ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN

Tópico
SEGURIDAD DE INFORMACIÓN

"Desarrollo de un sitio seguro de E-Commerce dedicado a la venta de arreglos florales y regalos especiales para cualquier ocasión"

Previa a la obtención del Título de Ingeniero en Computación especialización Sistemas Tecnológicos

Presentado por:

Steve Aguirre Wong
Julio Pintag Sanga
Walter Ramírez Bocca

GUAYAQUIL-ECUADOR
2005

AGRADECIMIENTO

Agradecemos a nuestros Padres, Hermanos y Familiares por su constante ayuda, apoyo y orientación durante nuestra carrera universitaria.

Adicionalmente a nuestros Maestros de la ESPOL en las diferentes materias, quienes colaboraron significativamente en nuestro desarrollo académico.

DEDICATORIA

Con mucho cariño a nuestros Padres.

TRIBUNAL DE GRADO

PRESIDENTE

Ing. Miguel Yapur Auad

DIRECTOR DE TÓPICO

Ing. Karina Astudillo Barahona

MIEMBROS PRINCIPALES

Ing. Otilia Alejandro Molina

Ing. Fabricio Echeverría Briones

DECLARACIÓN EXPRESA

"La responsabilidad por los hechos, ideas y doctrinas expuestos en esta tesis, nos corresponden exclusivamente y, el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

(Reglamento de Exámenes y Títulos profesionales de la ESPOL)

Steve Aguirre Wong

Julio Pintag Sanga

Walter Ramírez Bocca

RESUMEN

Seguridad de Información: es un tema que se ha puesto en auge debido al desarrollo que ha alcanzado el nivel de transaccionalidad y comercio a través de Internet; consecuentemente es de vital importancia implementar mecanismos de seguridad que estén en capacidad de prevenir, controlar, detectar y monitorear acciones no autorizadas sobre sitios web.

El incremento de los denominados "*hackers"* (intrusos informáticos) y sus acciones han demostrado que existen demasiadas vulnerabilidades tecnológicas a nivel mundial que comprometen a los especialistas a investigar y ofrecer a las organizaciones, esquemas de seguridad en las redes corporativas que les permita ofrecer servicios y procesar de manera segura la información de sus clientes.

Para demostrar la aplicabilidad de herramientas de seguridad y esquemas seguros de redes se ha desarrollado un sitio web de e-commerce denominado **"Contodomiamor.com"** que ofrece el servicio de venta de arreglos florales y obsequios complementarios. En este sitio web los clientes mediante su tarjeta de crédito podrán realizar compras, procesando la transacción de manera confiable y segura.

Para la construcción del sitio seguro se han tomado en consideración los principios elementales de seguridad de información que son: la confidencialidad de datos, la autenticación de clientes, la integridad de los datos y la disponibilidad de servicios en la web las 24 horas del día.

ÍNDICE GENERAL

ÍNDICE DE GRÁFICOS

CAPÍTULO 1

Introducción a la Seguridad de Información

1.1. Antecedentes

Si se analiza cómo se ha venido desarrollando la tecnología desde la década de los 90 hasta la actualidad, se identifica una automatización de servicios e incremento de transacciones a través de Internet. Estas transacciones electrónicas deben prestar las mismas e inclusive mayores medidas de seguridad que las realizadas en el comercio tradicional.

Según reporte de *"CERT Coordination Center"* (CERT/CC[1]); los incidentes de seguridad han ido incrementando gradualmente cada año; tal es así que en 1988 sólo se registraron seis incidentes en todo el año, en 1994 se reportó 2.241 incidentes de seguridad de computadoras; 40.241 sitios afectados por esos incidentes, 22.650 de esos ataques fueron contra servidores de *"sendmail"* (servidor de correo), donde todas las computadoras dentro de un específico rango de direcciones IP fueron probados con un *"exploit"*[2], de una vieja vulnerabilidad de sendmail. En el 2003 se reportaron 3.784 vulnerabilidades y 137.529 incidentes de seguridad. (http://www.cert.org/annual_rpts/index.html)

[1] Organización dedicada a recibir y publicar informes de ataques de seguridad
[2] Método para aprovechar la vulnerabilidad de un sistema.

Los intentos de sabotaje contra servidores y sitios web aumentaron en 36% en el 2004, en que los ataques notificados llegaron a 400.000. La información fue presentada en un nuevo informe de Zone-H, organización integrada por una red global de voluntarios dedicada a reunir estadísticas sobre ataques contra servidores y sabotajes de sitios web.

Según Zone-H, gran parte de los ataques tuvo motivaciones políticas, y especialmente en momentos de interés general como el aniversario de la invasión de Irak, se registró un fuerte incremento en los ataques recíprocos entre sitios pro islámicos y pro estadounidenses.

Las estadísticas indican que en 2004 se registraron 49 ataques individuales contra sistemas informáticos propiedad de las Fuerzas Armadas estadounidenses. Más de la mitad de los 400.000 ataques registrados fueron exitosos. En tales casos, los intrusos recurrieron a conocidos agujeros de seguridad en el software y a deficientes rutinas de seguridad por parte de los administradores de sistemas. Los ataques fueron perpetrados indistintamente por vándalos informáticos como por delincuentes organizados, comenta Zone-H en un informe. (http://www.cyberpirata.org/article3650.html)

Como se puede apreciar en las estadísticas dadas, la mayor parte de ataques de seguridad se presentan debido a vulnerabilidades ya conocidas y

que no son debidamente controladas por una buena administración de las seguridades.

1.2 Objetivos

En base a los antecedentes señalados y considerando que el comercio electrónico recién se está desarrollando en el Ecuador, se ha identificado la necesidad de implementar sistemas seguros y confiables que aseguren la integridad, confidencialidad y disponibilidad de las transacciones vía web.

En virtud de lo mencionado, se han definido los siguientes objetivos que serán desarrollados en este proyecto de graduación:

- Diseñar un esquema de red seguro que permita prevenir, resolver y manejar un ataque al sitio web, convirtiéndolo en un sitio confiable y seguro de comercio electrónico.

- Utilizar las herramientas tecnológicas actuales y de punta con respecto a seguridad de información en el esquema sugerido a desarrollar, con lo cual se presta un aporte para fomentar la cultura de seguridad en nuestro País.

- Implementar un servicio de venta de arreglos florales y regalos de ocasión a través de una página web, con forma de pago electrónica mediante tarjeta de crédito.

- Aportar mediante este proyecto a que los profesionales tecnológicos cambien las mentalidades de los empresarios en cuanto a la seguridad de información; y demostrar que un sitio seguro es realmente una inversión que protege y evita pérdidas económicas en sus negocios al comprometer su información ante potenciales ataques.

1.3 Premisas

En el diseño y elaboración del proyecto de graduación se partió de las siguientes premisas:

1. El hecho de desarrollar un sitio web que tenga conexión con el mundo externo a través de Internet abre la posibilidad de que existan riesgos a una infinidad de ataques elaborados por usuarios maliciosos, tanto externos como internos de la organización.

2. Las herramientas actuales del mercado tanto a nivel de hardware como de software, por ejemplo los denominados *"Firewalls"*, constituyen una gran arma de apoyo contra los ataques informáticos.

3. Una buena estrategia en la configuración de la red, reduce las posibilidades de ataque, implementando medidas para la protección de la misma.

Se buscará desarrollar un esquema de seguridad para enfocar las premisas anteriormente citadas.

1.4 Metodología

En esta sección se explicará la estrategia a utilizar para la elaboración de este proyecto:

1. Se realizará un análisis del mercado para determinar el tipo de negocio que se aplicará en el sitio web.
    a. Lluvia de ideas de negocios.
    b. Escoger el servicio que se va a ofrecer.
    c. Determinar la competencia y accesibilidad en ese mercado.
    d. Cómo y dónde se puede ofrecer el servicio
    e. A quién va dirigido este servicio

2. Se realizará un levantamiento de información de las herramientas de seguridad del mercado a través de:
    a. Investigación en Internet

b. Revisiones prácticas en empresas donde las herramientas han sido aplicadas.

3. Se realizará el análisis y diseño de la red, utilizando las herramientas investigadas y el conocimiento adquirido en el tópico.

4. Se desarrollará la aplicación sobre una base de datos robusta.

5. Se aprovechará la información disponible y bondades del código abierto (open - source) que ofrece el sistema operativo Linux.

La metodología a aplicar buscará implementar un alto nivel de seguridad, minimizando costos sin perder la efectividad en la protección contra intrusos.

1.5 Conceptos y procedimientos utilizados

1.5.1 Conceptos generales de redes e Internet

1.5.1.1 Acerca de Redes.

"El viejo modelo de una sola computadora que atendía todas las necesidades de computación de la organización ha sido reemplazado por uno en el cual un gran número de computadoras separadas pero interconectadas hacen el trabajo. Estos sistemas se llaman redes de computadoras." (Tanenbaum, 1997,2).

Tanenbaum (1997) destaca que los usos principales de las redes, tanto en las compañías como en las personas, son los siguientes:

- Distribución de recursos: permitir que servicios informáticos como programas, equipos y datos puedan estar disponibles a cualquier usuario de la red.
- Alcanzar alta confiabilidad: mediante la implementación de esquemas de replicación de archivos entre servidores remotos, se pueden mantener copias e información actualizada asegurando el procesamiento contínuo en negocios críticos.
- Comunicación: hace posible que dos o más personas físicamente distantes puedan trabajar colaborativamente en tiempo real.
- Acceso a información remota.
- Entretenimiento interactivo.

Según criterio de los autores, los usos más importantes son la distribución de recursos e integración de datos.

1.5.1.2 Tipos de Redes.

Las redes se clasifican por su escala, es decir de acuerdo a su tamaño físico. Principalmente se tienen dos grupos (Cisco Systems 2000):

- Redes de Área Local o LAN (Local Area Network)
- Redes de Área Amplia o WAN (Wide Area Network)

Redes de Área Local – LAN: son redes de propiedad privada dentro de un solo edificio o campus hasta aproximadamente un kilómetro de extensión. Se utilizan ampliamente para conectar computadoras personales y estaciones de trabajo en oficinas y fábricas para compartir recursos e intercambiar información. (Tanenbaum, 1997; Cisco Systems, 2000)

Según Cisco Systems (2000), las redes LAN se diseñan para lograr los siguientes objetivos:

- Permitir acceso múltiple a medios físicos que proporcionan altos anchos de banda.
- Controlar la red desde una administración local.
- Proveer conectividad permanente a servicios locales.
- Conectar físicamente dispositivos adyacentes.

Redes de Área Amplia – WAN: son redes que se extienden sobre un área geográfica extensa, en algunos casos un país o un continente. A medida que el uso de las computadoras en los negocios creció, fue evidente que las redes LAN no eran suficientes. La solución se basó en la interconexión de múltiples redes LAN y proveer accesos a computadoras o servidores en otras ubicaciones, originando las redes WAN (Cisco Systems, 2000).

En base a lo establecido por Cisco Systems (2000), las redes WAN se diseñan para lograr los siguientes objetivos:

- Permitir el acceso sobre interfaces seriales que operan a bajas velocidades.
- Proveer conectividad en forma permanente y parcial.
- Conectar dispositivos separados por grandes distancias, en algunos casos globales (hasta varios miles de kilómetros).

A través de las redes LAN y WAN, se busca comunicar los diferentes recursos dependiendo de la distancia geográfica.

1.5.1.3 El Modelo Referencial ISO/OSI

El modelo OSI "*Open Systems Interconnection*"[3] es un estándar referenciado por la Organización de Estándares Internacionales - ISO (de sus siglas en inglés *"International Standards Organization"*). El modelo referencial OSI se ocupa de la conexión de sistemas abiertos, es decir, sistemas que están abiertos a la comunicación con otros sistemas. (Tanenbaum, 1997).

El modelo OSI está compuesto por siete capas: la capa física, la capa de enlace de datos, la capa de red, la capa de transporte, la capa de sesión, la capa de presentación y en el nivel más alto, la de aplicación. Los principios

[3] Open Systems Interconnection: Interconexión de Sistemas Abiertos

que se aplicaron para llegar a las siete capas son los siguientes (Tanenbaum, 1997; Cisco Systems, 2000):

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

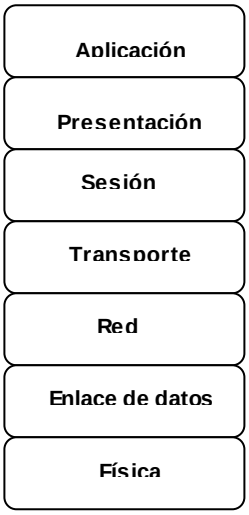

Figura1.1. Modelo de referencia OSI
Fuente: ISO

Los dispositivos de red desarrollados actualmente, se basan en el modelo de referencia OSI.

1.5.1.4 Acerca de Internet

Una definición bastante práctica y sencilla para describir Internet es la que se obtuvo en el Diccionario Enciclopédico Océano Uno (1997, 874): “Es una red descentralizada de computadoras distribuidas por el mundo, que ofrece múltiples maneras de acceder a una ingente cantidad de información, obtenida gracias a la interconexión de las computadoras de universidades, organismos gubernamentales y bases de datos de empresas especializadas. Ofrece también a sus usuarios servicios tales como: correo electrónico o grupos de debate”.

El Internet ha logrado unir fronteras, culturas y opiniones. Ha aportado significativamente a la investigación y al desarrollo cientifico.

1.5.1.5 TCP/IP: El lenguaje de Internet

TCP/IP (Transfer Control Protocol / Internet Protocol) es el lenguaje de Internet. Cisco Systems (2000) establece que en base a la arquitectura TCP/IP se hizo posible la comunicación de datos entre dos computadoras, en cualquier lugar del mundo, a la velocidad de la luz aproximadamente.

Mal llamado protocolo ya que realmente es una arquitectura basada en cuatro protocolos: el protocolo de acceso a la red, el protocolo IP, el protocolo TCP y el protocolo de aplicación (Cisco Systems, 2000).

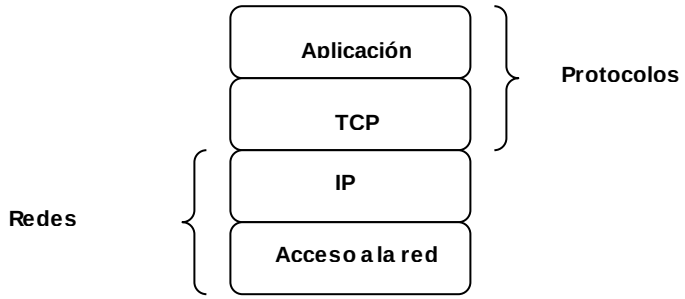

Figura 1.2. Arquitectura TCP/IP
Fuente: Cisco Systems

Todo computador que desea participar en Internet debe interpretar y utilizar este lenguaje para poder comunicarse.

1.5.1.5.1 Protocolo IP (Internet Protocol)

Según Tanenbaum (1997) la misión de este protocolo es permitir que los nodos o equipos ingresen paquetes en cualquier red y los hagan viajar de forma independiente a su destino (probablemente el destino sea una red diferente). Los paquetes inclusive pueden llegar en un orden diferente al que fueron enviados, en cuyo caso corresponde a los protocolos superiores reordenarlos.

IP es un protocolo que se ubica en la capa de red del modelo de referencia OSI, y se basa en direcciones lógicas proporcionadas por el administrador de red (Cisco Systems, 2000).

La funcionalidad de este protocolo es poder identificar lógicamente los paquetes, proporcionando información necesaria para que puedan ser transmitidos.

1.5.1.5.2. TCP (Transport Cotrol Protocol).

TCP es un protocolo que se encuentra en la capa de transporte del modelo OSI. La característica más importante de este protocolo es que está orientado a conexión; esto quiere decir que la entrega de paquetes es garantizada; además de ofrecer servicios de control de flujo, calidad de servicio y control de errores. (Cisco Systems, 2000).

Dado que TCP este un protocolo orientado conexión asegura la integridad de los datos, evitando la duplicidad y pérdida de información.

1.5.1.5.3 UDP (User Datagram Protocol)

UDP es un protocolo ubicado también en la capa de transporte del modelo OSI; se diferencia de TCP debido a que no es orientado a conexión; es decir no ofrece la seguridad que los paquetes sean entregados a su destino. Una de las características que lo hace interesante es su simplicidad; como no necesita tener una pista de la secuencia de los paquetes, las cabeceras del

paquete tienen un menor tamaño y por ende la entrega se hace con mayor rapidez. (Tanenbaum, 1997)

Debido a las características de UDP, éste es usado en aplicaciones donde es más importante la rapidez del flujo de información antes que la integridad de los datos.

1.5.2 Ataques de Seguridad

La diversidad de redes de hoy, exponen sus sistemas a una amplia variedad de posibles incidentes relacionados con la seguridad. Para lograr proteger sus sistemas se deben conocer los tipos de explotaciones o aprovechamientos que son típicamente realizados para romper un sistema computacional.

1.5.2.1 Métodos de exploración

1.5.2.1.1 Introducción

En esta sección se tratarán las técnicas y herramientas con las cuales un *"hacker"* puede determinar qué sistemas se encuentran activos y son accesibles.

Para que se pueda llevar a cabo un ataque de seguridad, es necesario dar con las debilidades del sistema por lo que el primer paso que el atacante

realiza es la exploración o búsqueda de información del sistema, para luego proceder con su objetivo final que es el ataque en sí del sistema.

Los métodos de exploración se dividen en barridos de ping, icmp[4], exploración de puertos y detección de sistemas operativos. (Scambray-McClure-Kurtz, 2001)

Se analizará cada uno de los cuatro métodos de exploración mencionados, con el fin de conocer y estar prevenidos ante estos tipos de ataques.

1.5.2.1.2 Ping de Red

El primer paso para determinar si un sistema se encuentra activo es llevar a cabo un barrido ping.

Como Scambray, McClure y Kurtz, (2001,34) señalaban "ping se utiliza tradicionalmente para enviar paquetes *ICMP ECHO tipo 8* a un sistema destino en un intento por obtener un *ICMP ECHO_REPLY tipo 0* que indique que el sistema destino está activo" nos muestra claramente que este método de exploración es básico para indicarnos el número de sistemas activos.

Existen en el mercado una gran cantidad de herramientas disponibles bajo los sistemas operativos Windosws y Unix que permiten utilizar la técnica de

[4] Protocolo usado para obtener información del estado de la red

barrido ping entre las cuales podemos destacar gping, fping y el producto denominado Pinger para Windows.

Si se habla del tema de seguridad a nivel general, lo primero que se puede venir a la mente es el tema de la vigilancia, ya sea esta a través de alarmas, o personal que vigile constantemente la zona asignada; de esta misma manera al hablar de seguridad informática un elemento que no puede faltar son los sistemas detectores de intrusos, denominados IDS por sus siglas en inglés (Intrussion Detection System).

Estos IDS dan la detección de una actividad inusual de ping sobre la red a tal punto que se puede obtener inclusive de qué direcciones fuentes provienen estos requerimientos para tomar acciones respectivas.

A nivel de prevención se puede implementar en el *"firewall"* (cortafuegos) que sólo ciertas direcciones IP tengan acceso al tráfico ICMP, como por ejemplo para comprobación interna de la actividad de la red.

1.5.2.1.3 Consultas ICMP

Existen herramientas que pueden entregar información valiosa de la red con sólo enviar un paquete ICMP.

En el sistema operativo Unix, la herramienta icmpquery puede entregar la hora del sistema, la máscara de red de un dispositivo con lo cual se puede obtener las subredes utilizadas.

A nivel de prevención se puede implementar en el *"firewall"* que sólo ciertas direcciones ip tengan acceso al tráfico ICMP, como por ejemplo para comprobación interna de la actividad de la red, además se puede restringir la entrada a la red de solicitudes de consultas ICMP de tipo 13 y 17 que permiten obtener la información de fecha y hora del sistema y máscaras de red respectivamente.

1.5.2.1.4 Exploración de puertos

Scambray, McClure y Kurtz, (2001,34) definen a la exploración de puertos como "el proceso de conexión a puertos UDP y TCP del sistema destino que constituye el objetivo para determinar qué servicios se están ejecutando o están en un estado *"LISTENING"* (de escucha).

El atacante en el momento que realiza una exploración de puertos puede identificar el tipo de sistema operativo y las versiones o aplicaciones específicas de un determinado servicio.

1.5.2.1.5 Tipos de Exploración de Puertos

Una conexión TCP necesita un acuerdo de 3 vías que son: el envío de un paquete SYN que es enviado por el cliente, la recepción del paquete SYN/ACK enviado por el servidor y finalmente el envío de un paquete ACK por parte del cliente.

Según Fyodor quien es uno de los pioneros en el desarrollo de técnicas de exploración de puertos estas se dividen en:

Exploración de conexión TCP: Ejecuta la conexión TCP completa, es decir cubre las 3 vías mencionadas anteriormente.

Exploración TCP SYN: es una exploración semiabierta, ya que se envía el paquete SYN, si se recibe el SYN/ACK se concluye que el servidor está escuchando, si se recibe un RST/ACK significa que no está escuchando, en cualquiera de las dos respuestas el sistema fuente enviará un RST/ACK para que no se establezca una conexión TCP completa y el sistema destino no detecte la exploración.

Exploración TCP FIN: Esta técnica envía un paquete FIN al puerto objetivo. El sistema objetivo debe devolver un RST para todos los puertos cerrados.

Exploración árbol de navidad TCP: Esta técnica envía paquetes FIN, URG y PUSH al puerto objetivo, y devuelve RST para todos los puertos cerrados.

Exploración nula TCP: Esta técnica apaga todas las banderas con lo cual el sistema objetivo devuelve RST para todos los puertos cerrados.

Exploración TCP ACK: Esta técnica se utiliza para proyectar los conjuntos de reglas de cortafuegos. Puede ayudar a determinar si el cortafuego es un simple filtro de paquetes que sólo permitirá las conexiones predefinidas o se trata de un firewall completo que realiza un filtrado de paquetes avanzado.

Exploración de ventanas TCP: Esta técnica puede detectar puertos abiertos así como puertos filtrados y no filtrados de algunos sistemas debido a una anomalía en la forma que se informa sobre el tamaño de las ventanas TCP.

Exploración TCP RPC: Se utiliza para detectar e identificar puertos de llamada de procedimiento remoto (RPC) y su número de versión y programas asociados.

Exploración UDP: Esta técnica envía un paquete UDP al puerto objetivo. Si el puerto responde con un mensaje similar a “puerto icmp no alcanzable”, el puerto está cerrado caso contrario el puerto está abierto.

Todas éstas técnicas de exploración tienen la finalidad de identificar los puertos y aplicaciones que se están ejecutando en el objetivo del ataque, básicamente es una recopilación de información que ayude identificar falencias y determinar el método de ataque a utilizar.

1.5.2.1.6 Herramientas exploradoras:

Se va a mencionar en esta sección algunas de las herramientas de exploración de puertos tanto para el entorno Unix como Windows.

Strobe: Funciona sobre unix e identifica el sistema operativo y el servicio que se está ejecutando, proporciona una lista de todos los puertos que están a la escucha.

Es sólo analizador TCP, no tiene la capacidad de realizar exploraciones UDP.

Udp_Scan: Realiza exploraciones UDP, pero su envío de mensajes en la exploración lo convierte en una herramienta fácilmente identificable en la detección de intrusos.

Netcat: Proporciona exploración UDP y TCP, en su ejecución da información muy bien detallada de cada puerto explorado.

Ahora entre las herramientas exploradoras sobre Windows se destacan: NetScanTools Pro 2000, SuperScan, NTOScanner y WinScan.

Detección y prevención: Detectar una actividad de exploración de puertos ayuda a advertir cuando se producirá un ataque y quien lo realizará.
Las principales acciones de detección de exploración de puertos son programas IDS basados en red. (Scambray, McClure y Kurtz, 2001)

Existen algunas herramientas dentro de Unix y Windows que permiten detectar la actividad de exploración de puertos.

La mejor prevención es desactivar todos los puertos innecesarios dentro de la funcionalidad que se requiera dar en el sistema, de esta manera se minimiza la exploración de los mismos, y se puede efectuar un control más efectivo a nivel de los puertos habilitados.

1.5.2.1.7 Detección de sistemas operativos

El siguiente objetivo dentro de un ataque de seguridad es obtener el tipo de sistema operativo en el que reside el sistema destino.

Hay formas básicas de obtener información del tipo de sistema operativo a través de la captura de comentarios de información que dan algunas herramientas como el ftp, telnet, pop, etc.

Ahora se analizará dos técnicas realmente potentes para detección de sistemas operativos según Scambray, McClure y Kurtz, (2001,65) que son el rastreo de pilas activo y pasivo.

Rastreo de pilas activo: el rastreo de pilas IP permite averiguar rápidamente y con bastante posibilidad de acierto cuál es el sistema operativo instalado en el host.

Utiliza técnicas de sondeo basándose en hipótesis razonables para determinar el sistema operativo utilizado.

Entre las técnicas de sondeo se tienen por ejemplo: la de enviar un paquete FIN a un puerto abierto o introducir una bandera TCP en la cabecera de un paquete SYN, y el comportamiento de respuesta es el que permite deducir qué sistema operativo se tiene en el Host.

Rastreo de Pilas pasivo: En esta técnica el atacante se limitará a observar de forma pasiva el tráfico de red para determinar el sistema operativo que se está utilizando.

Hay cuatro atributos asociados a cualquier sesión TCP/IP cuyas medidas dan la pauta de con que sistema operativo se cuenta, estos atributos son: el tiempo de vida del paquete saliente que define el sistema operativo o también denominado TTL, el tamaño de la ventana definido por el sistema operativo, el bit de no fragmentación (DF) y el tipo de servicio (TOS).

Se analiza en forma pasiva estos cuatro atributos y se comparan con una base de datos conocida para determinar el sistema operativo.

Detección y prevención: Las herramientas de detección de exploración de puertos son los más grandes aliados para detectar un rastreo de pilas activo y poder saber que alguien está queriendo obtener la información del tipo de sistema operativo con el que se cuenta.

La prevención en este caso es bastante compleja, porque tocaría realizar cambios en los sistemas operativos para variar su comportamiento y despistar a los intrusos, pero estos cambios pueden afectar de forma directa a la funcionalidad del sistema operativo como tal causando un problema mucho más grave.

Se debe trabajar en el tema de firewalls para que inclusive averiguando el sistema operativo que se tiene sea igual de complejo provocar un ataque de seguridad.

1.5.2.2 Tipos de Ataques

En la sección anterior se mencionó las técnicas de exploración, con un objetivo común de recopilar toda la información del sistema objetivo a nivel de actividad de la red, puertos abiertos, servicios activos, tipo de sistema operativo, etc.

Una vez obtenida toda esta información el atacante está listo para lo que realmente busca, que es tomar la acción que le permita alterar el sistema.

En esta sección se tratará qué tipos de ataques se pueden realizar y cuáles son sus consecuencias en el sistema.

1.5.2.2.1 Ataque de Denegación de Servicios (DOS)

Todo sistema informático implementado tiene como funcionalidad brindar algún o algunos tipos de servicios, ya sean esto a una comunidad de clientes internos o a clientes externos como es el caso de los sitios de comercio electrónico en Internet.

Cuando un atacante logra vulnerar un sistema provocando que este ya no pueda dar sus servicios, estamos frente a un ataque de denegación de servicios.

Según Scambray, McClure y Kurtz, (2001,539) existen cuatro tipos de ataque DOS, estos son: consumo de ancho de banda, inanición de recursos, defectos de programación y finalmente ataques DNS y de enrutamiento.

Consumo de ancho de banda: Esencialmente los atacantes consumirán todo el ancho de banda disponible en una red, esto puede suceder en una red local, pero es más probable que el atacante consuma los recursos remotamente.

Este tipo de ataque como se puede ver está orientado a consumir los recursos de red, por eso cuando se habla de los mensajes ICMP y de su peligro latente, se puede apreciar por ejemplo que fácilmente se puede enviar mensajes amplificados que inunden o saturen la red provocando la denegación del servicio.

Inanición de Recursos: Se diferencia del ataque de consumo de ancho de banda porque esta orientado más al consumo de recursos del sistema que a los recursos de red, enfocándose por ejemplo en la saturación de CPU, de memoria, cuotas del sistema de archivos, etc.

Defectos de Programación: En este caso el atacante aprovecha un fallo en la aplicación o sistema operativo, por ejemplo si un programa utiliza un *"buffer"*[5] de 128 bytes, se puede conseguir un desboradamiento de *"buffer"* y bloquear la aplicación.

Ataques de enrutamiento: El atacante consigue manipular la lista de distribución o enrutamiento para denegar el servicio a redes o sistemas legítimos, logrando con esto que el tràfico de red sea enviado a direcciones incorrectas creadas por los atacantes.

Ataque DNS : Los ataques DOS sobre servidores de nombres de dominio (DNS) convencerán al servidor objetivo para que almacene direcciones falsas en la memoria temporal, de esta manera cuando un servidor DNS realice una búsqueda el atacante ya ha redireccionado el servidor a un sitio falso.

1.5.2.2.2 Hijacking (Secuestro de Sesiones)

Por la red viaja todo tipo de información que se puede imaginar, como por ejemplo los usuarios de acceso al sistema, números de tarjetas de crédito, claves secretas, etc.

[5] Espacio de memoria asignado para una aplicación

El *“Hijacking”*, es definido por Scambray, McClure y Kurtz, (2001) como el acto de apropiación indebida de la información utilizando un descuido fundamental en el protocolo TCP con el cual se puede espiar la conexión y robar la sesión telnet, habilitar contraseñas para dispositivos de red o enviar un comando que se ejecutará en el sistema, entre otros.

“Hijacking” utiliza el método de intercepción para lograr su objetivo y apropiarse de información no autorizada.

1.5.2.2.3 Programas Maliciosos

Según William Stallings en la publicación del libro Network Security los programa maliciosos tienen 2 grandes clasificaciones: los que necesitan que el programa resida en un servidor para expandirse y los independientes es decir no necesitan un programa centralizado para su replicación.

Dentro de los que si necesitan un programa se tiene: Los trapdoors o puertas traseras, las bombas lógicas, los caballos de troya y los virus.,

Dentro de los independientes se tiene a las bacterias y los gusanos.

A continuación se mostrará como William Stallings define estos tipos de programas maliciosos.

Trapdoors: son programas escritos dentro de códigos fuentes reales de la aplicación, de tal manera que en un momento determinado de la ejecución de la aplicación se activan estas líneas de programas malicioso provocando un hueco de seguridad.

Bombas Lógicas: son códigos de programa que se activan con un evento, por ejemplo al realizar la función fecha se activa este código de programa que provoca un ataque de seguridad.

Caballos de Troya: son instrucciones embebidas en códigos de programación buenos que causan acciones malas como por ejemplo enviar los datos de tu clave secreta al atacante de la red.

Virus: son códigos de programación que se copia el mismo dentro de otros programas y puede provocar simplemente una alerta en la funcionalidad del sistema operativo o hasta la completa denegación de servicio si se habla de un virus más potente.

Bacterias: una bacteria se replica hasta lograr llenar el espacio en disco o usar todos los ciclos de CPU, es decir provoca el consumo de recursos que

terminará en una denegación de servicio por saturación de uso de los mismos.

Gusanos: es un programa que se replica a si mismo pero a través de la red usando el correo electrónico ya sea en el mensaje o en el documento insertado en el correo.

Todos estos programas maliciosos se encuentran ampliamente distribuidos en Internet, y constituyen una verdadera amenaza tanto para empresas como usuarios en general.

1.5.2.3 Vulnerabilidades de Seguridad

Existen catorce principales vulnerabilidades de seguridad que hay que tomar en cuenta según Scambray, McClure y Kurtz, (2001,736):

Control de acceso inadecuado al router: un ACL del router que se haya configurado erróneamente puede permitir la filtración de información a través de ICMP y permitir accesos no autorizados a determinados servicios.

Los puntos de acceso remoto no seguros y no vigilados proporcionan: uno de los modos más sencillos para acceder a su red corporativa.

Contar con excesivas relaciones de confianza: tales como los dominios de confianza de NT y los archivos .rhost y host.equiv de Unix pueden proporcionar al atacante un acceso no autorizado a sistemas sensibles.

Cuentas de usuario o de pruebas: con privilegios excesivos.

Software que no hayan sido convenientemente parchados: no estén actualizados, sean vulnerables o se dejen con su configuración predeterminada.

Carencia de directivas, procedimientos y directrices de seguridad aceptadas y convenientemente elaboradas.

Excesivos controles de acceso: a los archivos y directorios (recursos compartidos de NT, exportaciones mediante NFS en Unix.)

Servicios no autenticados: tales como Xwindows que permite a los usuarios capturar pulsaciones de tecla realizadas de forma remota.

Contraseñas reutilizadas, sencillas o fácilmente adivinables a nivel de estación de trabajo pueden poner en peligro la seguridad de sus servidores.

Servicios de internet mal configurados: especialmente archivos de comandos CGI en servidores web y FTP anónimos.

ACL de routers o de cortafuegos mal configurados: pueden permitir el acceso a sistemas internos.

Los hosts que ejecutan servicios innecesarios: tales como RPC, FTP, DNS, SMTP dejan caminos abiertos.

La filtración de información: puede proporcionar al atacante la versión del sistema operativo y de la aplicación, los usuarios, grupos, servicios compartidos.

Capacidades de registro: de vigilancia y de detección inadecuadas a nivel de red y de host.

Las vulnerabilidades mencionadas constituyen una amenaza potencial debido a que pueden ser aprovechadas en cualquier instante por atacantes internos o externos.

1.5.3 Firewalls

William Stallings en su libro “Network Security Essentials” (1999) define a un firewall como una “efectiva manera de protección de un sistema local o redes

de sistemas, contra una red basada en amenazas de seguridad; mientras refuerza el acceso al mundo exterior via WANs[6] o Internet".

Stallings también define las siguientes metas de diseño:

- Todo tráfico del interior al exterior debe pasar a través de un firewall
- Sólo tráfico autorizado (definido por las políticas de seguridad local) debe ser permitido pasar.
- El firewall así mismo debe ser inmune a cualquier penetración (hacer uso de sistemas confiables con un sistema operativo seguro)

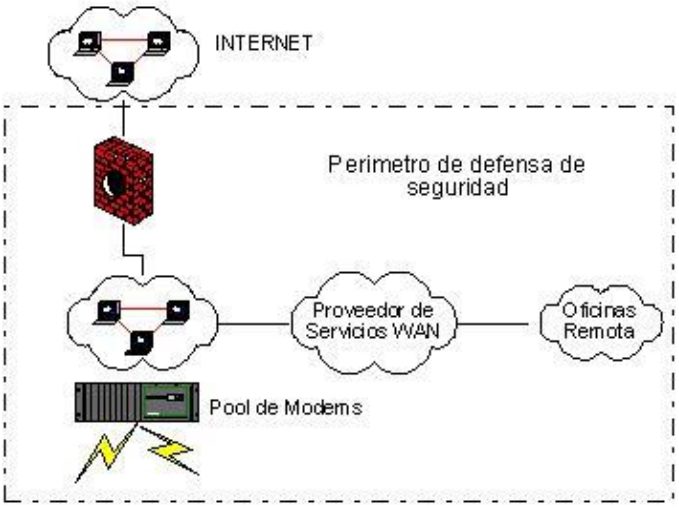

Figura 1.3 Firewall crea un perímetro de defensa
Fuente: Autores

[6] De las siglas Wide Area Network; es un terminado usado para expresar conexiones a redes grandes tal como una conexión entre ciudades.

Una analogía sencilla respecto al concepto de firewall, es considerarlo como una pared con orificios debidamente administrados; manteniendo un control respecto al tráfico que se permite circular de un lado de la pared al otro.

1.5.3.1 Características de un Firewall

Se puede distinguir en un Firewall cuatro técnicas de operación generales las cuales definen sus características (Stallings, 1999):

- Control de Servicio.- Determina el tipo de servicio de Internet que puede ser accedido; entrante o saliente.
- Control de dirección.- Determina la dirección en la cual un servicio es permitido fluir.
- Control de usuarios.- Control de acceso a un servicio que un determinado usuario puede acceder.
- Control de ambiente.- Control de como un servicio particular es utilizado.

Cada fabricante de estas herramientas da mayor o menor énfasis a cada una de las caracteristicas mencionadas, dependiendo de los objetivos en la implementación.

1.5.3.2 Tipos de Firewalls.

Existen cuatro tipos comunes de Firewalls (Stallings 1999):

- Ruteadores “Packet-Filtering”.
- “Application-level gateways”.

- “Circuit-level gateways”.
- “Bastion hosts”.

A continuación se explicará brevemente cada uno de los tipos en mención.

1.5.3.2.1 Ruteadores “Packet-filtering”.

O ruteadores filtradores de paquetes (de su traducción al español); aplica un conjunto de reglas a cada paquete IP entrante y luego lo reenvía o descarta. Los filtradores de paquetes operan en ambas direcciones. El filtrador de paquetes es típicamente configurado como una lista de reglas basadas en la concordancia en campos en la IP o en la cabecera TCP. Se pueden definir dos políticas por defecto: descartar o reenviar (Stallings, 1999).

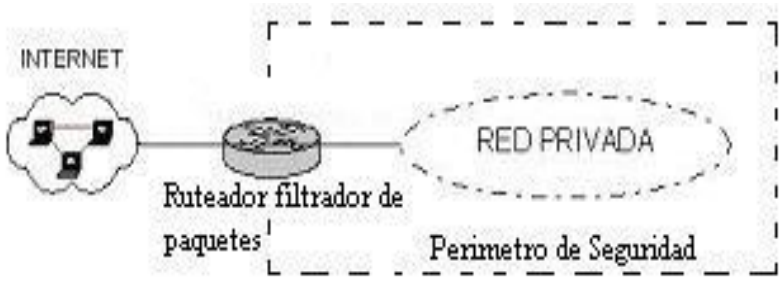

Figura 1.4 Firewall Ruteador “Packet Filtering”
Fuente: Network Security Essentials-(William Stallin, 1999,323)

Stallings (1999) define las siguientes ventajas:

- Simplicidad
- Transparencia a usuarios.

- Alta rapidez

Y desventajas:

- Dificultad en la configuración de reglas.
- Falta de autenticación.

El esquema de implementación más común en este tipo de firewall son las listas de accesos que se definen en un ruteador.

1.5.3.2.2 Application-level Gateway.

"Application-level gateway[7]*"* (Puerta de enlace a nivel de aplicación) o también llamado servidor proxy; actúa como un relay[8] de tráfico a nivel de aplicación (Stallings, 1999).

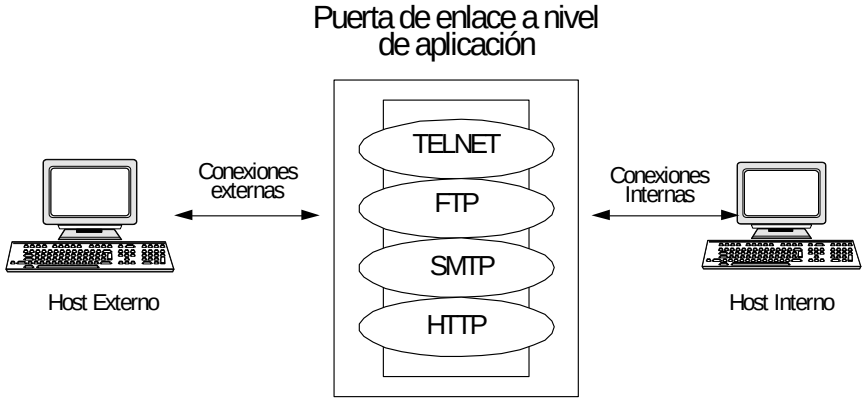

Figura 1.5 Aplication-level gateway
Fuente: Network Security Essentials-(William Stallin, 1999,323)

Este tipo de firewalls presenta las siguientes ventajas (Stallings, 1999).

[7] Gateway: puerta de enlace entre conexiones de red.
[8] Término usado para describir el proceso de actuar como intermediario en el traspaso de información de un lugar a otro.

- Mayor seguridad que los “packet filters”.
- Sólo necesita examinar un poco las aplicaciones permitidas.
- Facilidad en el desarrollo de auditorías y revisiones de bitácoras respecto al tráfico entrante.

La desventaja que presenta este tipo de firewall es que incorpora procesamiento adicional en cada conexión, incrementando la seguridad pero añadiendo latencia en la conexión.

1.5.3.2.3 Circuit-Level Gateway.

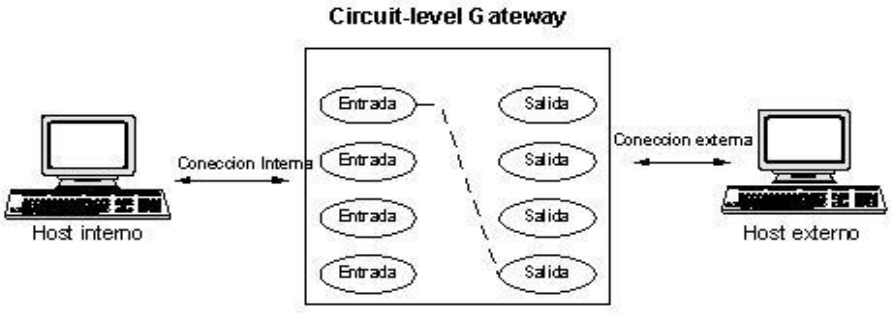

Figura 1.6 Circuit-Level Gateway
Fuente: Network Security Essentials-(William Stallings, 1999,323)

“Circuit-Level Gateway” (Puerta de enlace a nivel de circuito) es un sistema Stand-alone[9] o puede ser una función especializada realizada por un gateway a nivel de aplicación. Un *“Circuit-Level gateway“*, no permite

[9] Un sistema Stand-alone es un sistema independiente; es decir que no necesita de otra aplicación para funcionar.

conexiones TCP de tipo *"end-to-end"*[10]; más que las puertas de enlaces establecidas entre dos conexiones TCP (Stallings, 1999, 326).

La función de seguridad en este tipo de firewall consiste en determinar las conexiones TCP que seran permitidas, actuando como un puente entre la red interna y el Internet.

1.5.3.2.4 Bastion Host.

Un *"bastion host"* es un sistema identificado por el administrador del firewall como un crítico y fuerte punto en la seguridad de la red. Típicamente, el *"bastion host"* sirve como una plataforma para un *"Application-level"* o *"Circuit-level gateway"* (Stallings, 1999). Stallings enuncia las siguientes características comunes:

- La plataforma de hardware ejecuta una versión segura de su sistema operativo, haciéndolo un sistema confiable.
- Sólo se instalan los servicios que el administrador de red considera esenciales.
- Se puede requerir una autentificación preliminar antes que un usuario autorizado pueda acceder a los servicios del servidor *"Proxy"*.
- Cada *"Proxy"* mantiene una auditoría detallada de información por medio de una bitácora de todo el tráfico generado.

[10] Conexion end-to-end se refiere a un tipo de conexion directa entre pares de hosts

- Cada módulo de *"Proxy"* es un pequeño paquete de software específicamente diseñado para la seguridad de la red.

Todas estas características son esenciales en el *"bastion host"* y no hay que descuidar ninguna de ellas, dado que al ser un puente entre Internet y la red interna, también se convierte en el ingreso principal para que un intruso acceda a la red.

1.5.4 Acerca de Linux.

La historia de Linux se debe remontar hasta los principios del proyecto GNU[11](http://microlug.linux.net.uy/gnu/gnu.htm); el cual puede considerarse como el punto de partida de esta revolución del software libre, la historia de GNU es vista como la prehistoria de Linux; y esta puede ser resumida en los siguientes puntos principales.

Linux nace en 1991, de la mano de Linus Benedict Tolvalds, cuando era estudiante de informática de la Universidad de Helsinki, Finlandia. La idea vino principalmente cuando Linus observó el código fuente de Minix, un pequeño Unix[8] desarrollado por Andy Tannenbaum, gran experto en el área de los sistemas operativos. Linus decidió, entonces, como simple hobby,

[11] Las siglas GNU atienden a la aclaración en inglés **GNU´s Not Unix**, que viene a explicarnos en cuatro palabras que GNU no es lo mismo que Unix.

desarrollar su propio sistema operativo, basado en Minix, el cual ni siquiera tenía nombre.

En los próximos años, el kernel pudo ser portado a una gama extensa de arquitecturas: Alpha, SPARC, SPARC-64, Amiga, Atari, Macintosh, ARM/Strong-ARM, PA-RISC, PowerPC, MIPS, e inclusive la nueva arquitectura IA-64 de Intel (http://microlug.linux.net.uy/gnu/historia.htm).

Actualmente Linux es uno de los sistemas operativos más utilizados a nivel mundial (sobretodo en Internet), debido a su bajo costo de adquisición y su alto nivel de confiabilidad.

1.5.4.1. Características.

GNU/Linux es todo un sistema operativo libre, bajo las condiciones que establece la licencia GPL (*"GNU Public License"*). Tiene todas las características que uno puede esperar de un sistema Unix moderno: multitarea real, memoria virtual, bibliotecas compartidas, carga por demanda, soporte de redes TCP/IP, entre muchas otras funcionalidades.
(http://microlug.linux.net.uy/gnu/historia.htm).

Debido a su eficiente aprovechamiento de recursos, Linux tiene requisitos de hardware mínimos muy bajos. Una configuración mínima puede ser una 386 SX/16 con 1MB de RAM, y una disquetera (más teclado, tarjeta de vídeo, monitor, etc.) Esto es suficiente para arrancar y entrar al sistema. Para tener un sistema con todos los comandos importantes y una o dos aplicaciones pequeñas se requieren alrededor de 10 MB de disco duro. Para un sistema más completo, se aconsejan 4 MB de memoria, u 8 si se piensa utilizar una interfaz gráfica. Si se va a tener muchos usuarios y/o muchos procesos a la vez, serían aconsejables hasta 16 MB. 32 MB es más que suficiente para cargas pesadas a un máximo rendimiento. En lo que respecta a disco duro, depende de las aplicaciones que se instalen, se va desde los 10 MB básicos hasta los 350 MB de una distribución instalado con varias aplicaciones (incluye compiladores, paquetes de oficina, interfaz gráfica, etc.). Obviamente, un procesador más veloz siempre será ventajoso. El coprocesador matemático nunca es requisito, pero acelera aquellas aplicaciones de cálculo de punto flotante intensivo.

1.5.4.2. Distribuciones

Existen un sin número de distribuciones en la red entre ellas se pueden citar Guadalinex, Woody, Knoppix, DATA, Slax, Yubox, Debian, Mandrake, Suse, Fedora, Red Hat; etc (http://usuarios.lycos.es/putusoft/trucospc/distrib.htm). Siendo la más usada a nivel mundial Red Hat, cuya última versión comercial

es la cuarta (www.redhat.com). Red Hat dejó de dar soporte a su versión no comercial siendo la última la versión 9; luego de esto cambió de nombre a esta distribución a Fedora (http://www.fedora.redhat.com) siendo su última versión la 3. La alemana Suse también dejó de ser gratis una vez que Novell adquirió los derechos de esta distribución (http://www.novell.com/es-es/linux/suse/).

De las distribuciones gratis Mandrake y Debian son ahora las más usadas junto con Fedora; pero Ecuador tampoco se ha quedado atrás liberando su primera distribución en el presente año, YUBOX.

CAPÍTULO 2

Descripción de nuestro e-commerce y análisis de mercado

2.1 Descripción general

El proyecto de tópico - sitio web de comercio electrónico - está orientado a la venta de arreglos florales, en combinación con obsequios complementarios como: bombones, peluches, adornos, bebidas, libros, entre otros; categorizados para diferentes eventos y ocasiones.

En el diseño de la página se consideraron características como: facilidad de uso para usuarios expertos y novatos; interface agradable; y desventajas de la transaccionalidad propuesta por sitios web existentes en el mercado.

El esquema de pagos implementado está basado en transacciones con tarjetas de crédito sobre un enlace de transmisión seguro; es decir, mediante un protocolo de encriptación de datos se protege la información confidencial de los clientes como: datos generales, pin de la tarjeta, contraseña, fechas de expiración y cvv2[12].

Luego de analizar diferentes opciones para definir el nombre del sitio, se decidió denominarlo “Contodomiamor.com”.

[12] Código autorizado para transaccionar cuya información no está disponible en la banda magnética de la tarjeta.

El nombre seleccionado considera características como: facilidad para la retentiva de la marca propuesta en el proyecto, identificación total hacia el tipo de productos y bienes que se comercializa, originalidad en el mercado local y novedoso.

Para cubrir los detalles en temas logísticos, como la entrega de los bienes adquiridos al domicilio del cliente o destinatario, se supuso que existe una alianza estratégica con la compañía Servientrega del Ecuador; con el objetivo de contar con un alcance a nivel nacional en la entrega de los productos.

2.2 Investigación y estrategia de mercado

2.2.1 Encuestas generadas

Debido a que en el Ecuador actualmente no está totalmente adoptado el esquema de compras y pagos electrónicos, se realizó una investigación de mercado para conocer las oportunidades de ingresar al mercado local existente.

El cuestionario de investigación de mercado desarrollado considera los siguientes aspectos:

- Sexo y edad.
- Costumbre de obsequiar flores.
- Los tipos de obsequios adicionales que se suelen regalar.

- Eventos en los que se obsequian flores.
- Formas de pago utilizadas.
- Costumbre de realizar compras por Internet.
- Disposición del encuestado para adquirir los productos ofrecidos por Internet.

2.2.2 Análisis de los competidores directos

Utilizando motores de búsqueda en Internet, se identificó que a nivel local existen los siguientes competidores:

- www.braganca.com.ec
- www.florerialamarcelle.com
- http://daflores.com
- www.delejos.com

Por cada competidor se realizó un análisis de las fortalezas y debilidades que presentan.

www.braganca.com.ec

Fig 2.1 Web Site de Braganca
Fuente: www.braganca.com.ec

Fortalezas

- Interface de usuario agradable, el sitio posee un buen diseño gráfico.
- Brinda la facilidad de dos esquemas de pago:
  - En línea – utilizando el servicio Todo1.com, permite cancelar utilizando la tarjeta Diners y Visa Banco Pichincha.
  - Otras Tarjetas de Crédito – confirmación telefónica.
- Presenta al usuario una guía breve y concisa de cómo realizar sus pagos.
- Su posicionamiento actual en el mercado se encuentra en etapa de crecimiento y expansión.

Debilidades

- Restricción en el envío de productos, poseen cobertura solamente en las ciudades de Guayaquil y Quito.
- No está orientado a todos los niveles económicos, sus precios son elevados.
- Posee un universo limitado para seleccionar los arreglos florales, poca variedad.
- No ofrece promociones complementarias a los usuarios.

www.florerialamarcelle.com

Fig 2.2 Web Site de “La Marcelle”
Fuente: www.florerialamarcelle.com

Fortalezas

- Posee presencia en el mercado no electrónico.
- Goza de prestigio en el comercio tradicional.

Debilidades

- Diseño en la página web de estilo muy informal.
- La página no brinda la facilidad de observar un preliminar del arreglo floral seleccionado.
- La página está enfocada a clientes ya captados en el comercio tradicional, no es amigable para los potenciales nuevos clientes.

- No se ofrece forma de pago electrónico.
- No posee links de interés relacionados al tema.
- Presenta en el sitio promociones desactualizadas.

daflores.com

Fig 2.3 Web Site de "DaFlores.Com"
Fuente: http://daflores.com

Fortalezas

- Presencia en países Americanos: Argentina, Colombia, Ecuador, El Salvador, México, Panamá, Perú, Uruguay y Venezuela.
- Buena interface de usuario.

Debilidades

- El sitio presenta precios elevados al usuario final.

- El sitio posee solamente 4 opciones de tipos de arreglos: rosas, flores tropicales, arreglos varios y navideños.
- Si bien se presenta al usuario instrucciones sobre la manera de realizar sus pagos, las mismas no son lo suficientemente claras.

www.delejos.com

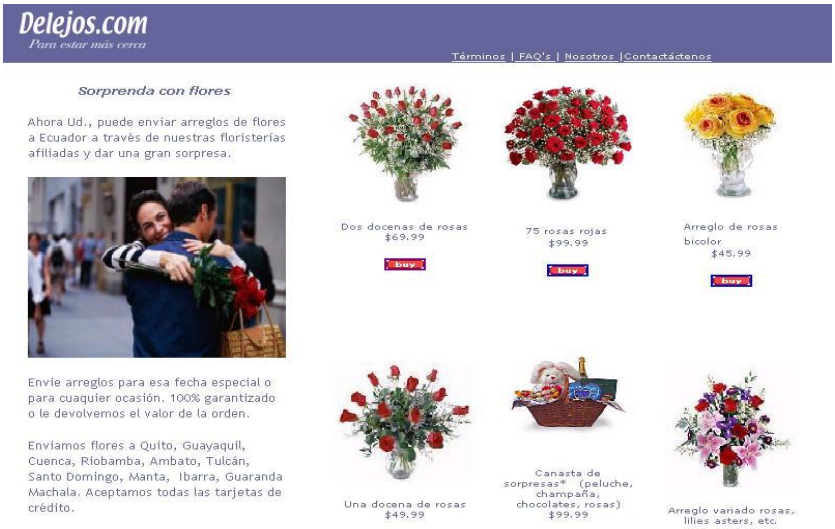

Fig 2.4 Web Site de “DeLejos.Com”
Fuente: www.delejos.com

Fortalezas

- Ofrece la alternativa de pago electrónica, mediante tarjeta de crédito.
- Posee una cobertura en el envío de arreglos a las principales ciudades del Ecuador: Guayaquil, Quito, Cuenca, Riobamba, Ambato, Tulcán, Santo Domingo, Manta, Ibarra, Guaranda, Machala.

Debilidades

- El sitio web presenta una limitada cantidad de arreglos florales a la venta (6).
- No ofrece alternativas para realizar búsquedas combinando criterios.
- Los precios son elevados.
- El diseño web desarrollado es poco creativo.

2.3 Nuestra propuesta y sus fortalezas

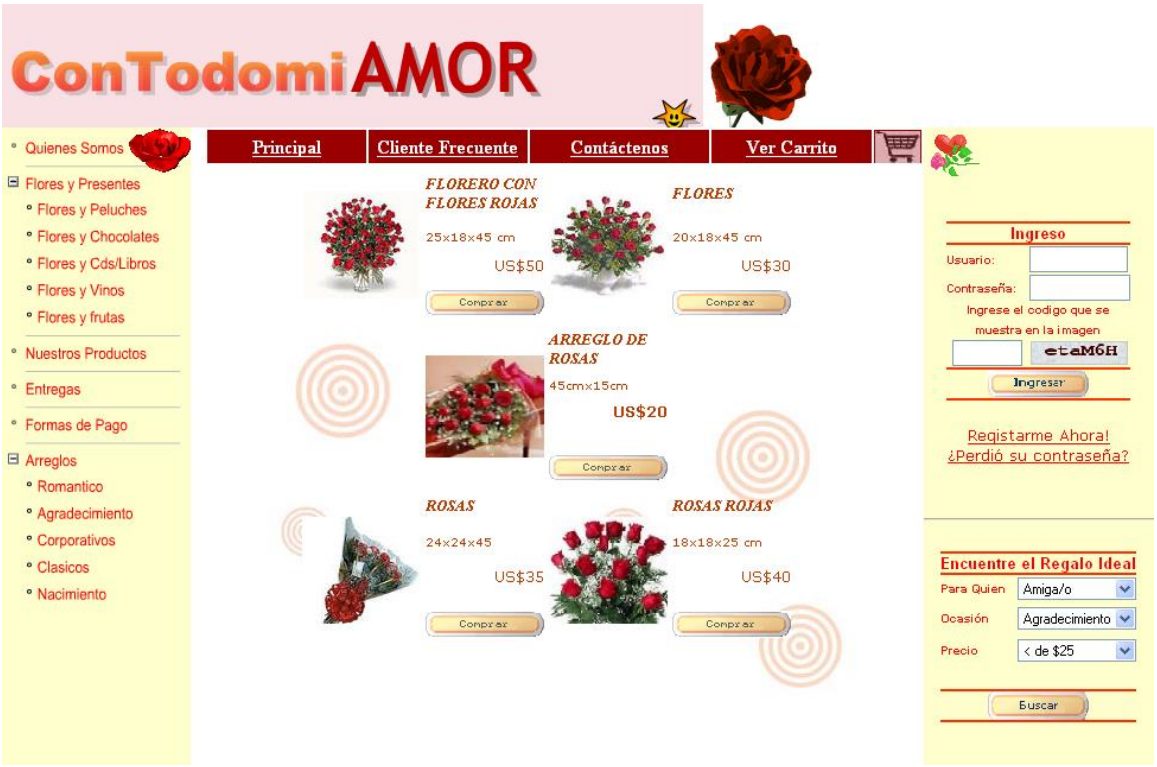

Fig 2.5 Página principal del sitio Web
Fuente: Autores

Fortalezas

- Se presenta al usuario un diseño web agradable y dinámico.
- Se ofrecen criterios de búsqueda combinables (precios, ocasiones, destinatarios).
- Se presenta la funcionalidad de listas de suscripción, con el objetivo de enviar newsletters y promociones.
- Se ofrece al cliente frecuente promociones y descuentos.
- Se pone a disposición del usuario precios accesibles.

- Cobertura en la entrega de obsequios a nivel nacional.
- El sitio y procesos se desarrollaron con TI de punta, implantando transacciones seguras vía web.
- Se brinda la alternativa de pago electrónico, mediante tarjetas de crédito.
- Personalización de mensaje adjunto en el obsequio

2.4 Segmentación del mercado de comercio electrónico

Luego de haber realizado la investigación de mercado inicial que consistió en elaboración de encuestas (detallado anteriormente en el punto 2.2.1) se obtuvo una perspectiva más clara de características como: ubicación geográfica, género, edad, nivel socio-económico, características del usuario respecto a la tecnología informática y uso de Internet.

