la Base de Datos Mysql.

```
# rpm -ivh MySQL-last-version.i386.rpm
# rpm -ivh MySQL-client- last-version.i386.rpm
# rpm -ivh MySQL-shared- last-version.i386.rpm
# mysql -u root
mysql> set password for 'root'@'localhost' = password('yourpassword');
mysql> create database snort;
mysql>exit
# chkconfig --level 3 mysql on
```

Se deben crear los permisos respectivos así como los script de generación de tablas que el Snort Center utilizará.

Ejecutar el script : *create_mysql* que se puede obtener de :
http://cvs.sourceforge.net/cgi-bin/viewcvs.cgi/snort/snort/contrib/

```
mysql -u root -p
mysql> connect snort
mysql> source create_mysql
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.*
to snort; So you can connect locally with this account
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort@localhost;
Creates a user that cannot delete alerts from database: may only need the local account
mysql> grant CREATE, INSERT, SELECT, UPDATE on snort.* to acidviewer; So you can
connect locally with this account
```

mysql> grant CREATE, INSERT, SELECT, UPDATE on snort.* to acidviewer@localhost;

Configurar las contraseñas para los usuarios creados: *snort* y *acidviewer:*

```
mysql> connect mysql
mysql> set password for 'snort'@'localhost' = password('yourpassword');
mysql> set password for 'snort'@'%' = password('yourpassword');
mysql> set password for 'acidviewer'@'localhost' = password('yourpassword');
mysql> set password for 'acidviewer'@'%' = password('yourpassword');
mysql> flush privileges;
mysql> exit
```

Instalación de ACID

Descomprimir los progremas que son necesarios:

```
# tar -zxvf acid-0.9.*.tar.gz -C /var/www/html
# tar -zxvf adodb242.tgz -C /var/www/html # tar -zxvf gd-1.8.4.tar.gz -C /var/www/html
# tar -zxvf jpgraph-1.9.1.tar.gz
# cd jpgraph-1.9.1/src
# mkdir /var/www/html/jpgraph
# cp –R * /var/www/html/jpgraph
```

Configurar el archive de parámetros:

```
# cd /var/www/html/acid
# vi acid_conf.php
```

Modificar las variables de acuerdo a los datos de su sistema:

$DBlib_path="../adodb";
$alert_dbname="snort";
$alert_user="snort";
$alert_password="xxxx";
$ChartLib_path="../jpgraph";

Configure el acidviewer

cp –R /var/www/html/acid /var/www/html/acidviewer
cd /var/www/html/acidviewer
vi acid_conf.php

Cambiar el valor de las variables:

$alert_user="acidviewer";
$alert_password="xxxx";

Ambos contextos creados (/acid y /acidviewer) se deben configurar con los respectivos controles de ingreso, esto se puede controlar desde el Apache Web Server.

mkdir /usr/lib/apache/passwords
htpasswd -c /usr/lib/apache/passwords/passwords admin
htpasswd /usr/lib/apache/passwords/passwords acidviewer

Adicione las líneas necesarias para protección de los directorios en su respectivo archivo de configuracion del servidor Web:

<Directory "/var/www/html/acid">
AuthType Basic
AuthName "yourcompany"
AuthUserFile /usr/lib/apache/passwords/passwords
Require user admin

AllowOverride None
</Directory>
<Directory "/var/www/html/acidviewer">
AuthType Basic
AuthName "yourcompany"
AuthUserFile /usr/lib/apache/passwords/passwords
Require user acidviewer
AllowOverride None
</Directory>

Reiniciar el servicio:

service httpd restart

Instalación de la Consola Central Snort Center

Descomprimir el programa y configurar el archivo de parámetros.

mkdir /var/www/html/snortcenter
cp –R * /var/www/html/snortcenter
cd /var/www/html/snortcenter
vi config.php
$DB_password
$DBlib_path = "../adodb"
$DB_user = "root" $DB_password="XXXX"
$hidden_key_num = "XXXXXXX"
Now we need to create the SnortCenter database:
mysql –u root –p mysql> CREATE DATABASE snortcenter;
mysql> exit

Cree la base de datos que usara el Snort Center :

```
# mysql –u root –p
mysql> CREATE DATABASE snortcenter;
mysql> exit
```

