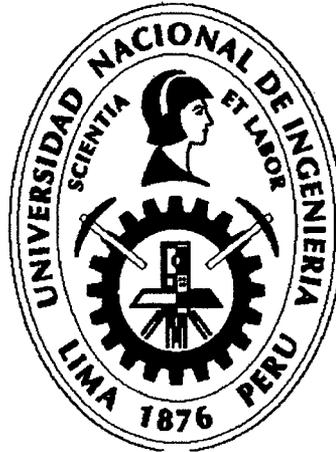


UNIVERSIDAD NACIONAL DE INGENIERÍA

Facultad de Ingeniería Industrial y de Sistemas

Sección Posgrado



**EL USO DE SOFTWARE LIBRE EN LA MINIMIZACIÓN DE
COSTOS EN CENTROS DE TECNOLOGÍA DE INFORMACIÓN
EN UNA UNIVERSIDAD PERUANA**

TESIS

**PARA OPTAR EL GRADO ACADÉMICO DE:
MAESTRO EN CIENCIAS CON MENCIÓN EN
INGENIERÍA DE SISTEMAS**

ELABORADO POR:

ING. PATRICIA LOURDES SALAS CHACÓN

ASESORA: DRA. GLORIATERESITA HUAMANI

LIMA – PERU

2014

Digitalizado por:

**Consortio Digital del
Conocimiento MebLatam,
Hemisferio y Dalse**

*A mis hermanos Jorge, Rosario, Jaime y Alfredo,
con afecto y cariño.*

*A Lourdes y Mario, por darme las oportunidades para
ser la profesional que hoy puedo ser.*

A Dios, por todo.

INDICE

DESCRIPTORES TEMÁTICOS	5
RESUMEN	6
ABSTRACT	7
INTRODUCCIÓN	8
<u>CAPÍTULO I</u> : PROTOCOLO DE INVESTIGACIÓN	10
1.1 Diagnóstico y Evaluación del Problema.....	10
1.1.1 De las Metas del Negocio a las Metas de TI –PROCESOS DE TI –COBIT	13
1.1.2 Procesos de TI por dominios -COBIT.....	14
1.1.3 Determinación del Modelo de Madurez del proceso seleccionado.....	15
1.2 Formulación del Problema.....	17
1.3 Objetivos.....	18
1.4 Importancia y Justificación de la Investigación.....	18
1.5 Hipótesis.....	22
1.6 Operalización de Variables.....	22
1.7 Limitaciones.....	24
<u>CAPÍTULO II</u> : MARCO TEÓRICO	25
2.1 Antecedentes.....	25
2.1.1 Software Libre.....	25
2.1.2 Experiencias de migración a Software Libre.....	28
2.1.3 Distribuciones Linux que empleadas para virtualizar escritorios con LTSP..	29
2.2 Marco Conceptual	30
2.2.1 Software Libre - Linux.....	30
A Comandos Básicos	31
B Directorio Personal	32
C Comandos Avanzados	44

D	Interprete de Comandos: Shell	57
E	Sistema de Archivos	65
2.2.2	Centro de Tecnología de Información - Data Center- Clasificación	74
2.2.2.1	CTIs Centralizados a Distribuidos	78
2.2.2.2	Niveles de disponibilidad de un Data Center - Norma ANSI/TIA 942.....	89
	Uptime Institute - TIER	
2.2.3	Virtualización.....	102
2.2.3.1	Tipos de Virtualización	107
2.2.3.2	Aplicaciones para Virtualización.....	110
2.3	Marco Teórico.....	114
2.3.1	Virtualización de escritorios	114
2.3.2	Linux Terminal Server Project - LTSP	116
2.3.3	Fases de Implementación de un Data Center / Centros de Datos.....	120
2.3.3.1	Estándares para la Implementación de un Centros de Datos.....	134
2.3.4	COBIT.....	139
2.3.4.1	Criterios de Información de COBIT.....	139
2.3.4.2	Recursos de TI.....	141
2.3.4.3	Los procesos requieren Controles.....	143
2.3.4.4	Controles del Negocio y Controles de TI.....	145
2.3.4.5	Generadores de Mediciones.....	145
2.3.4.6	Medición del Desempeño.....	148
2.3.4.7	Marco de Trabajo General de COBIT.....	148
2.4	Método de Costeo ABC.....	149
	<u>CAPITULO III: METODOS Y PROCEDIMIENTOS</u>	156
3.1	Tipo y diseño de la Investigación.....	156
3.2	Población y muestra.....	157
3.3	Técnicas e Instrumentos de Recolección de Datos.....	157
	<u>CAPITULO IV: RESULTADOS DE LA INVESTIGACIÓN</u>	158
4.1	Comparación de un centro de cómputo-LTSP con uno tradicional.....	158
4.2	Implantación de LTSP	163
4.3	Evaluación de Resultados.....	183
	CONCLUSIONES Y RECOMENDACIONES	186

CONCLUSIONES	186
RECOMENDACIONES	186
BIBLIOGRAFIA	187

APENDICES:

1. Encuesta de fin de semestre 2011-II a estudiantes de la Carrera Profesional de Ingeniería de Sistemas de Informática.....	190
2. Entrevista realizada al personal de soporte técnico de los laboratorios de cómputo de la Universidad Peruana de Ciencias e Informática.....	191
3. Determinación de las Metas de TI a partir de las Metas del Negocio, basado en el marco de trabajo de COBIT 4.1	192
4. Establecimiento de los Procesos de TI que requieren ser mejorados a partir de las Metas de TI, basado en el marco de trabajo de COBIT 4.1.....	193
5. Matriz de operalización de variables	194

ANEXOS

1. Librerías de trabajo de COBIT versiones 4.1 y 5
2. Instalación y configuración del servicio DHCP en Linux Ubuntu
3. Instalación y configuración del servicio TFTP en Linux Ubuntu
4. Instalación y configuración del servicio NFS en Linux Ubuntu
5. Instalación y configuración del servicio XDMCP en Linux Ubuntu
6. Guía de administración Ubuntu Desktop

DESCRIPTORES TEMÁTICOS

Implementación de Centros de Tecnologías de Información con software libre

Disminución de costos en CTIs

LTSP

Virtualización de escritorios con Software Libre

Linux

Cobit

Reutilización de equipos reciclados

RESUMEN

La presente investigación constituye un análisis técnico-económico en torno a la comparación entre la implementación de un Centro de Tecnología de Información convencional conformado por equipos de cómputo con Unidades de Procesamiento independiente con un Centro de Tecnología de Información virtualizado vía software libre.

Asimismo se detalla las ventajas tecnológicas que representa el empleo del Software Libre LTSP que comprende un conjunto de aplicaciones Servidor, las cuales proporcionan la capacidad de ejecutar Linux en computadores con pocas prestaciones de velocidad y de bajo costo, permitiendo reutilizar equipos que actualmente resultan obsoletos debido a los altos requerimientos de performance de los sistemas operativos comerciales.

ABSTRACT

This investigation is a technical-financial analysis regarding the comparison between implementing a conventional Computer Center equipped with independent System Units and a virtualized Computer Center with open source software.

Furthermore, shows the technology advantages about using open source software like LTSP which provides a bundle of server side applications that can run Linux in low end computers, which nowadays are obsolete because of private operating systems require high end hardware.

INTRODUCCION

Las multinacionales de hardware y software imponen una carrera de desarrollo tecnológico conllevando a que el equipamiento informático quede obsoleto en corto tiempo; sin embargo, muchas de las actividades que se realizan con apoyo de los ordenadores no requieren seguir esta tendencia de renovación de hardware.

El software Libre es cada vez más reconocido en el mercado por sus prestaciones, todos de alguna manera utilizan software libre, a través de navegadores, buscadores, productos comerciales, sistemas operativos, etc.; en estos momentos se tiene un considerable número de Proyectos libres, entre ellos el Proyecto de Terminal Server-LTSP, muy apreciado por permitir el funcionamiento de equipos de baja performance como terminales ligeros de un servidor LTSP.

