PRÁCTICA EMPRESARIAL EN LA ESCUELA DE INGENIERIA DE SISTEMAS E INFORMATICA DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

MONICA YAMILE RIVERA ORDOÑEZ

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FISICO-MECÁNICAS
ESCUELA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
BUCARAMANGA
2006

PRÁCTICA EMPRESARIAL EN LA ESCUELA DE INGENIERIA DE SISTEMAS E INFORMATICA DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

MONICA YAMILE RIVERA ORDOÑEZ

Trabajo de grado para obtener el título de Ingeniera de Sistemas

Tutor: Ing. Manuel Guillermo Flórez Becerra M.Sc.
Docente
ESCUELA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA – UIS

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FISICO-MECÁNICAS
ESCUELA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
BUCARAMANGA
2006

DEDICATORIA

Dedico este trabajo a todos aquellos que estuvieron a mi lado en este largo y difícil camino y que me apoyaron incondicionalmente.

A **Dios** por acompañarme día a día en mi camino y darme la fuerza para seguir adelante.

A **mi hija Silvia Juliana** por ser la personita que me ha alegrado en cada momento de tristeza y debilidad.

A **mis amigos** Edgar Fernando Téllez Cáceres (Juan) y Edwin Gregorio Hernández a quienes considero mis hermanos. Por su incondicionalidad, por creer en mí y porque me han enseñado que la distancia no es obstáculo para apoyarnos y hacernos presentes en los momentos más difíciles.

AGRADECIMIENTOS

Agradezco a todas las personas que en su momento me ofrecieron su colaboración:

Al ingeniero **Manuel Guillermo Flórez Becerra**, mi tutor y amigo. Por creer en mí y brindarme su apoyo no solo en la realización de la práctica sino en la fase final de la carrera cuando fui su auxiliar.

Al ingeniero **Erwin Meza**, mi amigo, compañero de código y mi ángel. Me dio su ayuda desinteresada durante toda la carrera y especialmente en el momento más crítico de la práctica.

Al ingeniero **Julio César Pérez Cortés**, mi jefe y amigo. Por entenderme y ayudarme a realizar la práctica acomodando mis horarios de trabajo y darme el tiempo necesario cuando más lo necesité.

A los ingenieros **Oscar Villamizar Blanco** y **Hina Luz Garavito**, mis amigos y compañeros de padecimientos. Por escucharme y acompañarme en los momentos de angustias y lograr levantarme el ánimo.

Al ingeniero **Walter Darwin Rey Cala,** exintegrante del grupo Trionix y mi amigo. Por ser una persona especial, muy cordial y ofrecerme su colaboración cuando era una extraña para él.

A los ingenieros **Luis Guillermo Ortiz, Erick Meneses** y **Diana Hortúa**, mis compañeros de oficina. Por acogerme en su espacio y compartirme sus conocimientos convirtiéndose en personas muy especiales para mí.

Al estudiante **Angel Vargas**, mi otro ángel. Por entrar en mi vida en un momento crítico ayudándome y aportándome su conocimiento.

A los usuarios del servidor, especialmente a **Oscar Acelas.** Por su paciencia y apoyo constante.

A la ingeniera **Diana Rojo,** primera practicante del servidor Cormorán. Por apoyarme en la primera etapa de la práctica cuando todo era confuso.

A los ingenieros **Sandra Milena Maldonado, Silvia González Gualdrón y Daniel González Olano** mis amigos incondicionales. Por ser especiales conmigo durante el tiempo que vimos materias, por vivir mis alegrías y mis tristezas junto a mí.

Al papá de mi hija, **Benito Rodríguez Méndez**. Por ofrecerme su apoyo económico y moral e impulsarme a continuar en mis momentos más duros.

A mi **mamá.** Por ayudarme en la fase final de mi carrera y mostrarme su apoyo en esta nueva etapa de mi vida.

TABLA DE CONTENIDO

Pag.

LISTA DE TABLAS

Pag

LISTA DE FIGURAS

Pag

TITULO: PRÁCTICA EMPRESARIAL EN LA ESCUELA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER[*]

AUTORA: MÓNICA YAMILE RIVERA ORDÓÑEZ[**]

Palabras claves: Práctica, servidor, administración, seguridad, copias de seguridad, imágenes, Linux Terminal Server Project (LTSP), Windows Terminal Server, manuales.

RESUMEN

La Escuela de Ingeniería de Sistemas e Informática (EISI) de la Universidad Industrial de Santander (UIS) cuenta con un Servidor Web (Cormorán) en el cual se implementó sistemas de recuperación de la información con el fin de incrementar su nivel de seguridad: copias de seguridad manuales y/o automáticas de los sitios alojados en el servidor, realización de imágenes de sus particiones, copia de la tabla de particiones y del sector de arranque.

Se realizaron diferentes investigaciones como: criptografía del disco duro a nivel de kernel, actualización de la versión de PHP instalada en Cormorán, Linux Terminal Server Project (LTSP), Windows Terminal Server y paralelo entre los dos sistemas de terminales Linux y Windows. El sistema LTSP fue implementado utilizando como servidor de terminales el equipo de respaldo de Cormorán y como clientes los equipos de cómputo de la sala 3 del laboratorio Villabona de la EISI.

La labor administrativa y de mantenimiento del servidor Cormorán fue permanente: creación de usuarios, creación de bases de datos, soporte a usuarios solucionando eventualidades en sus respectivos sitios y conectividad con sus respectivas bases de datos, rediseño del sitio de utilidades y software libre de Cormorán, documentación de las labores realizadas y actualización del manual del servidor. Se recomienda continuar con la administración en ambos servidores implementando nuevas políticas de seguridad en Cormorán y promoviendo el uso de las terminales.

---

[*] Trabajo de grado, modalidad práctica empresarial

[**] Facultad de Ingenierías Físico-Mecánicas.
Escuela de Ingeniería de Sistemas e Informática.
Universidad Industrial de Santander, UIS.
Tutor: Ingeniero Manuel Guillermo Flórez Becerra, Docente EISI.

TITLE: ENTERPRICE PRACTICE IN THE SYSTEMS ENGINEERING AND COMPUTER SCIENCE SCHOOL. UIS.[*]

AUTHOR: MÓNICA YAMILE RIVERA ORDÓÑEZ[**]

Keywords: Practice, server, administration, security, backups, images, Linux Terminal Server Project (LTSP), Windows Terminal Server, manuals.

ABSTRACT

The Systems Engineering and Computer Science School (EISI) from the Industrial University of Santander (UIS) has a Web Server (Cormoran) in which, information recuperation systems was implemented in order to improve the security level: Manual or automatic backups of all web sites hosted in the server, the realization of images of his partitions, copies of the partitions table and of the boot record.

Different Investigations were made as: Cryptography of kernel's level hard disk, updating of the version of PHP installed in Cormoran, Linux Terminal Server Project (LTSP), Windows Terminal Server and compare the two systems of terminals Linux and Windows. The system LTSP was implemented utilizing as terminal server the Cormoran's backup machine and as clients the computers of the data center 3 of the laboratory Villabona of the EISI.

The server Cormorán's administrative and maintenance work was permanent: Users' creation, creation of data bases, support to users solving eventualities at his respective sites and connectivity with his respective data bases, redesign the Cormoran's utilities and freeware site, documentation of the realized works and updating of the manual of the server. It is recommended to continue with the administration in both servers implementing political news of security in Cormoran and promoting the use of the terminals.

---

[*] Grade Work, managerial practical modality.

[**] Physical-Mechanical Engineering's faculty.
Systems Engineering and Computer science school. UIS.
Tutor: Engineer Manuel Guillermo Flórez Becerra, teacher EISI.

INTRODUCCION

La Escuela de Ingeniería de Sistemas e Informática de la Universidad Industrial de Santander cuenta actualmente con un Servidor Web el cual ofrece el servicio de hospedaje para los Sitios Web de los diferentes miembros de la comunidad EISI entre los cuales figuran los sitios de los estudiantes de proyectos de grado y/o de grupos de investigación, sitios de las diferentes asignaturas de los profesores, sitio de maestría, sitio del diplomado, sitio de la revista Conexxión, portal de la EISI y sitio de acreditación de la EISI entre otros. Este hecho muestra el impulso y la aceptación que día a día ha tenido el servidor Cormorán y muestra además el trabajo que se ha realizado para mantener un buen desempeño, justificándose de esta manera la presencia de un estudiante en práctica empresarial que esté pendiente de las novedades que se pudieran presentar en el servidor y prestar además los servicios que requieran los usuarios.

Durante el tiempo de duración de la práctica se realizaron diversas funciones las cuales fueron documentadas en cada uno de los informes presentados al comité de proyectos. Estos informes fueron evaluados y aprobados por el tutor de la práctica después de confirmar los procedimientos respectivos. En estos informes se mostraron específicamente cada una de las labores desempeñadas con el firme objetivo de servir como punto de referencia para los futuros practicantes en el momento en que necesiten realizar alguna actualización o realizar algún proceso presentado con anterioridad.

La esencia del trabajo desempeñado en esta práctica es la realización de copias de respaldo de la información del servidor como medida de recuperación de la información mediante procesos automáticos, la investigación de diferentes aspectos de seguridad como el cifrado del núcleo y la investigación e implementación de las terminales virtuales en Linux mediante el proyecto LTSP.

Se destaca el hecho de que todas las actividades se llevaron a cabo mediante la investigación de cada uno de los conceptos y probando los procesos descritos en la teoría en el PC de respaldo del servidor Cormorán, el cual fue un recurso totalmente indispensable para cumplir todos los objetivos.

1. DESCRIPCIÓN DE LA PRÁCTICA EMPRESARIAL

1.1 DESCRIPCIÓN DE LA EMPRESA

1.1.1 Nombre de la empresa.

Escuela de Ingeniería de Sistemas e Informática (EISI) de la Universidad Industrial de Santander.

1.1.2 Misión de empresa.

La Escuela de Ingeniería de Sistemas e Informática (EISI) comprometida con la misión institucional, tiene como propósitos: la formación de personas autónomas, creativas, que actúen según principios éticos universalmente aceptados, de alta calidad ciudadana y comprometidos con el desarrollo regional y nacional; y la construcción, innovación y mejoramiento del conocimientos, que permitan disponer de la fundamentación teórica, tecnológica e instrumental para administrar y tratar los sistemas de información, las comunicaciones y la automatización industrial.

La EISI forma, actualiza y proyecta el recurso humano en áreas de pregrado, postgrado y de educación continuada, soportadas en el respeto de los valores humanos, logrando profesionales competentes. La EISI define, establece, desarrolla y evalúa su proceso administrativo, pedagógico e investigativo, apoyándose en el enfoque sistémico y el reconocimiento propio y ajeno. Fundamenta su labor en el liderazgo, la pertenencia, la tolerancia y el trabajo unificado de profesores, estudiantes y demás colaboradores.

1.1.3 Visión de la empresa.

La Escuela de Ingeniería de Sistemas e Informática (EISI) se proyecta como una Unidad académica y administrativa, respaldada por la calidad humana de su personal administrativo, académico e investigativo, la formación científica de sus docentes, el nivel académico de sus estudiantes y su integración con las políticas institucionales y la sociedad para la generación, proyección y aplicación del conocimiento, poniéndolos en sus procesos de docencia, investigación e integración con la comunidad.

1.1.4 Organigrama.

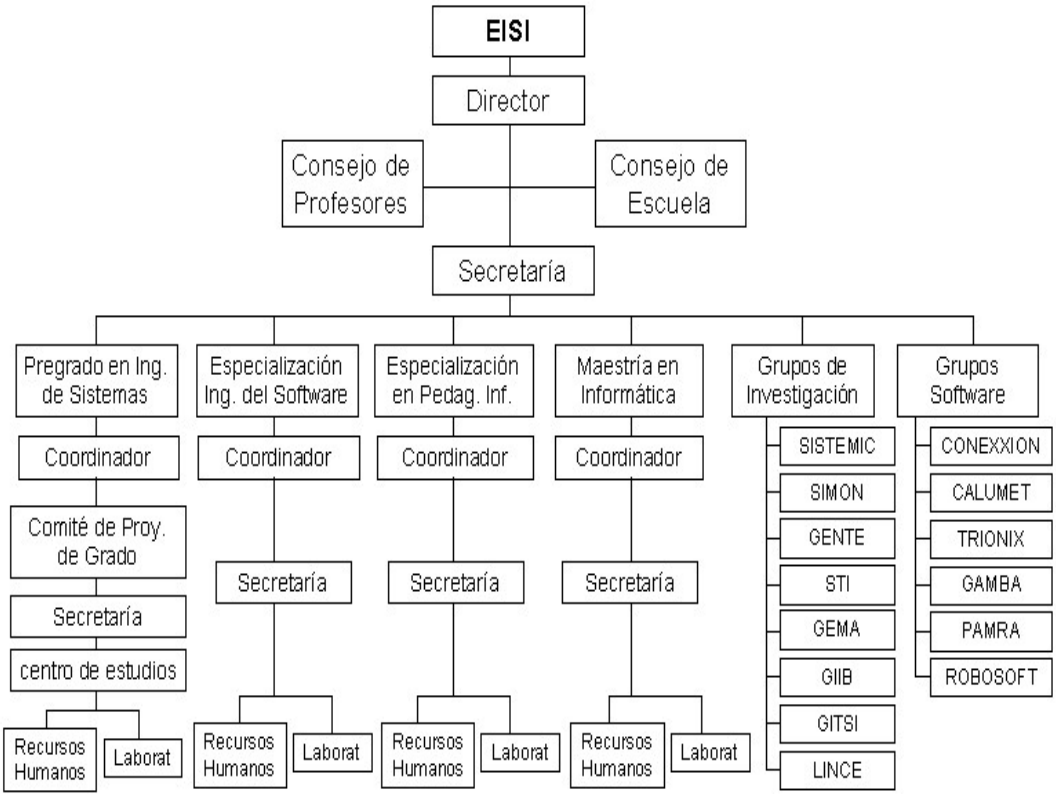

Figura 1. Organigrama EISI

1.2 DESCRIPCIÓN DEL PROYECTO

1.2.1 Objetivos Generales.

- ✓ Realizar labores administrativas en el servidor Cormorán de la Escuela de Ingeniería de Sistemas e Informática de la Universidad Industrial de Santander garantizando la funcionalidad de los servidores Web (Apache y Tomcat) y los servidores de Bases de Datos (Mysql y Postgres) para las aplicaciones de tipo Web desarrollados por los diferentes grupos de desarrollo de software de la EISI.

- ✓ Realizar un análisis sobre diferentes aspectos de la seguridad en el servidor Cormorán para aumentar su confiabilidad.

1.2.2 Objetivos Específicos.

- ✓ Revisión de los manuales de instalación, configuración y administración de los servidores Apache y Tomcat, Php, Postgres y Mysql, realizando y probando los procesos indicados en el respectivo manual sobre el equipo de respaldo.

- ✓ Redefinir las políticas de seguridad implementadas actualmente en el servidor para prevenir posibles pérdidas de información y reducir los posibles fallos en el equipo incluyendo copias de seguridad automáticas.

- ✓ Instalación y puesta en marcha de Linux Terminal Server Project (LTSP) en el servidor de la escuela utilizando como terminales los equipos de la sala del laboratorio de informática para tener acceso a un equipo Linux centralizado desde esta sala.

- ✓ Investigación de Windows Terminal Server utilizando como terminales los equipos de la sala del laboratorio de informática para tener acceso a un equipo Windows centralizado desde esta sala, condicionado a que se disponga del software.

- ✓ Rediseño de la página estática del listado de software libre para convertirla en una página dinámica.

- ✓ Monitorear el software Web desarrollado para administrar las salas de informática de la escuela.

- ✓ Administración del servidor realizando tareas como:
  - Crear usuarios
  - Copias de seguridad
  - Procesos para manejar la eficiencia del servidor (desfragmentacion del disco, monitoreo de los recursos del sistema)
  - Atender solicitudes

- ✓ Estudio de la compatibilidad de Php5 para una posible actualización en el servidor.

- ✓ Hacer un estudio de los posibles ataques a los que está expuesto el servidor para plantear posibles defensas.