Accediendo a la consola ACID

Ahora se puede acceder a los 2 contextos web creados utilizando un navegador:

http://servidor/acid/index.html
http://servidor/acidviewer/index.html

Cuando se carga por primera vez se observará una imagen como la mostrada en la figura inferior, se deberá realizar una configuración desde esta interfaz para completar su operación:

- Siga el enlace **Setup page**
- Continue con la opción **Create ACID AG**

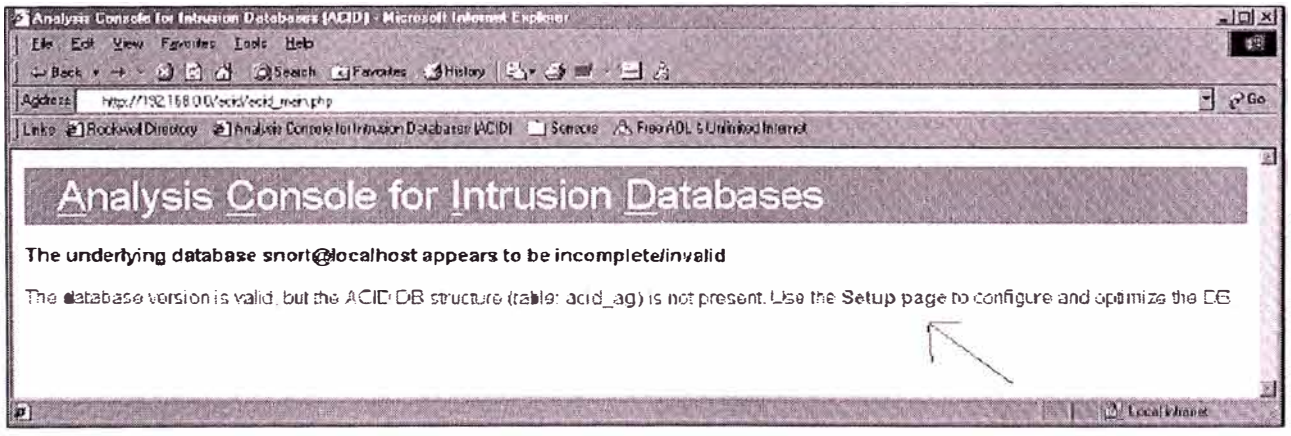

Fig A.1: Pagina inicial del modulo ACID

Accediendo a la consola del Snort Center :

Puede acceder al snort center vía:

http://server/snortcenter/

Los parámetros de acceso iniciales son
Usuario: admin.
Contraseña: change

Siga los siguientes pasos:

1.- Seleccione la opción ADMIN > Create DB Table
2.- Seleccione RULES > IMPORT/UPDATE RULES > UPDATE FROM INTERNET
3.- Seleccione ADMIN > ACTIVATE DEFAULT SNORT RULES
4.- Change el la contraseña de la cuenta ADMIN
5.- Cree un plugin de salida para los sensores, como se muestra en la figura y Seleccionando la opción de database.