Para entornos educativos, LTSP reduce tanto los costos por hardware al hacer posible el uso de máquinas con baja performance - Clientes ligeros, como los gastos por concepto de administración por tener que instalar y administrar desde el software del servidor todo el funcionamiento de los equipos clientes; minimizando el riesgo de pérdida de información en caso un terminal presente fallas físicas.

La presente investigación plantea la implementación de tecnologías basadas en Software Libre en un Centro de Tecnología de Información en un ámbito educativo, conllevando a la optimización de uso de activos de TI, tanto a nivel de implementación hardware-software como en su

administración. Al mismo tiempo permitió promover la investigación en tecnologías basadas en Software Libre en estudiantes de la universidad Peruana de Ciencias e Informática y promover la investigación.

El presente trabajo consta de cinco capítulos: el primero presenta el protocolo de investigación, donde se caracterizó el problema en base a un diagnóstico inicial empleando COBIT 4.1, se definen los objetivos, importancia de la investigación, Hipótesis, variables e indicadores y limitaciones; en el segundo se aborda el marco teórico, el tercero determina los métodos y procedimientos empleados, el cuarto muestra los resultados de la investigación, finalmente las conclusiones y recomendaciones.

CAPÍTULO I

PROTOCOLO DE INVESTIGACIÓN

1.1 Diagnóstico y Evaluación del Problema

La Universidad Peruana de Ciencias e Informática es una Institución Educativa con 10 años de existencia. Su visión, "Ser una Universidad líder con presencia internacional, que proyecte un modelo académico auténtico al servicio del estudiante y la sociedad, mediante una relación sinérgica entre ciencia, tecnología y cultura, utilizando procesos prospectivos en docencia, investigación y proyección social".

La Carrera Profesional de Ingeniería de Sistemas e Informática tiene una población estudiantil de 1500 alumnos. Cuenta con cinco (05) laboratorios: dos (02) laboratorios con cuarenta (40) equipos de cómputo Corei5, un (01) laboratorio con cincuenta (50) equipos Corei3 y un (01) laboratorio de veinte (20) equipos virtualizados con Windows 2007.

Adicionalmente cuentan con un (01) laboratorio de treinta (30) equipos de cómputo que fue dado de baja por su baja performance: (Pentium 4 con 256 y 512 MB de memoria RAM), algunos de ellos con fallas su disco duro.

- Respecto a la asignación de horas de laboratorio, se verificó cursos como por ejemplo: Sistemas Operativos e Ingeniería de Software I,

tiene asignado el mismo laboratorio a la misma hora, motivo por el cual deben turnar el uso de horas de laboratorio; la cantidad de laboratorios y equipos de cómputo no abastece el requerimiento actual y la administración de los mismos no satisface las expectativas de los usuarios, lo que fue ratificado por una encuesta de opinión realizada al alumnado y docentes al finalizar el semestre 2011-II (**Apéndice N° 1**), de cuyo resultado se tiene:

- ❖ El 65% aseveró que la cantidad de laboratorios de cómputo con que se cuenta no es suficiente.
 - ❖ El 80% señala, los equipos de cómputo todo el tiempo están infectados con diversos virus informáticos.
 - ❖ El 30% reclamó, no se tienen instalados los aplicativos requeridos de manera oportuna.
 - ❖ El 90% indicó, el laboratorio virtualizado con Windows sólo funciona con la Suit Ofimática Microsoft Office 2010 y Acrobat, se reportan problemas de performance con el uso de software de desarrollo en entorno Java NetBeans y problemas de compatibilidad con el resto de software empleado: Rational Rose, MS Project, entorno de desarrollo LAMP, entre otros.
- Al respecto, el personal de soporte, dos (02) técnicos, turno mañana y noche, señalaron: (**Apéndice N° 2**)
 - ❖ Los estudiantes introducen todo el tiempo USBs infectados con virus y a pesar que se mantiene actualizado el antivirus licenciado Node32, la base de datos de un antivirus no contiene las firmas de todos los virus existentes.
 - ❖ Los estudiantes acceden a páginas y descargan archivos infectados.

- ❖ Se tiene que estar reinstalando constantemente los equipos debido a que los estudiantes instalan programas, malogran archivos de sistema de los equipos, con lo cual algunas veces los docentes no encuentran instalados los aplicativos requeridos.
- ❖ No se tiene presupuesto asignado al área de soporte que permita incrementar la cantidad de técnicos para trabajos de soporte técnico, que de abasto a la demanda de trabajo actual.

Metas de Negocio:

Se mantuvo una entrevista con los stakeholders: miembros del directorio, responsable de sistemas, área virtual y producción y servicios, para identificar las metas de negocio de la universidad, al respecto establecieron como metas del negocio según se detalla:

Cuadro: Identificación de Metas de Negocio

n.º	Metas de Negocio identificadas	Selección de los Stakeholders
1	Reducir el costo de sus procesos.	miembros del directorio
2	Mejorar y Mantener la funcionalidad de procesos del negocio.	miembros del directorio
3	Lograr optimizar el coste de entrega de servicios.	miembros del directorio
4	Establecer continuidad y disponibilidad de servicios.	miembros del directorio
5	Mejorar la orientación y servicio al cliente.	miembros del directorio
6	Gestionar los riesgos de TI que afecten al negocio.	miembros del directorio
7	Proporcionar retorno de inversión en TI	miembros del directorio

8	Gestionar los cambios del Negocio.	responsable de sistemas, área virtual y producción y servicios
9	Mejorar y Mantener productividad operacional y de personal.	
10	Gestionar productos e innovación de negocios.	

Fuente: Entrevista con Stakeholders; Elaboración propia

1.1.1 De las Metas del Negocio a las Metas de TI –PROCESOS DE TI - COBIT

El marco de trabajo de COBIT, define un conjunto de metas de negocio agrupadas según las cuatro (04) perspectivas de Balanced Scorecard: Financiera, del cliente, interna y de aprendizaje y crecimiento (**Anexo N° 1**), que están presentes en las organizaciones, según su realidad.

Cada meta de negocio está asociada a metas de TI (**Apéndice N° 3**); cada meta de TI está asociada a procesos de TI (**Apéndice N° 4**). Los procesos resultantes son los que requieren ser mejorados, sin embargo se priorizó aquellos que son más críticos para el negocio según el diagnóstico efectuado.

Para la priorización se tomó en cuenta la opinión de los stakeholders que tienen poder de decisión en la organización, quienes en base a la información operativa, riesgos asociados a los procesos del negocio, visión, misión seleccionaron a su criterio los procesos del negocio a ser mejorados.

Para la presente investigación se trabajó sobre un (01) proceso (Garantizar la continuidad del servicio - DS4), al respecto se procedió a determinar su nivel de madurez con la finalidad de efectuar un análisis de brechas entre el estado actual del proceso y el deseado o requerido por la organización, todo ello tuvo como resultado las propuestas de mejora para dicho proceso, las cuales se plasmaron en

la formulación del presente proyecto que está alineado con las metas del negocio, es decir un proyecto de TI que genera o agrega Valor a la organización al dar soporte a procesos de la cadena de valor de la organización.