- ✓ Realizar un análisis sobre la factibilidad de trabajar con un disco criptografiado a nivel de Kernel.

- ✓ Actualizar los manuales de documentación del sistema, incluyendo nuevos capítulos y modificando los que sean necesarios.

- ✓ Realizar el empalme correspondiente con el nuevo practicante.

1.3 Justificación

En la escuela de Ingeniería de Sistemas e Informática de la Universidad Industrial de Santander se encuentra un Servidor Web utilizado actualmente por los profesores y por los diferentes grupos de estudiantes encargados del desarrollo de Software y de la elaboración de proyectos de grado. El servidor NO contaba con un nivel de seguridad adecuado para proteger su información y sus programas, siendo ésta la razón principal por la cual se necesita de un estudiante que realice una práctica para que además de organizar un sistema de seguridad cumpla con otras labores administrativas y atienda las solicitudes de los usuarios.

El sistema de backups se modificó para realizar de forma automática las copias de los diferentes sitios alojados en el servidor para que en caso de ocurrir algún suceso inesperado se pueda acudir a estas copias y de esta forma poder restablecer la información. El proceso de Backups se estaba realizando en forma manual siendo un proceso que tomaba mucho tiempo para organizar la información y posteriormente grabarla en medios externos (CD's).

Los manuales de instalación, configuración y administración del servidor fueron modificados permanentemente documentando cada proceso realizado en el servidor Cormorán y en el equipo de respaldo para que los futuros usuarios y practicantes cuenten con un manual totalmente al día, acorde con la funcionalidad del servidor.

1.3.1 Impacto.

La prioridad en el trabajo sobre el servidor Cormorán de la Escuela de Ingeniería de Sistemas e Informática de la Universidad Industrial de Santander radicó en aumentar su nivel de seguridad para que los profesores y los estudiantes encargados del desarrollo de Software y de elaboración de proyectos de grado puedan alojar sus Sitios Web con la confianza de estar protegido contra posibles ataques. Además, el servidor Cormorán cuenta en este momento con un sistema de Backups automáticos, eliminando el proceso manual para la elaboración de las copias de respaldo.

Al contar con una persona que se encargue del servidor Cormorán, habrá un respaldo de alguien que estará atendiendo solicitudes de los usuarios, monitoreando el software desarrollado para administrar las salas de informática de la escuela, actualizando el listado de software libre y actualizando también los manuales de documentación del sistema.

1.3.2 Viabilidad.

- ✓ Técnica

Se dispone en discos compactos del software necesario para instalar y configurar el Servidor Cormorán por lo que ya no es necesario buscar este tipo de recurso. Encontrar soporte técnico tanto del Sistema Operativo Linux RedHat y del software necesario para montar los servidores Web (Apache y Tomcat) y los servidores de Bases de Datos (Mysql y Postgres) es muy fácil gracias a Internet. Encontramos en forma gratuita cantidades de manuales, grupos de discusión, sitios completos para descargar nuevo software y que además muestran paso a paso su instalación y configuración para el correcto funcionamiento en el servidor Cormorán.

- ✓ Económica

Los gastos están representados en el uso de los equipos y tiempo de trabajo del tutor y del practicante. NO implica un costo en cuanto a pago de Licencias ya que Cormorán funciona bajo la plataforma LINUX utilizando Servidor Web APACHE y TOMCAT, servidores de Bases de Datos Mysql y Postgres y el lenguaje para páginas dinámicas PHP, los cuales no tienen valor comercial gracias a su Licencia GNU. La EISI además ya dispone de un punto de conexión a Internet para este equipo evitando los gastos de conexión.

- ✓ Social

Los profesores y los estudiantes encargados del desarrollo de Software y de la elaboración de proyectos de grado de la EISI se han beneficiado al contar con el servidor Cormorán ya que en él han encontrado el medio para publicar sus diferentes Sitios Web (la revista Conexxion, el portal de la Escuela, Sitios Web de algunas materias y algunos proyectos de grado). Son precisamente estos usuarios quienes necesitan seguir contando con este servidor y de alguien que lo administre y a además atienda las necesidades de los usuarios, entre ellas la seguridad.

1.3.3 Cronograma.

La práctica tuvo una duración de seis meses en la cual se desarrollaron las siguientes actividades.

Plan de trabajo	1				2				3				4				5				6			
Actividades específicas	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Revisión del manual de instalación, configuración y administración del servidor																								
Prueba del proceso de Instalación del Sistema Operativo Linux																								
Prueba de la configuración de los servidores Web (Tomcat y Apache).																								
Prueba de los servidores de bases de datos (Mysql y Postgres)																								
Administración de los servicios del servidor.																								
Atención de solicitudes de los usuarios.																								
Asignación y administración de usuarios.																								
Realización de copias de seguridad.																								
Monitorear el software de administración de las salas de informática de la EISI.																								
Instalación y puesta en marcha de Linux Terminal Server Project (LTSP).																								
Investigación de Windows Terminal Server																								
Rediseño de la página del listado de software libre para la comunidad UIS																								
Estudio de la compatibilidad de Php5																								
Redefinir e implementar políticas de seguridad en el servidor.																								
Estudio preliminar sobre seguridad																								
Análisis sobre la seguridad en el servidor Cormorán																								
Realización de Backups automáticas																								
Análisis de la factibilidad de criptografiar el disco duro a nivel de Kernel.																								
Actualizar los manuales de documentación del sistema																								
Realizar el empalme correspondiente con el nuevo practicante																								

Tabla 1. Cronograma de actividades de la práctica

2. MARCO TEÓRICO

La realización de la práctica requirió investigar acerca de diferentes temas:

- ✓ Instalación y configuración de los servidores Web (Apache y Tomcat) y de Bases de Datos (Mysql y Postgresql) para poner en funcionamiento el servidor Cormorán.

- ✓ Herramienta de desarrollo php para hacer el rediseño de la página estática del listado de software libre.

- ✓ Conceptos, instalación y configuración del Servidor de Terminales en Linux.

- ✓ Conceptos del Servidor de Terminales en Windows y la viabilidad de su instalación dependiendo de las licencias.

- ✓ Seguridad informática.

2.1 SERVIDOR WEB

Un Servidor Web es un programa que implementa el *protocolo HTTP* (HyperText Transfer Protocol). Este protocolo está diseñado para transferir lo hipertextos, páginas Web o páginas HTML (HyperText Markup Language): textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de sonidos.

Un Servidor Web se mantiene a la espera de peticiones http llevada a cabo por un *cliente http*. El cliente hace una petición al servidor y éste le responde con el contenido que el cliente solicita. El cliente es el encargado de interpretar el código HTML, es decir, de mostrar las fuentes, los colores y la disposición de los textos y

objetos de la página; el servidor tan sólo se limita a transferir el código de la página sin llevar a cabo ninguna interpretación de la misma. Los dos servidores Web instalados en Cormorán son Apache y Tomcat.

2.1.1 Servidor Apache.

El servidor http Apache es un servidor http de código abierto para plataformas Unix, Windows y otras, que implementan la noción de sitio virtual. 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. Su nombre se debe a que originalmente Apache consistía solamente en un conjunto de parches a aplicar al servidor de NCSA. Era, en inglés, *A Patchy Server* (un servidor parcheado). Apache presenta entre otras características mensajes de error altamente configurables, bases de datos de autenticación y negociado de contenido, pero fue criticado por la falta de una interfaz gráfica que ayude en su configuración.

2.1.2 Servidor Tomcat.

Tomcat (también llamado Jakarta Tomcat o Apache Tomcat) funciona como un contenedor de servlets desarrollado bajo el proyecto Jakarta en la Apache Software Foundation. Tomcat implementa las especificaciones de los servlets y de JavaServer Pages (JSP) de Sun Microsystems. Se le considera un servidor de aplicaciones.

Tomcat es un Servidor Web con soporte de servlets y JSPs. Tomcat incluye el compilador Jasper, que compila JSPs convirtiéndolas en servlets. El motor de servlets del Tomcat a menudo se presenta en combinación con el servidor Web Apache. Tomcat puede funcionar como servidor Web por si mismo en entornos con alto nivel de tráfico y alta disponibilidad.

2.2 BASES DE DATOS

Una Base de Datos es un conjunto de datos estructurados y organizados independientemente de su utilización y su implementación con los usuarios concurrentes. En informática existen los sistemas gestores de bases de datos (SGBD), que permiten almacenar y posteriormente acceder a los datos de forma rápida y estructurada.

2.2.1 Tipos de bases de datos.

Atendiendo a la *variabilidad de los datos almacenados* las bases de datos pueden dividirse en:

- ✓ Bases de datos estáticas:

Estas son bases de datos de sólo lectura, utilizadas primordialmente para almacenar datos históricos que posteriormente se pueden utilizar para estudiar el comportamiento de un conjunto de datos a través del tiempo, realizar proyecciones y tomar decisiones.

- ✓ Bases de datos dinámicas:

Estas son bases de datos más dinámicas, orientadas a almacenar información que es modificada con el tiempo, permitiendo operaciones como actualización y adición de datos, además de las operaciones fundamentales de consultas.

2.2.2 Modelos de bases de datos.

Un modelo de datos es básicamente una “descripción” de algo conocido como *contenedor de datos* (algo en donde se guarda la información), así como de los métodos para almacenar y recuperar información de esos contenedores. Los modelos de datos no son cosas físicas: son abstracciones que permiten la implementación de un sistema eficiente de *bases de datos;* por lo general se refieren a algoritmos, y conceptos matemáticos. Algunos modelos con frecuencia utilizados en las bases de datos son:

✓ Bases de datos jerárquicas

Estas son bases de datos que, como su nombre indica, almacenan su información en una estructura jerárquica. En este modelo los datos se organizan en una forma similar a un árbol, en donde un *nodo padre* de información puede tener varios *hijos*. El nodo que no tiene padres es llamado *raíz,* y a los nodos que no tienen hijos se los conoce como *hojas.* Una de las principales limitaciones de este modelo es su incapacidad de representar eficientemente la redundancia de datos.

✓ Bases de datos de red

Este es un modelo ligeramente distinto del jerárquico; su diferencia fundamental es la modificación del concepto de *nodo*: se permite que un mismo nodo tenga varios padres (posibilidad no permitida en el modelo jerárquico).

Fue una gran mejora con respecto al modelo jerárquico, ya que ofrecía una solución eficiente al problema de redundancia de datos; pero, aun así, la dificultad que significa administrar la información en una base de datos de red ha significado que sea un modelo utilizado en su mayoría por programadores más que por usuarios finales.

✓ Bases de datos relacionales

Éste es el modelo más utilizado en la actualidad para modelar problemas reales y administrar datos dinámicamente. En este modelo, el lugar y la forma en que se almacenen los datos no tienen relevancia (a diferencia de otros modelos como el jerárquico y el de red). Esto tiene la considerable ventaja de que es más fácil de entender y de utilizar para un usuario esporádico de la base de datos. La información puede ser recuperada o almacenada mediante "consultas" que ofrecen una amplia flexibilidad y poder para administrar la información. El lenguaje más habitual para construir las consultas a bases de datos relacionales es SQL, *Structured Query Language* o *Lenguaje Estructurado de Consultas*, un estándar implementado por los principales motores o sistemas de gestión de

bases de datos relacionales. Durante su diseño, una base de datos relacional pasa por un proceso al que se le conoce como normalización de una base de datos.

✓ Bases de datos orientadas a objetos

Este modelo propio de los modelos informáticos orientados a objetos, trata de almacenar en la base de datos los *objetos* completos (estado y comportamiento). Una base de datos orientada a objetos es una base de datos que incorpora todos los conceptos importantes de la programación orientada a objetos:

- Encapsulación: Ocultar datos del resto de los datos, impidiendo así accesos incorrectos o conflictos.
- Herencia: Reusabilidad del código.
- Polimorfismo: Sobrecarga de operadores o de métodos.

2.3 LENGUAJE DE SCRIPT PHP

El nombre es el acrónimo de "**P**HP: **H**ypertext **P**reprocessor" con licencia open-source .PHP Se trata de un lenguaje interpretado usado para la creación de aplicaciones para servidores, o creación de contenido dinámico para sitios web. PHP tiene la capacidad de ser ejecutado en la mayoría de los sistemas operativos tales como Unix, Linux, Windows y Mac OS X y puede interactuar con los servidores de Web más populares.

2.3.1 Usos de PHP.

✓ Programación de páginas Web dinámicas, habitualmente en combinación con el motor de bases de datos Mysql, aunque cuenta con soporte nativo para otros motores, incluyendo el estándar ODBC, lo que amplía en gran medida sus posibilidades de conexión.

✓ Programación en consola, al estilo de Perl, en Linux, Windows y Macintosh.

- ✓ Creación de aplicaciones gráficas independientes del navegador, que permite desarrollar aplicaciones de escritorio tanto para los sistemas operativos basados en Unix, como para Windows y Mac OS X.

2.3.2 Ventajas de PHP.

- ✓ Acceso a la mayoría de las bases de datos comerciales y por ODBC a todas las bases de datos posibles en sistemas Microsoft, a partir de las cuales podremos editar el contenido de nuestro sitio con absoluta sencillez.

- ✓ Capacidad de expandir su potencial utilizando la enorme cantidad de módulos.

- ✓ Posee una buena documentación en su página oficial.

- ✓ Es libre, por lo que presenta una alternativa de fácil acceso para todos.

- ✓ Permite las técnicas de Programación Orientada a Objetos.

2.4 LINUX TERMINAL SERVER PROJECT

Linux Terminal Server Project (LTSP) es una excelente plataforma para el uso de estaciones de trabajo sin disco que inicien desde un servidor de red. El LTSP es un proyecto Open Source con el propósito de crear las herramientas necesarias que harán la configuración de una estación de trabajo sin disco más fácil. LTSP es un paquete que permite hacer un servidor de terminales Linux.

Terminales livianos se conectan a este servidor y usan los programas que el servidor les ofrece. Las terminales suelen sólo desplegar la información, entonces es como si se estuviera trabajando en el servidor. La ejecución de los programas puede ser realizada en el servidor o en las terminales. Actualmente uno de los campos donde se utiliza bastante LTSP es en la educación, debido al bajo costo de implantación que suele tener.

2.4.1 Características.

Las estaciones no tienen software ni disco duro, son confiables e inmunes a intrusiones y virus. La tarjeta de red está configurada para asignar direcciones IP vía DHCP. Esta configuración es flexible en que puede tener fácilmente múltiples servidores LTSP.

2.4.2 Funcionamiento.

El sistema de funcionamiento del LTSP consiste en repartir por medio de la red el núcleo de Linux que es ejecutado por los clientes y que posteriormente ejecutaran secuencias de scripts típicos de una mini distribución. Los clientes podrán acceder a las aplicaciones por medio de una consola textual o por un servidor gráfico que se comparte utilizando el protocolo XDMCP. Durante la fase de inicio, la estación de trabajo sin disco obtiene su dirección IP y un kernel (núcleo) desde el servidor, montando luego su sistema de archivos raíz desde el mismo servidor vía NFS.

2.5 WINDOWS TERMINAL SERVER

Windows Terminal Services es una tecnología que permite a uno o varios usuarios, acceder en forma remota a través de la red a aplicaciones o información contenida en un servidor Windows 2000 o superior. Este modelo cliente – servidor, ayuda a mejorar las prestaciones de los clientes, ya que todo el procesamiento de las aplicaciones se realiza en el servidor; los datos desde los dispositivos como el monitor o teclado son transmitidos entre el servidor y el cliente de los servicios de Terminal. Los denominados *Servicios de Terminal* (Terminal Server) constituyen un componente incluido en la familia de servidores Windows 2000: Windows 2000 Server, Windows 2000 Advanced Server y Windows 2000 Datacenter Server.

2.5.1 Características.

El servicio Terminal Server permite el acceso multiusuario al sistema operativo Windows 2000, de forma que varias personas puedan ejecutar sesiones simultáneamente en un mismo equipo.