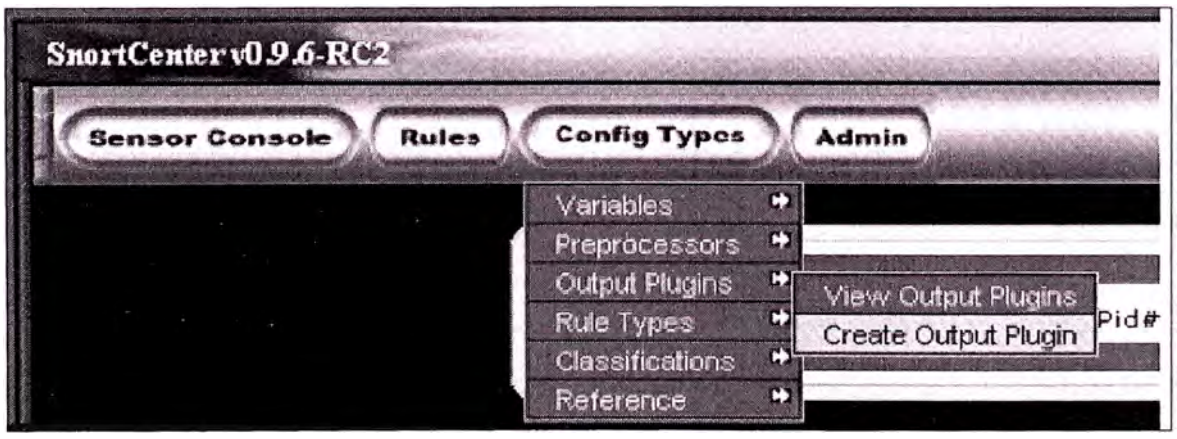

Fig A.2 Opciones de configuración del modulo Snort Center

Instalación de un sensor snort

Se debe instalar primero los componentes de la base de datos Mysql:

rpm –ivh MySQL-client-*.**.**-*.rpm
rpm –ivh MySQL-devel-*.**.**-*.rpm

Instale las fuentes de Snort

cp snort-last-version.*.tar.gz /usr/src/redhat/SOURCES
cd /usr/src/redhat/SOURCES
tar –zxvf snort-lasta-version.tar.gz
cd /usr/src/redhat/SOURCES/snort-lasta-version
./configure --with-mysql
make
make install

Crear el directorio de configuración y el directorio donde se almacenaran los eventos:

#mkdir /etc/snort
#mkdir /var/log/snort

Instalación del Agente Snort Center

Se deben instalar las dependencias para usar conexiones con Snort Center, para esto se usara el programa Net_SSL_eay

cp Net_SSLeayrpm-*-**.tar.gz /usr/src/redhat/SOURCES
cd /usr/src/redhat/SOURCES
tar –zxvf Net_SSLeay.rpm-*-**.tar.gz
cd Net_*
perl Makefile.PL

```
# make install
```

Inicio del agente de instalación:

```
# mkdir /opt/snortagent/
# cp snortcenter-agent-v0.1.6*.tar.gz /opt/snortagent
# cd /opt/snortagent
# tar -zxvf snortcenter-agent-v0.1.6*.tar.gz
# cd sensor
# ./setup.sh
```

ANEXO G

LISTA DE URLS PERMITAS CON TRÁFICO CIFRADO

TABLA Nº H.1. INSTITUCIONES DE CONFIANZA HABILITADOS PARA CONEXIONES SSL

Instituciones Bancarias y Financieras
zonasegura.bn.com.pe
www.continet.com.pe
bcpzonasegura.viabcp.com
www.netactiva24.com
wiesenet.sudameris.com.pe
zonasegura.financiero.com.pe
www.bifnet.com.pe
www.mibanco.com.pe
www.infocorp.com.pe
teletransfer.bcp.com.pe
www.citibank.com.pe
www.bbvacash.com
Instituciones Gubermentales
app.seace.gob.pe
enlinea.sunarp.gob.pe
www.sunat.gob.pe
Instituciones Educativas
mailhost.uni.edu.pe
infosil.sil.edu.pe
ocarina.ece.ucsb.edu

webaloe.ulima.edu.pe
www.pucp.edu.pe
Portales de Internet
www.digsigtrust.com
metalink.oracle.com
h20293.www2.hp.com
login.live.com
www.movistar.com.pe
servicioalcliente.integra.com.pe
www.paypal.com
www4.lanchile.cl
www.lenovo.com
profile.oracle.com
www.redhat.com
lists.sourceforge.net