1.1.2 PROCESOS DE TI POR DOMINIO - COBIT

DOMINIO: PLANEAR Y ORGANIZAR

- PO1 Definir un Plan Estratégico de TI
- PO2 Definir la Arquitectura de la Información
- PO3 Determinar la Dirección Tecnológica
- PO4 Definir los Procesos, Organización y Relaciones de TI
- PO5 Administrar la Inversión en TI
- PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia
- PO7 Administrar Recursos Humanos de TI
- PO8 Administrar la Calidad
- PO9 Evaluar y Administrar los Riesgos de TI
- PO10 Administrar Proyectos

DOMINIO: ADQUIRIR E IMPLEMENTAR

- AI1 Identificar soluciones automatizadas
- AI2 Adquirir y mantener software aplicativo
- AI3 Adquirir y mantener infraestructura tecnológica
- AI4 Facilitar la operación y el uso
- AI5 Adquirir recursos de TI
- AI6 Administrar cambios
- AI7 Instalar y acreditar soluciones y cambios

DOMINIO: ENTREGAR Y DAR SOPORTE

- DS1 Definir y administrar los niveles de servicio
- DS2 Administrar los servicios de terceros

DS3 Administrar el desempeño y la capacidad
<u>DS4 Garantizar la continuidad del servicio (Proceso Seleccionado)</u>
DS5 Garantizar la seguridad de los sistemas
DS6 Identificar y asignar costos
DS7 Educar y entrenar a los usuarios
DS8 Administrar la mesa de servicio y los incidentes
DS9 Administrar la configuración
DS10 Administrar los problemas
DS11 Administrar los datos
DS12 Administrar el ambiente físico
DS13 Administrar las operaciones

DOMINIO: MONITOREAR Y EVALUAR
ME1 Monitorear y Evaluar el Desempeño de TI
ME2 Monitorear y Evaluar el Control Interno
ME3 Garantizar el Cumplimiento Regulatorio

1.1.3 Determinación del Modelo de Madurez del proceso DS4 “Garantizar la continuidad del servicio” en un laboratorio de cómputo.

0 No Existente cuando (NIVEL ACTUAL)
No hay entendimiento de los riesgos, vulnerabilidades y amenazas a las operaciones de TI o del impacto en el negocio por la pérdida de los servicios de TI. No se considera que la continuidad en los servicios deba tener atención de la gerencia.
1 Inicial / Ad Hoc cuando

Las responsabilidades sobre la continuidad de los servicios son informales y la autoridad para ejecutar responsabilidades es limitada. La gerencia comienza a darse cuenta de los riesgos relacionados y de la necesidad de mantener continuidad en los servicios. El enfoque de la gerencia sobre la continuidad del servicio radica en los recursos de infraestructura, en vez de radicar en los servicios de TI. Los usuarios utilizan soluciones alternas como respuesta a la interrupción de los servicios. La respuesta de TI a las interrupciones mayores es reactiva y sin preparación. Las pérdidas de energía planeadas están programadas para cumplir con las necesidades de TI pero no consideran los requerimientos del negocio.

2 Repetible pero Intuitivo cuando

Se asigna la responsabilidad para mantener la continuidad del servicio. Los enfoques para asegurar la continuidad están fragmentados. Los reportes sobre la disponibilidad son esporádicos, pueden estar incompletos y no toman en cuenta el impacto en el negocio. No hay un plan de continuidad de TI documentado, aunque hay compromiso para mantener disponible la continuidad del servicio y sus principios más importantes se conocen. Existe un inventario de sistemas y componentes críticos, pero puede no ser confiable. Las prácticas de continuidad en los servicios emergen, pero el éxito depende de los individuos.

3 Definido cuando (NIVEL DESEADO)

La responsabilidad sobre la administración de la continuidad del servicio es clara. Las responsabilidades de la planeación y de las pruebas de la continuidad de los servicios están claramente asignadas y definidas. El plan de continuidad de TI está documentado y basado en la criticidad de los sistemas y el impacto al negocio. Hay reportes periódicos de las pruebas de continuidad. Los individuos toman la iniciativa para seguir estándares y recibir entrenamiento para enfrentarse con incidentes mayores o desastres. La gerencia comunica de forma regular la necesidad de planear el aseguramiento de la continuidad del servicio. Se han aplicado componentes de alta disponibilidad y redundancia. Se mantiene un inventario de sistemas y componentes críticos.

4 Administrado y Medible cuando

Se hacen cumplir las responsabilidades y los estándares para la continuidad de los servicios. Se asigna la responsabilidad de mantener un plan de continuidad de servicios. Las actividades de mantenimiento están basadas en los resultados de las pruebas de mantener un plan de continuidad de servicios. Las actividades de mantenimiento están basadas en los resultados de las pruebas de continuidad, en las buenas prácticas internas y en los cambios en el ambiente del negocio y de TI. Se recopila, analiza y reporta documentación estructurada sobre la continuidad en los servicios y se actúa en consecuencia. Se brinda entrenamiento formal y obligatoria sobre los procesos de continuidad. Se implementan regularmente buenas prácticas de disponibilidad de los sistemas. Las prácticas de disponibilidad y la planeación de la continuidad de los servicios tienen influencia una sobre la otra. Se clasifican los incidentes de discontinuidad y la ruta de escalamiento es bien conocida por todos los involucrados. Se han desarrollado y acordado KGIs y KPIs para la continuidad de los servicios, aunque pueden ser medidos de manera inconsistente.

5 Optimizado cuando

Los procesos integrados de servicio continuo toman en cuenta referencias de la industria y las mejores prácticas externas. El plan de continuidad de TI está integrado con los planes de continuidad del negocio y se le da mantenimiento de manera rutinaria. El requerimiento para asegurar continuidad es garantizado por los proveedores y principales distribuidores. Se realizan pruebas globales de continuidad del servicio, y los resultados de las pruebas se utilizan para actualizar el plan. La recopilación y el análisis de datos se utilizan para mejorar continuamente el proceso. Las prácticas de disponibilidad y la continua planeación de la continuidad están totalmente alineadas. La gerencia asegura que un desastre o un incidente mayor no ocurrirá como resultado de un punto único de falla. Las prácticas de escalamiento se entienden y se hacen cumplir a fondo. Los KGIs y KPIs sobre el cumplimiento de la continuidad de los servicios se miden de manera sistemática. La gerencia ajusta la planeación de continuidad como respuesta a los KGIs y KPIs.

Fuente: Elaboración propia basada en el Modelo de Madurez propuesto por el Marco de trabajo de COBIT 4.1 para el proceso DS4 "Garantizar la continuidad del servicio"

Color Rosado: Nivel actual (0)

Color Verde: Nivel deseado / requerido (3)

1.2 Formulación del Problema

Problema General

¿En qué medida la utilización software libre minimiza los costos asociados a la implementación y administración de un Centro de Tecnología de Información en una universidad peruana?

Problemas Específicos

- ¿Es Posible prolongar el tiempo de vida útil de equipos de cómputo de escritorio con el empleo de software libre?
- ¿De qué manera se puede cuantificar los beneficios de utilizar software libre en la implementación y administración de un Centro de Tecnología de Información?

1.3 Objetivos

1.3.1 Objetivo general

Utilizar software libre para minimizar los costos asociados a una adecuada a la implementación y administración de un Centro de Tecnología de Información utilizando Software Libre en la Universidad Peruana de Ciencias e Informática

1.3.2 Objetivos específicos

- Aplicar la tecnología LTSP para reutilizar equipos de cómputo de baja performance.
- Elaborar un benchmarking entre el funcionamiento de equipos y costos asociados antes y después de la implementación de software libre en un Centro de Tecnología de información en una universidad peruana.

1.4 Importancia y justificación de la Investigación

1.4.1 Importancia de la Investigación

La tendencia del software como producto tecnológico es cada vez desarrollar versiones con nuevas prestaciones para sus usuarios, pero este incremento de prestaciones va en relación directa con la performance de hardware requerida para ejecutar eficientemente dicho software, es en este sentido, que los equipos de cómputo, en

un par de años de uso, quedan obsoletos por no poder soportar eficientemente las nuevas versiones de software que están en el mercado.

Perú es un país en vías de desarrollo, según el INEI, el nivel de pobreza en el Perú el 2011 fue de 27.8%, y en algunos departamentos como Apurímac, Cajamarca, Huancavelica, Huánuco y Ayacucho presentan un rango entre 53% y 57%¹, con lo cual se torna necesario buscar tecnologías que permitan alargar el tiempo de vigencia de la inversión efectuada en la infraestructura de Centros de Tecnología de Información, tal es el caso de ordenadores, disminuir costos de mantenimiento a nivel de software, adicionalmente es de resaltar que la utilización de software libre como base no solo permite tener un ahorro por concepto de licencia de software, sino que favorece el trabajo de investigación en Centros de Estudio donde es su razón de ser.