Este estudio de mercado fue reforzado analizando las empresas (debilidades y fortalezas) que actualmente están tratando de cubrir las necesidades del usuario en este mercado, a través de sus sitios de ventas de arreglos florales publicados en Internet.

El segmento de mercado al cual se va a orientar el servicio que el sitio debe ofrecer, está integrado de la siguiente manera: (Autores, 2005)

- Mercado a nivel nacional: profesionales y usuarios de Internet en general que posean tarjeta de crédito, los cuales se encuentran con la dificultad de tener tiempo libre los días laborables en el horario de trabajo, para poder visitar lugares de interés con la finalidad de adquirir obsequios o detalles en general.

- Mercado a nivel internacional: compuesto por ecuatorianos residentes en el exterior que tienen familiares en el Ecuador, que se encuentran con la dificultad de enviar obsequios por los altos costos en los envíos.

CAPÍTULO 3

TOPOLOGÍA DE LA RED

3.1 DESCRIPCIÓN DEL ESQUEMA

En este capítulo se describirán dos modelos que son fruto del trabajo de investigación realizado en el análisis, desarrollo e implementación de este proyecto de graduación.

El primero al cual se llamará Diseño de Esquema Ideal se ha realizado pensando en maximizar la seguridad de la red sin escatimar en gastos; el segundo al cual se llamará esquema de laboratorio; es el que se ha desarrollado pensando en reducir costos de implementación, sin dejar a un lado la seguridad y de alguna manera demostrar la eficiencia de las herramientas que acá se mencionan. Cabe recalcar que ambos esquemas siguen la misma idea; la diferencia está en que el esquema de laboratorio ha sido implementado ajustándose al reducido presupuesto que se tiene para el proyecto.

3.1.1 Diseño de Esquema Ideal

A continuación se hace referencia a un modelo diseñado en base a la teoría anteriormente expuesta y en base al conocimiento adquirido sobre seguridades.

Detalle de los elementos involucrados en este esquema:

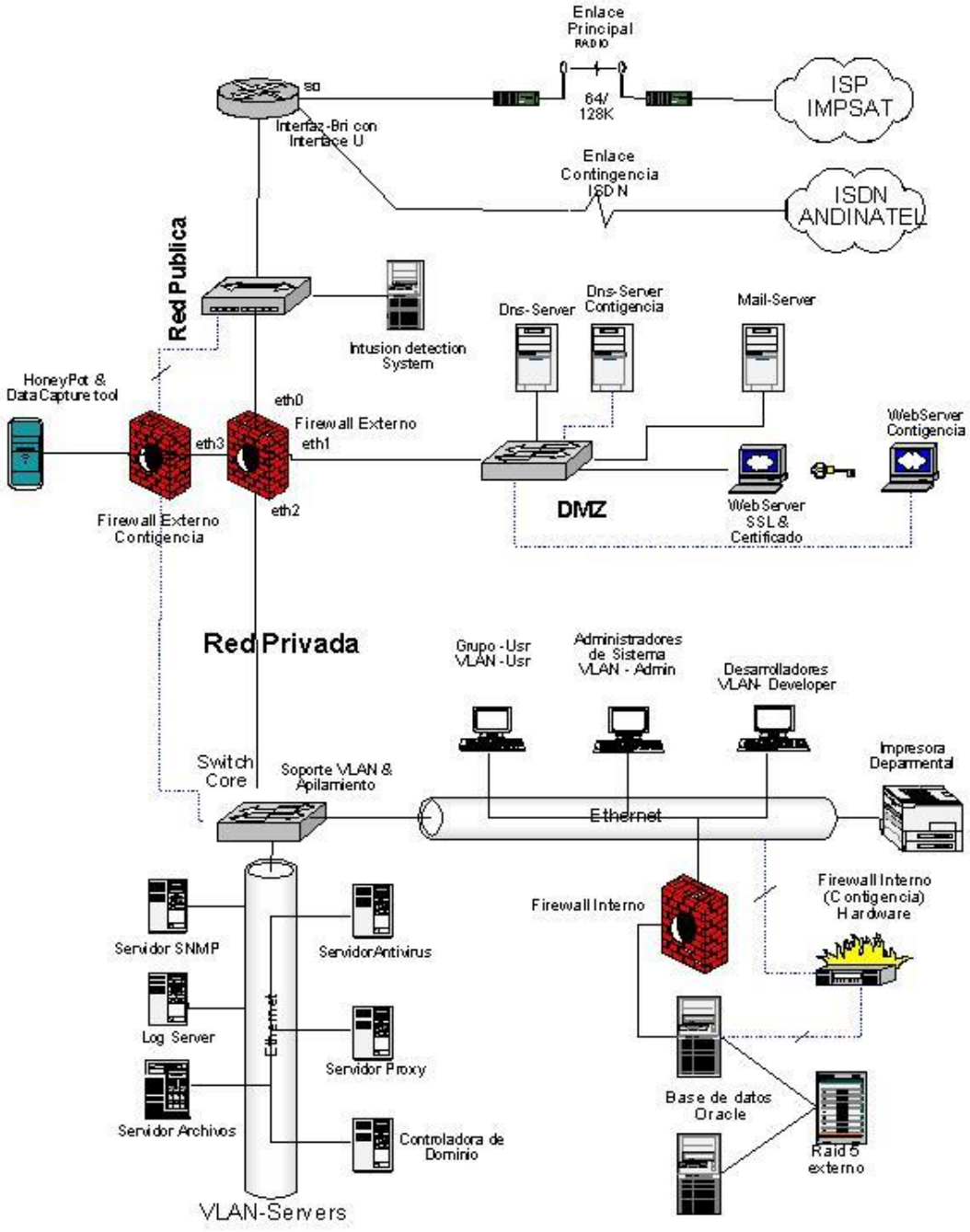

Figura 3.1 Esquema Ideal de Red Segura
Fuente: Autores

3.1.1.1 Firewalls

En esta sección se analizará uno a uno los firewalls que aparecen en el esquema ideal, se describirá su función en el esquema planteado e importancia.

Se observa como primer nivel de seguridad a un ruteador que tiene definido una lista de acceso *"Firewall Filtering"*, esto también protege al ruteador de ataques externos, especialmente si un *"Hacker"* trata de aprovechar un *"exploit"* para atacar las vulnerabilidades que tienen los sistemas operativos de los ruteadores. Es importante también tener actualizada la versión de sistema operativo, ya que de no hacerlo el ruteador podría ser fácilmente comprometido.

Un poco más abajo del gráfico, se observa a un Firewall más complejo que las ACLs del ruteador. Este Firewall debe proporcionar mayor seguridad que el anterior proporcionando bondades de detección de *"ip spoofing"* y denegación de servicio; además debe proporcionar una forma de integración con otras herramientas de seguridad tales como los detectores de intrusos; pudiendo alterar sus reglas de manera automática cuando el detector de intrusos detecta una actividad sospechosa. Este Firewall planteado debe tener cuatro interfaces de red: una para la red pública (aquella que se verá

en el Internert), una interfaz para la DMZ[13], otra para la conexión hacia la red privada y una para la red de los servidores señuelos. Las cuatro interfaces son necesarias para que cada red quede físicamente separada de la otra; reduciendo de esta manera el riesgo de que la red privada sea comprometida. Todo tráfico desde y hacia cualquier red debe ser definido como regla en el firewall.

Finalmente en la parte inferior del gráfico se observa el firewall interno, encargado por velar la seguridad del servidor de Bases de Datos de ataques de usuarios internos.

3.1.1.2 Detector de Intrusos y la red pública.

Dentro de la red pública conectada por un hub se encuentra un *"sniffer"* detector de intrusos, el cual permite analizar todo el tráfico que circula hacia y desde la WAN. Este *"sniffer"* (husmeador) mantiene una base de datos de patrones de ataques que se actualiza continuamente con nuevos patrones de ataques; esto con la finalidad de poder detectar ataques y potenciales amenazas, detenerlo oportunamente e informar sobre el hecho particular al administrador de red. Esta herramienta también debería ser capaz de poder interactuar con el firewall principal, para poder redireccionar direcciones IP y puertos al detectar una actividad sospechosa.

[13] Zona desmilitarizada

3.1.1.3 Red señuelo, Honey Pots y Data Capture Tool.

La red señuelo es aquel segmento de red donde se ubicarían los servidores que servirán de señuelo para atrapar al atacante, poder registrar sus actividades y de esta forma retroalimentar al detector de intrusos.

3.1.1.3.1. Honey Pots

Honey Pots o señuelos es un tema relativamente nuevo con respecto a seguridad; son capaces de emular el servicio de servidores de Internet tales como dns, ftp, web; etc. La idea es que una vez que el detector de intrusos descubra una actividad sospechosa interactúe con el firewall para direccionar al intruso a estos *"honeypots"*. Dentro e incorporado al kernel de estos Honey Pots se instalan herramientas capaces de registrar la actividad realizada por el intruso y notificar sobre el hecho al administrador de red y al detector de intrusos. Estos servidores se colocarían en una red adicional a la cual se llamará red señuelo (www.honeynet.org).

3.1.1.3.2. Data Capture Tool

Herramienta que se integra al kernel del sistema operativo y su funcionalidad se basa en registrar las actividades realizadas por el usuario. Al estar integrado al kernel del sistema operativo, es capaz de detectar actividades

aún cuando el usuario esté utilizando una sesión encriptada. Esta herramienta se instalaría en los servidores señuelo (www.honeynet.org).

3.1.1.4 Zona Desmilitarizada.

DMZ o Zona Desmilitarizada es el segmento de red destinado para los servidores publicables; es decir los servidores que de una u otra forma son accesados por los usuarios de Internet, tales como el servidor de correo, el servidor DNS para resolución de nombres y por supuesto el servidor WEB, donde se alojarán las páginas del sitio de e-comerce .

El servidor de correo ayudará para recibir los mensajes de los equipos administrables cuando éstos tienen problemas; mensajes de alerta del detector de intrusos, servidor de antivirus, además de proporcionar servicio de correo a los usuarios internos de la red. Por seguridad este debería manejar el protocolo SMTPS para envíos de correos y POP3S para descarga de los correos en los equipos clientes. El servidor DNS (Domain Name Server) permitirá la resolución de nombres a direcciones IP, es de acceso público por lo que no debería contener información de las máquinas internas; además debería contener los últimos parches de seguridad.

3.1.1.5 Red Privada y sus servidores.

La red privada es el segmento de red que es usado solo por usuarios pertenecientes a la organización. Dentro de la red privada se encuentran entre otros el servidor *"proxy"* de acceso a Internet; el cual recibe información del servicio de directorio (LDAP) para autentificar al usuario y asignarle los permisos de navegación correspondiente.

La controladora de dominio que permitirá a los usuarios conectarse a un dominio y ser autentificado proporcionando su usuario y contraseña; accediendo de esta forma a su cuenta que es administrado por políticas de grupo y usuario.

Servidores de archivos e impresoras para el acceso común de los usuarios de los departamentos.

Servidor de antivirus el cual tendrá la responsabilidad de descargarse las actualizaciones más recientes desde Internet y distribuirlo a los clientes de la red. También debe almacenar información de los eventos ocurridos en los clientes infectados y ser capaz de determinar heurísticamente código malicioso.

3.1.1.6 Servidores de monitoreo.

Para poder tener una red con alta disponibilidad es necesario poseer servidores que estén continuamente evaluando el estado de los servidores y equipos de comunicación; una herramienta bastante útil son los servidores SNMP (Simple Network Management Protocol), los cuales son capaces de recibir información *"traps"*[14] enviados por los servidores y equipos de networking; almacenar dicha información en su base de datos y enviar informes y reportes al administrador de red.

3.1.1.7. Red de Datos y Servidor de Base de Datos.

La red de datos es un segmento de red protegido por el firewall interno; dentro de este segmento se encuentran los servidores que contienen información de vital importancia en la organización. El servidor de base de datos al ser parte fundamental de la organización es necesario que tenga un esquema de replicación en línea con el servidor de contingencia. Para el efecto, el mismo debe tener un sistema cluster; el cual permite que ambos servidores actúen como uno solo; compartiendo tareas y obteniendo de esta forma balanceo de carga. Ambos deben grabar en un sistema RAID 5 externo, de tal forma que si uno de los servidores falla, el servicio no se ve interrumpido debido a que el servidor de contingencia tiene acceso inmediato a los datos.

---

[14] Envió de información SNMP de los equipos hacia el servidor SNMP; cuando ocurre una eventualidad.

3.1.1.8. Redes LAN Virtuales.

Una opción bastante útil en redes corporativas son las denominadas Virtual LANs (VLANs) o redes virtuales; las cuales permiten segmentar la red en varias subredes ganando de esta forma velocidad, disminuir colisiones[15] e incrementar la seguridad de la red; ya que a través de VLAN se puede tener a cada departamento dentro una red separada, limitando los dominios de *"broadcast"*[16].

Para que se puedan interconectar las VLANS es necesario un equipo que trabaje a nivel de capa tres del modelo de referencia OSI; generalmente se usa para este efecto switchs de capa tres; que además de brindar interconexión VLAN ofrecen seguridad al bloquear puertos inutilizados; asignar puertos a una dirección MAC específica, redundar enlaces y evitar lazos por medio de *"spanning tree"*[17] (Cisco CCNA 640-607, Seminario IV, 2004).

---

[15] Una colisión ocurre cuando dos elementos de red transmiten datos al mismo tiempo en un mismo segmento de red; lo que ocasiona que los paquetes trasmitidos se dañen.

[16] Envió de información de tipo difusión; es decir que es enviado a todos los equipos de la red.

[17] Este algoritmo cambia una red física con forma de malla, en la que se pueden formar bucles, en una red lógica en árbol en la que no se puede producir ningún lazo

3.1.2 Esquema de Laboratorio

Debido a las limitaciones en cuanto a la disponibilidad de equipos y presupuesto; se diseñó una red de laboratorio, en la cual se omitió varios servidores y en otros casos se instalaron en un solo servidor varios servicios; a pesar de eso la red implementada ofrece los suficientes niveles de seguridad para poder demostrar la eficiencia de las tecnologías utilizadas.

A continuación se realizará una breve explicación de la red implementada.

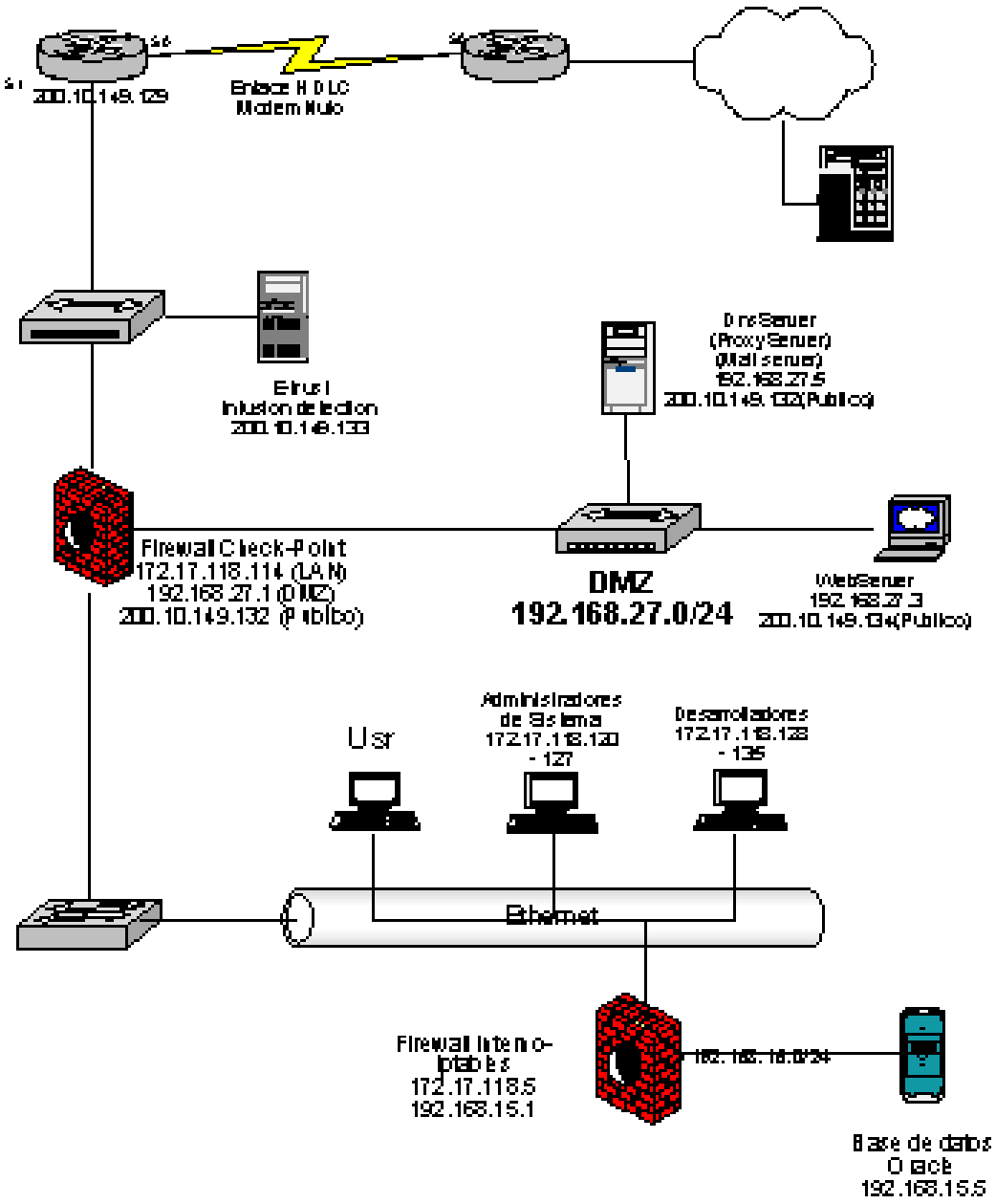

Figura 3.2 Esquema de Laboratorio
Fuente: Autores

En este esquema se observa como primer nivel de seguridad a un ruteador que tiene definido una lista de acceso (Firewall Filtering); para esto se aprovecha las bondades que ofrece IOS de Cisco (sistema operativo de ruteadores)

Dentro de la red pública, conectada por un hub se encuentra la herramienta *"E-trust Intrution detection"*; que es un sniffer detector de intrusos que permite analizar todo el tráfico que circula desde y hacia Internet.

Como Firewall principal se tiene al software *"Check-point NG",* el cual tiene un amplio reconocimiento por consultores de seguridad como Maint. Este firewall posee tres interfaces de red, una para la red pública, una para la DMZ o zona desmilitarizada y otra para la conexión a la red privada. Todo tráfico desde y hacia cualquier red interna/externa debe ser definido como regla en el mismo.

En la DMZ (Zona Desmilitarizada) se ubican todos los servidores publicables: servidor de correo, servidor WEB y un servidor para los servicios DNS (Domain Name Server) y Proxy. Una observación muy importante es que el servidor proxy no debería estar en la DMZ sino en la red interna; pero como se había mencionado anteriormente, esto se presenta solamente por cuestiones de costos. En el servidor de correo se implementó la herramienta

Sendmail; en el servicio DNS el programa Bind y en el servicio Proxy se utilizó el software Squid.

El firewall interno fue implementado con Iptables. Su principal funcionalidad es proteger al servidor de Bases de Datos de ataques internos. La base de datos se implementó con el manejador Oracle; herramienta ampliamente conocida en el medio por su robustez transaccional.

3.2 ESTRATEGIA DE SEGURIDAD

La seguridad de red involucra dos componentes principales: el primero es proteger la red, sus recursos e información sensible contra el acceso no autorizado y el segundo es la habilidad para recuperar datos ante eventos fortuitos (Stallings, 1999). A través de este subcapitulo se explicará sobre la estrategia de seguridad sugerida para mantener la red y sus sistemas lo más seguros posible.

3.2.1 Políticas de Seguridad

El término política de seguridad se suele definir como el conjunto de requisitos, definidos por los responsables directos o indirectos de un sistema, que indica en términos generales lo que está permitido y prohibido en el área de seguridad durante la operación general de dicho sistema. (http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec- html/node333.html& e =10313)

Una política bien definida es la base fundamental de un sistema seguro, aunque siempre ésta también depende del factor humano, el cual es el punto más vulnerable y persuasivo del sistema.

3.2.1.1 Políticas de Identificación

A continuación se detallan algunas políticas de identificación necesarias para mantener la seguridad física del sistema planteado. (Autores, 2005)

- Todo empleado debe poseer una tarjeta de acceso la cual permitirá dependiendo de su función o cargo, ingresar a ciertos departamentos.
- En el caso del centro de cómputo solo tendrá acceso el personal de ingeniería en sistemas, los cuales deberán registrar en la bitácora su hora de ingreso y de salida; además del motivo de ingreso.

En este punto es importante concientizar a los empleados sobre la responsabilidad en la custodia y uso de sus tarjetas de acceso.

3.2.1.2 Políticas de Horario.

Las políticas de horario se las define de acuerdo al rol del empleado. A continuación se detalla algunas políticas importantes que se tiene que considerar. (Autores, 2005)

- El personal solo tendrá acceso a su área de trabajo en su respectivo horario, a excepción del personal de ingeniería en sistemas, los cuales por razones de mantenimiento deberán muchas veces estar en el área, aún fuera de su horario habitual.
- En caso que un empleado necesite ingresar por razones laborales en horas extras; éste deberá informar a su superior; el cual deberá enviar un reporte a seguridad para permitir el acceso del mismo.

Con la definición de esta política, se desea eliminar la circulación injustificada de empleados fuera de su jornada de labores.

3.1.2.3 Políticas de Vigilancia

Parte de la seguridad física de los sistemas abarca políticas tales como que en el centro de cómputo se cuente con un circuito de cámaras, además de alarmas de seguridad y de incendios. Los guardias también juegan un papel muy importante en la seguridad. (Autores, 2005)

3.2.1.4 Políticas de Concientización y adiestramiento

Es muy importante para salvaguardar la seguridad de los sistemas, adiestrar y concientizar al personal para que tenga conocimiento de la importancia de la seguridad en los sistemas y el rol muy importante que juegan ellos para mantenerla.

A continuación se enumeran algunas recomendaciones que los usuarios deben tener presente, cuando elaboran sus contraseñas. (Autores, 2005)

- Las claves deben poseer como mínimo 8 dígitos entre números y letras y no deben seguir ningún patrón, ni llevar nombre de familiares ni ocasiones especiales.
- Los usuarios deben aprender sus claves y no anotarlas en un papel ya que esto podría llegar a manos no deseadas.
- Las claves tienen una validez de máximo 45 días, luego de la cual se debe pedir al usuario que cambie las mismas.

Otra consideración importante que deben tener los usuarios; es sobre cómo mantener seguro sus estaciones de trabajo. A continuación se detalla algunas políticas a considerar (Autores, 2005)

- Los usuarios deben bloquear sus equipos durante su ausencia o habilitar los protectores de pantalla.

- Los usuarios no deben ejecutar archivos de fuente extraña, especialmente si estos llegan por correo.

Con estas consideraciones se espera crear un sentido de concientización respecto a la definición y custodia de las contraseñas, así como medidas básicas que se deben seguir para proteger las estaciones de trabajo.

3.2.1.5 Políticas de Respaldo y contingencia.

A continuación se detallan algunas políticas de respaldo y contingencia que se deben tener presente en la compañía (Autores, 2005).

- Se debe poseer un enlace a Internet de contingencia que permita estar en línea aún cuando la conexión principal este inactiva.
- Generar respaldos periódicos de la información de la Base de Datos.
- Poseer equipos con configuración igual al de los servidores y equipos de comunicación principales, que sirvan como contingencia ante casos inesperados.

Con estas políticas se desea mantener la continuidad en las operaciones de la compañía, ante casos de emergencia o fallas técnicas.

3.2.2. Técnicas de Redundancia

3.2.2.1. Enlace de Contingencia

Además de poseer un enlace principal con Internet se debería contar con un enlace de contingencia con otro proveedor de servicios. En el contrato con el ISP de contingencia, se debe establecer que para el enlace de contingencia se debe cobrar por bytes transmitidos y recibidos, no por mensualidades ya que por ser de contingencia es muy probable que no se use el servicio en mucho tiempo. (Autores, 2005)

Algo muy importante a considerar es que se debe trabajar en el enlace principal y de contingencia con diferentes proveedores de servicios de Internet (ISP), ya que muchas veces los problemas que pueden presentar los ISP son en su *"backbone"*[18], por lo que sería poco recomendable contratar a la misma empresa para la contingencia.

Con respecto a contingencia a nivel LAN; una forma de implementar contingencias es usando switch que soporten VLANs, apilamiento complementado con spanning tree. Las VLANS permiten crear subredes y por ende separar los dominios de colisión; el apilamiento permite una recuperación rápida cuando un equipo o puerto falla. La técnica de *"spanning tree"* evita lazos que pueden producirse al tener enlaces redundantes. (Autores, 2005)

[18] Red principal de la organización

3.2.2.2. Contingencia de servidores

Como política de contingencia para los servidores se debe tener que existan servidores con la misma configuración y datos por lo menos para los servidores principales. Para el caso del proyecto de graduación debería implementarse contingencia para los servidores Web y Bases de datos; de tal forma que si ocurre una eventualidad, se estaría en capacidad para el reemplazo de los servidores principales. Se pueden utilizar técnicas como "clustering" sobre todo para la base de datos. También sería factible tener contingencia para los firewalls tanto externo como interno, así como para el ruteador principal.

3.2.2.3. Contingencia de Datos – RAID

El siguiente método es proteger los datos con dispositivos de almacenamiento con tolerancia a las fallas. Este conjunto redundante de dispositivos es categorizado por los niveles RAID de sus siglas en inglés Redundant Array Inexpensive Disk (Arreglos redundantes de discos económicos).

La solución planteada para la Base de Datos es implementar un Arreglo de Disco RAID 5 externo. El tener el arreglo de disco externo permite que tanto

el servidor principal como el de contingencia, tenga acceso inmediato a los datos.

El servidor de contingencia de la base de datos debe tener las mismas configuraciones y programas que el principal, para que la respuesta ante fallas del principal sea inmediata.

3.2.3 Recuperación de Datos

Como política de seguridad se deben realizar backup periódicos. A continuación se describe la forma como se deberían realizar las copias de seguridad en cintas:

Primero se debe realizar una copia de seguridad completa del día lunes; esto reactiva todos los "bits de archivo"[19]. El día martes, se ejecuta una copia de seguridad incremental en otra cinta. Esto guarda todos los archivos que se modifican el día martes en una cinta y reactiva el bit de archivo. Este proceso se repite para todos los otros días hábiles de la semana, cada uno en una cinta individual. Esto suministra una copia de seguridad completa de todos los archivos que se modifican durante esa semana. El siguiente día lunes, se vuelve a repetir todo el proceso. (Autores, 2005)

[19] Indica si un archivo se ha modificado o no. 1 si se ha hecho alguna modificación en el archivo 0 si no.

3.2.4 Recuperación ante Fallas eléctricas

Es necesario disponer de un generador de energía eléctrica de emergencia en caso que hubiera fallas en el suministro de la electricidad en el área donde se encuentra el centro de cómputo. (Autores, 2005) Contra fallas eléctricas es necesario disponer de UPS de tal forma que si se interrumpe el flujo de la energía eléctrica, los servidores se mantengan activos hasta que se haga el cambio manual a la planta de electricidad de emergencia.

3.3 ELEMENTOS DE LA RED

3.3.1 Servidores de Datos

Son los elementos principales de la organización ya que en éstos equipos se almacena información importante como: procesos, cuentas, clientes, proveedores, datos en general del negocio. Es importante invertir en esquemas de seguridad y redundancia para mantener protegidos a estos servidores.

3.3.2 Servidores Web.

“Una computadora que proporciona páginas Web a exploradores de Internet y otros archivos hacia aplicaciones a través del protocolo http. Incluye el hardware, sistema operativo, software de servidor web, protocolos TCP/IP y

contenido del sitio. Si el servidor web es utilizado internamente y no por el público, puede ser llamado servidor de intranet" (www.answers.com, 2005).

Debido a que estos servidores son accesados por usuarios desde todo el mundo, es necesario mantenerlos actualizados con los últimos parches de seguridad de acuerdo al servicio que ofrecen y mantener deshabilitados aquellos servicios que no son necesarios y que muchas veces vienen activados por defecto en los sistemas operativos. Estos servidores son ubicados en una zona de red conocida como zona desmilitarizada; con la finalidad que si uno de estos servidores web es atacado no comprometa la seguridad de los servidores privados y que son accesados solo desde la Intranet (red interna). También es importante mantener esquemas de redundancia y planes de contingencia debido a que estos elementos de red son los más vulnerables. Entre los servidores de Internet se puede mencionar: servidor de correo, dns, entre otros.

3.3.3 Servidores de aplicaciones y red Interna

Los servidores de aplicaciones son aquellos que ofrecen algún servicio de red a los equipos clientes de la red interna; éstos no son accedidos de ninguna manera por usuarios de Internet. Entre ellos se puede citar al servidor proxy, servidor de impresoras, servidor de archivos, servidor controlador de dominio, entre otros. También son importantes dentro de la

organización y es necesario mantener en ellos una alta disponibilidad y eficiencia.

3.3.4 Elementos de seguridad

Son hoy en día un elemento de vital importancia dentro de la organización. Son los que están continuamente realizando monitoreos y verificaciones de información que fluye desde y hacia Internet. Entre ellos se tienen herramientas como: detectores de intrusos, señuelos o *honey pots*, firewalls, sniffers, servidores snmp, antivirus entre otros.

3.3.5 Equipos de comunicación

Según la clasificación propuesta por Cisco Systems (2001), los equipos de comunicación se clasifican en dos grupos: equipos de interconexión LAN y equipos de interconexión WAN. Su principal funcionalidad es mantener interconectados los equipos de la red. Entre estos dispositivos se puede mencionar: hubs, switches, ruteadores, equipos WLAN, antenas, módems, multiplexores, repetidores; etc. En éstos equipos también es importancia tener esquemas de redundancia y contingencia.

3.3.6 Equipos Clientes

Son los equipos terminales y estaciones de trabajo que son utilizados por los usuarios de la red para realizar sus funciones diarias.

3.4 ESQUEMA DE SUBREDES Y DIRECCIONES IP

3.4.1. Red Pública

En el esquema de direcciones públicas se usó el siguiente direccionamiento.

Dirección de Red: 200.10.149.128 Máscara: 255.255.255.224. Dirección de Broadcast: 200.10.149.158

Lo que permitirá tener en esa red un máximo de 30 direcciones (2^5 -2) para los hosts y tener hasta 6 subredes (2^3-2).

No es muy necesario tener muchas direcciones públicas por lo cual 30 direcciones brinda un amplio rango, ya que incluso actualmente se está usando solamente 4 direcciones. Estas direcciones son proporcionas por nuestro ISP.

3.4.2. Zona Desmilitarizada

En el esquema de direcciones en la Zona Desmilitarizada se usó el siguiente direccionamiento:

Dirección de Red: 192.168.27.0 Máscara: 255.255.255.0 Dirección de Broadcast: 192.168.27.255

Lo que permitirá tener en esa red un máximo de 254 direcciones para los hosts (2^8 -2). Como se puede apreciar con este esquema de direccionamiento se pueden tener hasta 254 direcciones IP, que si se descuenta la dirección IP de la puerta de enlace, ofrece la posibilidad de tener un total de 253 servidores publicables. Estas direcciones son de clase C privadas y fueron escogidas por el administrador de red.

3.4.3. Red Privada

En el esquema de la red LAN se usó el siguiente direccionamiento:

Dirección de Red: 172.17.118.0 Máscara: 255.255.254.0 Dirección de Broadcast: 172.17.119.255

Con este esquema se podrá obtener una red con un máximo de 510 direcciones para los hosts (2^9 -2). Estas direcciones son de clase B privadas y fueron escogidas por el administrador de red.

3.4.5. Red de Base de Datos

En el esquema de direccionamiento de red donde se encuentra la Base de Datos se usó el siguiente direccionamiento:

Dirección de Red: 192.168.15.0 Máscara: 255.255.255.0 Dirección de Broadcast: 192.168.15.255

Lo que permitirá tener en esa red un máximo de 254 direcciones para los hosts (2^8 -2). Como se puede apreciar con este esquema de direccionamiento se pueden tener hasta 254 direcciones IP que si se descuenta la dirección de la puerta de enlace, brinda la posibilidad de tener un total de 253 servidores. Estas direcciones son de clase C privadas y fueron escogidas por el administrador de red.

CAPÍTULO 4

CONFIGURACIÓN DE SERVIDORES

4.1 CONFIGURACIÓN SERVIDOR DNS

En esta sección se guiará en la configuración de las tablas DNS realizada en el proyecto, usando para el efecto el paquete bind-9.2.1-16 que viene incluido en la distribución de Red Hat 9.

Normalmente BIND viene incluido en todas las distribuciones Linux RED HAT. En Red Hat 5.1 y menores se usa el paquete BIND 4.x que usa un formato ligeramente distinto, en sus archivos de configuración. Versiones mayores a BIND 8.x ofrece mayor funcionalidad que BIND 4.x; ya que este no se lo ha desarrollado, es mejor actualizarlo con su última versión. Afortunadamente, convertir sus archivos de configuración BIND 4.x a BIND 8.x es sumamente fácil. (http://www.tldp.org/LDP/lame/LAME/linux-admin-made-easy/domain-name-server.html).

A continuación se detalla los pasos para configurar el servicio DNS en Linux Red Hat9:

1. Habilitar el servicio DNS para el efecto el archivo *"/etc/host.conf"* debería lucir así:

```
# Lookup names via /etc/hosts first, then by DNS query
order hosts, bind
# We don't have machines with multiple addresses
multi on
# Check for IP address spoofing
nospoof on
# Warn us if someone attempts to spoof
alert on
```

Como se puede observar en la configuración se ha habilitado el chequeo de *"ip spoofing"*[20] y el envío de alertas si se detecta el mismo.

2. Configurar el archivo "/etc/hosts" no es tan necesario, pero sería bueno colocar aquí los servidores de mayor acceso. En el proyecto se colocó el nombre del servidor y su dominio.

```
127.0.0.1       dnssrv localhost.localdomain          localhost
192.168.27.5      dnssrv  dnssrv.contodomiamor.com  localhost
```

3. A continuación se detalla las directivas que se debe configurar en el archivo *"/etc/named.conf"*

[20] Termino usado para describir la falsificación de una dirección ip (Refiérase al capitulo 1)

En la directiva “Zone” se debe colocar el nombre del dominio:

```
zone "contodomiamor.com" IN.
```

Dentro de esa directiva se debe colocar el nombre del archivo a la que debe referirse para encontrar las entradas del dominio:

```
file "contodomiamor_com.db".
```

El nombre del archivo no es importante, lo que si es importante es que este archivo de estar ubicado en el directorio *“/var/named”*.

Adicionalmente se debe configurar la zona de resolución reversa; esto quiere decir que dado la IP el Servidor DNS resolver el nombre del servidor consultado.

```
zone "149.10.200.in-addr.arpa" IN
```

En cada zona se hace referencia a los archivos donde debe leer las entradas. Todos los archivos que contienen las entradas dns deben estar ubicados en el directorio *“/var/named”.*

```
file "200_10_149.rev";
```

Es muy importante dentro de las zonas en la directiva *"Allow-Update o Allow Transfer"* colocar la dirección del servidor DNS al que se le permite transferencia de entradas, generalmente aquí se debe colocar la IP del servidor DNS esclavo; en nuestro caso colocamos "none"; porque no queremos realizar transferencia de zonas. Si se omite esta opción, cualquiera en Internet tendría la habilidad de requerir tales transferencias y ésta información podría ser usada por los *"spammers"*[21] e *"IP spoofer"*.

4. Configurar tablas DNS en el directorio *"/var/named",* tal como se lo indicó en *"/etc/named.conf"*. A continuación se muestra el contenido del archivo *"contodomiamor_com.db".*

[21] Persona que roba o compra direcciones de correo electrónico sustraídas y remite e-mails no solicitados

Contenido del archivo contodomiamor_com.db

```
$TTL 86400
@       IN      SOA  dnssrv.contodomiamor.com.   root.contodomiamor.com. (
                              2003022702 ; Serial
                              28800      ; 8 hour Refresh
                              14400      ; 4 minutes Retry
                              3600000    ; 100 hour expire
                              86400 )    ;24 hour minimum
; Listar el nombre de los servidores en uso.
              IN      NS      dnssrv.contodomiamor.com.
              IN      MX      mail.contodomiamor.com.
;Listado de maquinas y direcciones publicas
apachesrv   IN A   200.10.149.134    ; LinuxRedHat9(WebServer)
mail    IN A   200.10.149.132              ; LinuxRedHat9(DNS-mail-Proxy)
;Alias (canonical) name
www   IN       CNAME        apachesrv
```

Primero se escribe el nombre del servidor dns (“dnssrv.contodomiamor.com”) y segundo la cuenta root del dominio (“root.contodomiamor.com.”)

```
@       IN      SOA  dnssrv.contodomiamor.com.   root.contodomiamor.com.
```

Luego se procede a configurar los parámetros de envío y recepción de entradas dns, así como el número serial. El serial es importante ya que en él se registra los cambios realizados; si no se modifica el serial, el *"demonio"*[22] del servicio *"named"(demonio que maneja al servicio dns)* asumirá que no se ha hecho ninguna modificación y por ende no aceptará los cambios realizados.

```
2003022702 ; Serial
28800      ; 8 hour Refresh
14400      ; 4 minutes Retry
3600000    ; 100 hour expire
86400 )    ;24 hour minimum
```

Los otros parámetros que se observar se refieren a los tiempos de refrescamiento de entradas, reintento de solicitudes; tiempo de expiración de una entrada adquirida y tiempo mínimo.

Posteriormente se debe listar el o los servidores DNS; local y al cual se pide solicitudes de resolución de nombre.

```
IN      NS      dnssrv.contodomiamor.com.
```

[22] Término usado para referirse a los manejadores de los servicios en los sistemas Unix.

Por último se debe listar los servidores que son parte del dominio. Algo muy importante son los *"Alias de Nombres"*[23]; para el proyecto se requería que el servidor responda al nombre "www.contodomiamor.com"; por lo cual se debe colocar el siguiente alias para realizar dicha referencia.

```
apachesrv   IN A   200.10.149.134    ;
;Alias (canonical) name
www   IN       CNAME        apachesrv
```

5. Configurar las zonas reversas. Estos archivos son necesarios para poder resolver el nombre dado una ip. Ahora se analizará la configuración del archivo 200_10_149.rev .

Contenido del archivo 200_10_149.rev

```
@       IN      SOA dnssrv.contodomiamor.com.   root.contodomiamor.com. (
                                2003022702 ; Serial
                                28800      ; 8 hour Refresh
                                14400      ; 4 hour Retry
                                3600000    ; 1000 hour expire
                                86400 )    ;24 hour minimum
; List servers listed as in forward lookup table
            IN      NS      dnssrv.contodomiamor.com.
            IN      MX      mail.contodomiamor.com.
```

[23] Llamados también "canonical name"; son los seudónimos que el servidor dns resolverá

```
; List of machines & address locales, in reverse
134    IN      PTR   apachesrv
132   IN       PTR   mail
```

Básicamente posee los mismos parámetros que se tiene en *"/var/named/contodomiamor_com.db",* lo que cambia son las entradas dns; debido a que en este archivo se las configura al revés; es decir primero se coloca la dirección ip seguido del nombre del host. Como se puede apreciar sólo es necesario colocar la parte de la dirección ip que identifica al host

6. Como paso final se debe reiniciar el servicio para que la configuración realizada tenga su efecto. Para lo cual se debe digitar el comando *"service named restart"* o si el servicio estaba parado ejecutar el comando *"service named start"*

4.2 CONFIGURACIÓN SERVIDOR PROXY

4.2.1. Acerca de Squid.

Squid es el programa más popular utilizado en la configuración de servidores Proxy en los sistemas operativos basados sobre UNIX. Presenta características como: confiabilidad, robustez y versatilidad. Squid es un software libre, por lo tanto además de estar disponible el código fuente, está libre del pago de costosas licencias o restricciones de uso a un determinado número de usuarios.

Entre otras cosas, Squid puede ejecutar las funciones de servidor Proxy y realizar caché con los protocolos HTTP, FTP, GOPHER y WAIS, Proxy de SSL, WWCP, aceleración HTTP, caché de consultas DNS y otras funciones como filtración de contenido, control de acceso por dirección IP y usuario. (Barrios, 2001).

4.2.2 Programas requeridos.

Para realizar la instalación y posteriormente la configuración de Squid se deberá tener instalado lo siguiente:

- squid-2.4.STABLE1
- kernel-2.4.18-24
- Parches de seguridad disponibles para la versión de Red Hat que se esté utilizando.

Según lo establece Barrios (2001) “ninguna versión de Squid anterior a la 2.4.STABLE1 se considera como apropiada debido a fallas de seguridad de gran importancia, y ningún administrador competente utilizaría una versión inferior a la 2.4.STABLE1.”

4.2.3 Instalación de los programas necesarios.

Regularmente el programa Squid no se instala por defecto a menos que especifique durante la instalación del sistema operativo, y Squid viene incluído en casi todas las distribuciones actuales.

El procedimiento de instalación es exactamente el mismo que con cualquier otro programa:

```
mount /mnt/cdrom/
rpm -Uvh /mnt/cdrom/*/RPMS/squid-*.i386.rpm
Ejec.
```

“Es importante tener actualizado el kernel por diversas cuestiones de seguridad, por este motivo no es recomendable utilizar versiones del kernel anteriores a la 2.4.18.” (Linux Security, 2004).

Para la red del proyecto de graduación se configuró (“squid-2.5.STABLE1-2”), versión que viene disponible con los paquetes del sistema operativo Red Hat 9.

4.2.4 Consejos antes de iniciar la configuración.

Se debe evitar dejar espacios vacíos en lugares indebidos. A continuación se presenta un ejemplo de cómo no se debe omitir el comentario de un parámetro:

Escenario Incorrecto:

```
# Opción incorrectamente descimentada
    http_access 3128
```

El siguiente es un ejemplo la manera correcta al descomentar un parámetro:

Escenario Correcto:

```
# Opción correctamente descomentada
http_access 3128
```

4.2.5 Configuración.

Squid utiliza el archivo de configuración localizado en la ruta /etc/squid/squid.conf, se podrá trabajar sobre este archivo utilizando el editor de texto de su preferencia. Existen un gran número de parámetros, de los cuales se recomienda configurar los siguientes: (Barrios, 2001)

- http_port
- cache_mem
- cache_dir

- Lista de Control de Acceso
- Regla de Control de Acceso
- httpd_accel_host
- httpd_accel_port
- httpd_accel_with_proxy

4.2.5.1. Parámetro http_port – puerto a ser utilizado por Squid.

Squid por defecto utilizará el puerto 3128 para atender peticiones, sin embargo se puede especificar que lo haga en cualquier otro puerto o varios puertos a la vez.

En el caso de un servidor Proxy por defecto, regularmente se utilizará el puerto número 80 y se valdrá del redireccionamiento de peticiones de modo tal que no habrá necesidad de modificar la configuración de los navegadores web para utilizar el servidor Proxy, bastará solamente con utilizar como puerta de enlace al servidor. Es importante recordar que los servidores web (como Apache) también utilizan este puerto, por lo que será necesario reconfigurar el servidor web a otro puerto disponible.

Actualmente no es del todo práctico utilizar un Proxy por defecto, a menos que se trate de un servicio de “Café Internet” u oficina pequeña, siendo uno

de los principales problemas el mal uso y/o abuso del acceso a Internet por parte del personal. Por este motivo puede resultar más conveniente configurar un servidor Proxy con restricciones por usuario, lo cual no es posible realizar con un Proxy por defecto, debido a que se requiere una autenticación inicial basada en nombre de usuario y contraseña.

Regularmente algunos programas utilizados comúnmente por los usuarios suelen traer por defecto el puerto número 8080 - servicio de caché WWW - para ser utilizado al configurar el servidor Proxy. Si se desea aprovechar esta característica, se puede especificar que Squid escuche peticiones en este puerto (Barrios, 2001); manera recomendada por el autor de la guía de la instalación.

```
#Default:
http_port 8080
```

4.2.5.2. Parámetro cache_mem.

El parámetro cache_mem establece la cantidad ideal de memoria para lo siguiente:

- Objetos en tránsito.
- Objetos Hot.
- Objetos negativamente almacenados en el caché.

Los datos de estos objetos son almacenados en bloques de 4 Kb. El parámetro cache_mem especifica un límite máximo en el tamaño total de bloques ubicados, donde los objetos en tránsito tienen mayor prioridad. Sin embargo los objetos Hot y aquellos negativamente almacenados en el caché podrán accesar la memoria no utilizada hasta que esta sea requerida. En el caso de ser necesario, si un objeto en tránsito es mayor a la cantidad de memoria especificada, Squid excederá lo que sea necesario para satisfacer la petición.

Por defecto se establecen 8 MB. Puede especificarse una cantidad mayor si así se considera necesario, dependiendo esto de los hábitos de los usuarios o necesidades establecidas por el administrador.

Si se posee un servidor con al menos 128 MB de RAM, es recomendable establecer 16 MB como valor para este parámetro (Barrios, 2001).

```
#Default:
cache_mem 16 MB
```

4.2.5.3. Parámetro cache_dir – objetos de Internet almacenados en el disco duro.

Este parámetro es utilizado para determinar el tamaño deseado de cache en el disco duro para Squid. Para entender esto un poco mejor, el autor recomienda responder la siguiente pregunta: ¿cuánto se desea almacenar en

objetos de Internet en el disco duro? Por defecto Squid utilizará un cache de 100 MB, de modo tal que encontrará la siguiente línea:

```
cache_dir ufs  /cache 100 16 256
```

Se puede incrementar el tamaño del cache hasta donde lo desee el administrador. Mientras más alto se configure el valor del cache, más objetos se almacenarán en éste y por lo tanto se utilizará menos el ancho de banda. Los números 16 y 256 significan que el directorio del cache contendrá 16 subdirectorios con 256 niveles cada uno.

Es muy importante considerar que si se especifica un determinado tamaño de cache y este excede al espacio real disponible en el disco duro, Squid se bloqueará inevitablemente; motivo por el cual hay que ser cauteloso al especificar este tamaño.

4.2.5.4. Controles de acceso.

Es necesario establecer Listas de Control de Acceso para definir una red o un grupo de máquinas en particular. A cada lista se le asignará una Regla de Control de Acceso que permitirá o negará el acceso a Squid.

4.2.5.4.1. Listas de control de acceso

Regularmente una lista de control de acceso se establece siguiendo la siguiente sintaxis:

```
acl [nombre de la lista] src [lo que compone a la lista]
```

Las listas de control de acceso permiten establecer reglas para el acceso a Internet, por ende sitios web. A continuación se presentan las listas de control de acceso a Internet definidas en el proyecto de graduación.

La siguiente lista de acceso define cualquier fuente.

```
acl all src 0.0.0.0/0.0.0.0
```

La siguiente lista de acceso define el acceso a los objetos cache.

```
acl manager proto cache_object
```

La siguiente lista de acceso define al localhost.

```
acl localhost src 127.0.0.1/255.255.255.255
```

La siguiente lista de acceso define los puertos a los cuales Squid accesará.

```
acl SSL_ports port 443 563
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443 563     # https, snews
```

```
acl CONNECT method CONNECT
```

La siguiente lista de control de acceso define a la red local la cual es la única que debería tener acceso al servidor proxy.

```
acl our-networks  src 172.17.118.0/255.255.254.0
```

La siguiente lista de acceso hace referencia al contenido del archivo "/etc/squid/sitios-denegados.conf", es decir sitios web que no se permitirá el acceso.

```
acl negados url_regex "/etc/squid/sitios-denegados.conf"
```

La siguiente lista de acceso hace referencia al contenido del archivo "/etc/squid/sitios- permitidos.conf", es decir sitios web que si se permitirá el acceso.

```
acl permitidos url_regex "/etc/squid/sitios-permitidos.conf"
```

Lo siguiente define una lista de control de acceso que indica que es necesaria la autentificación de los usuarios (Barrios, 2001).

```
acl password proxy_auth  REQUIRED
```

4.2.5.4.2. Reglas de Control de Acceso

Definen si se permite o no el acceso a Squid y se aplican a las listas de control de acceso (ACL); es más si las ACL no se aplican a las reglas de acceso, éstas no tendrían sentido ya que no cumplirían ninguna función. Deben colocarse en la sección de reglas de control de acceso definidas por el administrador, es decir, a partir de donde se localiza la siguiente leyenda (Barrios, 2001):

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

La sintaxis básica es la siguiente:

```
http_access [deny o allow] [lista de control de acceso]
```

Permite el acceso a los objetos cache al localhost, o servidor de administración.

```
http_access allow manager localhost
```

Rechaza el acceso a los objetos cache a los demás.

```
http_access deny manager
```

Se rechaza el acceso a páginas que no usen protocolos considerados seguros los cuales fueron definidos en la lista de control de acceso “Safe_ports”.

```
http_access deny !Safe_ports
```

Se rechaza conectarse a puertos que no se consideren seguros.

```
http_access deny CONNECT !SSL_ports
```

Se rechaza el acceso a ciertas páginas excepto ciertas páginas conocidas.

```
http_access deny negados !permitidos
```

Se permite el acceso al localhost.

```
http_access allow localhost
```

Se le permite el acceso sólo a nuestra red

```
http_access allow our-networks password
```

Se rechaza el acceso a cualquier otra red.

```
http_access deny all
```

A continuación se presenta el contenido de los archivos “sitios-denegados.conf” y “sitios-permitidos.conf”; sitios web prohibidos y permitidos respectivamente.

Contenido del archivo “sitios-denegados.conf”

```
www.academico.com
www.lamasbuena.com
www.latinchat.com
napster
sex
porn
mp3
xxx
adult
videos
```

Contenido del archivo “sitios-permitidos.conf”

```
www.sexualidadjoven.cl
cisco.netacad.net
curriculo
```

4.2.5.5. Parámetro cache_mgr.

Por defecto, si algo ocurre con el cache del servidor se enviará un mensaje de aviso a la cuenta webmaster del servidor (administrador). Para el caso del proyecto de graduación el correo será enviado a la cuenta ingenieria@contodomiamor.com.

```
cache_mgr ingenieria@contodomiamor.com
```

4.2.5.6. Cache con aceleración.

Cuando un usuario desea realizar una petición y accesa a un objeto en Internet, éste es almacenado en el cache de Squid. Si otro usuario hace una petición hacia el mismo objeto, y éste no ha sufrido modificación alguna desde que lo accedió el usuario anterior, Squid mostrará el que ya se encontraba en el cache en lugar de volver a descargarlo desde Internet.

Esta función permite navegar rápidamente cuando los objetos ya están en el cache de Squid y además optimiza significativamente la utilización del ancho de banda.

En la sección HTTPD-ACCELERATOR OPTIONS deben habilitarse los siguientes parámetros:

```
httpd_accel_host virtual

httpd_accel_port 0

httpd_accel_with_proxy on
```

4.2.5.7. Acceso por Autentificación.

Como se indicó en las reglas de control de acceso, es necesaria la autentificación para acceder al servicio de Proxy. Para este efecto se debe crear un archivo el cual va a contener todos los usuarios y sus contraseñas encriptadas. Para el caso del proyecto de graduación se creó el archivo "/etc/squid/squid-password" realizando el siguiente comando.

```
root# touch /etc/squid/squid-password
```

Luego se debe dar permiso de lectura y escritura al propietario.

```
root# chmod 600 /etc/squid/squid-password
```

Luego asignar como propietario de este archivo al usuario squid

```
root# chown squid:squid /etc/squid/squid-password
```

Por último se deben crear las cuentas de usuario, para el efecto se usa el siguiente comando.

```
root# passwd /etc/squid/squid-password username
```

A continuación se muestra el contenido de este archivo con sus contraseñas encriptadas: (Autores, 2005)

Contenido del archivo "squid-passwd"

```
administrator:CzdFteGGDYaUw
```

```
ingenieria:4Fxm5fD759x8Y
jpintag:iuMhZhe4VvXhQ
desarrollo:NEVexKc/li8sY
proxiuser:KkJvVk36LpQKo
```

4.2.6 Inicio del servicio.

Finalmente se debe iniciar el servicio de Squid, para el efecto se puede utilizar los comandos (Barrios, 2001)

```
Service squid Start
```

o a su vez

```
/etc/rc.d/inid.d/squid Start
```

4.3 CONFIGURACIÓN SERVIDOR SENDMAIL

4.3.1 Acerca de Sendmail.

Red Hat Linux utiliza Sendmail como agente de transferencia de correo (MTA – Mail Transfer Agent) para la entrega de los mensajes, ya sean estos destinados a usuarios del mismo sistema o a usuarios ubicados en destinos remotos. La mayoría de los administradores deciden utilizar Sendmail como agente MTA por su eficacia, escalabilidad y cumplimiento con los estándares de Internet más importantes, como el protocolo SMTP.

La función principal de Sendmail, al igual que la de otros agentes MTA, es transferir de forma segura los correos electrónicos entre los servidores, normalmente mediante el uso del protocolo SMTP. Sin embargo, Sendmail es altamente configurable y permite controlar casi cada aspecto de cómo se gestiona el correo, incluído el protocolo que se va a utilizar (Barrios, 2001).

Para que *"Sendmail"* pueda ofrecer un servicio seguro, es necesario mantener siempre actualizado la versión del mismo; dado que es común encontrar debilidades producto de versiones de *"Sendmail"* no actualizadas.

4.3.2 Instalación del software necesario.

Regularmente Sendmail no se instala de manera predeterminada a menos que especifique lo contrario durante la instalación del sistema operativo, sin embargo viene incluído en casi todas las distribuciones actuales. El procedimiento de instalación es exactamente el mismo que con cualquier otro programa:

```
mount /mnt/cdrom/
rpm -Uvh /mnt/cdrom/*/RPMS/sendmail-*.i386.rpm
Ejec.
```

En el caso del proyecto de graduación se instaló sendmail-8.12.8-4, el cual viene incluído en los discos de instalación de Linux Red Hat 9.

Es importante al igual que en los otros servicios tener el último parche de seguridad disponible. La necesidad de este servidor en el proyecto es sólo para uso interno y en especial para los administradores de la red para recibir reportes de fallas en los servicios activos.

4.3.3 Configuración de Sendmail.mc

A continuación se explican las principales directivas de configuración en el archivo "/etc/mail/sendmail.mc".

En la siguiente línea, en el parámetro Addr se debe colocar la dirección IP de autocomprobación (o "*loopback*") para que sólo el mismo servidor pueda usarlo como distribuidor de correo.

```
dnl DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1,  Name=MTA')
```

La directiva CW permite indicar el nombre del dominio de red a ser utilizado.

```
Cwcontodomiamor.com
```

4.3.4 Configuración de Access.

En el archivo de configuración "/etc/mail/access" se definen los otros servidores permitidos para que utilicen el servidor de Sendmail como

distribuidor de correo, ningún servidor que no esté definido en este archivo podrá utilizar esta funcionalidad.

Contenido del archivo "access"

```
# Check the /usr/share/doc/sendmail/README.cf file for a description
# of the format of this file. (search for access_db in that file)
# The /usr/share/doc/sendmail/README.cf is part of the sendmail-doc
# package.
#
# by default we allow relaying from localhost...
localhost.localdomain          RELAY
localhost                      RELAY
127.0.0.1                      RELAY
200.10.149.133                 RELAY
172.17.118.0/23                RELAY
```

4.3.5 Aplicar los cambios en la configuración.

Para que los cambios se vean reflejados en el archivo "/etc/mail/sendamil.cf" se debe ejecutar el siguiente comando.

```
m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
```

4.3.6 Configuración POP3

Para que los usuarios de un grupo determinado, en el caso del proyecto de graduación – usuarios de ingeniería - puedan descargar correos electrónicos

en sus máquinas es necesario habilitar el protocolo pop3 para lo cual se debe editar el archivo "/etc/xinet.d/ipop3", activando este servicio. Luego de la edición el archivo en mención se verá de la siguiente manera:

Contenido del archivo "ipop3"

```
# default: off
# description: The POP3 service allows remote users to access their mail \
#              using an POP3 client such as Netscape Communicator, mutt, \
#              or fetchmail.
service pop3
{
        disable                 = no
        socket_type             = stream
        wait                    = no
        user                    = root
        server          = /usr/sbin/ipop3d
        log_on_success      += HOST DURATION
        log_on_failure      += HOST
}
```

4.3.7 Inicio del servicio.

Finalmente se deben iniciar los servicios de Sendmail e ipop3, para el efecto se pueden utilizar los comandos:

```
Service sendmail Start
Service xinetd restart
```

O a su vez:

```
/etc/rc.d/inid.d/sendmail  Start
/etc/rc.d/inid.d/xinetd  Restart
```

4.4 CONFIGURACIÓN SERVIDOR WEB LINUX-APACHE

4.4.1 Servidor Web Seguro (Apache).

Para la implementación del servidor Web Seguro se instaló como servicio Web la versión de apache más estable, la versión 1.3.31 sobre Red Hat Linux 9; utilizando complementos de seguridad tales como el SSL (Security Socket Layer) a través de OpenSSL en su versión 0.9.7 y para poder integrar el módulo de SSL con apache se utilizó el ModSSL en su versión 2.8.17.

Debido que la programación Web está basada en el lenguaje PHP, también se instaló el soporte para páginas php usando php 4.3.8. Además se instaló librerías gráficas debido a que se manejan gráficos dinámicos en la programación.