GLOSARIO DE TERMINOS

- ACL: Listas de control de acceso (*Access Control List)* , mecanismo de control y filtrado de protocolos para equipos de comunicaciones.
- Ad-hoc : expresión para denotar algo que es adecuado para un determinado fin.
- Appliance :Equipo electrónico destinado a funciones especificas.
- Aplication tier : se refiere a una zona de clasificación dentro de una centro computo para los servicios de aplicaciones que la organización brinda a terceros.
- ARP: Adress Resolution Protocol, es el encargado de trasladar la direcciones IP en dirección Ethernet para ser usas en el rede de área local.
- ASCII Only Request Headers :
- ATM (Asynconous Transmision Mode): protocolo de alta velocidad par transmisión de voz datos , que utiliza el modo de transmisión asíncrona
- Back-End- Denominación que se le da a los elementos finales de conexión y de no directo acceso.
- Backbone: se refiere a las principales conexiones troncales de Internet o una red corporativa.
- bit ACK: (Acknowledgement): es parte del proceso de establecimiento de comunicación en redes de computadoras, y se le denomina también acuso de recibo.
- Black hole routing
- Bluetooth: es una norma que define un estándar global de comunicaciones inalámbricas, que permite la comunicación de voz y datos por enlaces de radiofrecuencia.
- Bootp (Bootstrap Protocol) : es un protocolo parta del estandar UDP, que se utiliza para obtener un direccion IP automáticamente.
- BPDU Bridge Data Packet Unit, paquete de saludo del protocolo spanning tree que se envia a intervalos configurables para intercambiar información entre los briges o switches de red.

- Broadcast : Es la transmisión simultanea de la misma data a todos los nodos conectados.
- BS-7799, estándar ingles para seguridad de administración de la seguridad de la información.
- Cache :es un conjunto de datos duplicados para permitir que se pueden consultar estas copias y no desde la fuente de origen.
- Cache_peer : es una parámetro de la configuración de un proxy para denotar otros servidores intermedios dentro de una jerarquía de almacenamiento de objetos que se consultan.
- CAM (Content Addessable Memory) : es una espacio de almacenamiento para switches de comunicación donde se guardan se registran las direcciones MAC y los puertos fisicos del ubicación de los mismos.
- Campus: palabra de origen latino que se refiere al conjunto de elementos dentro de un universidad.
- CheckPoint with Application Intelligence : Es una tecnología fabricante
- Cookies: es un fragmento de información que se almacena en el disco duro,
- Core: se refiere al conjunto principal de equipos de comunicación de una determinada infraestructura de comunicaciones.
- CDP (Cisco Discovery Protocol), protocolo que permite descubrir dispositivos de red.
- Confidencialidad: Entorno en el que los componentes o recursos son accedidos solo por el personal autorizado.
- Cross Site Scripting- Es un tipo de ataque de red que se basa el ocultamiento de cookies verdaderos y reemplazarlos por cookies falsos.
- Crackers: se le denomina asi a la persona que viola un sistema de seguridad informático para obtener beneficio personal o hacer daño a su objetivo.
- Data center : es el lugar donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización.
- Debug :nivel alto de obtención de registros de accesos o eventos en un sistema informático.
- DEC net : es el protocolo de comunicaciones desarrollado por DEC que consta de 5 capas, fisica, de control de enlace, de transporte y de servicios.
- Denial of service : son formas de ataques a sistemas informáticos mediante el cual se busca saturar algunos de los recursos de los sistemas , volviéndolos inaccesibles.

- DES Data Encryption Standard- sistema de cifrado de datos que utiliza un algoritmo con llave privada para su seguridad.
- Disponibilidad- Se refiere a que los recursos del sistema se encuentran accesibles a entes autorizados.
- DNS (Domain Name Resolution), servicio de nombres de dominio que traduce nos nombres de dominio en direcciones IP.
- DoS (Denial of Sevice) tipo de ataque informático que satura los sistemas imposibilitando su acceso.
- Echo Request: es parte del protocolo ICMP, y consiste en el envio de un mensaje para que el destino responsa con un mensaje denominado echo Reply.
- e-commerce : es la expresión para la comunicación de negocios comerciales y su dirección a través de métodos electrónicos como intercambio electrónico de datos y sistemas automáticos de recolección de datos.
- Enabled: Es una nivel de acceso privilegiado en equipos de comunicación Cisco.
- eTrust : Producto comercial de Computer Asociate , para el sistemas de protección contra intrusiones.
- extranet : son las redes de acceso externo para organizaciones asociadas que acceden a determinados servicios
- Finger : es un protocolo que proporciona informacion detallada de los usuarios de un sistema esten o no contectados en el momento de acceder al servicio.
- Fingerprint Scrambling: es una técnica de obtención de datos en base a ciertos parámetros que son enviados y analizados en un lado de la comunicación.
- Firewall- denominación para el sistema de protección y filtro de paquetes.
- Firewall-1 with VPN1 : es el producto de seguridad desarrollado por la empresa Check Point
- FR Frame Relay protocolo de transmisión de datos, para redes extensas.
- Frond End- Denominación que se le da a los elementos directamente ubicados al origen de la conexión.
- FTP (File Transfer Protocol), protocolo de transferencia de archivos.
- full connect: expresión para indicar conexión completa entre 2 dispositivos.
- gateway : expresión que se refiere a una puerta de enlace que sirve para conectarse con otra red de comunicaciones.