2.5.2 Funcionamiento.

En un servidor con Windows Terminal Services, las estaciones clientes se conectan al servidor utilizando una sesión de “Escritorio Remoto”. En general este esquema funciona de la siguiente forma:

- ✓ El equipo Servidor centraliza todo el procesamiento. El software que utilizan los clientes se instala sólo en este servidor.

- ✓ Las estaciones de trabajo se conectan al servidor utilizando el software cliente de Escritorio Remoto.

- ✓ Las estaciones de trabajo cliente funcionan con cualquier versión de Windows capaz de ejecutar el software cliente de Escritorio Remoto: Windows 95, Windows 98, Windows Millenium, Windows 2000 y Windows XP.

- ✓ Cada vez que un cliente se enciende, se conecta de inmediato al servidor. Esta sesión de escritorio remoto es similar a trabajar en un Windows XP en el PC del cliente.

2.6 SEGURIDAD INFORMATICA

Un sistema Linux instalado tal y como se distribuye suele representar una puerta abierta para cualquier intruso sin grandes conocimientos del sistema operativo y de la red. La seguridad es una característica de un sistema informático que indica si dicho sistema está libre de peligros, daños o riesgos. Como esta característica es muy difícil de conseguir, es conveniente hablar de fiabilidad o de sistemas fiables (probabilidad de que un sistema se comporte tal y como se espera de él) y no de sistemas seguros.

2.6.1 Aspectos de seguridad.

✓ La confidencialidad

Se refiere a que un sistema debe ser accedido únicamente por personal autorizado, el cual cuidará a su vez la privacidad de sus datos para que su información no sea utilizada por alguien más.

✓ La integridad

Significa que los datos sólo pueden ser modificados por usuarios autorizados de una manera controlada.

✓ La disponibilidad

Indica que los datos del sistema tienen que permanecer accesibles a usuarios autorizados; es el contrario de la negación de servicio.

2.6.2 Elementos de Seguridad.

✓ El hardware

Se refiere a los elementos físicos de un sistema informático, como CPUs, terminales, cableado, medios de almacenamiento secundario (cintas, CD-ROMs, disquettes) o tarjetas de red**.**

✓ El software

Conjunto de programas lógicos que hacen funcional al hardware, tanto sistemas operativos como aplicaciones.

✓ Los datos

Constituyen el principal elemento a proteger, ya que es el más amenazado y el más difícil de recuperar. Normalmente un servidor Linux está ubicado en un lugar de acceso físico restringido y en caso de pérdida de una aplicación este software se puede restaurar sin problemas, pero en caso de pérdida de una base de datos o de un proyecto de un usuario se debe recurrir al sistema de copias de seguridad.

2.6.3 Tipos de amenazas.

✓ Interrupción

Cuando hace que un objeto del sistema se pierda, quede inutilizable o no disponible.

✓ Interceptación

Se trata de una interceptación cuando un elemento no autorizado consigue un acceso a un determinado objeto del sistema.

✓ Modificación

Ocurre cuando además de conseguir el acceso modifica el objeto; Existe un caso especial de la modificación: la destrucción, entendiéndola como una modificación que inutiliza al objeto afectado.

✓ Fabricación

Se dice que un ataque es una fabricación si se trata de una modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el objeto original y el `fabricado'.

2.6.4 Origen de las amenazas.

✓ Personas

La mayoría de ataques a nuestro sistema van a provenir de personas que pueden causarnos enormes pérdidas. Los diferentes tipos de personas se dividen en dos grandes grupos: los atacantes pasivos, aquellos que fisgonean por el sistema pero no lo modifican -o destruyen-, y los activos, aquellos que dañan el objetivo atacado, o lo modifican en su favor. Generalmente los curiosos y los crackers realizan ataques pasivos (que se pueden convertir en activos), mientras que los terroristas y ex-empleados realizan ataques activos puros; los intrusos remunerados suelen ser atacantes pasivos si nuestra red o equipo no es su

objetivo, y activos en caso contrario, y el personal realiza ambos tipos indistintamente, dependiendo de la situación concreta.

✓ Amenazas lógicas

Se encuentran todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello (software malicioso, también conocido como malware) o simplemente por error (bugs o agujeros).

✓ Catástrofes

Las catástrofes (naturales o artificiales) son la amenaza menos probable contra los entornos habituales: simplemente por su ubicación geográfica, la probabilidad de sufrir un terremoto o una inundación que afecte a los sistemas informáticos en una gran ciudad es relativamente baja, al menos en comparación con el riesgo de sufrir un intento de acceso por parte de un pirata o una infección por virus. Sin embargo, el hecho de que las catástrofes sean amenazas poco probables no implica que contra ellas no se tomen unas medidas básicas, ya que si se produjeran generarían los mayores daños. Como ejemplos de catástrofes hablaremos de terremotos, inundaciones, incendios, humo o atentados de baja magnitud.

2.6.5 Mecanismos de Seguridad.

✓ Mecanismos de prevención:

Son aquellos que aumentan la seguridad de un sistema durante el funcionamiento normal de éste, previniendo la ocurrencia de violaciones a la seguridad; por ejemplo, el uso de cifrado en la transmisión de datos se puede considerar un mecanismo de este tipo, ya que evita que un posible atacante escuche las conexiones hacia o desde un sistema Unix en la red.

- ✓ Mecanismos de detección

S utilizan para detectar violaciones de la seguridad o intentos de violación; ejemplos de estos mecanismos son los programas de auditoría como Tripwire.

- ✓ Mecanismos de recuperación

Son aquellos que se aplican cuando una violación del sistema se ha detectado, para retornar a éste a su funcionamiento correcto; ejemplos de estos mecanismos son la utilización de copias de seguridad o el hardware adicional.

3. LINUX TERMINAL SERVER PROJECT

Se realizó una investigación acerca de las diferentes versiones de LTSP y se decidió trabajar con *LTSP 4.1*. porque es compatible con el Sistema Operativo instalado.

3.1 INTRODUCCION

Linux Terminal Server Project (LTSP) es un conjunto de aplicaciones para servidores que proporciona la capacidad de ejecutar Linux en estaciones de baja configuración, permitiendo reutilizar equipos que actualmente resultan obsoletos. LTSP (basado en RedHat Linux / Fedora Core) consiste en repartir en una red local el núcleo de Linux que conecta un potente PC que funciona como servidor con un conjunto de PC's de poca potencia llamados terminales.

A partir del arranque, el terminal se conecta al servidor y utiliza la RAM, el procesador y el disco duro del servidor. Todos los programas residen en el servidor y los terminales ejecutan en el todo software, pudiendo así reciclar hardware viejo. La cantidad de estaciones conectadas a un único servidor LTSP depende de las características del servidor y de las aplicaciones que se desean utilizar. Actualmente uno de los campos donde se utiliza bastante LTSP es en la educación debido a su bajo costo de implementación que suele tener.

3.2 CARACTERISTICAS

Las estaciones *no tienen software ni disco duro,* son confiables e inmunes a intrusiones y virus. La instalación por defecto necesita 2 tarjetas de red Ethernet: *eth0* y *eth1*. Una conecta el servidor a Internet, la otra crea una red privada para terminales. El servidor y *eth1* actúa como un gateway para las terminales a Internet y el resto de la red. La tarjeta *eth1* esta configurada para asignar direcciones IP vía DHCP. Un servidor privado de DHCP corre en *eth0* para asignar

el numero IP a las terminales. Esta configuración es flexible en que puede tener fácilmente múltiples servidores LTSP.

3.3 MODOS DE CONFIGURACION

La estación de trabajo puede ser configurada de tres maneras:

3.3.1 Interfaz X Window - Entorno Gráfico.

Utilizando X Window, la estación de trabajo puede ser usada para acceder a cualquier aplicación en el servidor, o en cualquier otro servidor dentro de la red.

3.3.2 Sesiones de Telnet basadas en caracteres.

Cada estación de trabajo puede invocar múltiples sesiones de telnet al servidor. Cada una de estas sesiones aparecerá en una pantalla virtual separada. Presionando desde Alt-F1 hasta Alt-F9 se cambiará entre cada una de dichas sesiones.

3.3.3 Prompt de Shell.

La estación de trabajo puede ser configurada para dejarte justo dentro de una sesión de Bash en la consola. Esto es muy útil para depurar problemas con X Window o con NFS.

3.4 FUNCIONAMIENTO

El sistema de funcionamiento del LTSP consiste en repartir por medio de la red el núcleo de Linux que es ejecutado por los clientes y que posteriormente ejecutaran secuencias de scripts típicos de una mini distribución. Los clientes podrán acceder a las aplicaciones por medio de una consola textual o por un servidor gráfico que se comparte utilizando el protocolo XDMCP. Durante la fase de inicio, la estación de trabajo sin disco obtiene su dirección IP y un kernel (núcleo) desde el servidor, montando luego su sistema de archivos raíz desde el mismo servidor vía NFS.

3.4.1 Paso 1.

- ✓ El terminal arranca y mediante Etherboot realiza una petición DHCP a la red, que es respondida por el servidor DHCP que le proporciona su IP y la localización del núcleo a descargar.

3.4.2 Paso 2.

- ✓ Mediante TFTP el terminal contacta con el servidor y se descarga el núcleo, que es cargado en memoria y al que se le pasa el control a continuación.

3.4.3 Paso 3.

- ✓ El kernel inicializa el sistema y los periféricos que reconozca.

3.4.4 Paso 4.

- ✓ El kernel carga una pequeña imagen ramdisk en memoria y la monta temporalmente como sistema de archivos raíz.

3.4.5 Paso 5.

- ✓ El kernel ejecuta el script linuxrc (/linuxrc) que realiza los siguientes procesos:

- ✓ Busca en el bus PCI alguna tarjeta de red. Por cada dispositivo PCI que encuentre, realiza una búsqueda en el archivo niclist (/etc/niclist) para encontrar alguna coincidencia. Una vez encontrada una coincidencia, el nombre del módulo de driver NIC es guardado para posteriormente cargarlo en el kernel. Si la tarjeta es ISA, el nombre del módulo del driver debe ser indicado en la línea de comandos del kernel.

- ✓ Ejecuta el cliente DHCP dhclient que realiza una nueva petición DHCP para hallar la ruta del directorio raíz a montar por NFS.

- ✓ Dhclient recibe la información DHCP del servidor y ejecuta el script dhclient-script (/etc/dhclient-script), que configura la interfaz de red eth0 con la información obtenida.

- ✓ El sistema de archivos raíz está montado en la RAM, por lo que en este momento se monta un nuevo sistema de archivos raíz mediante NFS desde el servidor (por defecto el directorio exportado es /opt/ltsp/i386. Para montar este directorio como raíz el script linuxrc realiza pivot_root (intercambio del sistema de archivos raíz), por lo que el sistema de archivos NFS será montado como /, y el sistema de archivos anterior será montado en /oldroot.

3.4.6 Paso 6.

- ✓ Se ejecuta el init (/sbin/init), que realiza los siguientes procesos:

- ✓ Init lee el fichero inittab (/etc/inittab) y de acuerdo a éste comienza a preparar el sistema.

- ✓ Se ejecuta el comando rc.local mientras el sistema esté en el estado sysinit.

- ✓ El script rc.sysinit crea un un ramdisk de 1MB para almacenar lo que vaya a ser escrito ó modificado. Este espacio será montado como /tmp

- ✓ El sistema de archivos /proc es montado.

- ✓ Se lee el fichero de configuración lts.conf (/etc/lts.conf), cuyos parámetros comentaremos más adelante y que serán establecidos como variables de entorno para usar por el script rc.sysinit.

- ✓ Se crea el archivos de intercambio swap y se habilita mediante el comando swapon.

- ✓ Se configura la dirección de red loopback (127.0.0.1).

- ✓ Se monta el directorio /home del usuario.

- ✓ Se crean el directorio /tmp y subdirectorios donde se guardarán los archivos temporales y se crea en él el fichero syslog.conf (/tmp/syslog.conf) que contiene información de a qué host de la red debe enviarse la información de los logs.

3.4.7 Paso 7.

- ✓ Se cambia el runlevel a 5, con lo que se ejecutarán todas las instrucciones contenidas en inittab (/etc/inittab)

- ✓ Se inicia una sesión de las X Windows System con el comando startx (/etc/screen.d/startx), que proporciona al usuario una interfaz gráfica.

- ✓ El servidor de las X Windows System enviará una petición XDMCP (X Display Manager Control Protocol) al servidor XDM (X Display Manager) que le responderá con una pantalla de inicio de login de usuario.

3.5 CARACTERISTICAS ESPECIFICAS DEL LTSP 4.1

- ✓ Nuevo Instalador ltspadmin: Este nuevo instalador es mucho más fácil para actualizar paquetes y para instalarlos. El instalador sabrá cual versión de paquetes tiene instalado y revisara el almacén de paquetes para ver si hay actualizaciones disponibles.

- ✓ Cambia de XFree86 a Xorg. LTSP esta ahora usando las librerías y servidores X del proyecto Xorg, mas bien que el proyecto XFree86.

- ✓ Soportes locales en CD y disquette. Usando supermount y samba en el cliente y el automounter en el servidor, nosotros podremos hacer los drivers en CD-ROM y floppy disponibles a los usuarios.

- ✓ Soporte de sonido con esd y nasd. Los demonios de sonido en el cliente ahora están incluidos para esound y nasd.

3.6 FORMAS DE INSTALAR LTSP 4.1

3.6.1 Instalador LTSP mediante rpm o tgz.

- ✓ Descargar e instalar los paquetes (RPM o TGZ)
  - ltsp_core
  - ltsp_kernel
  - ltsp_x_core
  - ltsp_x_fonts

- ✓ Iniciar sesión como root

- ✓ Desde una consola ejecutar ltspadmin

- ✓ Si tiene una versión anterior de LTSP ya instalada, es recomendable instalar los paquetes ltsp 4.1 en un directorio separado como /opt/ltsp4.1

- ✓ Instalar Todos los paquetes

- ✓ Escoja la opción Configure LTSP en el menú el cual causara que la utilidad ltspcfg se ejecute. Use esta utilidad para configurar los servicios.

3.6.2 Instalar LTSP mediante imagen ISO.

Los paquetes de imágenes ISO del LTSP-4.1 han sido creados para esos quienes quieren descargar un archivo sencillo e instalarlo en múltiples servidores sin requerimientos de descargas adicionales.

- ✓ Descargar la imagen ISO y guardarla en /tmp

- ✓ Iniciando sesión como root montar la imagen ISO, usando el dispositivo loopback:
  # mount -o loop /tmp/<imagen iso> /mnt

- ✓ Instalar el paquete ltsp-utils (El paquete ltsp-utils esta incluido con la imagen)

- ✓ Ejecutar ltspadmin como usuario administrador root para realizar la instalación de todos los paquetes.

- ✓ Escoger la opción Configure LTSP en el menú, el cual causará que la utilidad ltspcfg se ejecute. Esta utilidad configura los servicios del LTSP.

- ✓ Al terminar su trabajo se necesita desmontar la imagen ISO de /mnt
  # umount /mnt

3.7 INSTALACION Y CONFIGURACIÓN DE LTSP

La instalación y configuración del servidor LTSP se realizó en el equipo de respaldo de Cormorán y como terminales se utilizaron los PC's de la sala 3 del laboratorio Villabona. Para el desarrollo de la práctica fue indispensable conocer la dirección IP y la MAC de cada uno de los equipos clientes y también conocer la organización del cableado que cubre estos equipos clientes y el PC servidor en el sistema LTSP.

En un sistema LTSP el servidor de terminales LTSP establece conexiones con los PC's clientes mediante el servicio DHCP (en una misma organización es posible manejar varios DHCP) para asignar la dirección IP a los equipos clientes (la asigna el primer servidor DHCP que contesta). Es aconsejable conectar los terminales al mismo switch que el servidor LTSP (DHCP maneja prioridades con los PC's que están conectados a un mismo switch o hub de la red). Por este motivo es importante conocer la distribución de los diferentes puntos de la red que involucran el servidor ubicado en la sala 103 y los terminales ubicados en la sala 3 del Villabona.