El detalle de instalación que se muestra a continuación tiene como fuente de investigación documentos disponibles en internet de los cuales se pueden destacar los siguientes:

http://www.linux-cd.com.ar/manuales/rh9.0

http:///www.hostlibrary.com

A continuación se detallará paso a paso la instalación del servidor Web seguro.

4.4.2. Pasos previos a la Instalación.

Debido a que el servidor que se va a instalar debe tener soporte para la base de datos Oracle es necesario hacer unos pasos previos antes de realizar la instalación de php.

4.4.2.1. Instalar ORACLE_HOME

Para que la instalación Php-Oracle sea exitosa es necesario montar (mapear) en una carpeta del servidor web la carpeta donde esta el home de Oracle en el servidor de Base de datos. Para eso se usa el servicio NFS.

```
mount –t nfs 192.168.15.5:/u01/app/oracle/9i /u01/app/oracle/9i
```

4.4.2.2. Configurar variable de ambiente

Tanto para la instalación o para que el servicio Web esté activo es necesario indicar dónde se ubica el “home” (ruta de unix donde residen los archivos de la base de datos) de Oracle. Para hacer esto se necesita asignar la variable de ambiente (“ORACLE_HOME”) para el usuario “root” (usuario privilegiado). Para efectuar esto se edita el archivo “/root/.bashrc” y se agrega la siguiente línea.

```
export ORACLE_HOME=/u01/app/oracle/9i
```

4.4.2.3 Instalación del servidor Web.

Pasos iniciales:

- Conectarse como root y cambiar al directorio source.

```
cd /usr/local/src
```

- Obtener los siguientes paquetes “tar” (extensión que identifica archivos comprimidos en Linux) disponibles en internet.

```
http://www.php.net/distributions/php-4.3.8.tar.gz
http://httpd.apache.org/dist/httpd/apache_1.3.31.tar.gz
http://www.modssl.org/source/mod_ssl-2.8.17-1.3.31.tar.gz
http://www.openssl.org/source/openssl-0.9.7d.tar.gz
```

- Desempaquetar o descomprimir las aplicaciones.

```
tar  z xvf  php-4.3.8.tar.gz
tar zxvf  apache_1.3.31.tar.gz
tar zxvf  mod_ssl-2.8.17-1.3.31.tar.gz
tar zxvf  openssl-0.9.7d.tar.gz
```

Lo cual genera la siguiente estructura en Linux:

```
/usr/local/src/php-4.2.3.8
/usr/local/src/apache_1.3.31
/usr/local/src/openssl-0.9.7d
/usr/local/src/mod_ssl-2.8.17-1.3.31
```

- Instalar Open SSL

```
cd /usr/local/src/openssl-0.9.7d
./config --prefix=/usr/local/openssl
make
make test
make install
```

- AplicarParche de mod_ssl al Apache

```
cd /usr/local/src/mod_ssl-2.8.17-1.3.31
./configure --with-apache=../apache_1.3.31
```

- Instalar Apache con soporte SSL y DSO

```
cd /usr/local/src/apache_1.3.31
CFLAGS="-DEAPI"
export CFLAGS
SSL_BASE=../openssl-0.9.7d ./configure --
prefix=/usr/local/apache\
--enable-module=ssl \
--enable-shared=ssl \
--enable-shared=max \
--enable-module=so
make
make certificate
make install
```

- Instalar Php.

```
cd /usr/local/src/php-4.2.3.8
CFLAGS='-O2 -I/usr/local/src/openssl-0.9.7d -DEAPI' \
./configure \
--with-apxs=/usr/local/apache/bin/apxs \
--with-oci8=$ORACLE_HOME \
--with-gd=../gd-2.0.28 –with-png=/usr/lib \
--with-freetype=/usr/lib \
```

```
--enable-track-vars  \
--with-xml
make
make install
cp php.ini-dist /usr/local/lib/php.ini
```

Las librerías gd son librerías de soporte gráfico y las librerías frretype se utilizan para poder crear gráficos dinámicos.

- Editar el archivo config de Apache e iniciar el servidor web

```
cd /usr/local/apache/conf
vi httpd.conf
```

- Remover el signo # al inicio de las siguientes líneas

```
#AddType application/x-httpd-php  .php
#AddType application/x-httpd-php-source  .phps
```

- Agregar index.php a la lista válida de archivos directorios index

```
<IfModule  mod_dir.c>
DirectoryIndex  index.php  index.htm  index.html
</IfModule>
```

4.4.3 Iniciar el Servicio.

Para poder iniciar Apache como un servidor habilitado SSL se debe ejecutar el comando

```
/usr/local/apache/bin/apachectl  startssl
```

Proporcionar el *"PassPhrase"* (Frase Secreta) y el servicio será iniciado. Algo muy importante que se debe recordar es que antes de iniciar el servicio de apache se debe montar el directorio *"Home"* de Oracle usando NFS.

```
mount –t nfs 192.168.15.5:/u01/app/oracle/9i  /u01/app/oracle/9i
```

Para detener el servicio simplemente se usa el siguiente comando.

```
/usr/local/apache/bin/apachectl  stop
```

4.5 CONFIGURACIÓN SERVIDOR BASE DE DATOS ORACLE

Se utilizará el motor de base de datos relacional ORACLE 9i, instalado sobre sistema operativo Linux con Red Hat v.9.

4.5.1 Introducción

El objetivo de este manual es poder realizar una instalación adecuada de una base de datos robusta como es Oracle en su versión 9.2.1.0 sobre el sistema operativo Red Hat Linux 9, este esquema Linux-Oracle va a permitir manejar un sistema confiable a nivel de base de datos y se va a poder implementar

todas las seguridades que brinda el trabajar sobre un sistema operativo Linux.

La fuente de esta instalación es Dizwell Informatics y su autor es Howard J. Rogers.

4.5.2 Red Hat e Instalación del Oracle

Lo primero que se debe tener claro es que la versión 9i del Oracle no está certificada sobre Red Hat 9 por lo que se puede encontrar inconvenientes en la instalación que deben ser corregidos para poder garantizar un buen funcionamiento de la base de datos.

Se necesita al menos 256 MB de RAM en la máquina que va a ser el servidor de la Base de Datos y por lo menos 4gb de espacio en disco. No se necesita tener instalado el Java Development Kit, o Java Runtime Engine o cualquier herramienta relacionada con Java.

Se recomienda empezar formateando el disco y arrancar una nueva instalación del Sistema Operativo Red Hat 9.0 antes de iniciar la instalación de la base de datos.

4.5.2.1 Obteniendo el Programa.

Se debe obtener la versión gratuita de Red Hat 9 y los 3 cd's de instalación del oracle que se pueden bajar de la siguiente dirección http://technet.oracle.com.

Como se va a usar la versión gratuita de Red Hat se debe también descargar los siguientes archivos.

Glibc-2.3.2.5.i386.rpm
Glibc-common-2.3.2.5.i386.rpm
Glibc-devel-2.3.2.5.i386.rpm

Esto es necesario porque la versión gratuita de Red Hat viene con una versión del glibc que no funciona con el instalador del oracle, así que será necesario esta actualización de librerías.

4.5.2.2 Instalando Red Hat 9.0

Lo primero que solicita el instalador del Red Hat es que se escoga el tipo de instalación, se recomienda escoger la instalación ("Workstation") debido a que ésta contiene archivos necesarios para la correcta instalación de la base de datos.

Luego es necesario personalizar que conjunto de opciones se va a instalar, en este punto es importante que en la sección de (“Development”), se escoja las siguientes opciones: (“Development Tools, X Software Development, Gnome Software Development”).

De aquí en adelante se debe dar “click” [24] en (“Next”) en cada una de las opciones y esperar que la instalación concluya, al final se solicitará que se reinicie el equipo.

Al reiniciar el equipo el Red Hat solicitará la creación de una cuenta, esto no es necesario debido a que esto se lo va a administrar con la base de datos y para esto se debe utilizar el usuario “root”.

4.5.2.3 Compilando las librerías glibc

Como se mencionó en un párrafo anterior es necesario la compilación de las librerías glibc especificadas en la versión 2.3.2.5.

Se debe abrir una terminal y escribir lo siguiente

```
rpm –q glibc-2.3.2-5 glibc-common-2.3.2-5 glibc-devel-2.3.2-5
```

[24] Acción del mouse sobre algún lugar específico en la pantalla.

Se debería ver los siguientes mensajes de error.

```
package glibc-2.3.2-5 is not installed
package glibc-common-2.3.2-5 is not installed
package glibc-devel-2.3.2-5 is not installed
```

En este punto se sabe que hay un problema, si no se toma una acción en este momento puede que luego se tenga algun inconveniente en la instalación o en el funcionamiento de la base de datos.

Una vez que se ha obtenido los glibc se debe instalar de la siguiente manera.

```
rpm –Uvh –oldpackage glibc-2.3.2.5.i386.rpm glibc-common-2.3.2.5.i386.rpm
glibc-devel-2.3.2.5.i386.rpm
```

4.5.2.4 Preparando la instalación en Modo Gráfico

Oracle viene en 3 Cd's que se deben bajar de la siguiente dirección de internet: http://technet.oracle.com.

Se debe conectar como "root" y crear un directorio llamado "/oraclesource" y copiar cada uno de los cd de instalación.

```
mkdir /oraclesource
cp /mnt/cdrom* /oraclesource (Repetir por cada Cd )
```

Una vez que se haya realizado se debe comprobar si efectivamente se realizó la copia a disco de esta instalación.

```
ls  /oraclesoruce
```

El resultado debe ser el siguiente

```
lnx_920_disk1.cpio.gz
lnx_920_disk2.cpio.gz
lnx_920_disk3.cpio.gz
```

Ahora se procede a descomprimir los archivos

```
cd /oraclesoruce
gunzip  *.gz
```

El resultado debe ser lo siguiente

```
lnx_920_disk1.cpio
lnx_920_disk2.cpio
lnx_920_disk3.cpio
```

Se procede a desempaquetar los archivos cpio.

```
cpio –idmv < lnx_920_disk1.cpio
```

Se necesita repetir este comando para cada uno de los archivos y se debe comprobar por cada uno de ellos el número de bloques, estos deben ser (“ 1316436 bloques”) para el Cd 1, (“1177771 bloques”) para el Cd 2 y (“900067 bloques”) para el 3.

Si no se tiene exactamente estos números algún error tienen los instaladores y es mejor buscar la solución y no avanzar con la instalación.

Ahora si se revisa se tendrá creados 3 subdirectorios llamados Disk1, Disk2 y Disk3.

4.5.2.5 Asignando los parámetros del kernell

Este es un paso realmente importante, si se omite el mismo no pasarán ni tres minutos en que la instalación abortará con el error siguiente:
(“ORA-3031 End of file on Communication Channel error o el error ORA-27123 unable to attach to shared memory segment.”)

El asunto es que la instancia del Oracle consume la memoria compartida, y el Red Hat en base a su configuración asigna estos valores, de manera que si estos valores no son suficientes, simplemente el Oracle no puede trabajar.

Afortunadamente esto se soluciona alterando dos parámetros del kernel, estos son (“SHMMAX y SEM “).

“SHMMAX” es la máxima cantidad de memoria compartida que una aplicación puede utilizar, en Oracle se recomienda que se asigne la mitad de la memoria física “RAM”. Sin embargo si se está trabajando con un “PC” con 256 mb de ram instalado, con un 128 mb en el parámetro “SHMMAX” es más que suficiente.

“Sem” representa cuántos semáforos una aplicación puede usar. Para cambiar los parámetros hay que editar el archivo llamado “/etc/sysctl.conf”, se debe abrir con un editor de texto y cambiarlo de la siguiente manera

```
kernel.shmmax = 2147483648
kernel.sem = 250 32000 100 128
```

Se debe tener cuidado al poner estos valores, especialmente en el “sem” ya que hay que respetar el espacio en blanco entre cada número.

Para que los cambios tomen efecto es necesario reiniciar el equipo o ejecutar las siguientes instrucciones.

```
cd /proc/sys/kernel
```

```
echo 2147483648 > shmmax
echo 250 32000 100 128 > sem
```

4.5.2.6 Creando un propietario de la instalación.

No se puede instalar el Oracle como root, esta es una mala práctica y la seguridad se ve comprometida al administrar la base con este usuario tan privilegiado.

Se debe crear el usuario “oracle” quien será el propietario de la instalación. Ingresando como root se debe abrir una terminal y ejecutar lo siguiente:

```
groupadd dba
groupadd oinstall
groupadd oracle
useradd –g oinstall –G dba, oracle –m oracle
```

Ahora se debe asignar el password, al digitar:

```
passwd oracle
```

4.5.2.7 Creando una localidad para la instalación

Los ejecutables del oracle deben estar físicamente en algún lugar, y una buena idea es crear una localidad especial para mantener estos archivos identificables.

Se necesita crear un directorio principal y varios subdirectorios con sus correctos propietarios y permisos, digitar los siguientes comandos.

```
mkdir /opt/bin
chown oracle:dba /opt/bin
mkdir /u01
mkdir /u01/app
mkdir /u01/app/oracle
mkdir /u01/app/oracle/9i
chown –R oracle:dba /u01/app/oracle
```

Nótese que el usuario oracle ha sido declarado como propietario de estas localidades esto evitará fallas en la instalación por permisos.

4.5.2.8 Asignando las variables de ambiente

Finalmente se necesita asignar las variables de ambiente que el usuario oracle va a usar.

Se debe editar el archivo .bashrc que se encuentra en el directorio home del usuario oracle.

```
cd /home/oracle
gedit .bashrc
```

Debe verse lo siguiente

```
#. Bashrc
# User specific aliases and functions
# Source global definitions
if [ -f /etc/bashrc ] ; then
        . /etc/bashrc
fi
```

Las modificaciones que se deben hacer van entre las líneas (“#User specific aliases and functions”) y la línea (“#Source global definitions”). Las líneas que se debe agregar son:

```
export ORACLE_SID=lx92
export ORACLE_BASE=/u01/app/oracle
export ORACLE_HOME=/u01/app/oracle/9i
export NLS_LANG=AMERICAN_AMERICA.WE8ISO8859P1
export ORA_NLS33=$ORACLE_HOME/ocommon/nls/admin/data
export LD_LIBRARY_PATH=$ORACLE_HOME/lib:/lib:/usr/lib:/usr/local/lib
export PATH=$ORACLE_HOME/bin:/opt/bin:/bin:/usr/bin:/usr/local/bin:
/usr/sbin:/usr/X11R6/bin:/usr/local/java/bin:.
export JAVA_HOME=/usr/local/java
export
CLASSPATH=$ORACLE_HOME/jdbc/lib/classes12.zip:$ORACLE_HOME/JR
```

```
E:$oracle_home/jlib:$ORACLE_HOME/rdbms/jlib:$ORACLE_HOME/network/
jlib:.
Export LD_ASSUME_KERNEL=2.4.1
Export THREADS_FLAG=native
```

Se debe verificar que no se haya omitido nada al tipear estas líneas, en particular el PATH y el CLASSPATH, estas líneas no deben tener espacios en blanco.

El ORACLE_SID identificará el nombre de la instancia cuando finalmente se cree la base de datos.

Hay dos líneas importantes para la instalación sobre Red Hat y estas son: LD_ASSUME_KERNEL y THREADS_FLAG estos parametros no son importantes en Red Hat 8 pero son vitales en Red Hat 9 y permiten el manejo de hilos en los procesos relacionadas con la base de datos.

Finalmente se debe grabar el archivo y chequear si todo está trabajando correctamente conectándose con el usuario oracle y tipeando

```
echo $ORACLE_HOME  desde una terminal.
```

Se debe revisar las otras variables como por ejemplo:

```
echo $PATH
```

```
echo $ORACLE_SID
```

Si se ve que esto ocasiona error se debe revisar el .bashrc hasta dar con el problema para continuar con los siguientes pasos.

4.5.2.9 Empezando la instalación

Ahora se puede empezar la instalación. Se debe ingresar al sistema con el usuario “oracle” y tipear lo siguiente desde una terminal.

```
/oraclesource/Disk1/runInstaller
```

Cambiar el “path” (dirección) aquí si es necesario. Después de una pausa se verá la pantalla de Bienvenida, donde al dar (“next”) aparecerá la siguiente pantalla.

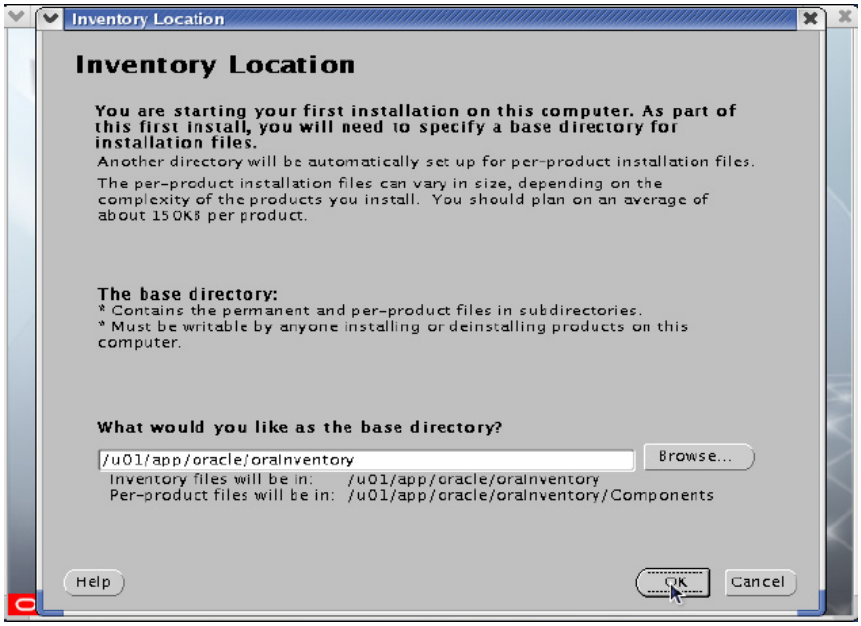

Fig 4.1 Bienvenida de instalación
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

El instalador almacena información acerca de que se está instalando y donde, en varios archivos los cuales juntos se conocen como el inventory. En esta pantalla se debe confirmar donde el inventory debería ser creado.El instalador sugiere una buena ruta que es el “$ORACLE_BASE/oraInventory”, se recomienda que la uses de esa manera y se dé (“Next”).

Pudiera ocurrir un error en este instante y se deberá revisar el archivo “.bashrc” para poder continuar.

Asumiendo que todo estuvo correcto, la siguiente pantalla es

Fig 4.2 Ingreso de Grupo de Administrador
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

Aquí se tiene que decidir en Linux cuál es el grupo que va a administrar los privilegios para la instalación. Basado en que se está trabajando con el usuario “oracle” el grupo debería ser “dba”, al digitar (“next”) se encontrará lo siguiente:

Fig 4.3 Privilegio de grupo
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

Para hacer del grupo “dba” un grupo privilegiado, se debe entrar como “root” y correr un programa que nos proporciona el oracle que hace los cambios necesarios.

Digitar:

```
Oracle > su –

Password : xxxxx

root > /tmp/orainstRoot.sh
```

Cuando el programa se complete se debe regresar a la pantalla de la instalación y dar (“Continue”).

Se debe ver lo siguiente ahora:

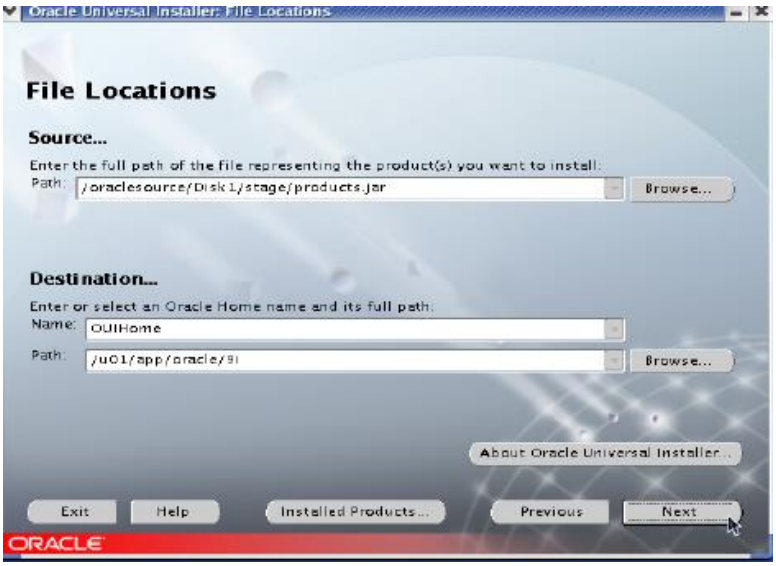

Fig 4.4 Ruta de los Archivos
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

El propósito de destino para la instalación debe ser "/u01/app/oracle/9i" y si el archivo ".bashrc" es correcto esta será la sugerencia que da el instalador, se aconseja no cambiar los valores recomendados.

Ahora se verá la pantalla de los productos disponibles para instalar, como se está instalando la base de datos se debe escoger la primera opción que es ("Oracle Database 9.2.0.1.0").

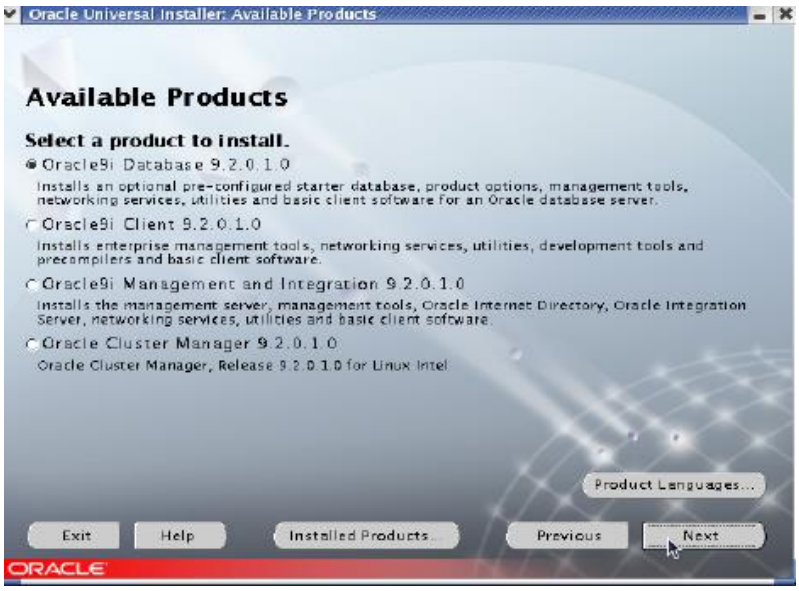

Fig 4.5 Productos Disponibles
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

Al dar click en (“next”) se preguntará por el tipo de instalación a seguir, hay dos tipos la versión enterprise y al versión estandar.

La versión estandar es mucho más pequeña que la enterprise, por eso se recomienda escoger la entreprise pero hay que tomar en cuenta que por ser una versión gratuita no se podrá contar con todos los extras que una versión enterprise licenciada puede ofrecer.

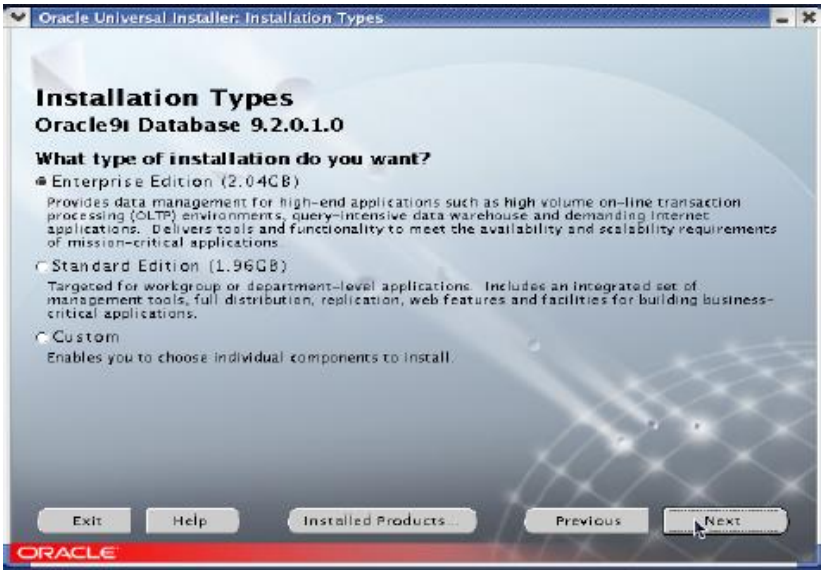

Fig 4.6 Tipos de Instalación
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

Luego de esto se tiene una pantalla que da varias opciones de configuración para la base de datos, se debe escoger la opción (“Sofware Only”) y seleccionar (“Next”), y esto permitirá ver todo lo que se instalará con la base.

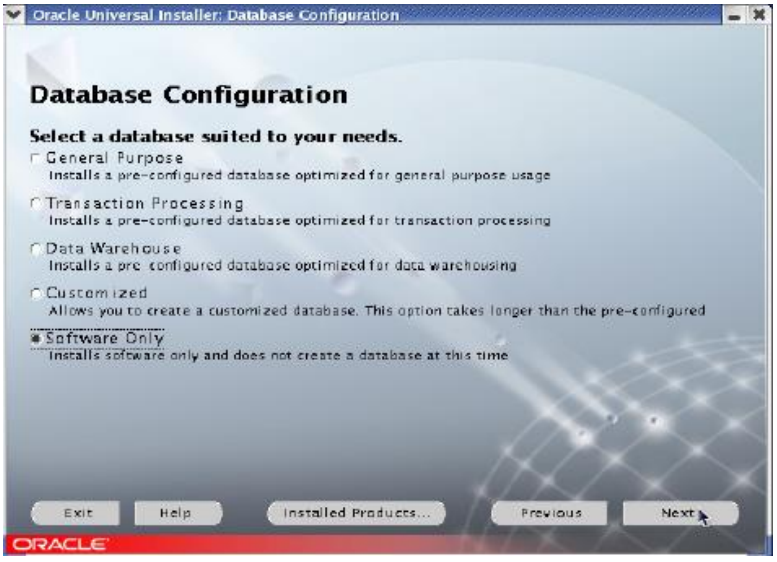

Fig 4.7 Configuración de la Base de Datos
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

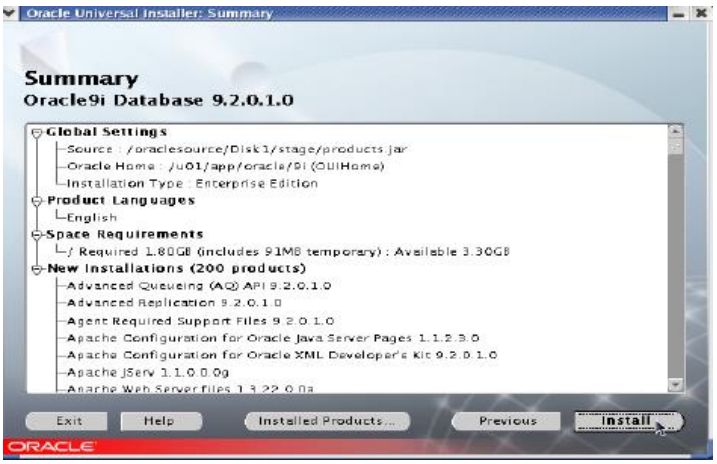

Fig 4.8 Sumario de la instalación
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

Finalmente se verá la siguiente pantalla, realmente la instalación tiene dos partes que son el instalado y la fase de enlace, realmente en el instalando no se va a encontrar ninguna novedad, más bien la fase de enlace es lo más complejo ya que aquí se efectúan las compilaciones y trabajan los ejecutables.

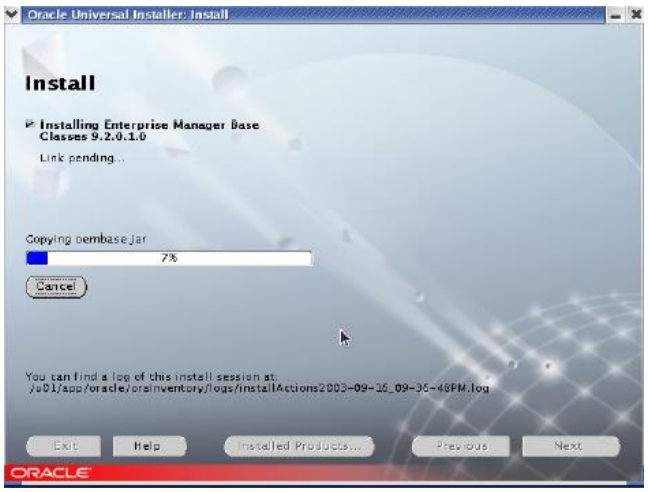

Fig 4.9 Avance de instalación
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

4.5.2.10 Errores durante la Fase de enlace.

El primer error posible que se puede presentar es en el “61%” del avance y es el siguiente (“Error in invoking target install of make file /xx/xx/ins_oemagent.mk”), si este error se llega a dar se debe abandonar la instalación y volver a reinstalar las librerías “glibc” ya que este error se produce cuando estas librerías no son las correctas. No omitir el error, es necesario corregirlo.

El otro error que puede ocurrir es en el 84% de la instalación y es el siguiente (“Error in invoking target install of make file /xx/xx/ins_oemagent.mk”).

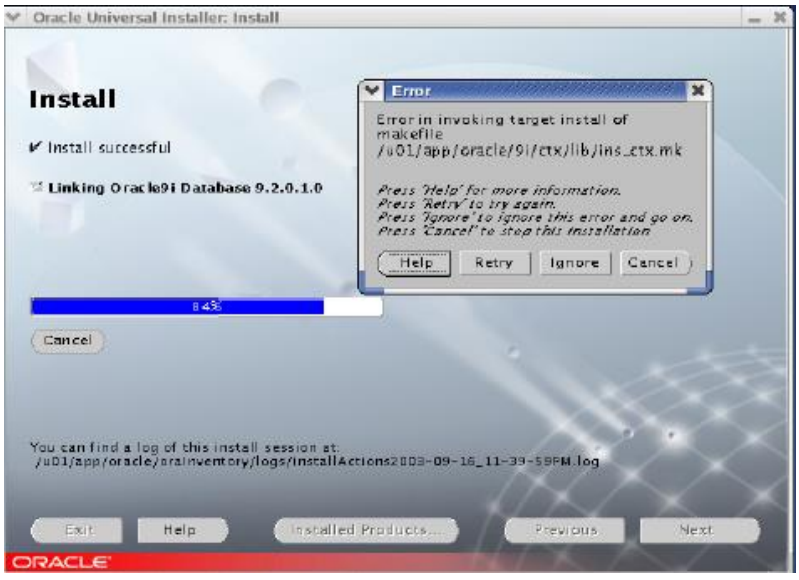

Fig 4.10 Error en la instalación
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

Afortunadamente este error tiene solución de la siguiente manera, abrir el archivo “env_ctx.mk”.

```
cd $ORACLE_HOME/ctx/lib
gedit env_ctx.mk
```

Ahora con el editor se necesita encontrar la siguiente línea

```
INSO_LINK  = -L$(CTXLIB)  $ (LDLIBFLAG)m $(LDLIBFLAG)sc_ca
```

Y cambiar por la siguiente línea:

```
INSO_LINK  = -L$(CTXLIB)  $ (LDLIBFLAG)m  $(LDLIBFLAG)dl
$(LDLIBFLAG)sc_ca
```

Una vez finalizada la corrección hay que grabar el cambio, volver a la pantalla de instalación y seleccionar (”Retry”).

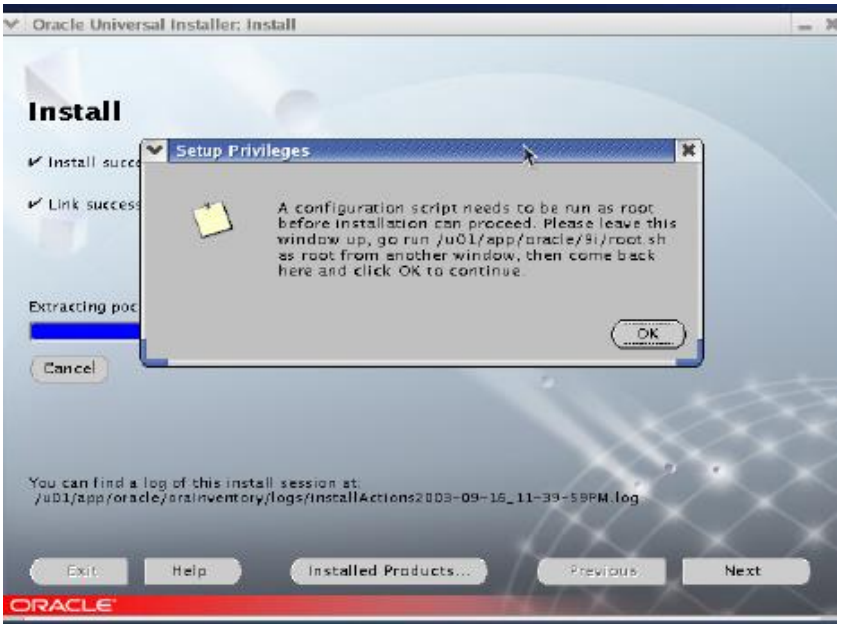

Fig 4.11 Ejecución de programa como root
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

Al finalizar la instalación se debe correr un "*script*" como "root":

Abrir una terminal y ejecutar:

```
Oracle > su –

Password: xxxxx

root > /u01/app/oracle/9i/root.sh
```

Al finalizar el "*script*" volver a seleccionar ("ok") en la pantalla de instalación y finalmente la instalación se ha realizado, se está listo para arrancar con la creación de la base de datos.

Fig 4.12 Final de Instalación
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

4.5.3 Creando la Base de Datos

4.5.3.1 Ejecutando el DBCA

Para empezar la creación de la base de datos hay que ingresar a una sesión del linux con el usuario “oracle” y digitar “dbca”, esta instrucción permite correr el asistente de configuración de la base de datos sobre esta plataforma donde Oracle está corriendo.

Después de unos minutos en el que el ambiente “java runtime” es ejecutado se observará la primera pantalla de bienvenida indicando que el asistente te permitirá crear o borrar una base de datos, dar click en el botón (“next”) para continuar.

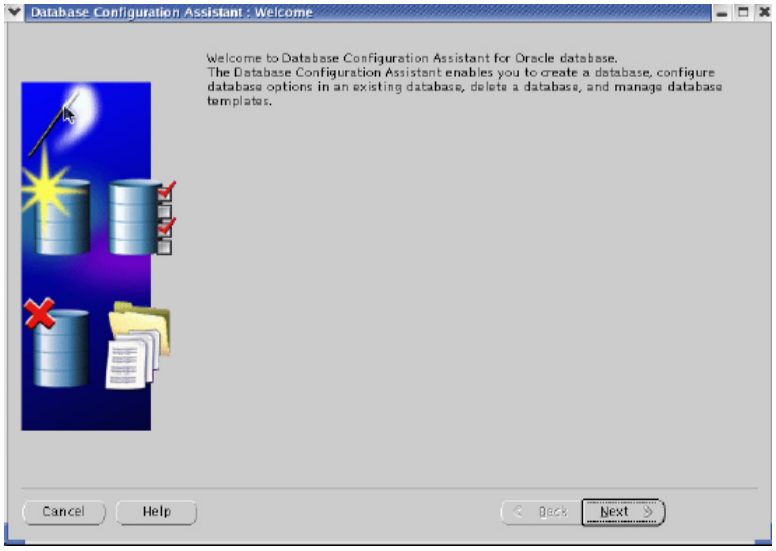

Fig 4.13 Asistente de configuración para la Base de Datos
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

La siguiente pantalla presenta las opciones a las que se puede acceder, en este caso se debe escoger la opción Create Database es decir la creación de la base de datos. Seleccionar (“Next”).

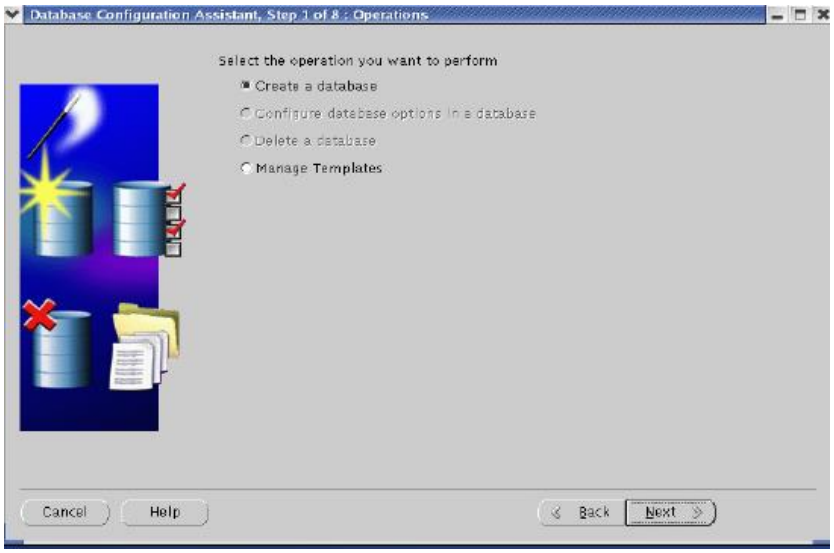

Fig 4.14 Tipo de Operación a realizar
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

El asistente ahora desea saber qué tipo de base de datos se quiere crear, las tres primeras opciones originan que el asistente clone una base de datos desde sus plantillas preestablecidas en cambio que la cuarta opción es inflexible porque si el Oracle especifica algunos parámetros como por ejemplo el tamaño de la base de datos o las opciones de funcionalidad, no se podrán cambiar las mismas.

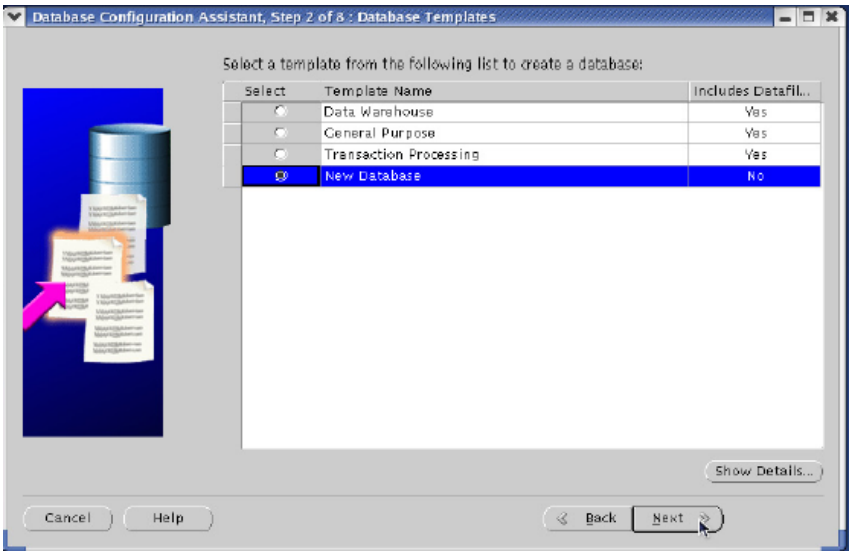

Fig 4.15 Elección de Plantilla
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

Se debe escoger la cuarta opción (“New Database”) es decir crear nueva base de datos y seleccionar (“next”).

En la siguiente pantalla, toda base de datos necesita un nombre y ahora se lo debe escoger. El nombre que se escoja debe ser el mismo que fue asignado

en el “ORACLE_SID”, y el dominio debe ser configurado para el esquema del proyecto (“contodomiamor.com”).

Digitar en el “Global Database Name” : “lx92.contodomiamor.com” y en el “SID”: “lx92”.

Se debe tener cuidado con las mayúsculas y minúsculas pues Oracle es sensitivo a las mismas.

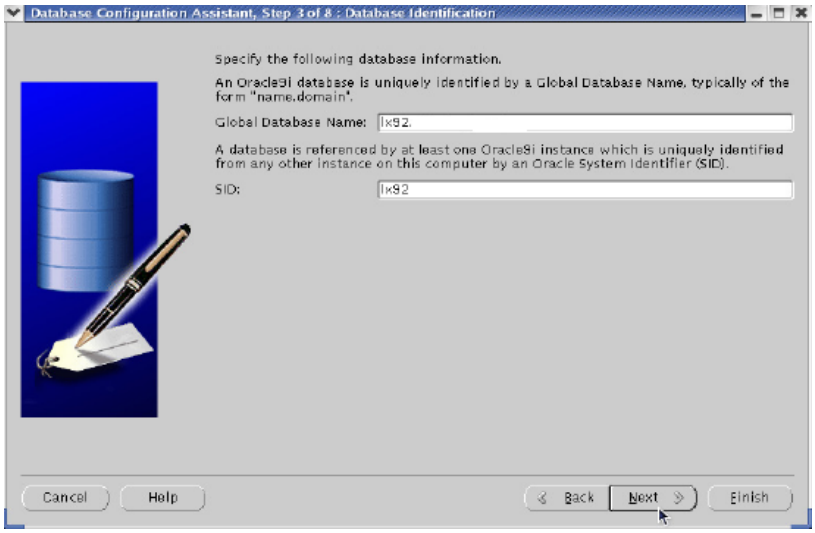

Fig 4.16 Ingreso de nombre de la base de datos
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

Seleccionar (“next”).

Ahora con la lista de opciones disponibles para la base de datos, hay que evaluar el tipo de licencia con la que se cuenta y el espacio disponible en el servidor.

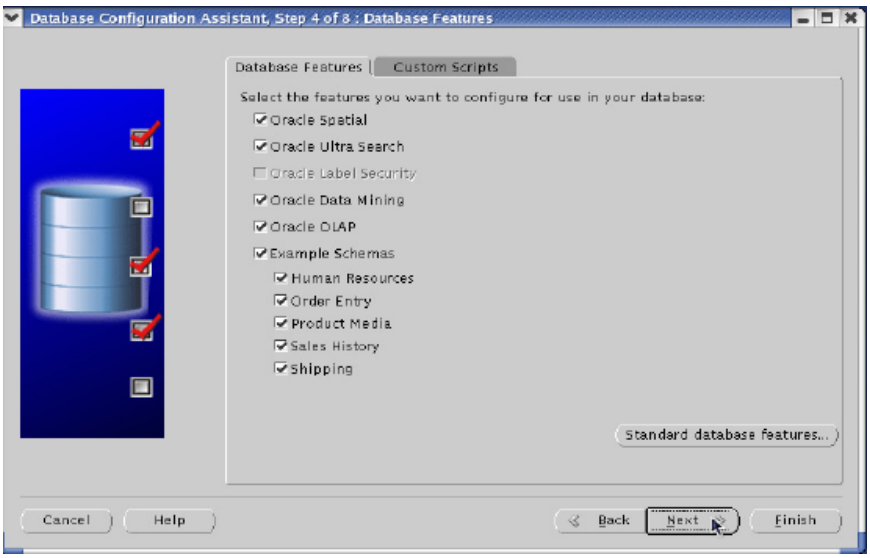

Fig 4.17 Funcionalidad de la base de datos
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

No hay que sorprenderse si salen mensajes de advertencia como el siguiente que indica que no hay espacio asignado para esta opción, en este caso se debe seleccionar un espacio para que trabaje apropiadamente o simplemente quitar la selección de esta opción.

Para el caso del proyecto y tomando en cuenta el gran tamaño de disco del servidor, se han escogido todas las opciones que salen habilitadas por cuestiones de licencia, inclusive hasta los ejemplos de esquemas de bases.

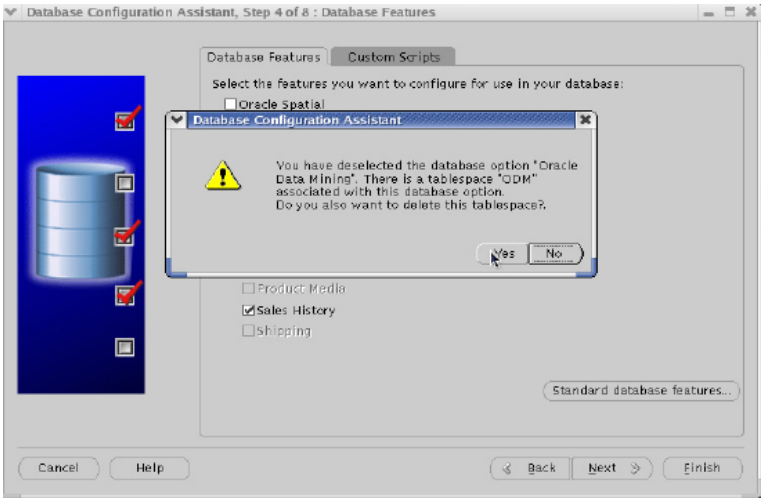

Fig 4.18 Asignar espacios en tablas
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

Seleccionar ("next").

Ahora se debe escoger el modo en el que el servidor actuará en el esquema, aquí hay dos opciones: la una es como servidor dedicado y la otra en modo compartido.

El servidor dedicado se debe usar cuando los clientes persistentemente se conectan a la base de datos, mientras que en modo compartido se recomienda cuando un número reducido de usuarios acceden a la base de datos.

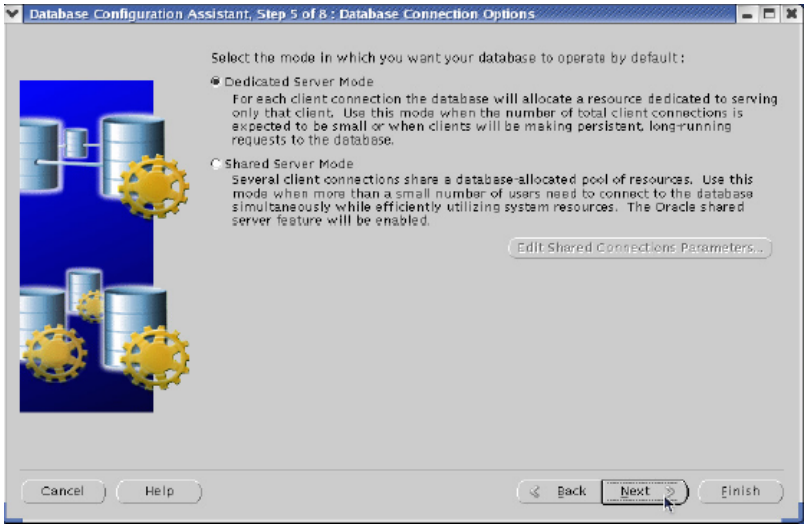

Fig 4.19 Tipo de Conexión
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

Escoger la opción servidor dedicado y seleccionar (“next”).

Es ahora donde el asistente empieza a ponerse más técnico y a recomendar medidas de parámetros, no siempre el asistente es la última palabra hay que analizar el impacto de estas configuraciones.

Primero se tiene que definir la cantidad de memoria que la instancia de Oracle va a tener, usualmente se debe ser generoso con este parámetro tomando en cuenta la cantidad de memoria disponible en el servidor, el manual recomienda mínimo 176 MB de RAM, pero lo ideal es 512.

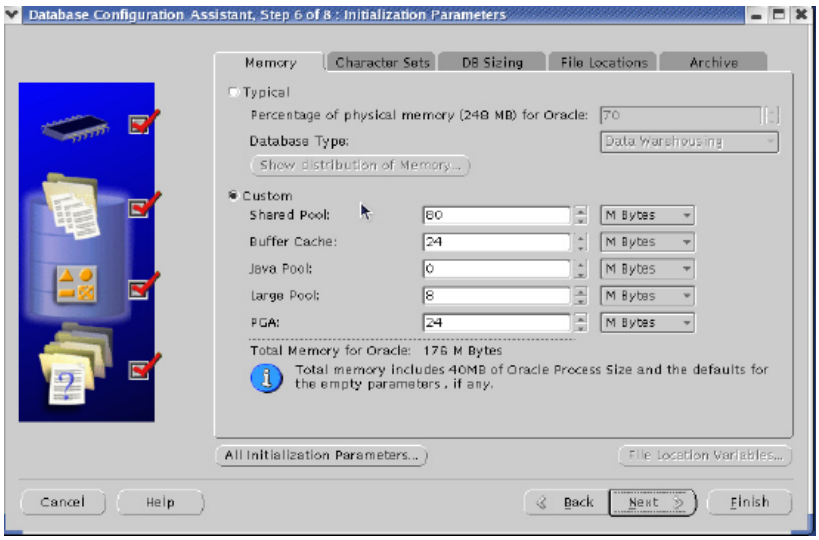

Fig 4.20 Parámetros de la Base de datos
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

Seleccionar la siguiente carpeta de esta pantalla.

El siguiente punto es para resolver el estandar de caracteres que la base va a manejar.

Toda base de datos Oracle tiene dos opciones: el “conjunto de caracteres” y el “conjunto nacional de caracteres”

Este conjunto de caracteres es configurado en las variables de ambiente y para el caso se debe usar el “default”[25] que indica la base y usar el conjunto nacional de caracteres UTF8[26] ya que representa los caracteres en inglés que usan cuatros bytes de longitud para representarlos mientras que la opción con 16 utiliza el doble lo cual sería un desperdicio de bytes.

[25] Valor por defecto
[26] UTF8: Universal Transformation Format, un método de convertir Unicode a 8 caracteres

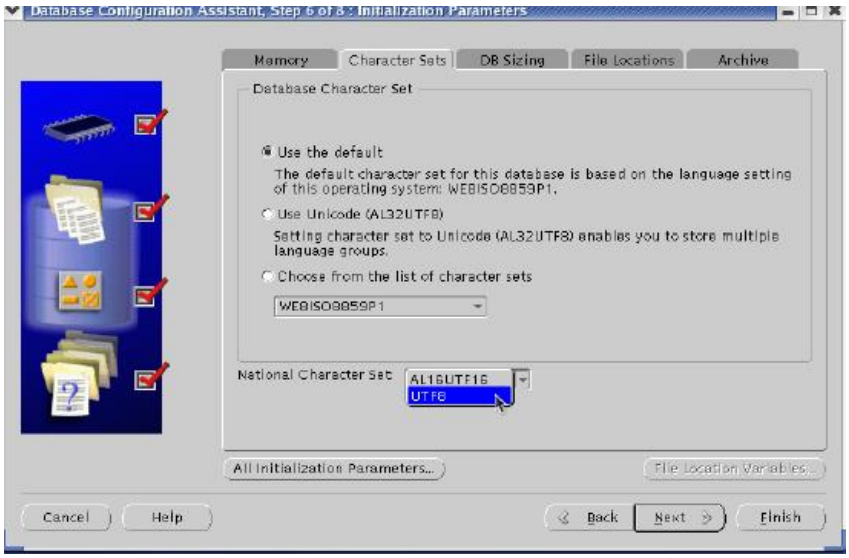

Fig 4.21 Manejo de caracteres
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

Seleccionar la siguiente carpeta.

En esta parte de la instalación el asistente propone que Oracle use 8k por cada bloque, pero lo recomendable es 4 ya que este tamaño de bloque es la unidad utilizada en cada entrada y salida que hace la base de datos, ahora si se lo relaciona con el sistema operativo este trabaja con 4k como unidad lo cual si se configura 8k para la base de datos serían 2 llamadas al archivo de sistema.

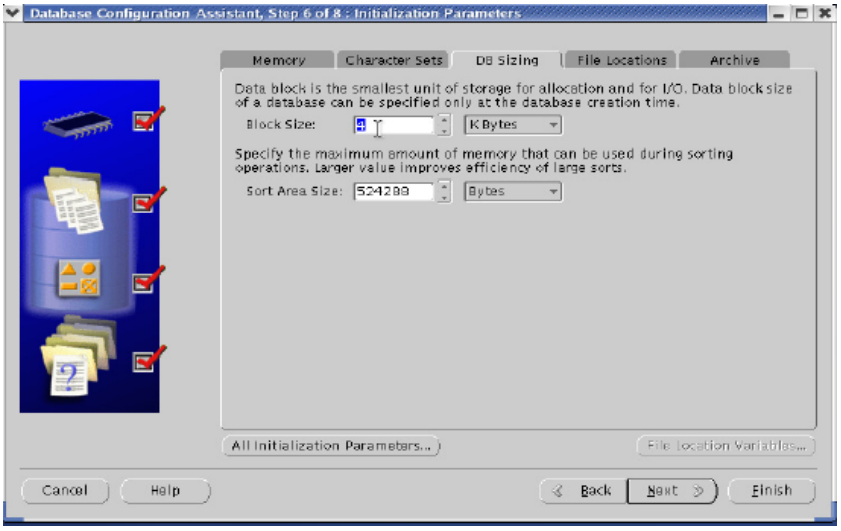

Fig 4.22 Asignar tamaño de bloques
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

Ahora se debe escoger la siguiente carpeta en la que se define los directorios para procesamiento del usuario, logs, aquí se ve la importancia de las variables de ambiente en la instalación del Oracle, si fue correctamente realizado, se debe aceptar en esta opción los valores por defecto propuestos por el asistente.

Seleccionar la siguiente carpeta.

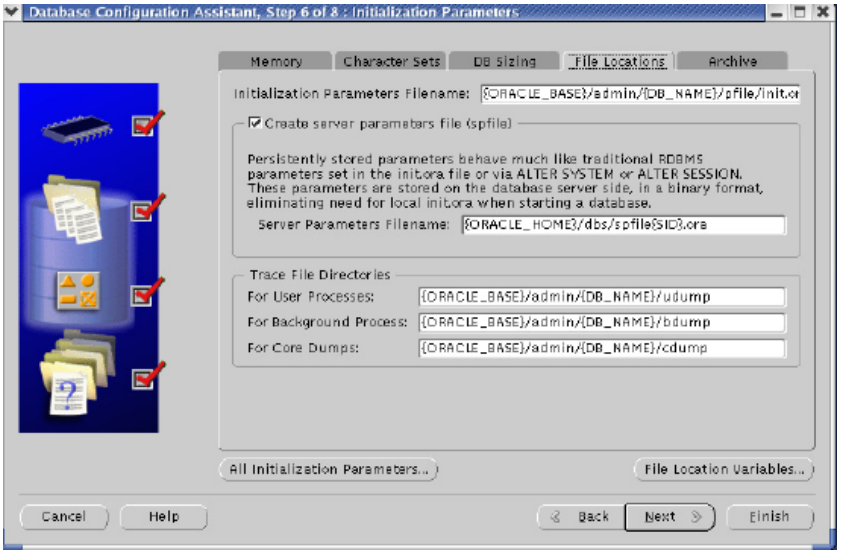

Fig 4.23 Directorios de procesamiento
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

En esta opción no hay mucho que hacer o cambiar, aquí se define si se usa archivos de logs que van a ayudar en los mecanismos de recuperación de la base de datos cuando se lo necesite.

Seleccionar la próxima carpeta.

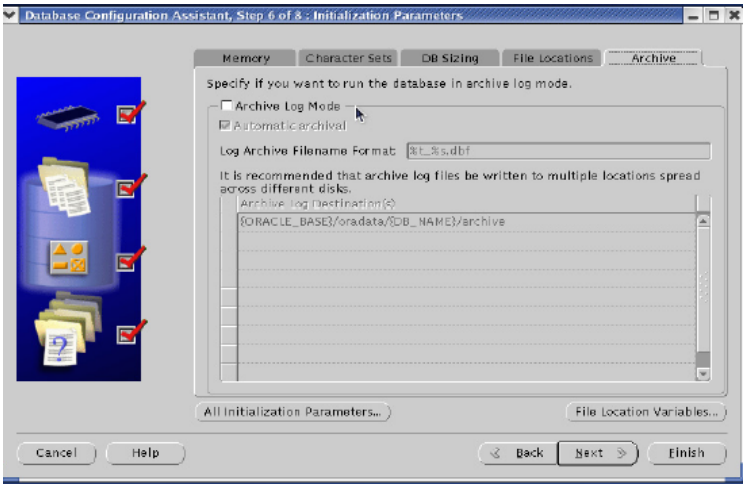

Fig 4.24 Archivos de Log
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

En esta pantalla se tiene un sumario de los tablespaces, archivos de datos y archivos de logs; al dar “click” en cada uno de ellos se puede revisar los directorios en donde se encuentran y finalmente en (“logs”) el asistente propone tres logs, se recomienda solo dos logs, de manera que se debe usar la opción (“Remove”) para eliminar el último log.

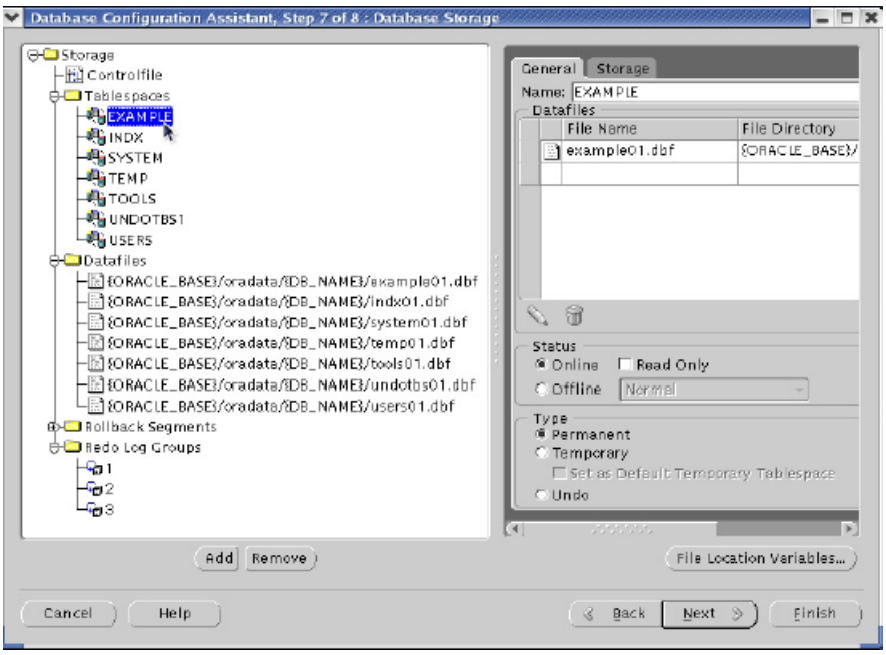

Fig 4.25 Sumario de instalación
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

Seleccionar (“Next”).

