

ESCUELA POLITÉCNICA DEL EJÉRCITO

SEDE LATACUNGA

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

**DISEÑO E IMPLANTACIÓN DE UN SISTEMA CON HERRAMIENTA OPEN
SOURCE PARA EL CONTROL Y ADMINISTRACIÓN DEL ACCESO A LA WEB:
LABORATORIO DE INTERNET DEL INSTITUTO TECNOLÓGICO SUPERIOR
AERONÁUTICO.**

**PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN
SISTEMAS E INFORMÁTICA**

YACHIMBA ESPINOSA MIGUEL ÁNGEL

Latacunga, mayo del 2004

CERTIFICACIÓN

Se certifica que el presente trabajo fue desarrollado por Yachimba Espinosa Miguel Angel, bajo nuestra supervisión.

Ing. Raúl Rosero
DIRECTOR

Ing. Edison Montaluisa
CODIRECTOR

DEDICATORIA

Esta tesis está dedicada a mi esposa Carmita Hidalgo Osorio y a mi hijo Markos Miguel Yachimba Hidalgo por el amor, el esfuerzo que día a día me brindaron, por todo el apoyo moral que siempre me dieron para seguir adelante y sobre todo por el tiempo que les pertenecía y no pude estar junto a ellos.

CONTENIDO

I ESTRATEGIAS PARA LA ADMINISTRACIÓN Y CONTROL DEL ACCESO A LA WEB VIA TCP/IP.

- 1.1 Modelo cliente servidor
- 1.2 Diseño orientado a la comunicación
- 1.3 Introducción a Firewalls
- 1.4 Que es un cortafuegos?
- 1.5 Filtrado de paquetes
- 1.6 Cortafuegos de filtrado de paquetes, ipfw
- 1.7 IPTABLES
- 1.8 Estructura y funcionamiento.
- 1.9 Enmascaramiento.

II ESTUDIO DEL LABORATORIO DE INTERNET DEL INSTITUTO TECNOLÓGICO SUPERIOR AERONAUTICO.

- 2.1 Campo de acción del estudio.
- 2.2 El control para el uso del servicio de Internet
- 2.3 Del registro para los usuarios del servicio de Internet.
- 2.4 Del control del tiempo de uso de Internet.
- 2.5 Del acceso a la web por parte de los usuarios.
- 2.6 El desconocimiento del beneficio económico y eficiencia real del servicio de Internet
- 2.7 Facilidad del servicio de Internet.
- 2.8 Establecimiento de reglas internas y externas para el acceso al servicio de Internet
- 2.9 Establecimiento de los niveles de acceso a la web.

III DISEÑO Y DESARROLLO DEL “SISTEMA DE ADMINISTRACIÓN Y CONTROL DEL ACCESO A LA WEB: LABORATORIO DE INTERNET DEL INSTITUTO TECNOLOGICO SUPERIOR AERONAUTICO”

- 3.1 Gestión del “Sistema Open Source para la administración y control del acceso a la WEB”.
- 3.2 Ciclo de vida del desarrollo del “Sistema de Administración y Control

del Acceso a la WEB”.

3.2.1 El Análisis del ámbito del “Sistema de Administración y Control del Acceso a la WEB”

- 3.2.1.1 Recopilación de información
- 3.2.1.2 Clasificación de la información
- 3.2.1.3 Análisis de la seguridad lógica del sistema
- 3.2.1.4 Especificación de requisitos del sistema

3.2.2 El Diseño y desarrollo del “Sistema de Administración y Control del Acceso a la WEB”

3.2.3 Pruebas del “Sistema de Administración y Control del Acceso a la WEB”

3.2.3.1 Diseño del plan de pruebas

3.3 Documentación del “Sistema de Administración y Control del Acceso a la WEB”

3.3.1 Manual del Administrador del “Sistema de Administración y Control del Acceso a la WEB”

3.3.2 Código Fuente del “Sistema de Administración y Control del Acceso a la WEB”

3.3.3 Plan de pruebas del sistema del “Sistema de Administración y Control del Acceso a la WEB”

IV DESARROLLO DEL PLAN DE CONTINGENCIA

- 4.1 Análisis del Plan de Contingencia
- 4.2 Identificación de los procesos críticos del negocio
- 4.3 Análisis de la Seguridad física:
- 4.4 Desarrollo del Plan de Contingencia
- 4.3 Implantación del Plan de contingencia.

V CONCLUSIONES Y RECOMENDACIONES

5.1.- CONCLUSIONES.....

5.2.- RECOMENDACIONES.....

REFERENCIAS BIBLIOGRÁFICAS Y DE LA WEB.....

ANEXOS.....

DISEÑO E IMPLANTACIÓN DE UN SISTEMA OPEN
SOURCE PARA EL CONTROL Y ADMINISTRACIÓN DEL
ACCESO A LA WEB: LABORATORIO DE INTERNET DEL
INSTITUTO TECNOLOGICO SUPERIOR
AEREONAUTICO.

El negocio del servicio de Internet esta llegando a una nueva era. El concepto de la comunicación por la red informática esta creciendo altamente y el numero de compañías o Instituciones que brindan este servicio esta incrementándose continuamente pero a su vez estas no poseen un software de administración eficaz e de allí la necesidad de administrar estos centros de servicio vía software que ayude en la supervisión técnica, y financiera, que les permita ir verificando la viabilidad de su negocio y de poder ampliarlo.

El Sistema de Administración y Control del Acceso a la Web para el INSTITUTO TECNOLOGICO SUPERIOR AEREONAUTICO, tiene como finalidad fortalecer las políticas existentes en la institución, y que deben ser reformuladas o añadirse nuevas a través de un análisis para lo cual se utilizarán instrumentos y metodologías de investigación:

La razón de realizar el presente sistema a través de la programación Open Source es que al ser cada vez más las empresas que apuestan por software Open Source (Código Abierto), y cada vez son más las que repiten la experiencia después de los buenos resultados que obtienen.

I.- ESTRATEGIAS PARA LA ADMINISTRACIÓN Y CONTROL DEL ACCESO A LA WEB VIA TCP/IP

1.1.- MODELO CLIENTE SERVIDOR

1.1.1.- INTRODUCCIÓN

Uno de los aspectos claves para contar con la capacidad de proponer, promocionar y llevar a cabo el presente sistema, es llegar a conocer la arquitectura del modelo cliente / servidor, los conceptos o ideas asociados al mismo; ya que este modelo es una plataforma abierta por excelencia, lo cual brinda la oportunidad de hacer una gran variedad de combinaciones de clientes y servidores al igualar o nivelar distintas aplicaciones o componentes de distintos proveedores.

Pero esta gran variedad de posibilidades de combinación implica que debemos tener en cuenta también una gran cantidad de elementos a considerar y evaluar al momento de enfrentar una solución informática para la Administración y Control del Acceso a la Web en el Laboratorio de Internet del Instituto Tecnológico Superior Aeronáutico, basada en la arquitectura cliente/servidor.

Podemos agrupar básicamente en dos aspectos la problemática cliente/servidor:

- a) La plataforma a elegir
- b) Las herramientas de desarrollo elegir.

a) La plataforma a elegir

Tiene relación con cuestiones aun más específicas como:

- La plataforma cliente elegir.
- Plataforma servidor
- Clase de middleware
- El administrador o servidor de base de datos
- Arquitectura de computación distribuida se tendrá que montar la solución.

b) Herramientas de desarrollo elegir.

Tiene relación con la toma de decisiones sobre el área de desarrollo y herramientas de cliente/servidor.

La mayor ventaja de esta tecnología es la flexibilidad en cuanto a que podemos elegir entre muchas opciones, esto mismo obliga a tener conocimientos importantes para la integración de las mismas, dado que el desarrollo de aplicaciones cliente/servidor requiere del manejo de elementos en el área de:

- Diseño de bases de datos
- Comunicación entre procesos
- Procesamiento de transacciones
- Generación de GUI (interfaces gráficas de usuarios)
- Servidor distribuido a lo largo de la red.

También las cosas han cambiado en cuanto a las interpretaciones que hasta no hace mucho tiempo se hacían, para unos el mundo de la computación estaba basado en el permanente desarrollo y mejoramiento en las PC, y para otros el verdadero entorno computacional lo conformaban los mainframe; Mantener éstas

posturas no tiene mucho sentido puesto que con cliente/servidor lo único válido, y el único camino, es mezclar o combinar.

Pensando ya en beneficios más específicos, siempre y cuando se adopten las decisiones correctas en cuanto al diseño del Sistema de Administración y Control del Acceso a la Web, esta arquitectura permitirá distribuir físicamente los procesos y los datos en forma más eficiente lo que en computación distribuida afecta directamente el tráfico de la red, reduciéndolo grandemente.

Pero cliente/servidor también tiene sus desventajas, como en la mayoría de las cosas, los mismos elementos que se presentan como potenciales ventajas, se pueden convertir también en los principales escollos en la implantación del Sistema de Administración y Control del Acceso a la Web con esta tecnología.

Las presiones comerciales de los distintos proveedores con objetivos distintos complica el desarrollo del presente sistema; ya que se requieren conocimientos de varias áreas, y que las decisiones tomadas respecto del diseño deben ser las adecuadas, de otra manera resultan más críticas con relación a desarrollos tradicionales, lo que obliga siempre a manejarlos en forma mucho más coherente y a tener un gran dominio de herramientas para lograr una adecuada implantación y explotación del Sistema de Administración y Control del Acceso a la Web.

1.2.- DISEÑO ORIENTADO A LA COMUNICACIÓN

1.2.1.- DEFINICIÓN DE CLIENTE SERVIDOR

La tecnología cliente/servidor es el procesamiento cooperativo de la información por medio de un conjunto de procesadores, en el cual múltiples clientes, distribuidos geográficamente, solicitan requerimientos a uno o más servidores centrales.

Desde el punto de vista funcional, se puede definir la computación cliente/servidor como una arquitectura distribuida que permite a los usuarios finales obtener acceso a la información en forma transparente aun en entornos multiplataforma.

En el modelo cliente servidor, el cliente envía un mensaje solicitando un determinado servicio a un servidor, y este envía uno o varios mensajes con la respuesta como se indica el la figura 01.

En un sistema distribuido cada máquina puede cumplir el rol de servidor para algunas tareas y el rol de cliente para otras es así que para la implantación del Sistema Web Access este cumplirá funciones de servidor al atender las peticiones de los terminales y hará las operaciones de cliente al acceder a la Web.

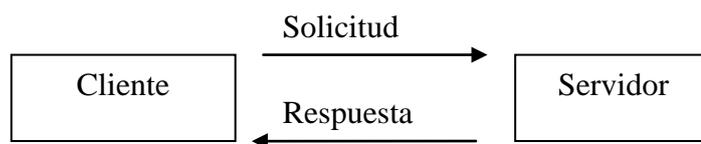


Figura 01 Modelo cliente servidor

La idea es tratar a una computadora como un instrumento, que por sí sola pueda realizar muchas tareas, pero con la consideración de que realice aquellas que son mas adecuadas a sus características.

La forma más estándar de aplicación y uso de sistemas clientes/servidores es mediante la explotación de las PC a través de interfaces gráficas de usuario; mientras que la administración de datos y su seguridad e integridad se deja a cargo de computadoras centrales tipo mainframe.

1.2.2.- CARACTERÍSTICAS QUE CUMPLEN LOS SISTEMAS CLIENTE/SERVIDOR:

- Se establece una relación entre procesos distintos, los cuales pueden ser ejecutados en la misma máquina o en máquinas diferentes distribuidas a lo largo de la red.
- Existe una clara distinción de funciones basada en el concepto de "servicio", que se establece entre clientes y servidores.
- La relación establecida puede ser de muchos a uno, en la que un servidor puede dar servicio a muchos clientes, regulando su acceso a recursos compartidos.
- Los clientes corresponden a procesos activos en cuanto a que son éstos lo que hacen peticiones de servicios a los servidores. Estos últimos tienen un carácter pasivo ya que esperan las peticiones de los clientes.
- No existe otra relación entre clientes y servidores que no sea la que se establece a través del intercambio de mensajes entre ambos. El mensaje es el mecanismo para la petición y entrega de solicitudes de servicio.
- Las plataformas de software y hardware entre clientes y servidores son independientes. Precisamente una de las principales ventajas de esta arquitectura es la posibilidad de conectar clientes y servidores independientemente de sus plataformas
- El concepto de escalabilidad tanto horizontal como vertical es aplicable a cualquier sistema cliente/servidor. La escalabilidad horizontal permite agregar más estaciones de trabajo activas sin afectar significativamente el rendimiento. La escalabilidad vertical permite mejorar las características del servidor o agregar múltiples servidores

1.2.3.- COMPONENTES DEL MODELO CLIENTE/SERVIDOR

Cliente/servidor es un modelo basado en la idea del servicio, en el que el cliente es un proceso consumidor de servicios y el servidor es un proceso proveedor de servicios.

Esta relación está establecida en función del intercambio de mensajes que es el único elemento de acoplamiento entre ambos. De estas líneas se desprenden los tres elementos fundamentales sobre los cuales se desarrollan e implantan los sistemas cliente/servidor:

El proceso cliente que es quien inicia el diálogo, el proceso servidor que pasivamente espera a que lleguen peticiones de servicio y el middleware que corresponde a la interfaz que provee la conectividad entre el cliente y el servidor para poder intercambiar mensajes.

Para entender en forma más ordenada y clara los conceptos y elementos involucrados en esta tecnología se puede aplicar una descomposición o arquitectura de niveles.

Esta descomposición principalmente consiste en los elementos estructurales de esta tecnología en función de aspectos más funcionales de la misma:

- Nivel de Presentación: Agrupa a todos los elementos asociados al componente Cliente.
- Nivel de Aplicación: Agrupa a todos los elementos asociados al componente Servidor.
- Nivel de comunicación: Agrupa a todos los elementos que hacen posible la comunicación entre los componentes Cliente y servidor.
- Nivel de base de datos: Agrupa a todas las actividades asociadas al acceso de los datos.

Este modelo de descomposición en niveles, permite introducir más claramente la discusión del desarrollo de aplicaciones en arquitecturas de hardware y software en planos.

a) Cliente.- El cliente es el proceso que permite al usuario formular los requerimientos y pasarlos al servidor, se lo conoce con el término front-end. Este normalmente maneja todas las funciones relacionadas con la manipulación y

despliegue de datos, por lo que están desarrollados sobre plataformas que permiten construir interfaces gráficas de usuario (GUI), además de acceder a los servicios distribuidos en cualquier parte de la red.

Las funciones que lleva a cabo el proceso cliente se resumen en los siguientes puntos:

- Interactuar con el usuario.
- Procesar la lógica de la aplicación.
- Generar requerimientos de bases de datos.
- Administrar la interfaz de usuario.
- Formatear resultados.
- Recibir resultados del servidor.

b) Servidor.- Es el proceso encargado de atender a múltiples clientes que hacen peticiones de algún recurso administrado por él. Al proceso servidor se lo conoce con el término back-end.

El servidor normalmente maneja todas las funciones relacionadas con la mayoría de las reglas del negocio y los recursos de datos.

Las funciones que lleva a cabo el proceso servidor se resumen en los siguientes puntos:

- Aceptar los requerimientos de bases de datos que hacen los clientes.
- Procesar requerimientos de bases de datos.
- Formatear datos para transmitirlos a los clientes.
- Procesar la lógica de la aplicación y realizar validaciones a nivel de bases de datos.

c) Middleware.- En su definición más simple, middleware es la interfaz que provee la conectividad entre aplicaciones clientes y aplicaciones servidoras, y entre aplicaciones y bases de datos.

Es una capa de software que protege a los desarrolladores de tener que manejar detalles de bajo nivel de diferentes protocolos de comunicación, sistemas operativos y arquitecturas de bases de datos. Este tipo de interfaces incluyen mensajería de red y accesos a bases de datos.

1.2.4.- ELECCIÓN DEL MODELO CLIENTE / SERVIDOR

Del análisis de la relación entre los elementos del modelo cliente servidor se ha definido el tipo de solución que se ajusta de mejor forma a la solución para el Desarrollo e Implantación del Sistema para la Administración y Control del Acceso a la Web con la utilización de Herramientas Open Source,

Los aspectos tomados en cuenta para la elección del modelo son, el tiempo de respuesta de los mensajes, tamaño de la base de datos de los alumnos del Instituto Tecnológico Superior Aeronáutico, y demás clientes del Laboratorio de Internet, distribución geográfica tanto de los procesos como de los datos.

En tal sentido se presenta, el modelo cliente servidor que mejor se ajusta a la presente problemática basado en los distintos tipos de cliente/servidor.

1.2.4.1.- Por tamaño de componentes.

El modelo elegido es el Servidor Grueso y Cliente fino (Fat Server /Thin Client) ya que en este modelo el proceso cliente es restringido a la presentación de la interfaz de usuario (ventanas de elección, información del estado de su cuenta, sesión etc.) mientras que el funcionamiento del Sistema, las reglas del negocio corren en el lado del servidor de aplicaciones (el control del tiempo, validación de usuarios) como se indica en la figura 02.

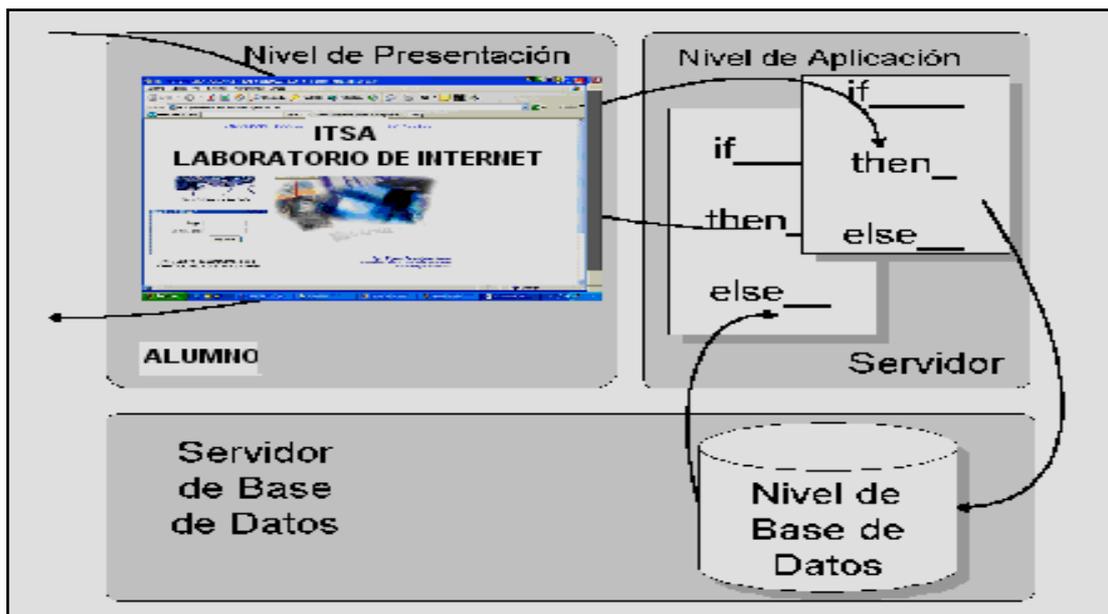


Figura 02 Modelo Servidor Grueso y Cliente fino

1.2.4.2.- Por planos o capas (tier)

De acuerdo a los niveles o planos de aplicación se ha elegido el modelo Cliente/Servidor Tres Planos ya que en este esquema el cliente envía mensajes directamente al servidor del Sistema para la Administración y Control del Acceso a la Web el cual debe administrar y responder todas las solicitudes de acceso echas por los clientes y es el quien dependiendo del tipo de solicitud, quien accede y se conecta con la base de datos para el respectivo permiso al cliente que realizo la solicitud.

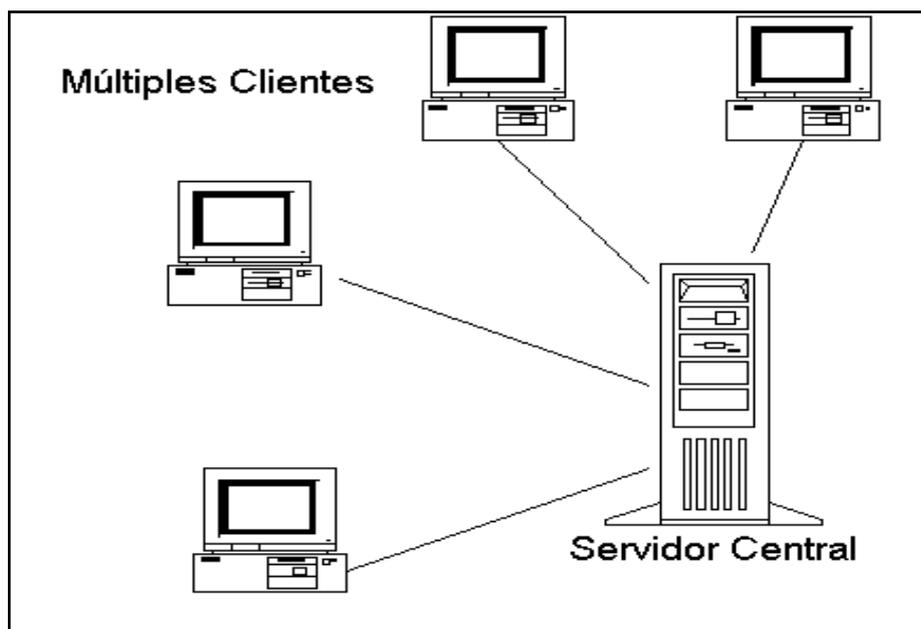


Figura 03 Modelo Cliente - Servidor por Planos

El servidor local tiene un comportamiento dual, dado que actúa como usuario al momento de acceder a la base de datos de los clientes del Laboratorio de Internet, o de servidor al momento de dar solución a las diversas solicitudes echas por las estaciones de trabajo.

1.2.4.3.- Comunicación entre el cliente y el servidor

Cada usuario, que realiza una solicitud, lo hace desde una computadora conectada a la red del Laboratorio de Internet, el sistema operativo puede ser desde, Windows 95 o superior, Linux, Mandrake. Los programas clientes permiten establecer la comunicación y el envío de mensajes hasta el servidor.

Los programas clientes de un terminal, para poder enviar un mensaje a un servidor, deben conectarse primero al Sistema Web Access que se encuentra en el server del Laboratorio de Internet. Que se encargará de entregar la respuesta al cliente correcto.

El ciclo de operación del cliente es el siguiente:

Conexión: el cliente envía un pedido de conexión al Sistema.

Si el Sistema acepta el pedido se crea una vía de comunicación.

Operación: el cliente envía mensajes y/o espera por respuestas a través de esa vía de comunicación. El flujo de mensajes es controlado por el cliente, y este debe ser consistente con la forma que la aplicación server espera los mensajes.

Desconexión: el cliente se desconecta, rompiendo la vía de comunicación, cuando no lo necesita más. Esto ocurre en el momento de cerrar la aplicación

1.2.5.- SERVIDOR DE LA BASE DE DATOS RELACIONAL.

El concepto de bases de datos relacional fue introducido a principios de 1.970 por E.F. Cood. Basado en la teoría matemática de conjuntos, las bases de datos representan los datos en tablas. Las tablas son colecciones de filas que consisten de columnas, (registros y campos en otra terminología).