1.4.2 Justificación

A Justificación Económica

La implantación de software libre en Centros de Tecnología de Información hacen posible no solo el ahorro por concepto de licenciamiento de software, sino también permite el ahorro de costos de administración de los recursos informáticos, toda vez que sus bondades técnicas disminuyen la cantidad de horas de trabajo requeridas para mantener operativos dichos recursos informáticos.

¹ <http://www.inei.gob.pe/web/NuestrasActividadesFlotantePrincipal.asp?file=14357.jpg>

B Justificación Técnica

Linux es un sistema operativo de libre de licenciamiento que es conocido no solo por su alto nivel de seguridad, sino por requerir menor cantidad de recursos de hardware que otros sistemas operativos con licenciamiento copyright. La tecnología de los equipos de cómputo en los que se instaló Linux es Pentium IV con 512 MB de memoria RAM como máximo, algunos de ellos sin disco duro, dicha performance es suficiente para una configuración de virtualización de escritorios remotos bajo Linux.

C Justificación Ambiental:

El uso de software libre en general y especialmente del sistema LTSP, permite independizar a quien lo implanta de la política de renovación forzosa de hardware y software. En lo relativo al hardware, esta independencia genera diversos beneficios:

1. Se alarga la vida útil de los equipos de 3-4 años a 8-10 años, con la consiguiente reducción de residuos peligrosos en forma de equipos.
 2. No todos los departamentos o instituciones tienen los mismos requerimientos de equipos. Así, es posible establecer políticas de utilización de hardware donde aquellos departamentos con mayores requerimientos cedan sus terminales a otros con menos exigencia que tengan implantado sistemas cliente-Servidor o Web. Extendiendo esta política, pueden establecerse sumideros de equipos para fines educativos, por ejemplo, donde pueda darse uso a equipos adquiridos hace 5 o más años.
-

3. La política de renovación forzosa de equipos y software hace inviable la existencia de un mercado de segunda mano, como ocurre en otros sectores, favorece tremendamente la economía local. Por otro lado, la existencia de ese mercado justifica el despiece de equipos viejos y la recuperación de piezas de equipos que no funcionan y de otro modo, se desechan íntegramente. Un mercado de segunda mano reduce la generación de residuos.
 4. Los equipos informáticos son uno de los responsables del aumento de la demanda de consumo eléctrico, que genera unos gastos evidentes. Reducir el consumo de los equipos ha sido una prioridad en fabricantes e instituciones. El hecho de que los PCs convertidos en terminales de sistemas LTSP no requieran el disco duro ni dispositivos permite que sean retirados, lo que reduce su consumo. Al no residir el software en el propio equipo, no hay ninguna razón para no apagarlo cuando no esté en uso, reduciendo una vez más el consumo de electricidad.
 5. Si en vez de PCs, adquirimos clientes ligeros de reciente fabricación, el ahorro energético es muy superior puesto que estos dispositivos son reducidos y de bajo consumo. Estudios de diversas multinacionales y entidades independientes así lo atestiguan. Además, el residuo que genera un cliente ligero es inferior al de un PC, tanto en volumen como en masa. También generan menor contaminación acústica.
-

1.5 Hipótesis

1.5.1 Hipótesis General

- El uso de software libre minimiza los costos de funcionamiento de un Centro Tecnológico de Información en la Universidad Peruana de Ciencias e Informática.

1.5.2 Hipótesis Específicas

- La aplicación del Software Libre-LTSP, posibilita reutilizar equipos de cómputo de baja performance.
- Es factible efectuar un benchmarking del funcionamiento y costo de implementación de software libre en un Centro de Tecnología de información de la Universidad Peruana de Ciencias e Informática.

1.6 Operalización de Variables

Se detalla la matriz de consistencia en el **Apéndice N° 5**

Variable Independiente

- **Uso de Software Libre:** Software que respeta la libertad de los usuarios sobre su producto adquirido y por tanto, una vez obtenido puede ser usado, copiado, estudiado, cambiado y redistribuido libremente. Según la *Free Software Foundation*, el software libre se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software.

En la presente investigación se tuvo de base la utilización del sistema operativo Linux y servicios asociados a LTSP.

Indicadores:

1. Performance
2. Usabilidad

3. Cantidad de fallas registradas.

Variables Dependientes

• **Minimización de costos de funcionamiento en un CTI:** Conjunto de actividades que permiten la operatividad de un Centro de Tecnologías de Información.

Indicadores:

4. Costos de implementación de un CTI
5. Costos por concepto de Licenciamiento de software
6. Costo de administración de un CTI

Instrumentos y Escala de medición

Variable independiente	Indicador	Instrumento	Escala de medición
Uso de Software Libre base	-Performance	-Ficha Documental comparativa	Igual Mejor Peor
	-Usabilidad	-Documental -Encuestas	Muy bueno <80-100] Bueno .<70-80] Regular <55-70] Malo (0-55]
	-Cantidad de fallas registradas.	-Reportes de fallas	-Comparación con el Reporte de Fallas del Sistema Convencional.

Variables Dependientes	Indicador	Instrumento	Escala de medición
Minimización de costos de funcionamiento en un CTI	-Costo de implementación de un CTI. -Costos por concepto de Licenciamiento de software. -Costos de administración de un CTI.	* Documental: - Flujo de caja. Análisis Financiero: TIR y Costo/Beneficio	Rentabilidad del Proyecto. Comparación de costos antes y después de la implantación de proyecto.
Variables Dependientes	Indicador	Instrumento	Escala de medición
Minimización de costos de funcionamiento en un CTI	-Costo de implementación de un CTI. -Costos por concepto de Licenciamiento de software. -Costos de administración de un CTI.	* Documental: - Flujo de caja. Análisis Financiero: TIR y Costo/Beneficio	Rentabilidad del Proyecto. Comparación de costos antes y después de la implantación de proyecto.

1.7 Limitaciones

La limitación radicó en el poco nivel de conocimiento de software libre por parte del personal técnico encargado de dar soporte técnico a los equipos informáticos de la institución, toda vez que significó efectuar una capacitación desde aspectos básicos hasta nivel medió.

CAPITULO II

MARCO TEÓRICO

2.1 Antecedentes

2.1.1 Software Libre

Según la Fundación de Software Libre (Free Software Fundación):

«Software libre» significa que el software respeta la libertad de los usuarios y la comunidad. En términos generales, **los usuarios tienen la libertad de copiar, distribuir, estudiar, modificar y mejorar el software**. Con estas libertades, los usuarios (tanto individualmente como en forma colectiva) controlan el programa y lo que hace.

Cuando los usuarios no controlan el programa, el programa controla a los usuarios. El programador controla el programa y a través del programa, controla a los usuarios. Un programa que no es libre, llamado «privativo», es por lo tanto un instrumento de poder injusto.

Por tanto, el «software libre» es una cuestión de libertad, no de precio. Para entender el concepto, se debe pensar en «libre» como en «libre expresión».

Un programa es software libre si los usuarios tienen las cuatro libertades esenciales:

- La libertad de ejecutar el programa para cualquier propósito (**libertad 0**).
- La libertad de estudiar cómo funciona el programa, y cambiarlo para que haga lo que el usuario quiera (**libertad 1**). El acceso al código fuente es una condición necesaria para ello.
- La libertad de redistribuir copias para ayudar a su prójimo (**libertad 2**).
- La libertad de distribuir copias de sus versiones modificadas a terceros (**libertad 3**). Esto le permite ofrecer a toda la comunidad la oportunidad de beneficiarse de las modificaciones. El acceso al código fuente es una condición necesaria para ello.