3.7.1 Distribución de Equipos de Cómputo del Sistema LTSP.

Los equipos de cómputo utilizados como terminales LTSP se encuentran ubicados en la sala 3 del laboratorio Villabona y su distribución es la siguiente:

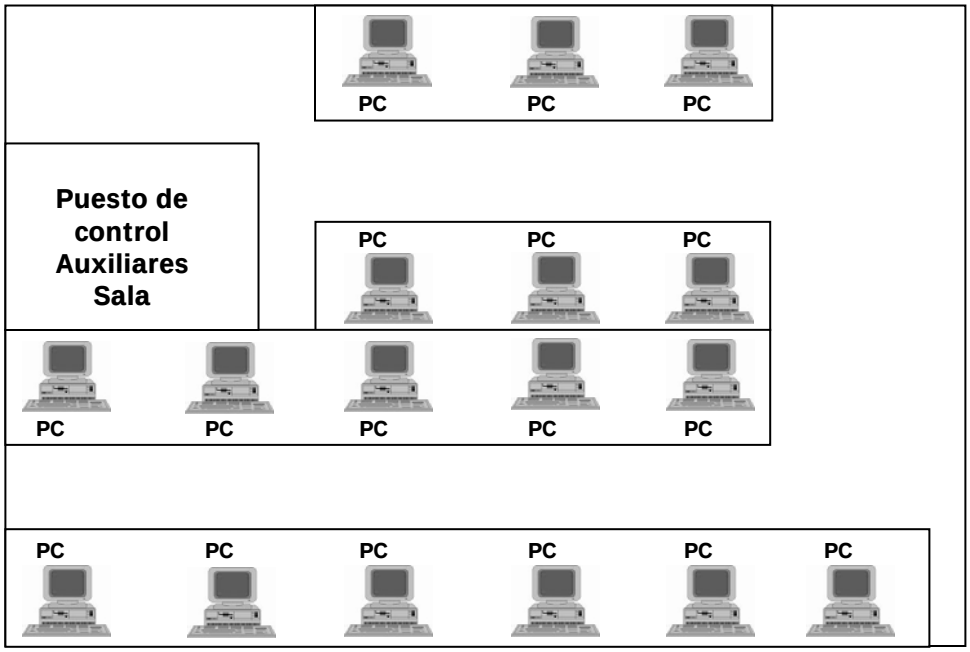

Figura 2. Distribución de equipos de cómputo del Sistema LTSP

El equipo de cómputo utilizado como servidor LTSP (PC 65) se encuentra ubicado en la oficina 103 del edificio Laboratorio de Pesados donde se encuentran los servidores de la EISI.

3.7.2 Direcciones IP, direcciones MAC y puntos de conexión de los equipos de cómputo del sistema LTSP.

Todos los equipos de cómputo utilizados como terminales LTSP se encuentran conectados en el Rack 1 Patch Panel 7 del centro de cableado del primer piso del edificio llamado *"Laboratorio de Pesados"*. El inconveniente es que este Patch Panel distribuye sus puntos para diferentes hubs, siendo esto una limitante para la funcionalidad del sistema LTSP. La siguiente información corresponde a las direcciones MAC, las direcciones IP de las terminales y la información acerca de los puertos ocupados por estos equipos en el Rack 1 de comunicaciones (Patch Panel 7) ubicado en el primer piso:

PC	MAC	IP	Puerto
31	00:0D:56:4E:C1:6B	192.168.84.31	26
32	00:0D:56:4E:AD:FA	192.168.84.32	24
33	00:0D:56:4E:AD:F8	192.168.84.33	25
34	00:0D:56:4E:AC:AB	192.168.84.34	08
35	00:0D:56:4E:AF:19	192.168.84.35	04
36	00:0D:56:4E:B0:42	192.168.84.36	01
37	00:0D:56:4E:AD:FB	192.168.84.37	02
38	00:0D:56:4E:AD:72	192.168.84.38	05
39	00:0D:56:4E:AF:2B	192.168.84.39	07
40	00:0D:56:4E:AC:A5	192.168.84.40	09
41	00:0D:56:4E:A8:FB	192.168.84.41	10
42	00:0D:56:4E:AD:37	192.168.84.42	13
43	00:0D:56:4E:C1:6F	192.168.65.43	12
44	00:0D:56:4E:C1:88	192.168.84.44	14
45	00:0D:56:4E:AD:85	192.168.84.45	15
46	00:0D:56:4E:AF:1C	192.168.84.46	17
47	00:0D:56:4E:AB:F7	192.168.84.47	16

El procedimiento seleccionado para la instalación y configuración del Sistema LTSP fué mediante la imagen ISO el cual se describe a continuación:

3.7.3 Configurar la NIC en el PC servidor.

- ✓ Dirección IP: 192.168.84.65
- ✓ Mascara de Subred: 255.255.255.0
- ✓ Dirección de Puerta de Enlace Predeterminada: 192.168.84.1

3.7.4 Reiniciar el demonio de la tarjeta de red.

Abrir una consola y digitar el comando */etc/rc.d/init.d/network restart*

3.7.5 Instalar LTSP 4.1 como imagen ISO.

- ✓ Descargar la imagen ISO y guardarla en /tmp

- ✓ Desde una consola ejecutar md5sum ltsp-4.1.1-1.iso

- ✓ Montar la imagen mediante mount -o loop /tmp/ ltsp-4.1.1-1.iso /mnt

- ✓ Instalar el paquete ltsp-utils mediante rpm -ivh ltsp-utils-0.11-0.noarch.rpm

3.7.6 Ejecutar ltspadmin como root.

- ✓ Seleccionar la primera opción del menu Install/Update LTSP Packages para instalar los paquetes LTSP
  - Especificar la ruta donde se encuentran los archivos: file:///mnt
  - Directorio en el cual desea ubicar el Sistema de Archivos /opt/ltsp
  - Proxy HTTP: none
  - Proxy FTP none

- ✓ Seleccionar todos los paquetes

Para instalar todos los paquetes incluidos en la imagen.

- ✓ Seleccionar “Show de status of all services”

Para verificar el estado de todos los servicios configurados.

- ✓ Seleccionar “Configure the services manually”

Para configurar los servicios manualmente. Esta es la parte más importante de la configuración del servidor LTSP. Se debe pasar paso a paso por cada uno de las diferentes opciones:

✓ Runlevel:

Actualmente esta configurado el runlevel 5 si no desea cambiarlo solo se debe presionar Enter. Runlevel 5 indica que el sistema esta en modo grafico.

select a runlevel (2,3,4,5) [5]:

✓ Interface selection

Detecta las tarjetas de red que están conectadas en el equipo y muestra la información de configuración de cada una.

Interface Usada: eth1
Direccion IP: 192.168.65.18
Netmask: 255.255.255.0
Network: 192.168.65.0
Broadcast: 192.168.65.255

✓ DHCP configuration

Hay dos pasos principales para configurar dhcpd:

1. Habilitar el demonio para ejecutarlo cuando el sistema es iniciado.
Do you want to enable the dhcpd.conf (y/n) ? y
2. Construir el archivo de configuracion
Do you want to build a dhcpd.conf file (y/n) ? y

✓ TFTP configuration

Es suficiente con presionar Enter para habilitar tftp. Sale mensaje informando que el tftp ha sido iniciado exitosamente

tftpd has been succesfully started.

✓ Portmapper configuration

El Portmapper ya está habilitado, solo se presiona Enter para continuar.

✓ NFS configuration

Para habilitar el NFS se presiona Enter. La configuración habilita el demonio NFS para arrancar el sistema.

✓ XDMCP configuration

XDMCP es el protocolo usado por el display manager para presentar una caja de dialogo de Login en la estación de trabajo. Para habilitar este servicio se presiona Enter. Algunas personas prefieren trabajar su servidor en Modo texto y las terminales en Modo gráfico. Para ello se debe configurar que no deshabilite el Login grafico en el servidor.

✓ create /etc/hosts entries

Para agregar entradas a /etc/hosts se presiona Enter.

✓ create /etc/hosts.allow entries

Para agregar entradas a /etc/hosts.allow se presiona Enter.

✓ create /etc/exports entries

Para agregar entradas a /etc/exports se presiona Enter.

✓ create lts.conf file

Para crear el archivo por defecto lts.conf se presiona Enter.

3.7.7 Verificar la instalación y configuración del LTSP.

✓ Versión del Kernel

Verificar cual es la versión del kernel que los PC's clientes van a utilizar. El kernel instalado se ubica en */tftpboot/lts***.** La verificación se realiza para poder modificar el archivo *dhcpd.conf* ubicado en */etc* en donde se debe especificar la versión del kernel que debe cargar los PC's clientes. Se eligió vmlinuz-2.4.26-ltsp-3.

- ✓ Ruta de instalación del LTSP
  - Verificar cual es la ruta donde se instaló el sistema de archivos del LTSP. Debe quedar en /opt/ltsp/i386

  - Para que el NFS funcione adecuadamente se le debe indicar cual es la ruta donde se encuentran los archivos que debe exportar. Si en el proceso de instalación del LTSP se utilizó la ruta que venía por defecto (/opt/ltsp) efectivamente allí se encontrarán los archivos ya instalados.

  - También el DHCP trabaja con la ruta /opt/ltsp. Se debe verificar que su archivo de configuración (/etc/dhcpd.conf) en la opción option root-path contenga la dirección IP del servidor de terminales y la ruta de los archivos de configuración del LTSP como se muestra a continuación:

- ✓ Revisar los archivos de configuración

  - Archivo /etc/hosts
    Este es el archivo de configuración del DNS. En este archivo se encuentran las direcciones IP de todos los posibles clientes de esta subred. Como el servidor tiene IP 192.168.84.65 entonces los PC's clientes tienen direcciones IP 192.168.84.XX. Estas direcciones van desde 192.168.84.1 hasta 192.168.84.254 exceptuando la IP del servidor.

  - Archivo /etc/hosts.allow
    En este archivo se reservan las direcciones con los octetos de IP de los equipos clientes que pertenecen a la subred de IP 192.168.84.

  - Archivo /etc/dhcpd.conf
    Este es el archivo de configuración del DHCP. Este archivo es muy importante porque es aquí donde se registra la información necesaria para

los PC's clientes. Aquí se registran tanto la dirección IP como la dirección física o MAC de cada uno de los PC's clientes. En este archivo se deben realizar varias operaciones:

1. Para versiones de LTSP 3.0 y superior se debe agregar la línea

ddns-update-style none;

2. Arreglar el nombre del dominio en la opción:

option domain-name “ltsp.com”;

3. Verificar que la ruta en *option root-path* contenga la dirección IP del servidor de terminales y la ruta del sistema de archivos del LTSP:

option root-path “192.168.84.65:/opt/ltsp/i386”;

4. Crear una red de trabajo compartido:

```
shared-network WORKSTATIONS {
        subnet 192.168.84.0 netmask 255.255.255.0 {
        }
}
```

5. Crear un grupo para todos los PC's clientes y agregarle la configuración de cada cliente. A continuación se muestra un ejemplo para dos PC’s clientes:

```
group   {
        use-host-decl-names      on;
        option log-servers       192.168.84.65;

        host ws031 {
         hardware ethernet    00:0D:56:4E:C1:6B;
         fixed-address        192.168.84.31;
         filename             "/lts/vmlinuz-2.4.26-ltsp-3";
         }
         host ws032 {
```

```
hardware ethernet    00:0D:56:4E:AD:FA;
fixed-address        192.168.84.32;
filename             "/lts/vmlinuz-2.4.26-ltsp-3";
}
                    }
```

Nota: Es indispensable conocer la dirección física o *MAC* de las tarjetas de Red de cada PC cliente. Además se le asignará una dirección IP distinta para cada PC cliente en la red, así como se le dará la versión del kernel que debe cargar.

Hardware ethernet: Dirección física de la tarjeta de Red

Fixed-address: Dirección IP configurada para el PC

Filename: Identificación del kernel que cargara el PC cliente.

El archivo dhcpd.conf para los PC's clientes de la sala 3 del laboratorio Villabona quedó configurado de la siguiente forma:

```
ddns-update-style                   none;
default-lease-time                  21600;
max-lease-time                      21600;

option subnet-mask                  255.255.255.0;
option broadcast-address            192.168.84.255;
option routers                      192.168.84.65;
option domain-name-servers          192.168.84.65;
option domain-name                  "ltsp.com";

option root-path   “192.168.84.65:/opt/ltsp/i386";
option option-128 code 128 = string;
option option-129 code 129 = text;

shared-network WORKSTATIONS {
subnet 192.168.84.0 netmask 255.255.255.0 {
      }
}
group   {
   use-host-decl-names      on;
```

```
   option log-servers          192.168.84.65;

host ws031 {
       hardware ethernet    00:0D:56:4E:C1:6B;
       fixed-address        192.168.84.31;
       filename             "/lts/vmlinuz-2.4.26-ltsp-3";
   }

host ws032 {
       hardware ethernet    00:0D:56:4E:AD:FA;
       fixed-address        192.168.84.32;
       filename             "/lts/vmlinuz-2.4.26-ltsp-3";
   }

host ws033 {
       hardware ethernet    00:0D:56:4E:AD:F8;
       fixed-address        192.168.84.33;
       filename             "/lts/vmlinuz-2.4.26-ltsp-3";
   }

host ws034 {
      hardware ethernet    00:0D:56:4E:AC:AB;
       fixed-address        192.168.84.34;
       filename             "/lts/vmlinuz-2.4.26-ltsp-3";
   }

host ws035 {
      hardware ethernet    00:0D:56:4E:AF:19;
       fixed-address        192.168.84.35;
       filename             "/lts/vmlinuz-2.4.26-ltsp-3";
   }

host ws036 {
       hardware ethernet    00:0D:56:4E:B0:42;
       fixed-address        192.168.84.36;
       filename             "/lts/vmlinuz-2.4.26-ltsp-3";
   }

host ws037 {
       hardware ethernet    00:0D:56:4E:AD:FB;
       fixed-address        192.168.84.37;
       filename             "/lts/vmlinuz-2.4.26-ltsp-3";
   }
host ws038 {
       hardware ethernet    00:0D:56:4E:AD:72;
```

```
        fixed-address       192.168.84.38;
        filename            "/lts/vmlinuz-2.4.26-ltsp-3";
    }

host ws039 {
        hardware ethernet   00:0D:56:4E:AF:2B;
        fixed-address       192.168.84.39;
        filename            "/lts/vmlinuz-2.4.26-ltsp-3";
    }

host ws040 {
        hardware ethernet   00:0D:56:4E:AC:A5;
        fixed-address       192.168.84.40;
        filename            "/lts/vmlinuz-2.4.26-ltsp-3";
    }

host ws041 {
        hardware ethernet   00:0D:56:4E:A8:FB;
        fixed-address       192.168.84.41;
        filename            "/lts/vmlinuz-2.4.26-ltsp-3";
    }

host ws042 {
        hardware ethernet   00:0D:56:4E:AD:37;
        fixed-address       192.168.84.42;
        filename            "/lts/vmlinuz-2.4.26-ltsp-3";
    }

host ws043 {
        hardware ethernet   00:0D:56:4E:C1:6F;
        fixed-address       192.168.65.43;
        filename            "/lts/vmlinuz-2.4.26-ltsp-3";
    }

host ws044 {
        hardware ethernet   00:0D:56:4E:C1:88;
        fixed-address       192.168.84.44;
        filename            "/lts/vmlinuz-2.4.26-ltsp-3";
    }

host ws045 {
        hardware ethernet   00:0D:56:4E:AD:85;
        fixed-address       192.168.84.45;
        filename            "/lts/vmlinuz-2.4.26-ltsp-3";
    }
```

```
host ws046 {
        hardware ethernet    00:0D:56:4E:AF:1C;
        fixed-address        192.168.84.46;
        filename             "/lts/vmlinuz-2.4.26-ltsp-3";
    }

host ws047 {
        hardware ethernet    00:0D:56:4E:AB:F7;
        fixed-address        192.168.84.47;
        filename             "/lts/vmlinuz-2.4.26-ltsp-3";
    }

}
```

- Archivo /etc/exports

  Este es el archivo de configuración del NFS. Es fundamental indicar la ruta del Sistema de Archivos para poderlo exportar a los PC's clientes. En el proceso de instalación del LTSP se especifica la ruta exacta del directorio. Si en el momento de instalarse se realizó por ejemplo sobre */opt/ltsp4.1* entonces el archivo *exports* cambiaría la ruta a */opt/ltsp4.1* y */var/opt/ltsp4.1/swapfiles* respectivamente. El archivo *exports* para exportar el Sistema de Archivos a los PC's clientes quedará configurado de la siguiente forma:

- Archivo /opt/ltsp/i386/etc/lts.conf

  Este es el archivo de configuración del LTSP que por defecto queda modificado con la información suministrada en el proceso de instalación. En este archivo no es necesario hacer modificaciones.