- Hacking : se refire a la intrusión de un sistema informatico con fines no destructivos ni de beneficios personales.
- Hardening: proceso por el cual se optimizar la seguridad de un determinado sistema operativo.
- HIDS Host Intrusion Detection System, sistema de detección de intrusiones local, ubicado en el mismo sistema que se protege.
- Host: denominación que se le da a una sistema que participa en una red del computadoras ya se solicitando servicio o brindandolos.
- HTTP HyperText Transfer Protocol: protocolo utilizado para acceder y visualizar el contenido de la World Wide Web
- HTTP Protocol Inspection HTTP Format Sizes
- ICMP : (Internet control messages) protocolo de control de mensajes de Internet Se utiliza como mecanismo de diagnostico de comunicación para redes de datos.
- IDS (Intrusion Detection System), sistemas de protección que detecta ataques informáticos en base a firmas o patrones que pose y compara.
- Integridad- se refiere a cuando los recursos solo son modificados por personal autorizados.
- IKE Security Associations: es el protocolo para el intercambio de credenciales simétricas para el establecimiento de comunicaciones seguras sobre redes IP. Esta formado por dos fases , la primera autentica la comunicación , y la segunda intercambio propuestas de asociación de seguridad.
- IP : Internet Protocol, es el protocolo estándar para las comunicaciones en Internet.
- IP directeted broadcast : es un datagrama el cual es enviado a una dirección de broadcast de una sub red en la cual no se encuentra ubicado el remitente. Este mecanismos es utilizado en algunas formas de ataques a redes de comunicación.
- IP fragments-Es una técnica de ataque que fragmenta la sección de la información o data de un paquete.
- IP ID- Es una técnica para determinar sistemas operativos remotos.
- IP redirect : es la propiedad de poder redirigir protocolos ICMP, sin embargo esta cualidad es tambien utilizada en formas de ataques de redes de comunicaciones.
- IPSec Internet Protocol Security, es el protocolo para transmisión de datos de forma segura a nivel de la capa IP.

- IP spoofing : es una forma de ataque a redes de comunicaciones que consiste en la suplantación de la dirección IP de origen.
- ip tcp synwait-time : es el mecanismo de protección en routers cisco para prevenir atraques del tipo flood, que permite configurar un tiempo limite de espera para una conexión abierta.
- ISO (Internacional Standard Organization) organización que desarrolla normas internacionales industriales y comerciales.
- ISO 27001: es un estándar para la seguridad de la información aprobado y publicado como estándar internacional en Octubre del 2005 por las ISO (Internacional Organization for Standardization). El mismos especifica los requisitos necesarios para establecer implementar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información.
- ISP Internet Services Provider, compañía que provee accesos a servios de Internet, a través de equipos de comunicación.
- IVR (Interactive Voice Response): consiste en un sistema telefónico que es capaz de recibir llamadas e interactuar con el humano a través de grabaciones de voz.
- Kerberos : es un protocolo de autenticación para redes de comunicación y garanticen su identidad mutuamente de manera segura.
- LAN Local Area Network, es un conjunto de elementos interconectados, localizados próximamente.
- LAND-Es un tipo ataque contra redes con sistema operativo Windows, que suplanta la dirección origen por la dirección destino provocando una saturación y colapso del sistema.
- Local interface spoofing : es una técnica de ataque similar a ataques tipo LAND.
- MOP (Maintenance Operations Protocol): se utiliza para proporcionar al router información de configuración cuando se comunica con redes DECNet. MOP es vulnerable a distintos tipos de ataques.
- Man-of Middle: es una forma de ataques de red a nivel de capa de red , que permite capurar trafico que no pertenece a un determinado destino.
- Mail SMTP Content- Es el sistema de filtro de contenido para correo electrónico que puede evitar diversas formas de infección de virus o a ataques.
- Max ping size: es la opción dentro del protocolo ICMP, controlar el máximo tamaño de la respuesta.