2.1.2 Experiencias de migración a Software Libre

Jesús Javier Estepa Nieto, en su investigación “Software Libre en países en vías de desarrollo”, da a conocer experiencias de migración en administración a software libre en diferentes lugares:

A.- Alemania:

Ayuntamiento de Munich: La ciudad de Munich, que con sus 1,3 millones de habitantes es la tercera ciudad más grande de Alemania, constituye el mejor ejemplo de la utilización del bajo coste de Linux para la búsqueda y negociación con Microsoft de un precio más reducido. En esta ciudad, el CEO de Microsoft visitó al alcalde con un precio especial.

A pesar de que el precio que Microsoft ofreció era significativamente inferior que el coste de migración al Software Libre, el ayuntamiento se decidió finalmente a favor de la alternativa libre, argumentando

que los costes a largo plazo de la dependencia del proveedor serían mayores que el margen de los descuentos a corto plazo.

Munich decidió migrar sus infraestructuras TI a Software Libre. La comunidad internacional del Software Libre sigue de forma muy cercana todo el proceso, que implica a pequeñas compañías locales, multinacionales del Software Libre y proveedores internacionales de Software Propietario. El proyecto recibe el nombre de LiMux.

La cronología del proceso fue la siguiente:

Estudio Preliminar:

2001: El ayuntamiento estudia alternativas a Microsoft.

2002: El ayuntamiento autoriza a los responsables TI a llevar a cabo un estudio preliminar.

2002/2003: Se realiza el Estudio Preliminar con la compañía Unilog.

Diseño Detallado:

2003: El ayuntamiento autoriza a los responsables TI a comenzar con el diseño detallado.

2003/2004: IBM y SuSE/Novell realizan este diseño detallado.

2004: Los responsables TI establecen las tareas para llevar a cabo el proceso de migración.

Migración:

2005: Fase de Preparación del Proyecto, en la que se incluyen las primeras ofertas.

2006 - 2008: Proceso de Migración a Linux.

B.- España

El Ayuntamiento de Zaragoza se convirtió en una de las ciudades pioneras de España en tener todos sus equipos funcionando con Linux, algo más de 2500 puestos informáticos. Significó un ahorro anual para el Consistorio de cerca de 1 millón en aspectos como la actualización, desarrollo, soporte, mantenimiento del software y la prolongación de vida útil del hardware. Este proceso, que se realizó de acuerdo con las recomendaciones nacionales y europeas, fue acometido por la Concejalía de Ciencia y Tecnología a través del Centro Municipal de Informática realizándose en tres fases. La primera fue la renovación de la llamada ofimática en Software Libre, es decir, modernizar todos aquellos programas que de forma más habitual se utilizan en el trabajo diario como pueda ser un procesador de textos, hojas de cálculo, acceso a internet o el correo electrónico. Una vez implantada y asimilada esta fase, se comenzó la segunda que significó la finalización del cambio con la implantación un sistema operativo GNU/Linux. Por último, se llevó a cabo procesos de adaptación de unas 1800 bases de datos Access que existían en el Ayuntamiento. Al principio se mantuvieron los dos sistemas operativos de forma simultánea para facilitar la adaptación y la formación de los trabajadores.

Todo el proceso, que se completó a finales de 2008, se realizó en colaboración con Novell, y requirió una inversión inicial y única de cerca de 700.000 € para la formación de los trabajadores del Ayuntamiento y para la migración a Software Libre propiamente dicha. El Gabinete de prensa y la Oficina de Relaciones con el Ciudadano ya están usando OpenOffice, y los siguientes fueron los funcionarios del Registro Municipal.

C.- Inglaterra

El ayuntamiento de la ciudad de Bristol ahorró más de 2 millones € a lo largo de 5 años en su migración de Microsoft Office a la suite StarOffice. El ayuntamiento tomó este movimiento como parte de sus esfuerzos para conseguir mejorar la eficiencia en el sector público dentro de un plan que promueve el gobierno.

El coste de StarOffice fue de 990.000 € mientras que el coste de Microsoft Office era de más de 2.5 € millones. Estos costes incluyeron los gastos en formación, soporte y migración para 5.500 usuarios.

La migración se llevó a cabo en el total de los 1.800 equipos y sus 5.000 usuarios.

Algunos continuaron trabajando con Microsoft Office, en los casos en los que fue necesario realizar tareas que todavía no eran soportadas por StarOffice.

2.1.3 Distribuciones Linux empleadas para virtualizar escritorios con LTSP

A.- Skolelinux²: Skolelinux se trata de una distribución Linux educativa implantada en más de cien centros educativos, distribuidos en Alemania y Noruega. Incluye, entre otros servicios y aplicaciones, el sistema LTSP. Se trata de una de las tecnologías del sistema ReciclaRed que permite la utilización de ordenadores tipo 486 o superiores como terminales para uso formativo.

² <http://www.slx.no/index.php>

B.- K12LTSP³: esta es la distribución Linux más veterana en la implantación de este tipo de sistemas.

C.- Edubuntu⁴: la fundación Shuttleworth Foundation está instaló 154 aulas en Sudáfrica y otros países limítrofes con 28 mil ordenadores obsoletos y para finales de 2005 fueron utilizados por 185 mil alumnos, en la URL "<http://www.tuxlab.org.za/tuxlabs.html>" de la fundación aparece el listado de centros en los que están implantados sistemas ReciclaRed (LTSP). También ha realizado implantaciones similares fuera de África, como la implantación de 160 equipos reutilizados en el Hospital infantil de Zagred, Croacia.

Una de las experiencias más conocidas en la Telecentros de Sao Paulo. Se trata de unos 6 mil centros educativos, cibercafés y salas donde el Gobierno Local ha implantado un aula en cada uno de ellos reutilizando equipos obsoletos, utilizando para ello sistemas ReciclaRed.

2.2 MARCO CONCEPTUAL

2.2.1 SOFTWARE LIBRE - LINUX

GNU/Linux (Linux) es uno de los términos empleados para referirse al sistema operativo libre similar a Unix que utiliza el núcleo Linux y herramientas de sistema GNU. Su desarrollo es uno de los ejemplos más prominentes de software libre; todo el código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera bajo los términos de la GPL (Licencia Pública General de GNU) y otras licencias libres.

³ <https://fedorahosted.org/k12linux>

⁴ <http://www.telecentros.sp.gov.br/>

A pesar de que Linux sólo es el núcleo de este sistema operativo una parte significativa de la comunidad, así como muchos medios generales y especializados, prefieren utilizar dicho término para referirse a la unión de ambos proyectos.

A las variantes de un sistema operativo GNU/Linux se las denomina distribuciones y su objetivo es ofrecer una edición que cumpla con las necesidades de determinado grupo de usuarios. Algunas de ellas son especialmente conocidas por su uso en servidores y supercomputadoras. No obstante, es posible instalarlo en una amplia variedad de hardware como computadoras de escritorio y portátiles.

A. Comandos Básicos de Linux

Para efectuar el cambio o la introducción de un *password* o *contraseña* se utiliza el comando *passwd*. El proceso a seguir es el siguiente:

passwd

(current) UNIX password: (se teclea la contraseña actual; no aparece en pantalla)

New UNIX password: (se teclea la nueva contraseña; no aparece en pantalla)

Retype new UNIX password: (se teclea de nuevo la nueva contraseña comprobando que se ha tecleado bien. Si no coincide no se cambia produce el cambio).

A continuación se describen algunos comandos sencillos de que pueden ser útiles para familiarizarse con los comandos del sistema.

<i>date</i>	Muestra por pantalla el día y la hora.
<i>cal 1949</i>	Muestra el calendario del año 1949.
<i>cal 05 1949</i>	Muestra el calendario de mayo de 1949.
<i>who</i>	Indica qué usuarios tiene el ordenador en ese momento, en qué terminal están y desde qué hora.
<i>whoami</i>	Indica cuál es la terminal y la sesión en la que se está trabajando.
<i>man comando</i>	Todos los manuales de <i>Linux</i> están dentro del propio sistema operativo, y este comando permite acceder a la información correspondiente al comando <i>comando</i> . Por ejemplo con <i>man who</i> aparecerá por pantalla y de forma formateada por páginas, la explicación del comando <i>who</i> . Se puede navegar a través de estas páginas con los cursores del teclado, y presionando <i>q</i> para salir.
<i>clear</i>	Este comando limpia la consola.