Las principales funciones del sistema de administración de bases de datos relacional son:

- Representar los datos como un conjunto de tablas.
- Facilitar el diseño, la visión y la modificación de los datos.
- Proveer operaciones relacionales como selección, proyección y unión.
- Proveer el acceso más rápido posible a los datos deseados.
- Asegurar la consistencia de los datos con control de transacciones atómicas.
- Asegurar los datos contra fallas de hardware y software con herramientas de recuperación basadas en bitácoras. (Journaling)
- Integración con lenguajes de programación, usando sentencias de manipulación de datos incluidas directamente en programas fuentes.
- Proveer fácil acceso a bases de datos remotas.
- Proveer un entorno interactivo para escribir y probar consultas a la base de datos.
- Proveer funciones para buscar, ordenar y realizar análisis estadísticos.
- Proveer herramientas de diseño y administración.

- Permite definición de datos en forma dinámica: crear tablas, almacenar datos, consultar, deshacer y reintentar.
- Permite cambios dinámicos a las definiciones de la base de datos; agregar, cambiar o eliminar campos, tablas e índices.
- Proteger los datos de usuarios no autorizados con un sofisticado control de seguridad.

En el modelo de implementación para el sistema Web Access la administración de bases de datos es en MySQL, esta herramienta provee todos los puntos que detallamos en la lista superior, en éste capítulo, veremos los puntos más importantes que se utilizan en el sistema cliente servidor.

1.2.5.1.- Diseño y definición

Para diseñar la base de datos, es necesario seguir determinados pasos:

- Análisis de requerimientos.
- Crear el diseño de la base de datos: Diseño lógico y diseño físico.
- Implementar la aplicación que utiliza la base de datos.
- Revisión y ajuste de la aplicación y la base de datos.
- Mantenimiento de la aplicación y de la base de datos.

El resultado del método de diseño elegido para construir la base de datos relacional de las cuentas de los clientes del laboratorio de Internet, será un conjunto de tablas o relaciones, código para restricciones, código para ejecutar ante determinados eventos, definiciones de áreas de almacenamiento.

1.2.5.1.1.- Diseño lógico.

Para el buen diseño lógico, se debe entender las relaciones existentes entre todos los objetos de la base de datos. En el diseño lógico se representan las entidades, se eliminan atributos redundantes y se produce un esquema con las tablas que representan los datos de forma óptima.

Es importante conocer qué tablas son mas accedidas, por qué usuarios y para qué cada acceso a la base de datos se ha denominar una transacción, entonces

es importante analizar cuales son las transacciones típicas que se realizarán en la base de datos para tenerlas en cuenta en nuestro diseño.

Para el modelo de base de datos relacional del Sistema de Administración y Control del Acceso a la Web, se aplica la normalización de las tablas para reducir la estructura a su forma más simple, remover las columnas redundantes e identificar todos los datos que son dependientes de otros.

Si existe demasiada normalización, tenemos mayor tiempo de acceso a los datos, debido a que se deben unir varias tablas para recuperar la información.

La normalización efectiva consiste de las siguientes tareas:

- Verificar que cada columna de cada tabla muestre un hecho relevante.
- Traer cierta cantidad de redundancia dentro de la tabla para mejorar la performance eliminando la necesidad de uniones que crucen mas de dos o tres tablas para las transacciones más realizadas por la/las aplicaciones.

Se debe contar con la siguiente información acerca de cada transacción:

- Medidas de base para tiempos de respuesta y cantidad de transacciones esperadas.
- Estimación de cantidad de accesos a la base de datos.

El análisis de datos genera la siguiente información:

- Una lista de tablas, columnas e índices.
- Un gráfico de entidad/ relación.

El almacenamiento histórico de la información obsoleta que se va acumulando en la vida de la base de datos por esta razón se ha de mantener siempre un tamaño razonable para la base de datos de los clientes del Laboratorio de Internet del ITSA.

Al desarrollar una adecuada estrategia para almacenar información y eliminarla de la base de datos, asegurará estar dentro de la capacidad de almacenamiento físico que nuestro sistema dispone ya que algunas tablas permanecen constantes mientras que otras tablas crecen sin límite.

1.2.5.1.2.- Diseño físico

La tabla de clientes tiene gran cantidad de datos, siendo la llave primaria el número de cedula del cliente convirtiéndose esta en la tabla principal que tiene los datos personales y algunos datos específicos sobre el cliente.

Las transacciones típicas en el sistema de administración del acceso a la Web acceden por algún número de cedula a las tablas del cliente ubican sus datos en la tabla de clientes. Además la mayoría de las veces que se accede a un cliente, se necesitan sus datos personales.

Teniendo en cuenta esta pequeña descripción, podemos realizar un diseño físico que mejore los tiempos de acceso a este tipo de transacciones.

Para poder realizar este tipo de optimización, se debe estudiar cuidadosamente las características del sistema, el hardware disponible, y el tipo de transacciones que se desea optimizar. Además se deben realizar varios cálculos que nos permitan obtener el mejor tamaño de página adecuado para optimizar los accesos a disco, y el espacio correcto para la asignación inicial de las áreas de almacenamiento.

1.2.6.- VENTAJAS DEL MODELO CLIENTE / SERVIDOR.

Menor costo total de la solución.

El enfoque cliente/servidor es económico, sobre todo cuando está unido al concepto de racionalización ya que se centralizan los procesos.

Acceso a la información.

El acceso a los datos es posible por otros medios, la arquitectura Cliente/Servidor constituye el ambiente ideal para facilitar el acceso a la información. El usuario no sólo puede tener un acceso transparente a toda la información que necesita, sino además está habilitado para procesarla como guste.

Menor costo de comunicaciones (sólo solicitudes y respuestas)

Ergonomía.

Un buen sistema Cliente/Servidor no se concibe sin una interfaz gráfica de usuario y sin una transparencia total. De esta manera, el cliente puede trabajar en el ambiente que más le convenga sin preocuparse de la conversión de interfaces y protocolos. Se concentra en el trabajo que debe realizar más que en la tecnología.

Buena tecnología en el lugar adecuado.

En teoría, un ambiente Cliente/Servidor puede conformarse de varias plataformas, sistemas operativos.

De ahí que haya muchas opciones para cada aplicación; por ejemplo HP con UNIX y con estaciones de trabajo Windows X para un servicio.

Muchos CPU's corriendo aplicaciones en lugar de un solo CPU.

Es posible usar interfaces de usuario mucho mas sofisticadas (gráficas, menús, etc.)

Modularidad.

En un ambiente Cliente/Servidor, es factible agregar o eliminar estaciones de trabajo y servidores, puesto que el sistema puede ser más o menos fácil de volver a configurar.

También es más sencillo implantar una aplicación nueva por medio de construir una extensión con un servidor y estaciones de trabajo nuevos.

1.2.7.- DESVENTAJAS DEL MODELO CLIENTE / SERVIDOR.

Incompatibilidad.

El ambiente Cliente/Servidor supone que la época en que IBM tenía todo el mercado dominado ha concluido. Con el fin de esta etapa, se debe recurrir a varios proveedores. Todos sabemos lo que sucede en estos casos: cuando hay algún problema, el proveedor inicial lo remite a otro proveedor.

Si las especificaciones se ponen por escrito, no hay problema; pero en la práctica cotidiana, las incompatibilidades mayores o menores entre computadoras, sistemas operativos, lenguajes, protocolos, interfaces y programas de aplicación superan las expectativas. Cuanto más elevado es el número de proveedores, las incompatibilidades son mayores.

Capacitación.

En casi todos los casos de implantación del modelo Cliente/Servidor, la principal dificultad es la capacitación de los usuarios. No se trata de sólo impartir cursos a los usuarios y a los ingenieros en computación, sino de cambiar toda una cultura, cual es más complicado y costoso.

Es necesario redefinir todas las funciones computacionales; la visión de los sistemas de cómputo se debe cambiar por completo, la polivalencia debe ubicarse en el primer plano así como cambiar desarrollar nuevos expertos. El costo de una capacitación a fondo puede ser superior a la del conjunto del sistema. Sin embargo, se debemos considerar que la capacitación es una inversión a largo plazo.

Costos.

Si bien el costo es uno de los principales factores que inclinan la balanza en favor de la arquitectura Cliente/Servidor, los inconvenientes antes mencionados conducen a reflexionar sobre la variedad de costos ocultos que conlleva: capacitación, solución de montones de pequeños problemas imprevistos, el tiempo perdido en reconciliarse con los proveedores, la reorganización y el desarrollo de aplicaciones que aún no se encuentran en el mercado.

Es útil contar con una base de datos distribuida, lenguajes de consulta, bases de datos independientes de estos últimos y, por último, aplicaciones independientes de las bases de datos y de los tipos de terminales.

Control de concurrencia mas complejo (varios sistemas operativos dirigiendo cada una a una CPU propia)

Dependencia de la red

1.2.8.- TAREAS DE LA APLICACIÓN

El sistema debe de manejar las siguientes tareas:

- Solicitar una conexión, o sesión con una fuente de datos.
- Enviar sentencias SQL a la fuente de datos.
- Definir áreas de almacenamiento y formatos de datos para los resultados de las sentencias SQL enviadas.
- Recibirlos resultados enviados por la fuente de datos.
- Procesar errores.
- Reportar resultados hacia atrás, a un usuario, si es necesario.
- Finaliza la sesión o conexión con la fuente de datos.

1.3.- INTRODUCCIÓN A FIREWALLS

1.3.1.- FIREWALLS Y SEGURIDAD EN INTERNET

1.3.1.1.- INTRODUCCIÓN

El establecimiento del perímetro para el Acceso a la Web es una de las principales razones para la operatividad del Laboratorio de Internet tomando en cuenta que cada semestre aumenta la demanda del acceso a los servicios de Internet tal es el caso del World Wide Web (WWW), Internet Mail (e-mail), y File Transfer Protocol (FTP).

El sistema de Administración y Control del acceso a la Web deberá incrementar todo lo concerniente a la seguridad del mismo, debido a que se expone la organización privada de sus datos así como la infraestructura de sus red a los Expertos de Internet (*Internet Crakers*), el Sistema Web Access, y la Base de Datos de los clientes del Laboratorio de Internet,.

La forma de detener estos peligros es mediante la implantación de políticas de seguridad para prevenir el acceso no-autorizado de usuarios a los recursos propios de la red privada, y protegerse contra la exportación privada de información todo esto en el nivel de aplicación del Sistema de Administración y Control.

1.3.2.- CONCEPTO FIREWALLS

El Firewall son líneas de código que controlan el trafico de la información permitiendo el paso o restricción de ciertas solicitud de ingreso o salida hacia determinada red, siendo esta una red interna Lan o una red externa Internet todo esto bajo la programación de las políticas surgidas del levantamiento de los requisitos del Sistema para que operen en el nivel de aplicación del modelo cliente / servidor.

Esta política de seguridad incluirá:

Política de autenticidad en acceso remoto o local a usuarios propios de la red.

El firewall sin una política de seguridad comprensiva es como poner una puerta de acero en una tienda.

1.3.3.- BENEFICIOS DE UN FIREWALL EN INTERNET

- Mantiene al margen los usuarios no-autorizados.
- Prohíbe potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles.
- Ayuda a simplificar los trabajos de administración
- Concentra la seguridad

- Centraliza los accesos
- Genera alarmas de seguridad Traduce direcciones (NAT)
- Monitorea y registra el uso de Servicios de WWW y FTP.
- Internet.
- Audita o registra el uso del Internet para que el Sistema de Administración y Control justifique el gasto que implica la conexión al Internet, a través del registro a los terminales dentro del modelo de finanzas del ITSA.

1.3.4.- LIMITACIONES DE UN FIREWALL

El firewall no puede protegerse de las amenazas a que esta sometido por traidores o usuarios inconscientes.

El firewall no puede proteger contra los ataques de la “Ingeniería Social”, por ejemplo un Hacker que pretende ser un supervisor o un nuevo empleado despistado.

El firewall no puede protegerse contra los ataques posibles a la red interna por virus informativos a través de archivos y software. Obtenidos del Internet por sistemas operativos al momento de comprimir o descomprimir archivos binarios, el firewall de Internet no puede contar con un sistema preciso de SCAN para cada tipo de virus que se puedan presentar en los archivos que pasan a través de el.

1.3.5.- COMPONENTES DEL SISTEMA FIREWALL

El firewall para el Sistema de Administración y Control del Acceso a la Web se compone de los siguientes obstáculos.

Ruteador Filtra-paquetes.

Gateway a Nivel-aplicación.

1.4.- QUE ES UN CORTAFUEGOS?

La definición de un cortafuego informático es: un ente controlador simple o compuesto que actuara como punto de conexión segura entre los clientes de la red Lan del laboratorio de Internet que desearán conectarse a la red Wan (Internet) haciendo cumplir las determinadas directivas de seguridad sobre la comunicación entre ellas que estarán programadas en el nivel de aplicación.

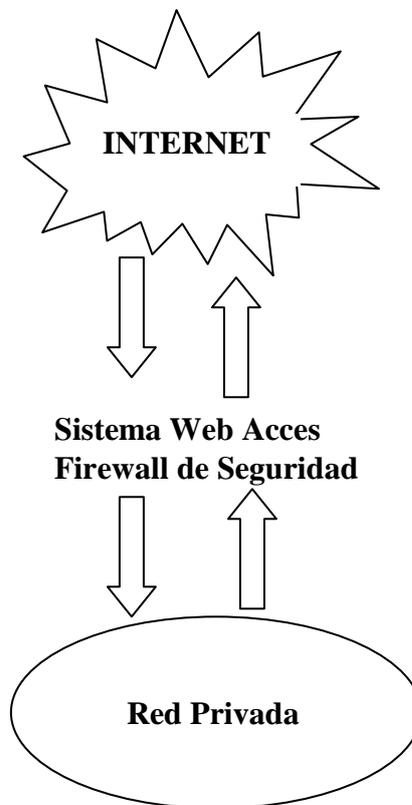


Figura 04 Ubicación del Firewall.

1.5.- FILTRADO DE PAQUETES

Basado en que el tráfico se mueve a través de una red en *paquetes*. Y que el paquete de red es una unidad de transmisión de información, que esta compuesto por diferentes elementos, como son:

- Datos.
- [Id.](#) de cabecera.
- Direcciones tanto del origen como del destino del paquete.
- Información complementaria para control de errores.
- Una colección de datos en diferentes tamaños y formatos.

Es así que para enviar un mensaje por red, el cliente/terminal que desea conectarse al Internet debe en primer lugar partir el mensaje de solicitud en diferentes paquetes usando las reglas del protocolo de red.

Cada paquete contiene una parte pequeña de los datos del mensaje de solicitud de Acceso a la Web. Cuando el servidor donde se encuentra el Sistema de Administración y Control, recibe la transmisión este reensamblará los paquetes y construye de nuevo el mensaje de petición del Acceso al Internet.

Cada paquete contendrá la información que le ayudará a navegar por la red y moverse hacia el servidor donde reside el Sistema de Administración y Control del Acceso a la Web. El paquete indicará al Sistema de dónde viene, a dónde va, qué tipo de paquetes.

El kernel de Linux contiene la característica interna de filtrado de paquetes, que le permite aceptar diversos protocolos en el sistema mientras que intercepta y para a otros. El filtro de red kernel 2.4 tiene tres *tablas* internas o *listas de reglas*. Son las siguientes:

- `filtro` — Ésta es la tabla por defecto para manejar paquetes de red.
- `nat` — Ésta tabla se usa para alterar paquetes que crean una nueva conexión.
- `mangle` — Esta tabla se usa tipos específicos de alteración de paquetes.

1.6.- CORTAFUEGOS DE FILTRADO DE PAQUETES, IPFW

1.6.1.- CONCEPTO IPFW

El Cortafuegos de filtrado de paquetes, IPFW es una de las familias de los *Firewalls*, el cual trabaja con el protocolo TCP/IP en el nivel de red y transporte, es por esa razón de su nombre IPFW.

Para el desarrollo del Sistema Web Access se ha elegido este ya que este trabaja sobre los datagramas y las cabecera IP de los mismos indicados en el capítulo anterior, además de que se implementa dentro del sistema operativo RED HAT 9.0 y funcionan en las capas de transporte y red.

A continuación se presente un gráfico de como trabaja este en el modelo de la comunicación.

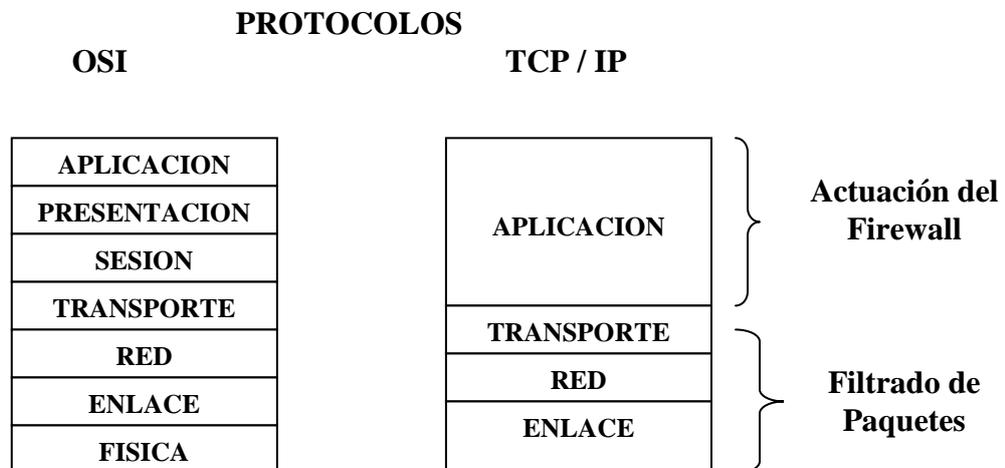


Figura 05 Modelo de Comunicación

1.6.2.- FILTRADO DE PAQUETES ENTRANTES EN UN IPFW.

El IPFW funciona filtrando las comunicaciones en ambos sentidos entre la red Lan del Laboratorio de Internet y la red externa que es el Internet mediante de una lista de reglas definidas a través de los requerimientos del Sistema de

Administración y Control, las cuales serán de aceptación, rechazo y denegación siendo la lista de reglas de entrada del Internet hacia la red Lan del Laboratorio totalmente independientes de la lista de reglas de filtrado de salida de la red Lan hacia el Internet

El filtrado se basa en:

- La dirección de origen.
- La dirección destino.
- El puerto origen.
- El puerto destino.
- El BIT de estado de TCP.

De esta forma se denegar el acceso a un a determinada pagina o a un determinado Host según el levantamiento de los requisitos del Sistema de Administración y Control.

Filtrado de dirección remota y local:

La forma de reconocer a un host problemático externo es a través de su IP y para evitar su ingreso siempre denegaremos:

- La dirección IP propia de la interfaz de red externa.
- La dirección IP propia de la interfaz de red interna.

La aceptación, rechazo y denegación son bastante similares, la diferencia radica en lo siguiente, cuando un IPFW rechaza una petición externa, envía una respuesta negativa diciendo que no acepta la comunicación, por el contrario, cuando un firewall descarta una petición, no envía ningún tipo de respuesta, es decir, que el agente externo que intentó establecer contacto, no sabrá ni siquiera si la máquina existía o estaba encendida.

1.5.2.- TÉCNICAS Y POLÍTICAS DE CREACIÓN DE LAS CADENAS

Estas técnicas consisten en:

Rechazar TODO por defecto y especificar aquello que deseemos ya que al rechazar todo ya que de esta forma existe una mayor seguridad en el diseño del Firewall para así poder llevar una política de seguridad mínimamente seria.
Estudio de las reglas de entrada y de salida para la interfaz interna y externa.

1.7.- IPTABLES

Iptables es como se conoce al módulo *Netfilter*, y con esta herramienta de cortafuegos se elaborará el Sistema de Administración y Control de Acceso al a Web bajo el sistema operativo RED HAT 9.0 ya este comando permite configurar la lista de reglas, así como configurar nuevas cadenas y tablas para ser usadas en si situación particular

¿Por qué Linux? Como todo sistema operativo UNIX tiene entre sus objetivos la seguridad, además es FREEWARE.

¿Por qué Red Hat 9.0?, el kernel que lleva es la versión 2.4.9, que soporta IPTables.

Además de realizar un mejor aprovechamiento de los recursos del sistema, la principal novedad del módulo *netfilter-iptables*, es la integración de las herramientas de filtrado (el cortafuegos propiamente dicho), de *NAT* y de manipulación (*MANGLING*).

NAT es el acrónimo de *Network Address Translation*. Lo que hace NAT básicamente es alterar las cabeceras de los paquetes IP, (principalmente las direcciones) y mantener un “registro de entrada y salida” de los paquetes modificados, para poder alterar los paquetes respuesta de igual forma.

1.8.- ESTRUCTURA Y FUNCIONAMIENTO DE IPTABLES.

Iptables trabaja con 3 tablas las cuales son:

- *filter*,
- *nat*

- y *mangling*

Es allí donde se plantearán las políticas de aceptación y negación para el acceso a la web

-Tabla nat: La tabla *nat* se utiliza para configurar el protocolo de Network Address Translation. Lo que hace NAT básicamente es alterar las cabeceras de los paquetes IP, (principalmente las direcciones) y mantener un “registro de entrada y salida” de los paquetes modificados, para poder alterar los paquetes respuesta de igual forma.

La tabla NAT trabaja con las siguientes cadenas:

La cadena PREROUTING se utiliza para alterar los paquetes tan pronto llegan al cortafuegos (del destino).

La cadena OUTPUT, se utiliza para alterar los paquetes generados localmente en el cortafuegos, antes de tomar ninguna decisión de enrutado.

La cadena POSTROUTING para alterar los paquetes que acaban de dejar el cortafuegos (el origen).

- Tabla mangle: La tabla de *mangling* o “manipulación”, permite manipular otros elementos de los paquetes.

Consta de dos cadenas, PREROUTING y OUTPUT.

- Tabla filter: En la tabla *filter*, se llevan a cabo la funcionalidad principal de iptables, el filtrado de paquetes. Como las anteriores, consta de varias cadenas predefinidas, en este caso INPUT, FORWARD y OUTPUT.

INPUT hace referencia a los paquetes entrantes cuyo destino es el propio cortafuegos.

FORWARD se emplea para decidir que hacer con los paquetes que llegan al cortafuegos y tienen como destino otro host, así podemos decidir si encaminarlos o no.

OUTPUT se utiliza para filtrar paquetes generados en el propio host con destinos externos.

1.9.- ENMASCARAMIENTO (IP-MASQUERADING)

1.9.1.- INTRODUCCIÓN

Con el crecimiento de la World Wide Web y la creciente necesidad de estar conectados a Internet existe un problema cuando utilizamos el clásico TCP/IP. La asignación de una dirección Internet de TCP/IP a cada una de las computadoras de la red de área local del Laboratorio de Internet del ITSA es una tarea pesada, molesta y no permite el control supervisado del acceso al Internet ya que cada terminal posee una salida independiente hacia la web.

Linux IP Masquerade o "IP Masq" es una característica del kernel que está disponible desde las versiones 1.2.x de los mismos permitiendo que una única máquina Linux donde residirá el Sistema de Administración y Control del Acceso a la Web para que actúe como un traductor entre una única dirección de IP y toda la red Lan interna. En términos técnicos este proceso es llamado NAT (Network Address Translation). Esto significa que una única dirección TCP/IP es traducida a muchas máquinas dentro de la red interna.

La red interna IP Masq presenta un esquema de TCP/IP totalmente diferente al externo y correr sobre cualquier tipo de topología de red como Ethernet o FDDI.

