Universidad Tecnológica de El Salvador

FACULTAD DE INFORMÁTICA Y CIENCIA APLICADAS
CARRERA DE TÉCNICO EN INGENIERIA DE REDES COMPUTACIONALES

TEMA:

MATERIAL DIDÁCTICO PARA EL SISTEMA DE CUATRO DIPLOMADOS MODULARES EN LINUX A SER IMPARTIDO POR LA ESCUELA INFORMÁTICA DE LA UNIVERSIDAD TECNOLOGICA.

INTEGRANTE:

ANDRÉS ANTONIO HERNÁNDEZ

PARA OPTAR AL GRADO DE:

TECNICO EN INGENIERIA EN REDES COMPUTACIONALES

MARZO DE 2008

SAN SALVADOR, EL SALVADOR, CENTRO AMERICA

Universidad Tecnológica de El Salvador

Autoridades

Lic. José Mauricio Loucel

Rector

Ing. Nelson Zárate Sánchez

Vicerrector Académico

Jurado Examinador

Ing. Sigfredo Portillo

Presidente

Ing. Daniel Ramírez

Primer vocal

Ing. Carlos Perdomo

Segundo vocal

Marzo 2008

San Salvador, El Salvador. Centro América

Índice

Introducción

Mediante los siguientes diplomados modulares que se van impartir en la Universidad por medio de la Facultad de Informática a través de la Escuela de Informática se impartirán una serie de diplomados con el objeto de desarrollar, adquirir, actualizar y perfeccionar competencias en el área de GNU/LINUX que cierta medida no son desarrolladas de forma suficiente en la carrera de tecnología que se ha seleccionado, o en su defecto participa población en general que no son estudiantes activos de la Universidad, pero que visualizan que dichos diplomados se adaptan a las necesidades y exigencias de las empresas tanto públicas como privadas.

Uno de los problemas fundamentales que actualmente enfrentan las casas de educación superior, se deben específicamente a no contar con conocimientos específicos para responder a las diferentes necesidades del mundo laboral, lo que lleva a hacer planteamientos de capacitaciones cortas llamadas Diplomados, para el desarrollo de las competencias que la población estudiantil presenta con una serie de deficiencias en el área de servidores Web como por ejemplo: PHP, MySQL, Seguridad Linux entre otras y que de alguna manera no son impartidas durante el desarrollo de una carrera técnica.

Mediante el conocimientos de estos distintos modulares el alumno inscrito podrá ya finalizado los cursos tener una ventaja muy significativa a comparación a los demás llevándolo de esa forma a competir con personas altamente calificadas para el mejoramiento del país.

CAPITULO I

GENERALIDADES

1.1 Situación problemática

La Facultad de Informática a través de la Escuela de Informática imparte diplomados con el objeto de desarrollar, adquirir, actualizar y perfeccionar competencias en el área de GNU/LINUX que cierta medida no son desarrolladas de forma suficiente en la carrera de tecnología que se ha seleccionado, o en su defecto participa población en general que no son estudiantes activos de la Universidad, pero que visualizan que dichos diplomados se adaptan a las necesidades y exigencias de las empresas tanto públicas como privadas.
Uno de los problemas fundamentales que actualmente enfrentan las casas de educación superior, se deben específicamente a no contar con conocimientos específicos para responder a las diferentes necesidades del mundo laboral, lo que lleva a hacer planteamientos de capacitaciones cortas llamadas Diplomados, para el desarrollo de las competencias que la población estudiantil presenta con una serie de deficiencias en el área de servidores Web como por ejemplo: PHP, MySQL, Seguridad Linux entre otras y que de alguna manera no son impartidas durante el desarrollo de un carrera técnica.

1.2 Enunciado del problema

¿De qué manera se puede desarrollar por medio de la plataforma operativa GNU/LINUX, un sistema de diplomados modulares en la Universidad Tecnológica de El Salvador?

1.3 Justificación

Una de la situaciones que actualmente afecta es la actualización, específicamente en el área de las tecnologías, debido a los cambios acelerados de un momento a otro; esto situación ha hecho que se presente una propuesta de diplomados con una metodología flexible en su desarrollo e implementación, con el objeto de solventar los problemas de actualización, específicamente en el área del software libre.

Esta propuesta está estructurada de tal forma que el estudiante pueda al finalizar el primer diplomado poder continuar con los demás, ya que tiene la modalidad de compartir dos de los módulos en cada uno de ellos, y desarrollar competencias de corto plazo debido a su estructura y metodología de desarrollo.

1.4 Objetivo General.

Elaborar el material didáctico para el sistema de cuatro diplomados modulares en LINUX, a hacer impartidos por la Escuela de Informática de la Universidad Tecnológica de El Salvador

1.4.1 Objetivos Específicos.

- ✓ Desarrollar los Lineamientos para el Sistema de los cuatro diplomados modulares en Linux /GNU, a hacer implementados en la Escuela de Informática de la Universidad Tecnológica de El Salvador.
- ✓ Elaborar los diseños instruccionales de cada uno de los diferentes módulos del sistema de diplomados modulares.

- ✓ Elaborar el material didáctico para el desarrollo de sus respectivos diplomados modulares impartidos por la Universidad Tecnológica de El Salvador.

1.5. Alcances

- ✓ **Lineamientos Para El Sistema de Cuatro Diplomados Modulares:**

  Con los lineamientos del sistema de cuatro diplomados modulares en LINUX/GNU se le permitirá facilitar a la Escuela de Informática la implementación de los diferentes diplomados que se realizaran.

- ✓ **Diseños Instrucciónales para el Sistema de Cuatro Diplomados Modulares**:

  En este punto se dará a conocer a los estudiantes que cursaran los diferentes diplomados los temas que se vera en el ciclo completo de cada uno de los diplomados como por ejemplo nombre del diplomado, nombre de módulo, horas clase, horas practicas, ponderación de evaluaciones, duración del ciclo

- ✓ **Material Didáctico para el Sistema de Cuatro Diplomados Modulares:**

  Por medio de los materiales didácticos se enfocara el uso, la configuración y la instalación adecuada de cada uno de los diplomados modulares que se implementaran en este proyecto, además de teoría general acerca de LINUX/GNU para el conocimiento básico del estudiante

1.6 Delimitaciones

1.6.1 DELIMITACION GEOGRAFICA:

El proyecto se llevara a cabo en la Universidad Tecnológica de El Salvador, Facultad de Informática y Ciencias Aplicadas, Escuela de Informática, ubicada sobre la calle Arce edificio N° 1020, San Salvador

1.6.2 DELIMITACION TEMPORAL:

El Proyecto de graduación comprenderá un tiempo estimado de 6 meses aproximadamente, dicho lapso está contemplado en reuniones cortas con el encargado de dar las instrucciones de cómo se elaborará el proyecto, así mismo con el asesor designado.

1.6.3 DELIMITACION ESPECÍFICAS:

Falta de enseñanza y material de apoyo especifico en las asignaturas impartidas por las diferentes cátedras a lo largo de nuestra carrera, poniendo de manifiesto el déficit de conocimiento de este Sistema Operativo.

1.7 Estudio de Factibilidad

1.7.1 FATIBILIDAD TECNICA:

El proyecto cuenta con la información necesaria para desarrollarse junto con sus recursos a nivel tanto de hardware y software. Sus respectivos requerimientos al software a instalar; puesto que la obtención de este Sistema Operativo (Linux) es gratuito.

1.7.2 FACTIBILIDAD ECONOMICA:

El proyecto es factible económicamente, ya que se cuenta con todos los requerimientos técnicos y humanos necesarios para la elaboración del trabajo. Ya que cuenta con el software, hardware y recurso humano los cuales son proporcionados por la Universidad Tecnológica de El Salvador y el grupo de trabajo.

1.7.3 FACTIBILIDAD OPERATIVA:

Debido a la adecuada estructura del proyecto, el cual incluye los lineamientos de implementación del diplomado los diseños intruccionales para cada modulo y el material didáctico de cada uno de ellos, se considera factible la implementación de dicho proyecto.

CAPITULO II

MARCO TEORICO DE REFERENCIA

2.1 ¿ Qué es Diplomado ?

El Diplomado, forma parte del sistema regular de especialización profesional, dirigido a titulados de carreras de educación superior, a profesionales que se desempeñen en actividades afines y a personas que acrediten debidamente su relación con los objetivos del Diplomado en particular. Tiene un periodo de duración dependiendo de lo que se enseñara en el diplomado por lo que puede llegar a estar distribuidas en a lo menos 2 semestres o 3 trimestres, donde se incluyen, laboratorios, tareas, proyectos u otras actividades.Es un programa que le sirve al estudiante para ejercitar una tarea determinada en su área de interés y en el que una vez concluido recibe certificado de participación. Su metodología parte de modelos temáticos, combinación de aspectos teóricos prácticos, conferencias o charlas de los docentes con la participación activa de los estudiantes y ejercicios prácticos de los mismos. Ahora bien: frente a los demás cursos, los diplomados tienen a su favor la intensidad horaria, la profundización del tema y la calidad de los conferencistas

Son cursos de estudios no conducentes a la obtención de títulos ni de grados académicos, curriculares dinámicos y flexibles, de profundización y actualización del conocimiento en diferentes áreas, que satisface necesidades específicas del contexto social, nacional e internacional. No constituyes estudios de postgrado

2.2 ¿Qué es un Módulo?:

Parte de un paquete didáctico que tiene por objeto cubrir objetivos particulares de

enseñanza.

Metodología de un diplomado

El diplomado se llevará a cabo mediante clases presénciales teórico-prácticas, exponiéndose los contenidos del temario y desarrollo de prácticas en un ambiente agradable lleno de profesionalismo.

El alumno participará activamente en los trabajos programados para la asignatura.

- La metodología a utilizar será activa en actividades de percepción, interpretación y expresión musical y corporal.

- Elaboración y exposición de los trabajos programados.

- Se desarrollarán actividades tanto individual como en grupos.

-Metodología teórico-práctica.

- Parte de los conocimientos teóricos se facilitará por escrito, comentándolo luego para su comprensión.

CARACTERISTICAS DE LOS DIPLOMADOS:

a. Formarán parte de los cursos de educación continua y permanente de las instituciones de Educación Superior.

b. Estarán conformados por un diseño curricular, basado en competencias, a partir de un diagnóstico de necesidades reales.

c. La duración mínima de un Diplomado estará determinada por la naturaleza del conocimiento y las actividades que se deseen desarrollar.

d. Para la aprobación del programa se condicionaran el logro de las competencias establecidas en la modalidad presencial con un 75% de asistencia como mínimo.

La **educación formal**, es el proceso integral correlacionado que abarca desde la educación primaria hasta la educación superior, y conlleva una intención deliberada y sistemática que se concretiza en un currículo oficial y se aplica en calendario y horario definido.

Se trataría de un tipo de educación reglado (por los diferentes reglamentos internos dentro del proyecto educativo de cada colegio), intencional (porque tienen como intención principal la de educar y dar conocimientos a los alumnos) y planificado (porque antes de comenzar cada curso, el colegio regula y planifica toda la acción educativa que va a ser transmitida en el mismo). Como características básicas podríamos señalar que este tipo de educación se produce en espacio y tiempo concretos, y que además con ella se recibe un título. Un ejemplo de este tipo de educación sería la recibida en los colegios.

Es aquel ámbito de la educación que tiene carácter intencional, planificado y regulado. Se trata aquí de toda la oferta educativa conocida como escolarización obligatoria, desde los primeros años de educación infantil hasta el final de la educación secundaria.

Ventajas:

- Se lleva un calendario de estudios.
- Se planifican los temas.
- Se calendarizan las evaluaciones.
- Existe fecha limite de estudios.

Desventajas:

- No hay recuperación de tiempo perdido.
- No existe una retroalimentación de todos los temas que no se pudieron ver con anterioridad.
- No hay prórroga para las evaluaciones.
- Requiere de mucha disciplina para poder llevar a cabo las actividades en las fechas calendarizadas.
- Se requiere de mucho tiempo para elaborar las planificaciones
- Es necesario tener una supervisión de los contenidos que se han impartido.

e. Las instituciones otorgarán un diploma certificado de aprobación a aquellos participantes que hayan cumplido con los requerimientos establecidos en el programa del curso.

f. Cada universidad de acuerdo con su estructura organizativa y políticas, establecerán los criterios de aprobación de la oferta de los diplomados.

2.3 Generalidades Linux:

Es un sistema operativo descendiente de UNIX. Unix es un sistema operativo robusto, estable, multiusuario, multitarea, multiplataforma y con gran capacidad para gestión de redes, Linux fue creado siguiendo estas características. En la década de los ochenta apareció un nuevo sistema, era una versión básica y reducida de Unix llamada Minix, su autor fue Andrew Tanenbaum, el objetivo era crear un acceso a este sistema sin tener que pagar licencias, basados en este sistema el señor Linus B. Torvalds, a mediados de 1991 empezó a trabajar en un proyecto para mejorar las deficiencias de Minix, Torvalds creó la primera versión de Linux (Contracción de Linux y Unix) numerada como versión 0.01. Esta versión solo contenía un Kernel muy rudimentario y para poder realizar cualquier operación se requería que la máquina tuviera instalado Minix. El 5 de Octubre de 1991 fue creada y publicada la versión 0.02 cuando Torvalds logro ejecutar programas como el Bash y el Gcc, después de esta publicación se distribuyo en forma gratuita el código de Linux e invito a todo aquel que pudiera aportar ideas nuevas y mejorar el código vía Internet, gracias a estos aportes Linux evoluciono rápidamente a las versiones 0.03, 0.10, 0.11 y 0.12. En Marzo de 1992 fue creada la versión 0.95

Linux es compatible con Unix. Dos características muy peculiares lo diferencian del resto de los sistemas que podemos encontrar en el mercado, la primera, es que es libre, esto significa que no tenemos que pagar ningún tipo de licencia a ninguna casa desarrolladora de software por el uso del mismo, la segunda, es que el sistema viene acompañado del código fuente. El sistema lo forman el núcleo del sistema (kernel) más un gran número de programas / librerías que hacen posible su utilización.