Como se ha visto, se ha realizado un trabajo importante hasta el momento analizando detalles que permitan escoger las mejores opciones que garanticen el correcto funcionamiento del sistema, en este punto el asistente

recomienda continuar con la creación o salvar en una plantilla todo lo realizado para usarlo en futuras instalaciones.

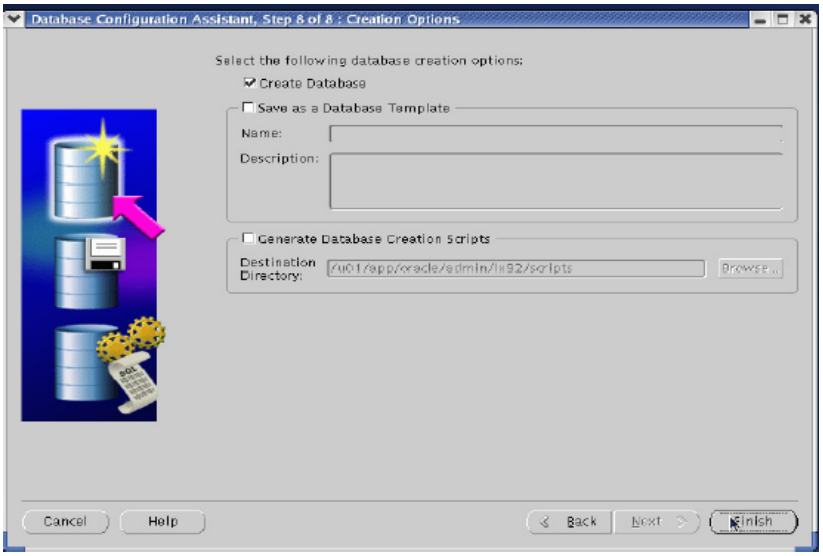

Fig 4.26 Plantilla de instalación
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

Ya se sabe el propósito, para esta instalación sólo escoger la creación de la base de datos y seleccionar (“next”).

Aquí se encontrará un simple resumen de lo escogido en la instalación de la base de datos.

Seleecionar (“ok”) en esta pantalla.

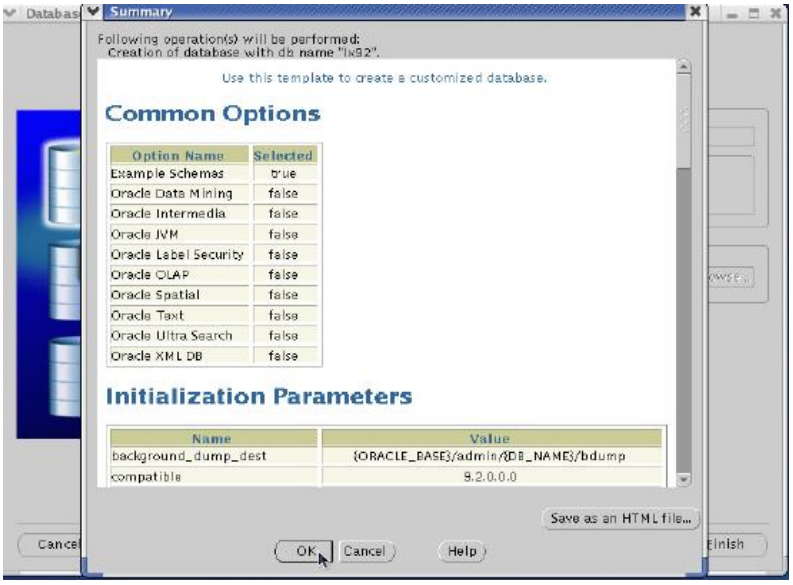

Fig 4.27 Sumario de Opciones
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

En este punto una barra de progreso debe aparecer, en la cual se va a crear la base de datos, la estructura de memorias para levantar la primera instancia, crea los archivos de datos y hace varios procesos internos. Este proceso puede tomar algún tiempo, hay que tener paciencia y esperar la finalización de la instalación.

Al final aparecerá la siguiente pantalla:

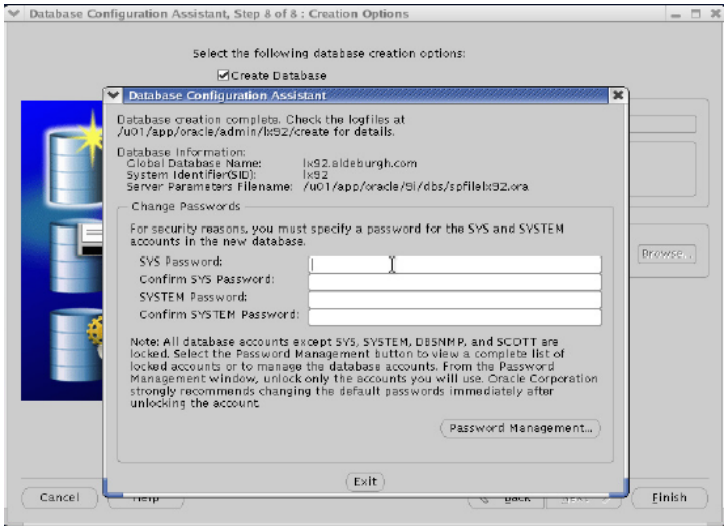

Fig 4.28 Final de instalación
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

Se debe escribir dos frases secretas diferentes para dos usuarios distintos, el usuario “SYS“ y el usuario “SYSTEM”.

Digitar los “password” y seleccionar (“ok”), con esto se ha finalizado la creación de la base de datos.

4.5.3.2 Chequeando que Trabaje Correctamente.

Abrir una terminal en Linux y digitar:

```
sqlplus “/ as sysdba”
```

Oracle usa el programa “sqlplus” para comunicarse con la base de datos, este comando permite ingresar como usuario privilegiado, y se puede levantar base de datos (startup), bajar la base de datos (shutdown), generar respaldos, recuperaciones, etc.

El carácter “/” indica que no se está usando login y password, y lo que la instrucción realiza es ver los privilegios del usuario con el que se está conectado a la sesión de Linux y para ser privilegiado debe estar en el grupo “dba”.

Una vez que haya conexión a la base se puede ejecutar un (“select”) a una tabla de sistema.

```
Select * from v$instance;
```

Se debe ver lo siguiente, esto indica que todo está correcto en la instancia de Oracle levantada.

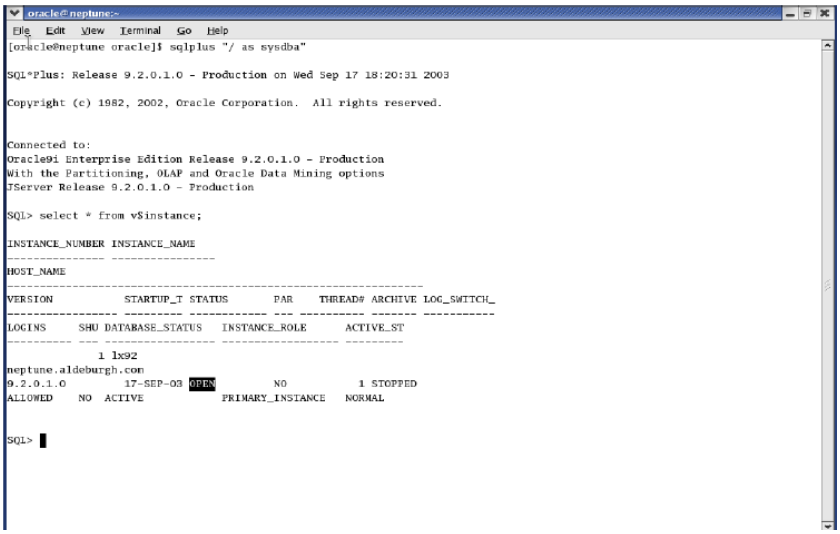

Fig 4.29 Prueba de conexión
Fuente: Howard J. Rogers, Dizwell Informatics, 2003

Ahora se debe ver las configuraciones adicionales para que la base de datos funcione remotamente y se pueda tener requerimientos de los clientes a la base.

4.5.3.3 Ingresando la red de comunicación.

Existen tres componentes para hacer que la base funcione exitosamente de manera remota, estos son el (“Listener”) el cual escucha los requerimientos realizados a la base de datos, y conoce que estas solicitudes pertenecen a una instancia determinada, el (“Tnsname”) quien resuelve el nombre (“lx92”) para que el (“Listener”) pueda saber la instancia a la cual está llegando la solicitud y finalmente se necesita un archivo llamado (“sqlnet.ora”) que lo usa el (“Tnsname”) para resolver los nombres.

4.5.3.4 Creando el Listener

Un Listener es un proceso que está corriendo continuamente en *“background”* esperando por un usuario que quiera contactarse con la base de datos. Este listener trabaja sobre el puerto 1521 y puede escuchar desde otros puertos si está corriendo en un ambiente de redes mixtas.

Este proceso necesita saber estos detalles: puerto por el que se escucha y con qué protocolo de comunicación, y se debe ingresar estas especificaciones en un archivo llamado (“listener.ora”).

Se puede usar el asistente para la creación del listener a través de la instrucción (“netca”), pero también se lo puede realizar de manera manual y es así como se procedió.

Ubicarse en la siguiente ruta : “/u01/app/oracle/9i/network/admin.”.

Ejecutar (“vi listener.ora”) y llenar el archivo con la información adjunta:

```
# LISTENER.ORA  Network Configuration File:
# /u01/app/oracle/9i/networ/admin/listener.ora
# Generated by Oracle configuration tools.


LISTENER =
 (DESCRIPTION =
   (ADDRESS = (PROTOCOL = TCP) (HOST =
oraclesrv.contodomiamor.com)  (PORT = 1521))
 )


SID_LIST_LISTENER  =
 (SID_LIST =
   (SID_DESC =
     (GLOBAL_DBNAME = lx92.contodomiamor.com)
     (ORACLE_HOME = /u01/app/oracle/9i)
     (SID_NAME = lx92)
```

```
  )
 )
```

Ahora se debe chequear si el listener está correctamente instalado. En una terminal digitar (“lsnrctl status“) y se debe ver lo siguiente:

```
LSNRCTL for Linux: Version 9.2.0.1.0 - Production on 05-DEC-2004 09:23:37

Copyright (c) 1991, 2002, Oracle Corporation.  All rights reserved.

Connecting to
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=oraclesrv.contodo
miamor.com)(PORT=1521)))
STATUS of the LISTENER
------------------------
Alias                     LISTENER
Version                   TNSLSNR for Linux: Version 9.2.0.1.0 - Production
Start Date                05-DEC-2004 00:02:29
Uptime                    0 days 9 hr. 21 min. 7 sec
Trace Level               off
Security                  OFF
SNMP                      OFF
```

```
Listener Parameter File   /u01/app/oracle/9i/network/admin/listener.ora
Listener Log File         /u01/app/oracle/9i/network/log/listener.log
Listening Endpoints Summary...

(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=oraclesrv.contodomi
amor.com)(PORT=1521)))

(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=oraclesrv.contodomi
amor.com)(PORT=8080))(Presentation=HTTP)(Session=RAW))

(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=oraclesrv.contodomi
amor.com)(PORT=2100))(Presentation=FTP)(Session=RAW))
Services Summary...
Service "lx92.contodomiamor.com" has 2 instance(s).
  Instance "lx92", status UNKNOWN, has 1 handler(s) for this service...
  Instance "lx92", status READY, has 1 handler(s) for this service...
Service "lx92XDB.contodomiamor.com" has 1 instance(s).
  Instance "lx92", status READY, has 1 handler(s) for this service...
The command completed successfully
```

4.5.3.5 Escogiendo un Método de Resolución de Nombres

De la misma manera que se realizo en el “listener”, se puede usar el comando “netca” o crear manualmente los archivos “sqlnet.ora” y “tnsname.ora”.

Ubicarse en la siguiente ruta: “/u01/app/oracle/9i/network/admin”. Ejecutar (“vi sqlnet.ora”) y completar el archivo con la información adjunta:

```
# SQLNET.ORA Network Configuration File:
/u01/app/oracle/9i/network/admin/sqlnet.ora
# Generated by Oracle configuration tools.
NAMES.DEFAULT_DOMAIN = contodomiamor.com
NAMES.DIRECTORY_PATH= (TNSNAMES)
```

Ubicarse en la siguiente ruta: “/u01/app/oracle/9i/network/admin.”. Ejecutar (“vi tnsnames.ora”) y completar el archivo con la información adjunta:

```
# TNSNAMES.ORA Network Configuration File:
/u01/app/oracle/9i/network/admin/tnsnames.ora
# Generated by Oracle configuration tools.
FLORESDB.CONTODOMIAMOR.COM =
 (DESCRIPTION =
  (ADDRESS_LIST =
```

```
    (ADDRESS = (PROTOCOL = TCP)(HOST =
oraclesrv.contodomiamor.com)(PORT  = 1521))
  )
  (CONNECT_DATA =
    (SERVICE_NAME = lx92.contodomiamor.com)
  )
 )
```

4.5.3.6 Prueba remota

Ahora se debe hacer una prueba para verificar el funcionamiento remoto. Cabe mencionar que (“FLORESDB”) es el nombre amigable que se asignó a la base de datos en el (“tnsnames.ora”)

Ejecutar la siguiente instrucción

```
sqlplus hr/hr@FLORESDB
```

Al ejecutar este comando saldrá el siguiente error

```
ERROR:
ORA-28000: the account is locked
```

Originalmente en la instalación el usuario (“hr”) está bloqueado por defecto, hay que ingresar con un usuario privilegiado para desbloquear la cuenta. Es necesario digitar lo siguiente:

```
Sqlplus "/ as sysdba"
SQL>alter user hr account unlock;
User altered
SQL>alter user hr identified by hr;
User altered
SQL> exit
Disconnected from Oracle 9i
```

Aquí se realizaron estas instrucciones con el usuario "SYS" que es privilegiado, por eso se pudo desbloquear la cuenta y cambiarle la contraseña.

Ahora si, para la prueba final es necesario digitar:

```
sqlplus hr/hr@FLORESDB
```

Se debe presentar el siguiente resultado:

```
SQL*PLUS: Release 9.2.0.1.0 – Production on
Connected to
Oracle9i Entreprise Edition Release 9.2.0.1.0 –Production
```

Con esto se finaliza el trabajo en la base de datos. En este momento se está en capacidad para instalar las bases de trabajo a través del diagrama entidad de relación sugerido.

4.5.3.7 Seguridad de Contenido

En el esquema del proyecto de graduación se adoptó la estrategia de proteger la información sensitiva mediante la encriptación de datos en la base. Específicamente, mediante sentencias de código en el lenguaje Php se encripta los datos del campo contraseña (tabla Clientes, campo cl_password).

La información que se transmite en la red interna, desde el servidor de base de datos hasta el servidor web, está protegida contra accesos no autorizados mediante el firewall principal – Checkpoint y el firewall interno. (Véase figura 3.2 “Esquema de Laboratorio”, página 64)

La información que la base de datos proporciona desde el servidor web al mundo exterior (Internet), viaja encriptada bajo el esquema del protocolo SSL. (Véase sección 4.4.1 Servidor Web Seguro, página 104)

CAPÍTULO 5

HERRAMIENTAS DE SEGURIDAD

El objetivo de este capítulo es describir las bondades de las herramientas de seguridad utilizadas en el proyecto, así como la configuración de las mismas sobre el esquema de red propuesto.

5.1 Secure Shell: SSH.

Para poder administrar los servidores de forma remota, se necesitaba una herramienta que permita ofrecer la seguridad de que ningún intruso pueda comprometer la información. Se escogió a SSH debido a sus características que lo hacen una herramienta de administración segura. A continuación se realiza una breve explicación de este protocolo, para luego finalizar con un detalle de la configuración de la misma.

5.1.1 Acerca de SSH

Red Hat[27] a través de su Web define a SSH (o *S*ecure *SH*ell) como un protocolo que permite crear conexiones seguras entre dos sistemas. Usando SSH, la máquina del cliente inicia una conexión con una máquina del servidor, estableciendo entre ambos una sesión encriptada.

[27] Red Hat es una organización norteamericana dedicada a comercializar su distribución de linux, además de ofrecer seminarios de capacitación y certificaciones.

5.1.2. Tipos de Protección.

Según Red Hat, SSH proporciona los siguientes tipos de protección:

- Después de la conexión inicial, el cliente puede verificar desde donde se realizó la última conexión al servidor.
- El cliente puede transmitir su información de autenticación al servidor, como el nombre de usuario y la contraseña, en formato cifrado.
- Todos los datos enviados y recibidos durante la conexión se transfieren por medio de encriptación fuerte, lo cual los hacen extremamente difícil de descifrar y leer.
- El cliente tiene la posibilidad de usar X11[28], aplicaciones lanzadas desde el intérprete de comandos del *"shell"*. Esta técnica proporciona una interfaz gráfica segura (llamada *reenvío por X11*), proporciona un medio seguro para usar aplicaciones gráficas sobre una red.

5.1.3. Vulnerabilidades relacionadas a SSH.

A continuación se listan algunas vulnerabilidades con respecto a ssh (Red Hat, 2000).

[28] X11 es el protocolo utilizado por distribuciones Linux para inicializar y ejecutar aplicaciones gráficas.

- Muchas versiones de OpenSSH[29] entre 2.3.1 y 3.3 contiene un error de entrada de validación que puede resultar en un desbordamiento de entero, y obtener de esta forma "escalación privilegiada"[30].
- Todas las versiones entre 2.3.1 y 3.3 contiene un *"bug"*[31] en el código *"PAMAuthenticationViaKbdInt"*
- OpenssH 3.2 y posteriores previenen la "escalación privilegiada", si la directiva *"UsePrivilegeSeparation"* está habilitada en el archivo *"/etc/sshd_config"*. OpenSSH 3.3 habilita esta directiva por defecto.

Aunque algunas versiones recientes no están afectadas, actualizar a OpenSSH 3.4 es recomendado, porque OpenSSH 3.4 agrega chequeo para una clase potencial de errores.

5.1.4 Configuración de sshd_config

Para la administración de los servidores se instaló *"openssh-3.4p1-2"*, las directivas básicas que se deben definir en el archivo sshd_config son las siguientes.

Especificar el puerto en que trabajará ssh, por defecto se usa el 22.

```
#Port 22
```

[29] Servicio que ofrece el protocolo SSH.
[30] A través de este método se puede tomar derechos de root, sin necesidad de saber la contraseña del mismo.
[31] Error de código encontrado en una versión de un programa.

Si se tiene dos interfaces de red se puede especificar que ssh escuche sólo por una. En el esquema del proyecto se permite conexiones de cualquiera de sus interfaces.

```
#ListenAddress 0.0.0.0
```

Es preferible que un usuario no se pueda conectar directamente como “root”, sino que primero se conecte como usuario sin privilegios y una vez establecida la comunicación conectarse como “root”.

```
PermitRootLogin no
```

Si se desea colocar un “banner”(mensaje) de bienvenida se lo puede especificar en la siguiente directiva. Por seguridad es preferible no colocar “banners” relacionados a la organización o a los empleados de la misma.

```
Banner /etc/banner
```

5.2 FIREWALL PRINCIPAL - CHECK POINT NEXT GENERATION

5.2.1 Introducción

"Secure Virtual Network" [32] es una arquitectura desarrollada por la compañía Check Point Software Technologies Ltd. orientada a proveer seguridad en la red, brindando a las empresas protección en sus negocios críticos en Internet, y en el tráfico de intranet y extranet.

El componente clave de la arquitectura SVN (Secure Virtual Network) es el producto "VPN-1/FireWall-1", herramienta que provee las siguientes características (Guía de inicio de Check Point, 2001):

1.- Control de acceso

2.- Autenticación de usuarios

3.- NAT[33]

4.- VPN[34]

5.- Auditoria y Reportes

6.- Detección de Intrusos

7.- Detección de actividades maliciosas

A continuación se explicará brevemente sobre la tecnología implantada por esta herramienta.

---

[32] Secure Virtual Networik (SVN): Red Virtual Segura
[33] NAT: Network Address Translation (Traducción de direcciones de red)
[34] VPN: Virtual Private Networking (Redes Virtulas Privadas)

5.2.2 VPN-1/FIREWALL-1

La tecnología *"Stateful Inspection"*[35] de Check Point, se basa en la examinación de todos los paquetes que pasan a través de las ubicaciones clave en la red, bloqueando los paquetes que se consideren no deseados, los cuales pueden ser alertados a través de log y correos internos de notificación.

La herramienta ("VPN-1/FIREWALL-1"), o el firewall de la arquitectura SVN de Check Point, es completamente transparente tanto para usuarios como para las aplicaciones y puede coexistir con otras herramientas de seguridad.

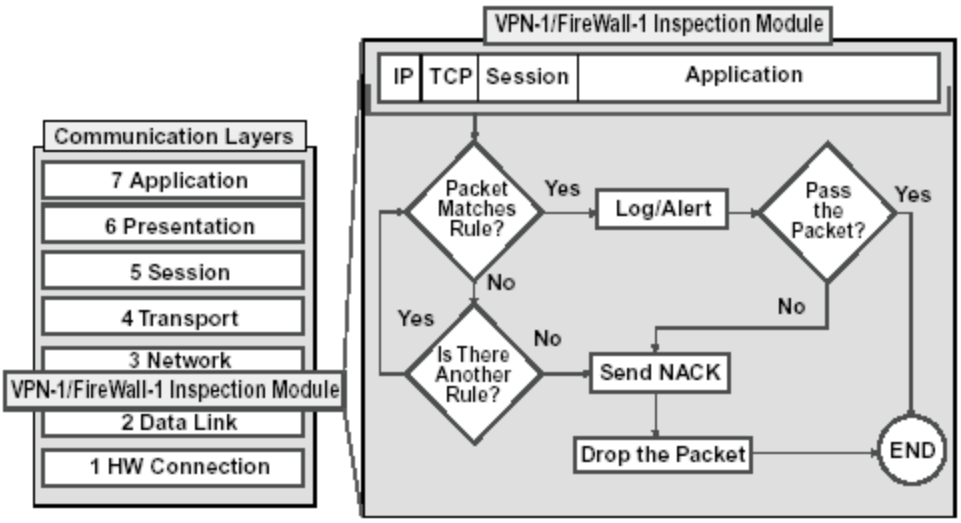

Figura 5.1 Módulo de Inspección VPN-1/Firewall-1
Fuente: Guía de inicio de Check Point

[35] Stateful Inspection: Inspección de estado

El módulo de inspección de (“VPN-1/FIREWALL-1”) opera entre la capa de Enlace de Datos y la capa de Red del modelo OSI, de esta manera puede interceptar los paquetes y no dejar que éstos pasen a las otras capas. El módulo de inspección examina la dirección IP, número de puerto y otra información requerida para determinar que el paquete se acepta o se rechaza en concordancia con la Política de Seguridad establecida.

5.2.3 Arquitectura VPN-1/FIREWALL-1

Según la Guía de Inicio de Check Point (2001) la herramienta VPN-1/FireWall-1 está integrada por 3 componentes:

1.- Interface Gráfica del Usuario

2.- Servidor de Administración

3.- Módulo VPN/Firewall

A continuación se dará una breve explicación respecto a cada uno de los componentes en mención.

5.2.3.1 Interface Gráfica del usuario (GUI) o editor de políticas

El editor de políticas de Check Point es una interface de usuario que permite la administración de políticas en términos de objetos de red, por ejemplo: equipos, redes y reglas.

En la herramienta ("VPN-1/Firewall-1") es posible definir 4 clases de políticas:

1.- Política de Seguridad: especifica el tipo de comunicación permitida para ingresar o salir de la red, adicionalmente el esquema bajo la cual las conexiones deben ser autenticadas y encriptadas.

2.- Política de Traducción de Direcciones de Red (NAT): especifica como una dirección IP inválida va a ser traducida en una dirección IP válida, estableciendo el uso eficiente de espacios en las direcciones IP privadas.

3.- Política de Calidad de Servicios: especifica la asignación de recursos de ancho de banda.

4.- Política de Seguridad de Escritorio: permite al administrador controlar el acceso hacia las computadoras personales dentro de la red local y de aquellos equipos que se conectan remotamente. (Guía de inicio de Check Point, 2001)

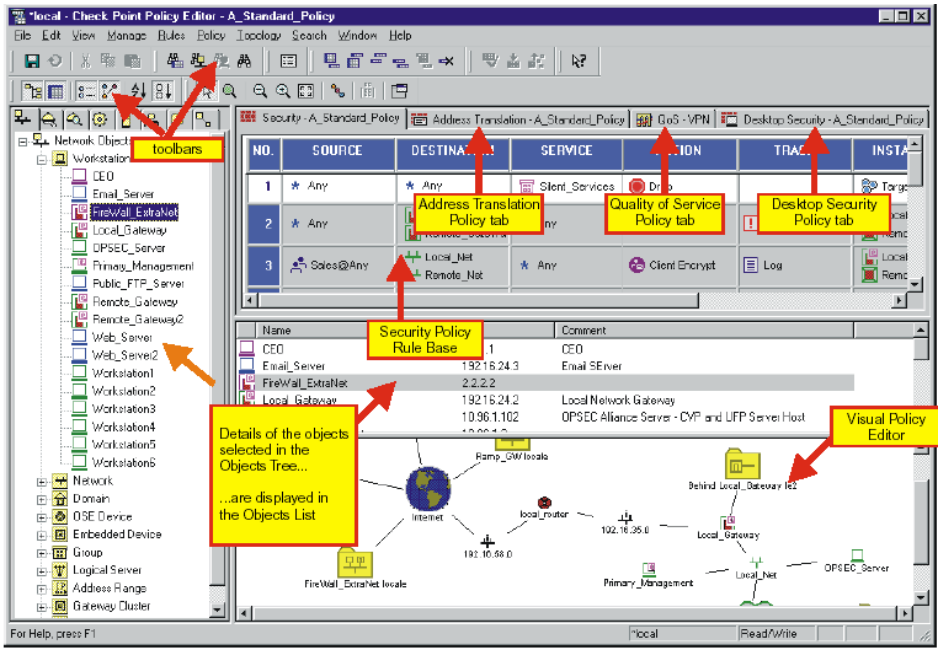

Figura 5.2 Editor de Políticas
Fuente: Guía de inicio de Check Point

Como se observa en la imagen del Editor de Políticas, de una manera gráfica es posible administrar las políticas definidas.

5.2.3.2 Servidor de Administración

Según la Guía de Inicio de Check Point (2001), las políticas de seguridad aplicadas por la herramienta VPN-1/Firewall-1 son definidas utilizando la Interface gráfica del usuario (GUI o editor de políticas) y son almacenadas en el Servidor de Administración.

El Servidor de Administración contiene y mantiene la base de datos del Check Point incluyendo los objetos de red definidos, usuarios definidos, políticas y archivos de log, número de puntos de control o puntos críticos.

El Editor de políticas (o GUI) y el Servidor de Administración pueden ser instalados en la misma máquina o en máquinas diferentes dentro una estructura Cliente Servidor.

5.2.3.3 Módulo VPN/FIREWALL

El módulo VPN se ejecuta en los servidores de salida hacia Internet (o gateways) y en los diferentes puntos de acceso externo hacia la red. (Guía de inicio de Check Point, 2001)

La política de seguridad se compila en el Servidor de Administración y luego es cargada al módulo VPN/FIREWALL, quien finalmente aplica la política definida. El módulo VPN/FIREWALL incluye el modulo de inspección que examina que todas las comunicaciones se realicen de acuerdo a las políticas establecidas.

5.2.3.4 Políticas de Seguridad

En la herramienta ("VPN-1/Firewall-1") de Check Point una política de seguridad se define en términos de una regla base y propiedades. (Guía de inicio de Chek Point, 2001)

A continuación se detallará brevemente los conceptos de regla base y propiedades.

Regla Base

Una regla base es un conjunto ordenado de reglas, contra el cual cada comunicación entrante o saliente será analizada. Para establecer una regla se deben definir en el ("Editor de Políticas") los siguientes datos: la fuente, el destino, el servicio y la acción a ser tomada para cada comunicación; por ejemplo si es permitido o negado.

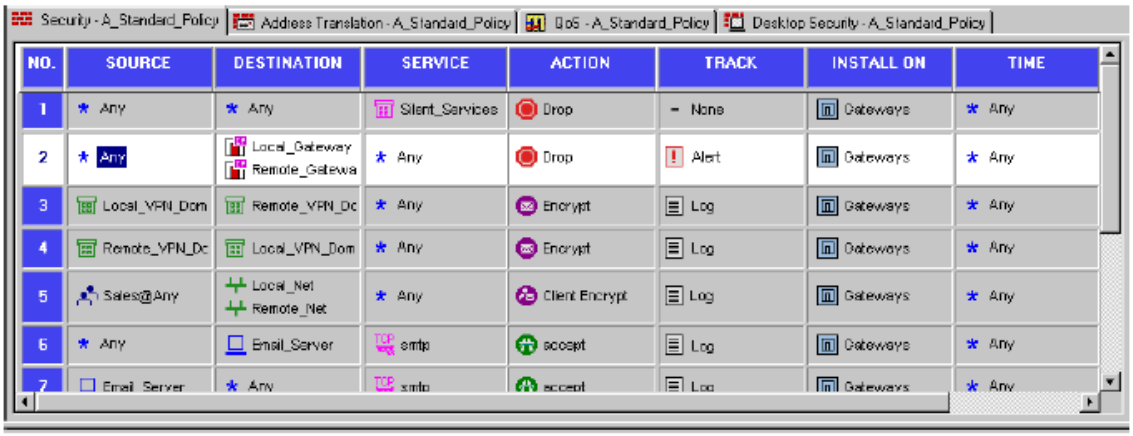

Figura 5.3 Reglas especificadas en el Editor de Políticas
Fuente: Guía de inicio de Check Point

Como se observa en el gráfico, todas las reglas son definidas en el ("Editor de Políticas") explicado anteriormente.

Propiedades

Las propiedades especifican aspectos generales de inspección en la comunicación, como por ejemplo: el periodo del tiempo de expiración en las sesiones de autenticación, o como la herramienta ("VPN-1/Firewall-1") maneja las conexiones TCP establecidas. (Guía de inicio de Chek Point, 2001).

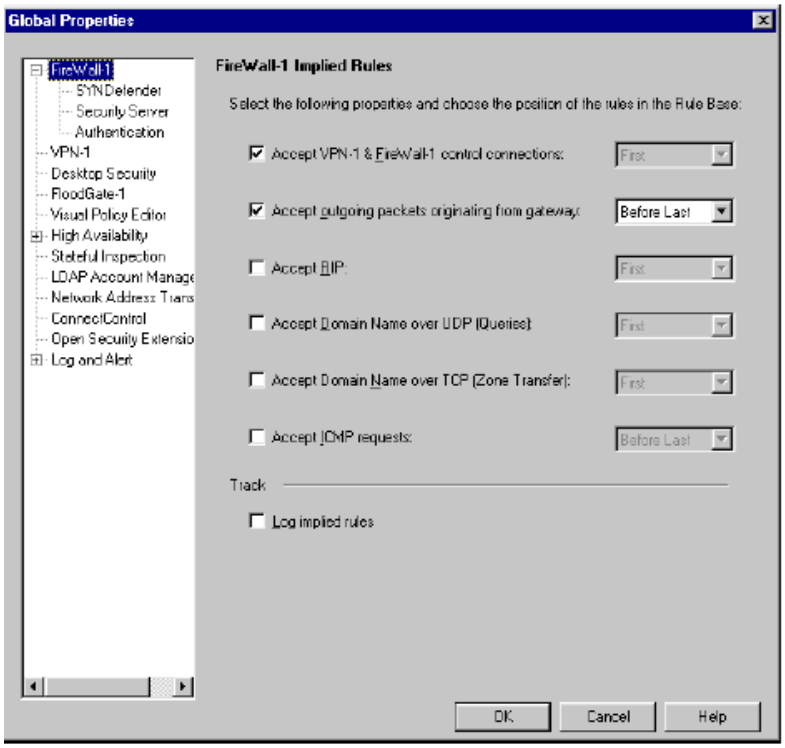

Figura 5.4 Ventana de Propiedades globales
Fuente: Guía de inicio de Check Point

Las propiedades son aplicadas para todas la reglas y no es necesario especificar detalles repetitivos en Políticas de Seguridad

5.2.3.5 Objetos de Red

La herramienta (“VPN-1/Firewall-1”) de Check Point mediante el (“Editor de Políticas”) brinda al administrador del *“firewall”* la funcionalidad de definir recursos de red en términos de objetos sencillos, como por ejemplo: servidores, redes, ruteadores, servicios, dominios de Internet, rangos de direcciones IP, entre otros; y cada objeto incluye sus respectivas propiedades (Guía de inicio de Chek Point, 2001).

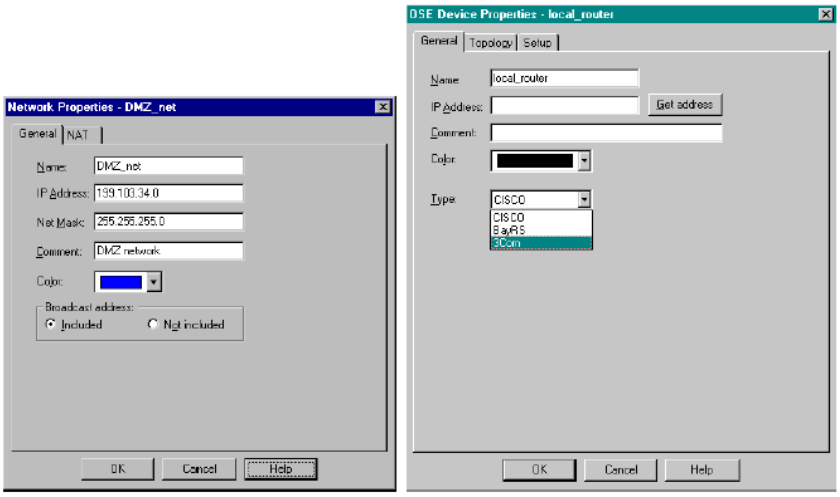

Figura 5.5 Definiciones de objetos de red y routers
Fuente: Guía de inicio de Check Point

En el proyecto de graduación se definieron objetos para cada servidor del esquema de laboratorio sugerido.

5.2.3.6 Usuarios

("VPN-1/FIREWALL-1") habilita los privilegios de acceso para que sean definidos a nivel de usuarios, ya sea sobre una base individual o mediante grupos.

Los grupos de usuarios pueden ser creados permitiendo la definición de sus privilegios de acceso, incluyendo la fuente y el destino autorizados, así como el esquema de autenticación de usuarios (Guía de inicio de Chek Point, 2001).

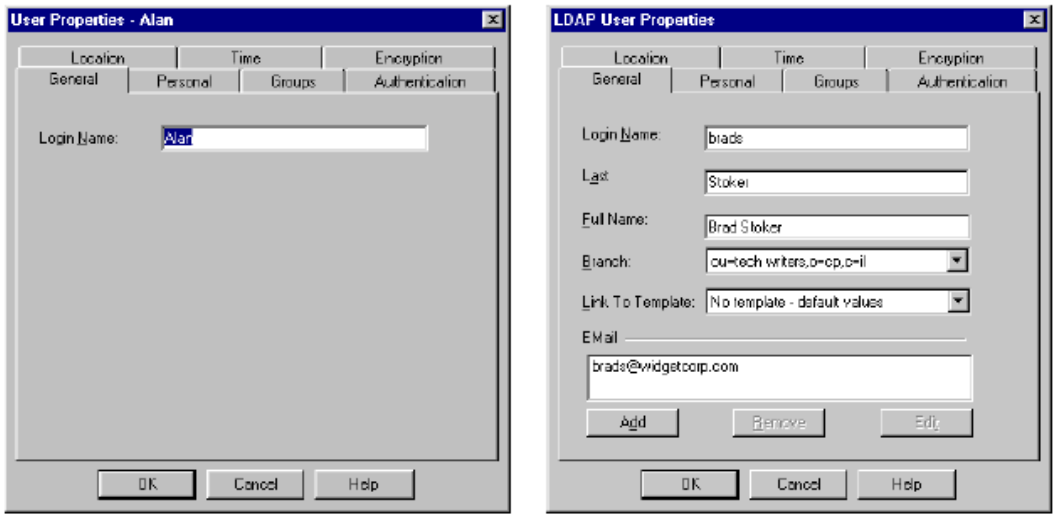

Figura 5.6 Propiedades de usuario.
Fuente: Guía de inicio de Check Point

En el proyecto de graduación se definió solamente un usuario administrador, responsable de manipular todos los objetos definidos.

5.2.3.7 Servicios

En (“VPN-1/Firewall-1”) mediante la herramienta (“Service Manager”)[36] se definen los servicios conocidos en el sistema, los cuales serán utilizados en la política de seguridad. La herramienta monitorea todos los servicios de red, inclusive aquellos que no han sido definidos.

El software (“VPN-1/Firewall-1”) incluye un conjunto predeterminado de servicios de Internet y TCP/IP, como por ejemplo: Telnet, Ftp, Smtp, rlogin, NFS, http, Gopher, Archie, ICMP, RIP, SNMP.

Nuevos servicios pueden ser definidos seleccionando el tipo de servicio y configurando sus atributos. Los servicios pueden ser agrupados en familias y jerarquías, con el objetivo de facilitar su administración.

VPN-1/FIREWALL-1 incluye los siguientes tipos de servicios: TCP (Transmission Control Protocol), UDP (User Datagram Protocol), RPC (Remote Procedure Call), ICMP (Internet Control Message Protocol), entre otros (Guía de inicio de Chek Point, 2001).

[36] Service Manager: Manejador de Serviciso

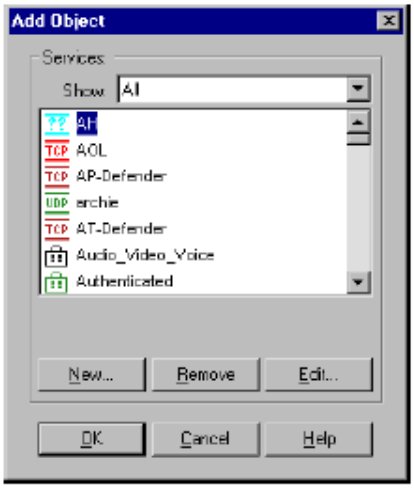

Figura 5.7 Ventana de Servicios
Fuente: Guía de inicio de Check Point

En el proyecto de graduación se habilitaron servicios como: Nfs, Http, Https, Ssh, Dns, entre otros.

5.2.3.8 Logs, pistas visuales

El (“Log Viewer”) de (“VPN-1/FIREWALL-1”) provee un rastreo visual para todas las conexiones registradas por el Check Point. Mediante esta herramienta se puede visualizar en línea y monitorear en tiempo real las actividades de la red. (Guía de inicio de Chek Point, 2001)

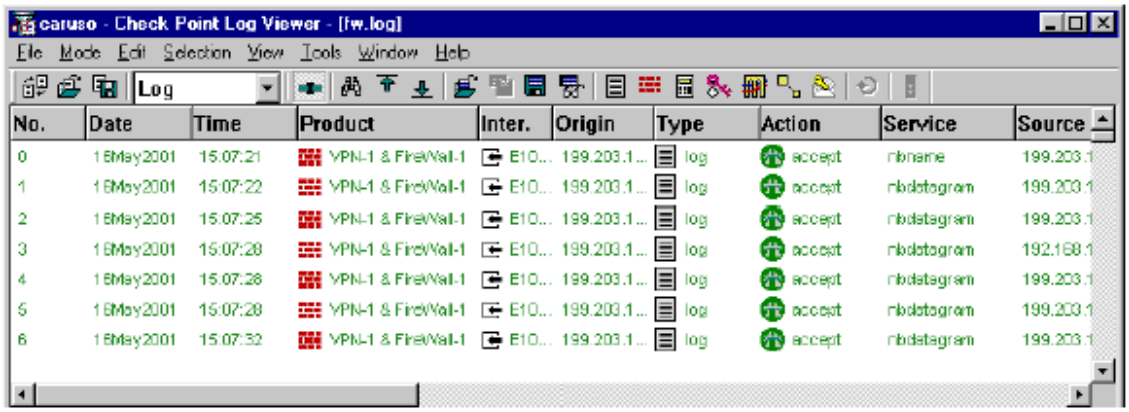

Figura 5.8 Vista del Log Viewer

Fuente: Guía de inicio de Chek Point

El administrador puede personalizar el ("Log Viewer") para que se presente por pantalla u oculten campos específicos o eventos. Adicionalmente se pueden realizar filtros o búsquedas sobre los registros del log para rápidamente localizar y rastrear eventos de interés.

5.2.3.9 Seguridad y Administración de la Red

Según la Guía de Inicio de Check Point (2001), la herramienta ("VPN-1/FIREWALL-1") incluye características de seguridad y administración de la red que se integran completamente a la Política de Seguridad de la empresa y son administradas a través de la interface gráfica.

El módulo de seguridad de VPN-1/FIREWALL-1, incluye las siguientes funcionalidades:

1.- Autenticación

2.- Network Address Translation (NAT)

3.- Virtual Private Networks (VPN)

4.- Seguridad de contenido

A continuación se explicará brevemente cada una de las funcionalidades mencionadas.

5.2.3.9.1 Autenticación

("VPN-1/FIREWALL-1") implementa un acceso seguro y autentificado hacia los objetos de la red, aplicado a usuarios locales y remotos. El Administrador puede determinar la manera que cada individuo es autentificado, los servidores y aplicaciones accesibles, y los horarios en los cuales se le concede el acceso al usuario (Guía de inicio de Chek Point, 2001).

VPN-1/Firewall-1 provee los siguientes métodos de autentificación.

- Autentificación de Usuario
- Autentificación de Cliente

- Autentificación de Sesión

Figura 5.9 Regla de Autentificación de usuario
Fuente: Guía de inicio de Chek Point

Estos métodos de autentificación implementan una manera segura y controlada para manipular los objetos definidos.

5.2.3.9.2 Network Address Translation - NAT

La capacidad de traducción de direcciones de red (NAT) del ("VPN-1/FIREWALL-1") provee un acceso completo a Internet para equipos internos que poseen a una dirección IP privada.

("VPN-1/FIREWALL-1") implementa mecanismos de NAT dinámico y estático. El NAT dinámico oculta direcciones internas inválidas por medio de una sola dirección IP, mientras que el NAT estático realiza un mapeo de cada dirección interna inválida a su correspondiente dirección válida.

("VPN-1/FIREWALL-1") provee los siguientes métodos para la configuración de NAT:

- Regla Base NAT Gráfica
- Configuración Automática

A continuación se presenta una breve explicación de los métodos de traducción de direcciones IP.

Regla Base NAT Gráfica

La interface gráfica de VPN-1/FIREWALL-1 simplifica al usuario la definición e implementación del NAT. Una regla base flexible de NAT permite al administrador especificar objetos por medio de nombres, en lugar que por direcciones IP.

NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE	
1	Local_Net	Local_Net	Any	Original	Original	Original	All
2	Local_Net	Any	Any	Local_Net (Hidin	Original	Original	All
3	Remote_Net	Remote_Net	Any	Original	Original	Original	All
4	Remote_Net	Any	Any	Remote_Net (Hc	Original	Original	All

Figura 5.10 Reglas bases de NAT

Fuente: Guía de inicio de Check Point

El administrador puede aplicar reglas para especificar direcciones IP destino, direcciones IP fuente o servicios.

Configuración automática

Las propiedades de NAT son definidas para objetos de red específicos, como por ejemplo estaciones de trabajo o redes.

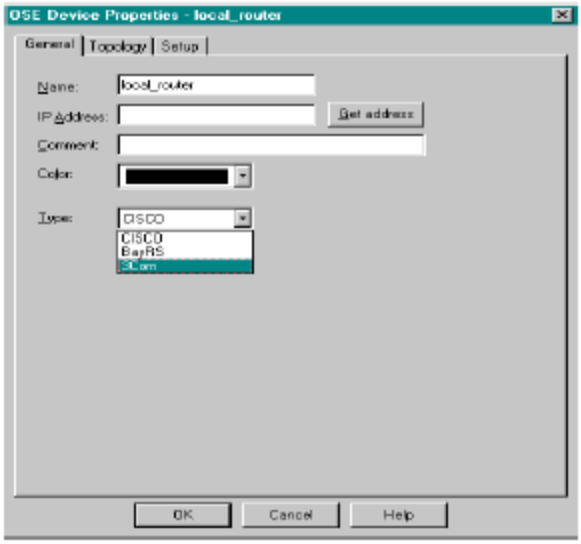

Figura 5.11 NAT automático para la Red
Fuente: Guía de inicio de Check Point

Las reglas de NAT son automáticamente generadas a partir de las propiedades definidas.

5.2.3.9.3 Virtual Private Networks - VPN

("VPN-1/FIREWALL-1") posee su módulo opcional de VPN que implementa protección a las comunicaciones sobre Internet y permite a la compañía diseñar su propio esquema de red privada virtual (VPN) utilizando segmentos de red públicos y privados.

Según la Guía de Inicio de Check Point (2001), (“VPN-1/FIREWALL-1”) provee la plataforma ideal para desarrollar redes privadas virtuales empresariales, encriptando las comunicaciones para garantizar la privacidad y seguridad de los datos.

Los productos VPN-1 de Check Point soporta los estándares de algoritmos y protocolos definidos en la industria, como por ejemplo: AES, DES, 3DES, IPSEC, certificados digitales, entre otros.

5.2.3.9.4 Seguridad de Contenido

(“VPN-1/FIREWALL-1”) provee seguridad de contenido para conexiones HTTP, SMTP Y FTP, incluyendo un chequeo de virus para transferencia de archivos, control de acceso para recursos de red específicos (por ejemplo URLs) y comandos SMTP.

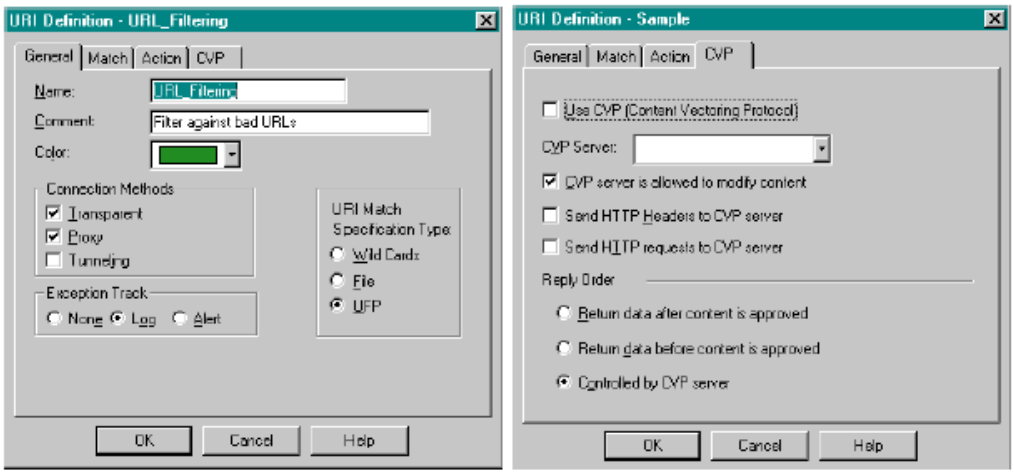

Figura 5.12 Definir URL filtradas
Fuente: Guía de inicio de Check Point

Figura 5.13 Definir la regla usando la dirección filtrada
Fuente: Guía de inicio de Check Point

Las dos figuras anteriores muestran cómo a través de reglas se puede preestablecer direcciones URL filtradas, logrando un mayor control respecto a la información que están accediendo los usuarios.

5.2.4 Instalación y Configuración

Para empezar la instalación de ("CheckPoint") en la red del proyecto de graduación, primero se deben revisar los servicios de red que están habilitados en el servidor, dejando solamente disponibles los estrictamente necesarios.

La instalación se realizará sobre un servidor Windows 2000 Server, y a través de los servicios administrativos se procedió a deshabilitar y en otros casos dejar en modo manual los siguientes servicios: ClipBook, Application Management, Com+, Distributed Link Tracking Server, Fax Service, File Replication, Indexing Service, Internet Connection Sharing, Intersite Messaging, Ipsec Policy Agent, Kerberos, Logical Disk Manager, Net Logon, NetMeeting, Network DDE, NT LM Security, Performance Logs y Alerts, Print Spooler, Remote Access Auto Connection, Routing y Remote Access, RPC Locator, Smart Card, Smart Card Helper, TCP/Netbios Helper Service, Terminal Service

Para empezar la instalación desde el Cd, dentro de la ventana (“Server/Gateway Components”) seleccionar (“VPN-1/FireWall-1”), dado que para el proyecto de graduación solo se va a utilizar esta opción de instalación. El resto de opciones, como por ejemplo Administración de Clientes, es para administrar remotamente el Check Point.

Figura 5.14 Solo seleccionar VPN-1/Firewall-1
Fuente: Cd de instalación de Check Point

Después de escoger la opción de instalación se muestra un resumen de los productos elegidos, posteriormente se debe continuar con la instalación de los mismos.

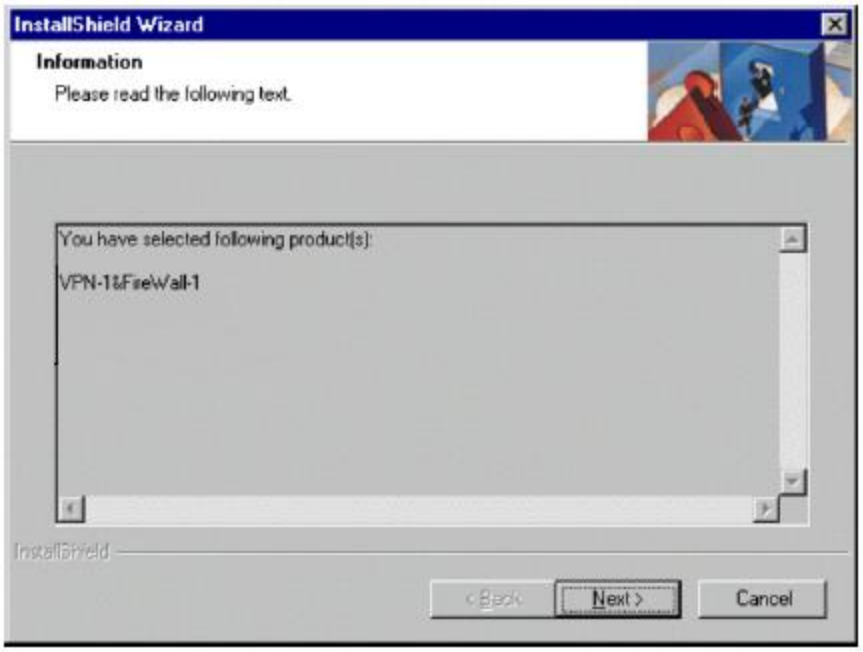

Figura 5.15 Seleccionar productos de instalación
Fuente: Cd de instalación de Check Point

Al seleccionar (“Next”), se presentará la siguiente pantalla:

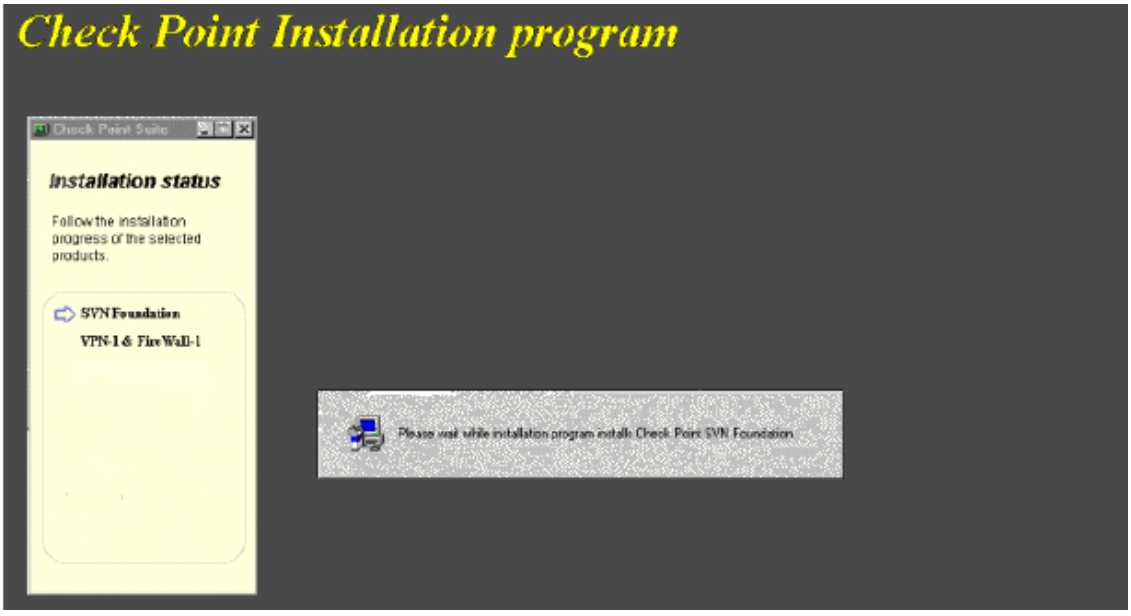

Figura 5.16 Estado de Instalación e Instalación del SVN Foundation
Fuente: Cd de instalación de Check Point

El (“SVN Foundation”) es utilizado por todos los productos de ChekPoint Next Generation.

Luego de este paso se empieza con la instalación del software VPN-1/Firewall-1

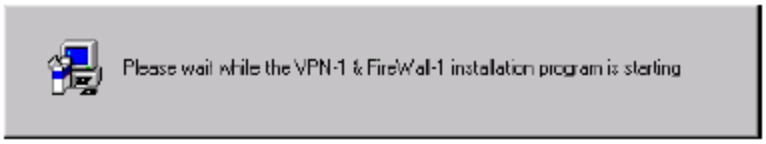

Figura 5.17 Mensaje de espera
Fuente: Cd de instalación de Check Point

Dentro de la ventana del VPN-1/Firewall-1 se selecciona el tipo de producto que se va a instalar en la máquina. En el caso del proyecto, se escoge la opción (“Enforcement Module”) y (“Primary Management”), ya que ésta máquina servirá tanto para instalar el software como para Administrar el producto.

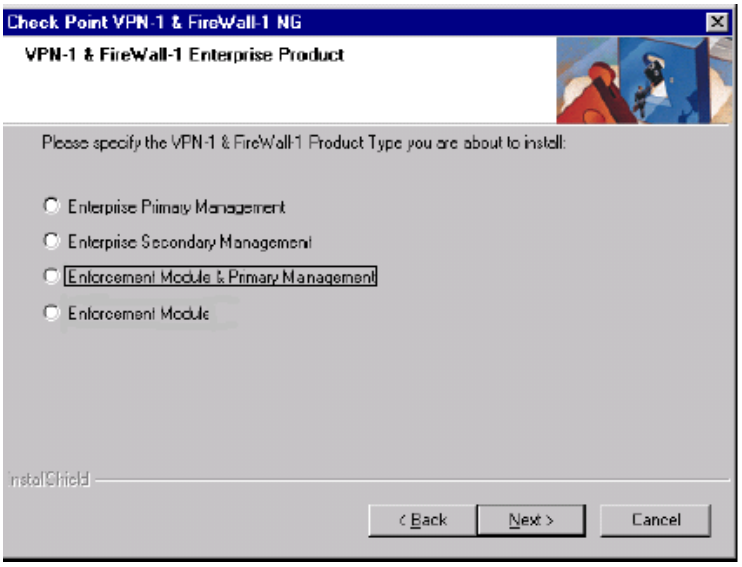

Figura 5.18 Ventana de Productos
Fuente: Cd de instalación de Check Point

Al seleccionar (“Next”), se desplegará la opción de (“Compatibilidad”). Esta opción permite mantener la compatibilidad respecto a versiones previas tales como la 4.0 y 4.1

En este caso como no se va a necesitar ningún componente de la versión previa, se instalará sin la compatibilidad tal como se presenta en la figura:

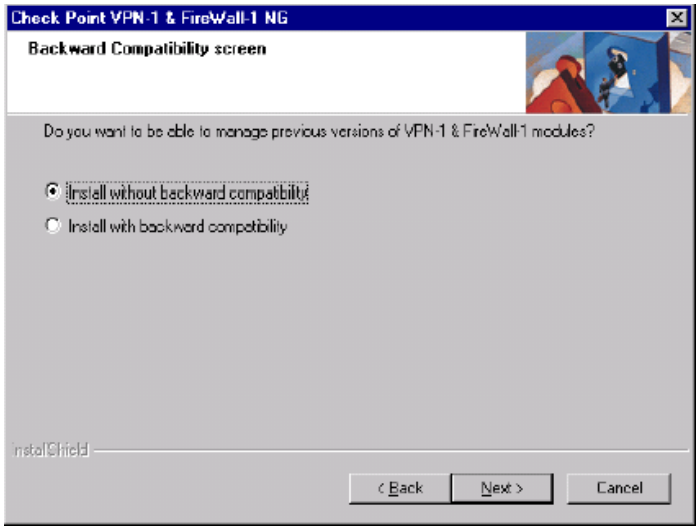

Figura 5.19 Compatibilidad de versiones
Fuente: Cd de instalación de Check Point

Al seleccionar ("Next"), en la siguiente ventana se escogerá la carpeta de instalación. El programa de instalación presenta por defecto un directorio y lo recomendable es hacerlo sobre ese directorio sugerido.