B. Directorio Personal

Como se ha visto anteriormente el directorio personal es un directorio con un determinado nombre asignado a un usuario. Los directorios personales habitualmente son subdirectorios de ***/home*** (en algunos casos se utiliza ***mnt***, u otro subdirectorio de orden inferior). Generalmente el nombre coincide con el del ***nombre de usuario***, aunque puede no ser así, y varios usuarios pueden estar

trabajando en el mismo directorio. Cada usuario de **Linux** puede crear una estructura en árbol de subdirectorios y archivos tan compleja como desee bajo su directorio personal pero normalmente nunca fuera de él.

B1. Listado del contenido de directorios: comando ls

Una de las acciones más habituales a la hora de trabajar es mostrar el contenido de un directorio, como se ha visto existen herramientas gráficas con este fin, no obstante el **shell** incluye un programa con este mismo fin: **ls**,

ls	Muestra los nombres de los ficheros y subdirectorios contenidos en el directorio en el que se está. Sólo se obtienen los nombres de los ficheros, sin ninguna otra información.
ls -a	Muestra todos los ficheros incluyendo algunos que ordinariamente están ocultos para el usuario (aquellos que comienzan por un punto). Se recuerda que el fichero punto . indica el directorio actual y el doble punto .. el directorio padre, que contiene, al actual.
ls -l	Esta es la opción de lista larga: muestra toda la información de cada fichero incluyendo: protecciones, tamaño y fecha de creación o del último cambio introducido,...
ls -c	Muestra ordenando por día y hora de creación.

- ls -t*** Muestra ordenando por día y hora de modificación.
- ls -r*** Muestra el directorio y lo ordena en orden inverso.
- ls subdir*** Muestra el contenido del subdirectorio ***subdir***.
- ls -l filename*** Muestra toda la información sobre el fichero.
- ls -color*** Muestra el contenido del directorio coloreado.

Las opciones anteriores pueden combinarse. Por ejemplo:

- ls -cr*** Muestra el directorio ordenando inversamente por fechas.
- El comando ***ls*** admite los caracteres de sustitución o metacaracteres (*) y (?). El carácter * representa cualquier conjunto o secuencia de caracteres. El carácter ? representa cualquier carácter, pero sólo uno.
- Por ejemplo:
- ls *.gif*** Muestra todos los nombres de ficheros que acaben en ***.gif***, por ejemplo ***dib1.gif, a.gif***, etc.
- ls file?*** Muestra todos los ficheros cuyos nombres empiecen por ***file*** y tengan un nombre de cinco caracteres, por ejemplo: ***file1, file2, filea***, etc.

B2. Comandos de administración de directorios

- **Creación de subdirectorios - Comando mkdir**

El comando *mkdir* (*make directory*) permite a cada usuario crear un nuevo subdirectorio:

mkdir subdir1

donde *subdir* es el nombre del directorio que se va a crear.

- **Borrado de subdirectorios - Comando rmdir**

Este comando borra uno o más directorios del sistema (*remove directory*), siempre que estos subdirectorios estén **vacíos**. Por ejemplo:

rmdir subdir1

donde *subdir* es el nombre del directorio que se va a eliminar.

- **Cambio de directorio. Comando cd**

Este comando permite cambiar de directorio a partir del directorio actual de trabajo. Por ejemplo,

cd /home/Pedro Pasa del directorio actual de trabajo al nuevo directorio */home/Pedro*, que será desde ahora el nuevo directorio.

cd dire Traslada al subdirectorio *dire* (que deberá existir como subdirectorio en el directorio actual).

cd .. Retrocedemos un nivel en la jerarquía de directorios. Por ejemplo, si estamos en */home/Pedro* y usamos este comando, pasaremos al escalafón inmediatamente superior de la jerarquía de directorios, en este caso a */home*.
Nota: al contrario que en *MS-DOS* en *Linux* no existe la forma **cd..** sin espacio entre **cd** y los dos puntos.

cd Sitúa nuevamente en el directorio personal del usuario.

- **Borrado de ficheros. Comando rm**

Este comando tiene las formas siguientes,

rm file1 file2

Este comando elimina uno o más ficheros de un directorio en el cual tengamos permiso de escritura. Con este comando resulta facilísimo borrar ficheros inútiles, y desgraciadamente, también los útiles. Por eso es conveniente y casi imprescindible emplear la opción **-i**, de la forma siguiente:

rm -i file1 file2

Con esta opción, *Linux* pedirá confirmación para borrar cada fichero de la lista, de si realmente se desea su destrucción o no. Se recomienda usar siempre este comando con esta opción para evitar el borrado de ficheros útiles. Por ejemplo, si se teclea,

rm -i superfluo

Aparece en pantalla el aviso siguiente:

remove superfluo?

y habrá que contestar *y* (yes) o *n* (not). En este comando se pueden utilizar los caracteres de sustitución (*** y *?*), como por ejemplo,

rm fich*

Borra todos los ficheros del directorio actual que comiencen por *fich*. El comando

rm *

Borra todos los ficheros del directorio actual, mientras que

rm -i *

Realiza una labor análoga, pero con previa confirmación.

- **Copia de ficheros. Comando cp**

Este comando tiene la siguiente forma,

cp file1 file2

y hace una copia de *file1* y le llama *file2*. Si *file2* no existía, lo crea con los mismos atributos de *file1*. Si *file2* existía antes, su contenido queda destruido y es sustituido por el de *file1*. El fichero *file2* estará en el mismo directorio que *file1*. Tanto *file1* como *file2* indican el nombre de un archivo, que puede incluir el la ruta al mismo si alguno de ellos no se encuentra en el directorio actual.

Otra posibilidad es:

cp file1 file2 namedir

Hace copias de *file1* y *file2* en el directorio *namedir*.

- **Traslado y cambio de nombre de ficheros. Comando mv**

mv file1 file2

El comando ***mv*** realiza la misma función que el anterior (***cp***) pero además destruye el fichero original. En definitiva traslada el contenido de ***file1*** a ***file2***; a efectos del usuario lo que ha hecho es cambiar el nombre a ***file1***, llamándole ***file2***. De igual forma,

mv file1 file2 namedir

traslada uno o más ficheros (***file1, file2,...***) al directorio ***namedir*** conservándoles el nombre. El comando,

mv namedir1 namedir2

cambia el nombre del subdirectorio ***namedir1*** por ***namedir2***.

El comando ***mv*** sirve así mismo para cambiar el nombre de los ficheros.

- **Situación actual. Comando pwd**

El comando ***pwd*** (***print working directory***) visualiza o imprime la ruta del directorio en el que nos encontramos en este momento. Este comando es uno de los pocos que no tiene opciones y se utiliza escribiendo simplemente ***pwd***.

- **Acceso a unidades de disco**

Linux a diferencia de ***Windows*** no utiliza letras ("a:", "c:", "d:", ...) para acceder a las distintas unidades de disco de un ordenador. En ***Linux*** para acceder al contenido de una unidad de disco o de

un CD-ROM este tiene que haber sido previamente "**montado**". El **montado** se realiza mediante el comando **mount**, con lo que el contenido de la unidad se pone a disposición del usuario en el directorio de **Linux** que se elija. Por ejemplo para acceder al CD-ROM se teclearía el siguiente comando:

```
mount -t iso9660 /dev/cdrom /mnt/cdrom
```

donde **-t iso9660** indica el tipo de sistema que usa la unidad de disco para guardar los ficheros (las más usuales son: **iso9660** en el caso de un CD-ROM, **vfat** en el caso de **Windows**, y **ext2** en el caso de **Linux**), **/dev/cdrom** indica el dispositivo que se va a montar. Todos los dispositivos están representados por un fichero del directorio **/dev**, por ejemplo en el caso de un disquete será seguramente **/dev/fd0**, por último **/mnt/cdrom** es el directorio en el que se pondrá a disposición del usuario el contenido del CD-ROM. Para montar disquetes se suele utilizar el directorio **/mnt/floppy**. De todas formas el usuario siempre puede crear un directorio vacío con el nombre que el elija para montar las unidades de disco que desee donde desee.