El sistema ha sido diseñado y programado por multitud de programadores alrededor del mundo. El núcleo del sistema sigue en continuo desarrollo bajo la coordinación de Linus

Torvalds, la persona de la que partió la idea de este proyecto, a principios de la década de los noventa. Día a día, mas y mas programas / aplicaciones están disponibles para este sistema, y la calidad de los mismos aumenta de versión a versión. La gran mayoría de los mismos vienen acompañados del código fuente y se distribuyen gratuitamente bajo los términos de licencia de la GNU Public License. En los últimos tiempos, ciertas casas de software comercial han empezado a distribuir sus productos para Linux y la presencia del mismo en empresas aumenta rápidamente por la excelente relación calidad-precio que se consigue con Linux.

Las plataformas en las que en un principio se puede utilizar Linux son 386-, 486-. Pentium, Pentium Pro, Pentium II/III/IV, Amiga y Atari, tambien existen versiones para su utilizacion en otras plataformas, como Alpha, ARM, MIPS, PowerPC y SPARC.

Características GNU/Linux

Las siguientes características están basadas en GNU/Linux.

En líneas generales podemos decir que se dispone de varios tipos de sistema de archivos para poder acceder a archivos en otras plataformas. Incluye un entorno gráfico X Windows (Interfaz gráfico estandard para máquinas UNIX), que nada tiene que envidiar a los modernos y caros entornos comerciales. Está orientado al trabajo en red, con todo tipo de facilidades como correo electrónico sites de oficina, juegos, trabajo de audio y video, etc... Linux tiene muchas características que lo hacen merecedor de la popularidad y confianza de personas y entidades alrededor del mundo, como por ejemplo la NASA que apostó por Linux en sus servidores, para investigación. Entre sus muchas características podemos mencionar:

Se distribuye su código fuente, lo cual permite a cualquier persona que así lo desee hacer todos los cambios necesarios para resolver problemas que se puedan presentar, así como también agregar funcionalidad. El único requisito que esto conlleva es poner los cambios realizados a disposición del público, esto debido a su licencia. Es desarrollado en forma abierta por cientos de usuarios distribuidos por todo el mundo, los cuales la red Internet como medio de comunicación y colaboración. Esto permite un rápido y eficiente ciclo de desarrollo. Cuenta con un amplio y robusto soporte para comunicaciones y redes, lo cual hace que sea una opción atractiva tanto para empresas como para usuarios individuales.

- **Linux y sus Shells:** Cada usuario de un sistema Linux tiene su propia interfaz de usuario o Shell. Los usuarios pueden personalizar sus shells adecuándolos a sus propias necesidades específicas. En este sentido, el Shell de un usuario funciona más como un entorno operativo que el usuario puede controlar.
- **Linux es Multitarea:** La multitarea no consiste en hacer que el procesador realize más de un trabajo al mismo tiempo (un solo procesador no tiene esa capacidad), lo único que realiza es presentar las tareas de forma intercalada para que se ejecuten varias simultáneamente. Por lo tanto en Linux es posible ejecutar varios programas a la vez sin necesidad de tener que parar la ejecución de cada aplicación.
- **Linux es Multiusuario:** Para que pueda desarrollar esta labor (de compartir los recursos de un ordenador) es necesario un sistema operativo que permita a varios usuarios acceder al mismo tiempo a través de terminales, y que distribuya los recursos disponibles entre todos. Así mismo, el sistema debería proporcionar la posibilidad de que más de un usuario pudiera trabajar con la misma versión de un mismo programa al mismo tiempo, y actualizar inmediatamente cualquier cambio

que se produjese en la base de datos, quedando reflejado para todos. En conclusión, en el sistema multiusuario, varios usuarios pueden acceder a las aplicaciones y recursos del sistema Linux al mismo tiempo. Y, por supuesto, cada uno de ellos puede ejecutar varios programas a la vez (multitarea).

- **Linux es Seguro:** El concepto de seguridad en redes de ordenadores es siempre difícil de abordar. Un sistema puede ser seguro para un determinado tipo de actividades e inseguro para otras. Si se quiere que el sistema sea seguro, se debe administrar de tal forma que se tengan controlados a los usuarios en todo momento. Para la ardua tarea de seguridad surgen nuevas herramientas constantemente, tanto para detectar intrusos como para encontrar fallos en el sistema y evitar así ataques desde el exterior.
- **Linux y las Redes de Ordenadores:** Cuando se trabaja con Linux se está ante un sistema operativo orientado al trabajo de redes de ordenadores.
    - Linux dispone de varios protocolos como PPP, SLIP, TCP/IP, PLIP, etc.., para la transferencia de archivos entre plataforma. Tiene a su disposición multitud de aplicaciones de libre distribución que permiten navegar a través de Internet y enviar y recibir correo electrónico, hacer una video-conferencia, transferir archivos, etc. Posee gran variedad de comandos para comunicación interna entre usuarios que se encuentren ubicados en plataformas distintas (gracias a utilidades como telnet).
    - Independencia de dispositivos Linux admite cualquier tipo de dispositivo (módems, impresoras) gracias a que cada una vez instalado uno nuevo, se añade al Kernel el controlador o driver necesario con el dispositivo, haciendo que el Kernel y el driver se fusionen. Lo importante de esto es que

el controlador funciona como un modulo completamente aislado del núcleo de Linux, dando así una mayor seguridad y estabilidad al sistema.

- **Multiplataforma:** Las plataformas en las que en un principio se puede utilizar Linux son 386-, 486-. Pentium, Pentium Pro, Pentium II,Amiga y Atari, tambien existen versiones para su utilizacion en otras plataformas, como Alpha, ARM, MIPS, PowerPC y SPARC.
- **Multiprocesador:** Soporte para sistemas con más de un procesador está disponible para Intel y SPARC.
- Funciona en modo protegido 386.
- **Protección de la memoria** entre procesos, de manera que uno de ellos no pueda colgar el sistema.
- **Carga de ejecutables por demanda:** Linux sólo lee del disco aquellas partes de un programa que están siendo usadas actualmente.
- **Política de copia en escritura** para la compartición de páginas entre ejecutables: esto significa que varios procesos pueden usar la misma zona de memoria para ejecutarse. Cuando alguno intenta escribir en esa memoria, la página (4Kb de memoria) se copia a otro lugar. Esta política de copia en escritura tiene dos beneficios: aumenta la velocidad y reduce el uso de memoria.
- **Memoria virtual** usando paginación (sin intercambio de procesos completos) a disco: A una partición o un archivo en el sistema de archivos, o ambos, con la posibilidad de añadir más áreas de intercambio sobre la marcha Un total de 16 zonas de intercambio de 128Mb de tamaño máximo pueden ser usadas en un momento dado con un límite teórico de 2Gb para intercambio. Este límite se puede aumentar fácilmente con el cambio de unas cuantas líneas en el código fuente.

- **Consolas virtuales múltiples:** varias sesiones de login a través de la consola entre las que se puede cambiar con las combinaciones adecuadas de teclas (totalmente independiente del hardware de video). Se crean dinámicamente y puedes tener hasta 64.
- **Soporte** para varios sistemas de archivo comunes, incluyendo minix-1, Xenix y todos los sistemas de archivo típicos de System V, y tiene un avanzado sistema de archivos propio con una capacidad de hasta 4 Tb y nombres de archivos de hasta 255 caracteres de longitud.
- **Acceso transparente a particiones MS-DOS** (o a particiones OS/2 FAT) mediante un sistema de archivos especial: no es necesario ningún comando especial para usar la partición MS-DOS, esta parece un sistema de archivos normal de Unix (excepto por algunas restricciones en los nombres de archivo, permisos, y esas cosas). Las particiones comprimidas de MS-DOS 6 no son accesibles en este momento, y no se espera que lo sean en el futuro. El soporte para VFAT, FAT32 (WNT, Windows 95/98) se encuentra soportado desde la versión 2.0 del núcleo y el NTFS de WNT desde la versión 2.2 (Este último solo en modo lectura).

2.4 SUSE LINUX Professional 9.3

características y beneficios

SUSE LINUX Professional ha sido diseñado con el fin de satisfacer las necesidades tanto de los usuarios técnicos con experiencia como de los recién llegados al mundo Linux y contiene las últimas versiones del software de código abierto líder del mercado, incluyendo:

- Un sistema operativo completo Linux: SUSE LINUX basado en el kernel Linux 2.6.11
- Entornos de escritorios intuitivos múltiples: última versión de KDE 3.4 y GNOME* 2.10
- Una completa gama de herramientas Internet: navegador de Internet Firefox* 1.0, correo electrónico y cliente de mensajería instantánea (con soporte para AOL, Yahoo!, MSN, Novell® GroupWise® Instant Messenger, entre otros)
- Suite ofimática: OpenOffice.org 2.0 (ofrece soporte para documentos de Microsoft* Office)
- Aplicaciones multimedia y gráficas líderes del mercado: organizador de fotos F-Spot, programas para gráficos Inkscape y GIMP 2.2, reproductores multimedia, grabadores de CD / DVD…
- Sistema de seguridad totalmente integrado: firewall, bloqueador de spam y antivirus
- Servicios de red avanzados: Apache Web Server, SAMBA, CUPS, DHCP, DNS y las bases de datos de código abierto más conocidas del mercado

- Innovador soporte para dispositivos móviles: conexiones Wi-Fi mejoradas, Bluetooth, PDA y sincronización con el teléfono móvil
- Vitalización robusta, basada en XEN
- Soporte para VoIP
- Múltiples herramientas de desarrollo: Mono® 1.1.4, KDevelop 3.2, Eclipse 3.0.1…

Disponibilidad y precio

SUSE LINUX Professional se ofrece en nuestro país a través del canal retail de Novell y las tiendas online. SUSE LINUX Professional 9.3 estará disponible a mediados del mes de abril a un precio sugerido de 89,90 euros (IVA incluido).

2.5 Red Hat Linux

Es una distribución Linux creada por Red Hat, que fue una de las más populares en los entornos de usuarios domésticos.

Es una de las distribuciones Linux de "mediana edad". La versión 1.0 fue presentada el 3 de noviembre de 1994. No es tan antigua como la distribución Slackware, pero ciertamente es más antigua que muchas otras. Fue la primera distribución que usó RPM como su formato de paquete, y en un cierto plazo ha servido como el punto de partida para varias otras distribuciones, tales como la orientada hacia PCs de escritorio Mandrake Linux (originalmente Red Hat Linux con KDE), Yellow Dog Linux, la cual se inició desde Red Hat Linux con soporte para PowerPC, y ASPLinux (Red Hat Linux con mejor soporte para caracteres no-Latinos).

Características especiales

Red Hat Linux es instalado con un instalador gráfico llamado *Anaconda*, de fácil uso para usuarios novatos. También tiene una herramienta llamada *Lokkit* para configurar un firewall.

A partir de Red Hat Linux 8.0, UTF-8, fue habilitado como la fuente de codificación predeterminada, también fue la primera versión en usar el tema de escritorio Bluecurve.

Red Hat Linux carece de muchas características debido a posibles problemas de derechos de autor y patentes. por ejemplo, el soporte para MP3 es deshabilitado en los reprodcutores Rhythmbox y XMMS; a cambio, Red Hat recomiendo el uso de Ogg Vorbis, que no tiene patentes. El soporte para MP3, de cualquie modo, puede ser instalado posteriormente, aunque se deben pagar regalias en Estados Unidos. El soporte par NTFS es algo olvidado, pero también puede ser instalado

2.6 Ubuntu Linux

Para una administración pública en la actualidad una distribución GNU/Linux no es un fin, sino un medio. Una herramienta que debe cumplir una serie de requisitos, tanto genéricos como específicos del ámbito (geográfico y funcional) al que va dirigida. Los esfuerzos de la

administración deben enfocarse sobre aquellos aspectos en que se detectan mayores carencias, no deben emplearse en reimplementar soluciones existentes y satisfactorias.

Una de las mayores virtudes del software libre reside en la reutilización y, para que se ponga de manifiesto es necesario concentrar una masa considerable de usuarios en torno a una serie de opciones comunes, de modo que cualquier esfuerzo que se haga en favor de ese núcleo común sea beneficioso para un elevado número de personas y que – visto de otra manera – el esfuerzo requerido para garantizar la calidad se reparta entre el mayor número posible de entidades o personas.

En este sentido Ubuntu se presenta como una distribución GNU/Linux a considerar en la evolución de las distribuciones GNU/Linux de las administraciones públicas. Las principales características de Ubuntu son:

Proyecto libre 100%. Pese a estar esencialmente patrocinado por una empresa, la distribución se declara públicamente 100% libre y perteneciente a la comunidad Ubuntu.

Ventajas:

Buena parte del trabajo requerido para estabilizar la distribución vendría dado por Ubuntu.