- Archivo /etc/xinetd.conf

  Este es el archivo de configuración del TFTP. Este archivo también queda configurado con la información suministrada en el momento de la instalación del LTSP. No es necesario realizar modificaciones en este archivo.

3.7.8 Reiniciar los servicios.

- ✓ Reiniciar la Tarjeta de Red
- ✓ Reiniciar NFS
- ✓ Reiniciar DNS
- ✓ Reiniciar TFTP
- ✓ Reiniciar DHCP

3.7.9 Crear el disquette universal.

- ✓ Descargar el disquete de Arranque universal

Abrir un navegador para descargar el disquete de Arranque Universal de la dirección *http://sf.net/project/showfiles.php?group_id=80408&release_id=165260*

- ✓ Descomprimir y grabar en disquete:

Abrir una consola y entrar a la ruta donde se encuentra el disquete previamente descargado en el numeral anterior. Luego escribir los siguientes comandos:

```
# unzip  BootDisk522.zip
# dd  if=ebnet522.dsk  of=/dev/fd0
```

3.7.10 Arrancar el PC cliente.

- ✓ Configurar el arranque del PC cliente

Para que el PC cliente reconozca el disquette universal se debe configurar en el setup la más alta prioridad de arranque por disquette.

- ✓ Insertar el disquette universal

Al arrancar el sistema por el disquette se visualizara el proceso de carga del sistema.

4. WINDOWS TERMINAL SERVER

4.1 SERVIDOR DE SERVICIOS DE TERMINAL SERVER

El servidor administra los recurso informáticos para cada sesión de cliente y ofrece un entorno único a todos los usuarios que tienen iniciada una sesión. El servidor recibe y procesa todas las pulsaciones del teclado y las acciones del ratón que realiza el cliente remoto, y dirige al cliente apropiado todo el resultado que aparece en la pantalla tanto para el sistema operativo como para las aplicaciones.

4.2 CLIENTE DE SERVICIOS DE TERMINAL SERVER

La sesión de Terminal se abrirá como una ventana en el escritorio de equipos cliente. Dentro de dicha ventana se ejecuta el escritorio remoto del servidor de Terminal. El equipo cliente sólo necesita la cantidad mínima de software necesario para establecer una conexión con el servidor y presentar la interfaz de usuario.

4.3 PROTOCOLO DE ESCRITORIO REMOTO

El Remote Desktop Protocol o RDP permite la comunicación entre cliente y el servidor. Este protocolo está optimizado para mover elementos de la interfaz gráfica al cliente. RDP es un protocolo de la capa de aplicación que se basa en TCP/IP para transportarlo por la red. RDP se basa en el estándar T.120 de International Telecommunication Union (ITU) para conferencia multicanal.

4.4 MODOS DE TRABAJO

Los Servicios de Terminal pueden ser habilitados en dos modos diferentes:

4.4.1 Servidor de aplicaciones.

En el modo de servidor de aplicaciones, puede distribuir y administrar aplicaciones desde un lugar centralizado, lo que ahorra a los administradores tiempo de

desarrollo y de distribución, así como el tiempo y el trabajo necesarios para el mantenimiento y la actualización. Puede instalar aplicaciones directamente en el servidor de Terminal Server o usar una instalación remota. Por ejemplo, puede usar la política de grupo y Active Directory para publicar paquetes de la aplicación de instalación de Windows en un servidor o grupo de servidores de Terminal Server. Las aplicaciones sólo pueden ser instaladas por un administrador, por cada servidor, y solamente si está habilitada la configuración apropiada de la política de grupo.

4.4.2 Administración remota.

La administración remota ofrece a los administradores de sistemas un método avanzado para administrar a distancia cualquier servidor de Windows 2000 a través de cualquier conexión TCP/IP. El modo de administración remota sólo instala los componentes de acceso remoto de los Servicios de Terminal Server. El modo de administración remota de los Servicios de Terminal ofrece las siguientes características y ventajas:

- ✓ Administración gráfica de los servidores Windows 2000 desde cualquier cliente de Servicios de Terminal (administrar archivos y compartir la impresión, modificar el registro de otro equipo de la red o realizar cualquier tarea como si estuviera usando la consola).

- ✓ Posibilidad de actualizaciones remotas, reboots y promociones de controladores de dominio.

- ✓ Acceso a servidores a través de conexiones bajo ancho de banda.

- ✓ Instalación de aplicaciones de forma remota y ejecución de las mismas.

- ✓ La sesión de la consola no se ve afectada mientras tiene lugar la administración remota.

- ✓ No se ve afectado el rendimiento.

- ✓ No se necesitan licencias.

- ✓ Dos administradores remotos pueden compartir una sesión con propósitos de colaboración.

4.5 FUNCIONAMIENTO

En un servidor con Windows Terminal Services, las estaciones clientes se conectan al servidor utilizando una sesión de “Escritorio Remoto”. En general este esquema funciona de la siguiente forma:

- ✓ El equipo Servidor centraliza todo el procesamiento. El software que utilizan los clientes se instala sólo en este servidor.

- ✓ Las estaciones de trabajo se conectan al servidor utilizando el software cliente de Escritorio Remoto.

- ✓ Las estaciones de trabajo cliente funcionan con cualquier versión de Windows capaz de ejecutar el software cliente de Escritorio Remoto: Windows 95, Windows 98, Windows Millenium, Windows 2000 y Windows XP.

- ✓ Cada vez que un cliente se enciende, se conecta de inmediato al servidor. Esta sesión de escritorio remoto es similar a trabajar en un Windows XP en el PC del cliente.

4.6 LICENCIAS

4.6.1 Licencias Requeridas.

La distribución de los Servicios de Terminal Server y los clientes de Servicios de Terminal Server en una red requiere las siguientes licencias:

- ✓ Licencia de Windows 2000 Server

Esta licencia se incluye al adquirir el producto.

- ✓ Licencia de acceso de cliente para Windows 2000 Server

Se requiere para cada dispositivo que se conecte con Windows 2000 Server. Las Licencias de acceso de cliente permiten a los clientes utilizar los servicios de archivos, impresión y otros servicios de red proporcionados por Windows 2000 Server. El componente de Servicios de Terminal Server de Windows 2000 Server requiere licencias por puesto para la licencia de acceso de cliente de Windows 2000 Server, excepto cuando se adquiere la licencia para el Conector de Internet de los Servicios de Terminal Server de Windows 2000. Cada equipo o terminal cliente requiere las siguientes licencias:

- ✓ Licencia de acceso de cliente para los Servicios de Terminal Server de Windows 2000 o licencia para Windows 2000

La licencia de acceso de cliente proporciona a cada equipo o terminal cliente basado en Windows el derecho legal de acceso a los Servicios de Terminal Server en un servidor de Windows 2000 Server. Por ejemplo, es necesaria para iniciar una sesión de terminal y ejecutar en el servidor aplicaciones basadas en Windows. La licencia de Windows 2000 permite la instalación del sistema operativo Windows 2000, además de proporcionar el derecho legal para el acceso a los Servicios de Terminal Server en un servidor de Windows 2000 Server. La Licencia de acceso de cliente para Terminal Server no se requiere para los clientes que sólo se conectan con servidores de Terminal Server en el modo de administración remota.

4.6.2 Licencias opcionales de Servicios de Terminal Server.

Además de las licencias de Servicios de Terminal Server requeridas, están disponibles dos licencias opcionales: la licencia de conector de Internet de los Servicios de Windows 2000 Terminal Server y la licencia de acceso de cliente de los Servicios de Terminal Server de Windows 2000 Work at Home.

- ✓ Licencia de conector de Internet para Servicios de Windows 2000 Terminal Server

Existe la posibilidad de adquirir, en lugar de licencias de acceso de cliente, la licencia del Conector de Internet para Servicios de Windows 2000 Terminal Server. Esta licencia se adquiere por separado y es una licencia complementaria de Windows 2000 Server que permite la conexión anónima de un máximo de 200 usuarios simultáneos con un servidor de Terminal Server a través de Internet. Los usuarios que tengan acceso a un servidor de Terminal Server con esta licencia no pueden ser empleados de la empresa.

- ✓ Licencia de acceso de cliente para Servicios de Terminal Server de Windows 2000 Work at Home

Aquellas organizaciones que deseen usar los Servicios de Terminal Server para proporcionar a sus empleados acceso desde sus casas al equipo de escritorio de Windows 2000 y a las aplicaciones de 32 bits basadas en Windows, disponen de la licencia de acceso de cliente para Servicios de Terminal Server de Work at Home mediante los programas de licencia de Microsoft Volume. Por cada Licencia de acceso de cliente para Windows 2000 Professional o los Servicios de Terminal Server que adquiera, puede comprar una licencia de acceso de cliente adicional para Servicios de Terminal Server de Windows 2000 Work at Home.

4.7 CREACIÓN DE DISCOS DE INSTALACIÓN DEL CLIENTE

Al instalar Servicios de Terminal Server Windows 2000 incluye la herramienta administrativa Creador del Cliente de Servicios de Terminal Server, con la que puede crear los discos de instalación para el software del cliente. Para crear los discos de instalación del cliente, hay que seguir los siguientes pasos:

- ✓ En el menú Herramientas administrativas, abrir Creador de cliente de Servicios de Terminal Server.

- ✓ Seleccionar el tipo de software Cliente de Servicios de Terminal Server que desea crear. Hay dos opciones: Serv. De Terminal Server para Windows de 16 bits (requiere 4 discos) y Serv. De Terminal Server para Windows de 32 bits (requiere 2 discos).

- ✓ Introducir un disco en la unidad destino.

- ✓ Después de copiar los archivos a los discos, cerrar el cuadro de diálogo Crear discos de instalación o hacer clic en Aceptar para crear más discos.

4.8 CONFIGURACIÓN DE LOS EQUIPOS DE CÓMPUTO

Antes de poder llevar a cabo este recorrido completo, se requiere la configuración siguiente:

4.8.1 Servidor.

Windows 2000 Server con soporte de red y con requerimientos mínimos de:

- ✓ Procesador de 2 Ghz
- ✓ 1 GB de memoria RAM
- ✓ 40 GB de disco duro
- ✓ Lector de CD o DVD
- ✓ tarjeta de red 10/100

4.8.2 Clientes.

Windows 95 o superior instalado con soporte de red.

4.9 DIFERENCIAS ENTRE WINDOWS TERMINAL SERVER Y LINUX TERMINAL SERVER.

	Linux	Windows
Instalación de Sistema Operativo	Sólo se instala en el servidor	Se instala en el servidor Windows 2000 Server y en los clientes Windows 2000 Professional
Plataforma de uso	Funciona sobre cualquier distribución	Funciona sobre Windows 2000 o superior
Creación de disquetes de arranque	Sólo uno	Uno o varios dependiendo del modo de trabajo.
Configuración del Terminal Server	Sólo se configura el servidor	Se configura servidor y clientes
Arranque de las terminales	Booteo desde disquete	Sobre Windows 2000 Professional como una aplicación
Licencias	Trabaja bajo la GNU/GPL	Debe adquirir licencias para el Sistema Operativo y para el servicio de Terminal Server por cada equipo

Tabla 2. Diferencias entre Windows Terminal Server y Linux Terminal Server

5. SEGURIDAD INFORMÁTICA

5.1 INTRODUCCIÓN

Siendo conscientes de la vulnerabilidad del sistema y los posibles ataques a los que está expuesto el servidor, se hace necesario implementar mecanismos de seguridad para garantizar la confidencialidad, integridad y disponibilidad de la información. Para ello se debe efectuar diferentes labores de prevención de violaciones de seguridad, detección de intrusos y recuperación de la información.

A continuación se muestra diferentes "mecanismos de recuperación de información" llevados a cabo en el servidor Cormorán:

5.2 REALIZACIÓN DE BACKUPS (COPIAS DE SEGURIDAD)

5.2.1 Consideraciones para realizar los Backups.

Teniendo en cuenta que existen problemas relacionados con los medios de almacenamiento y los peligros de su entorno cuando se realizan backups, se deben tener en cuenta las siguientes consideraciones:

- ✓ El backup debe ser diferente al medio del cual estamos tomando los datos originales: No sirve de mucho almacenar el backup de un disco duro en ese mismo disco.

- ✓ El backup no debe residir en el mismo lugar físico que el medio origen: El backup no debe permanecer en el mismo equipo, pues si ocurre un siniestro o robo en dicho lugar, el backup no habrá servido de nada. Lo ideal es generar varias copias del medio destino y guardarlo en diferentes

ubicaciones físicas dispersas. Debe tenerse en cuenta que el medio destino también puede presentar fallas a la hora de restaurar los archivos.

- ✓ El backup debe guardarse en un lugar seguro, seco y fresco: Tener en cuenta las condiciones del ambiente que requiere el medio para mantener los datos libres de peligro. No deben exponerse al calor, la humedad ni a campos electromagnéticos ya que se podrían dañar.

- ✓ El backup debe etiquetarse en forma ordenada y clara: Deben incluir la fecha, el tipo de backup efectuado, la especificación del origen del backup (ej.: unidad C:, máquina x; ruta completa de la carpeta inicial, etc.), el número del medio y la cantidad utilizada en total para ese backup (ej.: 1/3).

- ✓ Debe verificarse que los datos almacenados en el backup son los correctos: Debe verificar que se pueda acceder a los datos sin inconvenientes.

- ✓ Backup es backup: Cuando hablamos de backup no se refiere a cualquier mecanismo de recuperación de datos implementado en el sistema, como ser el espejado de discos, replicación de servidores o diferentes configuraciones RAID, sino a la copia de archivos en medios removibles.

5.2.2 Tipos de Backup.

Cuando se diseña un plan de backups para un sistema, se debe tener en cuenta algunas estrategias que ayudarán a que el plan sea más conveniente y lograr el mejor costo/beneficio posible, minimizando los tiempos de respuesta, es decir, el tiempo invertido en recuperar los datos en caso de cualquier desastre. Las clases de backup con los cuales se puede establecer una estrategia son:

✓ Backup Completo:

Se crea una copia de resguardo de todas las carpetas y archivos. Es ideal para crear la primera copia de todo el contenido de una unidad o bien de sus archivos de datos solamente. Entre sus Ventajas están:

- Todos los archivos seleccionados pasan a formar parte de este backup.
- Para restaurar uno o mas archivos, se los toma directamente de este backup.

✓ Backup Incremental:

Esta clase de backup solamente genera una copia de resguardo con todos aquellos archivos que hayan sido modificados (o aparenten haberlo sido debido a cambios en su fecha de modificación) o se hayan creado desde el último backup realizado, ya sea este último incremental o completo. Si se utiliza por primera vez en una unidad en vez de un backup completo, se comportará como este último, pero en los backups siguientes, irá copiando solamente lo nuevo o lo modificado.

Algunas ventajas son:

- Es mucho más rápido que el uso de sucesivos backups completos.
- Requiere menor cantidad de espacio en el medio destino que sucesivos backups completos.
- Se pueden ir manteniendo diferentes versiones de los mismos archivos en cada uno de los backups incrementales, con lo que se podría restaurar la versión deseada.

Algunas desventajas son:

- Se pueden estar copiando archivos cuyo contenido no haya sido modificado, ya que compara las fechas de modificación, y se pueden haber guardado sin que se hayan efectuado cambios en su contenido.

- Para restaurar determinados archivos o inclusive, todos, es necesario tener todos los medios de los backups incrementales que se hayan efectuado desde el último backup completo o primer backup incremental.
- Como consecuencia de esta búsqueda por varios backups, la restauración de unos pocos archivos toma mucho mas tiempo.