IP Masq permite realizar todo esto sin la necesidad de adquirir direcciones IP nuevas o dispositivos más costosos como un router. Además soporta un amplio rango de protocolos Internet como SMTP, FTP, I-ITTP, IRC.

Tabla 1: Direcciones IP privadas

Clases	Inicio Rango	Fin Rango	Máscara
1 x A	10.0.0.0	10.255.255.255	8
2 x B	172.16.0.0	172.32.255.255	16
3 x C	<u>192.168.0.0</u>	192.168.255.255	24

1.9.2.- DEFINICIÓN DE IP -MAS QUERADING (ENMASCARAMIENTO IP)

“IP Marquerade” es el nombre que se dá en Linux al sistema NAT (Network Address Translation) nativo, y que permite que toda una red corporativa acceda a Internet utilizando una única IP.

Este enmascaramiento, además de posibilitar el empleo de una única IP, proporciona cierta protección del tipo “cortafuegos”, ya que las máquinas externas (Internet) no pueden establecer conexiones con máquinas internas, a menos que sean éstas quienes lleven la iniciativa. De esta forma, si el servidor donde residirá el sistema Web Access está conectado a Internet con IP Masquerade habilitado, los ordenadores conectados a él también pueden conectarse a Internet, incluso aunque no tengan *una dirección IP oficial asignada*.

Esto permite a las maquinas del Laboratorio de Internet acceder de forma transparente a Internet Estas se ocultan tras la máquina pasarela (*gateway*), la cual aparece como el único sistema que está usando Internet. Romper la seguridad de un sistema configurado de forma correcta con IP Masquerade es considerablemente más difícil que romper un buen filtro de paquetes basado en cortafuegos (suponiendo que no existan fallos en ninguno). Esto garantiza que la red del laboratorio sea un poco más segura.

1.9.3.- NAT (NETWORK ADDRESS TRANSLATION)

Normalmente, los paquetes viajan en una red desde su origen (un ordenador) a su destino (www.kernelnotes.org) a través de varios enlaces diferentes. Ninguno

de estos enlaces altera realmente el paquete: simplemente lo envían un paso adelante pero si uno de estos enlaces hiciera NAT, podría alterar el origen o destino del paquete según pasa a través suyo.

Las razones principales para usar nat son:

Conexiones a Internet

La mayoría de los PSI (Proveedor de Servicios de Internet) dan una sola dirección IP cuando se conecta con ellos. Se pueden enviar paquetes con cualquier dirección, pero sólo se obtendrán respuestas de los paquetes con esa IP de origen. Si se desea utilizar varias máquinas diferentes para conectar a Internet a través de un enlace, se necesita NAT.

Este es, de lejos, el uso más común de NAT hoy en día, conocido normalmente como «enmascaramiendo» (masquerading) en el mundo de Linux.

Proxy transparente

Un “proxy “es un programa que se pone entre una red y el mundo real, filtrando las comunicaciones entre ambos. La parte transparente se debe a que la red nunca tendrá por qué enterarse de que está comunicándose con un proxy.

1.9.4. FUNCIONAMIENTO

IP Masq toma cada uno de los paquetes TCP/IP provenientes de la red interna del Laboratorio de Internet y los analiza con una tabla propia. Determinando así si el paquete debe ser enviado o no hacia la red Internet. IP Masq registra el origen del paquete y hacia donde es enviado. Entonces re-escibe la dirección origen del paquete inicial dándole la dirección IP externa del servidor Linux y lo envía a Internet. Cuando el servidor remoto recibe el paquete y responde, el servidor Linux es capaz de reconocer este paquete enmascarado y re-enrutarlo a donde corresponda.

Los módulos que soporta Nat para aplicaciones convencionales son: CuSeeMe (video conferencia), FTP (transferencia de archivos), IRC (para transferencias DCC), Quake (para multiples jugadores), Real Audio (video/ sound streaming), y IRCVdoLive (video conferencia).

1.9.5.- VENTAJAS DE LINUX IP-MASQUEDARE

Al ser posible conectar de 25 a 50 máquinas al servidor IP Masq donde reside el Sistema de Administración y Control del Acceso a la Web y proveer otros servicios como DHCP, SMTP, DNS, POP3 y NFS, en el ITSA se podría brindar el servicio de Internet a todos sus departamentos ya que se poseen 12 direcciones independientes para el acceso al Internet.

Otro de los beneficios del uso de IP Masquerade es que permite implementar el cortafuegos (firewall) de paquetes TCP/IP usando las herramientas estándar de Linux como iptables en la programación del sistema Web Access y así activar IP Masquedare por un "script" y además permite definir una serie de reglas para implementar un "firewall".

IP Masquerade funciona bien con 'máquinas clientes' con diferentes sistemas operativos y plataformas. Ha habido éxito con sistemas usando Unix, Windows 95, Windows NT, Windows para Trabajo en Grupo (con el paquete TCP/IP), OS/2, Sistemas Macintosh OS con Mac TCP, Mac Open Transport, DOS con el paquete NCSA Telnet, VAX, Alpha con Linux, e incluso Amiga con Am1TCP o AS225-stack.

1.9.6. PROBLEMAS CONOCIDOS

Algunos protocolos no funcionarán adecuadamente con masquerading porque presuponen cosas sobre números de puerto (o lo impiden datos cifrados en sus cadenas de información sobre direcciones y puertos), por lo que el chat en sistemas como xp pueden no correr por la actualización de Java.

El Masquerading no puede manejar todos los servicios de entrada. Existen formas de permitirlos, pero son completamente independientes de masquerading, y son realmente parte de la práctica estándar de cortafuegos.

1.9.7.- CLIENTES QUE FUNCIONAN

1.9.7.1.- Clientes Generales

HTTP

Todas las plataformas soportadas, navegadores web.

POP&SMTP

Todas las plataformas soportadas, clientes de correo electrónico.

Telnet

Todas las plataformas soportadas, sesión remota.

FTP

Todas las plataformas soportadas, con el módulo `lpmasq_ftp`

Archie

Todas las plataformas soportadas, buscador de archivos (nó todos los clientes archie son soportados).

NNTP (USENET)

Todas las plataformas soportadas, cliente de noticias USENET.

VRML

Windows (posiblemente soportado en todas las plataformas), navegación con realidad virtual.

Traceroute

Principalmente las plataformas basadas en UNIX, algunas variantes pueden no funcionar.

Ping

Todas las plataformas, con el parche ICMP.

Todo lo basado en IRC

Todas las plataformas soportadas, con el módulo Ip masqjrc .0

Cientes Gopher

Todas las plataformas soportadas.

Cientes WAIS Todas las plataformas soportadas.

1.9.7.1.2.- Clientes Multimedia**Real Audio l'layer**

Windows, envío de audio por red, con el módulo Ip masqraudio cargado.

True Speech Player Lib

Windows, envío de audio por red.

Internet Wave Player Windows, envío de audio por red.

Worlds Chat O.9a

Windows, programa Cliente-Servidor 3D de conversación.

Alpha Worlds

Windows, programa Cliente-Servidor 3D de conversación.

Internet Phone 3.2

Windows, comunicaciones de audio de Igual-a-igual

Powwow

Windows, comunicaciones tipo pizarra de audio texto de Igual-a-igual, la gente puede ponerse en contacto con Vd. si Vd. inicia la llamada, pero ellos no pueden llamarle.

CU-SeeMe

Todas las plataformas soportadas, con el módulo euseeme cargado, por favor mire en <http://ipmasq.home.ml.org/> para los detalles.

VDOLíve

Windows, con el parche vdolive.

1.9.7.1.3.- Otros Clientes

NCSA Telnet 2.3.08

DOS, un paquete que contiene telnet, ftp, ping, etc.

PC-anywhere para windows 2.0

MS-Windows, control remoto de PCs sobre TCP/IP, sólo funciona si es cliente pero no servidor.

Socket Watch

Usa ntp - protocolo de tiempo por red.

Linux net-accl package

Linux, paquete de administración de cuentas de red.

1.9.7.1.4 Clientes que NO funcionan

Intel Internet Phone Beta 2

Conecta pero la voz viaja en una dirección (sale) sólo.

Intel Streaming Media Viewer Beta 1

No puede conectar con el servidor.

Netscape CoolTalk No puede conectar con el lado opuesto.

Talk,ntalk

No funcionarán - requieren que sea escrito un proxy en el núcleo.

WebPhone

No puede funcionar por el momento (asume direcciones no válidas).

1.9.8 CASO DE ESTUDIO

Linux utiliza **ahora el software netfilter a través de una interfaz de nivel de usuarios llamada iptables para llevar a** cabo un filtrado de paquetes de estados completos. Utiliza la misma interfaz de nivel de usuario para llevar a cabo la traducción de direcciones de red (NAT), el enmascaramiento y el re-encaminamiento de puertos.

NAT básicamente permite re-escribir cabeceras de paquetes según pasan por el cortafuegos. Estas cabeceras pueden ser escritas según van saliendo del cortafuegos.

Estas cabeceras implican el cambio de la dirección original del sistema que inicia la conexión por la dirección externa del cortafuegos. Un servidor en Internet verá entonces una conexión que se origina en el cortafuegos o NAT.

Dado que la dirección original es la que se cambia, netfilter la denomina NAT del origen o SNAT.

Una forma especializada de SNAT, el enmascaramiento de IP, se utiliza para permitir que las estaciones de trabajo del Laboratorio de Internet con direcciones IP privadas (direcciones IP no encaminables hacia Internet) sean capaz de acceder a Internet. .

El otro tipo de NAT, o alteración de paquetes, que permite netfilter se llama NAT del destino o DNAT. Esta forma de alteración de la dirección se hace antes del .encaminamiento y se usa para tomar una conexión inicial al sistema NAT y redirigirla a un sistema interno.

En algunos circuitos, a este mecanismo se le denomina reencaminamiento de puertos, porque el reencaminamiento generalmente se basa en el puerto inicial de conexión.

Esto le permitiría tener sistemas independientes en la red del Laboratorio de Internet la cual será capas de manejar HTTP, FTP, correo, DNS y demás, pero aparentando que la máquina NAT es la que está haciendo todo el trabajo.

Esta particular forma de alteración de direcciones requiere que se disponga de una dirección IP encaminable.

Con mucha frecuencia, el software de cortafuegos de filtrado de paquetes se usa para ocultar una red pública interna y permitir que entre solamente cierto tráfico, como es el caso del esquema que se pretende para la red del Laboratorio de Internet.

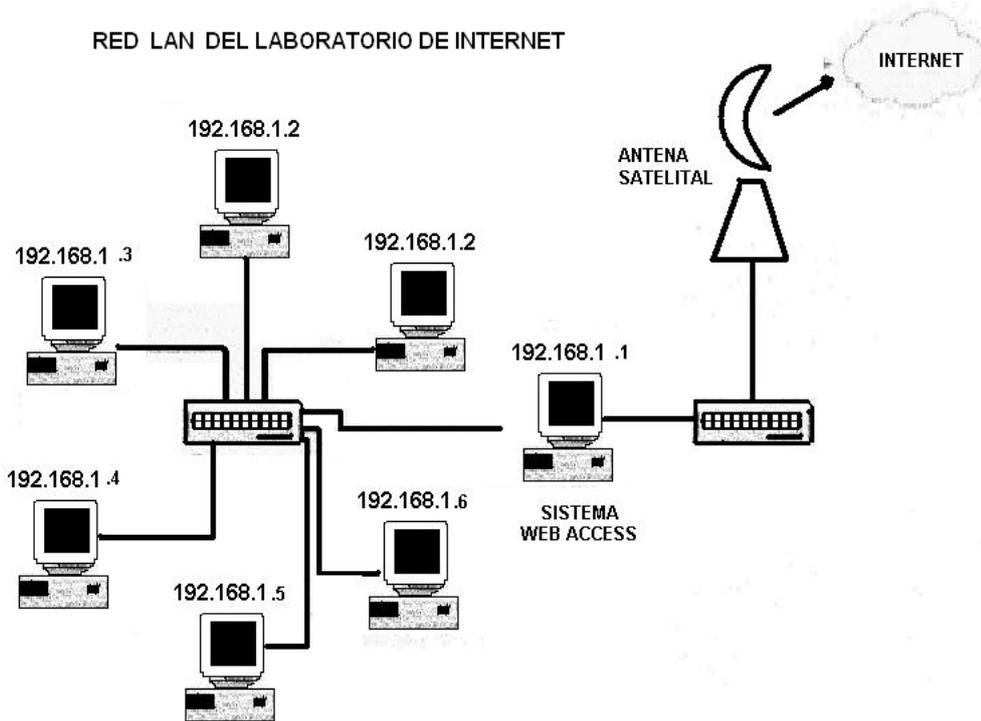


Figura 06 Red Lan del Laboratorio de Internet del Instituto Tecnológico Superior Aeronáutico

Utilizando el enmascaramiento de IP, la red del Laboratorio de Internet puede dar acceso a todas las máquinas conectadas, a una red externa como Internet, utilizando la dirección IP única (10.255.5.98) en el servidor de las doce que posee.

Todos los paquetes que vayan a Internet se enmascaran como si estuvieran enviados desde el servidor que está ejecutando el enmascaramiento de IP.

El servidor mantiene la información necesaria para encaminar los paquetes de la red de vuelta a las máquinas que los deben recibir.

Dependiendo de en que dirección vayan los paquetes cada conexión es tanto SNAT como DNAT, Sin embargo, es el paquete de la conexión inicial, esto es el paquete SYN (un paquete con solamente el bit SYN a 1), el que lo determina.

El seguimiento de la conexión permite que los paquetes de retorno vuelvan al sistema origen. El seguimiento de paquetes convierte a netfilter en una herramienta de filtrado de paquetes de estados completos, una expresión que significa que reconoce el estado de una conexión (nueva, establecida y relacionada).

Las conexiones establecidas relacionadas no se ejecutan con el conjunto completo de reglas, netfilter recuerda las reglas que afectan a la conexión, las utiliza, y se salta el resto.

1.9.8.2.- Componentes del kernel necesarios

El kernel de Linux que viene con la mayoría de las distribuciones de Linux está precompilado con todo lo que se necesita para utilizar enmascaramiento IP, es así que todo lo que se necesita para implementarlo es cargar algunos módulos del kernel y configurar algunas reglas sencillas de cortafuegos.

1.9.8.3.- Configuración

El enmascaramiento de IP se lleva a cabo a través de las utilidades del cortafuegos de filtrado de paquetes de los kernels modernos de Linux.

Cuando un paquete de salida de red llega a la máquina cortafuegos (el servidor que tiene el enmascaramiento de IP instalado), el cortafuegos reescribe los elementos de cada paquete para hacer que parezca que salen del cortafuegos, y no de la máquina que está detrás del cortafuegos. Los paquetes de retorno se modifican para que vuelvan a la máquina que envió los paquetes de salida originales. Para ninguno de los dos extremos de la transacción nada raro en absoluto parece estar pasando.

Algunos servicios, como FTP, necesitan un trato especial, de ahí el módulo para soportar el seguimiento de conexiones FTP.

Lo primero que se ha hecho para comenzar el enmascaramiento es crear una red con direcciones IP ficticias de los bloques de direcciones IP reservadas para redes privadas como se pueden ver en la tabla 1. y como es una red, literalmente amplia por lo que se utiliza uno de los bloques de la Clase C.

La herramienta iptables se usa configurar las reglas de reencaminamiento para el enmascaramiento de IP. Se usa la siguiente sintaxis:

```
iptables -t nat -A POSTROUTING -j MASQUERADE -o ppp+ -s  
red_IP_privada/máscara -d 0/0
```

En este comando, se reemplazara la red `-j Privada` por la primera dirección IP de la Tabla 1 de la clase de direcciones C, y se ha de reemplazar la máscara con el correspondiente valor de máscara.

La opción `-o` especifica la interfaz de salida. `ppp+` indica una interfaz ppp (normalmente `pppO`, el signo `+` significa cualquier interfaz ppp activa).

Puede sustituir `ppp~` or `eth0`, `1rO`, `ippO` y demás interfaces posibles.

Quedando la configuración para el Laboratorio de Internet con el siguiente comando:

```
iptahles -t nat -A POSTROUTING -j MASQUERADE -o ppp+ -s 192.168.0.0/24 -d  
0/0
```

El enmascaramiento de IP es una calle de un solo sentido. Puede ir de las máquinas de la red a Internet, pero, sin reglas especiales de reencaminamiento de paquetes, no puede entrar en sistemas que estén detrás del servidor de enmascaramiento desde Internet.

Esto significa que una máquina que tiene una dirección IP ficliiia y está detrás del servidor de enmascaramiento no puede servir páginas web a Internet, ni puede

aceptar conexiones FTP directas desde fuera, ni telnet, si ssh o transacciones seguras, y además, sin reglas especiales.

Para prohibir el reencaminamiento y que sólo pasen las direcciones enmascaradas, se lo realiza con la siguiente regla:

```
iptables -p FORWARD DENY
```

1.9.8.4.- Construcción del sistema NAT para el Laboratorio de Internet del ITSA

Utilizando todo lo anterior se va a construir un sistema NAT para una red del Laboratorio de Internet del ITSA

Los parámetros son los siguientes:

- Se dispone del bloque de direcciones IP 10.255.5.98 /111 otorgado por el proveedor de servicio de Internet Satelital NEDETEL.
- Al encaminador se le asigna la dirección 10.255.5.98 y 192.168.1.1 al cortafuegos NAT.
- La red interna es 192.168.1.2/30, y el sistema NAT (pasarela) es 192.168.1.1 (eth0).

Se tienen los siguientes sistemas en la red:

- 192.168.1.1 Servidor Web Apache.
- 192.168.1.1 Servidor de MySQL

Cada sistema ejecuta Webmin sobre SSL en el puerto 10000, pero se necesita administrar cualquier sistema interno desde fuera.

Todo el tráfico entrante entra por 192.168.1.1 (eth0). Se quiere utilizar 10.255.5.98 (eth1) para las conexiones de salida.

Se quieren permitir conexiones de salida a todos los puertos privilegiados (0-1023) y también al puerto 3306.

II.-ESTUDIO DEL LABORATORIO DE INTERNET DEL INSTITUTO TECNOLÓGICO SUPERIOR AERONÁUTICO

2.1.- CAMPO DE ACCIÓN

2.1.1.- ANTECEDENTES DEL ITSA

El Instituto tecnológico superior aeronáutico, ha venido cumpliendo con la noble tarea de formar, capacitar y profesionalizar al personal de aerotécnicos en las diferentes especialidades de aviación, pasando por sus aulas 37 promociones.

El I.T.S.A. pone a disposición de toda la colectividad tecnologías únicas a nivel nacional, con un real mercado ocupacional y una gran área potencial laboral para nuestros tecnólogos.

Misión

Formar tecnólogos militares y civiles, a través de una educación integral en las áreas técnica, científica y humanística, con el fin de aportar a la seguridad y desarrollo del país, así como planificar y ejecutar cursos de capacitación y perfeccionamiento en áreas afines a la aeronáutica.

Propulsar y estimular la formación de profesionales capaces de generar propuestas creativas, que permitan el desarrollo de nuestro país en general y del área aeronáutica particularmente.

Formar tecnólogos con el adecuado nivel técnico científico competitivos a nivel nacional e internacional.

Convertir al I.T.S.A. y sus integrantes en los catalizadores de ideas y generadores de acciones que posibiliten el desarrollo institucional, regional y nacional.

Brindar formación académica práctica, profesional y humanística a los tecnólogos que se gradúan en el I.T.S.A., a fin de formar hombres y profesionales íntegros.

2.1.2 ANTECEDENTES DEL LABORATORIO DE INTERNET

En el INSTITUTO TECNOLÓGICO SUPERIOR AERONÁUTICO (ITSA) se encuentra ubicado el Laboratorio de Internet cuyo inicio fue en el año 2000, con 2 computadoras para el servicio de Internet, con conexión digital telefónica, ampliado posteriormente a cinco computadoras, luego 10 equipos y actualmente contamos con 17 (diecisiete) computadoras, de las cuales únicamente diez poseen direcciones IP, para servicio de conexión a Internet satelital, en beneficio del personal de alumnos, administrativos y docentes de la institución.

El objetivo del laboratorio de Internet es brindar el mejor servicio de Internet a sus usuarios, a través de la venta del acceso a la red informática por un tiempo determinado para lo cual cuenta con 12 ordenadores cada uno con una dirección IP estática cada una independiente de la otra, con conexión satelital y siendo este servicio controlado por los laboratoristas de turno en forma manual, ocasionando el no tener un control eficaz de la administración del mismo, en determinadas actividades tales como:

2.2.- EL CONTROL PARA EL USO DEL SERVICIO DE INTERNET.

Este control depende del encargado de turno del Laboratorio de Internet, el cual designa los terminales a ser ocupados, el tiempo a navegar y el acceso a las diferentes paginas Web, todo esto en forma manual.

Adicional se debe de regir a las normas y políticas de la Institución la s cuáles consisten en:

Los alumnos Militares, Civiles, Profesores y Personal Administrativo deberán adquirir en el Laboratorio de Informática un ticket de alquiler por una hora de Internet, de igual manera los derechos de hoja de impresión los deben adquirir por un costo de:

- 5 centavos de dólar Por cada hoja/impresión matricial.ç**
- 20 centavos de dólar Por cada hoja/impresión a inyección tinta.**
- 40 centavos de dólar Por cada hoja/impresión a inyección color.**
- 50 centavos de dólar Por 1 hora de Internet.**

El valor del uso del servicio de Internet será incluido en el valor de la matrícula.

Los alumnos tienen derecho a utilizar 20 horas del servicio de Internet, durante el transcurso del Periodo Académico, para lo cual se le proporciona una tarjeta de control de uso en la oficina de los Laboratorios de Informática, la misma que es de uso personal e intransferible.

Cada alumno tiene derecho de 10 horas de Internet cada trimestre, si no se utiliza estas horas perderá automáticamente.

No existe reposición de tarjeta perdida.

En caso de existir máquinas disponibles y que no hayan sido reservadas, el encargado de turno podrá asignar estas horas a cualquier estudiante que lo requiera.

La reservación de los turnos para utilizar el servicio de Internet se receptará en la oficina de los Laboratorios de Informática con 48 horas de anticipación de acuerdo al horario establecido por el Jefe de Laboratorios.

El alumno no podrá transferir el turno reservado a otra persona.

Cuando un alumno haya agotado su tarjeta de control de horas podrá seguir utilizando el servicio de Internet previo a la presentación del carnet de identificación y el ticket de alquiler, cuyo costo es de 1 dólar por cada hora de servicio.

Los alumnos militares se sujetan al parrafo anterior.

Los horarios de atención del Laboratorio de Internet son de lunes a viernes de 7:30 a 24:00 en forma continua, los días sábados y domingos de 8:00 a 14:00

2.3.- EL CONTROL PARA EL USO DEL SERVICIO DE INTERNET A LOS ALUMNOS

Este es por medio de tarjetas impresas en cartulina, con cuadros representativos de treinta minutos dando un total de 20 horas semestrales, la cual es entregada por el encargado del laboratorio de Internet a cada alumno matriculado en un periodo académico, para lo cual revisa de una lista impresa (entregada por el departamento de secretaria académica), y si el alumno se encuentra matriculado procede a entregar dicha tarjeta, la cual contiene el nombre del alumno, su escuela, nivel, especialidad y la fecha de caducidad de la misma todo esto en forma manual.

Adicional debe de registrarse a los ítems mencionados anteriormente.

2.4.- PROCESO DE REGISTRO PARA LOS ALUMNOS DE LA INSTITUCIÓN.