Compartiríamos un colectivo de usuarios – para la base de nuestra distribución – mucho mayor , con lo que la detección de errores imprescindible para la depuración de la distribución sería más rápida y más profunda. La depuración de errores propia podría integrarse en el "bugtracking" de Ubuntu (Malone). Así mismo, la detección de hardware se beneficiaría de una base de usuarios tan amplia y distribuida geográficamente.

Se trataría de un cambio reversible, ya que Ubuntu deriva de Debian y, en caso necesario, el paso atrás sería esencialmente volver a realizar toda la estabilización por nuestros propios medios. No tendría que suponer una ruptura en la línea de actualizaciones para los usuarios.

Dispondríamos de actualizaciones de seguridad durante un periodo de 18 meses desde la liberación. El uso actual de "congelaciones" de la versión inestable (Sid) o de prueba (Sarge) de Debian significa no disponer de tales actualizaciones, salvo que las elaborásemos nosotros mismos.

Formaríamos parte de un amplio grupo de presión a nivel mundial frente a los fabricantes de hardware para la liberación de drivers o especificaciones. Todo ello con independencia de otras actuaciones que se realicen en materia de reconocimiento o compatibilidad de hardware.

Se podría integrar personal propio o contratado, fondos o proyectos de la administración en la maquinaria de Ubuntu.

Ubuntu decide las líneas a seguir y sus prioridades por una especie de sufragio censatario, por lo que las administraciones, con el peso de sus miles de usuarios tendrían parte en la toma de decisiones de Ubuntu, independientemente de que puedan añadir a la distribución base cuanto estimen necesario.

Canonical está en disposición de firmar un acuerdo de colaboración con las administraciones públicas en el que establecería formalmente y por escrito los compromisos antes citados de carácter libre, periodicidad de versiones y plazo de soporte.

Ubuntu podría servir como núcleo de agregación para iniciativas mucho más amplias y ambiciosas (que la simple derivación de una distribución) en materia de software libre.

Inconvenientes:

Ubuntu no incluye o no soporta todo el software que actualmente incluye nuestra distribución. Sería necesario integrar sobre la base de Ubuntu las aplicaciones adicionales requeridas y soportar su uso de manera separada. De todas maneras significa una reducción de la carga de trabajo respecto a la actualidad.

Componentized Linux no es integrable con Ubuntu si se pretende mantener las ventajas de una u otra alternativa, mucho menos las de ambas. El propósito básico de CL es facilitar el reparto de tareas en la estabilización de la distribución, propósito que perdería su sentido al venir mayoritariamente hechas desde Ubuntu. Otra ventaja de CL es la adhesión al estándar LSB 2.0, cosa que Ubuntu tiene también entre sus propósitos a corto/medio plazo.

2.7 Mandriva Linux 10.1

Es la rama del sistema operativo dirigida a aquellos que quieren un sistema Linux avanzado y estable. 10.1 Official proporciona un soporte de hardware sin parangón junto con una amplia integración con las tecnologías móviles e inalámbricas, tales como Bluetooth y WiFi.

Otras características clave son GNOME 2.6, soporte mejorado de portátiles y nuevos compiladores para un aún mejor rendimiento. Los usuarios entusiastas de todo lo "Avanzado" no necesitan buscar más.

El complemento ideal para cualquier producto Mandriva es el Mandriva Club, que ofrece una amplia gama de beneficios incluyendo acceso a más de 60,000 aplicaciones que corren en Mandriva Linux, además de un amplio surtido de privilegios, incluyendo la descarga de imágenes ISO de comerciales Mandrivalinux para miembros Silver y superiores. Suscribirse al Mandriva Club es la mejor manera de apoyar el desarrollo de Mandriva Linux.

Características

Las principales características de Mandriva Linux son:

- **Internacionalización**

Mandriva Linux está disponible en unos 74 idiomas. Especialmente de calidad son sus traducciones al Español, Catalán y Portugués.

- **Instalación, control y administración**

  El instalador de Mandriva Linux es, probablemente, el más amigable de entre las diferentes distribuciones de Linux, a coste de sus errores, en el cual entre los más destacados es la forma poco amigable de leer las dependencias insatisfechas de una por vez, y la única unidad reconocida es la lectora /hdc. El instalador está traducido a más de 70 idiomas.

  Mandriva Linux emplea Mandrake Control Center para la administración de Linux, en lugar de un editor de texto para cambiar aspectos de la configuración. Tiene muchos programas conocidos como Drakes o Draks, llamados de forma colectiva **drakxtools**, para configurar diferentes ajustes. Los ejemplos incluyen *MouseDrake* para configurar el ratón, *DiskDrake* para configurar las particiones de disco y *drakconnect* (antes conocido como *draknet*, pero forzado a cambiar su nombre después de que una compañía con el mismo nombre se quejara) para configurar una conexión de red. Están escritos usando GTK y Perl, y la mayoría de ellos pueden ser ejecutados tanto en modo gráfico como en modo texto.

- **Software**

  Mandriva Linux, que forma parte del grupo LSB (Linux Standard Base), viene con 12.306 paquetes de software (versión 2006), incluyendo juegos, programas de oficina, servidores y utilidades de Internet.

  Mandriva Linux, a diferencia de otras distribuciones, no se basa en un único entorno de escritorio. Así, Mandriva proporciona apoyo tanto a KDE (QT) como a Gnome (GTK), apoyando tanto el desarrollo de programas QT (Kat, buscador integrado en

KDE) como GTK (las herramientas de administración de Mandriva están escritas en GTK).

Para la administración de programas, Mandriva utiliza Urpmi, una herramienta disponible tanto en formato gráfico y como en formato Texto. Urpmi es una herramienta totalmente comparable a APT. Urpmi se encarga de resolver las dependencias de los paquetes rpm, facilitando enormemente la instalación, desinstalación de programas y la actualización del sistema.

Mandriva Linux tiene una gran comunidad de usuarios, que proporcionan ayuda, soporte y software para el usuario de Mandriva Linux.

¿Quiénes utilizan Mandriva Linux?

Usuarios individuales sin conocimiento específico de TI que necesitan de una distribución que sea sencilla de utilizar.

Usuarios experimentados que prefieren no gastar las horas instalando y configurando su equipo ya que Mandriva Linux no requiere de esfuerzo para instalar y mantener. Contra todo lo que algunos piensan, esta distribución permite su gestión tanto con asistentes, como con editores de texto a la vieja usanza.

Profesionales que necesitan sistemas poderosos, amplios y estables. Mandriva Linux es una de las más completas distribuciones Linux y está volviéndose una de las más favoritas en negocios[1].

2.8 Debian GNU/Linux

Es la principal distribución Linux del proyecto **Debian**, que basa su principio y fin en el software libre.

Creada por el proyecto Debian en el año 1993, la organización responsable de la creación y mantenimiento de la misma distribución, centrado en el kernel Linux y utilidades GNU. Éste también mantiene y desarrolla sistemas GNU basados en otros núcleos (Debian GNU/Hurd, Debian GNU/NetBSD y Debian GNU/kFreeBSD).

Nace como una apuesta por separar en sus versiones el software libre del software no libre. El modelo de desarrollo es independiente a empresas, creado por los propios usuarios, sin depender de ninguna manera de necesidades comerciales. Debian no vende directamente su software, lo pone a disposición de cualquiera en Internet, aunque sí permite a personas o empresas distribuir comercialmente este software mientras se respete su licencia.

Características

- La disponibilidad en varias plataformas hardware. La versión 4.0 incluye soporte para 11 plataformas (alpha, amd64, arm, hppa, i386, ia64, mips, mipsel, powerpc, s390 y sparc).
- Una amplia colección de software disponible. La versión 4.0 viene con 18733 paquetes.
- Un grupo de herramientas para facilitar el proceso de instalación y actualización del software (APT, Aptitude, Dpkg, Synaptic, Dselect , /etc/sources.list, etc).
- Su compromiso con los principios y valores involucrados en el movimiento del Software Libre.
- No tiene marcado ningún entorno gráfico en especial, puediéndose instalar, ya sean: GNOME, KDE, Xfce, Enlightenment u otro.

2.9 WEB SERVERS

2.9.1 Apache

Apache es un servidor web para GNU/Linux, el cual a su vez es confiable, eficiente y muy flexible en cuanto a la configuración.

Fue desarrollado por un conjunto de empresas que necesitaban un servidor Web y se unieron para hacer entre ellas lo que luego se convirtió en el proyecto Apache.

Configuración básica

Una vez que se ha instalado el servidor en un sistema GNU/Linux, según La distribución, el directorio raíz para las páginas web, puede encontrarse En distintos lugares del sistema. En Debian, el directorio que se utiliza es /var/www, en otras distribuciones puede ser /home/httpd, /var/www/html, etc.

El directorio raíz del sitio es el punto de partida para el contenido de http://dominio, donde dominio es el nombre de la máquina que se está configurando como servidor web (puede ser un dominio real, o simplemente el Nombre local de la máquina).

Si se colocan archivos en formato HTML dentro del directorio raíz, el servidor Los proveerá a quien los solicite. Por omisión, el archivo que el servidor Entrega, si no se pide ninguno en particular (es decir, si se accede directamente a http://dominio/, es index.html.

También es posible proveer archivos en otros formatos, como PHP o Perl, si se le agregan a Apache los módulos para que soporte estos lenguajes.

El archivo principal de configuración de Apache es /etc/apache/httpd.conf, en ese mismo directorio (/etc/apache) se encuentran otros archivos adicionales. Según la distribución puede llamarse /etc/httpd en lugar de /etc/apache. Usualmente el archivo de configuración que se instala por omisión contiene Mucha documentación acerca de las opciones posibles, que puede ser ´útil a La hora de configurar el servidor.

Directorios publica HTML

La instalación típica de Apache, le asigna a cada usuario su propio espacio web. Todo lo que se encuentre dentro del directorio public_html dentro del 11 directorio home del usuario, será publicado por el servidor web con el nombre de http://dominio/~usuario/.

En estos directorios se pueden poner archivos HTML, y también PHP o Perl, siempre y cuando el servidor este configurado para entender estos Lenguajes.

Algunas configuraciones generales

En el archivo de configuración, las siguientes líneas pueden ser cambiadas Y tienen los siguientes significados:

ServerAdmin el email del administrador del servidor

DocumentRoot el directorio raíz del servidor (según se explicó anteriormente).

Port el puerto donde el servidor está escuchando. Por omisión es el puerto 80, pero se puede cambiar.

Además de las configuraciones generales, se configuran distintas opciones para los diversos directorios.

<Directory />

Options SymLinksIfOwnerMatch

AllowOverride None

</Directory>

Esta configuración se refiere al acceso a cualquier archivo al disco rígido Es una configuración muy restrictiva. Con configuraciones específicas para determinado directorio podemos elegir opciones menos restrictivas.

<Directory /var/www/>

Options Indexes Includes FollowSymLinks MultiViews

AllowOverride None

Order allow,deny

Allow from all

</Directory>

Esta es la configuración del directorio raíz del sitio. Las opciones indicadas en la línea Options significan:

- Indexes Al acceder a un directorio, si no existe alguno de los archivos que se muestran por omisión (definidos por la directiva DirectoryIndex), se hace un listado de los archivos que hay en el directorio.
- Includes Para el uso de ServerSideIncludes, esto es, una página que incluye a otra utilizando un código especial que el apache interpreta para agregar esa página antes de mostrarla.
- FollowSymLinks Le indica al servidor que siga los symlinks (esto se aplica únicamente dentro del ´árbol del directorio establecido).
- SymLinksIfOwnerMatch Le indica al servidor que solamente siga los symlinks si el dueño del symlink coincide con el dueño del archivo destino (esto se utiliza dentro de la /, para proteger los archivos del sistema).
- MultiViews Permite enviar diferente contenido al cliente según la configuración de su navegador (preferencias de lenguaje, formatos predeterminados, etc).
- Las líneas de Order indican el orden en que se tienen que asignar o no los permisos para acceder a las páginas. En este caso el orden es allow,deny. Y la línea de Allow indica que se le de permisos a todo el mundo para acceder.

<IfModule mod_dir.c>

DirectoryIndex index.html index.htm index.shtml index.cgi index.php

</IfModule>

- Indica cuales son los archivos que el servidor busca para mostrar, cuando no se especifico ningún archivo. Se buscan en el mismo orden en que aparecen.

  <IfModule mod_userdir.c>

  UserDir public_html

  </IfModule>

Restricción de acceso

El servidor web Apache nos permite una restricción muy selectiva del Acceso que se quiere dar al contenido. Por ejemplo, a continuación se reproduce La configuración para los directorios de los usuarios (pública HTML), que Permite que se utilicen los métodos GET y POST para la transmisión de Información, pero deniegan todos los métodos peligrosos.

En este caso, se impide el acceso a cualquier archivo que comience con '.ht', esto es para que no se pueda acceder a los archivos .htaccess, y .htpasswd, que contienen la información de restricción específica dentro de los directorios.

Cambios dentro de los directorios

La directiva AccessFileName .htaccess dentro de la configuración general indica cual es el archivo que se utiliza para la configuración especifica dentro de cada directorio. Se trata de un archivo oculto (ya que comienza con.), que permite cambiar el comportamiento de determinados factores dentro del directorio, desde cual va a ser el archivo a mostrar de

forma predeterminada hasta requerir un usuario y una clave para poder acceder al contenido.

La utilidad principal consiste en que no es necesario modificar la configuración de todo el servidor ni reiniciar el apache si se quieren hacer pequeños cambios personalizados.

Para poder configurar estos valores particulares es necesario que el directorio en el que se quiera colocar el .htaccess tenga la directiva AllowOverride Acompañada de alguno del valor que corresponda al ´área que se quiera reconfigurar.