Cuando el usuario haya dejado de usar ese disco deberá "**desmontarlo**" mediante el comando **umount** antes de sacar el disquete o el CD-ROM. En este último caso debería escribir:

```
umount /mnt/cdrom
```

Para utilizar el comando **mount** de la forma anterior hace falta ser administrador o **root**. Para que un usuario común pueda utilizar disquetes, CD-ROM, etc. hay que editar el fichero **/etc/fstab** Por

ejemplo para que cualquier usuario pueda acceder a un disquete habrá que indicar la siguiente línea:

```
/dev/fd0 /mnt/floppy vfat user,noauto 0 0
```

También habrá que asegurarse de que el directorio ***/mnt/floppy*** sea accesible por todos los usuarios. Una vez seguidos los pasos anteriores cualquier usuario podrá "montar" un disquete escribiendo el siguiente comando:

```
mount /mnt/floppy
```

Al igual que antes el usuario deberá ejecutar el comando ***umount /mnt/floppy*** antes de sacar el disquete.

Nota: Existen en la actualidad distribuciones (p. ej. ***Linux Mandrake***) que realizan este proceso de forma automática por lo que las unidades de disquete y CD-ROM quedan accesibles a todos los usuarios de una forma sencilla, empleando los comandos:

```
mount /mnt/floppy  
umount /mnt/floppy
```

siempre que ***/mnt/floppy*** sea la ruta adecuada.

fsck /dev/[dispositivo] Chequea y repara el sistema de archivos de una partición no montada.

fsck.ext2 -vpf /dev/hdx Chequea y repara el sistema de archivos de una partición ext2 no montada.

fsck.ext3 -vpf /dev/hdx Igual pero con una partición ext3.

mkfs.ext2 /dev/hdXX Crea un sistema ext2 en la partición seleccionada.

mkfs.ext3 /dev/hdXX Crea un sistema ext3 en la partición seleccionada.

mkfs.ext2 /dev/fd0 Crea un sistema ext2 en el disquete.

mkswap /dev/hda2 Crea un sistema de ficheros swap.

tune2fs -O ^has_journal /dev/hdXX Convierte la partición de ext3 a ext2

tune2fs -j /dev/hdXX Convierte la partición de ext2 a ext3

B3. Enlaces a ficheros. Comando ln

En *Linux* un mismo fichero puede estar repetido con más de un nombre, ya que con el comando **cp** se pueden realizar cuantas copias se desee del fichero. Pero, a veces, es más práctico tener un mismo fichero con varios nombres distintos, y lo que es más importante, poder acceder a él desde más de un directorio. En *Linux* esto recibe el nombre de enlaces múltiples a un fichero. El ahorro de espacio de disco es importante al poder compartir un fichero más de

un usuario. Estos enlaces son muy prácticos a la hora de utilizar ficheros que pertenecen a directorios distintos. Gracias a los enlaces se puede acceder a muchos ficheros desde un mismo directorio, sin necesidad de copiar en ese directorio todos esos ficheros. La forma de este comando es,

In file1 file2

A partir de este momento el fichero ***file1*** tiene dos nombres: ***file1*** y ***file2***. A diferencia de los comandos ***cp*** y ***mv***, este comando toma más precauciones, ya que advierte previamente si el nombre ***file2*** está ocupado, y en este caso no se ejecuta.

In panacea subdir/panacea

Después de este comando el fichero ***panacea*** tendrá el mismo nombre, pero a efectos del usuario estará colocado en dos sitios distintos: en el directorio actual y en el subdirectorio ***subdir***.

Los ficheros enlazados a otro se borran como los ficheros normales. Si se borra el fichero original permanece su contenido en los ficheros enganchados.

B4. Propiedades de un fichero

Comando file

Este comando realiza una serie de comprobaciones en un fichero para tratar de clasificarlo. Su formato es:

file fich

Tras su ejecución este comando muestra el tipo del fichero e información al respecto del mismo.

Cambio de modo de los ficheros comandos *chmod*, *chown* y *chgrp*

Los permisos de cada fichero se pueden ver con el comando *ls -l*. Para cambiar los permisos de un fichero se emplea el comando ***chmod***, que tiene el formato siguiente:

chmod [quien] oper permiso files

quien Indica a quien afecta el permiso que se desea cambiar. Es una combinación cualquiera de las letras ***u*** para el usuario, ***g*** para el grupo del usuario, ***o*** para los otros usuarios, y ***a*** para todos los anteriores. Si no se da el ***quien***, el sistema supone ***a***.

oper Indica la operación que se desea hacer con el permiso. Para dar un permiso se pondrá un ***+***, y para quitarlo se pondrá un ***-***

permiso Indica el permiso que se quiere dar o quitar. Será una combinación cualquiera de las letras anteriores: ***r,w,x,s***.

files Nombres de los ficheros cuyos modos de acceso se quieren cambiar. Por ejemplo, para quitar el permiso de lectura a los usuarios de un fichero el comando es:

chmod a -r fichero.txt

Los permisos de lectura, escritura y ejecución tienen un significado diferente cuando se aplican a directorios y no a ficheros normales. En el caso de los directorios el permiso ***r***

significa la posibilidad de ver el contenido del directorio con el comando *ls*; el permiso *w* da la posibilidad de crear y borrar ficheros en ese directorio, y el permiso *x* autoriza a buscar y utilizar un fichero concreto.

Por otra parte, el comando ***chown*** se emplea para cambiar de propietario ("***change owner***") a un determinado conjunto de ficheros. Este comando sólo lo puede emplear el actual propietario de los mismos. Los nombres de propietario que admite ***Linux*** son los nombres de ***usuario***, que están almacenados en el fichero ***/etc/passwd***. La forma general del comando ***chown*** es la siguiente:

chown newowner file1 file2 ...

Análogamente, el grupo al que pertenece un fichero puede ser cambiado con el comando ***chgrp***, que tiene una forma general similar a la de ***chown***,

chgrp newgroup file1 file2...

Los grupos de usuarios están almacenados en el fichero ***/etc/group***.

C. Comandos Avanzados

C1 Espacio ocupado en el disco Comandos *du* y *df*

El comando ***du*** permite conocer el espacio ocupado en el disco por un determinado directorio y todos los subdirectorios que cuelgan de él. Para usarlo basta simplemente colocarse en el directorio adecuado y teclear, ***du***, éste comando da el espacio de disco utilizado en

bloques. Para obtener la información en bytes se debe emplear el comando con la opción **-h**: **du -h**

El comando **df** por el contrario informa del espacio usado por las particiones del sistema que se encuentren montadas.