- Message Queuing : es un servicio de administración de mensajes y encolamiento que permite que las aplicaciones se ejecuten en diferentes tiempos para comunicarse con redes heterogeneas y sistemas que podrían estar no activos.
- Módem : es el acrónimo de (modulador/demodulador) este actúa como un equipo terminal del circuito de datos, permitiendo la transmisión de un flujo de datos digitales a través de una señal analógica.
- MD5 Message Digest 5 , Algoritmo de reducción criptográfico
- NTP : Network Time Protocol, es una protocolo estándar para la sincronización del tiempo en distintos dispositivos de red.
- NULL : es un componente de la estructura del protocolo TCP/IP por el cual un atacante envia tramas con los bits TCP reseteados , con la intención de explorar si un determinados servicio esta abierto o no.
- OSSTMM (Open Source Security Testing Methodology Manual): es una metodologia por el cual se rigen las pruebas y evaluaciones de vulnerabilidades de un determinado sistema.
- Packet sanity- Se le denomina así al proceso de verificación de los componentes de los paquetes TCP/IP, se verifica cabeceras, banderas, entre otros.
- P2P : Pee-to-Peer , son las redes de intercambio de datos que utlizan la arquitectura de cliente servidor para su comunicación , sino la de cliente – cliente basándose en la filosofía de que todos los usuarios deben compartir en un sistema meritocratico , donde el que mas comparta mas privilegios tiene.,
- PAD(Packet Assembler/desemblador):
- Parameter Problem
- PBX(Private Branch eXchange) : es una central telefónica que se utiliza para negocios privados.
- Port scanning- Es el proceso de búsqueda sistemáticas de puertos y/servicios en una red de computadoras.
- Port Security- puerto de un equipo de comunicaciones como un switch, que posee características de seguridad al equipo que se encuentre conectado.
- PSTN- Publicwitched Telephone Network, es el sistema de telefonía basados en cables de cobre que porta señales analógicas.
- QoS (Quality of Service): es la expresión que de nota la garantía que se transmitirá cierta cantidad de datos en un tiempo dado.

- RAS Remote Access Services, servicio de acceso a distancia, que permite a los usuarios a acceder a un sistema a través de un modem o una conexión con la red.
- RC4 : es una sistema de cifradote datos utilizado ampliamente en Internet para protocolos como el TLS/SSL y WEP, RC4 genera un flujo pseudo aleatorio de bit que se combina con un texto plano usando la función lógica XOR.
- recovery password: procedimiento por el cual se puede acceder a la configuración del sistema si es que no se tienen las credenciales. Este procedimiento se realizar desde un acceso físico al dispositivo.
- rlogin: es una utilidad de software en sistemas Unix que permite conectarse a otros host via la red con un sistema de autenticación básico.
- Secure Platform- Es un Sistema Operativo adaptado de los Sistemas Linux que provee la empresa CheckPoint, para instalar sobre ella el producto Fiewall-1
- Scan : proceso por el cual se intenta determinar
- scheduler interval
- Secure Client: Software propietarario de Chekpoint, para realizar conexiones VPN
- Secure Platform: sistema operativo propietario basado en Linux , para la plataforma de seguridad de Check Point .
- Server Side Include
- SIP-Session Initiation Protocol, es un protocolo de Voz por IP que se transporta sobre protocolo UDP.
- SMTP(Simple Mail Transport Protocol) :protocolo de comunicación para la transferencia de correo electrónico.
- Smurfing, Es un técnica de ataques a redes TCP/IP que falsifica las direcciones del origen para provocar denegación de servicios.
- Sniffing, técnica de captura de información digital
- source routing: es el mecanismo que se implementa, para que durante el envió de un datagrama IP, este pueda controlar la ruta de envió. Este proceso es usado par formas de ataques de red.
- Spanning Tree, protocolo de comunicación de switches para el control de bucles y el manejo de redundancia de comunicación.
- Spoofing, es la técnica para la suplantación de la dirección del remitente para intentar la entrada ilegal a un sistema.