Por ejemplo, AllowOverride AuthConfig permite cambiar la configuración relacionada con los permisos para acceder al directorio, mientras que AllowOverride FileInfo Indexes permite modificar la información relacionada con el manejo de archivos y la configuración del archivo índice del directorio.

La directiva Requiere indica de qué manera se va a efectuar la validación. Si se utiliza Requiere user usuarios, solamente los usuarios listados pueden acceder al directorio. Por otro lado, si se utiliza Requiere group grupos, solo los usuarios que pertenezcan a los grupos listados pueden acceder al directorio. Finalmente, se utiliza Requiere valid-user, todos los usuarios Válidos pueden acceder.

2.9.2 Configuración de Sendmail

es el agente de transporte de correo (MTA) por defecto de FreeBSD. La responsabilidad de **sendmail** consiste en aceptar correo de agentes de correo de usuario (MUA) y en entregar dichos correos al agente de transporte de correo apropiado, según se especifique en su archivo de configuración. **Sendmail** también acepta conexiones de red provinientes de otros agentes de transporte y puede depositar el correo recibido en carpetas locales o entregarlo a otros programas.

sendmail utiliza los siguientes ficheros de configuración:

Filename	**Function**
/etc/mail/access	Base de datos de accesos de **sendmail**
/etc/mail/aliases	Carpeta de alias
/etc/mail/local-host-names	Listados de máquinas para las que **sendmail**acepta correo
/etc/mail/mailer.conf	Configuración del programa de correo
/etc/mail/mailertable	Tabla de entregas de correo
/etc/mail/sendmail.cf	Archivo de configuración principal de **sendmail**
/etc/mail/virtusertable	Usuarios virtuales y tablas de dominio

2.10 Seguridad y Linux.

En Linux, como en cualquier sistema operativo moderno y más con la introducción masiva de las redes interconectando los sistemas informáticos (y en concreto el auge de Internet), es importante tratar la seguridad y la estabilidad de nuestro sistema de cara a su correcto funcionamiento. Linux es un sistema en constante cambio, desarrollo y mejora y sus cambios no son auditados de manera exhaustiva, sin embargo cualquier problema en cuanto a seguridad, será solucionado por el enorme número de programadores que contribuyen en su desarrollo.

Introducción a la seguridad

Desde siempre ha sido necesario un mínimo de privacidad en la información y algo que nos garantice que nuestros sistemas no van a ser saqueados y vilipendiados por algún desaprensivo que presa del aburrimiento se divierte atentando contra nuestros sistemas informáticos.

Podemos clasificar la seguridad informática en dos ramas:

- *Seguridad Física* : La seguridad física se refiere a todo lo que respecta a problemas o incidentes ocasionados por causas no lógicas. Es decir, si un incendio arrasa la sala donde tenemos nuestro servidor y nosotros no hemos podido reaccionar para evitar este peligro este ha sido un problema de seguridad física.
- *Seguridad Lógica* : La seguridad lógica se referirá a todos aquellos incidentes ocasionados por software directamente y que influyen en el "interior" del ordenador. Un ejemplo de problema de seguridad lógica es por ejemplo un ataque con éxito contra las claves de un servidor.

Aquí trataremos únicamente lo que respecta a la seguridad lógica de nuestro operativo sin despreciar por ello los aspectos de seguridad física sobre los que existen interesantes estudios realizados y elaborados planes de contingencia antes incidentes físicos.

2.10.1 Seguridad Básica

Arranque del ordenador

Si tratamos los aspectos de la seguridad desde la base, hemos de considerar al arranque del ordenador. Es evidente que podemos montar un servidor de manera totalmente segura, pero

que si cualquiera puede acceder a la BIOS de esa máquina, esta se convertirá en un sistema potencialmente inseguro ya que cualquiera podrá modificar los parámetros de la maquina dejándola inutilizable o dejándola en una situación que permita acceder al sistema con total impunidad.

Es un caso clásico de sistema inseguro aquel en el cual la BIOS permite arrancar de disquete, de este modo cualquiera podría arrancar con un disquete del operativo y montando las particiones necesarias, modificar datos como el fichero de passwords, el fichero shadow, etc...

Seguridad y Permisos

El siguiente paso a abordar en un sistema *nix son los permisos. Los permisos nos dan la gran ventaja de poder autorizar o desautorizar a los demas usuarios del sistema a acceder a nuestros datos pudiendo categorizarlos por usuarios del mismo grupo al que pertenece el fichero, propietario del fichero y el resto de los usuarios. Es evidente que la seguridad de un sistema comienza por tener los permisos adecuados en los ficheros, si nosotros tenemos un fichero : /etc/passwd con permisos.

Fallos comunes

A lo largo de la programación en un sistema *nix se repiten una serie de patrones que a pesar de no ser los únicos son fallos que se observan regularmente en los programas para *nix (e incluso para otros operativos), como muestra hablaremos de los desbordamientos de pila (Stack Overflow) y de los "tmpraces" o "races" ya que son dos de los fallos de seguridad más significativos.

Comencemos con los "stacks overflow", estos fallos vienen de la mano de un desbordamiento de pila. El método seguido es el siguiente, se trata por algún método de desbordar la pila de un proceso que corre en estos momentos como otro usuario distinto al nuestro (generalmente el administrador del sistema), lo que conseguiremos al desbordar la pila del proceso es que se ejecute la dirección almacenada en la pila antes de que se haya producido el desbordamiento, de modo que se ejecutará lo que hemos introducido en esa dirección. Cuando estos fallos ocurren corremos el peligro que código arbitrario sea colocado en esa dirección de la pila para ser ejecutado de forma arbitraria

Estos fallos son productos de malos habitos de programación como el no chequear longitudes de parámetros, cadenas que van a ser pasadas a una función, etc...

Otro fallo habitual en programación es el de permitir los llamados "tempraces". Es común que algunos programas creen ficheros temporales para cualquier uso en su ejecución sin embargo también es común que se creen con un nombre fijo y el algunos casos ni tan siquiera se compruebe si existe ya este fichero. Estos malos usos de programación pueden dar lugar a comprometer la estabilidad del sistema. Imaginemos que /tmp que es donde usualmente se crean estos archivos pertenece la partición / , de modo que podremos crear un "hard link" por ejemplo con /etc/passwd. Si no existe comprobación alguna es posible que el programa escriba sobre el fichero de passwords e incluso posteriormente lo borre dejando el sistema en un grave compromiso de seguridad. La solución de estos problemas es usar la función de la librería estándar de C "tmpfile" que nos dará un path de fichero único. Del mismo modo /tmp no debería de estar asociado a la partición raiz si no tener una propia eliminando estos problemas.

Distribuciones y seguridad

Prácticamente todas las distribuciones (por lo menos las más utilizadas) tienen métodos de validar si el software que nosotros pensamos que estamos bajando es realmente el que creemos y que no ha sido modificado de manera maliciosa.

Es importante también asegurarnos de donde estamos obteniendo estos paquetes es decir validar la fuente de donde bajamos los paquetes que van a ser instalados en nuestros sistemas.

En las distribuciones el control de seguridad es incorporado en la estructura de paquetes con la que viene cada distribución. Vamos a analizar qué métodos acompañan a los tipos de paquetes más comúnmente usados para validar su seguridad.

Qué entendemos por *seguridad*?

Hay variadas definiciones de seguridad, que difieren más que nada en el énfasis en lo que se define como aquello que debe protegerse. Acá usaremos la división que puede considerarse clásica:

Confidencialidad: Se refiere a que los recursos del sistema están accesibles sólo a partes autorizadas (se conoce también como *secreto*)

Integridad: Los recursos sólo pueden ser modificados por partes autorizadas de maneras autorizadas

Disponibilidad: Los recursos están disponibles para las partes autorizadas en forma expedita (como definido por los requerimientos del sistema). El no cumplir con esta característica se denomina *negación de servicio* ("denial of service", DoS)

Como se indicó, hay diversas definiciones de seguridad. Son básicamente divisiones y particularizaciones de los anteriores, bastante generales y abstractos. Por ejemplo, se habla de *no repudiación*, significando que quien envió o recibió un mensaje no pueda negar eso a futuro. Igualmente, se habla de *privacidad* como distinto de *confidencialidad*, con significado de proteger la confidencialidad de un usuario (vale decir, su identidad) y no la de los datos.

Los anteriores implican alguna forma de *identificación* (indicar la identidad de las partes) y *autentificación* (verificar que las partes realmente son quienes dicen ser). Nótese que esto va en ambas direcciones, si requiero un servicio (por ejemplo, acceder a una máquina remota) interesa al servicio identificarme y verificar que soy quien digo ser. Al revés, me interesa identificar el servicio al que me conecto (por el nombre o dirección IP de la máquina que quiero usar, e indicando el port del servicio que me interesa), y verificar que es realmente el servicio solicitado (en este caso, que no sea suplantado ni el servicio que requiero ni la máquina en la que corre). Frecuentemente se lista *auditabilidad*, y a veces también *control de acceso* y *autenticidad*

Algunas máximas

Antes de entrar en el detalle de lo que se desea, deben tenerse en cuenta un par de puntos importantes:

- Cuando se habla de seguridad, normalmente se considera sólo el caso de un atacante que accede al sistema sin autorización. Siendo éste un caso importante, no debe olvidarse el efecto que pueden tener equipos que fallan, cortes de energía, fenómenos naturales, error humano, ...
- La seguridad absoluta no existe. Lo más que se puede hacer es disminuir la probabilidad o el impacto de situaciones no deseadas.
- Toda seguridad tiene un costo. Este costo no es sólo en términos de equipamiento (máquinas replicadas, alarmas contra intrusos, o sistemas de respaldo), el costo más importante (que suele olvidarse) es en términos de comodidad de uso (mantener sincronizadas las réplicas, tener a alguien que deba presentarse en corto plazo si suena la alarma, o el no poder usar el sistema mientras se hacen los respaldos mensuales).
- La cadena es tan fuerte como su eslabón más débil. Es inútil asegurar exhaustivamente el acceso al sistema donde están los datos a proteger contra acceso no autorizado si éstos aparecen en forma de listados en la basura.

En lo que sigue se discute más que nada el caso en que se pierdan datos. El mismo tipo de análisis puede (y debe) aplicarse a las demás dimensiones de la seguridad que interesen para una situación dada. Por ejemplo, es perfectamente factible que ciertos datos tengan poco valor en sí, pero que deban ser protegidos cuidadosamente contra divulgación o modificación no autorizadas.

El análisis que se haga deberá considerar como parte del "valor" de los recursos en cada una de las dimensiones condiciones adicionales, como pueden ser obligaciones legales (hay leyes que regulan el uso que pueden hacer las instituciones financieras con los datos de los

clientes), contractuales (una empresa de ingeniería estará obligada a guardar reserva de los proyectos de sus clientes), e incluso éticas (los datos de los pacientes de un médico son confidenciales). Un punto de importancia es el problema de imagen pública: En Internet, la imagen que tiene una empresa está dada por su reputación casi exclusivamente. Como el grueso público conoce aún menos de seguridad que los especialistas, incidentes como el reciente cracking de Microsoft, donde el (o los) atacantes habrían tenido acceso al repositorio de código fuente resultan alarmantes para los potenciales clientes, que de muchas empresas sólo conocen su página web. Además, de ser usada una máquina como herramienta para atacar a otras, en algunas legislaciones el responsable de la máquina usada para perpetrar un ataque puede ser legalmente responsable de éste, al menos en parte.

Recursos a proteger

Es importante tener claro cuáles son los recursos que deben protegerse. Igualmente, es importante determinar los riesgos a que están sujetos, y el impacto que tales riesgos puedan tener.

Valor de los recursos para nosotros

Típicamente los datos almacenados en un sistema son mucho más valiosos que el sistema mismo. Debe determinarse el costo de reponer los recursos bajo estudio (suponiendo que se pierden totalmente), y alguna idea de la probabilidad de tales desgracias. Esto determinará el costo que estaremos dispuestos a incurrir para protegerlos de posible pérdida.

Valor de los recursos para atacantes

Asimismo, debe considerarse el valor que estos recursos puedan tener para un posible atacante. Esto determinará en buena parte el costo en que éste estará dispuesto a incurrir para acceder a ellos. Esto, a su vez, da una pauta complementaria para determinar cuánto esfuerzo invertir en su protección.

Clasificación de riesgos

Hay varios criterios posibles para clasificar riesgos. Una clasificación simple es según él la fuente del problema:

- Hechos fortuitos
- Ataques externos (a través de la red)
- Ataques internos (usando acceso directo a los sistemas, o privilegios de usuario normal)

Para nuestros efectos, los hechos fortuitos son los menos interesantes (Tal vez por ser menos "computacionales", pero no por eso menos destructivos , los ataques externos son los más temidos (el cine ha glorificado la figura del adolescente con un PC, un modem, y demasiado tiempo libre). Sin embargo, no son éstos los más frecuentes, ni lejos los más dañinos.

Los ataques internos son lejos los más frecuentes (las estadísticas indican que son cerca de un 85% de los casos de ataques que se registran).

Una clasificación adicional se puede hacer por los objetivos de los atacantes:

- Ataques dirigidos a un blanco específico. Esto incluye desde espionaje industrial hasta el simple desafío por ingresar a sitios protegidos, pasando por vandalismo puro (destruir páginas web, borrar o destruir datos, etc).
- Ataques al azar. En esta clasificación cae la creación de virus y gusanos.
- Reclutamiento para ataques dirigidos. Una de las técnicas nuevas (se estrenó a principios del 2000) es penetrar un gran número de máquinas

  independientes, con la intención de usarlas para lanzar ataques de saturación coordinados ("Distributed Denial of Service", DDoS) contra blancos escogidos. De esto fueron víctimas entre otros Amazon y eBay.