Cuando un alumno desea hacer uso del servicio de Internet, este se acerca al encargado del Laboratorio para que este proceda a descontarle de la tarjeta el tiempo requerido y al mismo tiempo registra el nombre del alumno, la hora de inicio y la hora fin que el cliente hará uso del servicio de Internet, en una bitácora de registro de usuarios.

En caso de requerir más tiempo de servicio de Internet el alumno deberá acercarse con anticipación a su tiempo de terminación a solicitar el tiempo que el considere necesario para lo cual comenzará nuevamente el proceso de registro. Si el alumno no ocupa todo el tiempo solicitado, el encargado de turno le adjudica en la tarjeta de Internet el tiempo no consumido.

En caso de que el alumno haya terminado su tiempo de uso en la tarjeta de 20 horas este deberá acercarse a la sección de pagaduría para adquirir otra tarjeta de 20 horas de Internet o podrá ingresar en el proceso de registro para usuarios externos a la institución.

2.5 EL CONTROL PARA EL USO DEL SERVICIO DE INTERNET AL PERSONAL DE PLANTA DE LA INSTITUCIÓN.

Este control depende del encargado de turno del Laboratorio de Internet, el cual designa los terminales a ser ocupados, el tiempo a navegar y el acceso a las diferentes paginas Web, todo esto en forma manual.

Adicionalmente debe sujetarse a los siguientes literales de las políticas internas de la Institución:

Los señores profesores a tiempo completo podrán usar el servicio de Internet sin limite de tiempo previa la reservación del turno respectivo. El valor de uso será de dos (2) dólares mensuales.

El personal de profesores a tiempo parcial deberá adquirir en el Laboratorio el ticket de uso por un valor de cincuenta centavos de dólar por hora de servicio de Internet previa la reservación correspondiente.

Voluntariamente los profesores a tiempo parcial podrán inscribirse a tiempo completo, teniendo derecho a utilizar el servicio de Internet sin limite de tiempo.

2.6 REGISTRO AL PERSONAL DE PLANTA DE LA INSTITUCIÓN.

Cuando un docente o personal administrativo desea hacer uso del servicio de Internet, este se acerca al encargado del Laboratorio para que este proceda a registrar el nombre del usuario, la hora de inicio y la hora fin que el cliente hará uso del servicio de Internet, en la bitácora de registro de usuarios.

En caso de requerir más tiempo de servicio de Internet el cliente deberá acercarse con anticipación a su tiempo de terminación, a solicitar el tiempo que el considere necesario para lo cual comenzará nuevamente el proceso de registro.

Si el cliente no ocupa todo el tiempo solicitado, el encargado de podrá adjudicar la maquina a la persona que la necesite.

Este proceso es siempre y cuando el docente o personal administrativo del ITSA realice trabajos en beneficio de la Institución, en caso contrario este deberá ingresar en el proceso de registro para usuarios externos a la institución.

De igual forma deberá regirse a los siguientes literales.

El personal administrativo deberá adquirir en el Laboratorio el ticket de uso por un valor de cincuenta centavos de dólar por hora de servicio de Internet previa la reservación correspondiente.

Voluntariamente el personal administrativo podrán inscribirse a tiempo completo, teniendo derecho a utilizar el servicio de Internet sin limite de tiempo.

2.7 EL CONTROL PARA EL USO DEL SERVICIO DE INTERNET A USUARIOS EXTERNOS A LA INSTITUCIÓN

Este se lo realiza a través del siguiente proceso:

Proceso de registro al personal externo de la institución.

Cuando un usuario externo solicita hacer uso del servicio de Internet, este se acerca al encargado del Laboratorio para que este proceda a registrar el nombre del usuario, la hora de inicio y la hora fin que el cliente hará uso del servicio de Internet, en la bitácora de registro de usuarios y le entrega un ticket de alquiler de servicio en el cual consta:

El tipo de servicio.

El tiempo de alquiler

En caso de requerir más tiempo de servicio de Internet el cliente deberá acercarse con anticipación a su tiempo de terminación, a solicitar el tiempo que el considere necesario para lo cual comenzará nuevamente el proceso de registro.

2.8 DEL CONTROL DEL TIEMPO DE USO DE INTERNET.

Al no existir un control automatizado este puede sufrir los siguientes casos:

Un usuario puede llegar a una hora “x” y el registrador lo puede anotar en una hora “y”.

El usuario puede pedir un tiempo de uso y este tiempo puede ser sobrepasado y no controlado por el encargado de laboratorio por razones fuera de su alcance.

No se han establecido tiempos de acceso a la Web diarios para los alumnos los cuales pueden pasar un tiempo ilimitado en un computador y no

permitir el paso a otro usuario que desee realizar uso del servicio de Internet por lo que este acude a otro Cyber

2.9 DEL ACCESO A LA WEB POR PARTE DE LOS USUARIOS.

Este es controlado por el encargado de turno del laboratorio en forma visual pero por razones externas no lo puede realizar en un 100%, motivo por el cual los alumnos pueden ingresar a paginas no autorizadas establecidas por políticas de la Institución

2.10 EL DESCONOCIMIENTO DEL BENEFICIO ECONÓMICO Y EFICIENCIA REAL DEL SERVICIO DE INTERNET

Representa una desventaja para la institución ya que no existe un análisis estadístico tiempo de uso del Internet vs. cobro del tiempo de uso.

La no garantización del cobro o descuento del servicio de Internet a todos los usuarios del mismo por razones externas.

2.11 EFICIENCIA DEL SERVICIO DE INTERNET

La demora en el proceso de entrega de las tarjetas de Internet es demasiado larga ya que se debe esperar el cierre del periodo de matriculación para su respectiva emisión.

La ampliación de los terminales para satisfacer la demanda de usuarios, requiere de un nuevo contrato con la empresa que brinda el servicio ya que el servidor DNS no admite la integración de una dirección IP más al servicio.

Existen ocasiones en que el servicio de Internet es suspendido por razones externas por un tiempo indefinido y la no-existencia de un documento que explique los pasos a seguir ante dichas eventualidades provoca pérdidas económicas para la Institución.

2.12 DE LA RESERVACIÓN DE MAQUINAS PARA EL SERVICIO DE INTERNET

Este proceso se lleva a cabo en forma manual, con las anticipaciones respectivas por parte de los usuarios.

La búsqueda de una maquina disponible para el servicio de Internet es demasiada lenta y estresante para el encargado de turno ya que existe una gran demanda de usuarios y para realizar dicho proceso el encargado debe de revisar en la bitácora de Internet cual es la maquina mas próxima a ser desocupada.

2.13 DEL CONTROL A LOS SERVICIOS QUE BRINDA EL LABORATORIO.

Además del servicio de Internet, este laboratorio también brinda el servicio de impresiones, cuyos procesos son controlados de forma manual.

En relación al recurso humano se requiere de una persona que este constantemente presente para el registro de usuarios de Internet y control del mismo.

2.14 ESTABLECIMIENTO DE REGLAS INTERNAS Y EXTERNAS PARA EL ACCESO AL SERVICIO DE INTERNET

Estas están sujetas de acuerdo a las regulaciones de la institución las cuales son:

2.14.1 REGULACIONES PARA EL USO DEL LABORATORIO

1. Están autorizados los señores profesores a utilizar los laboratorios cuando los trabajos sean en beneficio del ITSA, en caso de requerir para trabajos

personales deberán cancelar el arancel correspondiente con su respectivo descuento.

2. Podrán ingresar al Laboratorio de Internet dos personas por cada computador, las personas cuyos nombres e identificación fueron anotados en la reservación.
3. Al momento de ingresar al Laboratorio de Informática los estudiantes deberán presentar su carné de identificación, el mismo que será verificado con el nombre de reservación.
4. Los usuarios que hubieran reservado horas de computador y no pudieran asistir a su turno, podrán cederlo a otra persona con autorización escrita, dentro del horario correspondiente.
5. El uso de las computadoras en las prácticas de laboratorio se realizara sin costo alguno.
6. Los usuarios no podrán ceder una parte del tiempo reservado para su turno a ninguna otra persona.

2.15 ESTABLECIMIENTO DE LOS NIVELES DE ACCESO A LA WEB.

Los niveles de acceso a la Web se han determinado del entorno del problema existen dados de acuerdo al tipo de clientes.

- ◆ Zona verde
- ◆ Zona amarilla
- ◆ Zona roja

Zona verde.

- ◆ Páginas de interés educativo.
- ◆ Buscadores o motores de búsqueda entre estos
- ◆ www.google.com
- ◆ www.elprisma.com
- ◆ www.monografias.com
- ◆ www.mimundo.com
- ◆ www.yahoo.com
- ◆ www.altavista.com

servidores de correo electrónico

- ◆ www.latinmail.com
- ◆ www.hotamail.com
- ◆ comerciales
- ◆ gobierno
- ◆ y todas aquellas que no vayan en contra de las políticas de la Institución

zona amarilla

- ◆ Páginas de software descargable ej
- ◆ www.download.com
- ◆ páginas que no se encuentran con el sello de seguridad (candado)
- ◆ páginas que sobrecarguen el ancho de banda
- ◆ www.elchat.com
- ◆ www.latinchat.com

zona roja

- ◆ Páginas de contenido pornográfico ya que en estas por lo general vienen los virus.

2.16 ANALISIS PARA LA ASIGNACION DEL TIEMPO DEL ACCESO A LA WEB

2.6.1 CAPACIDAD MÁXIMA DE TRABAJO DEL LABORATORIO DE INTERNET EN UN SEMESTRE.

Este caso se da en cuanto se tengan todos los recursos disponibles, en particular las 14 estaciones de trabajo, se labore los 183 días de un semestre y cada terminal trabaje las 16 horas diarias ininterrumpidamente.

a) Horario de trabajo del Laboratorio de Internet.

De 7:00 a 7:300 inspección pre básico de la red

De 7:30 a 23:30 ininterrumpidamente.

De 11:30 a 24:00 inspección pre básico de la red

a.1) Análisis capacidad horas

16	horas laborables	
* 5	días de la semana	
.....		
80	horas a la semana	
* 13	# de maquinas del laboratorio (14 puntos de red disponibles).	
.....		
1040	horas a la semana (hora / maquina)	
4	semanas al mes	
.....		
4160	horas al mes	
* 6	meses del semestre	
.....		
24960	horas al semestre	

Capacidad máxima de trabajo del laboratorio de Internet con 14 maquinas = 20800 horas

2.16.2 CAPACIDAD MINIMA DE TRABAJO DEL LABORATORIO DE INTERNET EN UN SEMESTRE.

Esta se da en cuanto se disponga de un número de estaciones igual a 9.

80	horas a la semana	
* 9	# de maquinas	
.....		
720	horas a la semana	hora / maquina
* 4	semanas al mes	
.....		
2880	horas al mes	
6	meses del semestre	
.....		
17280	horas al semestre	

Capacidad mínima de trabajo = 17280 horas

2.16.3 DEMANDA DE USUARIOS DEL LABORATORIO DE INTERNET EN UN SEMESTRE.

# de alumnos	530	personal de planta	60
# de horas asignadas	* 20	# horas asignadas	* 20

Demanda de alumnos 10600

demanda de docentes 1200

Particulares

En el mejor de los casos se asume que nos visitan 5 personas por día y solicitan 1 hora

4 horas solicitadas al día
* 5 días a la semana
.....
20 horas a la semana
* 4 semanas al mes
.....
80 horas al mes
* 6 meses del semestre
.....
480 horas al semestre

Demanda de usuarios invitados = 480 horas (valor aproximado)

Demanda de alumnos = 10600

Demanda de docentes = 1200

Demanda de usuarios/invitados = 480

TOTAL DE DEMANDA = 12280

2.16.4 ANÁLISIS SALDO HORAS DE TRABAJO DEL LABORATORIO DE INTERNET EN UN SEMESTRE..

CAPACIDAD MÁXIMA = 20800 CAPACIDAD MINIMA = 17280

DEMANDA = 12280 DEMANDA = 12280

SALDO 8520 SALDO 5000

III.- DISEÑO Y DESARROLLO DEL “SISTEMA DE ADMINISTRACIÓN Y CONTROL DEL ACCESO A LA WEB: LABORATORIO DE INTERNET DEL “INSTITUTO TECNOLÓGICO SUPERIOR AERONÁUTICO”

3.1.- GESTIÓN DEL SISTEMA OPEN SOURCE PARA LA ADMINISTRACIÓN Y CONTROL DEL ACCESO A LA WEB

Para una gestión del Sistema Open Source para la Administración y Control del Acceso a la Web altamente especializada y adaptada a los clientes del Instituto Tecnológico Superior Aeronáutico se realiza un seguimiento continuo de las necesidades de los usuarios finales tanto internos como externos al ámbito del problema, que proporciona una garantía y calidad servicio.

Para garantizar el adecuado desarrollo y funcionamiento del Sistema de Administración y Control del acceso a la Web se ha tomado en cuenta las siguientes palabras claves que son:

- Administración
- Eficiencia
- Análisis costo-eficiencia

El desarrollo de la administración requiere métodos, instrumentos, estrategias, medios y recursos para guiar a la planificación de la gestión del Sistema Open Source para la Administración y Control del Acceso a la Web en forma adecuada.

La eficiencia con que se vayan obteniendo los resultados dependerán de una buena planificación de los procesos

Al implementar el Sistema Web Access se obtendrá el verdadero costo beneficio en cuanto a:

Recurso Humano

Recurso Material

Recurso Económico

3.1.1 PLANIFICACIÓN DE LA GESTIÓN DEL SISTEMA OPEN SOURCE PARA LA ADMINISTRACIÓN Y CONTROL DEL ACCESO A LA WEB

Esta se basa en que los productos obtenidos en el tiempo sean de calidad, para lo cual se ha realizado la respectiva planificación para el desarrollo del Sistema y compararlo con lo que se obtiene en el tiempo.

ANEXO I Cronograma de Actividades

3.2 CICLO DE VIDA DEL DESARROLLO DEL “SISTEMA DE ADMINISTRACIÓN Y CONTROL DEL ACCESO A LA WEB”.

La elección del ciclo de vida ha sido la del interactivo incremental ya que en este se podrá seguir la planificación e ir realizando ajustes en el transcurso del desarrollo del sistema.

Las fases del ciclo de vida INTERACTIVO INCREMENTAL se definen de la siguiente manera:

3.2.1 EL ANÁLISIS DEL ÁMBITO DEL “SISTEMA DE ADMINISTRACIÓN Y CONTROL DEL ACCESO A LA WEB”

Se describen a continuación todas las características exteriores e interiores observables del entorno que rodea al problema, como son: funcionalidad, funcionamiento, flexibilidad.

a) Características exteriores

Funcionalidad.- El presente sistema tendrá la opción de llevar el control referente al registro de usuarios tanto internos como externos al ámbito del problema.

Flexibilidad.- En cuanto al acceso al Internet, a la modificación en los procesos que el Sistema maneja como son:

- Registro y cobro del valor del tiempo de Internet.
- Disponibilidad de tiempo para usuarios externos.

b) Características internas.

Flexibilidad en cuanto a:

El acceso al Sistema para acceder al Internet por parte de los usuarios.

Respaldos, exportación de la base de datos y del sistema a otro servidor.

Ampliación hacia nuevos módulos para el futuro los cuales dependerán de las nuevas políticas de la Institución

3.2.1.1.- Recopilación de información.

a) Administración de un Cyber Café

La Administración de un Cyber Café esta compuesta por:

- Control del acceso al Internet
- Estadísticas de uso de conexión al Internet en los terminales.
- Disponibilidad del tiempo para los usuarios
- Control de acceso a las máquinas terminales.

- Determinación de los tipos de usuarios.
- Facturación de los tiempos de conexión al Internet por parte de los usuarios.

b) De la Administración del Laboratorio de Internet

La administración del laboratorio de Internet se encuentra sujeta de acuerdo a políticas de la institución sobre los niveles de acceso y denegación al mismo esto incluye:

**c) Organigrama estructural del Instituto Tecnológico Superior Aeronáutico
ANEXO II**

d) De la población que rodea el problema.

Docentes del ITSA	68
Personal de planta del ITSA	24
Alumnos civiles y Militares	450

e) Periodo académico.

22 semanas laborables.

f) Del laboratorio de Informática del ITSA

Horas laborables del Laboratorio

13 horas diarias contempladas de lunes a viernes

7 horas el día sábado.

72 horas semanales.

g) Recurso humano del laboratorio de Internet.

Analista	01	Jefe Laboratorios Informática ITSA
Tecnólogos.	03	Administradores del Laboratorio
Alumnos	05	Pasantes del Laboratorio
Total	08	

h) Tecnología del Laboratorio de Internet.

Conexión Satelital	
Tipo de cableado	Estructurado
Topología de la red	Lan en estrella.
Número de maquinas	15
Sistema operativo de los terminales	Windows 98.
Direcciones IP	12 direcciones independientes

3.2.1.2 Clasificación de la información:

De acuerdo a la información obtenida de la organización del Instituto Tecnológico Superior Aeronáutico en base de las encuestas realizadas e información obtenida fruto de la investigación se establecen la siguiente clasificación:

a) Usuarios externos.

Son clientes que no tienen relación directa con el instituto, es decir que no son alumnos ni personal de planta cuyo fin es el de realizar una conexión al Internet

b) Usuarios internos

b.1.- Personal de planta.

Es el personal que orgánicamente esta con el pase en el ITSA, o que son empleados del mismo

b.2.- Personal docente

Personal cuya labor es la de impartir clases

b.3.- Alumnos del ITSA

Todas aquellas personas que se han matriculado en un periodo académico

c) Administrador de escuelas.

El laboratorio orgánicamente depende de la Escuela de telemática y esta a su vez del Vicerrectorado Académico el cuya función es controlar el normal funcionamiento de todos los laboratorios de la sus diferentes escuelas del ITSA

d) Administrador del Laboratorio de Internet

Es el jefe del los del laboratorio de Informática, cuya función el control y administración de los servicios a detallar:

Asignación del tiempo a navegar por parte de los clientes del Laboratorio.
Gestión de compras de nuevos equipamientos.

Controlar las actividades de los ayudantes de su turno e informar inconvenientes al superior

e) Administrador operador del Laboratorio de Internet

Son los encargados del laboratorio de Informática, cuya función es:
Administrar y controlar el acceso a la WEB a los usuarios.
Registrar a los usuarios que acceden al Internet
Controlar el tiempo de acceso de los alumnos al Internet.
Elaboración del informe económico del servicio de Internet

f) Administradores de la sección de pagaduría.

Es el encargado de la emisión de tarjetas de Internet a los usuarios que desean adquirir el servicio de Internet en el ITSA.

3.2.1.2.1.- Análisis para la asignación del tiempo del acceso a la Web.

a) Capacidad máxima de trabajo del laboratorio de Internet en un semestre.

Este caso se da en cuanto se tengan todos los recursos disponibles, en particular las 14 estaciones de trabajo, se labore los 183 días de un semestre y cada terminal trabaje las 16 horas diarias ininterrumpidamente.

CAPACIDAD MÁXIMA =	20800	CAPACIDAD MINIMA =	17280
DEMANDA =	12280	DEMANDA =	12280
SALDO	8520	SALDO	5000

Para cumplir con la demanda de los clientes internos de acuerdo a las encuestas que establecían un límite de 20 horas; se debería contar con las 14 estaciones de trabajo ya que en la realidad no siempre cada terminal trabaja ininterrumpidamente.

Se establece que el tiempo de asignación a los clientes internos para la navegación por Internet es el adecuado ya que en los casos de capacidad máxima y mínima existe un saldo positivo.

3.2.1.3.- Análisis de la seguridad lógica del sistema:

Para la elaboración de la matriz de seguridad se ha basado en el tipo de cliente que rodea al problema tomando en cuenta:

- ◆ Asignación y cambio periódico de passwords.
- ◆ Restricciones de tiempo para entrar al sistema.
- ◆ Incluye también la asignación de “capacidades” de acceso a escritura.
- ◆ Identificación de “dueños” de los archivos, quienes decidirán a quiénes le otorgan las capacidades antes descritas.

a) Establecimiento de ITOS.

Esto se basa en la determinación de campos de acción y responsabilidad de acuerdo al tipo de administrador de procesos.

a.1. Administrador nivel 1

Es el responsable de todo lo que pase y deje de pasar con el sistema teniendo este acceso total al sistema como son sus claves y bases de datos de los demás clientes que rodean al ámbito del Sistema. Esta función la cumple el Jefe de Laboratorios de Informática ITSA

a.2. Administrador nivel 2

Este se encuentra encargado de:

Dar mantenimiento de la base datos de los clientes internos, entendiéndose por mantenimiento alta, modificación y consulta.

Verificación del estado actual del Laboratorio en cuanto a la situación de los terminales.

a.3. Administrador nivel 3

Esta encargado del dar de alta a los clientes externos, entendiéndose por alta a la asignación de claves a los usuarios externos. Estas funciones las cumple el administrador de la sección de pagaduría del ITSA.

a.4. Administrador nivel 4

Su límite de acción esta delimitado a consultas acerca del estado actual del Laboratorio de Internet. Estas funciones las cumplen los ayudantes del Laboratorio

a.5. Administrador nivel 5

Su límite de acción esta delimitado a consultas acerca de la administración económica y situación actual del Laboratorio de Internet.

b) MATRIZ SEGURIDAD LOGICA DEL SISTEMA DE ADMINISTRACIÓN Y CONTROL DEL ACCESO A LA WEB

Administrador / Tipo de Acceso	ABC, de Administradores	ABC de usuarios	ABC; de Estaciones de trabajo	Venta de Ticket	Reportes	Control Estado del laboratorio	Cambio de clave
Web Master	si	no	Si	no	si	si	si
Administrador nivel 2	no	si	No	no	si	si	si
Administrador nivel 3	no	no	No	si	si	no	si
Administrador nivel 4	no	no	No	no	si	si	si
Administrador nivel 5	no	no	No	no	si	si	si

3.2.1.4.- ESPECIFICACIÓN DE REQUISITOS DEL SISTEMA ERS

Los parámetros que debe cumplir el sistema de acuerdo a la información obtenida de los procesos anteriores a través de las encuestas se basa en cuanto al tipo de cliente que rodea al problema.

3.2.1.4.1.- Requisitos usuario

a) Requisitos del Administrador nivel 1 del laboratorio de Internet

El sistema deberá permitir al administrador nivel 1 del laboratorio de Internet del ITSA:

Ingreso de los diferentes tipos de administradores del sistema dependiendo del tipo de acceso a los diferentes módulos.

Reportes del estado actual del laboratorio

Consultar y modificar los datos de los diferentes tipos de administradores.

Visualizar el estado económico del rendimiento del laboratorio

Visualizar reportes sobre la cantidad de clientes ingresados ya sean estos alumnos, profesores y usuarios externos, el tiempo de navegación otorgado, la fecha de ingreso y el nombre del administrador que realizó dicho cambio.

Cambio de la clave del súper administrador.

Modificar el precio del alquiler del tiempo de Internet.

b) Requisitos del Administrador nivel 2 del laboratorio de Internet

El sistema deberá permitir al Administrador de nivel 2:

Controlar el acceso a las máquinas desde el servidor a fin de poder bloquear una sesión de Internet.

Ingresar, consultar y modificar cliente internos del Laboratorio de Internet del ITSA

Tener acceso a las estadísticas del sistema referentes a los diferentes tipos de usuarios

Visualizar reportes sobre la cantidad de clientes ingresados ya sean estos alumnos y profesores.