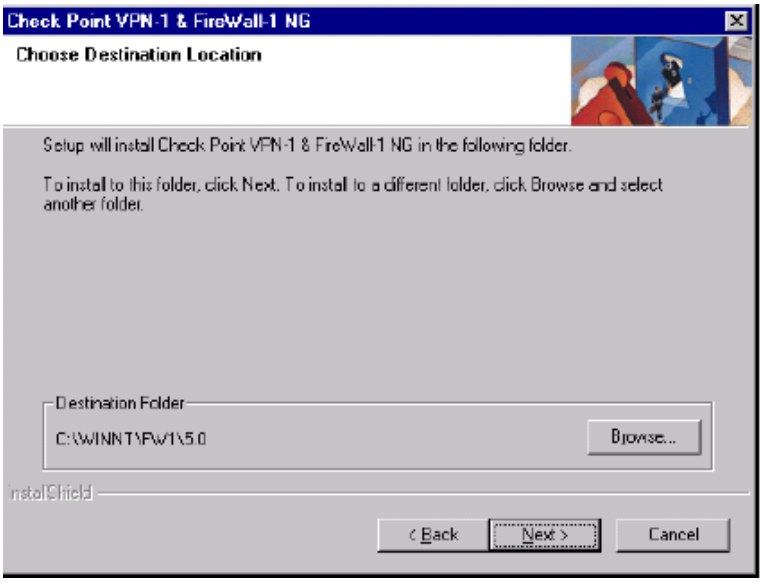

Figura 5.20 Directorio de Instalación.
Fuente: Cd de instalación de Check Point

Continuando con la instalación se tiene que escoger las opciones de (“Administración del producto”). Para el proyecto de graduación se escogió: (“Editor de Políticas”), (“Log Viewer”), (“Monitoreo de Tráfico”) y (“Herramientas de reporte”).

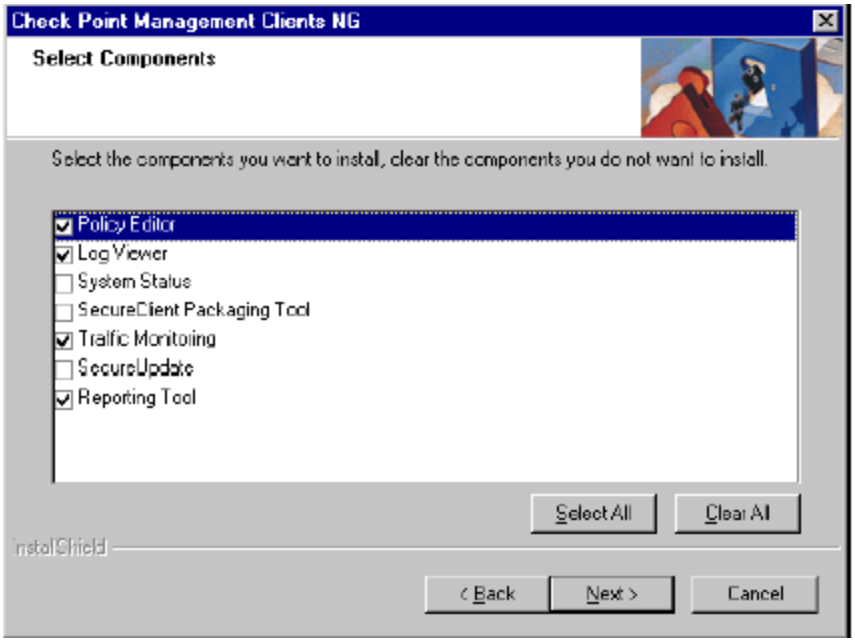

Figura 5.21 Componentes de Administración.
Fuente: Cd de instalación de Check Point

Finalmente un mensaje de agradecimiento (“Thank You”) aparece cuando la instalación se ha completado.

Figura 5.22 Instalación ha sido completada
Fuente: Cd de instalación de Check Point

Después de este cuadro de mensaje aparecerá la notificación respecto al reinicio del equipo.

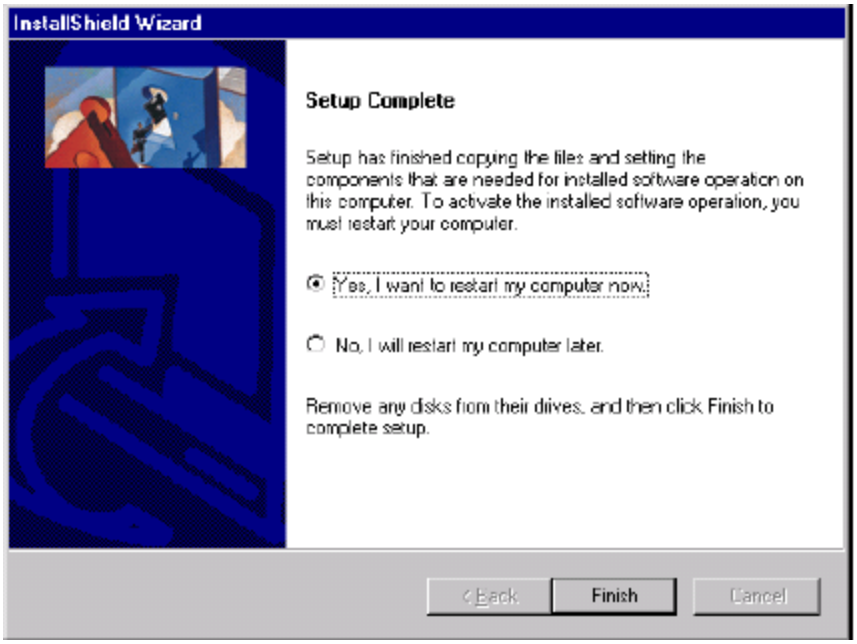

Figura 5.23 Instalación Completa
Fuente: Cd de instalación de Check Point

Al reiniciar el servidor se está en capacidad para empezar con la configuración de opciones, licencia de trabajo, interfaces de red, reglas y políticas.

5.2.5 Obtención de Licencia.

Para obtener la licencia se deben seguir los siguientes pasos:

1. Obtener la clave que viene en la cubierta del Cd de Instalación
2. Contactar al centro de usuarios a través de la dirección www.checkpoint.com/usercenter, para obtener la licencia permanente.
3. El user center se encarga de validar la clave y enviar vía correo electrónico los siguientes datos que conforman la licencia: Sku/Features y el Signature Key que son cadenas de texto formados por números, letras y caracteres especiales.

Una vez obtenida la licencia se selecciona (“Start/Programs/Check Point Management Clients/Check Point Configuration NG”), donde se tendrá las siguientes opciones a configurar: (“Licencias”), (“Administración”), (“GuiClients”), (“PKCS#11 Token”), (“Key Hit Session”), (“Fingerprint”).

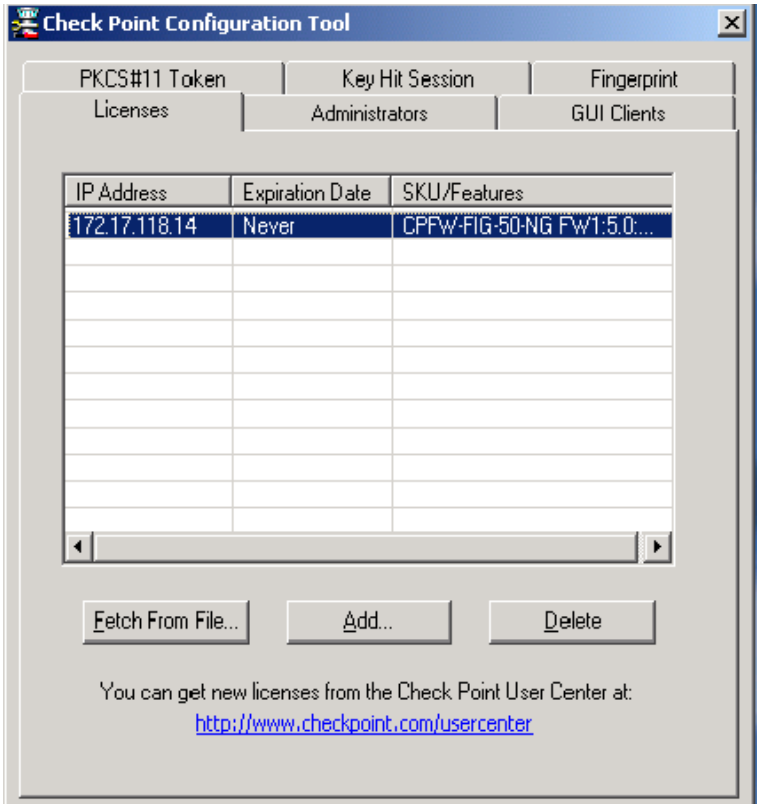

Figura 5.24 Configuración CheckPoint
Fuente: Software Check Point

Para adicionar la licencia que fue otorgada, hay que ubicarse en la carpeta de licencia y luego seleccionar (“Add”).

La licencia está dada inicialmente para la interface de red Lan que corresponde a la dirección IP 172.17.118.14 tal como se muestra en el gráfico de topología de la red (Véase figura 3.2 “Esquema de Laboratorio”, página 64).

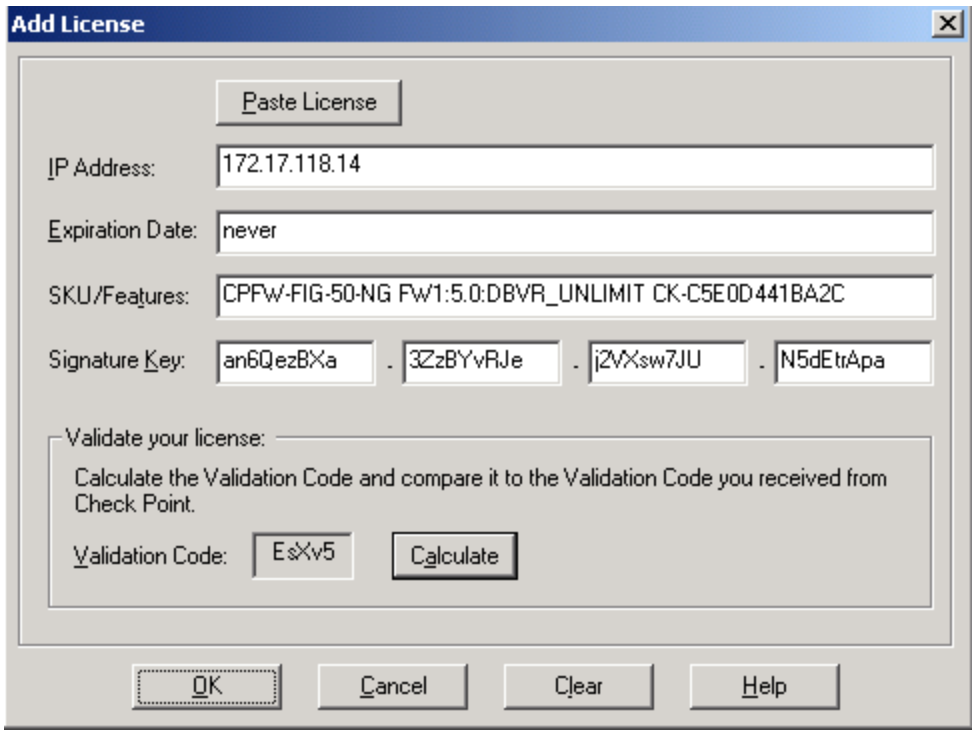

Figura 5.25 Adicionar la licencia
Fuente: Software Check Point

En el campo de (“Dirección IP”) se digita: (“172.17.118.14”).

En el campo de (“Expiration Date”) se digita (“Never”), ya que la licencia adquirida es permanentemente.

En el campo (“Sku/Features”) y (“Signature Key”), se ingresa la cadena recibida por correo electrónico. (Es necesario prestar atención a las minúsculas y mayúsculas ya que son consideradas como parte de la validación de las claves.)

Administrador

En esta carpeta se define el administrador del firewall. Es necesario establecer un nombre de usuario y contraseña que cumplan las medidas de seguridad básicas como por ejemplo: no digitar palabras fácilies de adivinar, nombres, fechas de nacimiento, edades, etc.

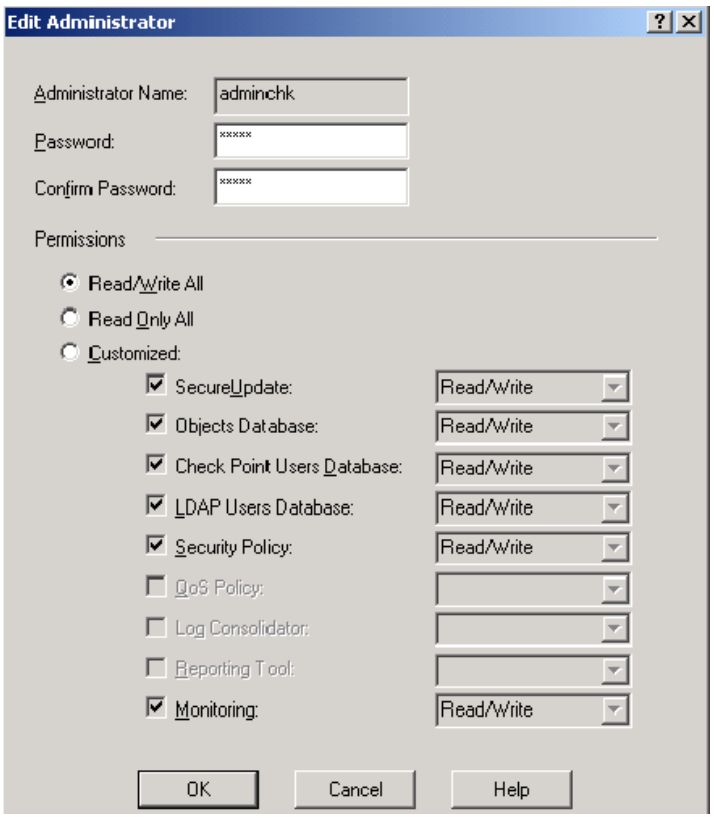

Figura 5.26 Administrador del sistema.
Fuente: Software Check Point

En el caso del proyecto de graduación, el usuario del administrador del Chek Point es “adminchk” y su contraseña es “serm2327wljl”. Este usuario va a ser el único administrador del sistema y tendrá por lo tanto permisos de lectura y escritura sobre el sistema.

GuiClients

En esta carpeta se definen los usuarios que van a acceder remotamente para administrar las reglas y objetos del firewall.

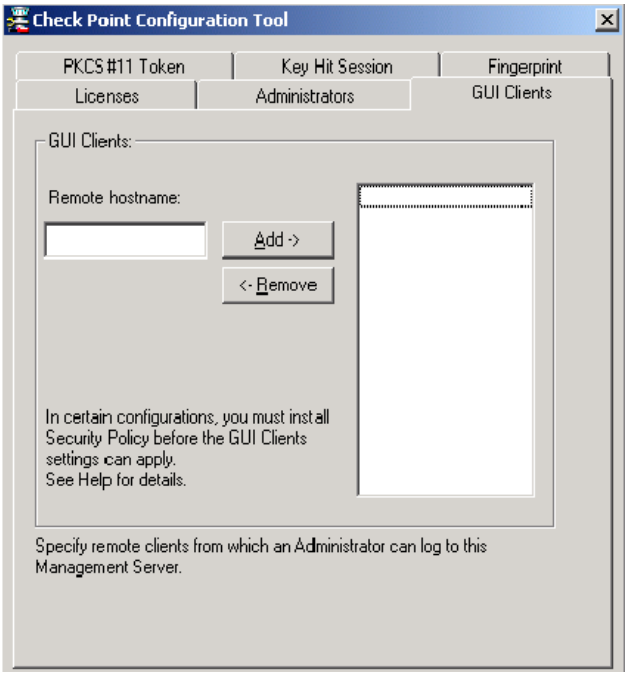

Figura 5.27 Gui Clients
Fuente: Software Check Point

En el caso del proyecto de graduación no se va a utilizar esta opción ya que es para manejar y administrar remotamente el sistema. Como fue explicado anteriormente, tanto el sistema como su administración estarán centralizados en el mismo equipo.

PKCS#11 TOKEN

En esta ventana se registra un token de criptografía usado por el ("VPN-1/Firewall-1") y se puede evaluar su funcionalidad.

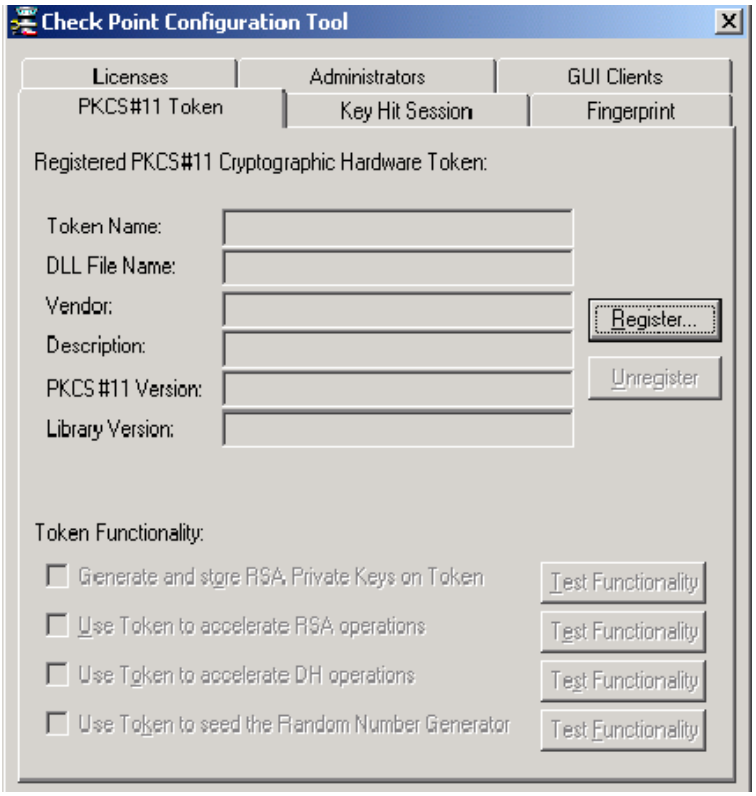

Figura 5.28 PKCS#11 TOKEN
Fuente: Software Check Point

En el proyecto de graduación tampoco se utilizó esta opción.

Key Hit Session

En esta carpeta se genera el dato aleatorio que se será utilizado como una semilla para operaciones de criptografía.

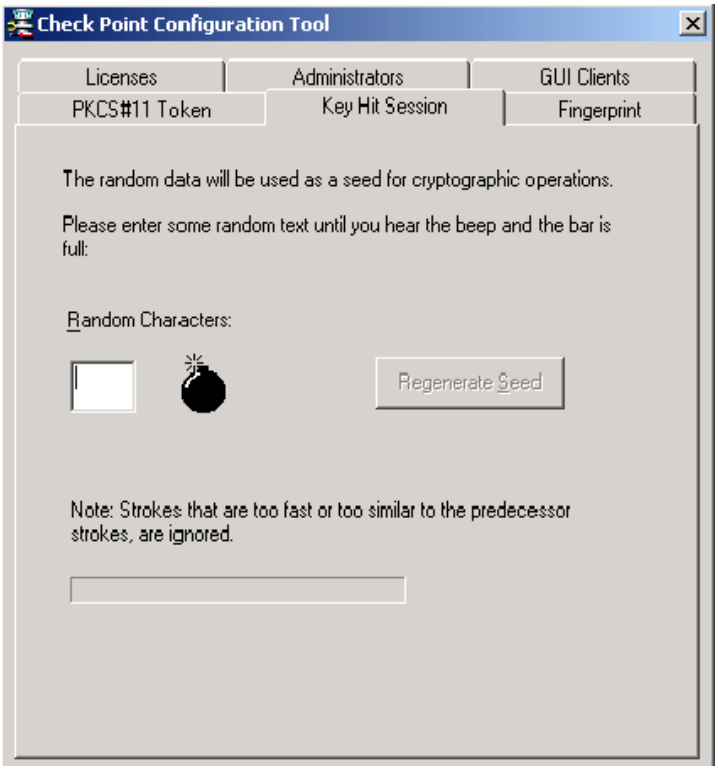

Figura 5.29 Key Hit Session.
Fuente: Software Check Point

Para generar claves de encriptación aleatoria es necesario ingresar caracteres, demorándose unos pocos segundos en los ingresos, sin tipear caracteres sucesivos, para obtener una clave satisfactoria.

Fingerprint

La ventana de ("fingerprint")[37] muestra la huella única del Servidor de Administración, la huella es un texto derivado del certificado del Servidor de Administración.

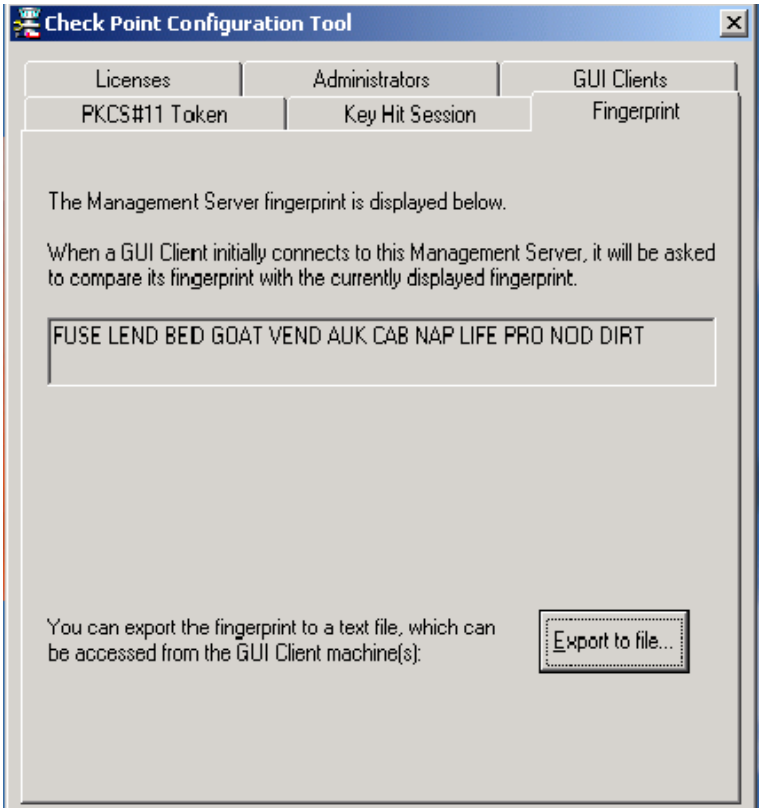

Figura 5.30 Fingerprint
Fuente: Software Check Point

Este es utilizado para verificar la identidad del Servidor de Administración cuando es accesado remotamente por un ("Gui Clients"). Al exportar el certificado este puede ser usado por el Gui Clients. En el proyecto de graduación esta opción no es utilizada.

[37] Fingerprint: fuella digital

5.2.6 Creación de Objetos

Una vez que se ha finalizado la instalación, de acuerdo al gráfico de red se procederá con la creación de los objetos de la red. Se iniciará con la definición de las estaciones de trabajo.

1.- Chkpntfw

Esta es la estación propia del firewall, para crear simplemente es necesario realizar un click derecho sobre (“Network Objects/Workstation”) y escoger (“New Workstation”).

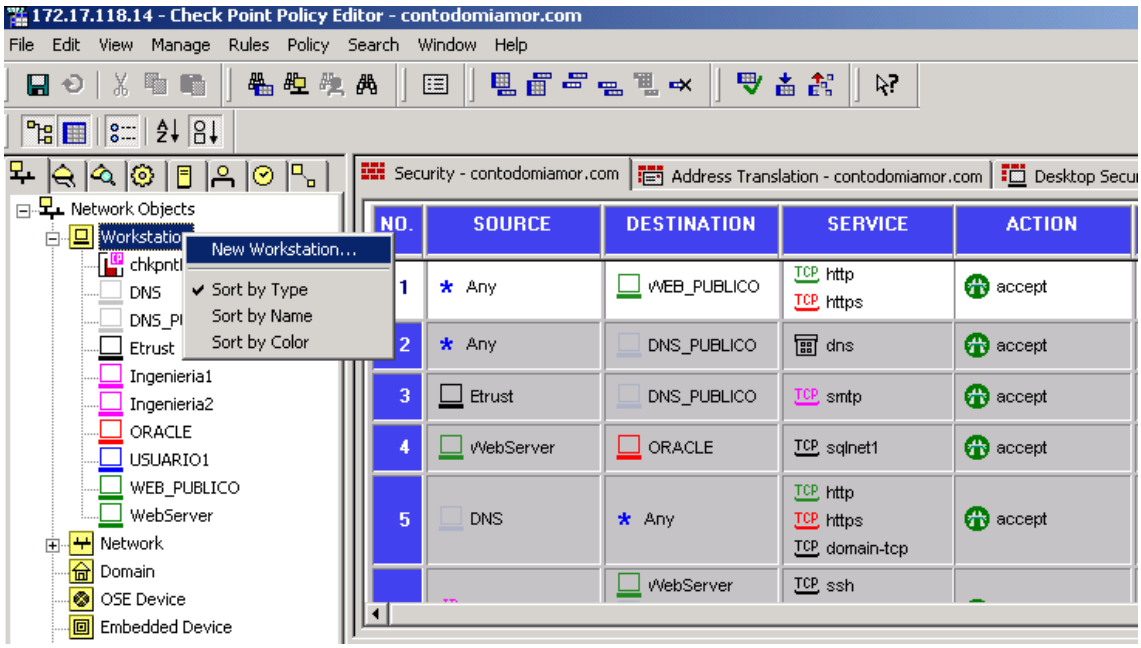

Figura 5.31 Creación de objetos de red
Fuente: Software Check Point

Luego de escoger la opción se tienen que establecer las propiedades, las cuales se dividen en cuatro: Generales, Topología, Nat y Advanced.

A continuación se ingresarán los datos en la propiedad (“Generales”):

Name: chkpntfw

Ip Address: 192.168.27.1 (es la dirección IP de la interface a la DMZ)

Comment: Opcional

Color: se escoge negro para llevar un orden por colores en los objetos.

Type: Gateway

Posteriormente se ingresan los datos en (“Topología”). Como este es el objeto firewall se deben definir las tres interfaces. Se escoge la opción (“Add”) y se procede con el ingreso de los datos por interface.

Interface 1

Name: EL90BCO

Ip Address: 200.10.149.132

Mascara de Red: 255.255.255.224

Ip Address dentro de la interface: Externa (Es la interface pública)

Anti-Spoofing: Habilitado con opción de Alerta

Interface 2

Name: rtl81391

Ip Address: 172.17.118.14

Mascara de Red: 255.255.254.0

Ip Address dentro de la interface: Interna (Es la interface interna)

Anti-Spoofin: Habilitado con opción de Alerta

Interface 3

Name: SISNIC7

Ip Address: 192.168.27.1

Mascara de Red: 255.255.255.0

Ip Address dentro de la interface: Interna (Es la interface DMZ)

Anti-Spoofin: Habilitado con opción de Alerta

El resto de propiedades como: (“Nat”), (“Vpn”), (“Autenticación”), (“Administración”) y (“Advanced”) no aplican ser configuradas para este objeto.

Los dos siguientes objetos que se crearán son (“DNS”) y (“DNS_PUBLICO”). Se van a manejar dos objetos DNS ya que se utilizará NAT para que la dirección IP real del servidor no sea vista desde el exterior.

2.- Objeto DNS

Se ingresan los siguientes datos en la sección (“Generales”):

Name: DNS

IP Address: 192.168.27.5 (es la dirección IP real del Servidor DNS)

Comment: Servidor DNS-PROXY

Color: se escoge gris para llevar un orden por colores en los objetos.

Type: Host

Topología:

No aplica

NAT:

Se utilizará el método de traducción estática

IP: 200.10.149.132 (Esta es la dirección con la que se ve el DNS desde las redes externas)

Instalar sobre: chkpntfw

3.- Objeto DNS_PÚBLICO

Se ingresan los siguientes datos en la sección (“Generales”).

Name: DNS_PUBLICO

Ip Address: 200.10.149.132 (es la dirección IP de DNS que se ve desde el exterior)

Comment: Sin comentario

Color: se escoge gris para llevar un orden por colores en los objetos.

Type: Host

Topologia, Nat y Advanced: No aplica

4.- Objeto para el E-Trust.

Se ingresan los siguientes datos en la sección (“Generales”).

Name: Etrust

IP Address: 200.10.149.133

Comment: Prueba Etrust

Color: se escoge negro para llevar un orden por colores en los objetos.

Type: Host

Topologia, Nat y Advanced : No aplica

A continuación se definirán los objetos del departamento de Ingeniería, área que se encargará de la administración de la red.

5.- Objeto Ingeniería1

Se ingresan los siguientes datos en la sección (“Generales”).

Name: Ingenieria1

IP Address: 172.17.118.120

Comment: Máquina de Ingeniería

Color: se escoge lila para llevar un orden por colores en los objetos.

Type: Host

Topologia, Nat y Advanced : No aplica

6.- Objeto Ingeniería2

Se ingresan los siguientes datos en la sección (“Generales”).

Name: Ingenieria2

IP Address: 172.17.118.125

Comment: Máquina de Ingeniería

Color: se escoge lila para llevar un orden por colores en los objetos.

Type: Host

Topologia, Nat y Advanced : No aplica

7.- Objeto Oracle

Se define un objeto para realizar el manejo de la base de datos en el firewall.

Se ingresan los siguientes datos en la sección (“Generales”).

Name: Oracle

IP Address: 172.17.118.5

Comment: Servidor ORACLE LINUX

Color: se escoge rojo para llevar un orden por colores en los objetos.

Type: Host

Topologia, Nat y Advanced : No aplica

Posteriormente se realiza la creación del objeto usuario, el cual permitirá que se pueda trabajar sobre la red establecida

8.- Objeto USUARIO1

Se ingresan los siguientes datos en la sección (“Generales”).

Name: USUARIO1

IP Address: 172.17.118.21

Comment: Usuario1

Color: se escoge azul para llevar un orden por colores en los objetos.

Type: Host

Topologia, Nat y Advanced : No aplica

Los dos siguientes objetos que se crearán son: (“WEBServer”) y (“WEB_PUBLICO”). Se van a manejar dos objetos WEB ya que se utilizará NAT con el objetivo que la dirección IP real no sea vista desde el exterior.

9.- Objeto WEBServer

Se ingresan los siguientes datos en la sección (“Generales”):

Name: WEBServer

IP Address: 192.168.27.3 (es la dirección IP real del Servidor Web)

Comment: Servidor WEB www.contodomiamor.com

Color: se escoge verde para llevar un orden por colores en los objetos.

Type: Host

Topología:

No aplica

NAT:

Se utilizará el método de traducción estática

IP: 200.10.149.134 (Esta es la dirección con la que se accesa al WebServer desde el exterior)

Instalar sobre: chkpntfw

10.- Objeto WEB_PÚBLICO.

Se ingresan los siguientes datos en la sección (“Generales”):

Name: WEB_PUBLICO

IP Address: 200.10.149.134 (es la dirección IP del web server que se ve desde el exterior)

Comment: Dirección Pública de servidor www.contodomiamor.com

Color: se escoge verde para llevar un orden por colores en los objetos.

Type: Host

Topologia, Nat y Advanced : No aplica

Una vez que se han ingresado todas las estaciones de trabajo, ahora se procederá a crear un objeto de red con el cual se va a identificar la red LAN.

11.- Objeto Red_Lan

Esta es la estación que define la red Lan, para crearla simplemente es necesario dar un click derecho sobre (“Network Objects/Network”) y a continuación escoger la opción (“New Network”).

En la sección (“General”) se establecen los siguientes parámetros:

Name: Red_Lan

IP Address: 172.17.118.0

Net Mask: 255.255.254.0

Comment: Usuarios de Red Lan

Color:Verde

Nota: Con esto queda creada la red interna 172.17.118.0/23

A continuación se definirá un rango de direcciones IP que representan las máquinas del departamento interno de Ingeniería.

12.- Objeto Ingeniería

Este es el objeto que define las direcciones IP para el área Ingeniería. Para crearla simplemente se da un click derecho sobre (“Network Objects/Address Range”) y se escoge (“New Address Range”).

En la sección (“General”) se establece lo siguiente:

Name: Ingenieria

First IP Address: 172.17.118.120

Last IP Address: 172.17.118.125

Comment: Rango de direcciones IPs de Ingenieria

Color:Lila

Con esto queda definido que desde la dirección IP 172.17.118.120 hasta la dirección IP 172.17.118.127 son direcciones para máquinas de Ingeniería.

5.2.7 Reglas

Las reglas siguientes definen el tráfico que es permitido pasar a través del firewall, definiéndose los servicios de Internet a la que la red interna tiene acceso y los servicios que la red interna ofrece al exterior.

Regla 1

En la primera regla del firewall configurado en el proyecto de graduación, se definió que desde cualquier dirección IP (“ANY”) se puede acceder al objeto (“WEB_PUBLICO”), utilizando los servicios de http y https. Se habilitarán las pistas de auditoría o logs.

Fuente:Any

Destination:WEB_PUBLICO

SERVICES: http,https

ACTION:ACCEPT

TRACK:LOG

INSTALL ON :CHKPNTFW

TIME: ANY

Con los valores configurados se permite el acceso web a la página del proyecto www.contodomiamor.com. Nótese que ésta regla se aplica sobre el objeto ("WEB_PUBLICO"), lo que permite mantener oculta la verdadera dirección IP del servidor web, previniendo un ataque malicioso.

Regla 2

En la segunda regla se define que desde cualquier dirección IP ("ANY") se puede acceder al objeto ("DNS_PUBLICO"), utilizando los servicios DNS y SMTP. Se habilitarán las pistas de auditoría o logs.

Fuente:Any

Destination:DNS_PUBLICO

SERVICES: dns, smtp

ACTION:ACCEPT

TRACK:LOG

INSTALL ON :CHKPNTFW

TIME: ANY

Con esta configuración se permite la resolución de nombres desde cualquier parte de internet hacia el servidor web del proyecto. Igualmente la regla se

aplica sobre el objeto (“DNS_PUBLICO”) protegiendo la verdadera dirección IP del Servidor DNS. Se habilitó el servicio SMTP debido a que este servidor debe estar en capacidad de aceptar correos de otros servidores SMTP; debido a que también cumple la función de servidor de correo.

Regla 3

En la tercera regla del firewall se define que se acepte el tráfico desde el objeto (“Etrust”) al objeto (“DNS_PUBLICO”), habilitando los servicios de SMTP. Se habilitarán las pistas de auditoría o logs.

```
Fuente:ETrust
Destination:DNS_PUBLICO
SERVICES: smtp
ACTION:ACCEPT
TRACK:LOG
INSTALL ON :CHKPNTFW
TIME: ANY
```

Con esta configuración se permite activar el servicio de correo para que cualquier evento sospechoso que detecte el “Etrust” sea enviado vía mail para su respectiva acción.

Regla 4

En la cuarta regla se define que se acepte el tráfico proveniente desde el ("WebServer") al objeto de la base de datos ("Oracle"). Los servicios de Oracle fueron habilitados en el puerto 1521 del "listener" y al servicio "NFS". Se habilitarán las pistas de auditoría o logs.

Fuente:WebServer
Destination:Oracle
SERVICES: sqlnet1 (Pto 1521) ; group NFS
ACTION:ACCEPT
TRACK:LOG
INSTALL ON :CHKPNTFW
TIME: ANY

Con esta configuración se permite enviar los requerimientos del Servidor Web a la Base de Datos y activar la unidad NFS del servidor de Oracle en el servidor Web, necesario para poder levantar el servicio web.

Regla 5

En la quinta regla se define que se permita al objeto ("DNS") realizar conexiones hacia servidores en Internet ("ANY") mediante los servicios de

http, https y tcp domain-tcp en el puerto 53 y smtp. Se habilitarán las pistas de auditoría o logs.

Fuente:DNS
Destination:Any
SERVICES: http,https,tco domain-tcp (Pto 53), smtp
ACTION:ACCEPT
TRACK:LOG
INSTALL ON :CHKPNTFW
TIME: ANY

Con esta configuración se permite que el servidor que cumple las funciones de correo, proxy y dns pueda descargar páginas http y https necesarios para el servicio de proxy; realizar consultas DNS para el servicio de dns y enviar correos SMTP para ofrecer el servicio de servidor de correos.

Regla 6

En la sexta regla se define que se acepte el tráfico proveniente desde las máquinas de Ingeniería (“AdressRange Ingenieria”) al (“WebServer”) y (“DNS”), por medio de los servicios ssh, ftp e icmp. Se habilitarán las pistas de auditoría o logs.

Fuente:AdressRange Ingenieria

Destination:WebServer,DNS

SERVICES: ssh,ftp,icmp

ACTION:ACCEPT

TRACK:LOG

INSTALL ON :CHKPNTFW

TIME: ANY

Con esta configuración se permite que las máquinas de Ingeniería puedan hacer ftp, ping y ssh a los servidores Web y Dns-Proxy. Es necesario recordar que los usuarios de ingeniería son los administradores de los servidores en el esquema sugerido del proyecto de graduación.

Regla 7

En la séptima regla se define que se acepte el tráfico proveniente desde las máquinas de Ingenieria (“AdressRange Ingenieria”) al objeto (“Etrust”), mediante los servicios de ICMP. Se habilitarán las pistas de auditoría o logs.

Fuente:AdressRange Ingenieria

Destination:ETrust

SERVICES: icmp

ACTION:ACCEPT

TRACK:LOG

INSTALL ON :CHKPNTFW

TIME: ANY

Con esta configuración se permite que las máquinas del área de Ingenieria puedan realizar comandos ping al servidor Etrust.

Regla 8

En la octava regla se define que desde la red interna (“Red_Lan”) se pueda acceder al objeto (“DNS”) a los servicios de dns, smtp y pop3. Se habilitarán las pistas de auditoría o logs.

Fuente: Red_Lan

Destination:DNS

SERVICES: smtp,pop3

ACTION:ACCEPT

TRACK:LOG

INSTALL ON :CHKPNTFW

TIME: ANY

Con esta configuración se habilita que los usuarios de la red interna tengan acceso para poder recibir/enviar correos.

Regla 9

En la novena regla se definió que los usuarios de la Red Lan (“Red_Lan“) puedan acceder al servicio de proxy del objeto (“DNS”). Se habilitarán las pistas de auditoría o logs.

Fuente:Red_Lan
Destination:DNS
SERVICES: proxy
ACTION:ACCEPT
TRACK:LOG
INSTALL ON:CHKPNTFW
TIME: ANY

Con esta configuración se habilitan a las máquinas de la Red Lan para que puedan navegar en Internet.

Regla 10

En la décima regla se rechaza o bloquea todo tráfico que no cumpla con cualquiera de las 9 reglas de aceptación. Se habilitarán las pistas de auditoría o logs.

Fuente:Any

Destination:Any

SERVICES: Any

ACTION:REJECT

TRACK:None

INSTALL ON :CHKPNTFW

TIME: ANY

Aprovechando las características de la tecnología de “Stateful Inspection” en CheckPoint no es necesario definir las reglas en dos sentidos, es decir sólo se define en una vía pero internamente en su funcionamiento se considera el sentido de regreso.

5.3 Monitoreo de actividad en la red – E-trust intrusion detection

“E-trust Intrusion detection” (software de la compañía Computer Associates); es una de las herramientas de detección de Intrusos más conocidas y usadas en el mercado. En esta sección se describirán las características del producto y la configuración realizada en la implementación del proyecto.

5.3.1 Características

En el manual incluído con el software de instalación, se destacan las siguientes características de esta herramienta:

- Control de acceso a la red: Usa reglas básicas para definir qué usuarios pueden acceder a recursos específicos en la red, asegurando sólo accesos autorizados a los recursos de la red.
- Ingeniería avanzada Antivirus: una ingeniería de escaneo de virus detecta el tráfico de red conteniendo virus de computadores. Protege a los usuarios de descargas inocuas de archivos infectados de virus. Las firmas de virus nuevas y actualizadas están disponibles en el website de Computer Associates.
- Librería de patrones de ataques: automáticamente detecta patrones de ataques del tráfico de red, aún mientras están en progreso. Regularmente las firmas de ataques actualizadas, disponibles en el website, aseguran que la aplicación permanezca actualizada.
- Tecnología “packet sniffing”: Opera en modo no detectable, permaneciendo invisible a los atacantes. Los hackers son a menudo atrapados, ya que ellos no saben que están siendo vigilados.
- Bloqueo de URL: Los administradores pueden designar los URL’s que los usuarios no están permitidos visitar, previniendo la navegación improductiva.
- Escaneo de patrones de palabras: Los administradores pueden definir patrones de palabras que pueden indicar violación de políticas. Esto previene que datos sensitivos sean enviados vía mail o web sin autorización.

- Uso de logs de la red: Habilita a los administradores de la red a realizar un seguimiento del uso de la red por los usuarios finales, aplicaciones, etc. Ayuda a mejorar la planeación de políticas de red.

Con todas estas características se busca analizar desde una manera más detallada todo el tráfico que puede contener código mailicioso antes que sea procesado por el Firewall.

5.3.2. Capacidades

Según Computer Associates Internacional (2001) con la implementación de eTrust en múltiples localidades dentro de la empresa, sus poderosas capacidades protegen la red entera. Esto incluye el monitoreo y respuesta a los eventos del lado empresa desde una consola remota o una centralizada de consolidación. También incluye un repositorio central de eventos, reportes adicionales y una presentación visual distribuida.

Provee del lado de la red, una protección confiable y distribuida en tiempo real, permitiendo que cada instancia del eTrust sea totalmente funcional y opere en forma autónoma, evitando dependencias en la disponibilidad de la red o tiempo de respuesta.

Monitoreo centralizado: los administradores de red pueden monitorear y controlar una o más estaciones local o remotamente. Instalando eTrust en

diferentes segmentos de la red (local o remotamente), los cuales estarían controlados por una estación central, el administrador puede ver alertas y generar reportes basados en la información consolidada.

Administración remota: usuarios remotos pueden acceder a una estación corriendo eTrust, usando TCP/IP. Una vez conectado, el usuario puede ver y monitorear los datos, cambiar las reglas, y crear reportes, dependiendo de los permisos definidos para el usuario administrador del eTrust.

Log de intrusos y análisis: provee un sistema comprensivo para capturar la información y convirtiendo los datos disponibles para su análisis. Después de la instalación del software y designando una localidad de archivo, el usuario define una regla que graba los datos de la sesión en un archivo. Entonces, los usuarios pueden usar el navegador de la aplicación para filtrar, ordenar y ver la información archivada y crear reportes detallados.

5.3.3. Conceptos básicos

5.3.3.1. Cómo procesa el tráfico de red

El eTrust una vez activado, escucha todo el tráfico TCP/IP que pasa a través de la red. Tiene la habilidad de identificar ataques en la red contra servidores específicos o contra la red entera. Se puede revisar el log de todas las actividades asociadas con sesiones sospechosas, obtener estadísticas y

reportes detallados de ellas, y reconstruir las sesiones de manera que habilita ver lo que fue hecho por usuarios específicos o la estructura de un ataque.

Puede reaccionar en tiempo real cuando un problema es encontrado, notificando al usuario vía mail, fax, etc. Como un firewall, también bloquea comunicaciones ilegales. (Computer Associates Internacional, 2001)

Procesa el tráfico de red de la siguiente manera:

1. Chequea cada nueva sesión en la red, para ver si este está definido como un servicio excluído.
2. Si es un servicio excluído, ignora la sesión.
3. Si no es un servicio excluído, la sesión es incluida en las estadísticas y el proceso continúa.
4. Entonces chequea que la sesión coincida con una definición de una de las reglas. El orden del chequeo es como sigue:

   Primero, chequea si el evento está definido como bloqueado por protocolo para todo el tráfico. Si hay una coincidencia, la sesión es terminada. Entonces, chequea si el evento está definido como un URL para ser bloqueado. Si hay coincidencia, la sesión es terminada.
5. Si la primera regla no es conocida, el programa chequea la segunda regla, así sucesivamente, hasta una regla que coincida, o que todas

las reglas hayan sido chequeadas. El orden del chequeo entre matrices es como sigue:

- Reglas de detección de intentos de intrusión
- Reglas de inspección de contenido
- Reglas de monitoreo de acceso y control a URL's
- Reglas de Monitoreo/Bloqueo/Alertas

Chequea cada sesión contra las reglas hasta que la sesión termine o una coincidencia ocurra.

6. Si hay una coincidencia, la acción definida para la sesión ocurre (log o notificación) y las demás reglas hacia abajo de la regla de coincidencia son ignoradas.

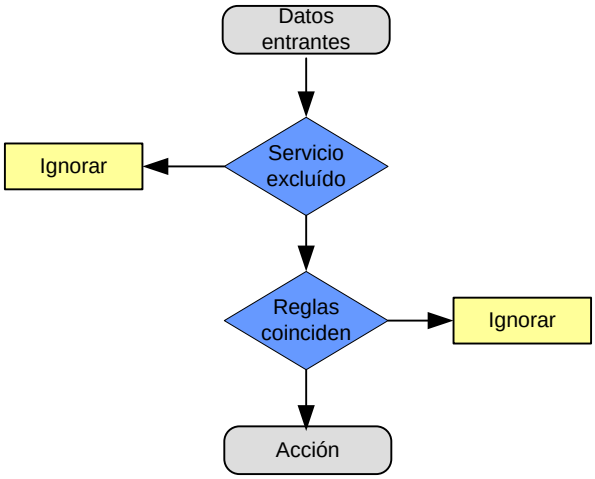

Figura 5.32 Orden de revisión de reglas
Fuente: CD de distribución E-trust

Todo tráfico es analizado en base al algoritmo propuesto por la herramienta, evaluando inicialmente servicios y luego reglas.

5.3.3.2. Arquitectura dos capas

La arquitectura dos capas, le da la habilidad de ver y administrar la información crítica de la red localmente o desde una estación remota. La arquitectura dos capas consiste en un componente Motor ("Engine") y un componente Visor ("Viewer") que separa los datos recolectados y analiza desde la vista y configuración de aplicación. (Computer Associates Internacional, 2001)

El componente Motor, opera como un servidor en una máquina Windows NT/2000, realiza las siguientes tareas:

- detecta intrusos
- graba datos de sesiones y estadísticas
- bloquea sesiones
- envía alertas y notificaciones al componente Vista
- actúa a las peticiones del Vista

Los datos recolectados por Motor son grabados en un espacio de trabajo (workspace). Cuando un Visor se conecta al Motor, el usuario ve una figura actual del "*workspace"* que es periódicamente actualizado. Toda la información crítica, alertas, y notificaciones, sin embargo aparecen en tiempo real.

El Visor realiza las siguientes tareas:

- presenta las alertas de intrusiones
- presenta los datos de la sesión y actualiza esta información manual o automáticamente en intervalos predefinidos
- presenta los logs de las sesiones en demanda desde el Motor
- permite la configuración del Motor (dependiendo de los permisos del usuario).

Un Visor puede correr remotamente o en la misma máquina como el Motor, y uno o más Visores pueden simultáneamente conectarse al mismo Motor.
Solo un Visor a la vez, local o remoto, puede bloquear un Motor y hacer cambios en la configuración. Para bloquear un Motor, el Visor debe tener derechos de administrador. Cuando un usuario bloquea un Motor, este usuario tiene total acceso al Motor y cualquier cambio hecho a su configuración será grabado.

5.3.3.3 Requerimientos de Software

Etrust funciona en su Versión “Standalone” con los siguientes sistemas operativos: Windows 98, Windows Me, Windows 2000 (original o SP1), Windows NT 4.0 (equipado con SP5o SP6).

Versión Engine Remota: Windows 2000 (original o SP1), Windows NT 4.0 (equipado con SP5o SP6) (Computer Associates Internacional, 2001)

Para la implementación del proyecto se utilizó la versión Standalone ubicado en la red pública.

5.3.3.4 Requerimientos mínimos de hardware

Según Computer Associates los requerimientos de hardware que eTrust necesita para operar adecuadamente son los siguientes:

- CPU Pentium II 500 MHz
- 128 MB RAM (256 MB recomendado)
- 500 MB de espacio libre en disco
- Al menos un adaptador de red estándar

Como se observa en la descripción sugerida, para el funcionamiento de esta herramienta no es necesario un equipo de gran rendimiento.

5.3.4 Definición de parámetros

El eTrust monitorea y bloquea eventos de red a través de reglas. Cuando se define una regla, se pueden seleccionar parámetros para la misma o definir los parámetros desde dentro de la matriz de la regla.

Los parámetros que se pueden definir son los siguientes:

- Objetos de la red
- Servicios
- Tipos de reglas
- Acciones
- Usuarios elegibles

A continuación se describirá brevemente cada uno de los parámetros mencionados.

5.3.4.1 Objetos de la red

Son estaciones o grupo de estaciones que pueden definirse como un cliente o servidor cuando se está definiendo los parámetros de una regla. Un objeto de red puede incluir:

- Todas o estaciones específicas de la red
- Un rango de estaciones
- Usuarios de estaciones de trabajo
- Estaciones que comparten un sufijo de dominio específico
- Un grupo de estaciones
- Todas las estaciones en la red interna
- Todas las estaciones fuera de la red interna
- Todos los objetos de red a excepción de objetos específicos

Cada objeto de la red definido es un participante del flujo de información entre la red interna e Internet.

5.3.4.2 Servicios

Cuando se definen reglas, se necesita decidir que servicios se monitorearán o bloquearán. Para definirlos, se debe indicar un nombre, el protocolo (TCP o UDP), el puerto o rango de puertos que usará.

5.3.4.3 Tipos de reglas

Un tipo de regla define el criterio de búsqueda para una sesión. Pueden ser basados en servicios o en contenido.

5.3.4.4 Acciones

Una acción es una respuesta que ocurre cuando una sesión coincide con las condiciones de la regla. eTrust incluye un número de acciones predefinidas y también permite crear una acción personalizada.

Pueden estar basadas en servicio, paquete o estadística.

Entre las más usadas están:

- Registro de detalles del evento
- Bloquear la sesión
- Enviar un mensaje mail
- Archivar un log

En el esquema del proyecto se utilizó el bloqueo de sesiones, el registro en logs y el envío de correo electrónico al administrador de la red.

5.3.4.5 Usuarios

Por la naturaleza sensitiva de la información que recolecta eTrust, sólo el administrador de la red tiene total acceso a las funciones del eTrust. Sin embargo, el administrador puede permitir que otros usuarios vean detalles de las reglas de coincidencia.

5.3.5. Configuración del proyecto

5.3.5.1 LOGIN

Una vez realizada la instalación, la primera vez que se inicia eTrust, aparecerá una ventana de diálogo, solicitando la contraseña del usuario ("ADMINISTRATOR"). Si se desea especificarla en ese momento se lo puede hacer, caso contrario se lo puede hacer luego una vez iniciado la sesión.

5.3.5.2 Configuraciones de Red

Las primeras configuraciones están relacionadas con las direcciones de red.

En la ruta "Menú→ Settings→Options" En el primer "Tab", llamado "Network", se especifica la dirección IP del equipo, en este caso: 200.10.149.128 y la submáscara: 255.255.255.224.

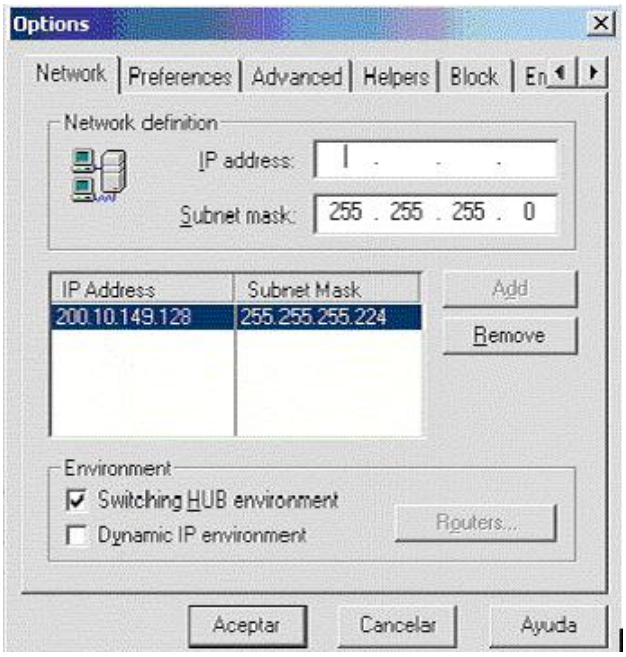

Figura 5.33 Configuración de Red
Fuente: CD de distribución E-trust

Después en el tab (“Preferences”) se debe configurar lo siguiente:

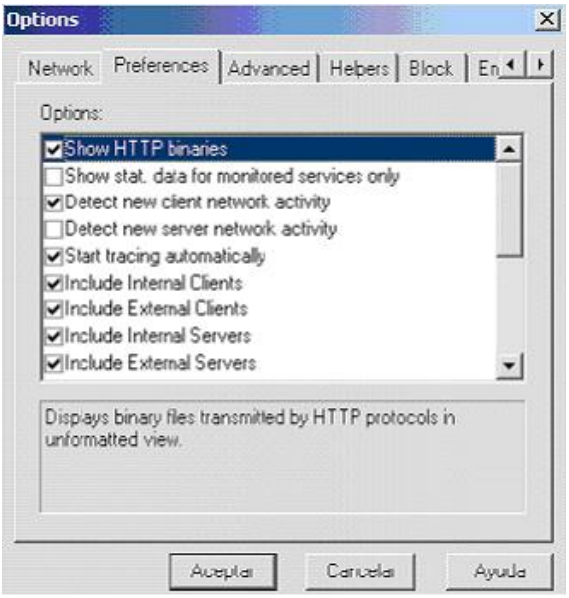

Figura 5.34 Configuración de Preferencias
Fuente: CD de distribución E-trust

Se mantienen activadas las opciones que vienen por defecto:

"Show http binaries". Presenta archivos binarios transmitidos por protocolos http en una vista sin formato.

"Detect new cliente network activity". Presenta una lista de nuevas actividades de red para cliente que el programa detecte.

"Start tracing automatically". Inicia automáticamente el monitoreo de la actividad de red, cuando el programa es activado.

"Include Internal Clients". Incluye todos los clientes internos de la red en el monitoreo.

"Include External Clientes". Incluye todos los clientes externos de la red en el monitoreo.

"Include Internal Servers". Incluye todos los servidores internos de la red en el monitoreo.

"Include External Servers". Incluye todos los servidores externos de la red en el monitoreo.

"Enable whole network detection". Habilita la detección de máquinas corriendo este software, aún si ellos están localizados fuera del segmento local.

"Enable active DNS name resolving". Habilita el programa de resolución de DNS para resolver todas las direcciones IP de la red.

"Show MAC (instead of IP) in dyanamic IP environment". Muestra la dirección MAC en vez de la dirección IP cuando no hay resolución de DNS.

"Enable email notification". Habilita el envío de notificaciones email a usuarios cuyos mensajes email están grabados para el sistema.

"Recover workspace automatically". Automáticamente invoca la aplicación Administradora para recuperar "workspace" después de una terminación anormal del programa.

Luego se procede a configurar el tab ("Email")

Figura 5.35 Configuración de Email
Fuente: CD de distribución E-trust

Se especifica la dirección IP del servidor de correo SMTP: 200.10.149.132

Y la dirección de correo del administrador, para enviar mensajes de alerta:

`idsadmin@contodomiamor.com`

5.3.5.3 REGLAS

Se activaron todas las reglas que vienen por defecto con el eTrust, de manera que siempre esté sensando el tráfico de red, sin importar el destino u origen.Se configuraron las acciones de la siguiente manera:

Log Mensaje de Alerta (Como sujeto la regla y en el cuerpo el detalle de la infracción) Email a ingenieria@contodomiamor.com“Sound Standard speaker beep".- El cual habilita la emisión de un sonido cuando se detecta una actividad sospechosa.