Otra clasificación útil considera las técnicas usadas. Se puede distinguir entre:

- Verdaderos *crackers*, con algún conocimiento de los sistemas atacados. Son los más peligrosos, pero afortunadamente los menos. Sin embargo, las vulnerabilidades que éstos descubren, y las herramientas que desarrollan para aprovecharlas, normalmente se difunden rápidamente entre la segunda categoría.
- Los llamados *script kiddies* son típicamente adolescentes cuya entretención consiste en coleccionar y usar herramientas que detectan vulnerabilidades y las explotan. La técnica básica es revisar y clasificar grandes números de sistemas (generalmente al azar), con la intención de crear bases de datos de máquinas potencialmente vulnerables. Al descubrirse alguna nueva vulnerabilidad, usan la base de datos para identificar blancos prometedores. Normalmente nada saben de los sistemas atacados (clásico fue el caso en que uno de éstos se hizo **root** en una máquina Sun (corriendo Unix), para dar el comando **format c:**). Se caracterizan por el uso de herramientas

automatizadas para identificar víctimas potenciales, e incluso para penetrarlas (de allí el apelativo).

Los ataques externos son los más temidos Sin embargo, no son éstos los más frecuentes, ni lejos los más dañinos.

Los ataques internos son lejos los más frecuentes (las estadísticas indican que son cerca de un 85% de los casos de ataques que se registran).

Un tipo de ataque particularmente insidioso es lo que se llama *ingeniería social*. Se refiere a engañar a una persona para que entregué información (por ejemplo, llamando por teléfono e indicando que es el supervisor, solicitando alguna clave "olvidada" con voz autoritaria) o inicie la acción destructiva (como en el caso del infame **I LOVE YOU**, ¿Quién es capaz de resistir leer una supuesta declaración de amor de parte de algún miembro del sexo opuesto al que conoce en la oficina?).

Calidad de software y seguridad

Para que se vea comprometida la seguridad de un sistema algún agente debe usar sus privilegios en forma no autorizada. El caso más frecuente es él en el que algún programa es engañado para que efectúe acciones no autorizadas.

Ejemplos típicos han sido los virus que se han distribuido por correo, aprovechando las facilidades de ciertos sistemas de correo para ejecutar automáticamente código que viene en mensajes, y los similares con aplicaciones de oficina. Éstos caen más

bien en el ámbito de diseño básicamente mal hecho, que debiera rehacerse. Claro que el costo de tal cambio es inmenso.

La otra gran fuente de problemas han sido errores de programación (un buen resumen es Secure Programs (HOWTO),que incluye discusión de las últimas clases de vulnerabilidades descubiertas, y Secure UNIX Programming FAQ , que incluye referencias a una gran cantidad de FAQs adicionales). La pregunta clara entonces es la relación entre calidad de software (ausencia de fallas) con su vulnerabilidad frente a ataques externos.

Un punto de interés es que el tipo de errores de programación que se reflejan en problemas de seguridad más comunes suelen dan lugar a caídas de los programas ante pruebas con datos al azar, como en Faz (hay una versión actualizada de la herramienta del caso en So urce Forje). En el año 1990, se probaron entre 49 y 85 utilitarios de cada uno de 5 sistemas Unix comerciales, con el resultado de 25 a 33% de fallas. Las pruebas se repitieron en 1995 en 9 sistemas, incluyendo una distribución de Linux y los utilitarios de GNU. Se probaron entre 47 y 80 programas en cada ambiente, con tasas de fallas entre 15 y 43% en los Unix comerciales. Esto se compara con un 9% para Linux y un 6% para GNU. Lo preocupante es que en los casos donde se pudieron determinar los errores en versiones del mismo sistema en 1990 y 1995, muchos de los errores originales seguían en el código, a pesar de estar ampliamente disponibles los resultados y las herramientas usadas. Eso sí, estos resultados son a lo más indicativos de la calidad general del software de cada sistema,

no indica necesariamente el nivel de seguridad de otro software que se distribuye con él. Las pruebas de 1995 no hicieron mella en los programas servidores probados. Para completar el cuadro, a principios del 2000 se repitió este tipo de pruebas sobre Windows NT. La tasa de fallas fue de 100%.

2.11 Administración Remota

2.11.1 Configurar VNC en Linux

El servidor VNC

Hay muchos servidores VNC, pero explicaremos el uso de **x11vnc** porque es el más sencillo de utilizar. La mayoría de servidores VNC requieren un desplaye de las X particular y, aunque ofrecen un escritorio remoto, lo que hacen es iniciar una nueva sesión gráfica en vez de ofrecer acceso a una sesión ya existente. Con **x11vnc** podremos permitir el acceso a una sesión X ya existente de una forma sencilla.

Instalando x11vnc

El programa seguramente estará disponible como paquete para poder ser instalado de forma sencilla por el sistema de paquetes de la distribución; pero si no lo estuviera, podemos bajar el código fuente de aquí y descomprimirlo, compilarlo e instalarlo de la siguiente forma:

tar -xvzf x11vnc-0.7.3.tar.gz

cd cd x11vnc-0.7.3

./configure

make

make install (este como root)

Con esto ya tendremos el servidor de VNC instalado y a listo para ser utilizado.

Arrancando el servidor

Para arrancar el servidor, abriremos una consola y escribiremos el comando **x11vnc**. Esto nos iniciará un servidor básico, sin contraseña, que permite el acceso a todo el mundo y que una vez ha desconectado el cliente, se cierra.

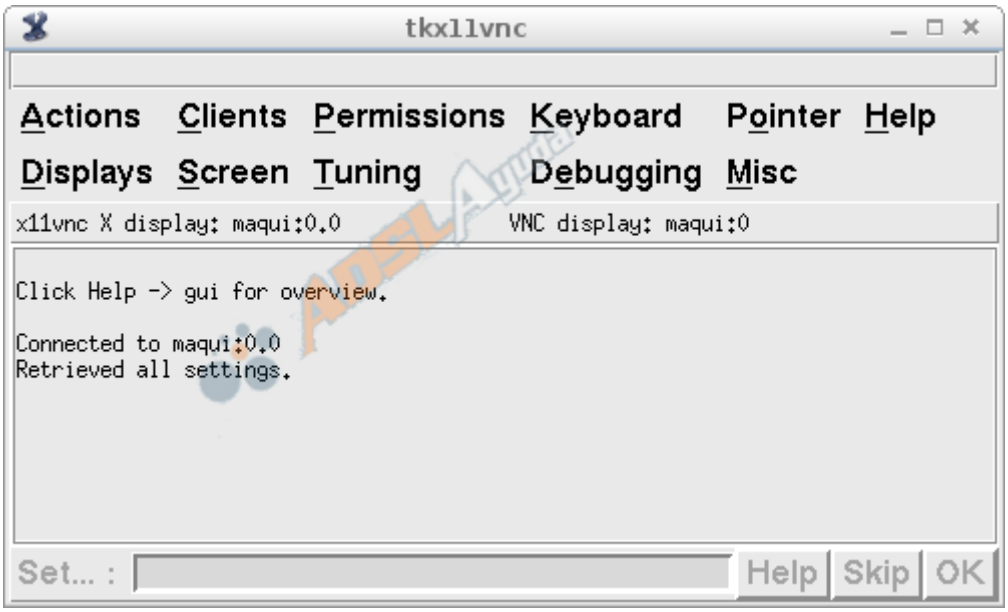
Veremos ahora qué parámetros podemos pasarle al inicio, para configurar el servidor de una forma más razonable:

- **-bg**: Nos inicia el servidor en segundo plano. Para poder cerrar la consola y que siga en marcha.
- **-passwd**: Establece la contraseña que se pedirá a los clientes al conectar.
- **-gui**: Inicia el interfaz gráfico (un poco precario) del servidor.

Sabiendo estos parámetros, podríamos iniciar el servidor de VNC de esta manera, para que nos aparezca su ventana de configuración:

x11vnc -bg -gui -passwd *mi_contraseña*

Se nos abrirá la pantalla de configuración, en la que podremos configurar las opciones del servidor:



Algunos de los parámetros no pueden ser configurados desde el interfaz y deben especificarse en el arranque (como es el caso de la contraseña), pero los parámetros básicos para controlar el acceso podremos configurarlos en el menú **Permissions**:

- **allow**: Lista de IPs (separadas por comas) a las que se permite acceso.
- **forever**: Hace que el servidor no termine al desconectar el cliente; que siga escuchando peticiones.
- **viewonly**: El cliente sólo podrá ver el servidor, pero no realizar acciones sobre él.

El interfaz del servidor podemos dejarlo abierto sin problemas; el servidor ya está funcionando y escuchando peticiones, o bien podemos cerrarlo y dejar corriendo el servidor en segundo plano. Si no lo cerramos, podremos administrar las conexiones, y cambiar la configuración *al vuelo* siempre que nos sea necesario.

También es posible pasarle como parámetro al comando cualquier cosa configurable desde el interfaz. Para obtener una lista detallada podéis consultar el ***man x11vnc***.

Por defecto el servidor escucha en el puerto **5900** por lo que tendremos que asegurarnos de que ningún cortafuegos esté bloqueando el tráfico a través de él, y si queremos permitir accesos desde el exterior, deberemos abrir el puerto en el router.

Terminando el servidor

Si hemos ejecutado el servidor en segundo plano, podremos finalizarlo con el comando:

killall x11vnc

Con estos sencillos pasos, ya tendremos el servidor VNC listo para recibir peticiones y mostrar de forma remota la sesión gráfica que estemos ejecutando.

El cliente VNC

Hay muchos clientes VNC que nos sirven y son sencillísimos de utilizar. Podemos aprovechar el sistema de paquetes de nuestra distribución para instalar el paquete **vncviewer** (o *xvncviewer*) que segurísimo que estará disponible, o bien descargar los clientes de las páginas oficiales:

- TightVNC Client
- RealVNC Client

Ambos vienen ya compilados y listos para ser utilizados. En el caso de *TightVNC* nos viene en formato *rpm* y en el caso de *RealVNC* nos viene comprimido, pero ya compilado y listo para ejecutarse.

Arrancaremos el cliente ejecutando: **vncviewer**

Se nos abrirá una ventana pidiéndonos el nombre del host (o dirección IP) del servidor VNC al que queremos conectar:

Simplemente introduciremos la dirección IP. Por ejemplo: **192.168.0.2**

Si el servidor VNC estuviera escuchando en un puerto diferente al 5900, introduciríamos la IP y el puerto de la forma: **ip:puerto** (por ejemplo: *192.168.0.2:6000*).

Con esto habremos configurado un servidor VNC para recibir peticiones de diferentes clientes y ofrecer un escritorio remoto, y un cliente para hacer conexiones desde nuestro Linux.

Tener acceso remoto a nuestro equipo puede ser muy útil. Con un servidor VNC podemos administrar remotamente servidores web o FTP, controlar el estado de descargas o tareas que requieren mucho tiempo como compilaciones o simplemente acceder desde cualquier lugar a toda la información que tenemos en el disco duro.

Antes de nada, habrá que tener claros unos conceptos:

1. VNC funciona creando *invitaciones*, es dicir, permite a un usuario remoto iniciar sesión en el servidor. Bajo Linux se inicia una sesión en el equipo en vez de ver directamente lo que en ese momento hay en la pantalla. Esto sólo ocurrirá cuando un segundo usuario se conecte usando la misma sesión que otro usuario activo.
2. La sesión se inicia con el usuario que crea la invitación, de modo que si creamos una invitación como **root** quien se conecte al servidor iniciará una sesión con

control absoluto sobre el sistema. Se puede crear más de una invitación, incluso de varios usuarios.

3. Cada invitación tiene un *identificador* del tipo **:1**, **:2** o **:5**. Para hacer la conexión habrá especificar este identificador de este modo: **192.168.0.10:2**. Cada una de estas invitaciones usa un puerto diferente. La primera invitación utiliza el puerto 5901, la segunda el 5902 y así sucesivamente. Se permiten varios usuarios simultáneos por invitación.

Una vez vistos los conceptos básicos, toca instalar el programa. Los paquetes RPM se pueden bajar **desde la sección de descargas**∞ de la página del proyecto o si preferís un paquete para una distribución en concreto lo podéis localizar en el buscador **RPM Pone**∞.

Antes de poner a funcionar el servidor VNC tendremos que configurar algún detalle. Si tenemos activo un firewall deberemos configurarlo de modo que permita el tráfico de paquetes por los puertos que vayamos a usar.

Para eso bastará con editar el archivo **/etc/sysconfig/iptables** y dejarlo más o menos así:

```
# Firewall configuration written by redhat-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
```

A INPUT -j RH-Firewall-1-INPUT

A FORWARD -j RH-Firewall-1-INPUT

A RH-Firewall-1-INPUT -i lo -j ACCEPT

A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT

A RH-Firewall-1-INPUT -p 50 -j ACCEPT

A RH-Firewall-1-INPUT -p 51 -j ACCEPT

A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 5901 -j ACCEPT

A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 5902 -j ACCEPT

A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited

COMMIT

Las líneas en negrita son las que abren los puertos. De haber ya alguno abierto bastaría con añadir las líneas con los puertos que nos interesen. Además, si usamos *router* deberemos redirijir los puertos a la IP del equipo servidor.