- Spywares Es una programa que utiliza la conexión a Internet de un usuario para obtener y enviar información sin autorización del mismo.
- SQL (Structured Quero Language): es una lenguaje de acceso a base de datos relacionales que permite especificar diversos tipos de operaciones sobre la mismas.
- SSH Secure Session Shell, es el protocolo que permite conectarse a otro equipo sobre una red, de manera cifrada, es el reemplazo de protocolos como rlogin, telnet, rcp entre otros.
- SSL Secure Socket Layer, protocolo de nivel de aplicación, para el intercambio de datos en la World Wide Web, de manera segura este protocolo es usado por los certificados y firmas digitales.
- SYN : es un bit de control dentro del segmento TCP , que se utilizar para sincronizar los números de secuencia iniciales de una conexión en el procedimiento establecido de tres fases (3 way hanshake)
- SYN attack – Es la forma de ataque vía el campo SYN del protocolo TCP, que envía rápidamente solicitudes y que no pueden ser respondidos con las misma velocidad.
- TACACS Terminal Access Controller Access-Control System, es el sistema de control de acceso centralizado, para equipos de comunicaciones
- Teardrop- Es una forma de ataque de la forma Denial of Service, que confunde la forma en que los routers manejan paquetes demasiado largos.
- TTL Transmision Transitor Logic, es el campo en la cabecera del paquete IP, el cual indica cuando debe durar este paquete antes de que sea descartado
- Timeout: expresión que denota la carencia o vencimiento de un tiempo dado.
- Traceroute: es una herramienta de diagnostico de redes que permite seguir las rutas de los paquetes que van desde un origen a destino.
- TTL: (Time To Live) : es un concepto utilizado en redes de comunicación para indicar por cuantos nodos puede pasar un paquete antes de ser descartado o devuelto.
- URL Uniform Resource Locator ,es una cadena de caracteres que define la ubicación de un archive o programa en el Internet
- VLAN Vitual Local Area Network, grupo de dispositivos de una red local que están configurados para se puede comunicar solo entre ellos, aislando del resto de manera lógica.

- UPS (Uninterrumped Power System) son sistemas de acumulación de energía, que permiten la continuidad de las operaciones en caso de falta de suministro eléctrico convencional.
- VLAN (Virtual Lan Area Network) : es una tecnología que permite crear redes de computadora logicamente independientes.
- VPN (Virtual Private Network) es el método de conexión que permite crear enlaces de comunicación privadas sobre redes públicas de datos.
- WAN Wide Area Network, son las conexiones distantes de redes de computadoras,
- Web General HTTP Word Catcher- Son los tipos de ataque que se producen contra servicios web, estos son provocados por los virus como: CodeRed,Nimbda entre otros.
- X.25 : red de conmutación de paquetes basada en protocolo HDLC , que establece mecanismos de direccionamiento entre usuarios negociación de características de comunicación, técnicas de recuperación de errores.
- XMAS: es parte del protocolo TCP/IP, y mediante el cual un atacante envía tramas con todos los bits TCP activos, con la intención de determinar servicios activos.
- Zero subset

BIBILIOGRAFIA

1. Internet Data Center
   http://www.microsoft.com/spain/technet/guias/internet_datacenter.mspx

2. Keith E Strassberg, Richard J Gondek, Gary Rollie “Firewall”
   MacGrawHill 2003

3. “Firewall and Smart Defense”
   http://www.checkpoint.com/support/technical/documents/docs_r60.html

4. Security Architecture for Enterprise
   http://www.cisco.com/safe

5. Harold F. Tipton "Information Security Management Handbooks"
   CRC Press LLC 2003

6. OSSTMM 2.1 Manual de Metodología Abierta de Testeo de Seguridad
   http://www.isecom.org/osstmm

7. Esquema 1 de la Norma IRAM-ISO IEC 17799
   http://www.iram.com.ar

8. “Seguridad en Unix y Redes”, Antonio Villalón Huerta, en
   http://www.rediris.es/cert/doc/unixsec/

9. Router Security Configuration Guide, National Security Agency,
   http://www.nsa.gov