✓ Backup Diferencial:

Es similar al incremental, la única diferencia es que compara el contenido de los archivos a la hora de determinar cuáles se modificaron de manera tal que solamente copia aquellos que hayan cambiado realmente y no se deja engañar por las fechas de modificación de los mismos.

Algunas ventajas son:

- Todas las del backup incremental, pero requieren aún menor espacio en el medio de destino.

Algunas desventajas son:

- Todas las del backup incremental, menos la última.
- No todas las herramientas del backup dan soporte a esta clase.

5.2.3 Definir la estrategia.

Las diferentes clases de backup se pueden combinar entre sí para definir una estrategia de backup. Pero antes se debe tener en cuenta dos factores importantes.

✓ Frecuencia del Backup:

Indica cada cuanto tiempo se debe hacer un backup y restringe junto con el medio destino la clase de backup que se puede efectuar. Dependerá del volumen de datos y de la frecuencia con la que se modifican los mismos (tanto cambios en archivos como la generación de nuevos). Si éstos son muy frecuentes y el costo

de los datos lo justifica ante el costo de los backups, se podrían hacer cada cierta cantidad de horas. Si se considera que no hace falta tanta frecuencia, podríamos hablar de uno por día y en el caso de un uso hogareño en el cual los cambios en los datos dependen del uso de la máquina, tal vez se debe considerar la opción de hacer un backup los días que modifiquemos datos y uno semanal fijo.

✓ Volumen de Datos a Resguardar:

Si no es muy grande y el tiempo de backup es corto lo mejor por las ventajas que ofrece es el backup completo. Si no es así, se debe pensar en la combinación de varias clases para obtener el mejor costo/beneficio.

5.2.4 Recomendaciones.

✓ Hacer varios backup

Independientemente de la combinación de clases de backup que seleccione, nunca se debe quedar con un solo conjunto de copias para recuperar desde allí los datos. Siempre debe tener al menos dos juegos de backup históricos ya que, por ejemplo, podría haber contraído un virus y efectuar un backup de todos los archivos con virus. Si en ese caso tiene el juego anterior, puede recuperarlos de este último y sino ya será tarde para recuperar los archivos con datos correctos. Hacer un backup de datos correctos es factible, por lo cual hay que guardar varios juegos y el costo será menor que la pérdida de todos los datos. A la hora de definir la estrategia, también deberemos tener en cuenta la herramienta a utilizar.

✓ No esperar al desastre

Una vez definida una estrategia de backup, debe probarse para asegurar su confiabilidad y si es necesario replantearla o mejorarla sobre la marcha. No debe esperarse a que ocurra un desastre para recuperar datos, debe realizarse pruebas para asegurar que la recuperación de datos es correcta en el momento previsto. Un backup del cual no se está seguro si se podrá realizar recuperación de datos no sirve para nada.

5.2.5 Scripts para la realización de backups en el servidor Cormorán.

Se realizaron en total 26 scripts para la elaboración de las copias de seguridad de los diferentes sitios alojados en el servidor. Estos scripts tienen la posibilidad de trabajar manualmente (para realizar un backup en el momento en que algún usuario lo solicite) o de forma automática cada fin de semana para posteriormente almacenarlos en CD's. Además de los scripts también fueron creados 5 directorios para almacenar los respectivos backups:

- completo_tomcat
- completo_apache
- cormoran
- especifico_tomcat
- especifico_apache

✓ Script de Inicio:

Para la realización manual de copias de seguridad existe un script de inicio llamado **menu** el cual ofrece las siguientes opciones de SISTEMA DE BACKUPS:

- Sitios Completos de Tomcat

  Realiza copias de seguridad como archivos comprimidos de forma independiente para cada Sitio Web de Tomcat alojado en el servidor: *acreditacion, eisi, conexxion, trionix, posnet,* y *foro.*

- Sitios Completos de Apache

  Realiza copias de seguridad como archivos comprimidos de forma independiente para cada Sitio Web de Apache alojado en el servidor: wpda, ecaes, meiweb, mia, proyectos, maestria, tdi, instaladores, elms, gema y mei .

- Sitios Cormorán

  Realiza la copia de seguridad de todo lo que encuentre en la ruta por defecto de apache /var/www/html (la página principal de Cormorán y los sitios alojados allí directamente).

- Sitios Específicos de Tomcat

  Realiza la copia de seguridad como archivo comprimido del Sitio Web de Tomcat que seleccione y lo almacena en el directorio especifico_tomcat.

- Sitios Específicos de Apache

  Realiza la copia de seguridad como archivo comprimido del Sitio Web de Apache que seleccione y lo almacena en el directorio especifico_apache.

✓ Script para la realización de backups de los Sitios Web Específicos de Tomcat:

Se creó un script llamado **setomcat** para realizar backups de algún Sitio Web Tomcat específico mediante opciones de menú. Los backups se almacenan como archivos comprimidos en el directorio *especifico_tomcat.* Las opciones de menú del script setomcat se listan a continuación:

- Sitio Acreditación
- Sitio EISI
- Sitio Conexxion
- Sitio Trionix
- Sitio Posnet
- Sitio Foro

✓ Script para la realización de backups de los Sitios Web específicos de Apache

Se creó un script llamado **seapache** para realizar backups de algún Sitio Web de Apache específico mediante un menú. Los backups se almacenan como archivos comprimidos en el directorio *especifico_ apache.* Las opciones de menú del script seapache se listan a continuación:

- Sitio webpda
- Sitio ecaes
- Sitio moodle gema
- Sitio meiweb
- Sitio mia
- Sitio mei
- Sitio proyectos
- Sitio maestria
- Sitio tdi
- Sitio instaladores
- Sitio eles
- Sitio completo gema
- Sitio completo mgflorez
- Sitio completo vmartinez

✓ Script para la realización de backups de todos los Sitios Web de Tomcat

Se creó un script llamado **sctomcat** para realizar backups de todos los Sitios Web de Tomcat. Los backups se almacenan como archivos comprimidos en el directorio *completo_tomcat.*

✓ Script para la realización de backups de todos los Sitios Web de Apache

Se creó un script llamado **scapache** para realizar backups de todos los Sitios Web de Apache. Los backups se almacenan como archivos comprimidos en el directorio *completo_apache.*

✓ Script para la realización de backups de todos los Sitios alojados en la ruta por defecto de Apache

Se creó un script llamado **scormoran** para realizar backups de la página principal de Cormorán y los sitios alojados en /var/www/html. El backup se almacena como archivo comprimido en el directorio *cormoran.*

✓ Automatización de los scripts

Los scripts descritos anteriormente se pueden ejecutar de forma manual o automatizarlos mediante el servicio **cron**. Actualmente los scripts **sctomcat, scapache** y **scormoran** se están ejecutando con una periodicidad semanal.

5.3 CREACIÓN DE IMÁGENES DE PARTICIONES DEL DISCO DURO

5.3.1 Introducción.

Tener una copia de un disco duro es ideal para restaurar el sistema después de la aparición de virus, corrupción, errores del disco duro, intervención del usuario. En linux, copiar cualquier dispositivo, ya sea un disco duro, un CD o un disquete se realiza con el programa dd en una sola línea:

```
# dd if=/dev/hda of=nombre_archivo_copia
```

"if" viene de "input file", o sea, la entrada, lo que se desea copiar.
"of" viene de "output file", o sea, la salida, el archivo donde se copiará todo.

El problema de este comando es que el tamaño de la imagen resultante será exactamente el mismo que el dispositivo original, incluso si se entuba con bzip2 para comprimir el archivo, saldrá una imagen bastante grande porque el espacio no utilizado también se guarda. Por ello, lo normal y más práctico es usar **Partimage** el cual se distribuye con licencia GNU GPL.

5.3.2 Características del Partimage.

- ✓ Con la aplicación PartImage incluida en el CD de Knoppix pueden realizarse y restaurarse copias de seguridad de particiones completas, ya sean estas Linux o Windows.

- ✓ Sirve pare crear imágenes de particiones para poder ser restauradas en varios equipos.

- ✓ Las imágenes creadas pueden ser almacenadas en otra partición o, a través de la red, en otro equipo.

- ✓ Knoppix incluye mediante partimaged, un servidor que quedará a la escucha para recibir la imagen generada en el ordenador del que se está realizando la copia de seguridad.

- ✓ Las imágenes de las particiones obtenidas con Partimage se pueden comprimir para que ocupen el mínimo espacio posible.

5.3.3 Sistemas de archivos soportados por Partimage.

Partition Image es muy similar al Ghost, pero más potente, teniendo soporte para los siguientes sistemas de ficheros:

- ✓ ext2fs/ext3fs: El estandard en Linux.
- ✓ ReiserFS: Sistema de journalist muy utilizado en Linux.
- ✓ FAT16/32: Sistema del DOS y Windows.
- ✓ HPFS: Sistema de archivos del OS/2.
- ✓ NTFS: Windows NT/2000/XP (soporte experimental)
- ✓ JFS: Journalised File System de IBM. (soporte Beta)
- ✓ XFS: Sistema Jourmalist de SGI. (soporte Beta)
- ✓ HFS: Hierarchical File System, propio del MacOS. (soporte Beta)

- ✓ UFS: Unix File System (Berkeley Fast File System -FFS y Solaris File System) (soporte Beta)

5.3.4 Requisitos mínimos.

- ✓ Una distribución Live-CD que contenga Partimage.

Partimage se puede descargar de internet (http://www.partimage.org) o se puede usar Live-CDs que tengan instalado Partimage, como por ejemplo: Knoppix, SystemRescueCD, Gentoo-Live... Resulta peligroso hacer una copia de una partición que está en uso, por lo que no se recomienda copiar la partición desde la que se ejecuta Partimage.

- ✓ Conocer perfectamente el disco duro,

Es indispensable saber cuales son las particiones existentes en el disco duro porque por ejemplo, si se hace la copia de hda1 y se restaura en hda5 SE PERDERÁN TODOS LOS DATOS de hda5 DE FORMA IRREVERSIBLE.

Se debe recordar que hda es el primer disco duro (correa primaria y configuración maestro), hdb es el segundo (correa primaria y configuración esclavo), hdc el tercero (correa secundaria y configuración maestro) y hdd (correa secundaria y configuración esclavo). Así mismo hda1, hda2, hda3 y hda4 suelen ser particiones primarias y extendida mientras que desde hda5 en adelante son particiones lógicas. También debe considerarse el tipo de disco duro, si es disco duro IDE Linux reconoce las particiones como hda, hdb, hdc o hdd según la explicación anterior. Pero si el disco duro es SCSI o SATA Linux reconoce las particiones como sda, sdb, sdc o sdd.

5.3.5 Realizar imágenes de particiones guardándolas localmente.

El procedimiento consiste en insertar un Live-CD y reiniciar el computador. Lo primero que hay que hacer una vez terminada la carga de linux es buscar un sitio donde guardar la copia, es decir, buscar una partición donde haya suficiente

espacio para colocar las copias. Esta partición debe estar debidamente montada para que se le pueda pasar la información. Se resalta el hecho que la partición a la cual se le va a realizar la copia NO DEBE ESTAR MONTADA.

Como ejemplo se explicará una copia de la partición del boot (hda3) sobre la partición del home (hda7) en un mismo PC llamado estacion1, utilizando un Live-CD KNOPPIX.

1. Al terminar la carga de Knoppix se debe asignar contraseña al usuario administrativo

2. Abrir una consola e iniciar sesión como root

3. Montar la partición donde desea almacenar la copia. En el ejemplo se refiere a hda7 que es el lugar donde se guardará la imagen del boot hda3.

4. Entrar a la partición recién montada.

5. Ejecutar el Partimage

6. El entorno del programa parece complicado, pero es bastante simple. Sólo se elige la partición a comprimir (hda3 que es la del boot), se escribe un nombre a la imagen, se elige la opción “Guardar partición en un nuevo fichero imagen” y pulsar F5.

7. Posteriormente se elige el nivel de compresión, si se desea verificar la partición destino antes de guardar la imagen (no es necesario normalmente), introducir un comentario y si se desea limitar el tamaño del archivo imagen (para guardarlos posteriormente en CDs).

8. Al finalizar el proceso de grabación mostrará una ventana informando el tiempo transcurrido durante la copia, la velocidad promedio de grabación y la cantidad de datos copiados.

5.3.6 Realizar imágenes de particiones por red.

En ciertas ocasiones es necesario realizar copias de particiones por red debido a que el computador no tiene espacio suficiente para guardar las imágenes o porque no tiene unidad quemadora. El procedimiento consiste en insertar un Live-CD en ambos computadores (el que necesita la copia y el que será utilizado para guardar la copia) y posteriormente reiniciarlos para iniciar la carga del Sistema Operativo del Live-CD. Debe tenerse presente que la partición elegida para guardar las imágenes de las particiones debe tener suficiente espacio y que además debe estar debidamente montada para que se le pueda pasar la información. Se recuerda el hecho que la partición a la cual se le va a realizar la copia NO DEBE ESTAR MONTADA.

Como ejemplo se realizará una copia de la partición del boot (hda3) del PC estacion1 por la red almacenándola sobre la partición del home (hda8) del PC estacion2, utilizando dos Live-CD KNOPPIX.

Para realizar este procedimiento debe aclarar los siguientes conceptos:

✓ Servidor de imágenes (estacion2):

Se refiere al PC que almacena las imágenes y por lo tanto la partición correspondiente debe estar debidamente montada (hda8).

✓ Cliente de imágenes (estacion1):

Se refiere al PC que envía las imágenes y por lo tanto ninguna de sus particiones deben montarse.

1. Insertar Live-CDs de Knoppix en ambos computadores y reiniciarlos.

2. Al terminar la carga de Knoppix se debe realizar dos operaciones:

- ✓ Asignar contraseña al usuario administrativo (root) en ambos equipos (servidor y cliente).
- ✓ Configurar la dirección IP en ambos equipos: 192.168.23.14 para estacion1 y 192.168.23.24 para estacion2.

3. En el PC servidor de imágenes (estacion2) abrir una consola e iniciar sesión como root.

4. Editar el archivo de configuración de usuarios de Partimage **partimagedusers** ubicado en /etc/partimaged para adicionar los usuarios que tienen privilegios de creación de imágenes root y knoppix

5. Montar la partición donde desea almacenar la copia (hda8)

6. Entrar a la partición recién montada

7. Ejecutar el Partimaged (con "d" al final). Partimaged es un programa que actuará de servidor

8. En el PC cliente de imágenes (Cormorán) abrir una consola, iniciar sesión como root y ejecutar el Partimage.

9. En este momento se visualizará una ventana preguntando si desea crear el inodo /dev/cloop0 el cual es necesario para continuar con el procedimiento. Con la tecla TAB se debe ubicar sobre SI y presionar ENTER.

10. Debe elegirse ahora la partición a comprimir, escribir un nombre para la imagen (ejemplo: boot_hda3), seleccionar la opción de “Guardar partición en un nuevo fichero imagen”, seleccionar la opción “Conectar con el servidor” y escribir la IP del PC que actúa como servidor de imágenes (192.168.23.24) y pulsar F5.

11. Se observará que Partimage solicita el nombre de usuario y contraseña del usuario que realizará las copias por red. Debe colocarse un nombre de usuario registrado en el archivo /etc/partimaged/partimagedusers del pc servidor de imágenes. En este caso se digita la información del usuario root y su respectiva contraseña (del pc servidor de imágenes).

12. Posteriormente se elige el nivel de compresión, si se desea verificar la partición destino antes de guardar la imagen (no es necesario normalmente), si se desea limitar el tamaño del archivo imagen (para guardarlos posteriormente en CDs) y presionar F5.

13. Ahora se debe introducir un comentario o una descripción de la partición que está guardando y presionar OK

14. Se observará una ventana con información de la partición que va a guardar. Se debe presionar OK para empezar el proceso de copia por red.

Nota: En el momento que se inicia el envío de la imagen por red se observa en el servidor de imágenes un mensaje indicando que está guardando la imagen desde el PC cliente que tiene dirección IP 192.168.23.14 y con nombre de la imagen boot_hda3.