Ahora ya está todo preparado para iniciar el servidor. Para eso bastará teclear en una consola:

vncserver :1 -name david -depth 16 -geometry 800x600

Como se ve, el primero parámetro especifica el identificador, el segundo indica el nombre de invitación (non tiene que ver con el usuario que la crea) y los dos últimos indican la profundidad de color y la resolución con la que se verá.

El siguiente paso es asociarle una contraseña a la invitación Para eso hay que teclear en la consola: **vncpasswd**

Pedirá primero una contraseña que dará control completo sobre la sesión. A continuación

pregunta si se quiere crear una contraseña para una conexión de observador. Esto permite que un usuario remoto controle el ratón y el teclado y otro sólo observe.

Sólo resta editar el archivo **/home/usuario/.vnc/xstartup** que especifica qué se va a ejecutar al iniciar la sesión. Por defecto se ejecuta **/etc/X11/xinit/xinitrc** que inicia el entorno gráfico X11 tal y como se usó por última vez. Yo recomiendo usar un gestor de ventanas más ligero como **FluxBox**∞. Para eso deberemos sustituir la línea **exec /etc/X11/xinit/xinitrc** por **exec fluxbox**.

Con esto ya estará el servidor funcionando. Para conectarnos a él deberemos usar un visor como cualquiera de los que se pueden descargar de las webs de los proyectos de **TightVNC**∞ o **VNC**∞.

Finalmente, para parar el servidor deberemos ejecutar esto especificando el identificador:

vncserver -kill :1

2.11.2 ¿Qué es Webmin?

Webmin es una interfase basada en Web que permite la Administración de Sistemas Unix. La idea general de Webmin es poner de forma accesible la configuración de la mayoría de programas/servicios que se usan normalmente en Unix (Linux, etc), de modo que con todo se logra mediante formularios Webs, pero a su vez, podemos editar los archivos de configuración en modo editor de texto (para aquellos *Pro's*).

¿Qué se puede hacer?

Lo bueno de Webmin es que el programa no está limitado a lo que los desarrolladores del mismo quieran, sino que es modular. Esto quiere decir que podemos instalar nuevos módulos, los cuales pueden ser descargados del mismo sitio, en la sección **Third-Party**

Modules.Aún así, para no complicarla, por defecto viene una extensa cantidad de módulos que normalmente suelen venir cargados en casi cualquier distribución Linux.
Entre los módulos destacados (mencionaré solo algunos, más una breve reseña):

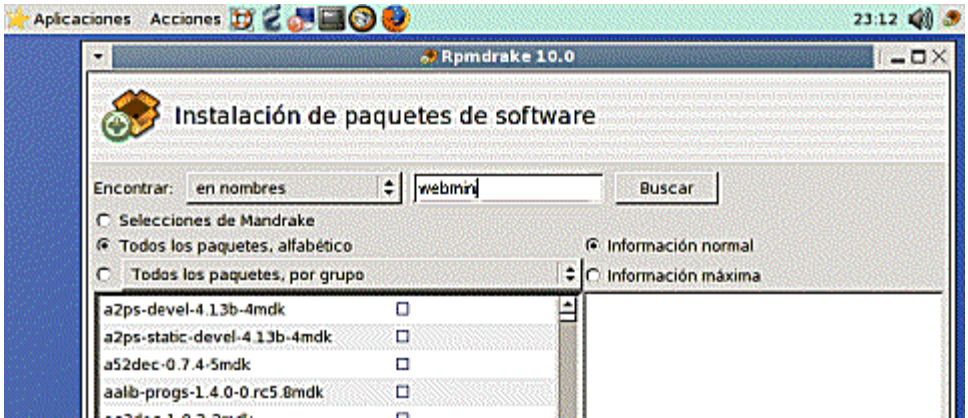
- **Apache WebServer:** Administrar las directivas y características del Servidor Web Apache.
- **Bandwidth Monitoring:** Podemos generar reportes del tráfico que provocamos en una conexión (Internet, Red, etc) de modo que si tenemos un ISP que nos cobra por tráfico, con esto tenemos un reporte real de nuestro consumo.
- **Bootup and Shutdown:** En Ubuntu tengo el BUM (Boot Up Manager) pero la verdad es que en muchos casos, los servicios que aparecen los desconozco y no me lista todos. Con esto, uno logra sacar todos los servicios que no se usan, y encima puede acceder al código que ejecutan.
- **Change Password:** Si bien es relativamente sencillo cambiar los passwords de los usuarios, ¿qué mejor que tenerlo todo accesible en una interfaz bonita?
- **DHCP Server:** Para todos aquellos que tengan una red, y necesiten tener un servidor DHCP (para que cada PC que se conecte a la red, tenga una IP asignada automáticamente), aquí tienen un administrador muy sencillo.
- **Disk Quota:** Si están en una red en donde hay muchos usuarios y estos requieren de tener una cuota asignada en disco (o quizás, para un servidor web/de archivos), este es el complemento ideal. Primero le creamos un usuario, y luego le asignamos la cuota desde aquí.

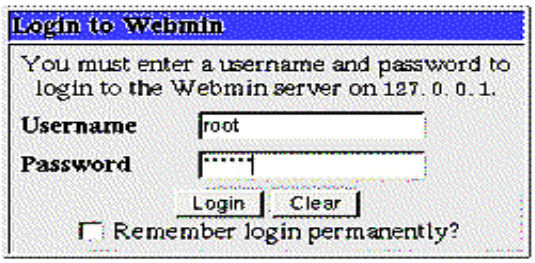
- **Disk and Network FS:** Aquí tenemos acceso a toda la información del disco (similar al comando *df*), representado gráficamente y con información extendida.
- **File Manager:** Para todo aquel acostumbrado a usar un cliente FTP, este módulo les será muy familiar, ya que permite asignar permisos de las carpetas con una interfase gráfica muy sencilla pero útil.

INSTALACIÓN

Para poder instalar Webmin, debemos ir a configuración desde el botón que se encuentra en el borde inferior izquierdo de nuestra pantalla y que normalmente dice "Inicio" o "Aplicaciones" (depende de la versión y del entorno gráfico usado). Una vez encontrado "Configuración" vamos a "Empaquetado" y desde allí a "Interfaz gráfica para instalar paquetes".

En el caso de la figura no aparece Webmin, y esto es así porque la aplicación ya está instalada. Normalmente colocando la palabra "webmin" en el buscador, será suficiente para que lo encuentre. No aparece solo la aplicación sino algunas otras relacionadas. Es conveniente instalar todo lo que tiene relación con Webmin. Para instalar solo habrá que hacer clic sobre el botón que aparece abajo y que dice ....instalar.Luego de un momento el programa estará instalado. Para saber si está bien instalado habrá que colocar sobre el navegador https://127.0.0.1:10000 y deberá aparecer la página que vimos al comienzo. Pero nos encontraremos con dos cosas:





2.13 PHP

Es un lenguaje de programación usado frecuentemente para la creación de contenido para sitios web con los cuales se puede programar las páginas html y los codigos de fuente. PHP es un acrónimo recursivo que significa "**P**HP **H**ypertext **P**re-processor" (inicialmente PHP Tools, o, *P*ersonal *H*ome *P*age Tools), y se trata de un lenguaje interpretado usado para la creación de aplicaciones para servidores, o creación de contenido dinámico para sitios web. Últimamente también para la creación de otro tipo de programas incluyendo aplicaciones con interfaz gráfica usando las librerías Qt o GTK+.

El fácil uso y la similitud con los lenguajes más comunes de programación estructurada, como C y Perl, permiten a la mayoría de los programadores experimentados crear aplicaciones complejas con una curva de aprendizaje muy suave. También les permite involucrarse con aplicaciones de contenido dinámico sin tener que aprender todo un nuevo grupo de funciones y prácticas.

Debido al diseño de PHP, también es posible crear aplicaciones con una interfaz gráfica para el usuario (también llamada GUI), utilizando la extensión PHP-Qt o PHP-GTK. También

puede ser usado desde la línea de órdenes, de la misma manera como Perl o Python pueden hacerlo, esta versión de PHP se llama PHP CLI (*Command Line Interface*).

Su interpretación y ejecución se da en el servidor web, en el cual se encuentra almacenado el script, y el cliente sólo recibe el resultado de la ejecución. Cuando el cliente hace una petición al servidor para que le envíe una página web, generada por un script PHP, el servidor ejecuta el intérprete de PHP, el cual procesa el script solicitado que generará el contenido de manera dinámica, pudiendo modificar el contenido a enviar, y regresa el resultado al servidor, el cual se encarga de regresárselo al cliente. Permite la conexión a diferentes tipos de servidores de bases de datos tales como MySQL, Postgres, Oracle, ODBC, DB2, Microsoft SQL Server, Firebird y SQLite; lo cual permite la creación de Aplicaciones web muy robustas.

PHP también tiene la capacidad de ser ejecutado en la mayoría de los sistemas operativos tales como UNIX (y de ese tipo, como Linux o Mac OS X) y Windows, y puede interactuar con los servidores de web más populares ya que existe en versión CGI, módulo para Apache.

Usos de PHP

Los principales usos del PHP son los siguientes:

Programación de páginas web dinámicas, habitualmente en combinación con el motor de base 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 o Shell scripting.

Creación de aplicaciones gráficas independientes del navegador, por medio de la combinación de PHP y Qt/GTK+, lo que permite desarrollar aplicaciones de escritorio en los sistemas operativos en los que está soportado.

Ventajas de PHP

- Es un lenguaje multiplataforma.
- Capacidad de conexión con la mayoría de los manejadores de base de datos que se utilizan en la actualidad, destaca su conectividad con MySQL
- Leer y manipular datos desde diversas fuentes, incluyendo datos que pueden ingresar los usuarios desde formularios HTML.
- Capacidad de expandir su potencial utilizando la enorme cantidad de módulos (llamados ext's o extensiones).
- Posee una amplia documentación en su página oficial ([1]), entre la cual se destaca que todas las funciones del sistema están explicadas y ejemplificadas en un único archivo de ayuda.
- Es libre, por lo que se presenta como una alternativa de fácil acceso para todos.
- Permite las técnicas de Programación Orientada a Objetos.
- Permite crear los formularios para la web.

Historia

Versión	**Fecha**	**Cambios más importantes**
PHP 1.0	8 de Junio de 1995	Oficialmente llamado "Herramientas personales de trabajo (PHP Tools)". Es el primer uso del nombre "PHP".
PHP Version 2 (PHP/FI)	16 de Abril de 1996	Considerado por el creador como la "más rápida y simple herramienta" para la creación de páginas webs dinámicas .

PHP 3.0	6 de Junio de 1998	Desarrollo movido de una persona a muchos desarrolladores. Zeev Suraski y Andi Gutmans reescriben la base para esta versión.
PHP 4.0	22 de Mayo de 2000	Se agregan avanzadas de dos etapas analizar/ejecutar la etiqueta-análisis sistema llamado entorno motor Zend.
PHP 4.1	10 de Diciembre de 2001	Introducidas las variables superglobals ($_GET, $_SESSION, etc.)
PHP 4.2	22 de Abril de 2002	Se deshabilitan register_globals por defecto
PHP 4.3	27 de Diciembre de 2002	Introducido la CLI, en adición a la CGI
PHP 4.4	11 de Julio de 2005	
PHP 5.0	13 de Julio de 2004	Motor Zend II con un nuevo modelo de objetos.
PHP 5.1	25 de Noviembre de 2005	
PHP 5.2	2 de Noviembre de 2006	Habilitado el filtro de extensiones por defecto
PHP 5.2.4	30 de agosto de 2007	

2.14 MySQL

Es un sistema de gestión de base de datos relacional, multihilo y multiusuario con más de seis millones de instalaciones[1]. MySQL AB desarrolla MySQL como software libre en un esquema de licenciamiento dual. Por un lado lo ofrece bajo la GNU GPL, pero, empresas que

quieran incorporarlo en productos privativos pueden comprar a la empresa una licencia que les permita ese uso.

Al contrario de proyectos como el Apache, donde el software es desarrollado por una comunidad pública, y el copyright del código está en poder del autor individual, MySQL es propiedad y está patrocinado por una empresa privada, que posee el copyright de la mayor parte del código. Esto es lo que posibilita el esquema de licenciamiento anteriormente mencionado. Además de la venta de licencias privativas, la compañía ofrece soporte y servicios. Para sus operaciones contratan trabajadores alrededor del mundo que colaboran vía Internet. MySQL AB fue fundado por David Axmark, Allan Larsson, y Michael Widenius.

Lenguajes de programación

Existen varias APIs que permiten, a aplicaciones escritas en diversos lenguajes de programación, acceder a las bases de datos MySQL, incluyendo C, C++, C#, Pascal, Delphi (via dbExpress), Eiffel, Smalltalk, Java (con una implementación nativa del driver de Java), Lisp, Perl, PHP, Python, Ruby, REALbasic (Mac), FreeBASIC, y Tcl; cada uno de estos utiliza una API específica. También existe un interfaz ODBC, llamado MyODBC que permite a cualquier lenguaje de programación que soporte ODBC comunicarse con las bases de datos MySQL.

Aplicaciones

MySQL es muy utilizado en aplicaciones web como MediaWiki o Drupal, en plataformas (Linux/Windows-Apache-MySQL-PHP/Perl/Python), y por herramientas de seguimiento de errores como Bugzilla. Su popularidad como aplicación web está muy ligada a PHP, que a menudo aparece en combinación con MySQL. MySQL es una base de datos muy rápida en la lectura cuando utiliza el motor no transaccional MyISAM, pero puede provocar problemas de integridad en entornos de alta concurrencia en la modificación. En aplicaciones web hay baja

concurrencia en la modificación de datos y en cambio el entorno es intensivo en lectura de datos, lo que hace a MySQL ideal para este tipo de aplicaciones.