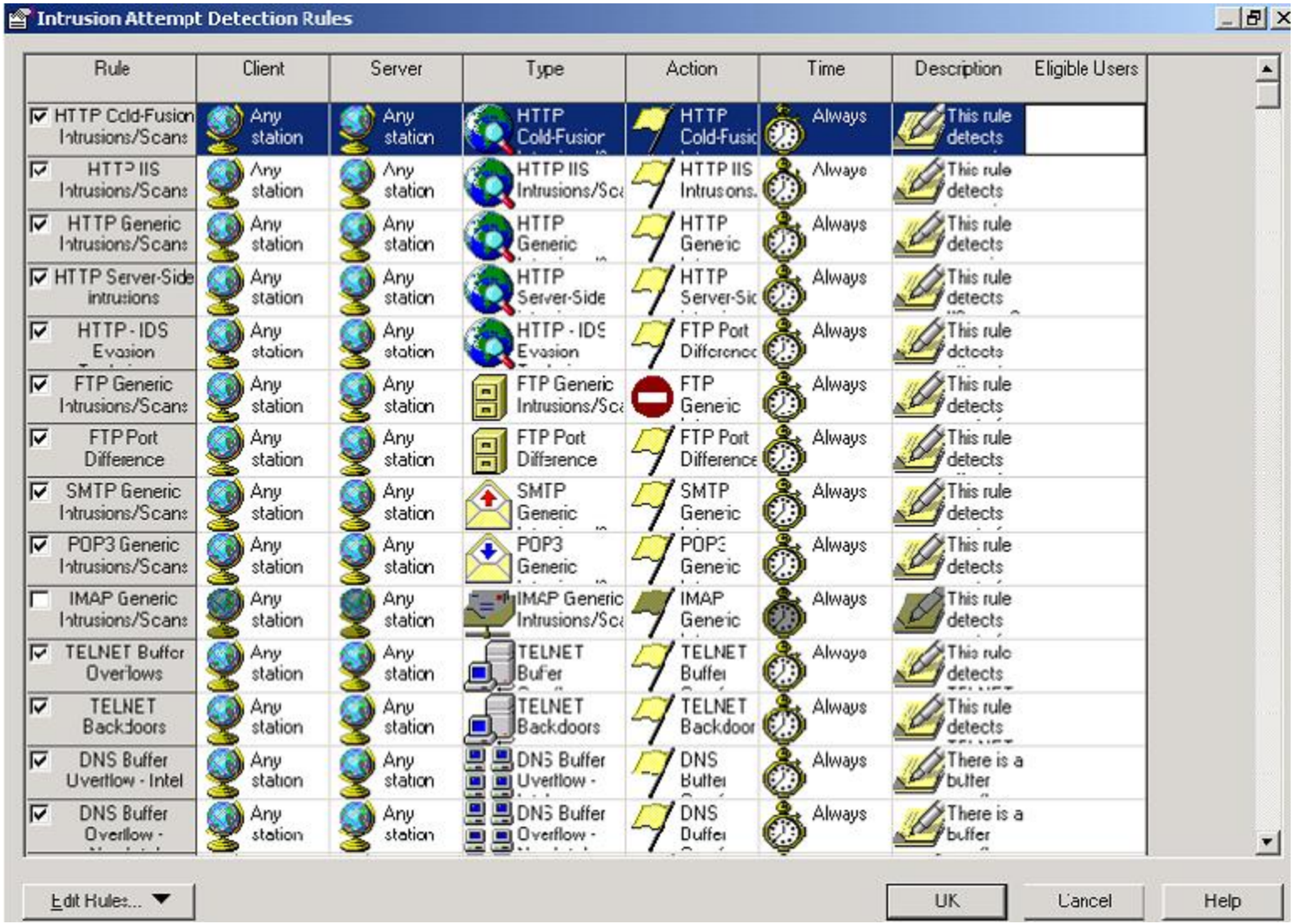

Figura 5.36 Matriz de Reglas de Detección de Intentos de Intrusión Fuente: CD de distribución E-trust

5.3.5.3.1 Reglas de Detección de Intentos de Intrusión

“HTTP Cold-Fusion Instrusions/Scan”.
“HHTP IIS Intrusions/Scans”.
“HTTP Generis Intrusions/Scans”.
“HTTP Server-Side intrusions”.
“HTTP – IDS Evasion techniques”.
“FTP Generic Intrusions/Scans”.
“FTP Port Difference”.
“SMTP Generic Intrusion/Scans”.
“POP3 Generic Instrusion/Scans”.
“IMAP Generic Intrusion/Scans”.
“TELNET Buffer overflow”.
“TELNET Backdoors”.
“DNS Buffer Overflow – Intel”.
“DNS Buffer Overflow – Non Intel”.
“Dig attack over TCP”.
“NetBus remote administration”
“cDc Back Orifice Backdoor”.
“BOOTPD Buffer Overflow”.
“INETD Buffer Overflow”.
“INETD Newline Vulnerability”
“Girlfriend 1.3 Backdoor”

“BncBuffer Overflow”.
“SCO Unix Calendar Vulnerability”
“Cisco DoS Vulnerability”
“Wingate Redirector DoS”
“Windows NT RAS DoS”
“Vulnerability in pop2d”
“Compaq Insight Manager”
“Cmail vulnerabilities”
“NetBus II Activity”
“Back Orifice 2000 – TCP”
“Back Orifice 2000 – UDP”
“FakeBO Buffer Overflow”
“World Cliente DoS Vulnerability”
“WebConfig DoS Vulnerability”
“Ultraseek Buffer Overflow”
“Connection to Trinoo Daemon”
“Connection to Trinoo Master”

El conjunto de reglas indicado viene predefinido en la herramienta, y pueden ser continuamente actualizadas para prevenir nuevos tipos de accesos maliciosos.

5.3.5.3.2 Reglas de detección de actividad sospechosa en la red

Cada flujo de información que circula por el segmento de red pública es analizado en busca de patrones de comportamiento propio de códigos maliciosos. El tipo de detección implementado por la herramienta se basa en paquetes y estadísticas.

A continuación se detalla los dos tipos de detecciones.

Reglas basadas en Paquetes

Las siguientes reglas analizan cada paquete entrante en búsqueda de fallas intencionales en las cabeceras de los mismos, con lo cual se trata de desestabilizar el sistema del equipo destino. La herramienta posee los siguientes tipos de reglas:

- *"Land attack":* Este tipo de regla captura los paquetes, donde la direcciones fuente/destino en el encabezado IP y los puertos fuente/destino en el encabezado IP son los mismos, y la bandera de sincronización en el encabezado TCP es establecido. Estos paquetes pueden causar que la máquina destino deje de responder.
- *"Null scan":* Esta regla captura paquetes donde no hay banderas fijadas en el encabezado TCP. Estos paquetes son enviados por *"scaners"*[88] para hacer una búsqueda de puertos invisibles en el destino, o detectar su sistema operativo.

[38] Husmeadores que revisan que servicios están publicados en la red

- *"Stealth FIN scan":* Esta regla captura los paquetes donde solo la bandera FIN está establecida en el encabezado TCP. Estos paquetes son enviados por *"scaners"* para hacer una búsqueda de puertos invisibles en el destino, o detectar su sistema operativo.
- *"Xmas scan":* Captura paquetes donde las banderas FIN, URG y PUSH están establecidas en el encabezado TCP.
- *"TCP scan with S fingerprinting":* Captura paquetes donde las banderas FIN, URG y PUSH están configuradas en el encabezado TCP.
- *"QUESO scan":* Captura paquetes donde el espacio reservado en el encabezado TCP no es igual a cero.
- *"TCP packets overlapping":* Un atacante envía paquetes TCP fragmentados que se traslapan en el destino. Esto puede causar que el sistema de detección de intrusos pierda el ataque.
- *"UDP flooding":* Un atacante envía un paquete UDP y TCP fragmentados que se traslapan en el destino. Esto puede causar que el sistema de detección de intrusos pierda el ataque.
- *"WinNuke attack":* Enviando fuera de banda (especialmente al puerto 139) puede causar un mal funcionamiento del Winsock.
- *"Broadcast, multicast or loopback source IP":* Apariencia *"Broadcast"*, *"multicast"* o "*anycast",* como la dirección IP del paquete fuente puede

indicar un intento para usar la estación destino como un amplificador de inundación.

- *"Smurf (Pong) attack".* Enviando *"ICMP echo request"* con el destino broadcast y modificar la dirección IP fuente puede causar denegación de servicio en la estación fuente por la gran cantidad de ICMP replicados que recibe.
- *"ICMP Redirect Packet":* Enviando mensaje *"ICMP Redirect"* con una dirección ilegal puede causar que la estación destino pare de responder o causa la degradación del rendimiento.

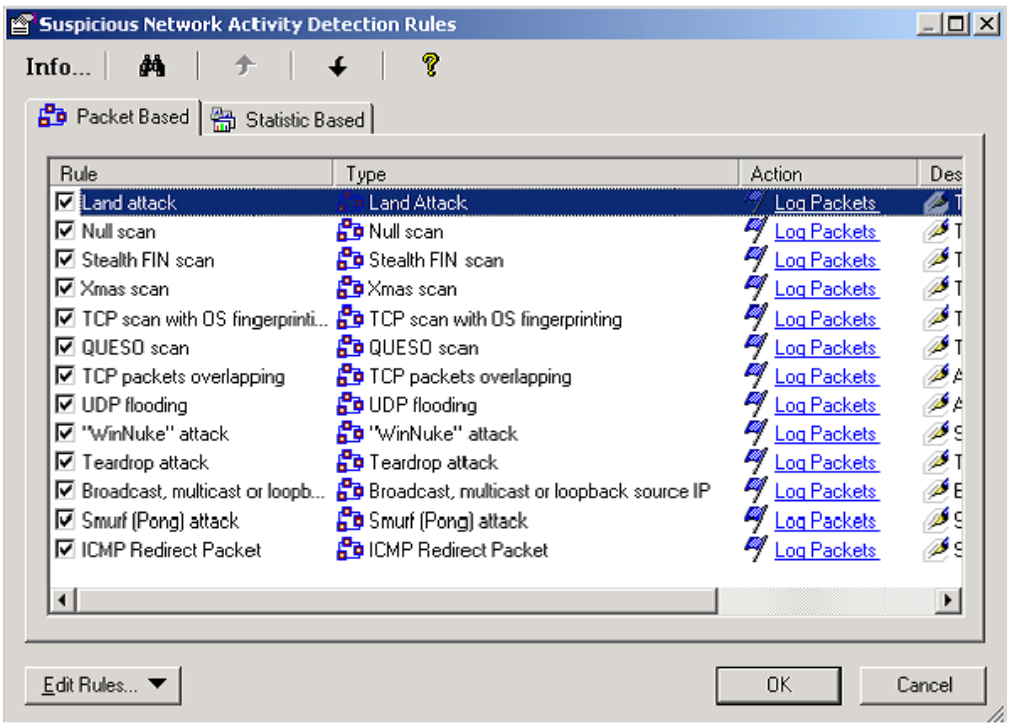

Figura 5.37 Reglas de detección de actividad sospechosa en la red basada en paquetes
Fuente: CD de distribución E-trust

Para el esquema del proyecto se habilitaron todas las reglas basadas en paquetes provistas por eTrust.

Reglas basadas en Estadística

A través de este tipo de reglas se realiza un análisis estadístico del flujo de información entrante buscando anormalidades que pueden ser origen de un ataque malicioso. A continuación se detallan las reglas basadas en estadística provistas por eTrust:

- *"Ping Flooding":* Paquetes ping ICMP son enviados con una alta frecuencia inusual.
- *"Ping Abuse":* Inusualmente paquetes ping ICMP muy largos son enviados.
- *"SYN attack":* Inusualmente grandes cantidades de sesiones TCP "medio abiertas" para un servidor.
- *"TCP Port scan":* inusualmente grandes cantidades de sesiones TCP abiertas para un servidor con un bajo promedio de cantidad de datos.
- *"UDP Port scan":* inusualmente gran cantidad de paquetes UDP son enviados a un host por un rango amplio de puertos.
- *"Sweep attack":* Frecuentemente se presenta enviando ICMP echo request a varios destinos puede ser usado para probar un sistema.
- *"Distribuided Denial of Service Attack":* Se puede enviar cantidades anormales de datos usando puertos aleatorios TCP o UDP así como comunicación ICMP.
- *"Stream-like DoS Attack":* Se puede decrementar dramáticamente la productividad del switching en hubs y routers.

- *"IP Spoofing":* Una dirección IP interna es acompañada con la dirección MAC del router.
- *"MAC Spoofing":* Dos direcciones MAC diferentes son detectadas con la misma dirección interna IP.
- *"eTrust Detection Spoofing":* Un atacante puede enviar gran cantidad de paquetes de detección forjados para causar condiciones de denegación de servicio en el Sistema Detector de Intrusos.

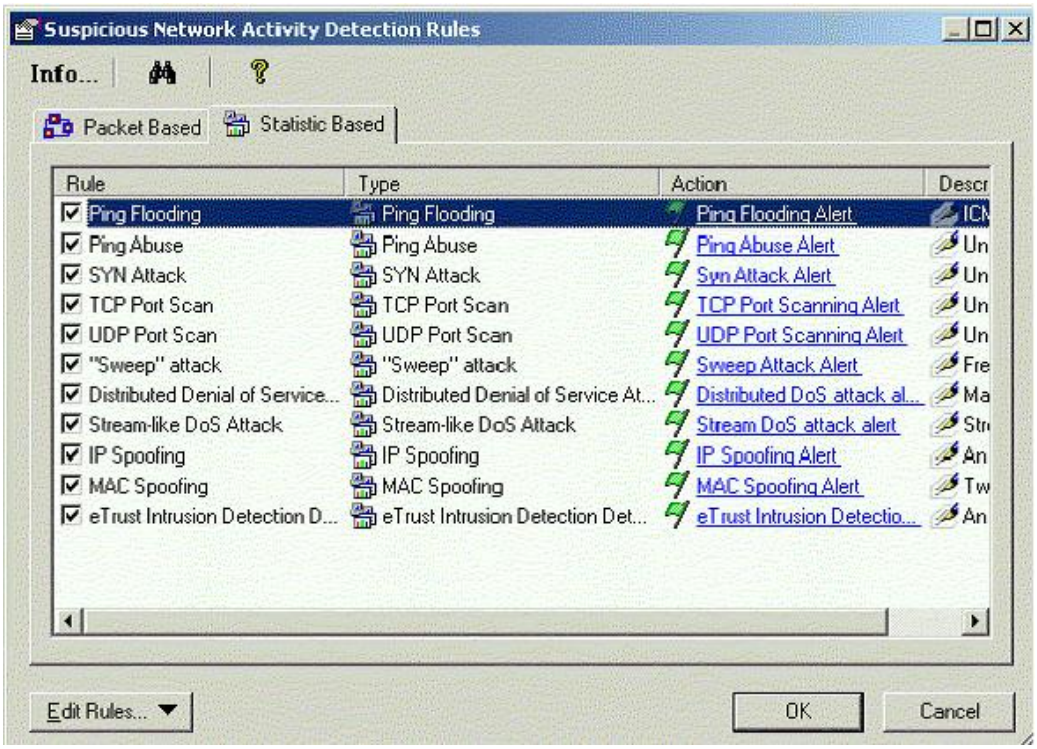

Figura 5.38 Reglas de detección de actividad sospechosa en la red basada en estadísticas
Fuente: CD de distribución E-trust

Para el esquema del proyecto se habilitaron todas las reglas basadas en estadísticas provistas por eTrust.

Nota Importante:

En el equipo donde se tiene instalado eTrust Intrusion Detection, en la configuración de red de Windows 2000 Server, sección (“Propiedades de Protocolo Internet TCP/IP”), (“Avanzadas”), (“Opciones”), se presenta la configuración opcional de Filtro TCP/IP.

Al ingresar, se presenta la siguiente opción:

Habilitar filtro TCP/IP (Todos los adaptadores)

Al ser seleccionado, presenta las siguientes dos opciones:

Permitir Todos (puertos TCP, UDP, IP)
Permitir Solo (puertos TCP, UDP, IP)

En todos los casos (puertos TCP, UDP, IP), se debe indicar (“permitir solo”) y dejar las listas en blanco.

Mediante esta configuración se permite que el equipo pueda analizar el tráfico pero no pueda responder a ninguna solicitud, de manera que se estaría simulando un modo no detectable, en caso de que un atacante esté monitoreando la red en busca de equipos de detección de intrusos.

5.4. LINUX IPTABLES.- Firewall de base de datos.

5.4.1. Acerca de iptables

Iptables; “IP packet filter administration” (administración de filtro de paquete IP), es la herramienta que permite configurar, mantener e inspeccionar las tablas de reglas de filtrado de paquetes IP en el kernel de Linux, desde su versión 2.4 (en 2.2 era ipchains). Con esta herramienta se puede crear un firewall adaptado a necesidades específicas (Fernández, 2000).

Su funcionamiento es simple: a Iptables se le proporcionan unas reglas, detallando en cada una de ellas determinadas características que debe cumplir un paquete y se especifica una acción. Las reglas tienen un orden, y cuando se recibe o se envía un paquete, las reglas se recorren ordenadamente hasta que las condiciones se cumplen. Finalmente la regla se activa realizando sobre el paquete la acción que le haya sido especificada.

Estas acciones se plasman en lo que se denominan objetivos, los cuales indican lo que se debe hacer con el paquete. Los objetivos más utilizados son bastante explícitos: “ACCEPT” (aceptar), “DROP” (caer) y “REJECT” (rechazar), pero también hay otros que permiten funcionalidades adicionales: “LOG”, “MIRROR”, “QUEUE”, “RETURN”, “MARK”, entre otros.

En cuanto a los paquetes, el sistema de filtrado de paquetes del kernel se divide en tres tablas, cada una con varias cadenas a las que puede pertenecer un paquete, de la siguiente manera:

- “filter”: tabla por defecto, para los paquetes que se refieran a nuestra máquina.
  - “INPUT”: paquetes recibidos para nuestro sistema
  - “FORWARD”: paquetes enrutados a través de nuestro sistema
  - “OUTPUT”: paquetes generados en nuestro sistema y que son enviados

- “nat”: tabla referida a los paquetes enrutados en un sistema con traducción de direcciones IP o enmascaramiento:
  - “PREROUTING”: para alterar la ruta de los paquetes según ingresen
  - “OUTPUT”: para alterar paquetes generados localmente antes de enrutar
  - “POSTROUTING”: para alterar los paquetes cuando están a punto para salir

- “mangle”: alteraciones más especiales de paquetes:
  - “PREROUTING”: para alterar los paquetes entrantes antes de enrutar

- “OUTPUT”: para alterar los paquetes generados localmente antes de enrutar

Dado que el soporte para el firewall está integrado en el kernel de Linux (Netfilter), para poder usar iptables se tendrá que asegurar que el núcleo admite el uso de iptables. (Fernández, www.elrincondelprogramador.com/autores.asp?id=10).

En la actualidad, la mayoría de sistemas basados en Linux poseen soporte para la implementación de iptables.

5.4.2. Uso básico de iptables

El ejecutable de iptables generalmente reside en la ruta “/sbin/iptables”. A continuación se presentan los comandos básicos de iptables (Israel E. Bethencourt, http://www.informaticos.biz/)

- Crear una nueva regla al final de las ya existentes en una cadena determinada

```
$ /sbin/iptables -A [chain] [especif_de_la_regla] [opciones]
```

- Insertar una regla en una posición determinada de la lista de reglas de una cadena determinada

```
$ /sbin/iptables -I [chain] [posición] [especif_de_la_regla] [opciones]
```

- Borrar una regla en una posición determinada de la lista de reglas de una cadena determinada

```
$ /sbin/iptables -D [chain] [posición]
```

- Borrar todas las reglas de una cadena determinada

```
$ /sbin/iptables -F [chain]
```

- Listar las reglas de una cadena determinada

```
$ /sbin/iptables -L [chain]
```

Estos son los comandos básicos y generales utilizados en la definición de reglas, por ende es importante conocer la sintaxis para estar de capacidad de configurar reglas.

5.4.3. Reglas definidas en el Firewall Interno

La principal funcionalidad del firewall interno es garantizar la seguridad del servidor de base de datos. A continuación se detalla cada una de las reglas definidas en el firewall.

5.4.3.1. Reglas generales

Las primeras reglas eliminan cualquier regla definida con anterioridad en el firewall.

```
/sbin/iptables -F
/sbin/iptables -t nat –F
```

A continuación se definen las políticas generales del Firewall; por defecto todo paquete entrante, saliente y que pasa a través del mismo es descartado.

```
/sbin/iptables -P INPUT DROP
/sbin/iptables -P OUTPUT DROP
/sbin/iptables -P FORWARD DROP
```

A continuación se establece que el equipo permita el traspaso de paquetes entre sus interfaces (Forwarding).

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Las siguientes reglas deniegan paquetes fragmentados, es decir aquellos que su tamaño está por debajo de 40 bytes[39]. Esto se aplica tanto para conexiones que son dirigidas al firewall (regla INPUT) y para aquellas que pasan a través de él (regla FORWARD). Los paquetes fragmentados son utilizados para realizar ataques de denegación de servicio. Esta regla evita ataques de tipo "Tiny Fragment Attack" (Ataque de fragmentos diminutos)

```
iptables -A INPUT -i eth0 -f -m length --length 0:63 -j DROP
iptables -A FORWARD -i eth0 -f -m length --length 0:63 -j DROP
```

A continuación se detallan las reglas correspondientes a conexiones locales al Firewall. Las primeras reglas permiten que el Firewall realice conexiones entre sí mismo a través de todas sus interfaces y direcciones IP.

```
/sbin/iptables -A INPUT -s 127.0.0.1/32 -d 127.0.0.1/32 -j ACCEPT
/sbin/iptables -A INPUT -s 172.17.118.5/32 -d 172.17.118.5/32 -j ACCEPT
/sbin/iptables -A INPUT -s 192.168.15.1/32 -d 192.168.15.1/32 -j ACCEPT
/sbin/iptables -A OUTPUT -s 127.0.0.1/32 -d 127.0.0.1/32 -j ACCEPT
/sbin/iptables -A OUTPUT -s 172.17.118.5/32 -d 172.17.118.5/32 -j ACCEPT
/sbin/iptables -A OUTPUT -s 192.168.15.1/32 -d 192.168.15.1/32 -j ACCEPT
```

En las reglas siguientes se otorgan determinados privilegios a la red 172.17.118.120/29 (esto incluye direcciones IP desde la 172.17.118.120

[39] Ethernet define que paquetes menores a 64 bytes son paquetes fragmentados pertenecientes a colisiones.

hasta la 172.17.118.127). La red en mención corresponde al departamento de Ingeniería, los cuales necesitan dichos permisos para poder monitorear y administrar los servidores dentro de la red de datos.

5.4.3.2. Conexiones Entrantes

Se define como conexiones entrantes a aquellas conexiones que el Firewall permite que se le realicen por alguna de sus interfaces. A continuación se detalla cada una de ellas.

Se permite que desde el área de Ingeniería se puedan realizar conexiones del tipo ssh (puerto 22) hacia el Firewall a través de la interfaz eth0.

```
/sbin/iptables -A INPUT -i eth0 -s 172.17.118.120/29 -p tcp --dport 22 -j ACCEPT
/sbin/iptables -A OUTPUT -o eth0 -d 172.17.118.120/29 -p tcp --sport 22 -j ACCEPT
```

Se permite la ejecución de comandos ICMP desde la red de ingeniería a las interfaces del Firewall.

```
/sbin/iptables -A INPUT -s 172.17.118.120/29 -p icmp --icmp-type echo-request -j ACCEPT
/sbin/iptables -A OUTPUT -d 172.17.118.120/29 -p icmp --icmp-type echo-reply -j ACCEPT
```

Dado que la política definida en las conexiones entrantes se basa en descartar los paquetes, solamente aquellos paquetes que coinciden con las reglas que se han establecido con el objetivo “ACCEPT” serán permitidos.

5.4.3.3. Conexiones Salientes

Se entiende por conexiones salientes a aquellas conexiones que el firewall puede realizar a través de sus interfaces.

Se permite que el Firewall establezca conexiones del tipo ssh hacia el servidor de base de datos Oracle.

```
/sbin/iptables -A OUTPUT -o eth1 -d 192.168.15.0/24 -p tcp --dport 22 -j ACCEPT
/sbin/iptables -A INPUT -i eth1 -s 192.168.15.0/24 -p tcp --sport 22 -j ACCEPT
```

Se permite que el Firewall pueda hacer ping a cualquier equipo de la red.

```
/sbin/iptables -A OUTPUT -d 0/0 -p icmp --icmp-type echo-request -j ACCEPT
/sbin/iptables -A INPUT -s 0/0 -p icmp --icmp-type echo-reply -j ACCEPT
```

Los paquetes que coincidan con las reglas definidas para conexiones salientes serán permitidas, todas las demás serán descartadas.

5.4.3.4. Forwarding

Las reglas que se describen a continuación, son aquellas que permiten el flujo de paquetes a través de las interfaces del firewall, cumpliendo la función de puerta de enlace.

Se permite el acceso al servidor Oracle (192.168.15.5) desde el servidor Web (200.10.149.134). Básicamente los servicios permitidos son oracle “listener” (manejador de peticiones de la base de datos - puerto 1521) y NFS (sistema de archivos de red).

```
/sbin/iptables -A FORWARD -s 200.10.149.134 -d 192.168.15.5 -p tcp -m multiport --dport 1521,2049,111 -j ACCEPT
/sbin/iptables -A FORWARD -s 192.168.15.5 -d 200.10.149.134 -p tcp -m multiport --sport 1521,2049,111 -j ACCEPT
/sbin/iptables -A FORWARD -s 200.10.149.134 -d 192.168.15.5 -p udp -j ACCEPT
/sbin/iptables -A FORWARD -s 192.168.15.5 -d 200.10.149.134 -p udp -j ACCEPT
```

Se permite que desde el área de Ingeniería se pueda administrar al servidor de bases de datos por medio de una sesión encriptada (ssh).

```
/sbin/iptables -A FORWARD -s 172.17.118.120/29 -d 192.168.15.5/32 -p tcp --dport 22 -j ACCEPT
/sbin/iptables -A FORWARD -s 192.168.15.5/32 -d 172.17.118.120/29 -p tcp --sport 22 -j ACCEPT
```

Se permite que desde el área de Ingeniería se pueda verificar que el servidor de base de datos se encuentra en estado activo, mediante la ejecución de comandos ping.

```
/sbin/iptables -A FORWARD -s 172.17.118.120/29 -d 192.168.15.5/32 -p icmp --icmp-type echo-request -j ACCEPT
/sbin/iptables -A FORWARD -s 192.168.15.5/32 -d 172.17.118.120/29 -p icmp --icmp-type echo-reply -j ACCEPT
```

Todos los paquetes que no coincidan con las reglas anteriormente definidas serán descartados.

5.5. Herramientas de monitoreo de seguridad de red.

Existen varias herramientas de monitoreo en el mercado, las cuales permiten monitorear servidores y equipos de comunicación. Las herramientas más comunes son aquellas que permiten capturar mensajes SNMP[40],

[40] Simple Network Management protocol.- protocolo usado para llevar registro de los eventos ocurridos en los servidores y equipos de red. La versión 3 soporta encriptación.

administrarlos y mostrarlos con una interfaz amigable. Herramientas como Zabbix de distribución libre, permiten registrar eventos ocurridos en equipos con soportes snmp por medio de OID (identificación de objeto Snmp); utilizándose para la administración de la interfaz Web.

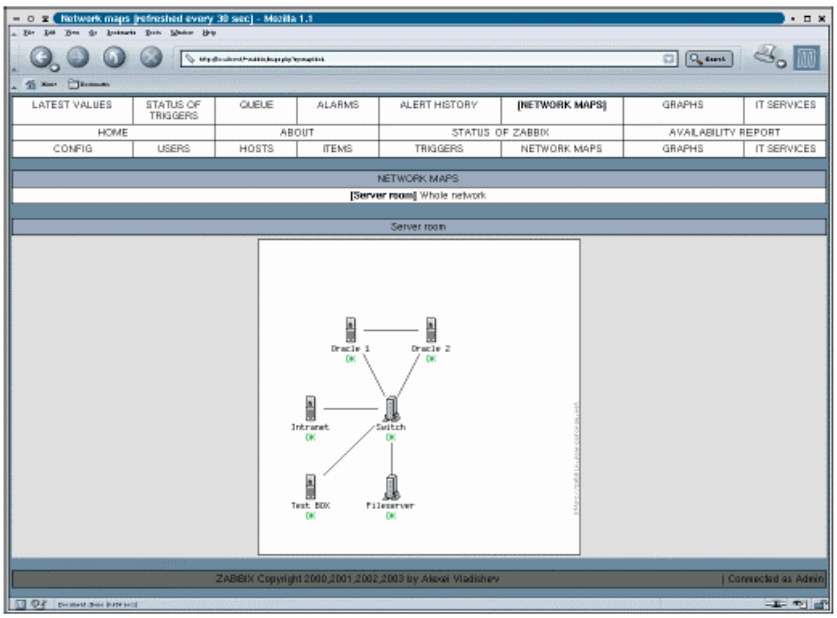

Figura 5.39 Zabbix, herramienta de monitoreo SNMP

Fuente: Alexey Vladishev (Manual Zabbix)

Herramientas de monitoreo SNMP propietarias tales como el 3Com Network Supervisor, permiten registrar eventos ocurridos en los equipos de comunicación 3COM.

Para mantener la red saludable también es necesario verificar si el sistema es vulnerable; para el efecto se utilizan herramientas que emiten un reporte o auditoría del estado del sistema. Para el efecto se tienen herramientas como

"LanWare" y "Shadow", las cuales permiten verificar si a un sistema le falta algún parche de seguridad o es vulnerable en algunos de los servicios que éste ofrece.

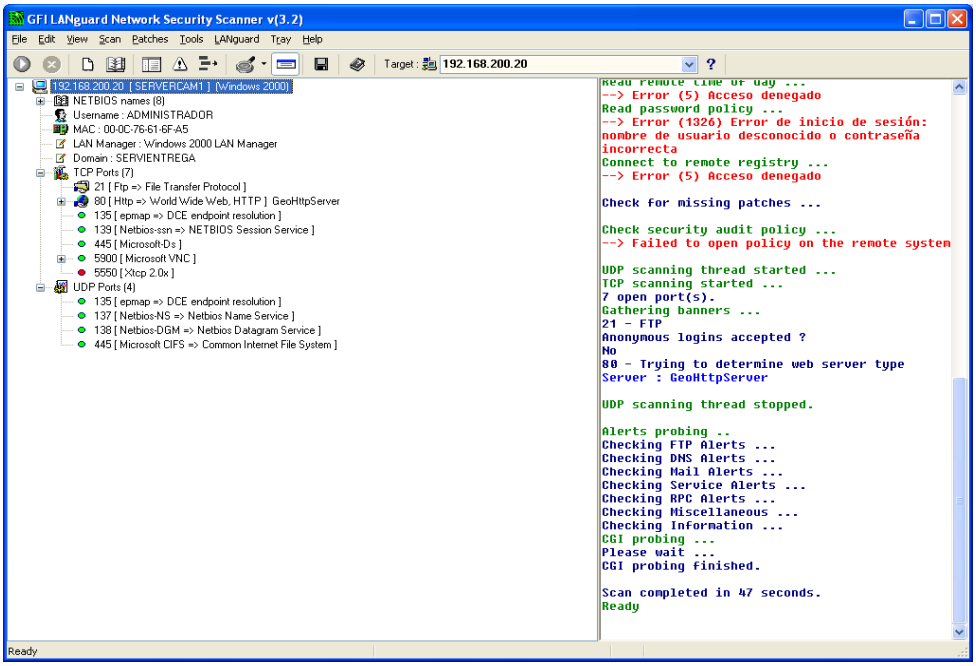

Figura 5.40 Languard, herramienta de análisis
Fuente: Captura de imagen de la aplicación

Los *"sniffers"* o husmeadores son de mucha utilidad si se desea analizar la actividad en la red. Entre estas herramientas se tienen al "Ethereal", "tcpdump" y "nmap" de Linux.

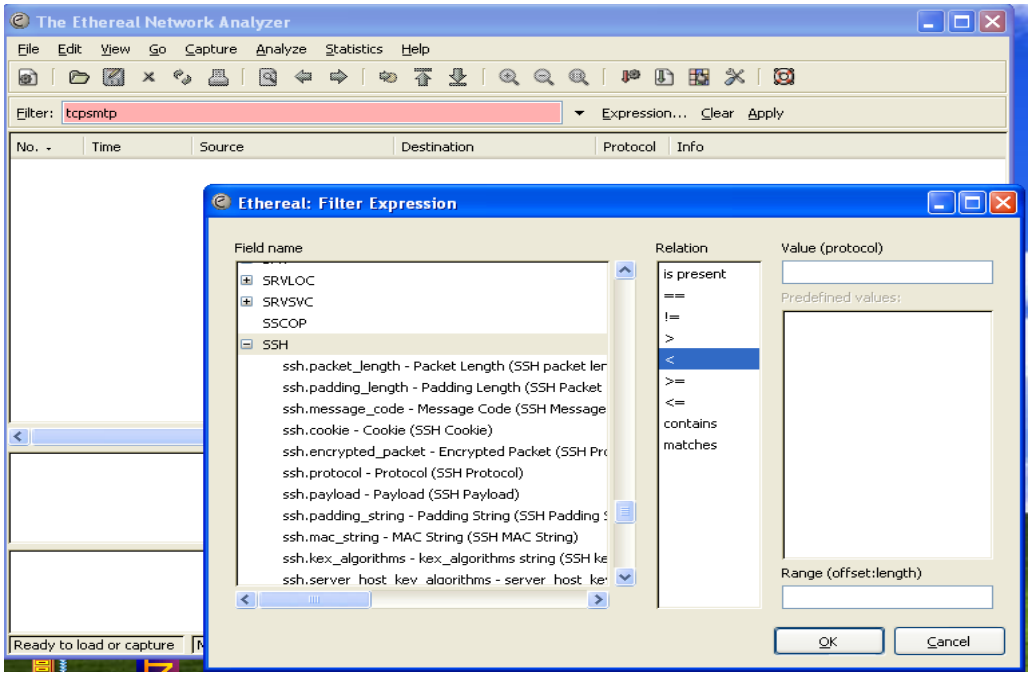

Figura 5.41 Ethereal, herramienta para analizar el tráfico de la red
Fuente: Imagen capturada de aplicación

El gráfico muestra la interface principal de la herramienta Ethereal, la cual es una de las herramientas mayormente utilizadas para analizar el tráfico que fluye en la red. Actualmente existen versiones disponibles tanto para ambientes Linux y Windows.

CAPÍTULO 6

IMPLEMENTACIÓN DEL SITIO WEB

6.1 Análisis y diseño de la Aplicación

6.1.1 Requerimientos Funcionales

A continuación se presentan los requerimientos o especificaciones funcionales del sitio web a implementar:

1. Diseñar un sitio web orientado a la venta de arreglos florales y obsequios complementarios.
2. Permitir ver todos los arreglos disponibles en el sitio organizados por tipo de obsequios y por ocasión.
3. Presentar opciones de búsqueda en base a tres parámetros: destinatario, ocasión y precio.
4. Permitir la creación y mantenimiento de usuarios del sitio web.
5. Permitir la compra de artículos y su edición en base al esquema de carrito de compras.
6. Permitir la consulta del histórico de compras realizadas.
7. Permitir ingresar los datos del destinatario en la compra y personalizar el mensaje adjunto.
8. Emitir el detalle de la factura.
9. Permitir el pago electrónico a través de tarjetas de crédito.
10. Permitir navegación informativa del sitio.

En el proyecto desarrollado se cumplió con los diez requerimientos funcionales mencionados.

6.1.2 Requerimientos No Funcionales

A continuación se detallan los requerimientos no funcionales o también llamadas especificaciones técnicas:

1. Implementar el sitio web bajo un esquema de transmisión segura.
2. Implementar un esquema de red confiable ante ataques externos maliciosos.
3. Autenticar el pago mediante tarjeta de crédito de los clientes.
4. Autenticación del sitio en funciones de ingreso de palabras secretas o "touring number"[41]
5. Requerimientos de hardware/software que permitan una navegación rápida y confiable en el sitio.

Estos requerimientos no funcionales fueron definidos considerando el tipo de negocio que se va a implantar vía el esquema de comercio electrónico, considerando proteger la información ingresada por los clientes.

[41] Número generado en la página que debe ser digitado por el usuario para garantizar que el sitio es genuino y no una falsificación.

6.1.3 Modelo de Análisis

La arquitectura del sistema a implementar será Cliente/Servidor, esto significa que el usuario de Internet interactúa con una página web que a su vez se comunica con un servidor web, procesando las transacciones y peticiones del usuario. El sitio será accesible utilizando un navegador de Internet: Internet Explorer o Netscape.

El servidor web maneja los requerimientos del cliente mediante sesiones que permanecen activas en el servidor mientras el usuario esté navegando en el sitio.

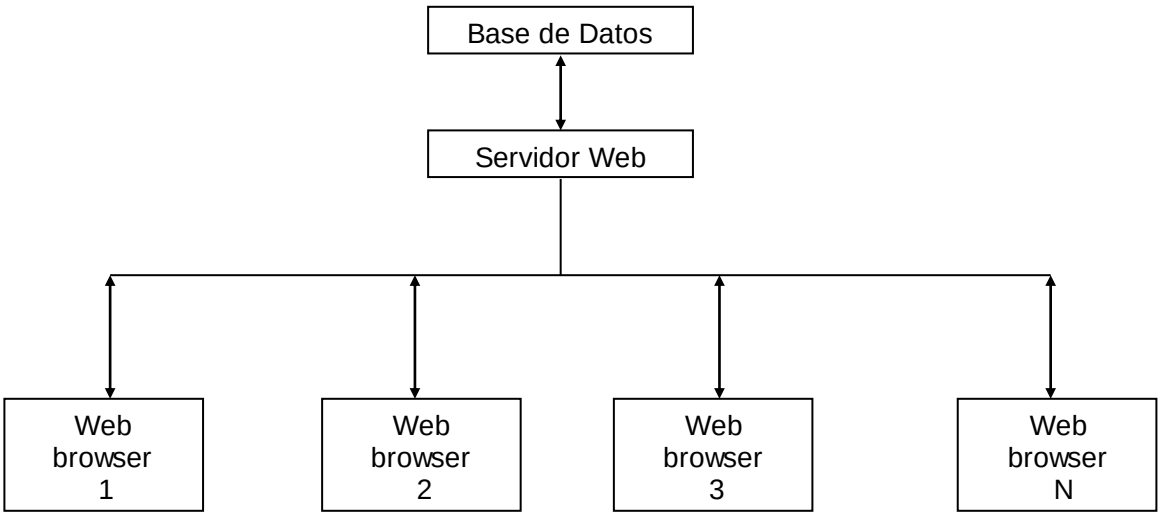

Figura 6.1 Manejo de sesiones en el proyecto.
Fuente: Autores

Como se muestra en la figura 6.1, el servidor web interpreta los requerimientos del usuario y direcciona éstas peticiones a la base de datos, o viceversa; desde la base de datos hacia el cliente.

Actores

Es importante previo al desarrollo de los casos de uso que se pueden dar en el sistema, la identificación de los actores que interactúan en el mismo.

Para los objetivos de este proyecto se ha identificado un actor: “Usuario” persona que accesa al sitio web para consultar o realizar compras.

6.1.4. Casos de Uso

Los casos de usos son las diferentes acciones que se pueden presentar dentro del sistema, a continuación se detallan los mismos:

Actor Iniciador	Caso de Uso
Usuario	▪ Selecciona opción informativa de Quiénes somos. ▪ Selecciona opción informativa de Nuestros productos. ▪ Selecciona opción informativa de Entregas. ▪ Selecciona opción informativa de Formas de Pago. ▪ Selecciona menú de categorías de Flores y Presentes. ▪ Selecciona categoría Flores y Peluches. ▪ Selecciona categoría Flores y Chocolates. ▪ Selecciona categoría Flores y Cds/Libros ▪ Selecciona categoría Flores y Vinos. ▪ Selecciona categoría Flores y Frutas. ▪ Selecciona menú de categorías de Arreglos ▪ Selecciona categoría Romántico. ▪ Selecciona categoría Agradecimiento. ▪ Selecciona categoría Corporativos. ▪ Selecciona categoría Clásicos. ▪ Selecciona categoría Nacimiento. ▪ Selecciona opción de Cliente Frecuente. ▪ Selecciona opción de Contáctenos. ▪ Registrar un cliente en el sitio. ▪ Solicitar recordatorio de contraseña. ▪ Realizar una búsqueda en base a criterios. ▪ Ingreso al sistema. ▪ Consulta de datos personales. ▪ Modificación de datos personales. ▪ Consulta de compras realizadas. ▪ Agregar item al carrito de compras. ▪ Eliminar item del carrito de compras. ▪ Selecciona opción de Ver Carrito ▪ Escoger opción de realizar pedido. ▪ Ingreso de forma de pago. ▪ Generación de resumen de factura y detalle de orden.

Fig 6.2 Listado de Casos de Uso del Sistema Fuente: Autores

A continuación se detalla cada uno de los treinta y un casos de uso identificados en el sistema.

6.1.5 Escenarios

Los escenarios se clasifican por casos de uso y se refiere a los diferentes resultados que el sistema da como respuesta a una acción tomada, de esta manera un escenario puede ser exitoso o puede ser de error o falla.

A continuación se detalla los escenarios por cada caso de uso:

6.1.5.1 Selecciona opción informativa de “Quiénes somos”.

Escenario exitoso:

Se presenta en la parte central del sitio la página informativa de “quiénes somos”

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com

Poscondiciones - Comportamiento esperado:

- Se visualiza en la página central la información de “quiénes somos”.

Otros escenarios: escoger la opción “quiénes somos” falla porque no se puede establecer conexión.

6.1.5.2 Selecciona opción informativa de ““nuestros productos””.

Escenario exitoso:

Se presenta en la parte central del sitio la página informativa de “nuestros productos”

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com

Poscondiciones - Comportamiento esperado:

- Se visualiza en la página central la información de “nuestros productos”.

Otros escenarios: escoger la opción “nuestros productos” falla porque no se puede establecer conexión.

6.1.5.3 Selecciona opción informativa de “entregas”

Escenario exitoso:

Se presenta en la parte central del sitio la página informativa de “entregas”

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com

Poscondiciones - Comportamiento esperado:

- Se visualiza en la página central la información de “entregas”.

Otros escenarios: escoger la opción “entregas” falla porque no se puede establecer conexión.

6.1.5.4 Selecciona opción informativa de “formas de pago”

Escenario exitoso:

Se presenta en la parte central del sitio la página informativa de “formas de pago”.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com

Poscondiciones - Comportamiento esperado:

- Se visualiza en la página central la información de “formas de pago”.

Otros escenarios: escoger la opción informativa de “formas de pago” falla porque no se puede establecer conexión.

6.1.5.5 Selecciona opción de “flores y presentes”

Escenario exitoso:

Se presenta en la parte lateral las opciones a escoger dentro de “flores y presentes”.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com

Poscondiciones - Comportamiento esperado:

- Se visualiza en la página lateral izquierda las opciones de “flores y presentes”.

Otros escenarios: al dar nuevamente “click” cierra el menú de opciones de “flores y presentes”.

6.1.5.6 Selecciona opción de “flores y peluches”

Escenario exitoso:

Se presenta en la parte central del sitio los items disponibles que entran en esta categoría.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com
- El usuario ha dado “click”en el menú “flores y peluches” para visualizar esta opción.

Poscondiciones - Comportamiento esperado:

- Se visualiza en la página central los obsequios disponibles para esta categoría, con el precio y la opción para empezar la compra.

Otros escenarios: escoger la opción de “flores y peluches” falla porque no se puede establecer conexión.

6.1.5.7 Selecciona opción de “flores y chocolates”.

Escenario exitoso:

Se presenta en la parte central del sitio los items disponibles que entran en esta categoría.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com
- El usuario ha dado “click”en el menú “Flores y chocolates” para visualizar esta opción.

Poscondiciones - Comportamiento esperado:

- Se visualiza en la página central los obsequios disponibles para esta categoría, con el precio y la opción para empezar la compra.

Otros escenarios: escoger la opción de “flores y chocolates” falla porque no se puede establecer conexión.

6.1.5.8 Selecciona opción de “flores y cds/libros”.

Escenario exitoso:

Se presenta en la parte central del sitio los items disponibles que entran en esta categoría.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com

- El usuario ha dado “click”en el menú “flores y cds/libros” para visualizar esta opción.

Poscondiciones - Comportamiento esperado:

- Se visualiza en la página central los obsequios disponibles para esta categoría, con el precio y la opción para empezar la compra.

Otros escenarios: escoger la opción de “Flores y Cds/Libros” falla porque no se puede establecer conexión.

6.1.5.9 Selecciona opción de “flores y vinos”

Escenario exitoso:

Se presenta en la parte central del sitio los items disponibles que entran en esta categoría.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com
- El usuario ha dado “click”en el menú “flores y vinos” para visualizar esta opción.

Poscondiciones - Comportamiento esperado:

- Se visualiza en la página central los obsequios disponibles para esta categoría, con el precio y la opcion para empezar la compra.

Otros escenarios: escoger la opción de “flores y vinos” falla porque no se puede establecer conexión.

6.1.5.10 Selecciona opción de “flores y frutas”

Escenario exitoso:

Se presenta en la parte central del sitio los items disponibles que entran en esta categoría.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com
- El usuario ha dado “click”en el menú “flores y frutas” para visualizar esta opción.

Poscondiciones - Comportamiento esperado:

- Se visualiza en la página central los obsequios disponibles para esta categoría, con el precio y la opción para empezar la compra.

Otros escenarios: escoger la opción de “flores y frutas” falla porque no se puede establecer conexión.

6.1.5.11 Selecciona opción de “categorías de arreglos”

Escenario exitoso:

Se presenta en la parte lateral las opciones a escoger dentro de “categorías de arreglos”

Precondiciones:

- El usuario tiene conexión a Internet.

- El usuario accesa al sitio www.contodomiamor.com

Poscondiciones - Comportamiento esperado:

- Se visualiza en la página lateral izquierda las opciones de “categorías de arreglos”.

Otros escenarios: al dar nuevamente “click” cierra el menú de opciones de “categorías de arreglos”.

6.1.5.12 Selecciona “Categoría Románticos”

Escenario exitoso:

Se presenta en la parte central del sitio los items disponibles que entran en esta categoría.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com
- El usuario ha dado “click”en el menú de “Categorías” para visualizar esta opción.

Poscondiciones - Comportamiento esperado:

- Se visualiza en la página central los obsequios disponibles para esta categoría, con el precio y la opción para empezar la compra.

Otros escenarios: escoger la opción de “Categoría Románticos” falla porque no se puede establecer conexión.

6.1.5.13 Selecciona “Categoría Agradecimientos”.

Escenario exitoso:

Se presenta en la parte central del sitio los items disponibles que entran en esta categoría.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com
- El usuario ha dado “click”en el menú de “Categorías” para visualizar esta opción.

Poscondiciones - Comportamiento esperado:

- Se visualiza en la página central los obsequios disponibles para esta categoría, con el precio y la opción para empezar la compra.

Otros escenarios: escoger la opción de “Categoría Agradecimientos” falla porque no se puede establecer conexión.

6.1.5.14 Selecciona “Categoría Corporativos”.

Escenario exitoso:

Se presenta en la parte central del sitio los items disponibles que entran en esta categoría.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com

- El usuario ha dado “click”en el menú de “Categorías” para visualizar esta opción.

Poscondiciones - Comportamiento esperado:

- Se visualiza en la página central los obsequios disponibles para esta categoría, con el precio y la opción para empezar la compra.

Otros escenarios: escoger la opción de “Categoría Corporativos” falla porque no se puede establecer conexión.

6.1.5.15 Selecciona “Categoría Clásicos”.

Escenario exitoso:

Se presenta en la parte central del sitio los items disponibles que entran en esta categoría.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com
- El usuario ha dado “click”en el menú de “Categorías” para visualizar esta opción.

Poscondiciones - Comportamiento esperado:

- Se visualiza en la página central los obsequios disponibles para esta categoría, con el precio y la opción para empezar la compra.

Otros escenarios: escoger la opción de “Categoría Clásicos” falla porque no se puede establecer conexión.

6.1.5.16 Selecciona “Categoría Nacimientos”.

Escenario exitoso:

Se presenta en la parte central del sitio los items disponibles que entran en esta categoría.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com
- El usuario ha dado “click”en el menú de “Categorías” para visualizar esta opción.

Poscondiciones - Comportamiento esperado:

- Se visualiza en la página central los obsequios disponibles para esta categoría, con el precio y la opción para empezar la compra.

Otros escenarios: escoger la opción de “Categoría Nacimientos” falla porque no se puede establecer conexión.

6.1.5.17 Selecciona opción informativa de “Cliente Frecuente”.

Escenario exitoso:

Se presenta en la parte central del sitio la página informativa de lo que implica ser un cliente frecuente

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com

Poscondiciones - Comportamiento esperado:

- Se visualiza en la página central la información de “cliente frecuente”.

Otros escenarios: escoger la opción informativa “cliente frecuente” falla porque no se puede establecer conexión.

6.1.5.18 Selecciona opción “Contáctenos”.

Escenario exitoso:

Se presenta en la parte central del sitio la aplicación de mail para dirigir un correo al administrador del sitio web.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com

Poscondiciones - Comportamiento esperado:

- Se visualiza en la página la aplicación de correo.

Otros escenarios: escoger la opción (“Contáctenos”) falla porque no se puede establecer conexión, o escoger la opción (“Contáctenos”) falla por problemas de servidor de correo.

6.1.5.19 Registrar un cliente en el Sitio.

Escenario exitoso:

Se presenta en la parte central del sitio el formulario de datos personales y se realiza el ingreso del nuevo usuario.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com
- El usuario da “click” en la opción “Registrarse”.

Poscondiciones - Comportamiento esperado:

Se ingresan los datos personales al sitio a través del formulario de cliente.

Otros escenarios: validación de datos en cada campo del formulario de datos, uso de “touring number” en formulario de datos, o el ingreso falla porque no se puede establecer conexión.

6.1.5.20 Solicitar recordatorio de Contraseña.

Escenario exitoso:

Se presenta en la parte central del sitio el formulario para ingreso de frase secreta.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com
- El usuario da “click” en la opción “Recordar contraseña”.

Poscondiciones - Comportamiento esperado:

Se ingresan los datos de pregunta/respuesta secreta y luego se recibe correo con frase recordatoria del sitio, el usuario cambia de estado a activado si por intentos fallidos se encontrase bloqueado.

Otros escenarios: uso de “touring number” en formulario de datos, el ingreso falla porque no se puede establecer conexión.

6.1.5.21 Realizar una búsqueda en base a criterios.

Escenario exitoso:

El usuario escoge los tres criterios de búsqueda y se presenta en la página central los items que cumplen la condición.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com
- El usuario escoge “Para Quién”.
- El usuario escoge “Ocasión”.
- El usuario escoge “Precio”.

Poscondiciones - Comportamiento esperado:

Se ingresan los tres criterios de búsqueda y luego se muestran los items que cumplen los criterios.

Otros escenarios: manejo de opciones para cada criterio, la búsqueda falla porque no se puede establecer conexión, o si la búsqueda no trae datos se presenta página pre-establecida para incentivar la venta.

6.1.5.22 Ingreso al Sistema.

Escenario exitoso:

El usuario ingresa su usuario/contraseña, y el sistema le da la bienvenida en la página central.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com
- El usuario debe estar registrado en el sitio.

Poscondiciones - Comportamiento esperado:

Se ingresan el usuario y contraseña, para estar conectado al sistema.

Otros escenarios:

- Ingreso de "touring number".
- El ingreso falla porque no se pudo establecer conexión.
- El ingreso falla por usuario o contraseña incorrecta y aumenta el número de intentos fallidos.
- El ingreso falla por "touring number" incorrecto.
- Opción de "ingreso" en página central al validar autenticación en el sitio.
- La cuenta del usuario se bloquea al llegar a tres intentos fallidos, el sistema solicitará recordatorio de contraseña para proceder a activar el usuario.

A partir de este escenario el usuario está en capacidad de realizar su compra.

6.1.5.23 Consulta de datos personales.

Escenario exitoso:

El usuario visualiza en la página central sus datos personales.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com
- El usuario debe estar autenticado en el sitio (ingreso).

Poscondiciones - Comportamiento esperado:

Se visualizan datos personales.

Otros escenarios: la consulta falla porque no se pudo establecer conexión.

6.1.5.24 Modificación de datos personales.

Escenario exitoso:

El usuario visualiza en la página central sus datos personales, de manera que puede cambiar los mismos.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com
- El usuario debe estar autenticado en el sitio (ingreso).

Poscondiciones - Comportamiento esperado:

Se visualizan datos personales, y se modifican los mismos.

Otros escenarios: validación de campos modificados, la modificación falla porque no se pudo establecer conexión, o uso de "touring number".

6.1.5.25 Consulta de compras realizadas.

Escenario exitoso:

El usuario visualiza en la página central su historial de compras realizadas.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com
- El usuario debe estar autenticado en el sitio(ingreso)

Poscondiciones - Comportamiento esperado:

Se visualizan historiales de compras, con un hipervínculo para ver el detalle de factura y de orden de la compra escogida.

Otros escenarios: la consulta falla porque no se pudo establecer conexión.

6.1.5.26 Agregar item al “carrito de compras”.

Escenario exitoso:

El usuario da comprar en un item y automáticamente ingresa al “carrito de compras”, acción que se visualiza en la página central.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com
- El usuario debe estar autenticado en el sitio (ingreso).
- El usuario debe digitar la opción ”comprar” en un item.

Poscondiciones - Comportamiento esperado:

Se visualiza el “carrito de compras” con el nuevo item agregado.

Otros escenarios: agregar item al carrito falla porque no se pudo establecer conexión.

6.1.5.27 Eliminar item del “carrito de compras”.

Escenario exitoso:

El usuario da eliminar un item del “carrito de compras”.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com
- El usuario debe estar autenticado en el sitio(ingreso).
- El usuario debe escoger el item a eliminar del “carrito de compras”

Poscondiciones - Comportamiento esperado:

Se visualiza el “carrito de compras” sin el item que se envió a borrar.

Otros escenarios: eliminar item del “carrito de compras” falla porque no se pudo establecer conexión.

6.1.5.28 Selecciona opción de “Ver Carrito”.

Escenario exitoso:

El usuario verifica los items agregados al “carrito de compras”.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com
- El usuario debe estar autenticado en el sitio(ingreso).
- El usuario debe haber agregado items al “carrito de compras”.

Poscondiciones - Comportamiento esperado:

Se visualiza el “carrito de compras” con los items agregados.

Otros escenarios: (“Ver Carrito”) falla porque no se pudo establecer conexión.

6.1.5.29 Realizar pedido.

Escenario exitoso:

El usuario ingresa los datos del destinatario y el mensaje que acompaña al presente.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com
- El usuario debe estar autenticado en el sitio(ingreso).
- El usuario debe haber agregado items al “carrito de compras”.
- El usuario debe haber solicitado el Pedido.

Poscondiciones - Comportamiento esperado:

Se visualiza los datos del destinatario que recibirá el(los) presentes.

Otros escenarios: validación de ingresos de datos en el formulario, el ingreso de los datos del destinatario falla porque no se pudo establecer conexión.

6.1.5.30 Ingreso de forma de pago.

Escenario exitoso:

El usuario ingresa los datos de su tarjeta de crédito.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com

- El usuario debe estar autenticado en el sitio(ingreso).
- El usuario debe haber agregado items al “carrito de compras”.
- El usuario debe haber solicitado el Pedido.
- El usuario debe haber completado el formulario de destinatario.

Poscondiciones - Comportamiento esperado:

Se visualiza y se verifica los datos de la tarjeta de crédito y se efectúa la transacción de pago.

Otros escenarios: cargar automáticamente datos preexistentes de la tarjeta, autenticación de la tarjeta, validación de campos de ingreso o, la transacción de pago falla porque no se pudo establecer conexión.

6.1.5.31 Generación de resumen de factura y detalle de orden.

Escenario exitoso:

El usuario visualiza su resumen de factura y detalle de la orden realizada.

Precondiciones:

- El usuario tiene conexión a Internet.
- El usuario accesa al sitio www.contodomiamor.com
- El usuario debe estar autenticado en el sitio(ingreso).
- El usuario debe haber agregado items al “carrito de compras”.
- El usuario debe haber solicitado el Pedido.
- El usuario debe haber completado el formulario de destinatario.
- El usuario debe haber efectuado el pago electrónico.

Poscondiciones - Comportamiento esperado:

Se visualizan los datos de la factura y detalle de orden

Otros escenarios: la visualización de resumen de factura y detalle de orden fallan porque no se pudo establecer conexión.

Resumen de transaccionalidad en el Sitio.

El siguiente flujo de transacciones resume la funcionalidad general del sitio:

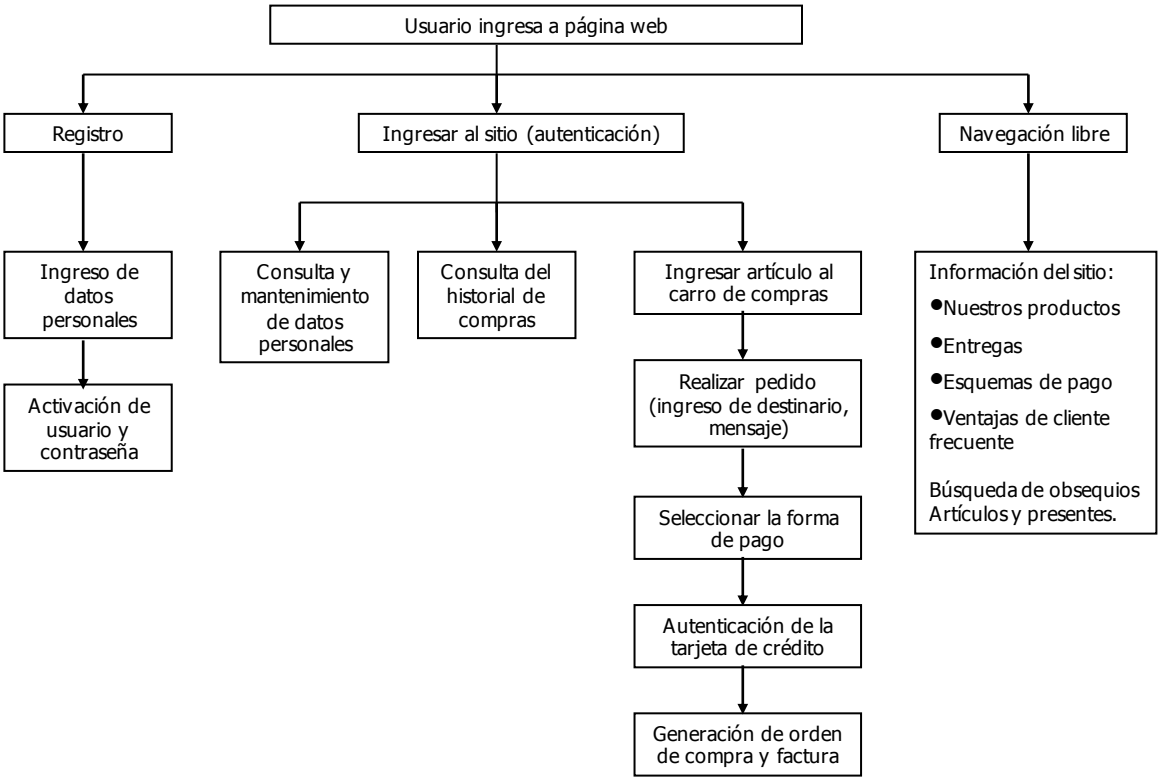

Figura 6.2 Transaccionalidad del sitio.
Fuente: Autores

El gráfico muestra todos los eventos que pueden presentarse en el sistema, así como la secuencia de los mismos.