Consultar el tiempo consumido tanto por alumnos, profesores y usuarios externos

Una interfase basada en páginas de Internet que faciliten el mantenimiento y operación del Laboratorio de Internet

Un control automático del acceso a las terminales para controlar los tiempos de uso y bloquear una estación cuando su tiempo haya culminado.

Conocer la duración y estado de las sesiones que se realizan desde las estaciones.

Cambio de la clave del administrador.

c) Requisitos del Administrador nivel 3.

El sistema deberá permitir: La opción de facturación para concepto de emisión del ticket de alquiler del servicio de Internet, consistirá en los siguientes datos:

RUC: Registro Único de Contribuyente este número pertenece al ITSA

Tiempo.- El solicitado por el cliente

Saldo.- Tiempo en minutos que dispone el cliente para navegar actualmente.

Saldo Total.- Es la suma del tiempo solicitado más el saldo actual.

Administrador.- Es el nombre de la persona que dará de alta a la modificación.

Costo Hora .- Es el valor a pagar por el tiempo solicitado, el cálculo para este cobro se lo realiza en base a una regla de tres con los siguientes datos:

60 minutos de Internet \$ 1 (un dólar)
 tiempo solicitado de Internet X

Función:

$$X = \frac{\text{tiempo_solicitado_internet} * 1}{60}$$

IVA.- Es el valor del impuesto a pagar al estado, calculado del 12% del costo del tiempo de navegación solicitado.

Costo Total.- Es la suma del valor costo más el valor IVA

Fecha Hora.- Es la fecha y hora en la cual se expide el ticket para el usuario.

Como se indica en la siguiente figura:

RUC :0591705393001			
Tiempo	Saldo	Saldo Total	Administrador
60	300	360	Miguel Yachimba
Costo Hora	IVA	Costo Total	Fecha Hora
1.00	0.120	\$1.12	2003-10-14 19:43:11

Figura 07 Ticket solicitado por el Administrador Nivel 03

Emitir reportes sobre el número de clientes, el tiempo otorgado y el total de los valores cobrados por él.

Una interfase basada en páginas de Internet que faciliten el mantenimiento y operación del Laboratorio de Internet

Cambio de la clave del administrador.

d) Requisitos del Administrador nivel 4

El sistema deberá permitir:

Un control automático del acceso a las terminales para controlar los tiempos de uso y bloquear una estación cuando su tiempo haya culminado.

Conocer la duración y estado de las sesiones que se realizan desde las estaciones.

Cambio de la clave del administrador.

e) Requisitos del Administrador nivel 5

El sistema deberá permitir:

Visualizar reportes sobre la cantidad de clientes ingresados ya sean estos alumnos, profesores y usuarios externos, el tiempo de navegación otorgado, fecha de ingreso y el nombre del administrador que realizó dicho cambio

Visualizar reportes sobre saldos, e ingreso económico del Laboratorio de Internet.

Consular el tiempo consumido tanto por alumnos, profesores y usuarios externos

Cambio de la clave del administrador.

f) Requisitos del cliente interno.

El sistema permitirá a los usuarios:

Realizar la validación en el sistema para iniciar la navegación en Internet.

No activar la estación para la navegación por Internet a menos que realice la validación del usuario.

Definir la duración de la sesión con el límite de dos horas diarias para la navegación:

Mostrar en una ventana el estado de su cuenta de navegación.

Mostrar en una ventana el control del tiempo de navegación, esta ventana aparecerá automáticamente cuando queden 5 minutos en la sesión y cada 30 segundos cuando falte menos de 2 minutos.

Ampliar el tiempo de la sesión y al cerrar la sesión el sistema indicará la duración de la sesión y el saldo de su cuenta de navegación.

3.2.1.4.2.- Requerimientos hardware

- Un computador Pentium con 700MHZ de velocidad.
- 256 KB de memoria RAM.
- Drive 3 1/2.
- CD-ROM.
- Disco duro con sistema operativo Linux RED HAT 9.0.
- 02 Tarjetas de red.

El requerimiento de memoria es importante ya que el servidor deberá ejecutar MySql, el servidor Web Apache y adicional soportar una carga de trabajo de 12 horas de trabajo diarias.

3.2.1.4.3.- Requerimientos Software

- Sistema operativo Linux Red Hat 9.0
- Servidor de bases de datos MySql
- Servidor de Internet Apache.
- Lenguaje de Programación PHP.

3.2.2.- DISEÑO Y DESARROLLO DEL “SISTEMA DE ADMINISTRACIÓN Y CONTROL DEL ACCESO A LA WEB”

Esta fase de diseño comprende de:

- Definición de clases y objetos del “Sistema de Administración y Control del Acceso a la Web”.
- Modelo Conceptual del “Sistema de Administración y Control del Acceso a la Web”.
- Diagrama de casos de uso.
- Estrategia para el Diseño del Sistema de Administración y Control del Acceso a la Web”.
- Desarrollo del modelo solución al problema de la Administración y Control del Acceso a la Web.
- Diseño de seguridades del “Sistema de Administración y Control del Acceso a la Web” para evitar la violación de la información
- Codificación de cada una de las unidades del “Sistema de Administración y Control del Acceso a la Web”

3.2.2.1.- Definición de clases y Objetos del Sistema de Administración y Control del Acceso a la Web.

a) Objeto: Alumnos, Profesores, Personal de Planta, Usuarios Externos

Clase: usuario.

Atributos: id, tipo _ usuario, login, password, nombre, escuela, nivel, tiempo, dia_navegacion, cupo_diario, cupo_temporal, administrador, fecha_ingreso.

Operaciones: Ingresar, consultar, modificar, eliminar.

b) Objeto: Administrador nivel1, Administrador nivel 2 Administrador nivel 3 Administrador nivel 4, Administrador nivel 5.

Clase: Administrador.

Atributos: id, tipo _ administrador, login, password, nombre, estado, administrador, fecha_ingreso.

Operaciones: Ingresar, consultar, modificar, eliminar.

c) Objeto: Terminal.

Clase: estaciones.

Atributos: id, nombre, num_ip, estado, usuario, inicio, limite, duración.

Operaciones: Ingresar, consultar, modificar, eliminar.

d) Objeto: Sesion.

Clase: sesion.

Atributos: num_sesion, tiempo, usuario, fecha.

Operaciones: consultar.

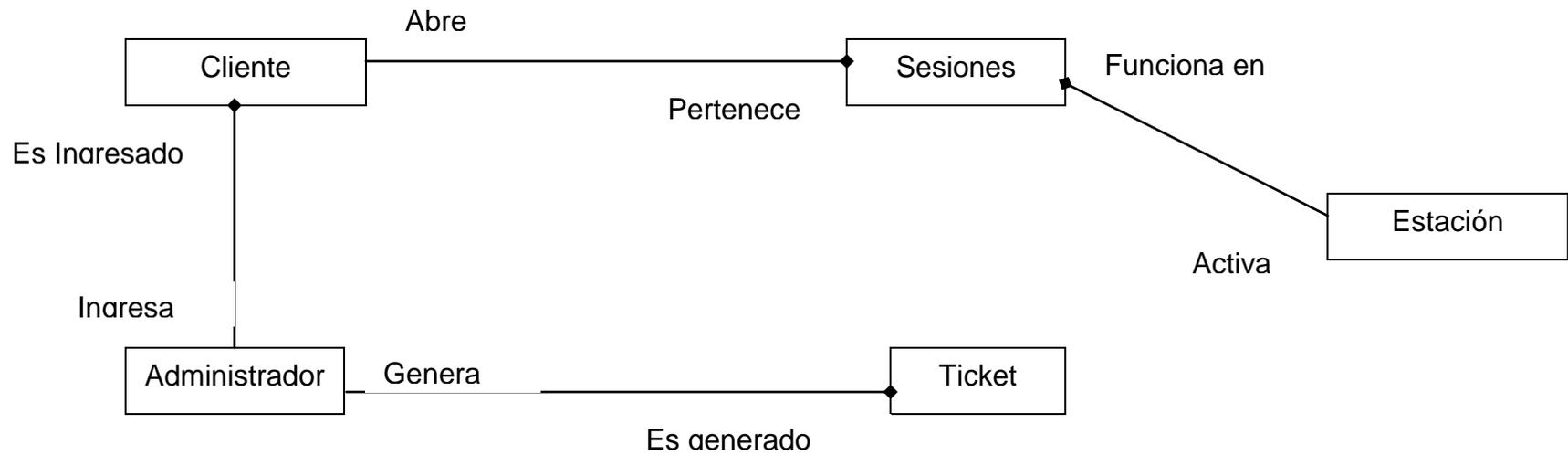
e) Objeto: Ticket.

Clase: ticket.

Atributos: num_ticket, tiempo, administrador, costo _ hora, IVA, costo_total, fecha.

Operaciones: Ingresar, consultar.

3.2.3.2 Modelo Conceptual del “Sistema de Administración y Control del Acceso a la Web”.



3.2.2.4.- Estrategia para el Diseño del Sistema de Administración y Control del Acceso a la Web”.

Para esta fase del diseño del sistema se ha tomado de la estrategia de **“DIVIDE Y VENCERÁS”** es así que al sistema se lo ha segmentado en subsistemas.

a) Modulo del Súper Administrador

- Ingreso de usuarios administradores en los diferentes niveles
- Consulta y modificación de los datos de los usuarios administradores del sistema.
- Reportes del ingreso económico por concepto del servicio de Internet.
- Reporte del estado actual del Laboratorio
- Ingreso de terminales al sistema (ABC)

b) Modulo del Administrador del nivel 2

Este comprende de:

- Modulo de alumnos
 - Ingreso de alumnos
- Modulo personal planta
 - Ingreso del personal de planta
- Módulo consulta de clientes
 - Modificación de los datos del cliente.
- Módulo reporte estado administrador
 - Cambio de clave
 - Reporte de clientes ingresados.
- Módulo estado actual del laboratorio
 - Cerrar la sesión en un determinado terminal
 - Visualización de la hora inicio y hora fin de una sesión

c) Modulo del Administrador del nivel 3

Del análisis del problema se ha determinado que la sección de pagaduría será la encargada del ingreso de los usuarios externo, por lo que este módulo comprende:

- Ingreso de clientes nuevos
- Ampliación del tiempo de navegación en clientes antiguos
- Emisión de ticket por el alquiler del servicio de Internet.
- Módulo reporte estado administrador
 - Cambio de clave
 - Reporte de clientes ingresados.
 - Reporte económico de los tiempos otorgados a los clientes.

d) Modulo del Administrador del nivel 4

Reporte del estado actual del Laboratorio de Internet.

Cambio de Clave

e) Modulo del Administrador del nivel 5

Reporte económico de los ticket emitidos por el administrador encargado

3.2.2.5.- Desarrollo del modelo solución al problema de la Administración y Control del Acceso a la Web.

a) Desarrollo modelo cliente servidor

El cliente en el terminal (sin importar el sistema operativo del Cliente) envía la petición de comunicación al servidor de paginas WEB a través del browse de Internet (este esta configurado con la dirección electrónica del servidor) :El servidor de paginas WEB Apache devuelve una pagina WEB realizada en php que consiste en un formulario de acceso al sistema, el cliente ingresa su número de cédula y clave de acceso y envía esta información por la URL al servidor, el cual recibe la pagina con los datos para validarlos con los datos del servidor de base de datos MySql, si los datos no son los correctos se presentara una pagina

de error en caso contrario el servidor envía un segundo formulario donde constan los datos del cliente como su saldo de navegación semestral y el cupo diario de navegación.

Este segundo formulario se envía al servidor de paginas Web: el tiempo que desea navegar, este analiza el valor del tiempo enviado con el valor del tiempo del cliente de la base de datos y si el dato cumple con los respectivos políticas este se muestra una pagina de inicio y una ventana de inicio de sesión y el cliente podrá ingresar al Internet quedando establecida de esta forma la comunicación cliente servidor.

b) Diseño de la comunicación cliente servidor, para el respectivo envío y recepción de mensajes.

Una vez establecida la comunicación es necesario indicar al cliente el estado actual de la misma, esto se logrará a través de la ventana de información de comunicación.

Para lo cual el cliente envía la petición de conexión con el servidor a través de la URL, si ya existe conexión cliente servidor este devuelve una ventana de información de sesión que contiene el estado actual de la conexión, con las opciones de cerrar la comunicación o ampliar la misma.

Si el cliente envía la información de cerrar la comunicación con el servidor, este responde con un mensaje de confirmación del mensaje, si la respuesta por parte del cliente es afirmativa el servidor cierra la comunicación enviando un una pagina donde se indica al cliente que la comunicación a finalizado.

Si el cliente envía la información de ampliar la comunicación con el servidor, este responde enviando un formulario donde el cliente enviará el tiempo para ampliar la comunicación, el servidor recibe esta información y procede a ampliar el tiempo de la comunicación con el cliente enviando el mensaje del tiempo en que se ha ampliado la comunicación.

c) Diseño firewall

El Ruteador en el Sistema de administración y Control del acceso a la WEB tomará las decisiones de rehusar y permitir el paso de cada uno de los paquetes que son recibidos, basándose en la revisión de información de los encabezados IP, si estos no corresponden a las reglas, se descarta o desplaza el paquete

Políticas del Firewall.-

La primera política del firewall es denegar todo y a partir de esto ir generando las nuevas reglas que serán aceptadas las cuales se basan en:

Perímetro de defensa

- Validación de estaciones

Permite al administrador de la red definir un (embudo) manteniendo al margen los usuarios no-autorizados fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques.

- Rechazo de paginas no autorizadas con contenido pornográfico
- Enmascaramiento de todas las direcciones ip de la red 192.168.1. X a través de la dirección 192.168.1.1.
- Validación de administradores, y de usuarios del Laboratorio de Internet.

3.2.2.6.- Diseño de seguridades del “Sistema de Administración y Control del Acceso a la Web” para evitar la violación de la información

- Diseño claves de acceso
- Clave encriptada para el súper administrador
- Clave en el sistema operativo
- Clave de acceso al los diversos módulos del sistema

- Las claves serán dadas por el sistema a través de la generación de números randomicos

3.2.2.7.- Codificación de cada una de las unidades del “Sistema de Administración y Control del Acceso a la Web

- Código Fuente Módulo del Web Master
- Código Fuente Módulo Administrador Nivel 2
- Código Fuente Módulo Administrador Nivel 3
- Código Fuente Módulo Administrador Nivel 4
- Código Fuente Módulo Administrador Nivel 5

3.2.3 PRUEBAS DEL “SISTEMA DE ADMINISTRACIÓN Y CONTROL DEL ACCESO A LA WEB”

3.2.3.1.- Diseño del plan de pruebas

Esta fase comprende en elaborar ejercicios de prueba y llevarlos a una matriz de comprobación como se indica a continuación

a) Ejercicios de entrenamiento a los usuarios.

Navegar por 10, 20, 30 y dos horas.

Abrir 3 sesiones al mismo tiempo en terminales distintos

Cambiar su clave 3 veces

Ampliar su tiempo 2 veces consecutivas

b) Diseño del Plan de Contingencias Cliente

No Prueba	No Ventana	Acción	Resultado esperado	Resultado obtenido	
				+	-
01	C_0	Cliente_x digita dirección electrónica diferente a la pagina de registro Del Sistema WEBACCESS	Pagina no encontrada	X	
02	C_01	Cliente ingresa No Cédula erróneo	Usuario no valido	X	
03	C_01	Cliente digita No cédula correcto y clave de acceso incorrecta	Clave no valida	X	
04	C_01	Cliente digita No cédula correcto y clave de acceso correcta, en un día x	Ventana C_02 con la información del estado de cuenta del Cliente_x.	X	
05	C_02	Cliente digita tiempo a navegar > al saldo general de navegación semestral	Saldo no disponible intente otra vez	X	

06	C_02	Cliente digita tiempo a navegar menor al saldo genera y > al cupo diario de navegación	Cupo diario de navegación no disponible intente otra vez	X	
07	C_02	Cliente digita tiempo a navegar menor o igual a cero	Ingrese un valor positivo mayor igual a cinco	X	
08	C_02	Cliente digita tiempo a navegar mayor o igual a cinco, menor igual al cupo diario y saldo general de navegación.	Ventana C_03 con la información del estado de la sesión, seguido por la ventana que se vincula con la pagina web, www.itsafae.com.	X	
09		Cliente hace clic en el icono del Internet Explorer	Ventana C_04 con la información del estado actual de la sesión y ventana C_03	X	
10	C_04, C_03	Cerrar sesión	Ventana C_05 Confirmación de cierre de sesión	X	
11	C_05	Cliente responde afirmativamente al cierre de sesión	Cierre de la sesión y salida de la Ventana C_06 con información del tiempo de duración de la comunicación.	X	

12	C_05	Cliente cancela el cierre de sesión	Retorno a la Ventana C_05.	X	
13	C_04, C_03	Ampliar el tiempo	Elección del tiempo a navegar en la ventana C_06	X	
14	C_06	Tiempo a ser ampliado menor igual al cupo diario y menor saldo general de navegación.	Información del tiempo ampliado en ventana C_07	X	
15	C_06	Tiempo a ser ampliado menor igual cero o caracteres especiales.	Ventana C_05	X	
16	C_01	Cliente_n digita su No cédula correcto y clave de acceso correcta en el mismo día x	Ventana C_02 con la información del estado de cuenta del Cliente_x con el valor del saldo general y cupo diario de navegación descontado del tiempo navegado en sesiones anteriores en un mismo día.	X	
17	C_01	Cliente_n digita su No cédula correcto y clave de acceso correcta en un fecha diferente al día x	Ventana C_02 con la información del estado de cuenta del Cliente_x con el valor del saldo general descontado del tiempo navegado en sesiones anteriores y cupo diario de navegación actualizado.	X	

18	C_01	Cliente_n digita su No cédula correcto y clave de acceso correcta en estaciones diferentes	Ventana C_02 con la información del estado de cuenta del Cliente_x.	X	
----	------	--	---	---	--

c) Ejercicios de entrenamiento al Web Master

Ingresar, consultar, buscar y modificar 10 administradores.

Ingresar, consultar, buscar y modificar 10 estaciones de trabajo.

Cambiar 3 veces su clave.

d) Diseño del Plan de Contingencias Web Master

No Prueba	No Ventana	Acción	Resultado esperado	Resultado obtenido	
				+	-
01	W_M_0	Web Master digita dirección electrónica diferente a la pagina de administración Del Sistema WEBACCESS	Pagina no encontrada	X	

02	W_M_01	Web Master ingresa login erróneo	Usuario no valido	X	
03	W_M_01	Web Master digita login correcto y clave de acceso incorrecta	Clave no valida	X	
04	W_M_01	Web Master digita login correcto y clave de acceso correcta.	Ventana C_02 con la información del menú de Súper administrador.	X	
05	W_M_02	Web Master da clic en la opción administradores.	Ventana W_M_03 con el menú de administradores	X	
06	W_M_03	Web Master elige la opción para ingresar administradores	Ventana W_M_04 con el casillero para ingresar el login del administrador	X	
07	W_M_04	Web Master digita el login del administrador a ingresar	Ventana W_M_05 con el formulario para llenar los datos del nuevo administrador	X	
08	W_M_05	Web Master elige la opción ingresar administrador.	Ventana C_06 con el mensaje de administrador ingresado.	X	

09	W_M_03	Web Master elige la opción para buscar administradores	Ventana W_M_04 con el casillero para ingresar el login del administrador	X	
10	W_M_04	Web Master digita el login del administrador a buscar	Ventana W_M_06 con el formulario con los datos del administrador	X	
11	W_M_03	Web Master elige la opción para modificar administradores	Ventana W_M_04 con el casillero para ingresar el login del administrador	X	
12	W_M_04	Web Master digita el login del administrador a modificar	Ventana W_M_07 con el formulario con los datos del administrador y la opción para modificarlos.	X	
13	W_M_02	Web Master da clic en la opción estaciones	Ventana W_M_08 con el menú de estaciones	X	
14	W_M_08	Web Master elige la opción para ingresar estaciones	Ventana W_M_09 con el casillero para ingresar la dirección IP de la nueva estación	X	
15	W_M_09	Web Master digita la dirección IP de la estación a ingresar	Ventana W_M_10 con el formulario para llenar los datos de la nueva estación	X	

16	W_M_10	Web Master elige la opción ingresar estación.	Ventana C_11 con el mensaje de estaciones ingresada.	X	
17	W_M_08	Web Master elige la opción para buscar estación	Ventana W_M_09 con el casillero para ingresar la dirección IP de la estación	X	
18	W_M_09	Web Master digita la dirección IP de la estación a buscar	Ventana W_M_12 con el formulario con los datos de la estación	X	
19	W_M_08	Web Master elige la opción para modificar estaciones	Ventana W_M_09 con el casillero para ingresar la dirección IP de la estación	X	
20	W_M_09	Web Master digita la dirección IP de la estación a modificar	Ventana W_M_13 con el formulario con los datos de la estación y la opción para modificarlos.	X	
21	W_M_02	Web Master da clic en la opción Estado Actual.	Ventana W_M_14 con el menú del estado del laboratorio.	X	
22	W_M_14	Web Master elige la opción últimas sesiones	Ventana W_M_15 muestra las últimas diez sesiones en el terminal seleccionado	X	

23	W_M_15	Web Master digita número de sesiones que desea visualizar	Ventana W_M_16 muestra las sesiones en el terminal seleccionado	X	
24	W_M_14	Web Master elige la opción cerrar sesion.	Ventana W_M_17 con el mensaje de confirmación de cierre de conexión.	X	
25	W_M_17	Web Master responde afirmativamente	Ventana W_M_18 información de la sesión	X	
26	W_M_17	Web Master responde negativamente	Ventana W_M_14	X	
27	W_M_02	Web Master da clic en la opción Reportes.	Ventana W_M_15 con el menú de los reportes a visualizar.	X	
28	W_M_15	Web Master elige la opción fecha	Ventana W_M_16 formulario con la fecha a elegir para el reporte.	X	
29	W_M_16	Web Master elige fechas correctas para el reporte.	Ventana W_M_17 informe de los clientes ingresados en la fecha elegida	X	
30	W_M_02	Web Master elige opción cambiar clave.	Ventana W_M_18 formulario para el ingreso de nueva clave.	X	

31	W_M_18	Web Master ingresa clave diferente en los casilleros.	Ventana W_M_18 setfocus retorna al primer casillero.	X	
32	W_M_18	Web Master ingresa claves idénticas entre los casilleros.	Ventana W_M_19 mensaje su clave se ha cambiado con éxito.	X	

e) Ejercicios de entrenamiento al Administrador nivel 2.

Ingresar, consultar, buscar y modificar 10 usuarios (alumnos y profesores)

Cambiar 3 veces su clave

f) Diseño del Plan de Contingencias Administrador Nivel 2.

Anexo III

g) Diseño del Plan de Contingencias Administrador Nivel 3

Anexo IV

h) Ejercicios de entrenamiento al Administrador nivel 3

Ingresar, 10 usuarios.

Ampliar a 10 usuarios su saldo de Internet.

Cambiar 3 veces su clave.

3.2.4 IMPLANTACIÓN DEL SISTEMA.

Esta fase incluye:

Conferencia a los clientes internos.

Configuración del servidor.

Instalación del Sistema de Administración y Control del acceso a la WEB con herramienta Open Source.

a) Conferencia a los clientes internos.

A fin de explicar el funcionamiento del módulo cliente del laboratorio de Internet

b) Configuración del servidor.