Especificaciones

Plataformas

MySQL funciona sobre múltiples plataformas, incluyendo AIX, BSD, FreeBSD, HP-UX, GNU/Linux, Mac OS X, NetBSD, Novell Netware, OpenBSD, OS/2 Warp, QNX, SGI IRIX, Solaris, SunOS, SCO OpenServer, SCO UnixWare, Tru64, Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Vista y otras versiones de Windows.

Características de la versión 5.0.22

- Un amplio subconjunto de ANSI SQL 99, y varias extensiones.
- Soporte a multiplataforma
- Procedimientos almacenados
- Triggers
- Cursors
- Vistas actualizables
- Soporte a VARCHAR
- INFORMATION_SCHEMA
- Modo Strict
- Soporte X/Open XA de transacciones distribuidas; transacción en dos fases como parte de esto, utilizando el motor InnoDB de Oracle
- Motores de almacenamiento independientes (MyISAM para lecturas rápidas, InnoDB para transacciones e integridad referencial)
- Transacciones con los motores de almacenamiento InnoDB, BDB Y Cluster; puntos

de recuperación(savepoints) con InnoDB

- Soporte para SSL
- Query caching
- Sub-SELECTs (o SELECTs anidados)
- Replication with one master per slave, many slaves per master, no automatic support for multiple masters per slave.
- indexing y buscando campos de texto completos usando el motor de almacenamiento MyISAM
- Embedded database library
- Soporte completo para Unicode
- Conforme a las reglas ACID usando los motores InnoDB, BDB y Cluster
- Shared-nothing clustering through MySQL Cluster

Características adicionales

- Usa GNU Automake, Autoconf, y Libtool para portabilidad
- Uso de multihilos mediante hilos del kernel.
- Usa tablas en disco b-tree para búsquedas rápidas con compresión de índice
- Tablas hash en memoria temporales
- El código MySQL se prueba con Purify (un detector de memoria perdida comercial) así como con Valgrind, una herramienta GPL
- Completo soporte para operadores y funciones en cláusulas select y where.
- Completo soporte para cláusulas group by y order by, soporte de funciones de agrupación

- Seguridad: ofrece un sistema de contraseñas y privilegios seguro mediante verificación basada en el host y el tráfico de contraseñas está cifrado al conectarse a un servidor.
- Soporta gran cantidad de datos. MySQL Server tiene bases de datos de hasta 50 millones de registros.
- Se permiten hasta 64 índices por tabla (32 antes de MySQL 4.1.2). Cada índice puede consistir desde 1 hasta 16 columnas o partes de columnas. El máximo ancho de límite son 1000 bytes (500 antes de MySQL 4.1.2).
- Los clientes se conectan al servidor MySQL usando sockets TCP/IP en cualquier plataforma. En sistemas Windows se pueden conectar usando named pipes y en sistemas Unix usando ficheros socket Unix.
- En MySQL 5.0, los clientes y servidores Windows se pueden conectar usando memoria compartida.
- MySQL contiene su propio paquete de pruebas de rendimiento proporcionado con el código fuente de la distribución de MySQL.

MySQL es un sistema de administración de bases de datos. Una base de datos es una colección estructurada de tablas que contienen datos. Esta puede ser desde una simple lista de compras a una galería de pinturas o el vasto volumen de información en un red corporativa. Para agregar, acceder a y procesar datos guardados en un computador, usted necesita un administrador como MySQL Server. Dado que los computadores son muy buenos manejando grandes cantidades de información, los administradores de bases de datos juegan un papel central en computación, como aplicaciones independientes o como parte de otras

aplicaciones. MySQL es un sistema de administración relacional de bases de datos. Una base de datos relacional archiva datos en tablas separadas en vez de colocar todos los datos en un gran archivo. Esto permite velocidad y flexibilidad. Las tablas están conectadas por relaciones definidas que hacen posible combinar datos de diferentes tablas sobre pedido.

Tipos de compilación del servidor

Hay tres tipos de compilación del servidor MySQL:

1. **Estándar:** Los binarios estándar de MySQL son los recomendados para la mayoría de los usuarios, e incluyen el motor de almacenamiento InnoDB.
2. **Max** (No se trata de MaxDB, que es una cooperación con SAP): Los binarios incluyen características adicionales que no han sido lo bastante probadas o que normalmente no son necesarias.
3. **MySQL-Debug:** Son binarios que han sido compilados con información de depuración extra. No debe ser usada en sistemas en producción porqué el código de depuración puede reducir el rendimiento.

CAPÍTULO III

PROYECTO TEMATICO

3.1 Proyecto Temático.

Para la implementación del proyecto se iniciará realizando una respectiva descripción de la Educación informal específicamente lo relacionado a los diplomados y luego las especificaciones de la propuestas.

El Diplomado, forma parte del sistema regular de especialización profesional, dirigido a titulados de carreras de educación superior, a profesionales que se desempeñen en actividades afines y a personas que acrediten debidamente su relación con los objetivos del Diplomado en particular. Tiene un periodo de duración dependiendo de lo que se enseñara en el diplomado por lo que puede llegar a estar distribuidas en a lo menos 2 semestres o 3 trimestres, donde se incluyen, laboratorios, tareas, proyectos u otras actividades.

Es un programa que le sirve al estudiante para ejercitar una tarea determinada en su área de interés y en el que una vez concluido recibe certificado de participación. Su metodología parte de modelos temáticos, combinación de aspectos teóricos prácticos, conferencias o charlas de los docentes con la participación activa de los estudiantes y ejercicios prácticos de los mismos. Ahora bien: frente a los demás cursos, los diplomados tienen a su favor la intensidad horaria, la profundización del tema y la calidad de los conferencistas

Son cursos de estudios no conducentes a la obtención de títulos ni de grados académicos, curriculares dinámicos y flexibles, de profundización y actualización del conocimiento en diferentes áreas, que satisface necesidades específicas del contexto social, nacional e internacional. No constituyes estudios de postgrado

El proyecto esta enfocado al planteamiento de cuatro diplomados, estructurados de tal forma que existen un eje común entre cada uno de ellos, y estableciendo punto de especialización para el desarrollo de estos.

Cada uno de los diplomados esta formado por módulos; se define como modulo la parte de un paquete didáctico que tiene por objeto cubrir objetivos particulares de enseñanza, estableciendo metodologías y procesos de desarrollo para su implementación, y secuencia al momento de la ejecución.

La estructura que se presenta para el desarrollo de los diplomados es la siguiente:

Diplomado No. 1

Nombre: **Servidores WEB**

Módulos a implementarse en este modulo:

1. *Introducción a LINUX-GNU*
2. *Servicios de redes con LINUX*
3. Servidor Web Apache
4. Servidor de correo SendMail

Diplomado No. 2

Nombre: **Seguridad con Linux**

Módulos a implementarse en este modulo:

1. *Introducción a LINUX-GNU*
2. *Servicios de redes con LINUX*
3. Seguridad Básica
4. Seguridad Avanzada

Diplomado No. 3

Nombre: **Administración remota**

Módulos a implementarse en este modulo:

1. *Introducción a LINUX-GNU*
2. *Servicios de redes con LINUX*
3. Terminal Server VNC
4. Wedmin

Diplomado No. 4

Nombre: **Desarrollo Web**

Módulos a implementarse en este modulo:

1. *Introducción a LINUX-GNU*
2. *Servicios de redes con LINUX*
3. PHP
4. My SQL

Cada diplomado esta formado por 4 modulo, de los cuales dos de ellos se repiten para cada diplomado, esta modalidad nos permite, desarrollar competencias en los participantes de tal forma le permite para cada uno de ellos contar con las bases para poder dale continuidad al proceso del conocimiento especializado.

3.2 Cronograma

Mes	AGOSTO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE				DIC		
Semana/Actividad	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3
Búsqueda general de información																			

FASE 1 Definir los parámetros para el desarrollo de los diplomados																			
FASE 2 Elaboración de los Diseños Instruccionales																			
FASE 3 Elaboración de las guías de trabajo																			

3.3 Documentación Técnica

Se implementara el desarrollo del diplomado mediante manuales y materiales didácticos con los cuales esperamos que la población estudiantil aproveche al máximo para presentarse en un ámbito más competitivo para que puedan mejorar tanto académicamente como intelectualmente.

3.4 Evaluación Técnica y Económica

3.4.1 Evaluación Técnica

Se cuenta con el recurso técnico necesario como es el hardware , el software y el recurso humano para que por medio de ellos brinde los servicios al sistema operativo y con esto se planteara el ambiente idóneo para el adecuado control de los usuraos y de los recursos de información .

3.4.2 Evaluación Económica

En el parte económica no se adquirirá ningún equipo informático ya que la Escuela de Informática de la Universidad Tecnológica de El Salvador cuenta ya con el Hardware requerido para implementar este proyecto, esto significa que la Universidad Tecnológica de El Salvador en ningún momento realizara un gasto económico ya que los encargados de costear estos gastos para la implementación será la empresa proveedora del proyecto si es que no se tiene ya el equipo antes proporcionado, por lo que se lleva a la conclusión de que este proyecto cuenta con la factibilidad económica necesaria para su respectiva implementación en la Universidad Tecnológica de El Salvador.

3.5 Tecnología y Recursos Seleccionados

Para llevar a cabo el siguiente punto es necesario tener en cuenta varios factores o productos para poder realizar dicho diplomado con los que se contara con los recursos tecnológicos y humanos.

3.6 Presupuesto Proyectado

El proyecto en si no posee gasto alguno ya que la Universidad Tecnológica de El Salvador cuenta con estos recursos físicos de hardware para entrar en ejecución., aun asi se hace una

presentación económica de posibles gastos al no contar con el recurso físico.

Nª	**Cantidad**	**Nombre**	**Descripción General del Equipo y Accesorios**	**Precio Unitario**	**Precio Total**
1	25	computadoras	a. Disco duro de 80 GB b. Tarjeta de red c. Memoria RAM 512 Mb d. Monitor e. Mouse f. Teclado g. 6 puertos USB	$450	$11,250
2	1	Servidor	a. Disco duro de 120GB b. Tarjeta de red c. Memoria RAM 1Gb d. Monitor e. Mouse f. Teclado g. 6 puertos USB	$700	$700
3	1	Distribución	Sistema Operativo	Gratis	Gratis

		UBUNTU			
4	2	Instalación y configuración	UBUNTU LINUX	$100	$200
5	1	Guía Técnica del Administrador	Pasos Técnicos de cómo administrar UBUNTU		
6					

3.7 Oferta Técnica:

Presentamos como oferta Técnica cuatro módulos de Diplomado en Plataforma Linux,

Basados en guías escritas y prácticas cada uno para desempeño del alumno.

Diplomado No. 1

Nombre: Servidores WEB

Módulos a implementarse en este modulo:

- ✓ Servidor Web Apache
- ✓ Servidor de correo SendMail
- ✓ Introducción a LINUX-GNU
- ✓ Servicios de redes con LINUX

Diplomado No. 2

Nombre: Seguridad con Linux

Módulos a implementarse en este modulo:

- ✓ Seguridad Básica
- ✓ Seguridad Avanzada
- ✓ Introducción a LINUX-GNU
- ✓ Servicios de redes con LINUX

Diplomado No. 3

Nombre: Administración remota

Módulos a implementarse en este modulo:

- ✓ Terminal Server VNC
- ✓ Webmin
- ✓ Introducción a LINUX-GNU
- ✓ Servicios de redes con LINUX

Diplomado No. 4

Nombre: Desarrollo Web

Módulos a implementarse en este modulo:

- ✓ PHP
- ✓ My SQL
- ✓ Introducción a LINUX-GNU
- ✓ Servicios de redes con LINUX

3.8 Oferta Económica:

Para implementación de este diplomado se debe contar por lo menos:

- ✓ 5 a 10 Computadoras Completas
- ✓ (Monitor, Mouse, teclado, etc) **Costo $500.00 c/u**

  Pentium 4 3.0Ghz

  Memoria RAM 512MB

  Lector/ Quemador DVD
- ✓ El Sistema Operativo es Gratuito
- ✓ Swicht 24 puertos Costo $80

CAPITULO IV

PROPUESTA

4.1 Articulo.

4.1.1 ¿Cómo se concibió el proyecto?

Gracias a la facultad de ciencias aplicadas a través de la escuela de informática surgió la necesidad de desarrollar ciertos diplomados en Linux/Gnu ya que uno de los problemas fundamentales que enfrentan las diferentes áreas de informática tanto software y hardware que en estas áreas se necesita reforzar a el estudiante cuando ya haya terminado su carrera de informática tanto en las carreras técnicas , la licenciatura e incluso la ingeniería con temas como por ejemplo Servidores Web, PHP, MySQL, Seguridad en Linux., Con el objeto de adquirir, actualizar y perfeccionar la competencia en el área, Con lo cual dichos diplomados se adaptan a las necesidades y exigencias de las empresas públicas y privadas.

4.1.2 ¿Cómo lo desarrollamos?

Esta serie de diplomados están conformados por cuatro diplomados modulares en Linux que están divididos en 4 módulos cada uno, contando con 2 módulos comunes y 2 diferentes.