6.1.6 Diagrama Entidad-Relación

El diagrama de base de datos está integrado por quince entidades, las mismas que se describen a continuación:

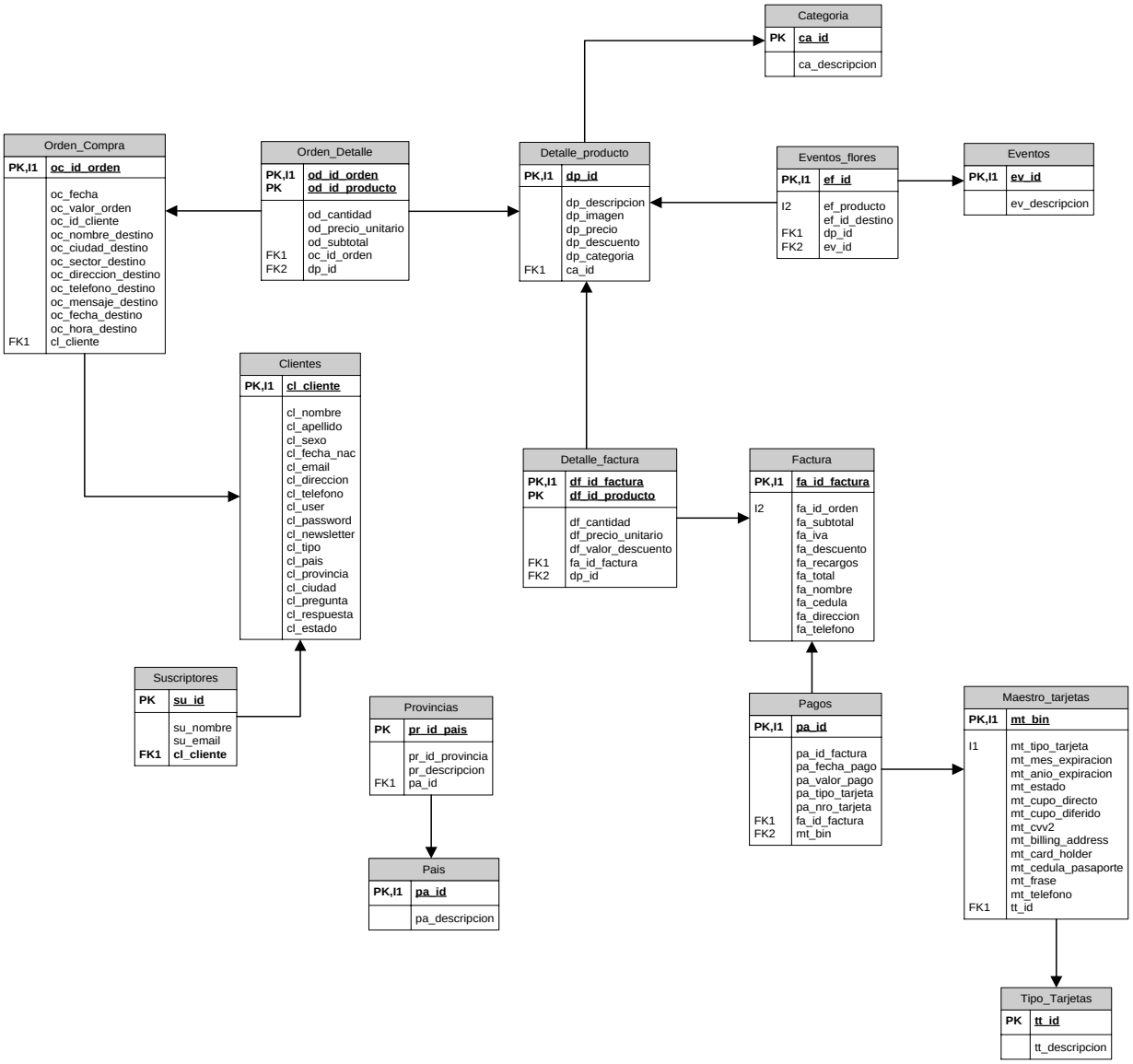

Figura 6.3 Diagrama entidad-relación del proyecto.
Fuente: Autores

Detalle_producto: tabla de los ítems disponibles a la venta en el sitio. Se registran datos como: nombre y descripción del artículo, ubicación de la imagen en el servidor web, precio del item.

Categoría: tabla de categorías en base a las cuales se van a clasificar los artículos. En el sitio web se cargaron las siguientes categorías: flores y peluches, flores y chocolates, flores y cd's, flores y vinos, flores y frutas, romántico, agradecimiento, corporativo, clásicos y nacimiento.

Eventos: tabla de las diferentes ocasiones en base a las cuales puede clasificarse un artículo para ser obsequiado. En el sitio web se cargaron los siguientes eventos: agradecimiento, aniversario, romántico, cumpleaños, nacimiento, graduación.

Eventos_flores: dado que un artículo puede estar clasificado para ser obsequiado a más de un evento, se creó esta entidad para manejar la relación de muchos a muchos existente entre las entidades: ("detalle_producto") y ("eventos").

Clientes: entidad utilizada para administrar los usuarios registrados en www.contodomiamor.com. Se almacenan datos generales como: nombre y

apellido, fecha de nacimiento, email, dirección, teléfono, usuario y contraseña encriptada.

Suscriptores: entidad relacionada a (“Clientes”), se actualiza si el usuario al momento de registrarse en el sitio notifica que desea recibir comunicaciones periódicas o newsletters.

Orden_compra: entidad utilizada para almacenar datos generales de la compra a ser realizada por el usuario. Presta facilidades para personalizar el obsequio a ser entregado, registrando datos como: nombre del destinatario, mensaje adjunto, teléfono, fecha y hora de entrega.

Orden_detalle: entidad que registra el detalle de los ítems seleccionados por el usuario. Se registran datos como: código de artículo, cantidad, precio y subtotal. Es el desglose por artículo de la orden de compra del usuario.

Factura: dado que un usuario puede cancelar su pedido y no completar la transacción de compra cerrando simplemente la ventana del browser, en el análisis funcional inicial se decidió segregar las potenciales ventas respecto a las ventas completadas.

Adicionalmente, considerando el esquema de pagos disponible en el sitio mediante tarjetas de crédito, puede darse el caso que un usuario cancele con una tarjeta de crédito en la cual el titular es otra persona.
Esta entidad registra el resumen de la venta realizada al usuario, registrando datos como: total en ventas brutas, impuestos, datos generales de la persona que paga la compra.

Detalle_factura: entidad en la cual se registran uno a uno los ítems a ser facturados al usuario.

Maestro_tarjetas y Tipo_Tarjetas: entidades utilizadas para simular un agente externo, la compañía emisora de la tarjeta de crédito. Se registran datos referentes a la tarjeta como: número de bin, nombre del titular, dirección, fecha de expiración, cupo disponible, frase secreta.

País y provincias: tabla de países y sus principales provincias.

Las quince entidades fueron definidas considerando el tipo de negocio desarrollado, venta de arreglos florales y obsequios; adoptando un enfoque en la transaccionalidad de la venta y pagos, mas no control de inventarios.

6.2 Desarrollo y presentación de las páginas

6.2.1 Flujo de ventanas y layouts

A continuación se presenta las pantallas que conforman el sitio:

Página principal

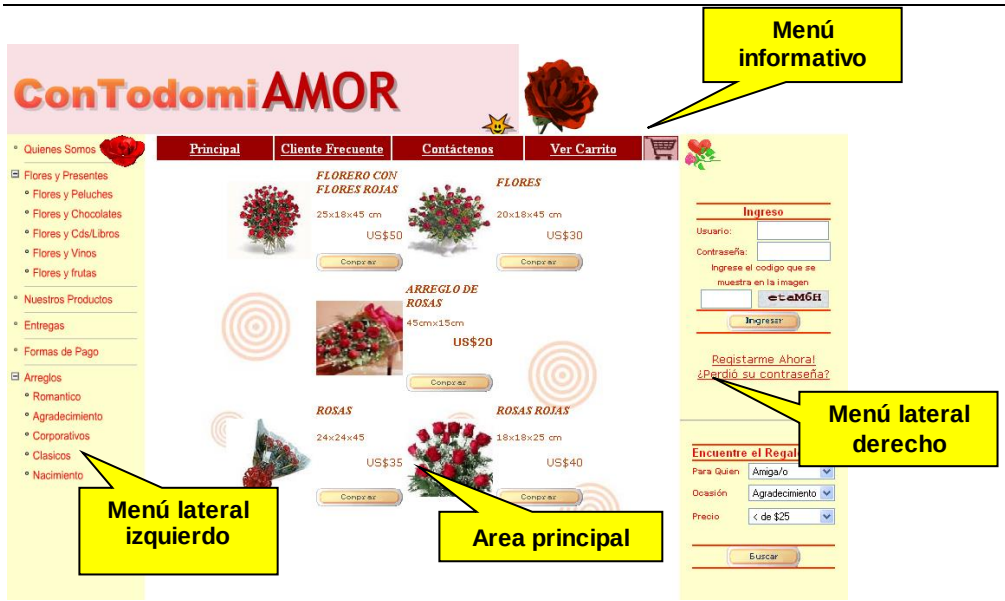

Figura 6.4 Página principal del sitio web.
Fuente: Autores

Menú lateral izquierdo

Figura 6.5 Funcionalidad del menú lateral izquierdo.
Fuente: Autores

Menú informativo

Figura 6.6 Funcionalidad del menú informativo
Fuente: Autores

Menú lateral derecho

Está divido en tres funcionalidades:

1) Menú de Ingreso de Clientes
2) Registro
3) Criterios de búsqueda

1) Ingreso de Clientes

Figura 6.7 Funcionalidad del menú lateral derecho.
Fuente: Autores

2) Registro de Usuario

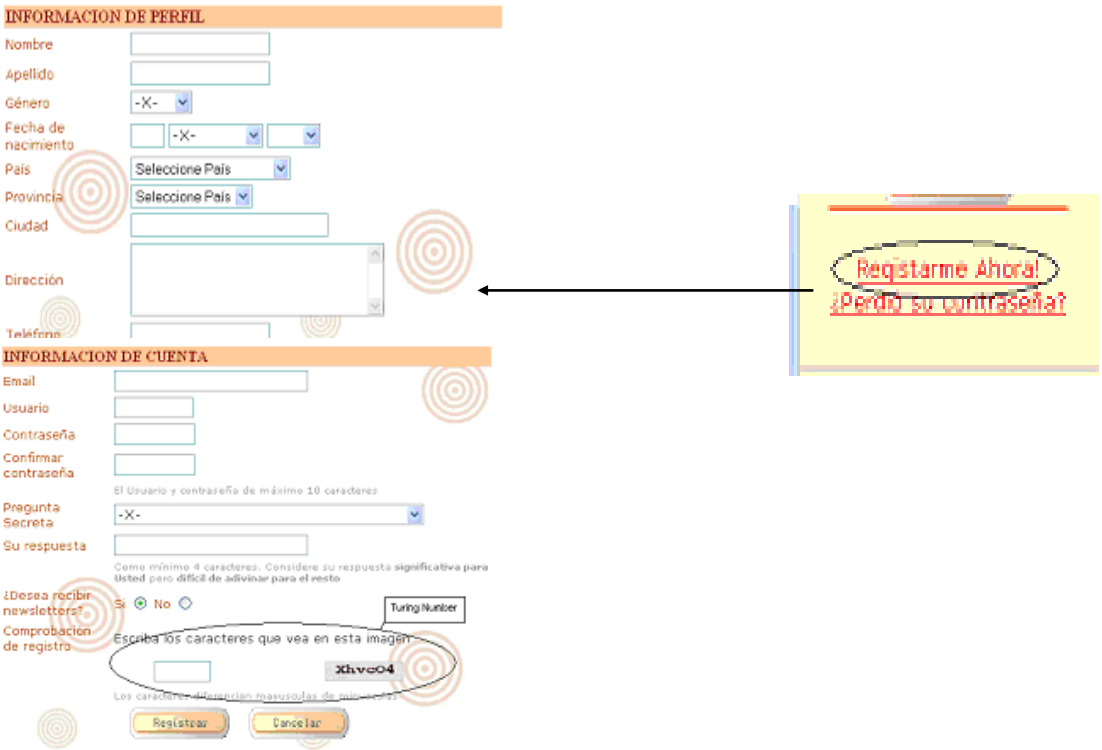

Figura 6.8 Registro de un nuevo usuario
Fuente: Autores

3) Criterios de Búsqueda

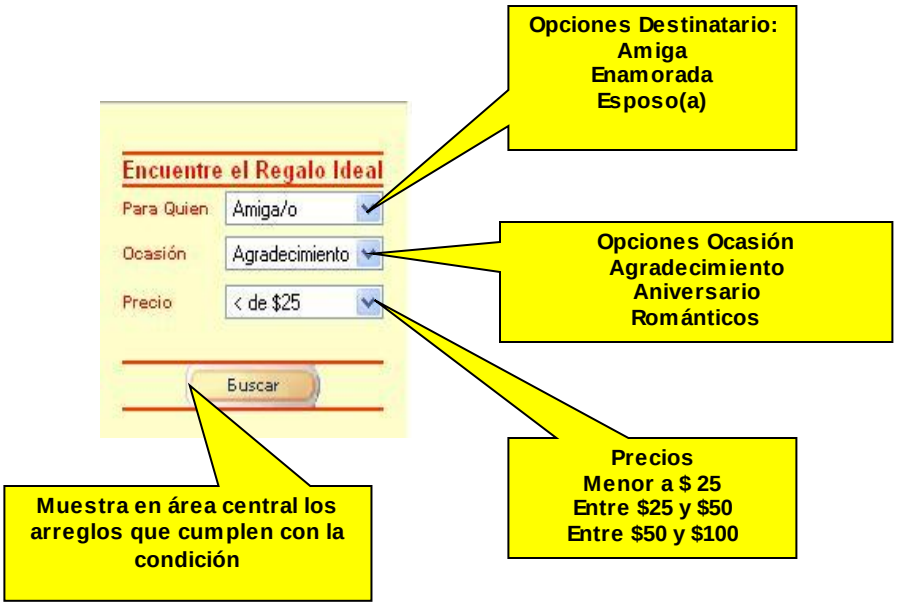

Figura 6.9 Criterios de búsqueda de obsequios.
Fuente: Autores

Mantenimiento de Datos

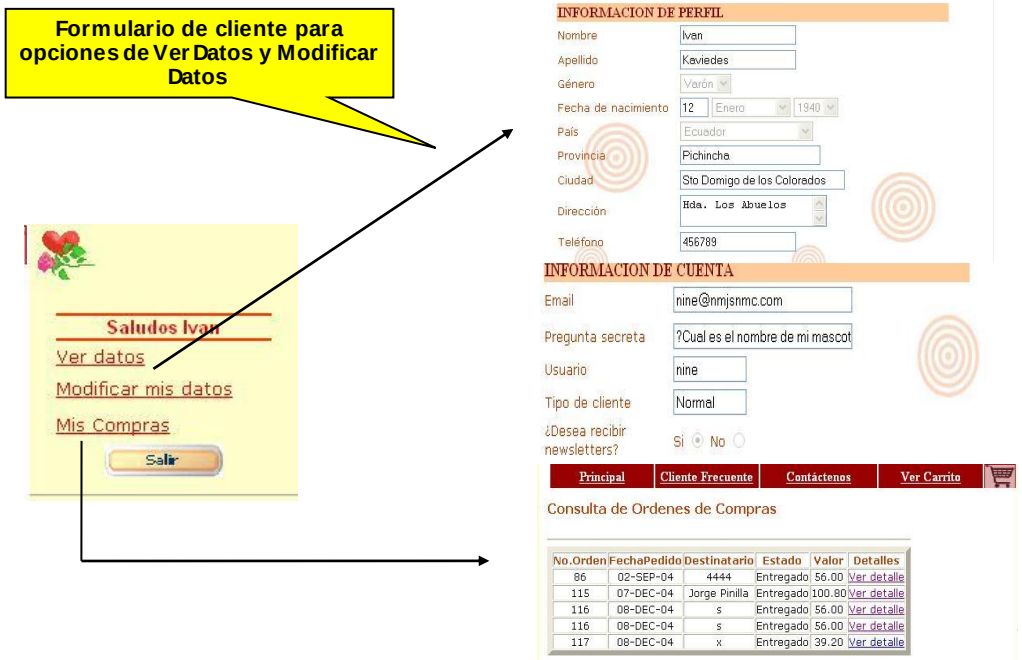

Figura 6.10 Mantenimiento de datos del usuario

Fuente: Autores

Consulta de órdenes de Compras

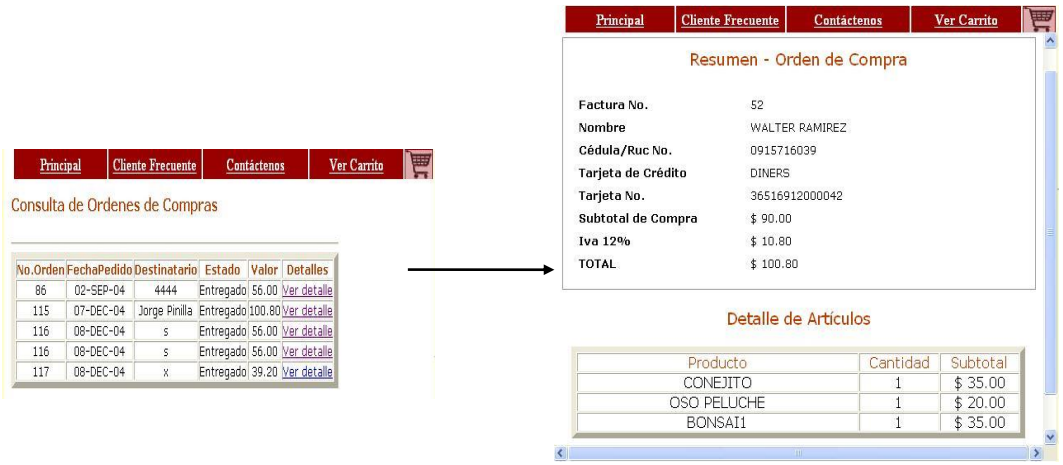

Figura 6.11 Consulta de órdenes de compra realizadas
Fuente: Autores

Proceso de Compra

1) Carrito de Compras

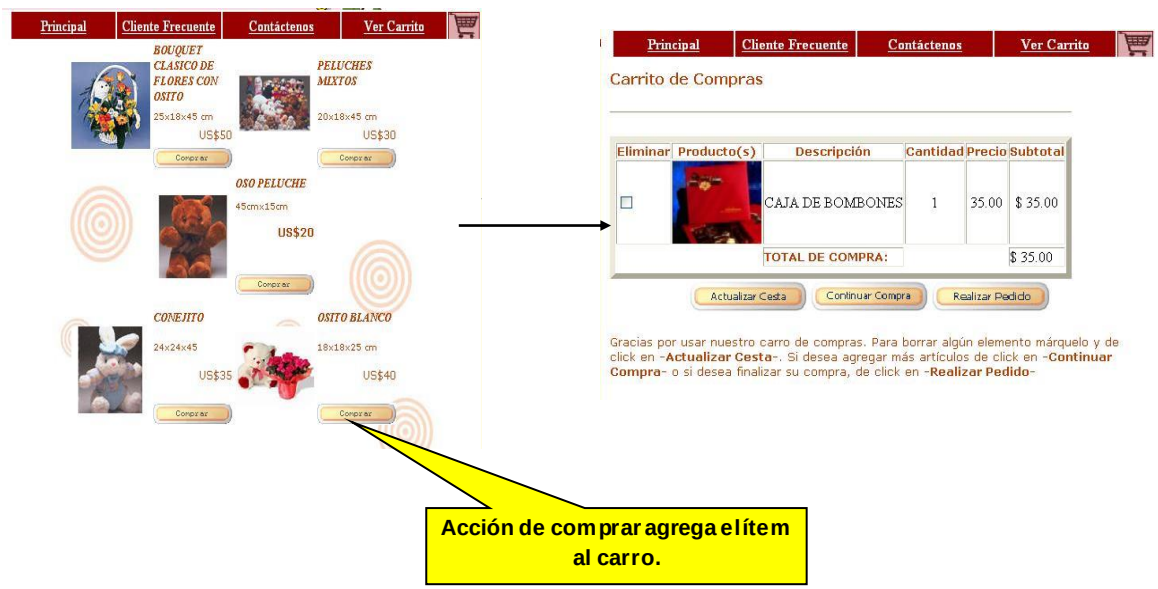

Figura 6.12 Carrito de compras

Fuente: Autores

2) Formulario de Destinatario

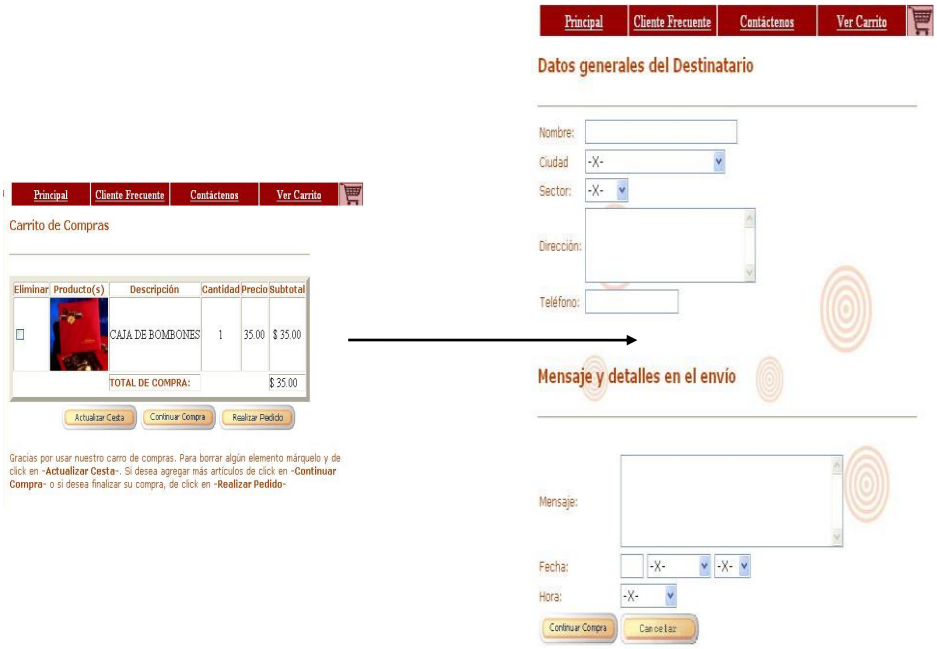

Figura 6.13 Formulario de ingreso de datos para el destinatario.
Fuente: Autores

3) Transacción de Pago

Figura 6.14 Transacción de pago
Fuente: Autores

6.2.2 Implementación de las páginas

6.2.2.1 Estructura Principal:

La página principal del sitio es (“index.htm”), contiene a través de los denominados “frames”, la siguiente estructura:

Frame	Programa	Tipo de Programa	Descripción
Superior	top.htm	Html	Página que referencia al flash principal.
Superior	Sup.htm	Html	Página que referencia la parte superior del sitio.
Superior	movie14.html	Html	Página que referencia al flash principal.
Superior	movie14.fla	Flash	Flash principal que muestra el nombre del sitio contodomiamor.com
Superior	presentacion.fla	Flash	Flash central que muestra imagen animada de flores con nuestro lema Díselo con Flores.
Central	Menú_superior.htm	Html	Muestra las opciones del menú horizontal superior.
Central	Body.htm	Html	En él se referencia el flash de presentación central.
Izquierdo	left.htm	Html	Referencia al menú vertical hecho en xml.
Izquierdo	menuvertical.xml	Xml	Muestra las opciones que van en este sector del sitio.
Derecho	rigth.php	Php	Muestra las opciones que van en este sector del sitio.

Fig 6.15 Estructura principal de la página
Fuente: Autores

La página web (“index.htm”) es el punto de inicio a toda la funcionalidad desarrollada en el sitio.

6.2.2.2 Opciones Menú superior

A partir del (“menu_superior.htm”) se derivan las siguientes funcionalidades:

Opción	Frame	Programa	Tipo de Programa	Descripción
Principal	Central	Body.htm	Html	Muestra en la parte central el flash de presentación del sitio.
Cliente Frecuente	Central	Cliente_frecuente.htm	Html	Muestra en la parte central la información de cliente frecuente.
Contáctenos	Central	Body.htm	Html	Abre la aplicación de correo.
Ver Carrito	Central	carro_compras.php	Php	Muestra la historia de compras realizadas.

Fig 6.16 Estructura de las páginas-Menu Superior
Fuente: Autores

Las opciones del Menú superior se las puede visualizar en la Figura 6.7 de la página 287, básicamente hace referencia a páginas de tipo informativo.

6.2.2.3 Menú lateral izquierdo

A partir de (“left.htm”) y (“menuvertical.xml”) se derivan las siguientes funcionalidades:

Opción	Frame	Programa	Tipo de Programa	Descripción
Quienes Somos	Izquierdo	quienes_somos.htm	Html	Muestra en la parte central el flash de presentación del sitio.
Flores y Peluches	Izquierdo	pagina_dimamica.php Parámetro: Producto = 1	Php	Muestra en la parte central los arreglos de esta categoría.
Flores y Chocolates	Izquierdo	pagina_dimamica.php Parámetro: Producto = 2	Php	Muestra en la parte central los arreglos de esta categoría.
Flores y Cd/Libros	Izquierdo	pagina_dimamica.php Parámetro: Producto = 3	Php	Muestra en la parte central los arreglos de esta categoría.
Flores y Vinos	Izquierdo	pagina_dimamica.php Parámetro: Producto = 4	Php	Muestra en la parte central los arreglos de esta categoría.
Flores y Frutas	Izquierdo	pagina_dimamica.php Parámetro: Producto = 5	Php	Muestra en la parte central los arreglos de esta categoría.

Nuestros Productos	Izquierdo	nuestros_productos.htm	Html	Muestra en la parte central la información de nuestros productos.
Entregas	Izquierdo	entregas.htm	Html	Muestra en la parte central la cobertura de entregas.
Entregas	Izquierdo	Oficinas.htm	Html	Muestra donde están ubicadas las oficinas del sitio.
Formas de Pago	Izquierdo	formaspagos.htm	Html	Muestra en la parte central la información de las formas de pagos.
Formas de Pago	Izquierdo	Comocomprarlinea.htm	Html	Es un enlace de formas de pago que da una ayuda en línea para comprar.
Arreglo romántico	Izquierdo	pagina_dimamica.php Parámetro: Producto = 6	Php	Muestra en la parte central los arreglos de esta categoría.
Arreglo agradecimiento	Izquierdo	pagina_dimamica.php Parámetro: Producto = 7	Php	Muestra en la parte central los arreglos de esta categoría.
Arreglo	Izquierdo	pagina_dimamica.php	Php	Muestra en

corporativo		Parámetro: Producto = 8		la parte central los arreglos de esta categoría.
Arreglo clásico	Izquierdo	pagina_dimamica.php Parámetro: Producto = 9	Php	Muestra en la parte central los arreglos de esta categoría.
Arreglo nacimiento	Izquierdo	pagina_dimamica.php Parámetro: Producto = 10	Php	Muestra en la parte central.

Fig 6.17 Estructura de las páginas – Menú lateral izquierdo
Fuente: Autores

Las opciones del Menú lateral izquierdo se las puede visualizar en la Figura 6.6 de la página 286, básicamente se presentan opciones categorizadas por tipos de arreglos o combinaciones de arreglos florales con obsequios complementarios.

6.2.2.4 Menú lateral derecho inicial

A partir de (“rigth.php”) se derivan las siguientes funcionalidades:

Opción	Frame	Programa	Tipo de Programa	Descripción
Ingreso	Derecho	Login.php	Php	Realiza la transacción de autenticación al sitio y muestra menú final derecho.
Ingreso	Central	Logincentral.php	Php	Realiza la transacción de autenticación en el área central del sitio.
Ingreso	Derecho	Imageeditor.php	Php	Generación de imagen alfanumérica aleatoria
Ingreso	Central	Ingresar.php	Php	Muestra información para ingreso cuando se desea agregar una compra pero no está autenticado
Bienvenida de Ingreso	Central	Bienvenida.php	Php	La transacción de ingreso muestra en la parte central la bienvenida al sitio
Menú final derecho	Derecho	Rigth2.php	Php	Muestra opciones para usuarios autenticados
Registrarme ahora	Derecho	ing_cl.php	Php	Muestra formulario de ingreso de datos en área

				central y los valida.
Transacción de Registro	Central	Ingresa_cliente.php	Php	Realiza la transacción de registro al sistema.
Perdió su contraseña	Derecho	Recordar_clave.html	Html	Formulario informativo y de ingreso para recordar clave
Entrega de nueva contraseña	Central	validar_usuario.php	Php	Ingreso, validación para nueva contraseña
Entrega de nueva contraseña	Central	Password.php	Php	Generación de nueva contraseña
Regalo Ideal	Derecho	criterios.php	Php	Muestra en area central los arreglos que cumplen las condiciones ingresadas

Fig 6.18 Estructura del sitio-Menú lateral derecho inicial
Fuente: Autores

En las opciones del Menú Lateral derecho inicial básicamente realiza dos funciones: la autenticación de usuarios y la búsqueda personalizada de arreglos florales.

6.2.2.5 Menú lateral derecho final

A partir de (“rigth2.php”) se derivan las siguientes funcionalidades

Opción	Frame	Programa	Tipo de Programa	Descripción
Ver Datos	Derecho	datoscliente.php Parámetro: Modificar = 0	Php	Muestra los datos personales del cliente de manera informativa.
Modificar mis Datos	Derecho	datoscliente.php Parámetro: Modificar = 1	Php	Muestra los datos personales y realiza las validaciones de los mismos.
Modificar mis Datos	Central	Modifica_cliente.php	Php	Realiza la transacción de modificación de los datos del cliente.
Mis Compras	Central	Ver_ordenes.php	Php	Muestra el historial de compras realizadas
Detalle de Compras	Central	consulta_orden.php	Php	Por cada compra realizada muestra su detalle.
Salir	Derecho	Salir.php	Php	Destruye la sesión y muestra en área central.

Fig 6.19 Estructura del sitio – Manú lateral derecho final
Fuente: Autores

En las opciones del Menú Lateral derecho final básicamente realiza dos funciones: consultar o modificar datos personales del cliente y búsquedas personalizadas.

6.3 Manual y políticas de usuario

6.3.1 Navegación Libre.

El usuario abre el navegador de internet (Microsoft Explorer o Netscape) y debe digitar el url: http://www.contodomiamor.com. A continuación se observará el siguiente contenido que presenta en la página central la imagen animada de presentación. Esta imagen también se la obtiene directamente usando la opción Principal del menú horizontal superior

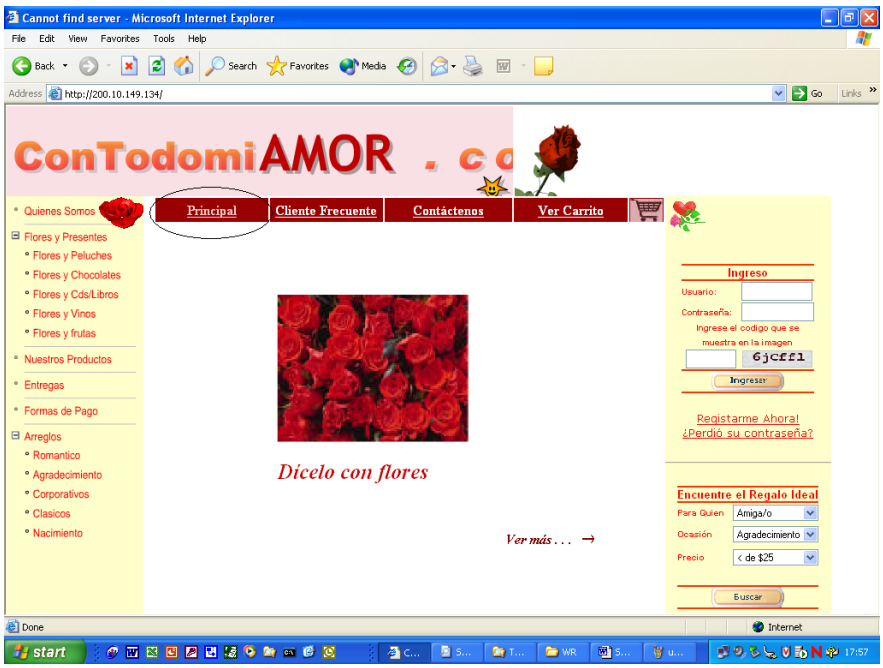

Figura 6.20 Página principal del sitio
Fuente: Autores

Luego de ingresar al sitio, el usuario sin estar registrado o haberse autenticado, puede realizar consultas y observar los artículos que www.contodomiamor.com tiene disponibles a la venta. Puede observar las opciones informativas que el sitio presenta y puede registrarse, estas opciones no necesitan autenticarse al sitio.

6.3.1.1 Opciones Informativas

6.3.1.1.1 Quiénes Somos: está ubicada en el menú lateral izquierdo y presenta la información de cómo nació la empresa, cuáles son los objetivos entre los cuales destaca la experiencia tecnológica que se posee para el desarrollo de sitios web seguros.

Figura 6.21 Página de Quiénes somos
Fuente: Autores

Al final de esta información se presenta un enlace para ver las oficinas donde opera la empresa.

6.3.1.1.2 Nuestros Productos

Esta opción también está ubicada en el menú lateral izquierdo y presenta información general acerca de los productos que se ofrecen. Tiene un enlace que lleva directamente a ver la cobertura de entregas que se tiene en la actualidad.

Figura 6.22 Página de Nuestros Productos
Fuente: Autores

En esta página se describe brevemente el tipo de artículos (arreglos florales y obsequios complementarios) que se ofrecen para la venta.

6.3.1.1.3 Entregas

Esta opción se presenta en el menú lateral izquierdo y presenta información al usuario sobre la cobertura que se ofrece y de la alianza estratégica con la mejor empresa de envío y recepción en el Ecuador que es Servientrega.

Esta opción presenta un enlace hacia el sitio web de Servientrega informado las áreas de cobertura a nivel nacional y un enlace para ver las oficinas en donde opera contodomiamor.com

Figura 6.23 Página de coberturas a nivel nacional
Fuente: Autores

Para el desarrollo del proyecto, se propone una alianza estratégica con una compañía local que se encargará de los detalles logísticos en la entrega de obsequios.

6.3.1.1.4 Formas de Pago

Esta opción se presenta en el menú lateral izquierdo y muestra las formas de pago que el sitio permite y un breve paso a paso de cómo realizar la compra en el sitio. Adicionalmente se presenta un enlace para observar dónde estan ubicados los locales.

Figura 6.24 Página de formas de pago.
Fuente: Autores

En esta página se informa al cliente que la única forma de pago disponible es mediante tarjetas de crédito.

6.3.1.1.5 Cliente Frecuente

Esta opción se ubica en el menú horizontal superior e informa al usuario del tipo de cliente que puede llegar a ser en nuestro sitio, gozando de las ventajas de cada una de éstas categorías e indicando las políticas que rigen en las mismas.

Figura 6.25 Página de cliente frecuente
Fuente: Autores

Cabe destacar que en la implementación del proyecto no se desarrolló esta funcionalidad dado que el objetivo del tópico está orientado a esquemas de

seguridad; sin embargo el diseño de la base de datos permite futuras actualizaciones.

6.3.1.1.6 Contáctenos

Esta opción está ubicada en el menú superior izquierdo y da la funcionalidad de enviar un email a la administración del sitio, adjuntando las inquietudes que existan y que serán contestadas a la brevedad posible por el equipo de contodomiamor.com

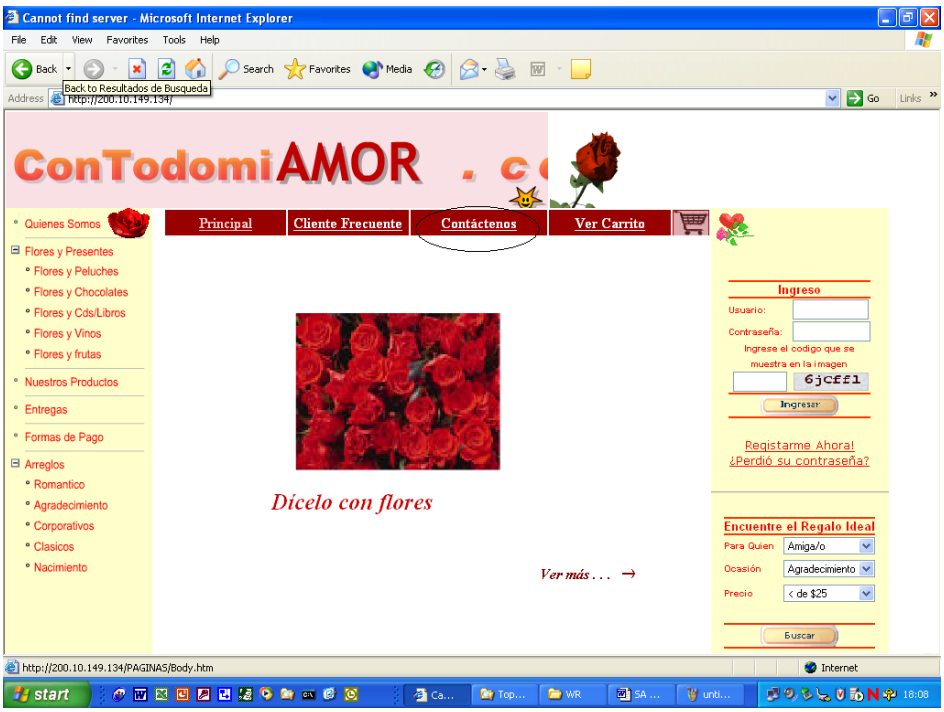

Figura 6.26 Página de Contáctenos
Fuente: Autores

El editor de correo a ser utilizado es el programa por defecto en el equipo del cliente.

6.3.1.2 Opciones de Productos Disponibles

6.3.1.2.1 Menú de Flores y Presentes

Está ubicado en la parte lateral izquierda y presenta 5 opciones regalos que son: flores y peluches, flores y chocolates, flores y cd/libros, flores y vinos, flores y frutas.

Figura 6.27 Menú de Flores y Presentes
Fuente: Autores

Los arreglos incluídos en cada una de las opciones, se presentan en el área central del sitio.

6.3.1.2.2 Menú de Arreglos

Está ubicado en la parte lateral izquierda y presenta 5 opciones de arreglos que son: romántico, agradecimiento, corporativos, clásicos y nacimientos.

Figura 6.28 Tipos de arreglos
Fuente: Autores

De manera similar al menú anterior, cuando se selecciona un tipo de arreglo este será mostrado en el área central del sitio.

6.3.1.2.3 Regalo Ideal

Esta opción se la tiene disponible en el menú lateral derecho en la parte inferior, se manejan tres criterios de búsqueda que son:

- Para Quién. Presenta las siguientes opciones: amiga(o), enamorada(o), esposa(o), futura conquista, mamá y papá.
- Ocasión: Presenta las siguientes opciones: agradecimiento, aniversario, romántico, cumpleaños, nacimiento, graduación.
- Precio: Presenta 4 rangos de precios: menor a 25, entre 25 y 50, entre 50 y 100, mayor a 100.

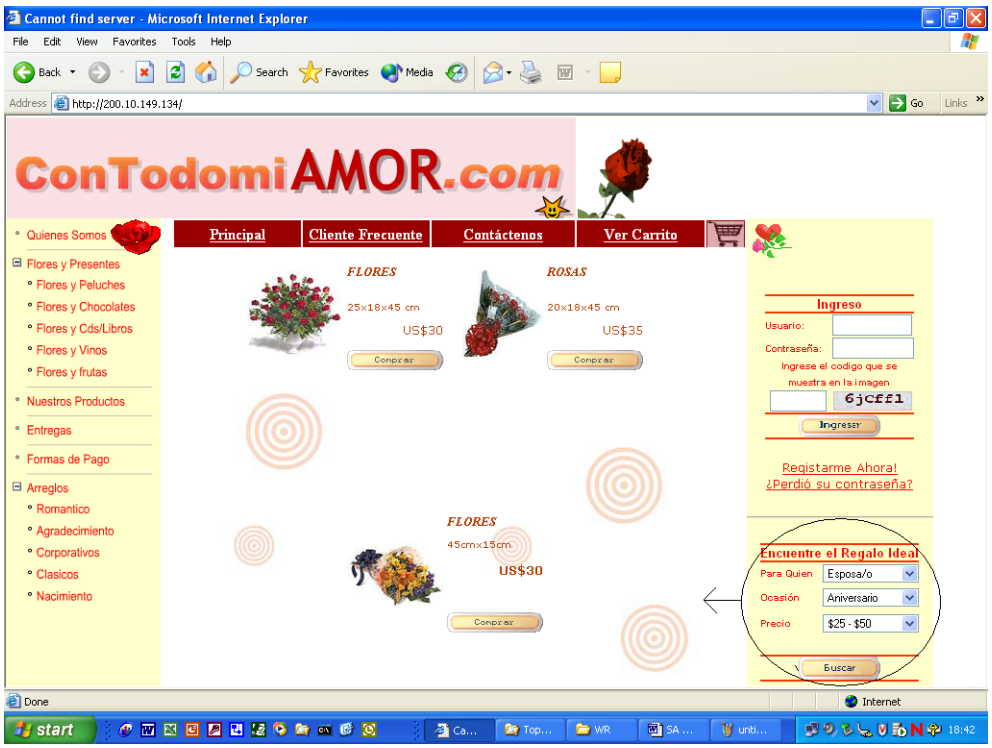

Figura 6.29 Sección de Encuentre el Regalo Ideal
Fuente: Autores

El equipo de (“contodomiamor.com”) ha clasificado cuidadosamente los arreglos que cumplan con las características que solicita el usuario a través de esta opción de regalo ideal.

6.3.1.3 Registro de Usuario

La opción de Registro aparece en el menú lateral derecho con el nombre de (“Registrarme Ahora”), el cual permitirá llenar el perfil personal y el perfil de cuenta.

6.3.1.3.1 Perfil Personal

La opción de registro aparece en el menú lateral derecho con el nombre de (“Registrarme Ahora”), esto mostrará el formulario de cliente en la parte central del sitio dividiendo en dos el tipo de información: la primera parte solicitando los datos personales tales como: nombre, apellido, sexo, fecha de nacimiento, país de origen, provincia, ciudad, dirección, teléfono.

Figura 6.30 Información de perfil del usuario
Fuente: Autores

A continuación se explicará brevemente sobre los datos que deben ser ingresados en la sección (“Información de Perfil”).

6.3.1.3.2 Perfil de cuenta y Validación de imagen

Solicita datos del usuario en el sitio como son: dirección de correo, nombre de usuario, contraseña, pregunta secreta.

Esta opción presenta al final el manejo de autenticación de sitio a través de un esquema en el cual el usuario debe digitar los caracteres que ve en la imagen generada en el sitio.

Figura 6.31 Información de perfil de cuenta
Fuente: Autores

El objetivo del “touring number” es evitar que programas maliciosos (robots) generen cuentas de manera excesiva, saturando los recursos del sitio.

6.3.1.3.3 Registro Exitoso

Todos los campos de los formularios están validados de manera que el usuario debe ingresar la información correcta sino el registro no se podrá realizar.

Si el registro es exitoso la siguiente pantalla se mostrará:

Figura 6.32 Registro de usuario exitoso
Fuente: Autores

Luego del registro exitoso el cliente ya está en capacidad de realizar transacciones de compra en el sitio.

6.3.2 Navegación con Autenticación

6.3.2.1 Ingreso

La opción de ingreso al sistema aparece en el menú lateral derecho, donde se debe digitar el usuario, la contraseña y el “touring number”.

Figura 6.33 Digitación de datos: usuario/contraseña y “touring number”
Fuente: Autores

Si el ingreso es exitoso, se mostrará la siguiente pantalla que da la bienvenida y permite nuevas opciones de consultas de datos y de compras.

Figura 6.34 Ingreso de usuario al sitio web y bienvenida.
Fuente: Autores

En el mensaje de bienvenida se estableció saludar al usuario con su primer nombre.

6.3.2.2 Ver Datos personales

Está ubicado en el menú lateral izquierdo y muestra de forma no modificable los datos personales del usuario. Esta opción sólo aparece si el cliente se autentificó en el sitio a través de su usuario y contraseña.

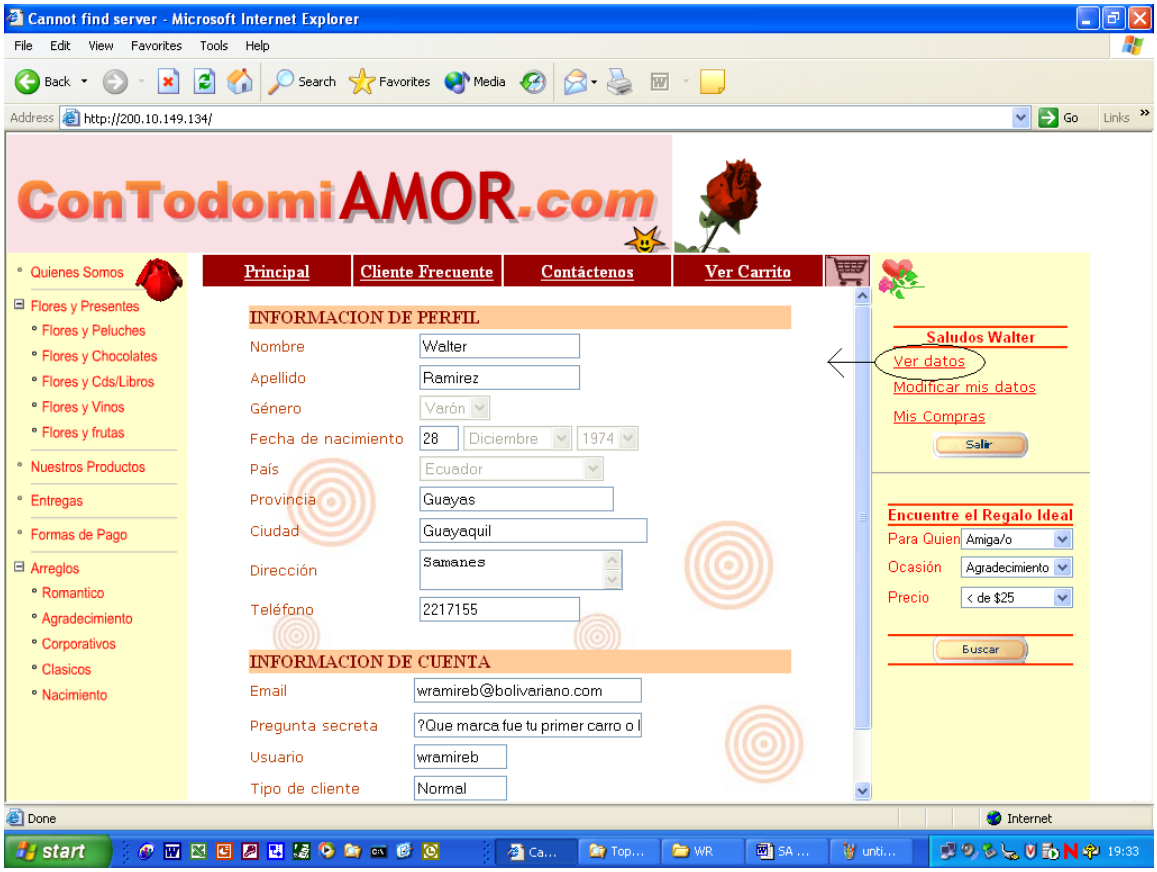

Figura 6.35 Observar datos personales
Fuente: Autores

Para editar la información del usuario es necesario seleccionar el enlace (“Modificar mis datos”), la cual se describe a continuación.

6.3.2.3 Modificar Datos personales

Está ubicado en el menú lateral izquierdo y muestra de forma modificable los datos personales del usuario. Esta opción solo aparece si el cliente se autenticó en el sitio a través de su usuario y contraseña.

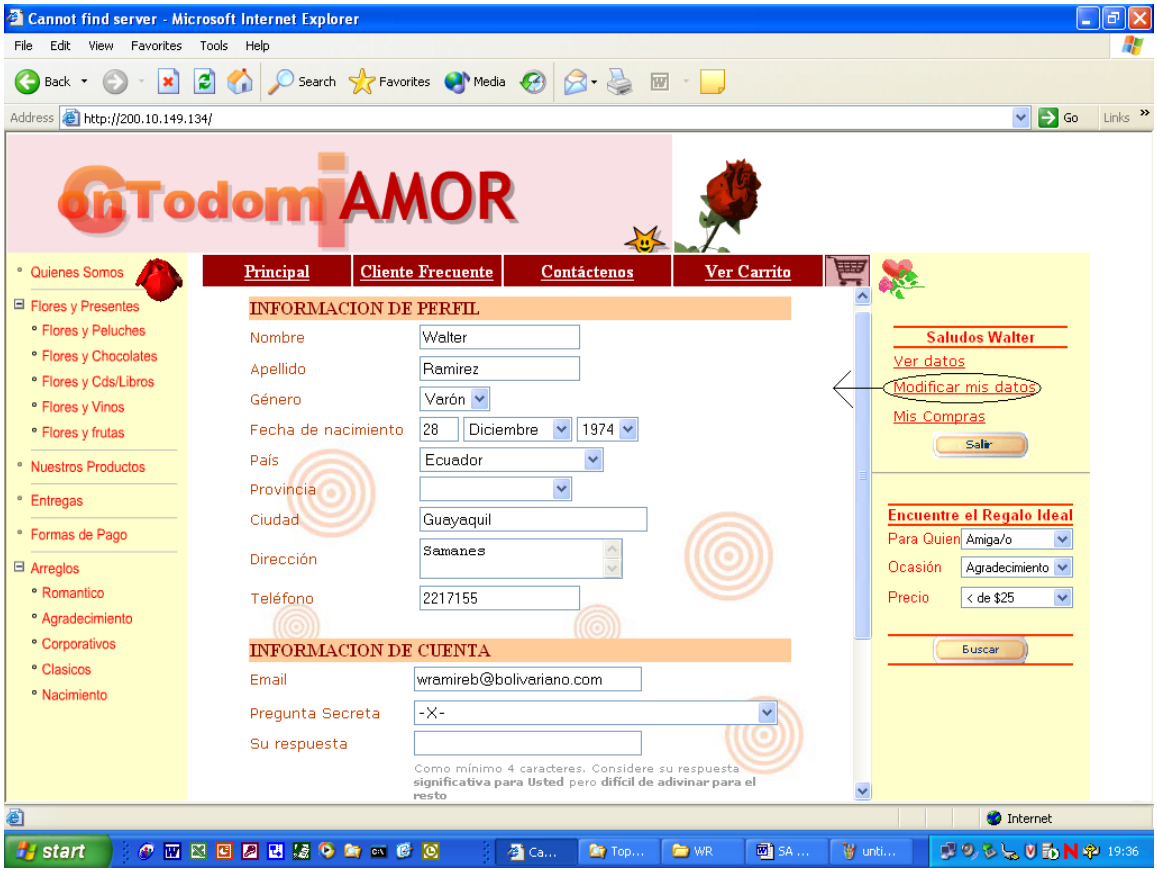

Figura 6.36 Modificación de datos del perfil
Fuente: Autores

En la modificación de los datos solamente se permite al alteración de datos generales como: dirección, teléfono.

6.3.2.4 Consulta de Compras realizadas

Está ubicado en el menú lateral izquierdo y muestra el historial de compras realizadas por el usuario, mostrando inclusive el estado actual del pedido.

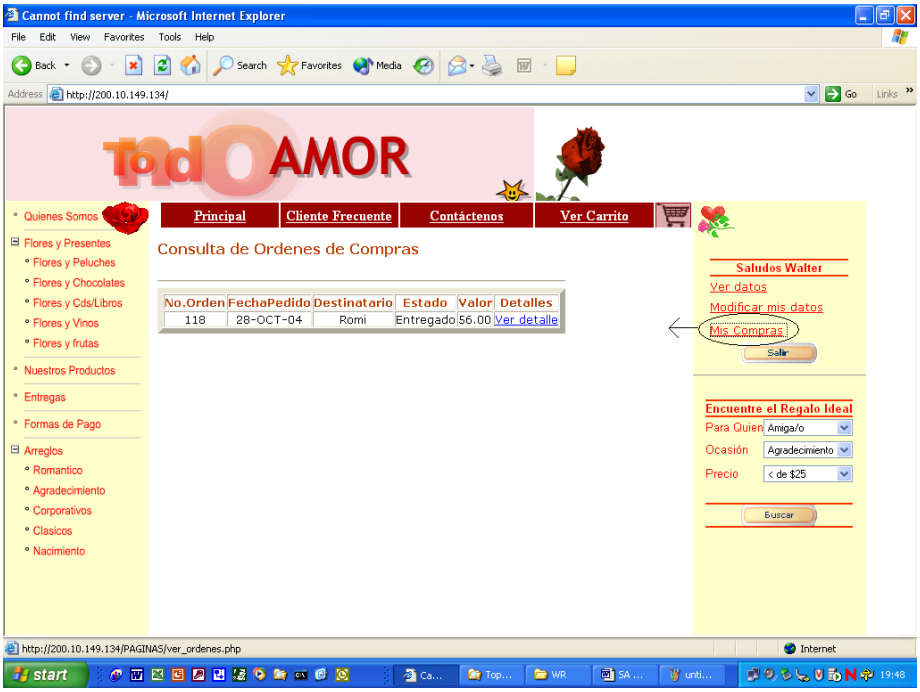

Figura 6.37 Consulta de órdenes de compra
Fuente: Autores

En la consulta de compras realizadas se muestra el resumen de la orden de compra: fecha de la transacción, destinatario, total.

Figura 6.38 Detalle de orden de compra
Fuente: Autores

En el detalle de la orden de compra se presenta información como: tipo y número de tarjeta de crédito utilizada, listado y cantidades de los artículos adquiridos.

6.3.2.5 Realizar una Compra

6.3.2.5.1 Agregando al carro de compras

Cada arreglo al mostrarse en la página central viene acompañado de un botón (“comprar”), el mismo que automáticamente agrega el ítem al carro de compras y visualiza el mismo en el sitio.

Figura 6.39 Agregando artículos al carrito de compras
Fuente: Autores

Como se observa en la imagen, al agregar un item al carro de compras se actualiza el total a pagar en la transacción.

6.3.2.5.2 Eliminando artículos del carro de compras

Para eliminar ítems del carro de compras, se debe marcar el artículo en la primera columna del carro de compras y dar el botón (“Actualizar Cesta”).

Figura 6.40 Eliminando artículos del carrito de compras
Fuente: Autores

Se pueden eliminar los ítems agregados en el carro de compras, en cualquier momento antes de seleccionar el botón (“Realizar Pedido”).

6.3.2.5.3 Continuar Compra

Esta opción retorna al usuario a la página de arreglos con lo cual se pueden añadir más ítems al carro de compras.

Figura 6.41 Continuar comprando
Fuente: Autores

La función principal del botón (“Continuar Compra”) es quitar de la vista del usuario el carro de compras, continuando con la elección de artículos.

6.3.2.5.4 Realizar Pedido

Esta opción direcciona a la página de ingreso de datos del destinatario donde se personaliza el mensaje a enviar.

Figura 6.42 Ingreso de datos del destinatario
Fuente: Autores

Cabe destacar que la opción (“Realizar pedido”) es una preliquidación de la compra, puesto que el usuario no podrá ingresar más artículos en esta compra.

6.3.2.5.5 Pago mediante Tarjeta de Crédito

Una vez que se ingresan los datos del destinatario y se personaliza el mensaje, aparece el formulario de ingreso de tarjeta de crédito. En este formulario se debe llenar los datos de tipo de tarjeta, número de bin, nombre del propietario, fecha de expiración, dirección, cvv2 (el número que consta en la parte de atrás de las tarjetas y que no está almacenado en la banda magnética) y la frase secreta.

Figura 6.43 Página de pago mediante tarjeta de crédito
Fuente: Autores

Todos estos datos deben ser ingresados tal como constan en el establecimiento que emitió la tarjeta, ya que el servidor del establecimiento verifica los datos ingresados autentificando el pago.

6.3.2.5.6 Resumen de Pago

Al finalizar el pago, se muestra en el área central el (“Resumen de Factura”) y el detalle de artículos.

Figura 6.44 Página de resumen de factura
Fuente: Autores

Cabe mencionar que esta es la última pantalla en el flujo de la transacción de compra realizada por el cliente.

6.3.2.6 ¿Perdió su contraseña?

Si el usuario ha extraviado su contraseña, se brinda la funcionalidad de generar una nueva clave de acceso.

Para solicitarla, es primordial que el cliente recuerde la respuesta secreta que ingresó al momento del registro inicial en el sitio.