Para esto se deben instalar algunos programas en el servidor como son:

Instalación y Configuración del Servidor Apache, Modulo Php y MySql

ANEXO V

c) Instalación del Sistema de Administración y Control del acceso a la WEB con herramienta Open Source.

c.1. Consideraciones previas a la instalación.

Configuración de la red local

Configuración de las tarjetas de red del servidor

Ethernet 01: 192.168.1.1 .- Para la red de aérea local del Laboratorio de Internet

Ethernet 02: 10.255.5.98.- Para la salida hacia el Internet.

1.1.- Configuración de las estaciones de trabajo.

A partir de la dirección 192.168.1.2 hasta la dirección 192.168.1.25

- **Dirección ip:** 192.168.1.n
- **Máscara:** 255.255.255.0
- **Puerta de enlace o gateway:** 192.168.1.1
- **DNS:** 192.168.1.1.

La puerta de enlace o gateway corresponde a la dirección del servidor Linux donde se encuentra el sistema webaccess

El DNS debe ser activado para que funcionen todos los servicios de Internet desde las estaciones (p.e. Telnet, FTP, etc).

3.2.5 DOCUMENTACIÓN DEL “SISTEMA DE ADMINISTRACIÓN Y CONTROL DEL ACCESO A LA WEB”

Esta fase incluye:

- Manual del Administrador del “Sistema de Administración y Control del Acceso a la WEB”

Consta de 5 manuales que se encuentran en el CD de la tesis en la carpeta manuales los cuales se detallan a continuación:

Web Master
 Administrador nivel 2
 Administrador nivel 3
 Cliente
 Indicaciones Generales

- Código Fuente del “Sistema de Administración y Control del Acceso a la WEB”
- Plan de pruebas del “Sistema de Administración y Control del Acceso a la WEB”

IV DESARROLLO DEL PLAN DE CONTINGENCIA

4.1 ANÁLISIS DEL PLAN DE CONTINGENCIA

4.1.1 INTRODUCCIÓN

Este plan se ha elaborado entre el 2002 y Enero de 2003 para el registro y control de la seguridad informática de los laboratorios de Informática del ITSA así como las contingencias que se pudieran producir con el SISTEMA DE ADMINISTRACION Y CONTROL DEL ACCESO A LA WEB y la administración de los laboratorios de Informática del Instituto Tecnológico Superior Aeronáutico.

Los laboratorios de informática del Instituto Tecnológico Superior Aeronáutico tienen por objetivo fundamental ser el lugar de trabajo para la practica de distintas actividades docentes que se desarrollan en las diferentes Escuelas como son las de Mecánica, Logística y Telemática.

A la vez trata de ayudar a los estudiantes que no poseen un computador para realizar sus tareas y deberes, convirtiéndose de esta manera en un centro de soporte tecnológico y pedagógico para todos los miembros de la facultad.

La definición de los Laboratorios de Informática del Instituto Tecnológico superior Aeronáutico indica que son una unidad de servicio a la docencia, investigación, extensión y administración académica, adscrito al Vicerrectorado Académico.

4.1.2 OBJETIVO ÁMBITO Y RESULTADOS ESPERADOS:

- Establecer las medidas organizativas y técnicas para asegurar la integridad, disponibilidad y confidencialidad de información en soporte informático en el Instituto Tecnológico Superior Aeronáutico.
- Es aplicable al personal y equipos que intervienen en el mantenimiento de la función informática de los laboratorios de Informática del ITSA y contempla el software de base, al Sistema de Administración y Control del Acceso la Web así como accesos a áreas de uso restringido y el hardware.

Los Resultados esperados son: Establecer los controles necesarios en la función informática de los laboratorios de informática del ITSA y en el uso del Sistema Web Access con el fin de garantizar la integridad y confidencialidad de la información en soporte informático.

4.1.3 NORMAS DE OBLIGADO CUMPLIMIENTO PARA LA GESTIÓN DE USUARIOS:

Cada Usuario del Laboratorio de Internet dispondrá de:

- a) Una cuenta de Usuario al Sistema Web Access con acceso sólo a aquellos procesos del Sistema Web Access y/o datos a los que deba tener acceso, para lo cual se establecerán claves con vencimiento no más allá de 90 días.
- b) Horarios y equipos desde los que puede acceder al Sistema Web Access.
- c) Claves de acceso individual a cada una de las aplicaciones que requieran autenticación segura.

4.1.4 FUNCIONES DEL PERSONAL Y OBLIGACIONES GENERALES:

- Es responsabilidad de todos los usuarios del Sistema de:

- a) Entrar al Sistema con su clave, no anotar la misma en soporte papel y salir ordenadamente del sistema si piensa abandonar la estación de trabajo por un tiempo superior a 5 minutos.
- b) Entrar al Sistema por los equipos y accesos habilitados al mismo por el Responsable del Laboratorio de Internet.
- c) No realizar copias ilegales de software: No instalar aplicaciones ni nada ajenos a la Institución. Comunicar al Web Master del Sistema Web Access de las incidencias que ocurran con el mismo.
- d) El Web Master responsable de Informática, por su carácter especial, depositará todas las claves con permisos especiales de seguridad en la caja fuerte de la Organización en sobre cerrado con fecha y hora de actualización.
- e) Los accesos a las zonas: Sala del Servidor, Sala de Instalación de Concentración de Cable de Red están restringidos y sólo puede accederse mediante solicitud de permisos a Responsable de Informática y/o Mantenimiento.
- f) En Caso de fallo eléctrico general debe comunicarse con urgencia con el subalterno de semana (Supervisor general de la seguridad del ITSA, etc). Se procederá en caso de prolongarse por más de quince minutos con una parada en frío y ordenada de todos los sistemas informáticos. Este así como otros problemas del mismo tipo están descritos en el Plan de Contingencias Informáticas.

- g) Usar el correo electrónico sólo para su cometido en virtud de sus atribuciones laborales. Rechazar cualquier correo electrónico que no quede perfectamente identificada su procedencia.

La sección de los Laboratorios de Informática deberá realizar las siguientes tareas periódicamente:

a) Planificación Auditoria de PC's de todos los Laboratorios de Informática revisando los siguientes puntos:

- Aplicaciones instaladas. Ver mediante Panel de Control-Agregar o quitar programas. Anotar en la hoja del archivo correspondiente
- Desinstalar los juegos de Windows. Borrar los archivos Mshearts.exe, sol.exe y winmine.exe de la carpeta c:\windows. Anotar Pc's con juegos en archivo de incidencias de la auditoria.
- Actualizar/Anotar direcciones IP en la carpeta de Direcciones IP de Informes Técnicos y puntos de Cableado. Indicarlo también en las hojas de PC.
- Actualizar antivirus de todos los Pcs. Automatizar su actualización.

b) Auditoria del Sistema Web Access.

- El Sistema Web Access se someterán a una Auditoria Interna o Externa, que verifique el cumplimiento del presente Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, cada año.
- El informe de auditoria dictaminará sobre la adecuación de las medidas y controles al presente Reglamento, identificará sus deficiencias y propondrá las medidas correctoras o complementarias necesarias. Deberá, incluir los datos, hechos y

observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

- Solicitar a la Dirección:
 - a) El cumplimiento del presente plan de Seguridad así como de los Planes de Contingencias correspondientes.

4.1.5 FUNCIONES DEL PERSONAL Y OBLIGACIONES ESPECÍFICAS:

4.1.5.1.- Del Jefe de Laboratorios del Instituto Tecnológico Superior Aeronáutico.

- La función del jefe de los laboratorios de Informática es velar por el correcto funcionamiento del mismo, lo que incluye actividades de coordinación, administración distribución y calendarización de actividades de los coordinadores y auxiliares de los diferentes laboratorios.
- Elaborar la precuota presupuestaria anual, previendo necesidades de material de consumo, repuestos y accesorios, dotación de equipos y muebles, personal, mantenimiento de los equipos, sustitución por obsolescencia de los mismos, servicios a contratar, y demás que se consideren necesarios.
- Supervisar al personal del Laboratorio.

4.1.5.2.- Funciones del Coordinador del Laboratorio de Internet y Computación Básica:

- Controlar el uso de Internet y regulación (solo coordinador del laboratorio de Internet)

- Efectuar un elevamiento de satisfacción mensual según encuestas anexadas
- Informar a los superiores acerca de cualquier inconveniente que no pudiera solucionarse de forma inmediata
- Apoyar al correcto funcionamiento de los laboratorios

- Coordinar con las escuelas los horarios de uso de los laboratorios en las distintas carreras para evitar superposiciones horarias
- Instalación de software
- Mantenimiento de software
- Contactar a los docentes que tienen asignados laboratorios diariamente, receptando sus dificultades diarias y solucionándolas para la siguiente clase
- Delegar tareas a los ayudantes de turno
- Controlar las actividades de los ayudantes de su turno e informar inconvenientes al superior
- Brindar a cualquier usuario de los laboratorios ya sean docentes o alumnos una solución a los requerimientos de uso académico de los mismos
- Velar por el buen funcionamiento del Laboratorio.
- Planificar el uso de las diferentes aulas y llevar el control de las mismas.
- Establecer los procedimientos para la solicitud y control de uso del Laboratorio.
- Elaborar la precuota presupuestaria anual, previendo necesidades de material de consumo, repuestos y accesorios, dotación de equipos y muebles, personal, mantenimiento de los equipos, sustitución por obsolescencia de los mismos, servicios a contratar, y demás que se consideren necesarios.
- Elaborar un plan anual de mantenimiento preventivo para el Laboratorio.
- Reportar a la Dirección de Servicio, los daños y otras necesidades de mantenimiento correctivo.
- Sugerir al Jefe del Departamento de Laboratorios y Proyectos, candidatos para responsables académicos del Laboratorio.

- Llenar periódicamente, los formatos de evaluación del personal al servicio del laboratorio.
- Promover el desarrollo de actividades profesionales basadas en la informática.

4.1.5.2 Funciones del Coordinador del Laboratorio de Redes.

a) Funciones Generales

- Coordinar e instrumentar con las distintas cátedras, el desarrollo de los trabajos prácticos que requieren
- Atender las consultas de los alumnos y docentes en los temas relacionados
- Administrar el uso de los equipamientos del laboratorio, tanto por parte del cuerpo docente como de las distintas áreas del instituto
- Mantener en perfectas condiciones el equipamiento
- Instruir a los alumnos en el uso de los equipos
- Controlar el cumplimiento de las pautas para la realización de los trabajos prácticos y el uso académico de los mismos

b) Funciones Especificas.

- Reportar y documentar las fallas y problemas respecto al rendimiento técnico de los equipos de comunicaciones y llevar un registro de ellas.
- Integrar los distintos ambientes computacionales mediante enlaces de comunicación eficientes y ajustados a las necesidades de interconexión.
- Elaborar y mantener una lista actualizada de las actividades a desarrollar y un cronograma aproximado de cumplimiento de las mismas, previo acuerdo con el Jefe del Departamento de Cómputo y ajustados debidamente a los proyectos institucionales.

- Planear, elaborar y activar el plan de contingencia de la infraestructura de comunicaciones de datos de la institución.
- Planear y supervisar la ejecución del plan de mantenimiento de los equipos utilizados en su área.
- Estudiar los requerimientos de los usuarios en lo relacionado al hardware y software de comunicaciones suministrado por el instituto y asesorarlos en el uso de estas herramientas.
- Desarrollar, documentar y divulgar estándares y especificaciones para el uso de facilidades y sistemas de comunicación de datos en el Instituto.
- Probar los sistemas de comunicaciones de datos y evaluar los resultados.
- Mantener permanente actualización en las variaciones y novedades tecnológicas en comunicación de datos y en las normas legales y decretos que regulan las actividades a desarrollar en su área, así mismo como los diferentes estándares de la industria aceptados en nuestro país y universalmente.
- Evaluar las necesidades de reemplazo de los equipos de comunicación institucionales, emitiendo conceptos en cuanto a la compatibilidad, características técnicas, capacidades, garantías de mantenimiento y finalidades operativas.
- Mantener informado al Jefe Inmediato de todas las anomalías que se presenten en el desarrollo de sus tareas y suministrar la información que se requiere para tomar decisiones.
- Asesora al personal indicado, en la construcción de las diferentes interfaces y conectores que sean necesarios en la instalación, y para los cuales se tengan los recursos técnicos y materiales en la Universidad.
- Documentar y realizar la conexión, configuración y prueba de los distintos equipos de telecomunicaciones del instituto Tecnológico Superior Aeronáutico , como módems, bridges, routers, servidores, terminales, etc.

- Cumplir las demás funciones inherentes a su oficio y que le sean asignadas por autoridad competente.

4.1.5.3.- Del los Auxiliares o Asistentes de Laboratorios del Instituto Tecnológico Superior Aeronáutico

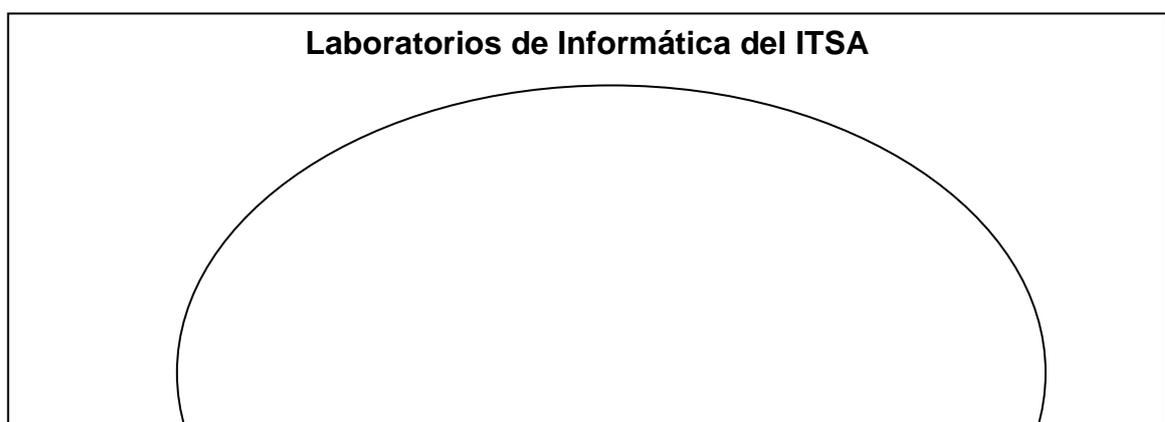
Estos deberán seguir las siguientes normas.

- Instalación de estaciones de trabajo
- Verificación del correcto funcionamiento de las estaciones de acuerdo a los requerimientos académicos
- Atención a las consultas de los docentes y alumnos
- Transportar equipamiento a las aulas
- Mantener la limpieza y el orden en los laboratorios
- Controlar contenidos inapropiados en los discos de las estaciones así también como periódicamente realizar un mantenimiento de software en las mismas
- Dejar en condiciones operativas los laboratorios antes del comienzo de la clase
- Mantener el inventario de los laboratorios actualizado
- Recibir las planillas de solicitud de cuentas de Internet y asesor para su instalación

4.2 IDENTIFICACIÓN DE LOS PROCESOS CRÍTICOS DEL NEGOCIO

4.2.1 OBTENCIÓN DEL MAPA DE SERVICIOS

Mapa del negocio



LAB_INTERNET

LAB_REDES

LAB_COMPUTACION
BASICA

4.2.2 IDENTIFICACIÓN DE SERVICIOS CRÍTICOS.

La garantía de un servicio se basa en la identificación de los mismos es así que se tiene:

4.2.2.1 Tipos de servicio de la unidad

Servicios finales de los Laboratorios de Informática del ITSA.

- Internet.
- Impresiones.

Servicios internos de los Laboratorios de Informática del ITSA.

- Mantenimiento de estaciones de trabajo del Laboratorio de Internet, Redes y Computación Básica.

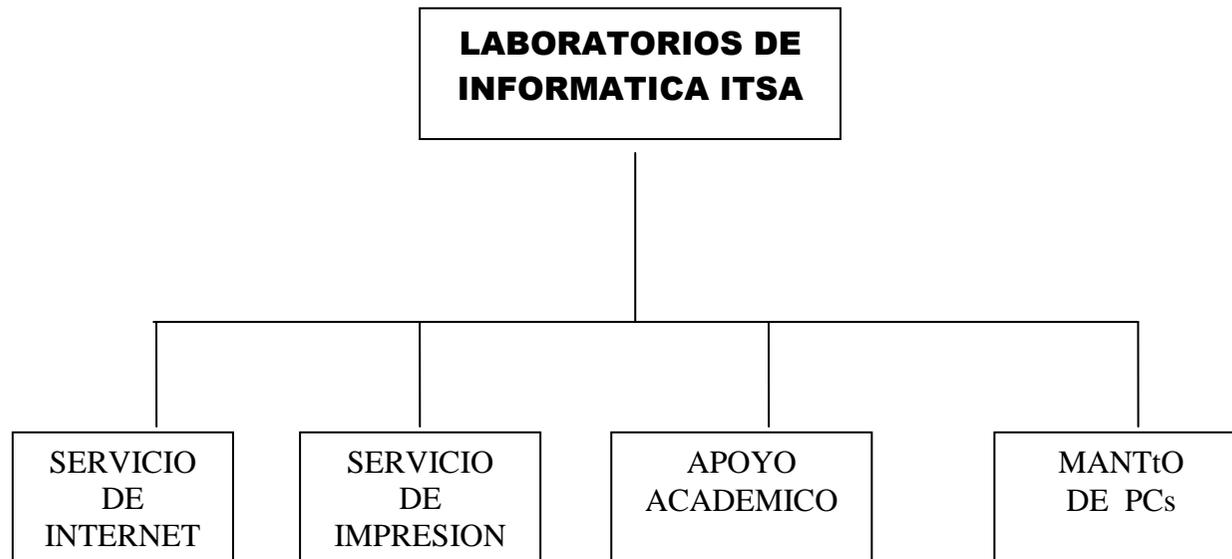
Servicios críticos de los Laboratorios de Informática del ITSA.

- Internet
- Impresiones
- Mantenimiento de los PCs

Servicios auxiliares de los Laboratorios de Informática del ITSA.

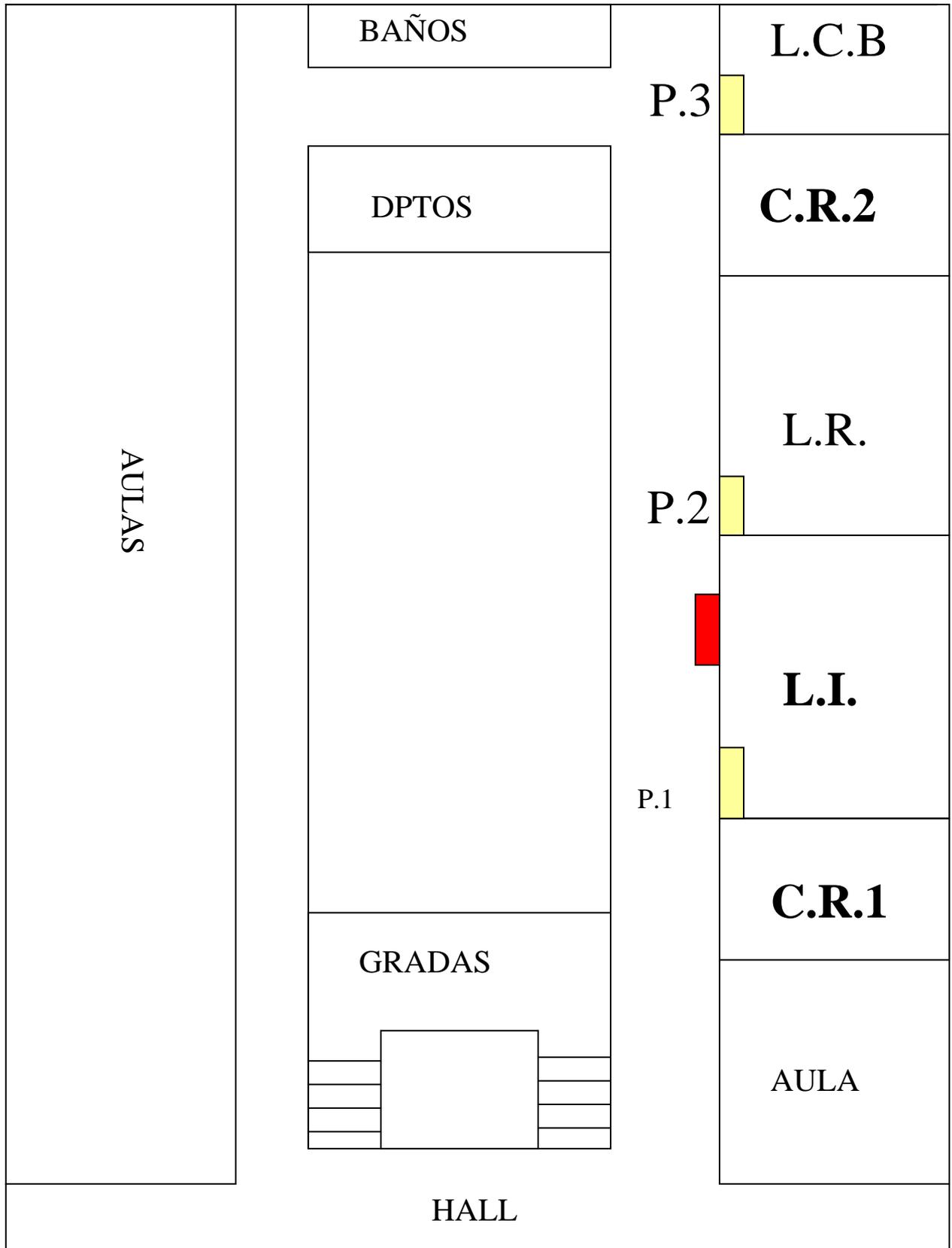
- Accesorio técnico en lo relacionado a temas informáticos a los departamentos adjuntos al mismo.

Mapa de



4.2 ANÁLISIS DE LA SEGURIDAD FÍSICA

4.3.1 DIAGRAMA DE LA UBICACIÓN DE LOS LABORATORIOS DE INFORMATICA DEL INSTITUTO TECNOLÓGICO SUPERIOR AERONÁUTICO



4.3.2 ACCESO A LAS OFICINAS Y LABORATORIOS.

Puertas cuentan con doble seguridad de llaves las cuales las poseen todos los que laboran en dicha sección.

Ventoleras las cuales pueden ser fácilmente desinstaladas.

Sistema contra incendios el cual se encuentra ubicado a 5 m de la puerta del laboratorio de Internet

4.3.3 RECURSOS CON LOS QUE CUENTAN LOS LABORATORIOS DE INFORMATICA DEL ITSA.

4.3.3.1.- HARDWARE

- 37 PCs Intel Pentium I, II,III.
- Cableado estructurado para 27 terminales
- 01 Rack de piso de 5 pies
- 01 Switch D-LINK de 100 Mbps.
- 01 Antena Satelital.

4.3.3.2.- SOFTWARE.

- Windows 95
- Linux Red Hat 9.0
- Sistema de Administración y Control del Acceso al Internet.
- Antivirus F-Prot
- Office 97.

4.3.3.3.- COMUNICACIONES

- 01 Línea telefónica interna (ext 437)

4.3.3.4.- HUMANO

- 01 Analista Informática
- 02 Tecnólogos en Informática
- 01 Aerotécnico con especialidad en Informática.
- 04 alumnos de telemática

4.3.3.5.- EQUIPAMIENTO

- 01 Laboratorio de Computación Básica
- 012 Laboratorio de Redes
- 01 Laboratorio de Internet
- 01 Oficina.