Dependiendo lo que el estudiante desearía seguir estudiando para aumentar sus conocimientos den el área respectiva podrá escoger entre 4 diferentes Diplomados modulares entre los cuales estarán a su elección:

4.1.3 ¿Qué logramos con el proyecto?

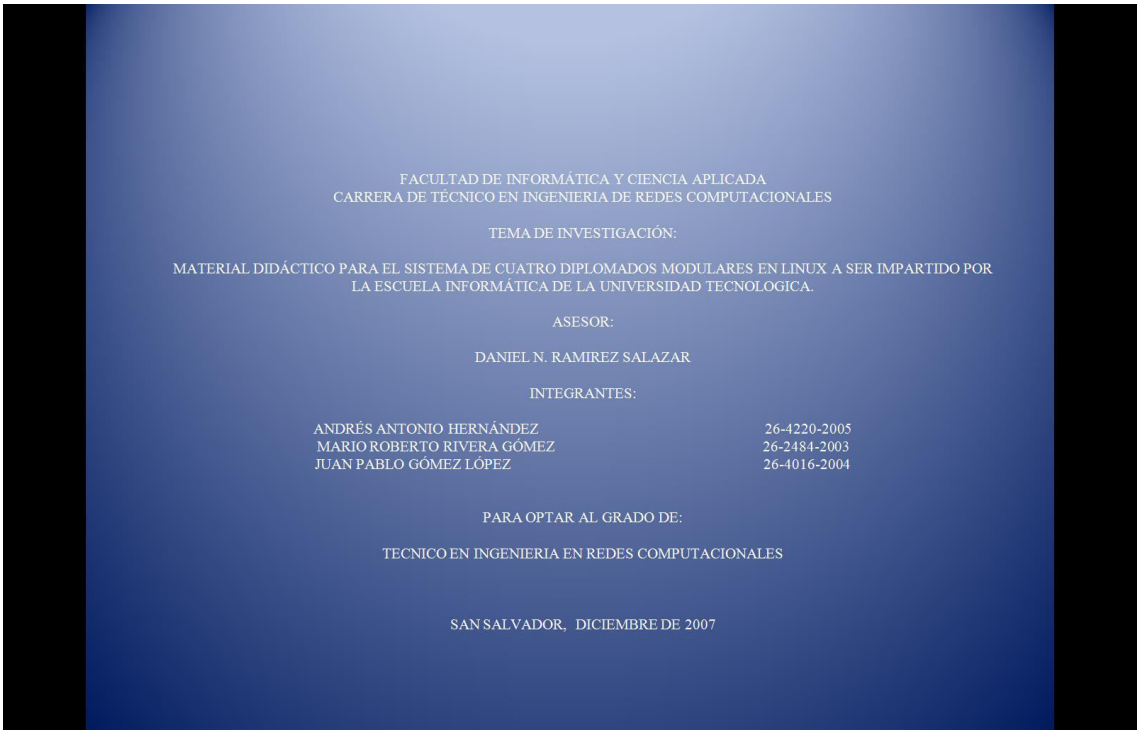
Con la implementación del proyecto se lograra complementar las deficiencias que se tuviera por parte de los estudiantes en las carreras informáticas en las cuales no tocaron

con tanta profundidad del desarrollo en el área de servidores web, seguridad, administración remota, PHP y MySQL

4.1.4 ¿Qué sigue después de este proyecto?

Terminado con la elaboración de este proyecto se venderá por medio de los integrantes del grupo que hicieron posible esta presentación a las empresas proveedoras que estén interesadas en estos diplomados modulares a parte de la Universidad Tecnológica de El Salvador.

4.2 Presentación del Proyecto



PROYECTO

MATERIAL DIDÁCTICO PARA EL SISTEMA DE CUATRO DIPLOMADOS MODULARES EN LINUX A SER IMPARTIDO POR LA ESCUELA INFORMÁTICA DE LA UNIVERSIDAD TECNOLOGICA.

OBJETIVO GENERAL

Elaborar el material didáctico para el sistema de cuatro diplomados modulares en LINUX, a hacer impartidos por la Escuela de Informática de la Universidad Tecnológica de El Salvador

OBJETIVOS ESPECIFICOS

1. Desarrollar los Lineamientos para el Sistema de los cuatro diplomados modulares en Linux /GNU, a hacer implementados en la Escuela de Informática de la Universidad Tecnológica de El Salvador.

2. Elaborar los diseños instruccionales de cada uno de los diferentes módulos del sistema de diplomados modulares.

3. Elaborar el material didáctico para el desarrollo de sus respectivos diplomados modulares impartidos por la Universidad Tecnológica de El Salvador.

SITUACION PROBLEMÁTICA

La Facultad de Informática a través de la Escuela de Informática imparte diplomados con el objeto de desarrollar, adquirir, actualizar y perfeccionar competencias en el área de GNU/LINUX que cierta medida no son desarrolladas de forma suficiente en la carrera de tecnología que se ha seleccionado, o en su defecto participa población en general que no son estudiantes activos de la Universidad, pero que visualizan que dichos diplomados se adaptan a las necesidades y exigencias de las empresas tanto públicas como privadas.

Uno de los problemas fundamentales que actualmente enfrentan las casas de educación superior, se deben específicamente a no contar con conocimientos específicos para responder a las diferentes necesidades del mundo laboral, lo que lleva a hacer planteamientos de capacitaciones cortas llamadas Diplomados, para el desarrollo de las competencias que la población estudiantil presenta con una serie de deficiencias en el área de servidores Web como por ejemplo: PHP, MySQL, Seguridad Linux entre otras y que de alguna manera no son impartidas durante el desarrollo de un carrera técnica.

DELIMITACIONES

DELIMITACION GEOGRAFICA:

El proyecto se llevara a cabo en la Universidad Tecnológica de El Salvador, Facultad de Informática y Ciencias Aplicadas, Escuela de Informática, ubicada sobre la calle Arce edificio N° 1020, San Salvador

DELIMITACION TEMPORAL:

El Proyecto de graduación comprenderá un tiempo estimado de 6 meses aproximadamente, dicho lapso está contemplado en reuniones cortas con el encargado de dar las instrucciones de cómo se elaborará el proyecto, así mismo con el asesor designado.

DELIMITACION ESPECÍFICAS:

Falta de enseñanza y material de apoyo especifico en las asignaturas impartidas por las diferentes cátedras a lo largo de nuestra carrera, poniendo de manifiesto el déficit de conocimiento de este Sistema Operativo.

¿ Qué es Diplomado ?

Es un programa que le sirve al estudiante para ejercitar una tarea determinada en su área de interés y en el que una vez concluido recibe certificado de participación. Su metodología parte de modelos temáticos, combinación de aspectos teóricos prácticos, conferencias o charlas de los docentes con la participación activa de los estudiantes y ejercicios prácticos de los mismos. Ahora bien: frente a los demás cursos, los diplomados tienen a su favor la intensidad horaria, la profundización del tema y la calidad de los conferencistas

¿Qué es un Módulo?

Parte de un paquete didáctico que tiene por objeto cubrir objetivos particulares de enseñanza.

Metodología de un diplomado

- El diplomado se llevará a cabo mediante clases presénciales teórico-prácticas, exponiéndose los
- contenidos del temario y desarrollo de prácticas en un ambiente agradable lleno de profesionalismo.
- El alumno participará activamente en los trabajos programados para la asignatura.
- La metodología a utilizar será activa en actividades de percepción, interpretación y expresión
- Elaboración y exposición de los trabajos programados.
- Se desarrollarán actividades tanto individual como en grupos. Metodología teórico-práctica.
- Parte de los conocimientos teóricos se facilitará por escrito, comentándolo luego para su comprensión.

Ventajas:

- ✓ Se lleva un calendario de estudios.
- ✓ Se planifican los temas.
- ✓ Se calendarizan las evaluaciones.
- ✓ Existe fecha limite de estudios.

Desventajas:

- ✓ No hay recuperación de tiempo perdido.
- ✓ No existe una retroalimentación de todos los temas que no se pudieron ver con anterioridad.
- ✓ No hay prórroga para las evaluaciones.
- ✓ Requiere de mucha disciplina para poder llevar a cabo las actividades en las fechas calendarizadas.
- ✓ Se requiere de mucho tiempo para elaborar las planificaciones
- ✓ Es necesario tener una supervisión de los contenidos que se han impartido

GENERALIDADES LINUX /GNU

- Es un sistema operativo descendiente de UNIX. Unix es un sistema operativo robusto, estable, multiusuario, multitarea, multiplataforma y con gran capacidad para gestión de redes.

- Linux es compatible con Unix. Dos características muy peculiares lo diferencian del resto de los sistemas que podemos encontrar en el mercado, la primera, es que es libre, esto significa que no tenemos que pagar ningún tipo de licencia a ninguna casa desarrolladora de software por el uso del mismo, la segunda, es que el sistema viene acompañado del código fuente. El sistema lo forman el núcleo del sistema (kernel) más un gran número de programas / librerías que hacen posible su utilización.

CARACTERISTICAS DE LINUX/GNU

- **Linux y sus Shells:** Cada usuario de un sistema Linux tiene su propia interfaz de usuario o Shell. Los usuarios pueden personalizar sus shells adecuándolos a sus propias necesidades específicas. En este sentido, el Shell de un usuario funciona más como un entorno operativo que el usuario puede controlar.

- **Linux es Multitarea:** La multitarea no consiste en hacer que el procesador realize más de un trabajo al mismo tiempo (un solo procesador no tiene esa capacidad), lo único que realiza es presentar las tareas de forma intercalada para que se ejecuten varias simultáneamente. Por lo tanto en Linux es posible ejecutar varios programas a la vez sin necesidad de tener que parar la ejecución de cada aplicación.

- **Linux es Multiusuario:** Para que pueda desarrollar esta labor (de compartir los recursos de un ordenador) es necesario un sistema operativo que permita a varios usuarios acceder al mismo tiempo a través de terminales, y que distribuya los recursos disponibles entre todos. Así mismo, el sistema debería proporcionar la posibilidad de que más de un usuario pudiera trabajar con la misma versión de un mismo programa al mismo tiempo, y actualizar inmediatamente cualquier cambio que se produjese en la base de datos, quedando reflejado para todos.

- **Linux es Seguro:** El concepto de seguridad en redes de ordenadores es siempre difícil de abordar. Un sistema puede ser seguro para un determinado tipo de actividades e inseguro para otras. Si se quiere que el sistema sea seguro, se debe administrar de tal forma que se tengan controlados a los usuarios en todo momento. Para la ardua tarea de seguridad surgen nuevas herramientas constantemente, tanto para detectar intrusos como para encontrar fallos en el sistema y evitar así ataques desde el exterior.

Bibliografía

MARGARITA MANTEROLA Y MAXIMILIANO CURIA, Configuración de Servicios de Red en GNU/Linux, [en línea PDF] Versión Beta - Octubre 2003 [15 de septiembre 2007]
<http://www.gnuservers.com.ar/cursos/redes/configuracion.pdf>

CHRISTOPHER SHUMWAY. Configuración SendMail, [en línea]. Escrito por Bill Lloyd. Reescrito por Jim Mock. Manual de FreeBSD, Cap. 26[20 de septiembre de 2007]
<http://www.freebsd.org/doc/es_ES.ISO8859-1/books/handbook/sendmail.html>

HORST H. VON BRAND, Universidad Técnica Federico Santa María Departamento de Informática, Seguridad en Linux, [en línea] Casilla 110-V Valparaíso, Chile, 20 de noviembre de 2000 [30 de septiembre de 2007]
<http://linux.ubiobio.cl/pasados/primero/documentacion/hvb/seguridad/t1.html>

LAURA MOLINA, Instalación y configuración del apache [en línea PDF], octubre 2004, [15 de octubre 2007]
<http://www.cs.cinvestav.mx/Estudiantes/TesisGraduados/2004/tesisLauraMolina.pdf>

NACX, configuración de una vnc, [en línea] 2001-2007 ADSL AYUDA [18 de octubre 2007] <http://www.adslayuda.com/Linux-vnc_linux.html>

AUTOR: FEDERICO ALMADA, Webmin: Administrar Linux fácilmente, [en línea], Fecha de publicación: 26/03/2007, [25 de octubre de 2007]
<http://www.techtear.com/2007/03/26/webmin-administrar-linux-facilmente/>

TODOMANDRAKE, Linux es libre, [en línea] Copyright 2000 - 2005 Miro International Pty Ltd. All rights reserved. [01 de noviembre de 2007]
<http://www.linux-es-libre.org/libertad/Documentos/Webmin/index.html>

ES.WIKIPEDIA.ORG, que es MySQL, Español Manual Referencia Oficial Ver 5.0 MySQL en español. Extensión mejorada de MySQL para PHP.[en línea]pagina modificada ultima vez el 3 de enero de 2008 [10 de noviembre de 2007]
<http://es.wikipedia.org/wiki/MySQL>

MYSQL-HISPANO.ORG, Introducción a MySql, [en línea] 08 de Agosto de 2006. Spain – España [15 de noviembre de 2007]
<http://www.webestilo.com/mysql/>

JOEL BARRIOS DUEÑAS, introducción mysql,[en línea] lunes, 05 de febrero 2007españa[20 de noviembre de 2007]
<http://www.linuxparatodos.net/portal/staticpages/index.php?page=como-mysql-quickstart>

OSMOSIS LATINA, Instalación MySQL en Plataformas Linux. Diseñado bajo estándares: XHTML CSS[en línea], año 2006, [25 de noviembre de 2007] <http://javaweb.osmosislatina.com/mysql_linux.htm>