15. Al terminar el proceso de grabación en el pc que envió la imagen se observará una ventana informando el tiempo transcurrido durante la copia, la velocidad promedio de grabación y la cantidad de datos copiados.

5.3.7 Realizar imágenes de todo el disco duro.

Partimage no tiene la opción de grabar todo el disco duro, así que se realiza el siguiente procedimiento:

1. Realizar las imágenes de todas las particiones del disco duro con el procedimiento explicado anteriormente.

2. Conseguir la tabla de particiones del disco duro.

3. Conseguir el sector de arranque del disco duro (MBR).

5.3.8 Recuperar imágenes de particiones por red.

El proceso de restauración de la imagen es el mismo que se utiliza para la creación de imágenes pero con algunas variantes. Se debe tener presente que tanto para crear la imagen como para restaurar una partición, ésta NO debe estar montada, por lo que si por cualquier motivo se ha montado la partición, debe desmontarse previamente desde la consola como usuario root.

Como ejemplo se realizará la restauración de la partición del boot (hda3) del PC estacion1 la cual se encuentra guardada en la partición del home (hda8) del PC estacion2.

Se inicia el procedimiento de la misma forma que en numeral 5.3.6 (arranque, configuraciones iniciales de asignación de contraseña para el usuario administrativo, asignación de IP's, y asignación de privilegios de usuario para la creación de imágenes), luego se realiza lo siguiente:

1. En el PC servidor de imágenes (estacion2) se debe montar la partición (hda8) donde se encuentra almacenada la copia (boot_hda3.000)

2. Entrar a la partición recién montada.

3. Ejecutar el Partimaged (con "d" al final).

4. En el PC cliente de imágenes (estacion1) abrir una consola, iniciar sesión como root y ejecutar el Partimage.

5. En este momento se visualizará una ventana preguntando si desea crear el inodo /dev/cloop0 el cual es necesario para continuar con el procedimiento. Con la tecla TAB se debe ubicar sobre SI y presionar ENTER.

6. Debe elegirse la partición que desea restaurar, especificar la ruta donde tiene la imagen guardada (/mnt/hda8/boot_hda3.000), seleccionar la opción de “Restaurar partición de un fichero imagen”, seleccionar la opción “Conectar con el servidor”, escribir la IP del PC que servidor de imágenes (192.168.23.24) y pulsar F5.

7. Se observará que Partimage solicita el nombre de usuario y contraseña del usuario que realizará las copias por red. Debe colocarse un nombre de usuario registrado en el archivo **/etc/partimaged/partimagedusers** del pc servidor de imágenes. En este caso se digita la información del usuario **root** y su respectiva contraseña (del pc servidor de imágenes).

8. La opción de "simulación de la restauración" no escribe nada en el disco duro sólo sirve para comprobar que la imagen no está corrupta. Y la de "Borrar bloques libres con cero valores" sirve para asegurarnos de que la partición será sobreescrita completamente.

Nota: En caso de tener la imagen en varios trozos partimage se encargará de ir restaurando las imágenes. Al presionar F5 saldrá una ventana de confirmación de restauración.

9. Se observará una ventana con información de la partición que va a restaurar. Se debe presionar OK para empezar el proceso de copia por red.

5.3.9 Recuperar todo el disco duro por red.

Si se desea recuperar un disco duro completo con varias particiones se tiene que invertir el proceso de copiado un disco duro completo. Para este procedimiento son necesarias las imágenes de todas las particiones del disco duro, así como la tabla de particiones y el Master Boot Record del disco duro que se desea restaurar.

1. Restaurar el sector de arranque o Master Boot Record.

2. Restaurar la tabla de particiones del disco duro mediante el siguiente comando:

3. Ejecutar el procedimiento 5.3.8 para la restauración de las imágenes de las particiones del disco duro por red

6. ANÁLISIS SOBRE LA FACTIBILIDAD DE TRABAJAR CON UN DISCO CRIPTOGRAFIADO A NIVEL DE KERNEL.

6.1 CIFRADO A NIVEL DEL NUCLEO

Cifrar el sistema de archivos en el que se ejecuta Linux significa que incluso si se reinicia la máquina en la modalidad de mantenimiento, no se podrá acceder a los datos contenidos en el sistema de archivos cifrado sin conocer la contraseña. Se podrá borrar archivos o incluso el sistema completo, pero no se sabrá lo que había en él.

Existen tres modos de cifrar un sistema de archivos utilizando los cifrados de núcleo: aplicando los parches de cifrado al núcleo y compilándolo de nuevo, utilizando el módulo cryptoapi o ejecutando Suse 2.7 o posterior, que ya tiene los parches aplicados al núcleo. Este último método ofrece además la ventaja de que las correspondientes utilidades del sistema de archivos (mount, umount y losetup) ya están compiladas.

6.2 MÓDULOS DEL NÚCLEO

Quizá la manera más sencilla desde muchos puntos de vista sea volver a compilar el núcleo, pero el uso del módulo cryptoapi tiene la ventaja de que sólo hay que compilar el módulo y no todo el núcleo y por tanto no es necesario reiniciar el sistema para activar las funciones de cifrado. Sin embargo, ambos métodos requieren compilar de nuevo las herramientas util-linux.

Se puede añadir parches al núcleo para añadir las funciones de cifrado, volver a compilar el núcleo e instalarlo, o bien es posible compilar el módulo de cifrado aparte. La primera opción parece ofrecer menos complicaciones: descargar el parche, configurar el núcleo para los módulos de cifrado deseados y volver a

compilar, pero los propios parches pueden no estar actualizados con el resto del núcleo, lo que ocasiona problemas a veces.

6.2.1 Cifrar el núcleo mediante el módulo cryptoapi.

1. Descargar el módulo cryptoapi de por ejemplo la siguiente dirección: http://kent.dl.sourceforge.net/sourceforge/cryptoapi/cryptoapi-2.4.7.0.tar.gz

2. Descomprimir el archivo descargado

```
# tar xvzf cryptoapi-2.4.7.0.tar.gz
# cd cryptoapi-2.4.7.0
```

3. Configurar el núcleo y compilarlo de la forma habitual:

```
# ./configure
# make
# make install
```

4. Crear las dependencias del módulo:

```
# depmod
```

Nota: Los módulos ya están instalados junto con los demás módulos. Para utilizarlos se debe cargar el módulo cryptoloop:

```
# modprobe cryptoloop
```

Nota: De esta manera los módulos de cifrado se cargaran cuando se necesiten.

6.3 VOLVER A COMPILAR LAS HERRAMIENTAS

Además de instalar y ejecutar los módulos de cifrado es necesario contar con herramientas de usuario para montar y desmontar los sistemas de archivo cifrados. El núcleo proporciona el cifrado, pero las herramientas necesarias para utilizarlo corren de nuestra cuenta, eso significa que será necesario compilar las herramientas util-linux con los parches de cifrado pertinentes. Hay que prestar atención a las siguientes instrucciones, de lo contrario es riesgoso dañar herramientas importantes del sistema.

1. El código más reciente de las herramientas util-linux se encuentra siempre disponible en el directorio Utils de los servidores del código fuente del núcleo y en el sitio principal del mismo. Descargaremos el archivo comprimido ylo descomprimiremos donde convenga (/usr/src por ejemplo).

2. Obtener el parche pero se debe comprobar que la versión coincida con la de las herramientas util-linux que tenemos instaladas. El más reciente se encuentra disponible generalmente en el directorio pub/linux/kernel/people/hvr de los servidores del núcleo.

3. Descomprimir el parche y copiarlo en el directorio creado:

```
# gunzip util-linux-x.xx.patch.gz
# cp util-linux-x.xx.patch /usr/src/util-linux-x.xx
```

4. Entrar en el directorio y aplicarlo con el mandato patch:

```
# cd /usr/src/util-linux-x.xx
# patch -p1 < util-linux-x.xx.patch
```

Nota: El parche debería aplicarse sin errores. Si se produce alguno, se debe comprobar que la versión del parche y de las herramientas coinciden. No queremos compilar todos los módulos ya que eso estropearía algunas cosas, como por ejemplo el mandato password, y no es cosa que convenga. Para evitarlos se puede editar el archivo Makefile, pero es laborioso y resulta fácil olvidarse de algo o cometer errores.

6.4 CREAR UN SISTEMA DE ARCHIVOS

La mejor manera de proceder consiste en compilar las utilidades que se necesiten comenzando por ejecutar y compilar algunas de las bibliotecas de mandatos que se deseen utilizar.

1. Ir al directorio de montaje y ejecutar los mandatos necesarios:

```
# ./configure
# make -C lib setproctitle.o xstrncpy.o.env.o
# cd mount
# make losetup mount umount
```

Nota: Estos mandatos se encuentran normalmente en los directorios bin y sbin. Para mayor seguridad se puede realizar copias de las versiones antiguas. Si no es necesario, se puede copiar mount y umount en bin y losetup en sbin.

2. Revisar que los permisos sean los correctos utilizando el comando install desde este directorio:

```
# install -m 755 losetup /sbin
# install -m 4755 -o root mount umount /bin
```

Nota: Ya está todo listo para crear y montar el sistema de archivos.

3. Crear el archivo que contendrá el sistema de archivos cifrado.

Se debe generar un archivo de pega con datos aleatorios, que podremos montar y formatear. El archivo debe tener un tamaño fijo (no puede ser dinámico), así que se debe decidir con cautela el espacio que se necesitará para los datos cifrados. El archivo se crea mediante:

```
# dd if=/dev/urandom of=/home/owner/crypto bs=1M count=100
```

Nota: Esto originará un archivo llamado “crypto” en el directorio principal de un usuario llamado “owner”. Como es de suponer, el archivo se puede crear en cualquier parte, pero hay que recordar que el usuario que desee montarlo deberá tener los correspondientes derechos de archivo para acceder a él, por eso resulta recomendable colocarlos en el directorio “home” del usuario. Por lo que respecta al nombre, aquellos realmente obsesionados con la seguridad pueden preferir un nombre inocente para ocultar el hecho de que se dispone de un sistema de archivos cifrado, tal como “backup.tgz”

6.5 DISPOSITIVO LOOP-BACK (DE RETORNO)

El siguiente paso consiste en adjuntar este archivo a un dispositivo loop-back. Las distribuciones habituales admiten varios dispositivos con nombre “/dev/loopx”, donde x es un número entre 0 y 9. Si nuestra configuración es diferente a esta, es posible que debamos ajustar los siguientes mandatos de manera acorde.

1. Suponiendo que el módulo descifrado seleccionado ya está cargado, el dispositivo loop-back se configura de la siguiente manera:

```
# losetup -e serpent /dev/loop0 /home/owner/crypto
```

Nota: Solicitará que indiquemos el tamaño de clave (si el cifrado seleccionado lo requiere) y una contraseña que es vital no olvidar. De esta manera se enlaza el

archivo como un dispositivo loop-back, con la capa de cifrado entre los datos del archivo y las peticiones de datos dirigidas desde el dispositivo y hacia el mismo. El cifrado se proporciona mediante la opción –e y también se puede utilizar la opción –a para definir el tamaño de clave.

2. Dar formato al dispositivo como a cualquier sistema de archivos:

```
# make2fs /dev/loop1
```

Nota: Si se presentan problemas a la hora de montar el dispositivo, volveremos a darle formato mediante el mandato anterior. No se sabe porque es necesario hacerlo dos veces, pero el caso es que soluciona los problemas aparecidos en varios sistemas.

3. Montar el sistema de Archivos
Crear un directorio para asignar el dispositivo y montar la unidad:

```
# mkdir -p /home/owner/mnt/crypto
# mount -t ext2 /dev/loop1 /home/owner/mnt/crypto
```

Nota: Habiendo creado el sistema de archivos se puede almacenar en él cualquier cosa que se desee.

6.6 DESMONTAR EL SISTEMA DE ARCHIVOS

El sistema de archivos se desmonta de la manera habitual:

```
# umount /home/owner/mnt/crypto
```

6.7 RETIRAR EL DISPOSITIVO LOOP-BACK

Es importante tener en cuenta que en este punto el sistema de archivos no está protegido. El dispositivo loop-back sigue activado, y cualquiera podría montarlo con facilidad. Para proteger el sistema de archivos es necesario retirar también el dispositivo loop-back:

```
# loop -d /dev/loop1
```

Nota: Esto puede resultar un poco complicado, así que podríamos incluir una referencia al dispositivo loop-back en el archivo fstab. El inconveniente de ello es que alguna persona curiosa podría deducir de esta manera la presencia de un sistema de archivos cifrado, aunque seguiría sin saber la contraseña de acceso.

```
home/owner/crypto
/home/owner/mnt/crypto ext2 user,noauto,loop,encryption=serpent,keybits= 128 0 0
```

Nota: La ventaja de esto es que el dispositivo loop-back se destruye automáticamente cuando se desmonta la partición y no hay que indicar el tamaño de la clave cada vez que se monta. Así mismo, el propio mandato mount sigue el rastro de estos dispositivos, de manera que si hay más de un sistema de archivos mediante dispositivos loop-back, no debe preocuparse de que se mezclen.

7. ESTUDIO DE LA COMPATIBILIDAD DE PHP5 PARA UNA POSIBLE ACTUALIZACIÓN EN EL SERVIDOR

7.1 INTRODUCCIÓN

El servidor cormorán actualmente trabaja con la versión **4.3.2-8** de **php**, la cual viene por defecto con el Sistema Operativo. Todos los Sitios Web alojados están funcionando correctamente con esta versión de php, pero ahora surge la necesidad de trabajar con una versión superior debido a que algunos estudiantes de proyectos de grado están implementando sus Sitios Web con php5 como por ejemplo el sitio **meiweb.** Este sitio fue desarrollado como proyecto de grado utilizando un paquete llamado LAMP el cual incluye instaladores de Apache (httpd-2.0.49.tar), Mysql(mysql-4.1.8.tar) y PHP(php-5.0.5.tar). Para poner el funcionamiento el sitio **meiweb** se utilizó el equipo de respaldo del servidor cormorán para realizar las siguientes pruebas:

7.2 INSTALAR EL PHP-5.0.5 SOBRE LA VERSIÓN EXISTENTE DEL PHP4.3.2-8

Inicialmente junto con el estudiante Oscar Acelas (uno de los desarrolladores del sitio meiweb) se pensó instalar el php-5.0.5 sobre la versión existente del php4.3.2-8 pero hubo conflicto de dependencias.

7.3 DESINSTALAR APACHE, PHP Y MYSQL EN EL SERVIDOR PARA REALIZAR LA INSTALACIÓN DE LOS PAQUETES DEL LAMP

Seguidamente se desinstaló el php (php-4.3.2-8) (el cual funciona actualmente el servidor) para realizar la instalación del paquete PHP (php-5.0.5.tar) que viene con el LAMP. El resultado no fue satisfactorio porque la versión del php5 recién instalado no encontró una librería específica que permite hacer el enlace con el servidor Apache.

7.4 UTILIZAR FUNCIONES DE PHP5 E IMPLEMENTARLAS SOBRE PHP4 PARA QUE LOS SITIOS WEB DESARROLLADOS SOBRE PHP5 SEAN COMPATIBLES CON PHP4

Este trabajo fue realizado por parte del estudiante Oscar Acelas quién utilizó las funciones de transición que vienen con el compilador del php5 para implementarlas en su Sitio Web y ponerlo en funcionamiento sobre el servidor cormorán. Sobre el servidor no se hizo ningún cambio para poder montar el sitio meiweb, los cambios se realizaron directamente en las páginas del Sitio meiweb por parte del estudiante Oscar Acelas. Se recomienda además, no utilizar las funciones sobre php5 que no formen parte del php4, para de esta forma no tener conflicto con las versiones.

7.5 MONTAR EL SISTEMA OPERATIVO SIN EL APACHE, PHP Y MYSQL QUE VIENEN POR DEFECTO

Se realizó en el equipo de respaldo del servidor cormorán, el montaje del Sistema Operativo sin los paquetes Apache, php y Mysql que vienen por defecto. No hubo conflicto durante la instalación y configuración de los paquetes del LAMP. Se procedió a crear un espacio de trabajo para un Sitio Web que utilizara las versiones de apache-2.0.46, php4.3.2-8 y Mysql-4.1.9-0 con el fin de probar la funcionalidad con las versiones instaladas del LAMP.