Adicionalmente el ITSA cuenta con una planta de energía eléctrica alterna que alimenta únicamente al primer y tercer piso.

4.4 DESARROLLO DEL PLAN DE CONTINGENCIA

4.4.1 SELECCIÓN DE LA ESTRATEGIA GLOBAL DE RESPALDO

La selección de la estrategia se ha basado en :

Identificación de eventos y análisis de alternativas de respaldo por evento

- Confección del Centro de Respaldo
- Función del Centro de Respaldo
- Distribución del centro
 - Personal técnico y Operadores
- Material auxiliar

4.4.1.1.- Identificación de eventos y análisis de alternativas de respaldo por evento

EVENTOS	TIME FRAME	TRspR	TAS	Trsp ACUM
1. Pérdida de la Antena del servicio de Internet Satelital	7 días	30 días	1 día	31 días
2. Desconexión del servicio de Internet por parte del proveedor		7 días	-	7 días
3. Desconfiguración del sistema operativo en un terminal.	1 día	2 días	1 día	3 días.
4. Desconfiguración de la red de área local		3 días	7 días	10 días
5. Desconfiguración del servidor		1 día	1 día	2 días

6. Desconfiguración del Sistemas WEB ACCESS		-	1 día	1 día
7. Robo del servidor, terminales e impresoras.		30 días	7 días	35 días
8. Daños irreparables de los terminales y/o servidor		30 días	7 días	35 días
9. Perdida de la base de datos del Sistema Web Access		No recuperable	-	-
10. Perdida de los archivos de los Laboratorios de Informática del ITSA		No recuperable	-	-

No- Evento	Identificación de alternativas	Selección
1.	<ul style="list-style-type: none"> • Compra de una nueva antena • Elaboración de una antena nueva 	<ul style="list-style-type: none"> • • Compra de una nueva antena
2.	<ul style="list-style-type: none"> • Comunicarse constantemente con el proveedor para el establecimiento de la conexión por parte del proveedor • Contactar un nuevo proveedor 	<ul style="list-style-type: none"> • • Comunicarse constantemente con el proveedor para el establecimiento de la conexión por parte del proveedor
3.	<ul style="list-style-type: none"> • Realizar configuración Básica para la red Lan • Formateo e instalación del sistema operativo. 	<ul style="list-style-type: none"> • Realizar configuración Básica para la red Lan • Formateo e instalación del sistema operativo

4.	<ul style="list-style-type: none"> • Realizar configuración básica de la red en los terminales • Formateo de los terminales 	<ul style="list-style-type: none"> • Realizar configuración Básica para la red Lan
5.	<ul style="list-style-type: none"> • Instalación del Sistema Operativo Linux Red Hat 9.0 	<ul style="list-style-type: none"> • Instalación del Sistema Operativo Linux Red Hat 9.0
6.	<ul style="list-style-type: none"> • Instalación del servidor de base de datos MySql • Instalación del servidor de paginas web Apache • Instalación del interprete de comandos PHP • Instalación del Sistema Web Access • Instalación de la base de datos de los clientes del sistema Web Access 	<ul style="list-style-type: none"> • Instalación del servidor de base de datos MySql • Instalación del servidor de paginas web Apache • Instalación del interprete de comandos PHP • Instalación del Sistema Web Access • Instalación de la base de datos de los clientes del sistema Web Access

7.	<ul style="list-style-type: none"> • Compra de nuevos Equipos. • Establecer nuevas medidas de seguridad. 	<ul style="list-style-type: none"> • Establecer nuevas medidas de seguridad.
8.	<ul style="list-style-type: none"> • Compra de nuevos Equipos. • Establecer nuevas medidas de seguridad. • Instalación y configuración de los sistemas. 	<ul style="list-style-type: none"> • Establecer nuevas medidas de seguridad. • Instalación y configuración de los sistemas.
9.	<ul style="list-style-type: none"> • Montar equipo de respaldos de base de datos del sistema Web Access. 	<ul style="list-style-type: none"> • Montar equipo de respaldos de base de datos del sistema Web Access.
10.	<ul style="list-style-type: none"> • • Montar equipo de respaldos de los archivos de los Laboratorios de Informática del Itsa. 	<ul style="list-style-type: none"> • • Montar equipo de respaldos de los archivos de los Laboratorios de Informática del Itsa.

Estrategias globales:

- Para el caso de cortes de energía eléctrica:
- Al poseer el ITSA una planta eléctrica con la ayuda de la extensión eléctrica alimentar al servidor y a 4 estaciones de trabajo desde el primer o tercer piso.
- Se ha designado al laboratorio de redes que posee 10 estaciones de trabajo los cuales tendrán dos sistemas operativos para que en el un sistema se configure para la conexión a la Internet y así este funciones como Laboratorio de Internet alternativo
- En todos las 17 estaciones de trabajo realizar 2 particiones con la siguiente distribución:
 - En la partición principal debe constar de l Sistema operativo y demás aplicaciones y en la partición secundaria los archivos de cada terminal.
 - Esto se lo realizará con el fin de que si se debe formatear el disco duro del terminal, no se pierdan los archivos.

4.4.2. CONFECCIÓN DEL CENTRO DE RESPALDO

4.4.2.1.- Función del Centro de Respaldo.

Este centro esta destinado para entrar en funcionamiento en cualquier situación de contingencia.

4.4.2.1.- Distribución del centro

Se lo ubicará en la oficina de Internet.

Su seguridad de acceso será con llave y las ventoleras deberán ser cubiertas con mallas metálicas.

Se aprovecha la existencia de la ext 437 para la comunicación.

4.4.2.1.1.- Personal técnico y Operadores

Analista Acuña Maria Eugenia.

4.4.2.3.- Material auxiliar

Discos removibles

01 caja disquetes

Mobiliario (02meseas 04sillas, 01 estanteria)

01 impresora lexmark z 55

01 impresora epson lx 300

4.3 IMPLANTACIÓN DEL PLAN

EN esta fase se ha determinado la estrategia global de respaldo la cual consiste en:

- Requerimientos previos.
- Fase de alerta
- Fase de transición
- Fase de recuperación
- Documentación del plan
- La vuelta a la normalidad

4.5.1. REQUERIMIENTOS PREVIOS.

Estos son importantes para asegurar la operatividad, la implantación y funcionalidad del plan de contingencias

4.5.1.1.- Catálogo de requerimientos previos a la implantación y puesta en marcha del plan.

- 01 Candado para la seguridad del CPU del servidor
- 01 Caja de seguridad para los respaldos de la documentación, catálogos, software y base de datos de los Laboratorios.
- 01 extensión eléctrica de 100 m con 05 tomas de para energía eléctrica con separación de 5m cada una.
- UPS con 5 minutos de almacenaje de energía eléctrica.
- 01 Caja de disquetes para respaldo de archivos y base de datos.
- 01 caja de CDs para respaldo de archivos y base de datos.

4.5.1.2.- Descripción de la estrategia de seguridad.

Para esta fase se describen los servicios a respaldar.

Internet.- Servicio que brinda el Laboratorio a los alumnos para que estos puedan realizar sus consultas investigativas

Software Base

Sistema Operativo Windows X.- Sistema instalado en los terminales para el acceso al Internet y demás tareas de investigación

Sistema Operativo Linux.- Sistema instalado en el Servidor para la implantación del Sistema de Administración y Control del Acceso a la Web.

Microsoft Office 97.- Aplicación para la realización de tareas administrativas.

Sistema Web Access.- Sistema de administración y control del acceso al Internet el cual esta conformado además por otras aplicaciones como son:

- Servidor de paginas Web APACHE
- Interprete de comandos PHP.
- Servidor de Base de Datos MySql.

Base de datos Web Access.- La base de datos de las cuentas de todos los usuarios del Internet del ITSA.

Archivos.- La documentación administrativa de los Laboratorios del ITSA.

Impresión.- Servicio mediante el cual los alumnos presentan sus trabajos elaborados.

4.5.1.3 Matriz de la seguridad del Sistema Web Access

Administrador / Tipo de Acceso	ABC, de Administradores	ABC de usuarios	ABC; de Estaciones de trabajo	Venta de Ticket	Reportes	Control Estado del laboratorio	Cambio de clave
Web Master	Si	no	si	no	si	si	si
Administrador nivel 2	No	Si	no	no	si	si	si
Administrador nivel 3	No	no	no	si	si	no	si
Administrador nivel 4	No	no	no	no	si	si	si
Administrador nivel 5	No	no	no	no	si	si	si

4.5.2. Organización de los equipos.

Equipo de Director.

Responsable: Analista acuña Maria Eugenia.

Equipo de Emergencia.

Responsable: Cbop.. Yachimba Miguel Angel

Equipo de Recuperación.

Responsable: Cbop. Yachimba Miguel Angel

Equipo de Seguridad.

Responsable: Analista acuña Maria Eugenia.

Equipo de Sistemas.

Responsable: Cbop. Yachimba Miguel Angel

Equipo de Coordinación de Logística.

Responsable: Cbop. Chilñuisa Nelson

Equipo de Comunicaciones

Responsable: Cbos. Moyota Antonio

Equipo de base de datos.

Responsable: Analista acuña Maria Eugenia.

4.5.2. ORGANIZACIÓN DE LOS EQUIPOS.

Equipos de emergencia:

Lista de contactos telefónicos de los miembros del centro de respaldo Informático del ITSA y teléfonos de Emergencia del ITSA.

Grado	Equipo	Nombre	Dirección	Teléfono
Analista	Director	Acuña Herrera Maria Eugenia	Pujilí: Calle Iván Salinas y Simón Bolívar	Ltga: 032723096 Uio: 022405640
Cbop.	Recuperación, Respaldos Sistema	Yachimba Espinosa Miguel Ángel	Ltga: Antonia Vela y Padre Semante.	098563225
Cbop.	Sistemas, Logística	Chiluiza Amaguaya Nelson Narciso	Cdla La Paz	097342823
Cbos.	Ayudante Laboratorios	Laverde Amores Bolívar Enrique	Pujilí: Barrio San Juan	098109906
Cbos.	Comunicaciones.	Moyota Anaguano José Antonio	Riobamba	
Almn.	Ayudante Laboratorios .	Vizute Carrasco Daniel Alfonsop	Riob: Av La Prensa y Olivos	032602073 Villa A-37
Almn.	Ayudante Laboratorios.	Gualotuña Churuchumbi Byron Patricio	Quito: La Pulida calle 6 lote 550	022298397 Villa Apache
Almn.	Ayudante Laboratorios	Ramos Guatumillo Franklin Danilo	Pelileo: Juan de Velasco y Quitus	2830120 Villa A-37

Equipo director

Funciones:

- Comunica las estrategias y procedimientos a seguir en caso de contingencia.
- Publicar y hacer conocer a todos los equipos de emergencia acerca de los cambios en el plan de contingencias de los Laboratorios de Informática del ITSA.
- Llevar el control de los servicios a respaldar.

Responsables:

Analista Acuña Maria Eugenia.

Cbop. Yachimba Miguel

Equipo de Recuperación.

Funciones:

- Coordinar con los demás equipos la recuperación de hardware y software para la reposición o equipamiento para el Cold backup.

Responsables

Cbop. Yachimba Miguel

Cbop. Chiluiza Nelson

Equipo de Seguridad.

Funciones:

- Implantar los controles de seguridad física en el Centro de Respaldos y Laboratorios de Informática del ITSA a fin de evitar perdidas materiales.
- Coordinar acciones conjuntas con el Departamento de seguridad Aérea y Terrestre del ITSA (ALA 12).

Responsables

Analista Acuña Maria Eugenia

Cbop. Chiluiza Nelson

Equipo de Coordinación de Logística.

Funciones

- Coordinar la adquisición de los repuestos y demás requerimientos de los Laboratorios de Informática del ITSA
- Coordinar acciones conjuntas con el Departamento de seguridad Aérea y Terrestre del ITSA (ALA 12).

Responsables:

Cbop. Chiluzza Nelson.

Cbos. Laverde

Equipo de Sistemas.

Este equipo laborara en dos fases que son:

Al servidor:

Funciones:

- Poner operativo al sistema operativo del servidor así como al Sistema de Administración y Control del Acceso a la Web.
- Actualizar el antivirus del sistema operativo semanalmente.

Responsable.

Cbop. Yachimba Miguel

Cbos. Moyota Antonio.

A los terminales

Función:

- Poner operativos los sistemas informáticos de los terminales de los Laboratorios de Internet, Redes y Computación Básica, así como el software base de los mismos
- Actualizar el antivirus del sistema operativo semanalmente.
- Revisar que las aplicaciones instaladas en las estaciones de trabajo sean las autorizadas, diariamente.

Responsables:

1. Cbop. Chiluzza Nelson.
2. Cbos. Moyota Antonio.
3. Cbos. Laverde
4. Almn Gualotuña
5. Almn Ramos
6. Almn Vizquete

Grupo de Comunicaciones.**Función**

- Establecer y comprobar la red de telefonía existente.
- Actualizar la lista de contactos telefónicos de los miembros del Centro de Respaldo del ITSA y teléfonos de emergencia.

Responsables:

Cbos. Moyota

Almn Gualotuña.

Grupo de Base de datos.**Funciones:**

- Velar por la integridad de los datos de la Base de datos que maneja el Sistema de Administración y Control del Acceso a la Web.
- Sacar respaldos de la Base de Datos y archivos relacionados con el Laboratorio de Informática del ITSA en los soportes de backup y mantener 1 copia consigo y otra en la caja de seguridad de Bases de datos.

Responsables

Analista Acuña Maria Eugenia.

Cbop. Yachimba Miguel

4.5.3 Desarrollo de los procedimientos operativos.

- Fase de alerta
- Fase de transición
- Fase de recuperación.

4.5.3.1 Fase de alerta

Documentación requerida

- Equipos de emergencia
Nombre Cargo Teléfono Backup

- Lugar de reunión
 - Oficina Internet.

4.5.3.2 Fase de transición

Funciones del:

Equipo Director

- Comunica las estrategias y procedimientos a seguir.
- Reasignar funciones si fuera necesario

Equipo de recuperación

- Coordinar con el equipo de logística para el traslado equipos
- Adquisición de hardware y software para la reposición o equipamiento para el Cold backup.

Equipo Logístico

Coordinar el transporte de hardware, y Software al Centro de Respaldo temporal el cual estará ubicado en el la oficina del laboratorio de redes.

- Envío urgente de hardware y Software.
- Lista de personal a desplazar (priorizada)
- Reserva de alojamiento.
- Reserva de vehículos de transporte.

Grupo de Base de Datos.

Coordinar con el equipo logístico para el traslado de los soportes de backup de la diferentes Bases de datos.

Responsable de seguridad

Implantar los controles de seguridad física en el CPD alternativo

Equipo de sistemas

Poner operativos los sistemas informáticos

- Instalar el sistema operativo base y software base.

Equipo de comunicaciones

Establecer y comprobar la red de telefonía alterna

Documentación requerida

Ubicación sobre la ubicación del centro de respaldo

Oficina de redes.

Inventarios de servicios Backup

Datos sobre configuraciones del sistema.

4.5.3.2 Fase de recuperación

Grupo de Sistemas

Restauración del Software y los datos.

Planificación de las entradas y salidas de los soportes magnéticos

Efectuar cambios en los aplicativos

Grupo de comunicaciones

Arranque de la red de teleproceso.

Soporte y mantenimiento de la red de comunicaciones.

Coordinar la posible adquisición / contratación de líneas adicionales.

Grupo de base de datos.

Establecimiento de los CUT OFFS para efectuar la reconciliación de de la base de datos a partir de los logs

Verificación de la reconciliación de la base de datos.

Equipo director

Supervisión general del procedimiento

Administración y dirección.

Auditoria

Verificación del cumplimiento de los requerimientos,

Verificación de las medidas de seguridad y su cumplimiento

- Seguridad física
- Seguridad lógica

Control de la política de Backup y de los soportes magnéticos.

4.5.4 DEFINICIÓN DE LA ESTRATEGIA DE VUELTA A LA NORMALIDAD

4.5.4.1 Funciones de los diferentes equipos

Equipo de sistemas

- Valorizar los daños en los sistemas
 - Costes de reparación
 - Costes de reposición

Equipo de soporte técnico

- Valorizar os daños de volumen técnico
 - Costes de reparación
 - Costes de reposición

Equipo de recuperación

- Recuperar los equipos y datos
- Inventariar los recursos de volumen técnico útiles:

- Eléctricos
- Iluminación
- Telefonía
- Detección y extinción de incendios
- Mobiliario

4.5.4.2 Restauración del procedimiento

Los procedimientos y conceptos serán los mismos a las fases de transición en el centro de respaldo.

4.6 PRUEBAS Y MANTENIMIENTO

4.6.1 REALIZACIÓN DE LA PRUEBA.

Estas sirven para comprobar la eficacia del plan de contingencia mediante su cuantificación en el tiempo y resultados esperados:

Prueba de notificación.

Esta se sujeta al organigrama de notificación del desastre.

- Desastre
- Disparo del plan de contingencia

Mantenimiento

Para esta fase se establecido el siguiente organigrama del equipo de mantenimiento

Grupo de trabajo.- Conformado por los miembros de los equipos de emergencia.

Comité

Encargados de analizar y aprobar o negar las propuestas de cambio y esta conformado por los jefes de cada equipo de emergencia.

Coordinador

Su función es la de publicar y hacer conocer a todos acerca de los cambios en el plan de contingencias de los Laboratorios de Informática del ITSA.

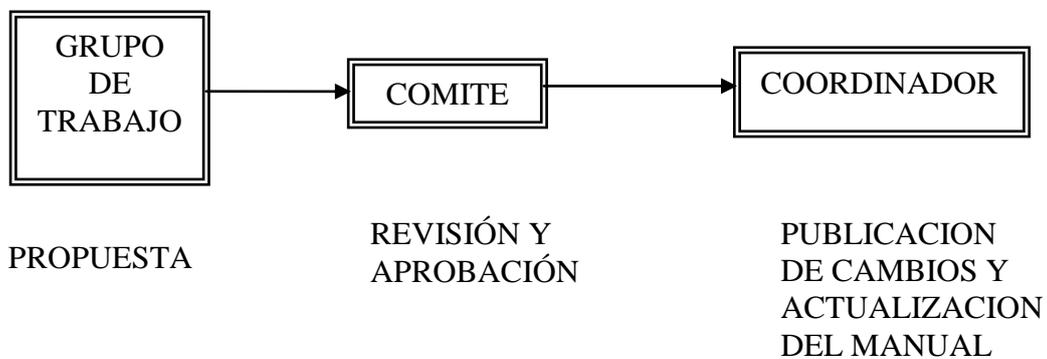
Responsable

Equipo Director.

Mecanismo de control de cambios

Para realizar los cambios en los procesos se lo realizará a través del seguimiento del siguiente órgano regular.

ORGANIGRAMA PARA CAMBIO EN LOS PROCESOS.



CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

El diseñar e implementar un sistema Open Source para la Administración y Control del acceso a la WEB en el Laboratorio de Internet del INSTITUTO TECNOLOGICO SUPERIOR AEREONAUTICO en base a la arquitectura del modelo cliente / servidor, ha permitido reforzar aun más el concepto o ideas asociados al mismo; ya que al ser este modelo una plataforma abierta por excelencia brindo la oportunidad de hacer una gran variedad de combinaciones en la plataforma del cliente y servidores (como servidor de base de datos y servidor de la aplicación).

Dentro de los procesos que son manejados en la arquitectura Cliente/Servidor, se determino 3 elementos básicos que deben de distribirse entre el cliente y el servidor, estos elementos son:

1. El manejo de Datos.
2. La aplicación.
3. La presentación.

El servidor de aplicación, ha sido la base para la llamada computación cliente / servidor de 3 capas ya que los sistemas abiertos representa una segunda razón de importancia que justifican el uso del servidor de aplicación, al ser portadle a una diferente plataforma puesto que el servidor de aplicación de Web Access escrito en PHP, puede ser instalado en muchos sistemas operativos diferentes sin mayores cambios.

El modelo cliente servidor a permitido que el servidor sirva a una multitud de clientes, ahorrando a cada uno de ellos el problema de tener la información

instalada y almacenada localmente.

El enmascaramiento, se lo ha utilizado principalmente para la conexión de todos los terminales del Laboratorio de Internet a través de una sola dirección IP.

Con el enmascaramiento el servidor del Sistema Web Access identifica a cada uno de los equipos de la red interna que intenta tener acceso a la web, y es el mismo servidor del Sistema de Administración y Control el que realiza la petición por sí mismo, en lugar de que la máquina cliente lo haga. Así, el servidor toma la dirección IP de la máquina que hace la solicitud, la "enmascara" con la dirección IP que le ha sido asignada, la envía, y cuando llega el paquete de respuesta lo "reenvía" a la máquina que realizó la petición

NAT no es un proxy, los proxies trabajan en un nivel superior de la pila de protocolos, bien en el nivel de TCP/UDP o incluso en el nivel de aplicación, lo que implica que los clientes deben configurarse para hacer uso del servicio.

Para cumplir con la demanda de los alumnos según los estudios realizados en base al análisis, se debería contar con las 14 estaciones de trabajo y el tiempo de navegación para Internet es de: 20 horas ya que en los casos de capacidad máxima y mínima existe un saldo positivo.

El gran problema con el Sistema de Administración y Control del Acceso a la Web hecho a la medida son las reglas de negocios, que no son otra cosa sino las políticas y procedimientos que el Instituto Tecnológico Superior Aeronáutico usa para guiar su relación con sus clientes y otros agentes, así como también sus procedimientos internos.

El estudio y evaluación del entorno de seguridades del "Sistema Open Source para la Administración y Control del Acceso a la WEB WEBACCESS" identifico que los procesos que necesitan un nivel de seguridad específico son

el ingreso de administradores, la identificación de usuarios al sistema y el cambio de claves de los usuarios del sistema.

La elaboración del Plan de Contingencia para los laboratorios de Informática del Instituto Tecnológico Superior Aeronáutico estableció que el mecanismo para respaldar y asegurar la información; es mediante la implantación del “Centro de Respaldo”.

5.2.- RECOMENDACIONES

Es de importancia realizar un análisis del sistema de Administración y Control del Acceso a la Web que en la actualidad posee el Instituto Tecnológico Superior Aeronáutico para luego, con la base de ese análisis hecho poder determinar cuales son los procesos que se observan que están débiles o que están cubiertas de manera ineficiente.

La actualización del firewall es necesaria por los ante nuevos ataques, intrusos y políticas de la Institución.

No sobrepasar el límite de 50 direcciones IP ya que al aumentar el número de direcciones se reduce el tráfico de red.

La seguridad es un proceso, no un producto valoración que debe ser tomado muy en cuenta por los directivos del Instituto Tecnológico Superior Aeronáutico a fin de satisfacer las necesidades del cliente.

REFERENCIAS BIBLIOGRÁFICAS

<http://www.rinconastur.com/php/php12a.php>

<http://www.programatuweb.com/manuales/jscript/lesson01.php?PHPSESSID=4b80133d66369ffb0c70253d6221e243>

<http://www.ciudadfutura.com/mundopc/cursos/firewalls/fire6.htm>

<http://www.rinconastur.com/php/php12a.php>

<http://www.programatuweb.com/manuales/jscript/lesson01.php?PHPSESSID=4b80133d66369ffb0c70253d6221e243>

ANEXOS

ANEXO I Cronograma de Actividades.