Figura 6.45 Página de recordar de contraseña
Fuente: Autores

Se solicita el nombre, apellido y correo electrónico para verificar que el usuario que desea obtener una nueva contraseña está previamente registrado en el sitio.

6.3.2.6.1 Ingreso de respuesta secreta

Al verificar que el usuario ya está registrado previamente en el sitio, se procede a presentarle la pregunta secreta (la cual fue ingresada en el registro inicial).

Figura 6.46 Página de ingreso de respuesta secreta
Fuente: Autores

Se valida lo siguiente: que la respuesta proporcionada por el usuario sea correcta, así como el “touring number” (utilizado también en el registro inicial).

6.3.2.6.2 Entrega de nueva contraseña

Finalmente, una vez que se han completado exitosamente los dos pasos anteriores, el sistema generará una nueva clave.

Figura 6.47 Generación de nueva contraseña
Fuente: Autores

La nueva contraseña se presenta por pantalla y está habilitada para su inmediato uso.

6.4 Desarrollo de carro de compras

6.4.1 Introducción

Para el desarrollo del “carrito de compras” en el lenguaje de programación php, se investigó vía web los diferentes tipos de implementaciones realizadas.

Para el diseño de nuestro sitio se orientó el análisis y diseño en 2 puntos importantes: el acceso a la base de datos y una interface agradable y amigable al usuario.

Php trae consigo un estable manejo de sesiones que se aprovechó para disminuir los accesos a la base de datos, ya que por estadísticas es muy alto el número de usuarios que ingresa ítems al carro y al final no realiza la compra.

6.4.2 Manejo de Sesiones

Para recordar un poco la infraestructura implementada, es necesario recordar que sobre el web server descansa el lenguaje de programación php, es decir este corre del lado del servidor.

Una sesión en php lo que hace es generar un archivo temporal cargando la información que se necesita mantener en la vida de la sesión, evitando con

esto grabar datos a la base con el objetivo de poder consultarlos nuevamente.

En la implementación del “carrito de compras” se manejó sesiones mientras el usuario continue haciendo las operaciones de añadir o eliminar, una vez que el decida pasar a la siguiente etapa de la compra que es llenar los datos del destinatario, en este momento se procede a grabar la información de la orden junto con la del destinatario a la base de datos, disminuyendo los requerimientos innecesarios al servidor de datos.

6.4.3 Implementación

El detalle del código fuente se incluye como Anexos.

CONCLUSIONES Y RECOMENDACIONES

Una vez finalizada la investigación e implementación del proyecto de graduación, se puede como destacar como aspectos relevantes las siguientes conclusiones y recomendaciones.

- En base al esquema de red desarrollado en el proyecto de graduación, se puede concluir que un esquema seguro debe ser implantado utilizando herramientas de bloqueo y detección en el segmento que enlaza la red objetivo con el exterior.

- En la opinión de los Autores, la primera regla para evitar ataques a sitios web es adoptar una actitud preventiva; es decir bloqueando los potenciales puntos de amenazas, tanto a nivel externo e interno de la organización.

- Se ha demostrado que mediante el uso de herramientas “open-source” (implantado en el firewall interno – servidor de base de datos), además de ofrecer un bajo costo en términos económicos es posible implementar esquemas confiables y seguros.

- Mediante la implementación de “touring numbers” incorporados a los esquemas de autenticación de usuarios, se concluye que se puede incrementar el nivel de seguridad actual en el Ecuador, dado que este mecanismo no ha sido adoptado por los sitios web locales.

- Considerando la realidad ecuatoriana respecto a medidas de protección ante ataques externos, es criterio de los Autores que la incorporación de sistemas de detección de intrusos aporta significativamente a incrementar la seguridad dado que apoya a los sistemas tradicionales basados en firewalls.

- Se concluye que una alternativa muy eficiente para asegurar la confidencialidad de la información que viaja por Internet, se logra mediante el uso de sesiones SSL; dado que su implementación no es compleja en términos tecnológicos.

- La página desarrollada implementa una interfaz amigable y fácil de usar, permitiendo al cliente varias opciones para escoger el regalo ideal para su ser querido y una forma de pago que brinda seguridad al cliente.

- A lo largo del proyecto se hace énfasis del peligro que ocasiona sistemas no correctamente auditados y actualizados, también de las vulnerabilidades existentes y las medidas a tomar para prevenirlos, con lo cual se espera lograr fomentar una cultura de seguridad tanto en los administradores de red como a nivel gerencial.

- Finalmente se concluye que en el diseño e implementación de una red no solo es importante la funcionalidad y rapidez de la misma, sino también la seguridad y respuesta inmediata ante sucesos inesperados a través de sistemas de contingencias.

Considerando el continuo avance y cambio tecnológico en la actualidad, es importante recalcar que este proyecto es un primer paso en fomentar la cultura de seguridad informática en nuestro País.

ANEXOS

Implementación

1.1 Inicio de la Sesión

Si el cliente no está autenticado, muestra la página de ingreso en el sitio.

```
<?php session_start();
if(($_SESSION['id_cliente']) < 1 or ($_SESSION['id_cliente'] == ''))
{
header("Location: ingresar.php");
}
?>
```

1.2 Tabla de Compras

Muestra el "carrito de compras" con sus columnas eliminar, producto, descripción, cantidad, precio y subtotal.

```
<html>
<head><title>Carrito</title>
<script language="JavaScript">
function ejecutar() {
   document.form2.submit();
};
</script>
</head>
<body>
<form action="<?php echo $_SERVER['PHP_SELF'];?>"
method="POST"><table border="6" cellpadding = "0" cellspacing = "1">
 <?php
 if($_SESSION['id_cliente'] > 0)
  {
echo "<p align ='center'><font face=Verdana size='3'
color='#BB3D00'><strong>Carrito de Compras</strong></p><hr>";
  echo"<tr><td><font face=Verdana color='#BB3D00'
size='2'><strong>Eliminar</strong></td><td align='middle'><font
face=Verdana color='#BB3D00'
size='2'><strong>Producto(s)</strong></td><td align='middle'><font
face=Verdana color='#BB3D00'
```

```
size='2'><strong>Descripción</strong></td><td><font  face=Verdana
color='#BB3D00' size='2'><strong>Cantidad</strong></td><td><font
face=Verdana
color='#BB3D00'size='2'><strong>Precio</strong></td><td><font
face=Verdana color='#BB3D00'
size='2'><strong>Subtotal</strong></td></tr>";
};
?>
```

1.3 Agregar al carro
Valida la sesión y procede a guardar en el arreglo de sesión el item de la compra

```
<?php



//VERIFICAR  SI ESTA CONECTADO EL CLIENTE
//Valores viajan de form

$codigo= $_GET['codigo'];
$descripcion= $_GET['descripcion'];
$precio= $_GET['precio'];
$cantidad=$_GET['cantidad'];
$ban=$_GET['ban'];
if ( $ban == 1)
{
 if($_SESSION['id_cliente'] > 0)
  {
 //echo "ENTRO PARA AGREGAR A CARRO";
//vars en la ses
  $contador_sesion = $_SESSION["contador"];
  $_SESSION["carro_codigo[$contador_sesion]"] = $codigo;
  $_SESSION["carro_desc[$contador_sesion]"] = $descripcion;
  $_SESSION["carro_cantidad[$contador_sesion]"] = $cantidad;
  $_SESSION["carro_precio[$contador_sesion]"] = $precio;
  $_SESSION["carro_estado[$contador_sesion]"] = "I";
  $_SESSION["contador"] = $_SESSION["contador"] + 1;

 }
}
```

1.4 Actualizar Cesta
Si el usuario ha escogido eliminar, este codigo barre cada uno de los items y procede a modificar los arreglos de sesión

```
//SI HIZO SUBMIT ACTUALIZAR CESTA
else {
  $max=$_SESSION["contador"];
  $ind=0;
  while($ind<$max){
    $variable = "chk".$ind;
    $chk=$_POST[$variable];
    if(($chk==$ind) && ($chk != null)){
      $_SESSION["carro_estado[$ind]"] = "E";
     }
    $ind++;
  }
 }
```

1.5 Mostrar Arreglos

Mostrar los arreglos agregados adjuntando los botones de actualizar cesta, continuar compra y realizar pedido

```
//SIEMPRE MUESTRO TODO EL ARREGLO

if($_SESSION['id_cliente'] > 0)
{
$ind=0;
$total_compra = 0;
$max=$_SESSION["contador"];
while($ind<$max){

     if ($_SESSION["carro_estado[$ind]"]=="I"){

     echo "<tr>
            <td><input type='checkbox' name='chk".$ind."'
value='".$ind."'>".$arr_usu[$ind]."</td>
            <td><img
src=../IMAGENES/".$_SESSION["carro_codigo[$ind]"]."></td>
            <td align='middle'>".$_SESSION["carro_desc[$ind]"]."</td>
            <td align='middle'>".$_SESSION["carro_cantidad[$ind]"]."</td>
                 <td
align='middle'>".number_format($_SESSION["carro_precio[$ind]"],2,'.',',')."</t
d>
            <td align='middle'>$
".number_format(($_SESSION["carro_cantidad[$ind]"]*$_SESSION["carro_pr
ecio[$ind]"]),2,'.',',')."</td></tr><tr></tr>";
      $total_compra = $total_compra +
($_SESSION["carro_cantidad[$ind]"]*$_SESSION["carro_precio[$ind]"]);

     }
         $ind++;
  }
echo "<tr>
            <td></td>
            <td></td>
            <td><font face=Verdana color='#BB3D00' size='2'><strong>TOTAL
DE COMPRA:</strong></td>
            <td></td>
                 <td></td>
            <td>$
".number_format($total_compra,2,'.',',')."</td></tr><tr></tr><tr></tr><tr></tr>";
```

```
 }
if($_SESSION['id_cliente'] > 0)
{

echo "<br>
<table border='0' align='center'>
  <tr>
  <td><input type = image src='../BOTONES/ActualizarCesta.gif'  width='129'
height='32' border='0' name = 'sub' <ALT='Submit'>
  <a href='pagina_dinamica.php?producto=1'  target='mainFrame'><img
src='../BOTONES/ContinuarCompra.gif'  width='129' height='32'
border='0'></a>
  <a href='destino.php'><img  src='../BOTONES/RealizarPedido.gif'
width='130' height='32' border='0'></a></td>
  </tr>
</table>";

echo "<p><font face=Verdana color='#BB3D00' size='2'>Gracias por usar
nuestro carro de compras. Para borrar alg&uacute;n elemento
m&aacute;rquelo y de “click”en <strong> -Actualizar Cesta-</strong>. Si
desea agregar m&aacute;s art&iacute;culos de “click”en <strong>-Continuar
Compra-</strong> o si desea finalizar su compra, de “click”en <strong>-
Realizar Pedido-</strong></p>";

 }
?>
</form>
</body>
</html>
```

1.6 Solicitar Pedido

Referencia a la página destino.php, aquí se verá en primera instancia las validaciones de los datos del formulario de destino, el diseño del formulario de destino y la llamada a grabar_orden.php quien realmente envía la solicitud a la base de datos

```
<!-- Uso de frmlarios.html  -->
<HTML>
<SCRIPT language="JavaScript1.3">
 function validar(){
  if(document.frm.destinatario.value=="")
```

```
  {alert("El campo Destinatario está vacío");}
   else {
      if(document.frm.ciudad_dest.value==0)
       {alert("Debe seleccionar una Ciudad");}
         else {
          if(document.frm.sector_dest.value==0)
            {alert("Debe seleccionar un Sector");}
              else{
               if(document.frm.direccion_dest.value=="")
                {alert("Debe ingresar la Direccion");}
                  else{
                   if(document.frm.telefono_dest.value=="")
                    {alert("Debe ingresar un Telefono");}
                      else
                      {
                       if(document.frm.mensaje_envio.value=="")
                       {alert("Debe ingresar un Mensaje");}
                        else
                        {  if(document.frm.dia_envio.value=="")
                           {alert("Debe ingresar un Día");}
                           else
                           {
                            if(document.frm.mes_envio.value=="0")
                            {alert("Debe escoger un Mes");}
                            else
                            {
                            if(document.frm.anio_envio.value=="0")
                                  {alert("Debe escoger un año");}
                                   else
                                   {
                                     if(document.frm.hora_envio.value=="0")
                                     {alert("Debe ingresar una hora de entrega");}
                                      else
                                        {
                                         document.frm.submit();
                                             }}}}}}}}}}
                                             };

</SCRIPT>
<HEAD><TITLE>Ingrese  los datos del destinatario</TITLE></HEAD>
<BODY background="../IMAGENES/fondo1.jpg">
<FORM NAME='frm' method = 'post' ACTION='grabar_orden.php'>
<?php
```

```
echo " <p><font color='#BB3D00' size='4' face=Verdana><strong>Datos
generales del Destinatario</strong></p><hr>
  <TABLE BORDER=0>
 <TR>
  <TD><font color='#BB3D00' size='2' face=Verdana>Nombre:</TD>
  <TD><INPUT TYPE='text' NAME='destinatario' SIZE=35
MAXLENGTH=35></TD>
 </TR>
 <TR>
  <TD><font color='#BB3D00' size='2' face=Verdana>Ciudad</TD>
  <TD><select name='ciudad_dest'>
        <OPTION VALUE=0 selected>- X -</OPTION>
        <OPTION VALUE=1>Guayaquil</OPTION>
        <OPTION VALUE=2>Quito</OPTION>
        <OPTION VALUE=3>Cuenca</OPTION>
        <OPTION VALUE=4>Esmeraldas</OPTION>
        <OPTION VALUE=5>Atacames</OPTION>
        <OPTION VALUE=6>Portoviejo</OPTION>
        <OPTION VALUE=7>Manta</OPTION>
        <OPTION VALUE=8>Samborondón</OPTION>
        <OPTION VALUE=9>Babahoyo</OPTION>
        <OPTION VALUE=10>Quevedo</OPTION>
        <OPTION VALUE=11>Machala</OPTION>
        <OPTION VALUE=12>Tulcán</OPTION>
        <OPTION VALUE=13>Ibarra</OPTION>
        <OPTION VALUE=14>Otavalo</OPTION>
        <OPTION VALUE=15>Sto. Domingo de los Colorados</OPTION>

        <OPTION VALUE=16>Latacunga</OPTION>
        <OPTION VALUE=17>Ambato</OPTION>
        <OPTION VALUE=18>Guaranda</OPTION>
        <OPTION VALUE=19>Riobamba</OPTION>
        <OPTION VALUE=20>Azogues</OPTION>
        <OPTION VALUE=21>Loja</OPTION>
        <OPTION VALUE=22>Nueva Loja</OPTION>
        <OPTION VALUE=23>Tena</OPTION>
        <OPTION VALUE=24>Puyo</OPTION>
        <OPTION VALUE=25>Macas</OPTION>
        <OPTION VALUE=26>Zamora</OPTION>
        <OPTION VALUE=27>Pto. Baquerizo Moreno</OPTION>
  </select></TD>
 </TR>
 <TR>
  <TD><font color='#BB3D00' size='2' face=Verdana>Sector:</TD>
```

```
 <TD><select name='sector_dest'>
      <OPTION VALUE=0 selected>- X -</OPTION>
      <OPTION VALUE=1>Norte</OPTION>
      <OPTION VALUE=2>Centro</OPTION>
      <OPTION VALUE=3>Sur</OPTION>
      <OPTION VALUE=4>Otro</OPTION>
 </select> </td>
</TR>
 <TR>
 <TD><font color='#BB3D00' size='2' face=Verdana>Dirección:</TD>
 <TD><textarea name='direccion_dest' cols='30' rows='4'></textarea></TD>
 </TR>
 <TR>
 <TD><font color='#BB3D00' size='2' face=Verdana>Teléfono:</TD>
 <TD><INPUT TYPE='text' NAME='telefono_dest' SIZE=20
MAXLENGTH=20></TD>
 </TR>
 </TABLE>
 <a> </a>
<p><font color='#BB3D00' size='4' face=Verdana><strong>Mensaje y
detalles en el envío</strong></p><hr>
 <TABLE BORDER=0>
 <TR>
 <TD><font color='#BB3D00' size='2' face=Verdana>Mensaje:</TD>
 <TD><textarea name='mensaje_envio' cols='40' rows='5' ></textarea></TD>
 </TR>
 <TR>
 <TD><font color='#BB3D00' size='2' face=Verdana>Fecha:</TD>
 <TD><INPUT TYPE='text' NAME='dia_envio' SIZE=2 MAXLENGTH=2>
 <select name='mes_envio'>
      <OPTION VALUE='0' selected>- X -</OPTION>
      <OPTION VALUE='JAN'>Enero</OPTION>
      <OPTION VALUE='FEB'>Febrero</OPTION>
      <OPTION VALUE='MAR'>Marzo</OPTION>
      <OPTION VALUE='APR'>Abril</OPTION>
      <OPTION VALUE='MAY'>Mayo</OPTION>
      <OPTION VALUE='JUN'>Junio</OPTION>
      <OPTION VALUE='JUL'>Julio</OPTION>
      <OPTION VALUE='AUG'>Agosto</OPTION>
      <OPTION VALUE='SEP'>Septiembre</OPTION>
      <OPTION VALUE='OCT'>Octubre</OPTION>
      <OPTION VALUE='NOV'>Noviembre</OPTION>
      <OPTION VALUE='DEC'>Diciembre</OPTION>
 </select>
```

```
 <select name='anio_envio'>
      <OPTION VALUE='0' selected>- X -</OPTION>
      <OPTION VALUE='2004'>2004</OPTION>
      <OPTION VALUE='2005'>2005</OPTION>
 </select>
 </TR>
<TR>
<TD><font color='#BB3D00' size='2' face=Verdana>Hora:</TD>
<TD><select name='hora_envio'>
      <OPTION VALUE='0' selected>- X -</OPTION>
      <OPTION VALUE='8:00 a.m.'>8:00 a.m.</OPTION>
      <OPTION VALUE='9:00 a.m.'>9:00 a.m.</OPTION>
      <OPTION VALUE='10:00 a.m.'>10:00 a.m.</OPTION>
      <OPTION VALUE='11:00 a.m.'>11:00 a.m.</OPTION>
      <OPTION VALUE='12:00 p.m.'>12:00 p.m.</OPTION>
      <OPTION VALUE='1:00 a.m.'>1:00 p.m.</OPTION>
      <OPTION VALUE='2:00 a.m.'>2:00 p.m.</OPTION>
      <OPTION VALUE='3:00 a.m.'>3:00 p.m.</OPTION>
      <OPTION VALUE='4:00 a.m.'>4:00 p.m.</OPTION>
      <OPTION VALUE='5:00 a.m.'>5:00 p.m.</OPTION>
      <OPTION VALUE='6:00 a.m.'>6:00 p.m.</OPTION>
      <OPTION VALUE='7:00 a.m.'>7:00 p.m.</OPTION>
      <OPTION VALUE='8:00 a.m.'>8:00 p.m.</OPTION>
 </select></TD></tr>";
?>
<br>
<tr><td><img src='../BOTONES/ContinuarCompra.jpg'   width='120'
height='30' border='0' name = 'sub' on”click”k='validar()'></td>
<td><a href=carro_compras.php><img  src='../BOTONES/cancelar.gif'
width='120' height='30' border='0' name = 'sub'></a></td>
 </TR>
</table>
</FORM>
</BODY>
</HTML>
```

1.7 Orden de Compra

Referencia a la página grabar_orden.php, en primera instancia carga por referencia las variables enviadas por el php que lo ejecutó que es destino.php, luego abre la conexión a la base de datos, barre en un cursor todos los item que se encuentren en el arreglo de sesion (items de carro de compras) y graba en las tablas de orden_detalle y orden_compra y finalmente llama al formulario de ingreso de tarjeta a través del programa pagos.php

```
<?php session_start(); ?>
<?php
$nombre = $_POST['nombre'] ;
$nombre_destino = $_POST['destinatario'];
$ciudad_destino = $_POST['ciudad_dest'];
$sector_destino = $_POST['sector_dest'];
$direc_destino  = $_POST['direccion_dest'];
$telefono_destino = $_POST['telefono_dest'];
$mensaje_destino  = $_POST['mensaje_envio'];
$dia = $_POST['dia_envio'];
$mes = $_POST['mes_envio'];
$anio = $_POST['anio_envio'];
$fecha_destino =$dia."-".$mes."-".$anio;
$hora_destino  = $_POST['hora_envio'];
$id_cliente = $_SESSION["id_cliente"];

$c1 =
ocilogon("dba01","user0103","FLORESDB.CONTODOMIAMOR.COM");
$stmt = ociparse($c1,"select sec_orden.nextval  from dual");
ociexecute($stmt,OCI_DEFAULT);
while (ocifetch($stmt)){
$id_orden= ociresult($stmt,"NEXTVAL");
}
//GRABAR DETALLE DE ORDEN DEL CARRO DE COMPRAS

$ind = 0;
$max=$_SESSION["contador"];
while($ind<$max){
if ($_SESSION["carro_estado[$ind]"]=="I"){
 $subtotal = $_SESSION["carro_cantidad[$ind]"]*
$_SESSION["carro_precio[$ind]"];
 $acumula_total = $acumula_total + $subtotal;
 $imagen = $_SESSION["carro_codigo[$ind]"];
```

```
 $car_cantidad = $_SESSION["carro_cantidad[$ind]"];
 $car_precio = $_SESSION["carro_precio[$ind]"];
 $stmt = ociparse($c1,"select * from detalle_producto
                where dp_imagen = '".$imagen."'");
 ociexecute($stmt);
 while (ocifetch($stmt)){
   $id_producto= ociresult($stmt,"DP_ID");
  }
 $stmt1 = ociparse($c1,"insert into orden_detalle values(:bind1, :bind2,
:bind3, :bind4, :bind5)");
 ocibindbyname($stmt1, ":bind1",$id_orden);
 ocibindbyname($stmt1, ":bind2",$id_producto);
 ocibindbyname($stmt1, ":bind3",$car_cantidad);
 ocibindbyname($stmt1, ":bind4",$car_precio);
 ocibindbyname($stmt1, ":bind5",$subtotal);
 ociexecute($stmt1);
}
$ind++;
}
//GRABAR CABECERA DE ORDEN DE COMPRA
$fecha_sistema = DATE("d-M-Y");
$stmt = ociparse($c1,"insert into orden_compra values(:bind1, :bind2, :bind3,
:bind4, :bind5, :bind6, :bind7, :bind8, :bind9, :bind10, :bind11, :bind12)");
ocibindbyname($stmt, ":bind1",$id_orden);
ocibindbyname($stmt, ":bind2",$fecha_sistema);
ocibindbyname($stmt, ":bind3",$acumula_total);
ocibindbyname($stmt, ":bind4",$id_cliente);
ocibindbyname($stmt, ":bind5",$nombre_destino);
ocibindbyname($stmt, ":bind6",$ciudad_destino);
ocibindbyname($stmt, ":bind7",$sector_destino);
ocibindbyname($stmt, ":bind8",$direc_destino);
ocibindbyname($stmt, ":bind9",$telefono_destino);
ocibindbyname($stmt, ":bind10",$mensaje_destino);
ocibindbyname($stmt, ":bind11",$fecha_destino);
ocibindbyname($stmt, ":bind12",$hora_destino);
ociexecute($stmt);
ocilogoff($stmt);
$_SESSION["id_orden"]=$id_orden;
$_SESSION["total_compra"]=$acumula_total;
header("Location: pagos.php");
exit;
?>
```

1.8 Pago con Tarjeta

Está dividido en dos programas, el pago.php que muestra y valida el formulario de tarjetas y el ingresa_factura_pago.php que realiza la autenticación de la tarjeta y finaliza la transacción de pago, grabando las tablas detalle_factura, factura, pagos y actualizando el maestro de tarjetas con el nuevo saldo y elimina el arreglo de sesión del carro de compras.
Pagos.php()

```
<?php
session_start();
$ind=0;
$id_cliente = $_SESSION["id_cliente"];
$c1 =
ocilogon("dba01","user0103","FLORESDB.CONTODOMIAMOR.COM");

$stmt = ociparse($c1,"select * from
orden_compra,factura,pagos,tipo_tarjetas,maestro_tarjetas
                where oc_id_cliente ='".$id_cliente."' and
                oc_id_orden = fa_id_orden and
                fa_id_factura = pa_id_factura and
                pa_tipo_tarjeta = tt_id and
                pa_nro_tarjeta = mt_bin");
ociexecute($stmt);
$contador = 0;
while (ocifetch($stmt)){
$nro_tarjeta = ociresult($stmt,"PA_NRO_TARJETA");
$tipo_tarjeta = ociresult($stmt,"PA_TIPO_TARJETA");
$propietario = ociresult($stmt,"MT_CARD_HOLDER");
$mes = ociresult($stmt,"MT_MES_EXPIRACION");
$anio = ociresult($stmt,"MT_ANIO_EXPIRACION");
$direccion = ociresult($stmt,"MT_BILING_ADDRESS");
}
ocilogoff($stmt);
?>
<HTML>
<HEAD><TITLE>Ingreso de datos de clientes</TITLE></HEAD>

<BODY background="../IMAGENES/fondo1.jpg">
 <FORM NAME='frm' method = 'post' ACTION='ingresa_factura_pago.php'>
 <p><font color="#BB3D00" size="4" face=Verdana><strong>Pago mediante
tarjeta de crédito</strong></p><br><img src =
'../IMAGENES/tarjetas.jpg'><hr>
```

```
<TABLE BORDER=0>
<TR>
 <TD><font color="#BB3D00" size="2" face=Verdana>Tipo de Tarjeta:</TD>
 <TD><select name='tarjetas'>
      <?if ($tipo_tarjeta==null){?>
      <OPTION VALUE='0' selected> - X - </OPTION>
      <OPTION VALUE='1'>Visa</OPTION>
      <OPTION VALUE='2'>Diners</OPTION>
      <OPTION VALUE='3'>Mastercard</OPTION>
      <?}?>
      <? if ($tipo_tarjeta==1){?>
      <OPTION VALUE='0'> - X - </OPTION>
      <OPTION VALUE='1' selected>Visa</OPTION>
      <OPTION VALUE='2'>Diners</OPTION>
      <OPTION VALUE='3'>Mastercard</OPTION>
      <?}?>
      <?if ($tipo_tarjeta==2){?>
      <OPTION VALUE='0' > - X - </OPTION>
      <OPTION VALUE='1'>Visa</OPTION>
      <OPTION VALUE='2' selected>Diners</OPTION>
      <OPTION VALUE='3'>Mastercard</OPTION>
      <?}?>
      <?if ($tipo_tarjeta==3){?>
      <OPTION VALUE='0' > - X - </OPTION>
      <OPTION VALUE='1'>Visa</OPTION>
      <OPTION VALUE='2'>Diners</OPTION>
      <OPTION VALUE='3' selected>Mastercard</OPTION>
      <?}?>
 </select></TD>
</TR>
<TR>
 <TD><font color="#BB3D00" size="2" face=Verdana>Número de
Tarjeta:</TD>
 <TD><INPUT TYPE='text' NAME='numero_tc' VALUE='<?echo
$nro_tarjeta;?>' SIZE=14 MAXLENGTH=14></td>
</TR>
<TR>
 <TD><font color="#BB3D00" size="2" face=Verdana>Propietario:</TD>
 <td><INPUT TYPE='text' NAME='cardholder' VALUE='<?echo
$propietario;?>' SIZE=40 MAXLENGTH=40></td>
</TR>
<TR>
 <TD><font color="#BB3D00" size="2" face=Verdana>Fecha de
expiración:</TD>
```

```
<TD><select name='mes_expira'>
      <?if ($mes==null){?>
      <OPTION VALUE="0" selected>- X -</OPTION>
      <OPTION VALUE="01">Enero</OPTION>
      <OPTION VALUE="02">Febrero</OPTION>
      <OPTION VALUE="03">Marzo</OPTION>
      <OPTION VALUE="04">Abril</OPTION>
      <OPTION VALUE="05">Mayo</OPTION>
      <OPTION VALUE="06">Junio</OPTION>
      <OPTION VALUE="07">Julio</OPTION>
      <OPTION VALUE="08">Agosto</OPTION>
      <OPTION VALUE="09">Septiembre</OPTION>
      <OPTION VALUE="10">Octubre</OPTION>
      <OPTION VALUE="11">Noviembre</OPTION>
      <OPTION VALUE="12">Diciembre</OPTION>
      <?}?>
      <?if ($mes=="01"){?>
      <OPTION VALUE="0" >- X -</OPTION>
      <OPTION VALUE="01" selected>Enero</OPTION>
      <OPTION VALUE="02">Febrero</OPTION>
      <OPTION VALUE="03">Marzo</OPTION>
      <OPTION VALUE="04">Abril</OPTION>
      <OPTION VALUE="05">Mayo</OPTION>
      <OPTION VALUE="06">Junio</OPTION>
      <OPTION VALUE="07">Julio</OPTION>
      <OPTION VALUE="08">Agosto</OPTION>
      <OPTION VALUE="09">Septiembre</OPTION>
      <OPTION VALUE="10">Octubre</OPTION>
      <OPTION VALUE="11">Noviembre</OPTION>
      <OPTION VALUE="12">Diciembre</OPTION>
      <?}?>
      <?if ($mes=="02"){?>
      <OPTION VALUE="0" >- X -</OPTION>
      <OPTION VALUE="01">Enero</OPTION>
      <OPTION VALUE="02" selected>Febrero</OPTION>
      <OPTION VALUE="03">Marzo</OPTION>
      <OPTION VALUE="04">Abril</OPTION>
      <OPTION VALUE="05">Mayo</OPTION>
      <OPTION VALUE="06">Junio</OPTION>
      <OPTION VALUE="07">Julio</OPTION>
      <OPTION VALUE="08">Agosto</OPTION>
      <OPTION VALUE="09">Septiembre</OPTION>
      <OPTION VALUE="10">Octubre</OPTION>
      <OPTION VALUE="11">Noviembre</OPTION>
```

```
        <OPTION VALUE="12">Diciembre</OPTION>
        <?}?>
        <?if ($mes=="03"){?>
        <OPTION VALUE="0" >- X -</OPTION>
        <OPTION VALUE="01">Enero</OPTION>
        <OPTION VALUE="02">Febrero</OPTION>
        <OPTION VALUE="03" selected>Marzo</OPTION>
        <OPTION VALUE="04">Abril</OPTION>
        <OPTION VALUE="05">Mayo</OPTION>
        <OPTION VALUE="06">Junio</OPTION>
        <OPTION VALUE="07">Julio</OPTION>
        <OPTION VALUE="08">Agosto</OPTION>
        <OPTION VALUE="09">Septiembre</OPTION>
        <OPTION VALUE="10">Octubre</OPTION>
        <OPTION VALUE="11">Noviembre</OPTION>
        <OPTION VALUE="12">Diciembre</OPTION>
        <?}?>
        <?if ($mes=="04"){?>
        <OPTION VALUE="0" >- X -</OPTION>
        <OPTION VALUE="01">Enero</OPTION>
        <OPTION VALUE="02">Febrero</OPTION>
        <OPTION VALUE="03">Marzo</OPTION>
        <OPTION VALUE="04" selected>Abril</OPTION>
        <OPTION VALUE="05">Mayo</OPTION>
        <OPTION VALUE="06">Junio</OPTION>
        <OPTION VALUE="07">Julio</OPTION>
        <OPTION VALUE="08">Agosto</OPTION>
        <OPTION VALUE="09">Septiembre</OPTION>
        <OPTION VALUE="10">Octubre</OPTION>
        <OPTION VALUE="11">Noviembre</OPTION>
        <OPTION VALUE="12">Diciembre</OPTION>
        <?}?>
        <?if ($mes=="05"){?>
        <OPTION VALUE="0" >- X -</OPTION>
        <OPTION VALUE="01">Enero</OPTION>
        <OPTION VALUE="02">Febrero</OPTION>
        <OPTION VALUE="03">Marzo</OPTION>
        <OPTION VALUE="04">Abril</OPTION>
        <OPTION VALUE="05" selected>Mayo</OPTION>
        <OPTION VALUE="06">Junio</OPTION>
        <OPTION VALUE="07">Julio</OPTION>
        <OPTION VALUE="08">Agosto</OPTION>
        <OPTION VALUE="09">Septiembre</OPTION>
        <OPTION VALUE="10">Octubre</OPTION>
```

```
<OPTION VALUE="11">Noviembre</OPTION>
<OPTION VALUE="12">Diciembre</OPTION>
<?}?>
<?if ($mes=="06"){?>
<OPTION VALUE="0" >- X -</OPTION>
<OPTION VALUE="01">Enero</OPTION>
<OPTION VALUE="02">Febrero</OPTION>
<OPTION VALUE="03">Marzo</OPTION>
<OPTION VALUE="04">Abril</OPTION>
<OPTION VALUE="05">Mayo</OPTION>
<OPTION VALUE="06" selected>Junio</OPTION>
<OPTION VALUE="07">Julio</OPTION>
<OPTION VALUE="08">Agosto</OPTION>
<OPTION VALUE="09">Septiembre</OPTION>
<OPTION VALUE="10">Octubre</OPTION>
<OPTION VALUE="11">Noviembre</OPTION>
<OPTION VALUE="12">Diciembre</OPTION>
<?}?>
<?if ($mes=="07"){?>
<OPTION VALUE="0" >- X -</OPTION>
<OPTION VALUE="01">Enero</OPTION>
<OPTION VALUE="02">Febrero</OPTION>
<OPTION VALUE="03">Marzo</OPTION>
<OPTION VALUE="04">Abril</OPTION>
<OPTION VALUE="05">Mayo</OPTION>
<OPTION VALUE="06">Junio</OPTION>
<OPTION VALUE="07" selected>Julio</OPTION>
<OPTION VALUE="08">Agosto</OPTION>
<OPTION VALUE="09">Septiembre</OPTION>
<OPTION VALUE="10">Octubre</OPTION>
<OPTION VALUE="11">Noviembre</OPTION>
<OPTION VALUE="12">Diciembre</OPTION>
<?}?>
<?if ($mes=="08"){?>
<OPTION VALUE="0" >- X -</OPTION>
<OPTION VALUE="01">Enero</OPTION>
<OPTION VALUE="02">Febrero</OPTION>
<OPTION VALUE="03">Marzo</OPTION>
<OPTION VALUE="04">Abril</OPTION>
<OPTION VALUE="05">Mayo</OPTION>
<OPTION VALUE="06">Junio</OPTION>
<OPTION VALUE="07">Julio</OPTION>
<OPTION VALUE="08" selected>Agosto</OPTION>
<OPTION VALUE="09">Septiembre</OPTION>
```

```
        <OPTION VALUE="10">Octubre</OPTION>
        <OPTION VALUE="11">Noviembre</OPTION>
        <OPTION VALUE="12">Diciembre</OPTION>
        <?}?>
        <?if ($mes=="09"){?>
        <OPTION VALUE="0" >- X -</OPTION>
        <OPTION VALUE="01">Enero</OPTION>
        <OPTION VALUE="02">Febrero</OPTION>
        <OPTION VALUE="03">Marzo</OPTION>
        <OPTION VALUE="04">Abril</OPTION>
        <OPTION VALUE="05">Mayo</OPTION>
        <OPTION VALUE="06">Junio</OPTION>
        <OPTION VALUE="07">Julio</OPTION>
        <OPTION VALUE="08">Agosto</OPTION>
        <OPTION VALUE="09" selected>Septiembre</OPTION>
        <OPTION VALUE="10">Octubre</OPTION>
        <OPTION VALUE="11">Noviembre</OPTION>
        <OPTION VALUE="12">Diciembre</OPTION>
        <?}?>
        <?if ($mes=="10"){?>
        <OPTION VALUE="0" >- X -</OPTION>
        <OPTION VALUE="01">Enero</OPTION>
        <OPTION VALUE="02">Febrero</OPTION>
        <OPTION VALUE="03">Marzo</OPTION>
        <OPTION VALUE="04">Abril</OPTION>
        <OPTION VALUE="05">Mayo</OPTION>
        <OPTION VALUE="06">Junio</OPTION>
        <OPTION VALUE="07">Julio</OPTION>
        <OPTION VALUE="08">Agosto</OPTION>
        <OPTION VALUE="09">Septiembre</OPTION>
        <OPTION VALUE="10" selected>Octubre</OPTION>
        <OPTION VALUE="11">Noviembre</OPTION>
        <OPTION VALUE="12">Diciembre</OPTION>
        <?}?>
        <?if ($mes=="11"){?>
        <OPTION VALUE="0" >- X -</OPTION>
        <OPTION VALUE="01">Enero</OPTION>
        <OPTION VALUE="02">Febrero</OPTION>
        <OPTION VALUE="03">Marzo</OPTION>
        <OPTION VALUE="04">Abril</OPTION>
        <OPTION VALUE="05">Mayo</OPTION>
        <OPTION VALUE="06">Junio</OPTION>
        <OPTION VALUE="07">Julio</OPTION>
        <OPTION VALUE="08">Agosto</OPTION>
```

```
        <OPTION  VALUE="09">Septiembre</OPTION>
        <OPTION  VALUE="10">Octubre</OPTION>
        <OPTION  VALUE="11" selected>Noviembre</OPTION>
        <OPTION  VALUE="12">Diciembre</OPTION>
        <?}?>
        <?if ($mes=="12"){?>
        <OPTION  VALUE="0" >- X -</OPTION>
        <OPTION  VALUE="01">Enero</OPTION>
        <OPTION  VALUE="02">Febrero</OPTION>
        <OPTION  VALUE="03">Marzo</OPTION>
        <OPTION  VALUE="04">Abril</OPTION>
        <OPTION  VALUE="05">Mayo</OPTION>
        <OPTION  VALUE="06">Junio</OPTION>
        <OPTION  VALUE="07">Julio</OPTION>
        <OPTION  VALUE="08">Agosto</OPTION>
        <OPTION  VALUE="09">Septiembre</OPTION>
        <OPTION  VALUE="10">Octubre</OPTION>
        <OPTION  VALUE="11">Noviembre</OPTION>
        <OPTION  VALUE="12" selected>Diciembre</OPTION>
        <?}?>
</select>
<select name='anio_expira'>
        <?if ($anio==null){?>
       <OPTION  VALUE="0" selected>- X -</OPTION>
         <option value="2004"  >2004</option>
       <option value="2005">2005</option>
       <option value="2006">2006</option>
         <option value="2007">2007</option>
         <option value="2008">2008</option>
         <option value="2009">2009</option>
         <option value="2010">2010</option>
         <option value="2011">2011</option>
        <?}?>
        <?if ($anio=="2004"){?>
         <option value="2004"  selected>2004</option>
       <option value="2005">2005</option>
       <option value="2006">2006</option>
         <option value="2007">2007</option>
         <option value="2008">2008</option>
         <option value="2009">2009</option>
         <option value="2010">2010</option>
         <option value="2011">2011</option>
        <?}?>
        <?if ($anio=="2005"){?>
```

```
  <option value="2004" >2004</option>
<option value="2005" selected>2005</option>
<option value="2006">2006</option>
  <option value="2007">2007</option>
  <option value="2008">2008</option>
  <option value="2009">2009</option>
  <option value="2010">2010</option>
  <option value="2011">2011</option>
 <?}?>
 <?if ($anio=="2006"){?>
  <option value="2004" >2004</option>
<option value="2005">2005</option>
<option value="2006" selected>2006</option>
  <option value="2007">2007</option>
  <option value="2008">2008</option>
  <option value="2009">2009</option>
  <option value="2010">2010</option>
  <option value="2011">2011</option>
 <?}?>
 <?if ($anio=="2007"){?>
  <option value="2004" >2004</option>
<option value="2005">2005</option>
<option value="2006">2006</option>
  <option value="2007" selected>2007</option>
  <option value="2008">2008</option>
  <option value="2009">2009</option>
  <option value="2010">2010</option>
  <option value="2011">2011</option>
 <?}?>
 <?if ($anio=="2008"){?>
  <option value="2004" >2004</option>
<option value="2005">2005</option>
<option value="2006">2006</option>
  <option value="2007">2007</option>
  <option value="2008" selected>2008</option>
  <option value="2009">2009</option>
  <option value="2010">2010</option>
  <option value="2011">2011</option>
 <?}?>
 <?if ($anio=="2009"){?>
  <option value="2004" >2004</option>
<option value="2005">2005</option>
<option value="2006">2006</option>
  <option value="2007">2007</option>
```

```
          <option value="2008">2008</option>
          <option value="2009" selected>2009</option>
          <option value="2010">2010</option>
          <option value="2011">2011</option>
        <?}?>
        <?if ($anio=="2010"){?>
          <option value="2004" >2004</option>
        <option value="2005">2005</option>
        <option value="2006">2006</option>
          <option value="2007">2007</option>
          <option value="2008">2008</option>
          <option value="2009">2009</option>
          <option value="2010" selected>2010</option>
          <option value="2011">2011</option>
        <?}?>
        <?if ($anio=="2011"){?>
          <option value="2004" >2004</option>
        <option value="2005">2005</option>
        <option value="2006">2006</option>
          <option value="2007">2007</option>
          <option value="2008">2008</option>
          <option value="2009">2009</option>
          <option value="2010">2010</option>
          <option value="2011" selected>2011</option>
        <?}?>
    </select></td>
          </tr>
 <TR>
  <TD><font color="#BB3D00" size="2" face=Verdana>Dirección:</TD>
  <TD><input type="text"  name="direccion" value='<?echo  $direccion;?>'
SIZE=40 MAXLENGTH=100 ></TD>
 </TR>
 <TR>
  <TD><font color="#BB3D00" size="2" face=Verdana>CVV2:</TD>
  <TD><INPUT  TYPE='password'  NAME='cvv2'  SIZE=10 MAXLENGTH=10
></TD>
 </TR>
 <TR>
  <TD><font color="#BB3D00" size="2" face=Verdana>Frase secreta:</TD>
  <TD><input type='password'  name="frase"  size=30></textarea></TD>
 </TR>
<tr>
<td><input  type = image src='../BOTONES/ContinuarCompra.jpg'   width='129'
height='30'   name = 'sub'></td>
```

```
<td><a href='../index.htm'><img  src='../BOTONES/cancelar.gif'  width='129'
height='30' border='0'></a></td>
</tr>
 </TABLE>
</FORM>
</BODY>
</HTML>
```

ingresa_factura_pago.php()

```
<?php session_start(); ?>
<html>
<head>
<title>Resultados  de Busqueda</title>
</head>
<body>
<?php
$tarjeta = $_POST['tarjetas'];
$nro_tarjeta  = $_POST['numero_tc'];
$cardholder = $_POST['cardholder'];
$mes_expira = $_POST['mes_expira'];
$anio_expira = $_POST['anio_expira'];
$direccion  = $_POST['direccion'];
$cvv2 = $_POST['cvv2'];
$frase  = $_POST['frase'];
$id_orden = $_SESSION['id_orden'];
$compra_subtotal = $_SESSION['total_compra'];
$iva_subtotal = $compra_subtotal * 0.12;
$compra_final = $compra_subtotal + $iva_subtotal;
$fecha_hoy = DATE("d-M-Y");
$valor_descuento  = 0;
$recargos = 0;
$falla = 0;

/* VERIFICAR DATOS DE LA TARJETA */
$c1 =
ocilogon("dba01","user0103","FLORESDB.CONTODOMIAMOR.COM");

$stmt = ociparse($c1,"select * from maestro_tarjetas,tipo_tarjetas
                where mt_bin ='".$nro_tarjeta."' and
                mt_tipo_tarjeta =".$tarjeta." and
                mt_mes_expiracion ='".$mes_expira."' and
```

```
                mt_anio_expiracion ='".$anio_expira."' and
                mt_cvv2 ='".$cvv2."' and
                mt_biling_address ='".$direccion."' and
                mt_card_holder ='".$cardholder."' and
                mt_frase ='".$frase."' and
                mt_estado = 'A' and
                mt_tipo_tarjeta = tt_id");
ociexecute($stmt);
$contador = 0;
while (ocifetch($stmt)){
$saldo_tarjeta = ociresult($stmt,"MT_CUPO_DIRECTO");
$cedula = ociresult($stmt,"MT_CEDULA_PASAPORTE");
$telefono = ociresult($stmt,"MT_TELEFONO");
$desc_tarjeta = ociresult($stmt,"TT_DESCRIPCION");
$contador = $contador + 1;
}
if ($contador == 0)
{
  //echo "TARJETA DE CREDITO CON DATOS INVALIDOS O NO ACTIVA";
  ocilogoff($stmt);
  $falla = 1;
  //AQUI VA UN ECHO DICIENDO QUE LA TARJETA DE CREDITO CON
DATOS INVALIDOS O NO ACTIVA
echo "<table width='400' border='0' align='center' cellpadding='0'
cellspacing='1' bgcolor='#999999'>
          <tr>
          <td><table width='400' border='0' align='center' cellpadding='10'
cellspacing='1' bgcolor='#FFFFFF'>
            <tr>
          <td width='126'><img src='../BOTONES/warning.gif' width='128'
height='137'></td>
          <td width='400'>
<table width='90%' border='0' cellspacing='6' cellpadding='0' >
    <tr>
    <td align='middle'><font color='#BB3D00' face=Verdana><strong>Los
datos ingresados no son correctos o su tarjeta no est&aacute
activa.</strong></td>
    </tr>
    <tr>
    <td>
    <table width='400' border='0' cellspacing='8' cellpadding='0'>
    <tr>
```

```
    <td width='400' align='middle'><p><font color='#BB3D00'
face=Verdana><strong>Por favor verifique los datos
ingresados</strong></p>
    <p><font face=Verdana><a href='../PAGINAS/pagos.htm'>Haga
“click”para corregir los datos</p>
    </td>
    </tr>
   </table></td>
   </tr>
   </table>
   </td>
   </tr>
   </table></td>
   </tr>
   </table>";
}
else
 { //TARJETA DE CREDITO VALIDA
  if ($compra_final > $saldo_tarjeta){
   ocilogoff($stmt);
   $falla = 1;
   //AQUI VA UN ECHO DICIENDO QUE LA TARJETA DE CREDITO ESTA
CON SALDOS INSUFICIENTES
echo "<table width='400' border='0' align='center'
cellpadding='0'cellspacing='1' bgcolor='#999999'>
         <tr>
         <td><table width='400' border='0' align='center' cellpadding='10'
cellspacing='1' bgcolor='#FFFFFF'>
           <tr>
         <td width='126'><img src='../BOTONES/warning.gif' width='128'
height='137'></td>
         <td width='400'>
<table width='90%' border='0' cellspacing='6' cellpadding='0' >
    <tr>
    <td align='middle'><font color='#BB3D00'
face=Verdana>Advertencia:</td>
    </tr>
    <tr>
    <td>
    <table width='400' border='0' cellspacing='8' cellpadding='0'>
    <tr>
    <td width='400' align='middle'><p><font color='#BB3D00'
face=Verdana>Su tarjeta tiene saldos insuficientes para completar su
transacci&oacuten.</p>
```

```
    <p><font face=Verdana><a href='../PAGINAS/pagos.htm'>Haga
“click”para seleccionar otra tarjeta</p>
    </td>
    </tr>
   </table></td>
   </tr>
   </table>
   </td>
   </tr>
   </table></td>
   </tr>
   </table>";
   }
  else
   /* EMPIEZA LA TRANSACCION DE PAGO */
   {
    $stmt1 = ociparse($c1,"select sec_factura.nextval  from dual");
    ociexecute($stmt1,OCI_DEFAULT);
    while (ocifetch($stmt1)){
    $id_factura= ociresult($stmt1,"NEXTVAL");
    }
    $ind = 0;
    $max=$_SESSION["contador"];

    while($ind<$max){
    if ($_SESSION["carro_estado[$ind]"]=="I"){
     $carro_codigo = $_SESSION["carro_codigo[$ind]"];
     $stmt2 = ociparse($c1,"select * from detalle_producto
                where dp_imagen ='".$carro_codigo."'");
     ociexecute($stmt2,OCI_DEFAULT);
     while (ocifetch($stmt2)){
       $id_producto= ociresult($stmt2,"DP_ID");
      }
     $car_cantidad = $_SESSION["carro_cantidad[$ind]"];
     $car_precio  = $_SESSION["carro_precio[$ind]"];
     $stmt3 = ociparse($c1,"insert into detalle_factura values(:bind1, :bind2,
:bind3, :bind4, :bind5)");
     ocibindbyname($stmt3, ":bind1",$id_factura);
     ocibindbyname($stmt3, ":bind2",$id_producto);
     ocibindbyname($stmt3, ":bind3",$car_cantidad);
     ocibindbyname($stmt3, ":bind4",$car_precio);
     ocibindbyname($stmt3, ":bind5",$valor_descuento);
     ociexecute($stmt3);
      } //DEL IF DE SOLO ARTICULOS CON ESTADO I
```

```
    $ind++;
    } //DEL WHILE DE TODOS LOS ARTICULOS
     //ociexecute($stmt3);

     //GRABAR CABECERA DE FACTURA



    $stmt4 = ociparse($c1,"insert into factura values(:bind1, :bind2, :bind3,
:bind4, :bind5, :bind6, :bind7, :bind8, :bind9, :bind10, :bind11)");
    ocibindbyname($stmt4, ":bind1",$id_factura);
    ocibindbyname($stmt4, ":bind2",$id_orden);
    ocibindbyname($stmt4, ":bind3",$compra_subtotal);
    ocibindbyname($stmt4, ":bind4",$iva_subtotal);
    ocibindbyname($stmt4, ":bind5",$valor_descuento);
    ocibindbyname($stmt4, ":bind6",$recargos);
    ocibindbyname($stmt4, ":bind7",$compra_final);
    ocibindbyname($stmt4, ":bind8",$cardholder);
    ocibindbyname($stmt4, ":bind9",$cedula);
    ocibindbyname($stmt4, ":bind10",$direccion);
    ocibindbyname($stmt4, ":bind11",$telefono);
    ociexecute($stmt4);


    $stmt5 = ociparse($c1,"select sec_pago.nextval from dual");
    ociexecute($stmt5,OCI_DEFAULT);
    while (ocifetch($stmt5)){
    $id_pago= ociresult($stmt5,"NEXTVAL");
    }

    $stmt6 = ociparse($c1,"insert into pagos values(:bind1, :bind2, :bind3,
:bind4, :bind5, :bind6)");
    ocibindbyname($stmt6, ":bind1",$id_pago);
    ocibindbyname($stmt6, ":bind2",$id_factura);
    ocibindbyname($stmt6, ":bind3",$fecha_hoy);
    ocibindbyname($stmt6, ":bind4",$compra_final);
    ocibindbyname($stmt6, ":bind5",$tarjeta);
    ocibindbyname($stmt6, ":bind6",$nro_tarjeta);
    ociexecute($stmt6);

    $afecta_saldo = $saldo_tarjeta - $compra_final;

    $stmt7 = ociparse($c1,"update maestro_tarjetas set
                mt_cupo_directo = ".$afecta_saldo."
```

```
                where mt_bin ='".$nro_tarjeta."' and
                mt_tipo_tarjeta =".$tarjeta);

   ociexecute($stmt7);

   ocilogoff($stmt);
  } // del else de EMPIEZA LA TRANSACCION DE PAGO
} // del else de TARJETA DE CREDITO VALIDA
?>
<?php
if ($falla == 0){
//FORMULARIO DE INFORMACION FINAL DEL PAGO

echo "<table width='400' border='0' align='center'
cellpadding='0'cellspacing='1' bgcolor='#999999'>
        <tr>
        <td><table width='400' border='0' align='center' cellpadding='10'
cellspacing='1' bgcolor='#FFFFFF'>
          <tr>
        <td width='126'><img src='../BOTONES/success.gif' width='128'
height='137'></td>
        <td width='200'>
    <table width='90%' border='0' cellspacing='6' cellpadding='0' >
    <tr><td align='middle'><font size='2' color='#BB3D00' face=Verdana>Su
pago se ha realizado con &eacutexito.</td></tr>
    <tr>
    <td>
    <table width='400' border='0' cellspacing='8' cellpadding='0'>
    <tr>
    <td width='400' align='middle'><font size='2' color='#BB3D00'
face=Verdana><p>A continuaci&oacuten encontrar&aacute el detalle de su
factura, este detalle
    se adjuntar&aacute en su estado de cuenta respectivo.</p></td>
    </tr>
   </table></td></tr></table>
   </td></tr></table></td>
   </tr></table>";
//Tabla de Cabecera de Factura
$compra_subtotal= number_format($compra_subtotal,2,'.',',');
$iva_subtotal= number_format($iva_subtotal,2,'.',',');
$compra_final= number_format($compra_final,2,'.',',');
 echo "<br>
<table width='550' border='0' align='center' cellpadding='0'cellspacing='1'
bgcolor='#999999'>
```

```
        <tr>
        <td><table width='550' border='0' align='center' cellpadding='10'
cellspacing='1' bgcolor='#FFFFFF'>
          <tr>
    <td align='middle'><font color='#BB3D00' size='4'
face=Verdana>Resumen de Factura</td></tr>
    <tr>
    <td>
    <table width='550' border='0' cellspacing='8' cellpadding='0'>
    <tr><td width='200' align='left'><font size='2'
face=Verdana><strong>Factura No.</strong></td><td><font size='2'
face=Verdana>".$id_factura."</td></tr>
    <tr><td width='200' align='left'><font size='2'
face=Verdana><strong>Nombre</strong></td><td><font size='2'
face=Verdana>".$cardholder."</td></tr>
    <tr><td width='200' align='left'><font size='2'
face=Verdana><strong>Cédula-Ruc No.</strong></td><td><font size='2'
face=Verdana>".$cedula."</td></tr>
    <tr><td width='200' align='left'><font size='2'
face=Verdana><strong>Tarjeta de Crédito</strong></td><td><font size='2'
face=Verdana>".$desc_tarjeta."</td></tr>
    <tr><td width='200' align='left'><font size='2'
face=Verdana><strong>Tarjeta No.</strong></td><td><font size='2'
face=Verdana>".$nro_tarjeta."</td></tr>
    <tr><td width='200' align='left'><font size='2'
face=Verdana><strong>Subtotal de Compra</strong></td><td><font size='2'
face=Verdana>$ ".$compra_subtotal."</td></tr>
            <tr><td width='200' align='left'><font size='2'
face=Verdana><strong>Iva 12%</strong></td><td><font size='2'
face=Verdana>$ ".$iva_subtotal."</td></tr>
    <tr><td width='200' align='left'><font size='2'
face=Verdana><strong>TOTAL</strong></td><td><font size='2'
face=Verdana>$ ".$compra_final."</td></r>
   </table></td></tr>
   </td></tr></td>
   </tr></table></table>";

//Tabla del detalle de Factura
echo "<BR>
   <p align='center'><font color='#BB3D00' size='4' face=Verdana>Detalle de
Artículos</p>
<table border='1'>
<table align ='center' border='6' width = '550' cellpadding='0' cellspacing='1'>
      <tr>
```

```
      <td width='400' align='middle'><font  face=Verdana
color='#BB3D00'>Producto</td>
      <td width='75' align='middle'><font  face=Verdana
color='#BB3D00'>Cantidad</td>
      <td width='75' align='middle'><font  face=Verdana
color='#BB3D00'>Subtotal</td>
      </tr>";
     $stmt8 = ociparse($c1,"select * from detalle_factura
                where df_id_factura =".$id_factura);
     ociexecute($stmt8,OCI_DEFAULT);
     while (ocifetch($stmt8)){
          $tempo_id_producto= ociresult($stmt8,"DF_ID_PRODUCTO");
          $tempo_cantidad= ociresult($stmt8,"DF_CANTIDAD");
          $tempo_precio=
number_format(ociresult($stmt8,"DF_PRECIO_UNITARIO"),2,'.',',');
          $stmt9 = ociparse($c1,"select * from detalle_producto
          where dp_id = ".$tempo_id_producto);
          ociexecute($stmt9,OCI_DEFAULT);
          while (ocifetch($stmt9)){
                $tempo_detalle_producto=
ociresult($stmt9,"DP_DESCRIPCION");
          }
      echo "<tr>
      <td width='400' align='middle'>".$tempo_detalle_producto."</td>
      <td width='100' align='middle'>".$tempo_cantidad."</td>
      <td width='100' align='middle'>$ ".$tempo_precio."</td>
      </tr>";
      }

echo "</table></table>";
// BORRAR ELEMENTOS DEL CARRO YA COMPRADOS
$max=$_SESSION["contador"];
$ind=0;
while($ind<$max){
     $_SESSION["carro_estado[$ind]"] = "E";
   $ind++;
 }
}
?>
</BODY>
</HTML>
```

BIBLIOGRAFÍA

- "Network Security Essentials Aplication and Standars" - William Stallings –1999 Editorial: Prentice Hall
- E-trust Intrusion Detection - Manual de Referencia- Compùters Associates
- Tanenbaum Andrew (1997). Redes de Computadoras. México:Prentice Hall
- Check Point Software Technologies Ltd (2001). Getting Started Guide.
- Redwood City: Check Point Software Technologies Ltd.
- Cisco Systems (2000). Cisco Certified Network Associate Curriculum
- Océano (1997). Diccionario Enciclopédico Océano uno Color. España: Litografía Roses S.A.
- "Hackers 2 Secretos y soluciones para la seguridad de redes" – Joel Scambray, Stuart McClure,George Kurtz – 2001 Editorial McGraw-Hill
- Sitios web
    - www.answers.com
    - www.honeynet.org
    - www.cert.org
    - www.cyberpirata.org
    - www.retronet.com.ar
    - www.redhat.com
    - www.insecure.org

- es.wikipedia.org
- es.tldp.org
- www.dtic.ua.es
- www.novell.com/es-es/linux/suse/
- fedora.redhat.com
- microlug.linux.net.uy
- usuarios.lycos.es
- microlug.linux.net.uy