Se escogió el Sitio Web de Computadores para Educar **wpda** debido a que utiliza Apache, php y Mysql. Se realizó el procedimiento indicado anteriormente en el numeral 32 del manual “paso a paso para la instalación y configuración del servidor Cormorán” donde se describe la creación del usuario, permisos, propietario, creación de Base de Datos, etc.

En este procedimiento se resalta el hecho de que no hay necesidad de convertir el password de la base de datos a formato compatible para la versión de PHP y Mysql.

El resultado obtenido fue la total funcionalidad del Sitio **wpda** con su respectiva conexión a la Base de Datos comprobándose la compatibilidad de la versión 5.0.5 de php con los sitios que funcionaban con la versión 4.3.2-8.

Seguidamente se montó el sitio **meiweb** utilizando el mismo procedimiento, confirmándose también su total funcionalidad.

8. REDISEÑO DEL SITIO DE UTILIDADES Y SOFTWARE LIBRE DE CORMORÁN

8.1 INTRODUCCIÓN

El Sitio Web del listado de software libre fue diseñado por la anterior practicante para brindar a la comunidad EISI de forma rápida algunos instaladores de software para Linux de uso frecuente. Cuando el servidor Cormorán fue víctima del ataque informático, éste contaba con copias de respaldo de todos los Sitios Web que tenía alojados así como de sus bases de datos, pero no contaba con copia de seguridad del software de instalación y su respectivo Sitio Web. Los instaladores fueron rescatados por la red cuando aún estaba inutilizable el servidor Cormorán esperándose que en la misma ubicación se encontrara su Sitio Web. Para volver a poner en funcionamiento el servidor Cormorán fue necesario realizar todo el procedimiento descrito en el manual del servidor el cual incluye la instalación del Sistema Operativo (incluyendo el formateo del equipo) perdiéndose de esta manera toda la información que estuviera allí. Como estrategia de recuperación de la información del Sitio Web de Instaladores, se optó por contactar a la anterior practicante para pedir una copia de respaldo del Sitio de Instaladores a quien en repetidas ocasiones se le solicitó el favor de que enviara la copia del Sitio de Instaladores pero nunca la envió. Esta situación ocasionó que se tuviera que realizar de nuevo el diseño del Sitio Web de los Instaladores para poder ofrecer un ambiente agradable en el proceso de descarga del software ofrecido por el servidor Cormorán, la cual por razones de tiempo no pudo realizarse de forma dinámica.

El sitio web que a continuación se muestra, presenta cuatro páginas las cuales siguieron el diseño de las páginas de las políticas del Servidor Cormorán:

8.2 PÁGINA PRINCIPAL DEL SITIO WEB DE SOFTWARE LIBRE

Esta página se puede acceder mediante la dirección http://cormoran.uis.edu.co/instaladores en la cual se encuentran tres categorías (servidores, bases de datos y utilidades). Cada una de ellas con una descripción de su contenido:

Figura 3. Página principal del sitio de software libre

8.3 PÁGINA DE SOFTWARE PARA SERVIDORES

En esta página se lista el software para instalar y configurar el servidor Apache y el servidor Tomcat, así como los módulos necesarios para su correcto funcionamiento conjunto. Se adiciona también en esta categoría diferentes versiones de Java.

Figura 4. Página software para servidores

8.4 PÁGINA DE SOFTWARE PARA BASES DE DATOS

En esta página se lista el software necesario para instalar y configurar los servidores de bases de datos Mysql y Postgres, además de herramientas gráficas para su administración.

Figura 5. Página software de bases de datos

8.5 PÁGINA DE UTILIDADES

En esta página se lista software de diferentes navegadores, comunicaciones entre equipos Linux - Linux (ssh) comunicaciones entre equipos Windows -Linux (putty, winscp), quemadores (k3b), mensajería instantánea (amsn), reproductores de video y skins, entre otros.

Figura 6. Página software de utilidades

9. ADMINISTRACIÓN DEL SERVIDOR

9.1 CREACION DE USUARIOS

En el transcurso de la práctica fueron creados algunos usuarios y también fueron eliminados otros (como en el caso del usuario gitsi al finalizar su proyecto de grado -portal wap de la UIS). Actualmente existen 11 usuarios Apache y 6 usuarios Tomcat.

9.2 CREACION DE BASES DE DATOS

Muchos de los sitios alojados en el servidor Cormorán requieren una base de datos la cual puede ser creada en PostgreSQL o en MySQL. Actualmente existen 15 bases de datos MySQL y 3 bases de datos PostGreSQL.

9.3 ASIGNACIÓN DE PERMISOS DE LOS DIRECTORIOS DE TRABAJO DE LOS USUARIOS

Algunas veces se presentan inconvenientes para actualizar la información que se ha cargado a las áreas de trabajo de los usuarios desde sus estaciones de trabajo debido a que los permisos de estos archivos no son los adecuados. Para arreglar este inconveniente se hace indispensable reasignar los permisos de usuario a los archivos.

9.4 MODIFICAR Y/O ASIGNAR DIRECCIONES IP A LAS BASES DE DATOS

Frecuentemente se presentan algunos usuarios solicitando la posibilidad de modificar sus bases de datos remotamente desde otro PC diferente al que normalmente usan para esta tarea.

9.5 ELABORACIÒN DE SCRIPTS

El trabajo realizado hasta el momento en el servidor Cormorán incrementando la seguridad y automatizando algunas tareas no es un proceso acabado. Por el contrario día a día surgirán nuevas necesidades que tendrán que ser cubiertas mediante automatización de scripts como los realizados en esta práctica:

9.5.1 Script para borrar los archivos y directorios temporales de la ruta de trabajo de los usuarios de Tomcat.

Existe un directorio de almacenamiento de temporales donde se encuentra un directorio por cada sitio Tomcat alojado en el servidor. Cuando estos directorios se van llenando, los cambios impuestos por sus respectivos usuario no son registrados, produciendo como consecuencia que no funcione de forma conveniente para el usuario de ese sitio. Para evitar borrar los temporales manualmente surgió la idea de crear un script (temporales.sh).

9.5.2 Script para reiniciar los servidores Apache y Tomcat.

Después de borrar temporales es necesario reiniciar los servidores Apache y Tomcat, por lo que también se creó el script (reiniciar.sh).

9.5.3 Script para realizar copias de seguridad comprimidas de los sitios web de los usuarios Apache y Tomcat.

Una política de seguridad en el servidor Cormorán establece la realización de copias de todos los sitios web alojados para una futura recuperación de información. Se realizaron 26 scripts entre los cuales se automatizaron solo los que ofrecen la posibilidad de realizar las copias completas de los sitios de Tomcat (sctomcat), de los sitios de apache (scapache) y de la ruta por defecto del servidor (scormoran.

9.5.4 Automatización de scripts.

Automatizar scripts significa ejecutar procesos de forma automática con cierto intervalo de tiempo. Para ello se usa la utilidad **cron** la cual lanza procesos con una periodicidad determinada, como por ejemplo copias de seguridad u otro tipo de procesos que deben ser lanzados de forma desatendida. El paquete Cron provee dos utilidades, el demonio cron y el editor de tareas crontab.

9.6 REESTRUCTURACIÓN DEL MANUAL DE USUARIO

Cuando surge algún problema que afecte el correcto funcionamiento del servidor o de alguno de sus sitios se debe buscar siempre la mejor forma de solucionarlo. Pero esta solución debe quedar documentada pensando que en el futuro posiblemente sea necesaria esta información; de esta manera se busca mejorar la eficiencia en la administración del servidor. Como una de las labores del administrador del servidor debe establecerse una actualización constante los manuales del sistema.

En el manual se realizó una modificación muy conveniente en el orden de los procedimientos, ya que cuando se hizo la revisión minuciosa del manual se encontró que hacía falta muchos procedimientos y/o aclaraciones. Además se agregó documentación nueva de los temas que se listan a continuación:

Investigación, Instalación, configuración y conclusiones de Linux Terminal Server Project
Investigación acerca de Windows Terminal Services
Investigación acerca de Seguridad Informática
Creación de diferentes scripts (copias de seguridad, borrar temporales de Tomcat y reiniciar servidores Apache y Tomcat).
Creación de imágenes de las particiones del Servidor
Investigación acerca de cifrado del núcleo
Investigación acerca de la compatibilidad de PHP4 con PHP5

10. CONCLUSIONES

Tener configurado el servidor de terminales LTSP ofrece a cualquier equipo de la red local poder cargar Linux y todas sus aplicaciones sin necesidad de tener instalado este sistema operativo ya que éste es tomado directamente del servidor LTSP haciendo uso de un disquette de arranque. De esta forma se está reduciendo el tiempo de instalación, mantenimiento y actualización del sistema operativo y las aplicaciones en cada equipo de la red local que desea trabajar con Linux. Actualmente uno de los campos donde se utiliza bastante LTSP es en la educación, debido al bajo costo de implantación que suele tener. También mediante el sistema LTSP se podría reutilizar equipos de tecnología obsoleta evitando ser dados de baja.

Microsoft Windows Terminal Services facilita las tareas de administración y manutención de la sala de cómputo, disminuyendo considerablemente el tiempo dedicado a estas tareas debido a que la administración se realiza centralizadamente en el servidor y no en cada estación de trabajo, ya sea para actualizar el sistema, respaldar información, o aumentar la capacidad de la red. Implantar este sistema en la UIS presentaría inconvenientes debido a que generaría costos por conceptos de licencias.

Como mecanismo de seguridad para recuperar la información del servidor Cormorán se realizaron scripts de copias de seguridad comprimidas que se ejecutan automáticamente con frecuencia semanal y con la opción de ejecutarse de forma manual para que en cualquier momento si algún usuario lo solicita pueda obtener su copia.

Otro mecanismo de seguridad como labor de recuperación implementada en el servidor Cormorán fue crear imágenes de todas sus particiones y realizar las copias de su sector de arranque y tabla de particiones. Estas copias son realizadas por red con una periodicidad mensual.

El disponer de imágenes y copias de seguridad automáticas hacen que se aumente el nivel de seguridad y robustez del servidor en razón que para la recuperación en casos de eventualidades se dispone de los mecanismos y copias que garantizan en corto tiempo la continuidad y funcionamiento del servidor.

No se implementó la actualización de los paquetes de PHP5 en el servidor Cormorán debido a que su instalación mediante los paquetes respectivos se realiza sobre una instalación del Sistema Operativo en el cual no se haya instalado Apache, php y Mysql que viene por defecto, lo cual implicaría volver a reinstalar totalmente el servidor.

La labor de administración del servidor fue permanente y básicamente consistió en darle solución a los diferentes problemas presentados a los diferentes usuarios del servidor desde el momento en que se les creaba su área de trabajo.

La actualización del manual del servidor Cormorán fue una labor constante durante el periodo que comprendió esta práctica, en la cual no sólo se incluyeron nuevos capítulos sino que se reestructuró la información y el orden de los temas que ya estaban incluidos.

11. RECOMENDACIONES

Ampliar las capacidades físicas del servidor Cormorán específicamente de disco duro debido a que cada día los sitios que están alojados en el servidor crecen constantemente y porque surgen más solicitudes de espacios para nuevos sitios.

Sacar de la partición raíz (donde se encuentra el sistema operativo) el área de almacenamiento de los usuarios normales con el fin de organizar la periodicidad de los backups de imágenes.

Seguir conservando el PC de respaldo del Servidor Cormorán para que además de funcionar como Servidor de Terminales también actúe como servidor de respaldo de Cormorán cuando sea necesario, como en algún momento ya sucedió. Además adquirir un nuevo equipo sobre el cual hacer las pruebas correspondientes a los temas de investigación de los siguientes practicantes.

Impulsar el uso de las Terminales Virtuales y además buscar diferentes imágenes de disco de arranque para las tarjetas de red que trabajan con equipos de cómputo viejos.

Revisar el software de control de las salas de informática para ponerlo en funcionamiento.

Destinar al servidor un área exclusiva para que sólo tengan acceso las personas autorizadas.

BIBLIOGRAFÍA

ROJO, Diana. Manual de instalación, configuración y administración del servidor cormorán, Primera Edición. Segundo periodo académico 2005.
Este libro es el manual de usuario del servidor Cormorán en el cual se muestra el montaje del Sistema Operativo y los servicios precisos para el correcto funcionamiento del servidor.

http://es.wikipedia.org/wiki/Linux_Terminal_Server_Project
Es un sitio donde muestra una descripción de Linux Terminal Server Project o LTSP como un conjunto de aplicaciones para servidores ofreciendo la capacidad de ejecutar Linux en computadores de poca velocidad, permitiendo reutilizar equipos que actualmente resultan obsoletos debido a los altos requerimientos que piden los sistemas operativos.

http://sourceforge.net/project/showfiles.php?group_id=17723
Sitio Web de donde se encuentran disponibles los rpm, tgz o iso del ltsp en diferentes versiones.

http://www.ltsp.org/documentation/ltsp-4.1/ltsp-4.1.3-en.html
Página Web donde muestra el proceso de instalación y configuración del LTSP 4.1 tanto en el servidor como en los clientes.

https://listas.hispalinux.es/mailman/listinfo/ltsp-es
Pagina Web para suscribirse a la lista de distribución de LTSP en español.

www.rom-o-matic.net
Sitio Web para construir el disquette de arranque de LTSP mediante la marca de la NIC y la MAC.

http://sourceforge.net/project/showfiles.php?group_id=80408&release_id=165260
Página para descargar el disquette de arranque universal **BootDisk522b.zip**

http://fferrer.dsic.upv.es/cursos/Windows/Avanzado/ch06.html
Página Web donde muestra conceptos de Windows Terminal Server.

http://support.microsoft.com/default.aspx?scid=kb;es-es;823313
Página Web donde muestra información de las licencias de Windows Terminal Server.

http://www.microsoft.com/spain/download/servidores/windows2000/activar-licencias-de-acceso-de-cliente.doc
Página Web donde muestra cómo activar un servidor de licencias de Servicios de Terminal Server e instalar Licencias de acceso de cliente (CAL) a través de Internet.

http://www.microsoft.com/spain/download/servidores/windows2000/Configuración-de-Terminal-Services.doc#_Toc513131856
Página Web donde muestra el proceso de configuración de Windows Terminal Server.

http://www.microsoft.com/spain/download/servidores/windows2000/Distribuirlos-servicios-de-terminal-server.doc
Página Web donde muestra el plan de distribución de los Servicios de Terminal Server.

http://www.microsoft.com/spain/servidores/windows2000/documentacion/default.aspx
Página Web donde presenta el procedimiento para configurar Terminal Server en Windows 2000 Server.

http://www.microsoft.com/terminalservices
Sitio Web de Microsoft donde se encuentra información acerca los requerimientos, licencias, procedimientos y todo lo relacionado con el Terminal Services.

http://www.champinet.com/download/doc/unixsec-2.0.pdf
pdf acerca de seguridad informatica en sistemas unix.

http://www.nautopia.net/archives/es/varios_backups_y_recuperacion/backups/manual_partimage.php
Pagina Web donde muestra como realizar imágenes de particiones Linux sobre una misma partición del disco duro utilizando knoppix.

http://www.fentlinux.com/web/?q=node/691
Pagina Web donde muestra como realizar imágenes de particiones Linux sobre una misma partición del disco duro.

http://intercentres.cult.gva.es/cefire/12400551/asesorias/informat/manual-knoppix/c1347.html
Pagina Web donde muestra como realizar imágenes de particiones Linux sobre una partición de un PC conectado a la red.

http://www.omerique.net/twiki/bin/view/TIC/PartitionImage
Pagina Web de un tutorial de Partimage.

http://www.citi.umich.edu/projects/nfsv4/feb_2002_rel/rpcsec_patch.html
Página Web que muestra información del cryptoapi.

http://kent.dl.sourceforge.net/sourceforge/cryptoapi/cryptoapi-2.4.7.0.tar.gz
Sitio Web de donde se descargó cryptoapi2.4