ANEXO II Organigrama Estructural del Instituto Tecnológico Superior Aeronáutico.

ANEXO III Diseño del Plan de Contingencias Administrador Nivel 2..

ANEXO IV Diseño del Plan de Contingencias Administrador Nivel 3.

ANEXO V Instalación y Configuración del Servidor Apache, Modulo PHP y MySql

ANEXO VI Encuestas.

ANEXO VII Nomenclatura del diagrama de la ubicación de los laboratorios de informática del Instituto Tecnológico Superior Aeronáutico

ANEXO VIII Glosario de Términos

ANEXO III DISEÑO DEL PLAN DE CONTINGENCIAS ADMINISTRADOR NIVEL 2.

No Prueba	No Ventana	Acción	Resultado esperado	Resultado obtenido	
				+	-
01	A_0	Administrador nivel 02 digita dirección electrónica diferente a la página de administración Del Sistema WEBACCESS	Página no encontrada	X	
02	A_01	Administrador nivel 02 ingresa login erróneo	Usuario no valido	X	
03	A_01	Administrador nivel 02 digita login correcto y clave de acceso incorrecta	Clave no valida	X	
04	A_01	Administrador nivel 02 digita login correcto y clave de acceso correcta.	Ventana C_02 con la información del menú de Súper administrador.	X	

05	A_02	Administrador nivel 02 da clic en la opción usuarios.	Ventana A_03 con el menú de usuarios	X	
06	A_03	Administrador nivel 02 elige la opción para ingresar usuarios	Ventana A_04 con el casillero para ingresar el No de C_I del cliente	X	
07	A_04	Administrador nivel 02 digita el No de C_I del cliente a ingresar	Ventana A_05 con el formulario para llenar los datos del nuevo cliente	X	
08	A_05	Administrador nivel 02 elige la opción ingresar cliente.	Ventana C_06 con el mensaje de cliente ingresado.	X	
O9	A_03	Administrador nivel 02 elige la opción para buscar usuarios	Ventana A_04 con el casillero para ingresar el No de C_I del cliente	X	
10	A_04	Administrador nivel 02 digita el No de C_I del cliente a buscar	Ventana A_06 con el formulario con los datos del cliente	X	
11	A_03	Administrador nivel 02 elige la opción para modificar usuarios	Ventana A_04 con el casillero para ingresar el No de C_I del cliente	X	

12	A_04	Administrador nivel 02 digita el No de C_I del cliente a modificar	Ventana A_07 con el formulario con los datos del cliente y la opción para modificarlos.	X	
13	A_02	Administrador nivel 02 da clic en la opción Estado Actual.	Ventana A_14 con el menú del estado del laboratorio.	X	
14	A_08	Administrador nivel 02 elige la opción últimas sesiones	Ventana A_15 muestra las últimas diez sesiones en el terminal seleccionado	X	
15	A_09	Administrador nivel 02 digita número de sesiones que desea visualizar	Ventana A_16 muestra las sesiones en el terminal seleccionado	X	
16	A_10	Administrador nivel 02 elige la opción cerrar sesión.	Ventana A_17 con el mensaje de confirmación de cierre de conexión.	X	
17	A_08	Administrador nivel 02 responde afirmativamente	Ventana A_18 información de la sesión	X	

18	A_09	Administrador nivel 02 responde negativamente	Ventana A_14	X	
19	A_08	Administrador nivel 02 da clic en la opción Reportes.	Ventana A_15 con el menú de los reportes a visualizar.	X	
20	A_09	Administrador nivel 02 elige la opción fecha	Ventana A_16 formulario con la fecha a elegir para el reporte.	X	
21	A_02	Administrador nivel 02 elige fechas correctas para el reporte.	Ventana A_17 informe de los clientes ingresados en la fecha elegida	X	
22	A_14	Administrador nivel 02 elige opción cambiar clave.	Ventana A_18 formulario para el ingreso de nueva clave.	X	
23	A_15	Administrador nivel 02 ingresa clave diferente en los casilleros.	Ventana A_18 setfocus retorna al primer casillero.	X	
24	A_14	Administrador nivel 02 ingresa claves idénticas entre los casilleros.	Ventana A_19 mensaje su clave se ha cambiado con éxito.	X	

ANEXO IV DISEÑO DEL PLAN DE CONTINGENCIAS ADMINISTRADOR NIVEL 3.

No Prueba	No Ventana	Acción	Resultado esperado	Resultado obtenido	
				+	-
01	P_0	Administrador nivel 03 digita dirección electrónica diferente a la página de administración Del Sistema WEBACCESS	Página no encontrada	X	
02	P_01	Administrador nivel 03 ingresa login erróneo	Usuario no valido	X	
03	P_01	Administrador nivel 03 digita login correcto y clave de acceso incorrecta	Clave no valida	X	
04	P_01	Administrador nivel 03 digita login correcto y clave de acceso correcta.	Ventana C_02 con la información del menú de Administrador nivel 3 (Pagaduría).	X	

05	P_02	Administrador nivel 03 da clic en la opción clientes.	Ventana P_03 con el casillero para ingresar el No de C_I del cliente	X	
06	P_03	Administrador nivel 03 digita el No de C_I de un cliente que ya existe	Ventana P_04 con el formulario para aumentar el tiempo de navegación	X	
07	P_04	Administrador nivel 03 elige la opción modificar.	Ventana C_05 con la información del costo del ticket.	X	
08	P_05	Administrador nivel 03 elige la opción Agregar Tiempo.	Ventana C_06 con el mensaje de tiempo agregado.	X	
09	P_03	Administrador nivel 03 digita el No de C_I de un cliente que no existe	Ventana P_07 con el formulario para ingresar datos del cliente y el tiempo de navegación	X	
10	P_07	Administrador nivel 03 elige la opción aceptar.	Ventana C_08 con la información del costo del ticket.	X	

11	P_08	Administrador nivel 03 elige la opción Agregar Clave.	Ventana C_09 con el mensaje de cliente agregado.	X	
12	P_02	Administrador nivel 03 elige la opción reportes	Ventana P_10 menú de reportes.	X	
13	P_10	Administrador nivel 03 elige la opción General.	Ventana C_11 con la información del reporte económico general por el expendido.	X	
14	P_10	Administrador nivel 03 elige la opción Individual.	Ventana C_11 con la información detallada del reporte económico por el expendido.	X	
15	P_02	Administrador nivel 03 elige opción cambiar clave.	Ventana P_12formulario para el ingreso de nueva clave.	X	
16	P_12	Administrador nivel 03 ingresa clave diferente en los casilleros.	Ventana P_12setfocus retorna al primer casillero.	X	
17	P_12	Administrador nivel 03 ingresa claves idénticas entre los casilleros.	Ventana P_13 mensaje su clave se ha cambiado con éxito.	X	

ANEXO V INSTALACION Y CONFIGURACION DEL SERVIDOR APACHE, MODULO PHP Y MYSQL EN EL SISTEMA OPERATIVO LINUX RED HAT 9.0

Para la configuración de estos paquetes siga los siguientes procedimientos:

- a) Copie la carpeta instaladores del CD que acompaña a la presente tesis al directorio /home del Sistema operativo Linux Red Hat 9.0.
- b) A continuación procedemos a descomprimir (haciendo doble clic sobre los paquetes de apache_1.3.27, php-4.3.2, squid-2-3-STABLE3-src.tgz y sudo) en la dirección /usr/local/src/, con este comando se crearán los directorios apache__1.3.27, php-4.3.2, squid-2.3.STABLE3 y
- c) Copiar la carpeta Mysql al directorio /usr/local/src

1.- INSTALACIÓN DE MYSQL

Antes de instalar MySQL es necesario ejecutar los siguientes comandos:

```
# cd /usr/local
```

Con esto ingresamos a dicho directorio y ejecutamos:

```
#rpm -ihv My*
```

Ahora es importante definir las claves de acceso del administrador (usuario *root*) para MySQL, cambiando 'mysql' por la clave que desee utilizar y 'localhost' por el nombre del su servidor. No olvide colocar las comillas!:

```
# bin/mysqladmin -u root -p password 'mysql'
```

El sistema responderá:

Enter password:

Simplemente de Enter.

Posteriormente teclee:

```
# bin/mysqladmin -u root -h 'localhost' -p password 'mysql'
```

El sistema responderá:

Enter password:

Simplemente de Enter.

Con esto quedará instalado MySQL en el servidor.

2.- EL SERVIDOR APACHE

Es el servicio que se encarga de resolver las peticiones de páginas de Internet de los clientes utilizando el protocolo de Internet http.

A continuación se presentan las instrucciones de instalación de Apache en el servidor Linux.

2.1.- INSTALACIÓN DE APACHE.

Ingresa al directorio `/usr/local/src/ apache_1.3.27` y ejecute los siguientes comandos:

```
# ./configure --prefix=/usr/local/apache --enable-module=so
```

```
# make
```

```
# make install
```

Apache quedará instalado en el directorio

`/usr/local/apache`.

Para que Apache se inicie cada vez que se prenda el servidor reemplace el archivo `rc.local` del directorio `/etc/rc.d/rc.local` con el archivo `rc.local` de la carpeta instaladores y reiniciamos el computador

Nota:

Abra un navegador y escriba el nombre del servidor o la dirección IP que se especificó en el archivo de configuración y deberá poder ver la página de prueba de Apache que indica:

¡Funcionó! ¡El Servidor de Red Apache ha sido instalado en ese sitio!

3.- INSTALACIÓN DE MÓDULOS DE PHP

Ingresa al directorio `/usr/local/src/ php-4.3.2` y ejecute el siguiente comando:

```
#!/configure --with-mysql --with-apache=/usr/local/apache
```

Este proceso tarda un poco. Al finalizar mostrará el siguiente anuncio:

WARNING

You chose to compile PHP with the built-in MySQL support. If you are compiling a server module, and intend to use other server modules that also use MySQL (e.g, mod_auth_mysql, PHP 3.0, mod_perl) you must NOT rely on PHP's built-in MySQL support, and instead build it with your local MySQL support files, by adding --with-mysql=/path/to/mysql to your configure line.

License:

This software is subject to the PHP License, available in this distribution in the file LICENSE. By continuing this installation process, you are bound by the terms of this license agreement. If you do not agree with the terms of this license, you must abort the installation process at this point.

Thank you for using PHP

A continuación ejecutamos el comando:

```
# make
```

```
# make install
```

A continuación copiamos el archivo libphp4.a del directorio /usr/local/src/php-4.3.2/.libs al directorio /usr/local/apache_1.3.27/src/modules/php4

Nos ubicamos en el directorio

/usr/local/apache_1.3.27 y ejecutamos el comando

```
#--prefix=/usr/local/apache
```

```
# make
```

```
# make install
```

3.1.- CONFIGURACIÓN DE APACHE.

Después de realizar la instalación es necesario configurar el servidor reemplazando el archivo de configuración **httpd.conf**. (que se encuentra en el directorio `usr/local/apache/conf`) con el archivo `httpd.conf` de la carpeta `/home/instaladores`.

```
#reboot
```

Para probar si la instalación tuvo éxito se recomienda reiniciar el servidor

```
# /usr/local/apache/bin/apachectl restart
```

Posteriormente, después de reiniciar el servidor Apache, comprobar si la instalación de PHP fue realizada con éxito. Entre al directorio raíz del servidor Apache:

```
# cd /usr/local/apache/htdocs
```

Crear una carpeta con el nombre prueba y copie el archivo `info.php` de la carpeta:

```
/home/instaladores al directorio /usr/local/apache/htdocs/prueba:
```

Al abrir esta página desde el navegador:

```
http://localhost/prueba/info.php
```

Debe aparecer una página con toda la información de configuración de PHP en el servidor

PHP Version 4.3.2



System	Linux servidor.itsa.com 2.4.20-8 #1 Thu Mar 13 17:54:28 EST 2003 i686
Build Date	Aug 26 2003 21:43:57
Configure Command	'./configure' '--with-mysql' '--with-apache=/usr/local/src/apache_1.3.27'
Server API	Apache
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/lib/php.ini
PHP API	20020918
PHP Extension	20020429
Zend Extension	20021010
Debug Build	no
Thread Safety	disabled
Registered PHP Streams	php, http, ftp

This program makes use of the Zend Scripting Language Engine:
Zend Engine v1.3.0, Copyright (c) 1998-2003 Zend Technologies



PHP Credits

A continuación copiamos el contenido de la carpeta WebAccess al directorio /usr/local/apache/htdocs/

3.2.- INSTALACION DE SQUID

Ingresa a la carpeta `cd squid-2.3.STABLE3` y ejecute

```
# ./configure
```

```
# make
```

```
# make install
```

Copie el archivo squid.conf de la carpeta instaladores en el directorio /usr/local/squid/etc

3.3.- INSTALACION DE SUDO

Ingresa a la carpeta `/usr/local/src/sudo-1.6.3p7` y ejecute los siguientes comandos

```
# ./configure
```

```
# make
```

```
# make install
```

Copie el archivo sudores de la carpeta instaladores en el directorio /etc

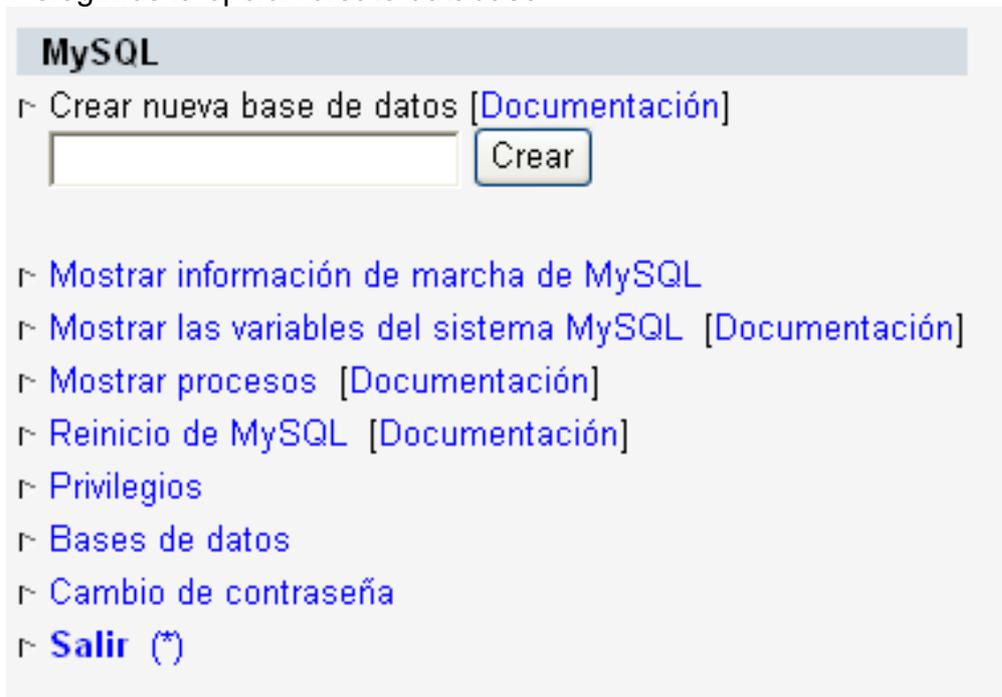
3.4.- INSTALACION DE LA BASE DATOS

Antes de crear la base de datos copiamos la carpeta phpmyadmin en el directorio /usr/local/apache/htdocs.

A continuación o creamos la base de datos utilizando el scrip de phpmyadmin desde el navegador

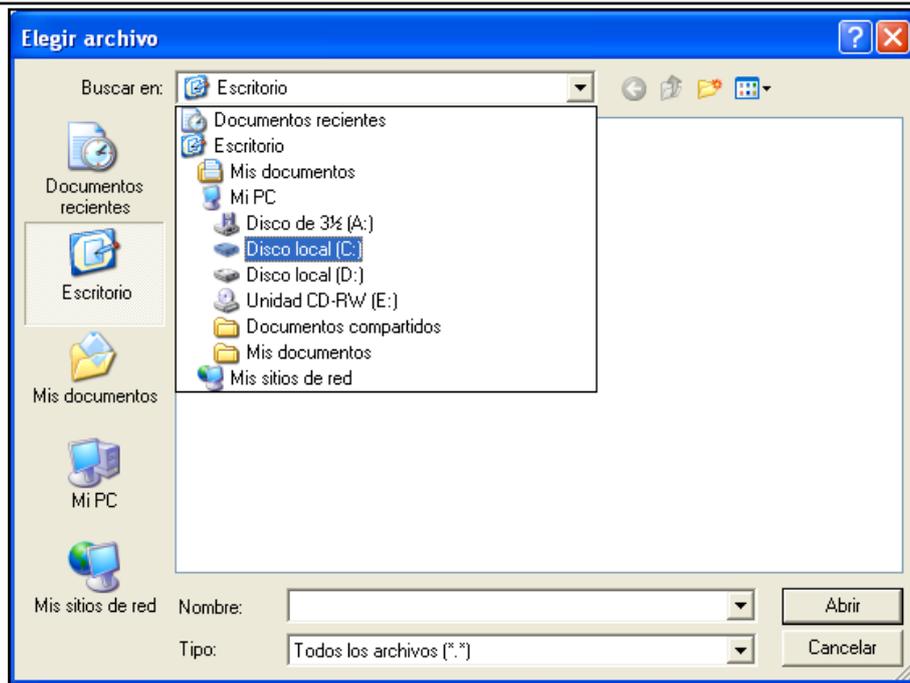
<http://localhost/phpmyadmin>

Y elegimos la opción create database



The screenshot shows the MySQL interface for creating a new database. At the top, there is a header 'MySQL'. Below it, the option 'Crear nueva base de datos' is selected, with a link to '[Documentación]'. There is an empty text input field for the database name and a 'Crear' button. Below this, a list of other MySQL options is visible, including 'Mostrar información de marcha de MySQL', 'Mostrar las variables del sistema MySQL [Documentación]', 'Mostrar procesos [Documentación]', 'Reinicio de MySQL [Documentación]', 'Privilegios', 'Bases de datos', 'Cambio de contraseña', and 'Salir (👤)'.

Procedemos a exportar las tablas de la base datos clientesitsa de la carpeta instaladores con la ayuda del scrip seleccionando la opcion sql



Reinicie el servidor y digite en el browse la siguiente dirección <http://localhost/index.php> y a continuación debe presentarse la siguiente pagina WEB



ANEXO VI ENCUESTAS

A) ENCUESTA DEL SERVICIO DE INTERNET AL CLIENTE.

La presente encuesta pretende mejorar el servicio de Internet que el Instituto Tecnológico Superior Aeronáutico brinda a sus clientes a través de su opinión personal para lo cual solicitamos sea lo más sincero posible.

1. Usted es:

Alumno del ITSA Docente Personal Administrativo Otro:.....

2. ¿Es necesario para usted el servicio de Internet?

Si No

En caso de ser negativa su respuesta explique su razón:

.....

3. ¿Qué tiempo ingresa usted al servicio de Internet?

Al día:

A la semana:

Al mes:

Al semestre:

4. ¿ El tiempo otorgado para su acceso a Internet en el periodo académico de acuerdo a su necesidad es:

Suficiente

caso

Exclente

5. Escriba el tiempo que desearía que se le otorgue en el periodo académico

.....

6. ¿En que ocupa más su tiempo de Internet otorgado en cada semestre académico?

.....

7. Acerca del registro manual de su tiempo de Internet usted cree que:

Debería ser automatizado : si no

Seguir como esta : si no

8. En caso de ser automatizado como le gustaría que este funcionara.

.....

.....

.....

.....

.....

.....

B) ENCUESTA AL PERSONAL DIRECTIVO DEL INSTITUTO TECNOLÓGICO SUPERIOR AERONÁUTICO

La presente encuesta tiene como objetivo mejorar el servicio de Internet que el Instituto Tecnológico Superior Aeronáutico brinda a sus clientes a través de su colaboración a las siguientes preguntas.

Usted como Directivo del Instituto Tecnológico Superior Aeronáutico:

1. A que funciones del sistema de Administración y Control del Acceso al Internet le gustaría tener acceso:

- Realizar consultas del estado económico a cualquier hora del día laborable
Si No
- Conocer el número de personas que hacen uso del servicio de Internet en cualquier tiempo del periodo académico.
Si No

2. Que otras opciones, desearía que el Sistema de Administración y Control le brindase:

.....
.....
.....
.....
.....

Gracias por la colaboración, sus respuestas servirán en el proceso del análisis para el desarrollo del Sistema de Administración y Control del Acceso a la WEB para los usuarios del Laboratorio de Internet del ITSA.

C) ENCUESTA ADMINISTRADOR DEL LABORATORIO DE INTERNET

La presente encuesta tiene como objetivo mejorar el servicio de Internet que el Instituto Tecnológico Superior Aeronáutico brinda a sus clientes a través de su opinión personal por lo cual solicitamos sea lo más sincero posible.

1. Encierre en un círculo la respuesta que usted considere; a cerca de sus funciones como administrador del laboratorio de Internet en el proceso de la administración del acceso a la web.

Usted:

- Registra al usuario que hace uso del servicio de Internet si no
- Controla el tiempo de conexión de los clientes si no
- Restringe el acceso a paginas no autorizadas si no
- Elabora informes económicos acerca del servicio de Internet si no

2. Que otras funciones usted realiza en todo lo relacionado con el control y administración del acceso al Internet del laboratorio de Internet.

.....
.....
.....

Gracias por la colaboración, sus respuestas servirán en el proceso del análisis para el desarrollo del sistema de administración y control del acceso a la web para los usuarios del Laboratorio de Internet.

**ANEXO VII NOMENCLATURA DEL DIAGRAMA DE LA UBICACIÓN DE
LOS LABORATORIOS DE INFORMATICA DEL INSTITUTO TECNOLOGICO
SUPERIOR AERONÁUTICO.**

C.R.1. Centro de RespalDOS No- 1

C.R.2. Centro de RespalDOS No- 2.

L.I. Laboratorio de Internet.

L.R. Laboratorio de Redes.

L.C.B. Laboratorio de Computación Básica.

ANEXO VIII

TEMARIO

Arquitectura Cliente/Servidor:

Una arquitectura es un conjunto de reglas, definiciones, términos y modelos que se emplean para producir un producto.

La arquitectura Cliente/Servidor agrupa conjuntos de elementos que efectúan procesos distribuidos y computo cooperativo.

Cliente

Un *cliente* funciona en su ordenador local, se comunica con el servidor remoto, y pide a éste información.

Gateway Término empleado para describir un sistema capaz de direccionar paquetes IP entre redes que ejecuten el Protocolo TCP/IP.

IP: Internet protocol

Nat

Red de comunicación.

Es todo aquel conjunto de elementos basados en hardware y software que permite establecer un enlace entre los clientes y los servidores, se clasifican por su tamaño LAN, MAN y WAN.

Paquete. Unidad de transmisión de información a través de una Red, que puede estar compuesta por diferentes elementos, como datos, Id. de cabecera, las direcciones tanto del origen como del destino del paquete, e información complementaria para control de errores.

Red (informática). Conjunto de ordenadores conectados directamente por

cable, remotamente vía Modem, o por otro procedimiento de comunicación.

Servidor

Un *servidor* es un ordenador remoto, en algún lugar de la red, que proporciona información según una petición

Webacces Sistema de Administración y Control del Acceso a la Web.

Rpm –ihv

Comando para instalar paquetes ejecutables de Linux

Targz

Extensión de los paquetes comprimidos en Linux.

Make, make install

Comandos para crear carpetas en donde residirán los programas ejecutables.