C.2 Visualización sin formato de un fichero

Comando cat

Este comando permite visualizar el contenido de uno o más ficheros de forma no formateada. También permite copiar uno o más ficheros como apéndice de otro ya existente. Algunas formas de utilizar este comando son las siguientes:

cat filename Saca por pantalla el contenido del fichero **filename**.

cat file1 file2... Saca por pantalla, secuencialmente y según el orden especificado, el contenido de los ficheros indicados.

cat file1 file2 >file3 El contenido de los ficheros **file1** y **file2** es almacenado en **file3**.

cat file1 file2 >>file3 El contenido de **file1** y **file2** es añadido al final de **file3**.

cat >file1 Acepta lo que se introduce por el teclado y lo almacena en **file1** (se crea **file1**). Para terminar se emplea **<ctrl>d**

C.3 Comando head

head -7 filename

Escribe las 7 primeras líneas del fichero filename

C.4 Visualización de ficheros con formato

Comando pr

Este comando, a diferencia de ***cat***, imprime por consola el contenido de los ficheros de una manera formateada, por columnas, controlando el tamaño de página y poniendo cabeceras al comienzo de las mismas. Está muy en relación con el comando ***lp*** de salida por impresora. Las formas más importantes que admite son las siguientes:

pr file Produce una salida estándar de 66 líneas por página, con un encabezamiento de 5 líneas (2 en blanco, una de identificación y otras 2 líneas en blanco).

pr -ln file Produce una salida de n líneas por página (cuando el tamaño de papel de impresora, por ejemplo, tiene un número de líneas distinto de 66)

pr -p file Hace una pausa para presentar la página, hasta que se pulsa ***<return>*** para continuar

pr -t file Suprime las 5 líneas del encabezamiento y las del final de página.

pr -wn file Ajusta la anchura de la línea a n posiciones.

pr -d file Lista el fichero con espaciado doble.

pr -h `caracteres` file el argumento o cadena de caracteres ***`caracteres`*** se convertirán en la cabecera del listado.

pr +n file Imprime el fichero a partir de la página n.

Además de los ejemplos anteriores, se pueden combinar varias opciones en un mismo comando, como por ejemplo en: ***pr -dt file*** la salida de este comando es por la consola, pero puede redireccionarse a otro fichero, por ejemplo, si ejecutamos el comando: ***pr file1 > file2*** se crea un fichero nuevo llamado ***file2*** que es idéntico a ***file1***, pero con formato por páginas y columnas.

C.5 Visualización de ficheros pantalla a pantalla. Comandos *more* y *less*

Estos comandos permiten visualizar un fichero pantalla a pantalla. El número de líneas por pantalla es de 23 líneas de texto y una última línea de mensajes, donde aparecerá la palabra *more*. Cuando se pulsa la barra espaciadora (el espacio en blanco), se visualizará la siguiente pantalla. Para salir de este comando (terminar la visualización) se pulsa ***<ctrl>d*** o ***q***. Por ejemplo: ***more file***

El comando ***less*** es muy similar al anterior pero permite el desplazamiento a lo largo del texto empleando las teclas de cursores pudiendo desplazarse hacia arriba o abajo de un fichero.

C.6 Búsqueda en ficheros

Comandos *grep*, *fgrep* y *egrep*

El comando ***grep*** localiza una palabra, clave o frase en un conjunto de directorios, indicando en cuáles de ellos la ha encontrado. Este comando rastrea fichero por fichero, por turno, imprimiendo aquellas líneas que contienen el conjunto de caracteres buscado. Si el conjunto de caracteres a buscar está compuesto por dos o más palabras separadas por un espacio, se colocará el conjunto de caracteres entre apóstrofes ('). Su formato es el siguiente:

```
grep 'conjuntocaracteres' file1 file2 file3
```

Siendo 'conjuntocaracteres' la secuencia de caracteres a buscar, y ***file1***, ***file2***, y ***file3*** los ficheros donde se debe buscar. Veamos un nuevo ejemplo:

```
grep 'TRIANGULARIZACION MATRIZ' matrix.f scaling.f
```

Este comando buscará ***TRIANGULARIZACION MATRIZ*** entre las líneas de los ficheros ***matrix.f*** y ***scaling.f***. Este comando permite seleccionar, entre todas las líneas de uno o más ficheros, aquellas que contienen un motivo que satisface una expresión regular determinada.

```
grep [-opcion] expresión_regul ar [referencia...]
```

Las opciones principales son:

- c*** lo único que se hace es escribir el número de las líneas que satisfacen la condición.
- i*** no se distinguen mayúsculas y minúsculas.

I se escriben los nombres de los ficheros que contienen líneas buscadas.

N cada línea es precedida por su número en el fichero.

s no se vuelcan los mensajes que indican que un fichero no se puede abrir.

v se muestran sólo las líneas que no satisfacen el criterio de selección.

A continuación se muestran algunos ejemplos.

<i>grep "d" text</i>	líneas que comienzan por d.
<i>grep "[^d]" text</i>	líneas que no comienzan por d.
<i>grep -v "C" file1</i>	quita las líneas de file1 que comienzan con C y copia en file2.

C7 Comandos tar y gzip

Tanto el comando **tar** como **gzip** son ampliamente empleados para la difusión de programas y ficheros en **Linux**. El primero de ellos agrupa varios ficheros en uno solo o "**archivo**", mientras que el segundo los comprime. En conjunto estos dos programas actúan de forma muy similar a programas como **Winzip**. Para crear un nuevo archivo se emplea:

tar -cvf nombre_archivo.tar fichero1 fichero2 ...

Donde fichero1, fichero2 etc. son los ficheros que se van a añadir al archivo **tar**. Si se desea extraer los ficheros se emplea

tar -xpvf nombre_archivo.tar fichero1 ...

tar -vtf archivo.tar Muestra el contenido del archivo .tar sin descomprimirlo.

tar -zvcf archivo.tgz directorio Empaqueta y comprime (tgz) directorios o ficheros.

tar -zvxf archivo.tgz Desempaqueta y descomprime un archivo.tgz

tar -zvtf archivo.tgz Muestra el contenido de un tgz sin descomprimirlo ni desempaquetarlo.

tar -jvcf archivo.tbz2 directorio Empaqueta y comprime (tbz2) directorios o ficheros.

tar -jvxf archivo.tbz2 Desempaqueta y descomprime el archivo.tbz2

tar -jvtf archivo.tbz2 Muestra el contenido sin desempaquetar ni descomprimir el .tbz2

Al contrario que tar que agrupa varios ficheros en uno, ***gzip*** comprime un único fichero con lo que la información se mantiene pero se reduce el tamaño del mismo. El uso de ***gzip*** es muy sencillo

gzip fichero

Se comprime fichero (que es borrado) y se crea un fichero con nombre ***fichero.gz***. Si lo que se desea es descomprimir un fichero se emplea entonces:

gzip -d fichero.gz

Recuperando el fichero inicial. Es típico emplear ***tar*** y ***gzip*** de forma consecutiva, para obtener ficheros con extensión ***tar.gz*** o ***tgz*** que contienen varios ficheros de forma comprimida (similar a un fichero ***zip***). El comando ***tar*** incluye la opción ***z*** para estos ficheros de forma que para extraer los ficheros que contiene:

tar -zxf fichero.tar.gz

bzip2 ficheros Comprime ficheros al formato ***bz2***

bzip2 -d fichero.bz2 Descomprime un fichero.***bz2***

bzip2 -c fichero.bz2 Muestra el contenido de un fichero.***bz2*** sin descomprimirlo.

C.8 Comandos de impresión

- **Comando *lpr***

El comando ***lpr*** se emplea para imprimir una serie de ficheros. Si se emplea sin argumentos imprime el texto que se introduzca a continuación en la impresora por defecto. Por el contrario.

lpr nombre_fichero

Imprime en la impresora por defecto el fichero indicado.

lpr -#n fichero

Realiza “n” copias del fichero, donde n es un numero natural (1,2,3,4,5 ...).

- ***lpq***

Muestra los documentos en la cola.

- ***lprm***

Cancela la impresión del documento actual.

- ***lprm n***

Cancela la impresión del trabajo n, siendo n un número natural.

- ***pr +2 l70 -w 80 -h "Comandos" fichero -t***

Formatea un archivo de texto para la impresión.

-t

No imprimirá cabeceras ni pies de página.

l70

Establece la longitud de la página de 70 líneas (66 por defecto).

-w 80

Establece el ancho de línea en 80 caracteres (72 por defecto).

-h "Comandos"

Establece "Comandos" como cabecera de cada página.

pr l70 -d comandos.txt | lpr

Una vez formateado el texto lo manda a la cola de impresión

C.9 Formatos

tidy fichero.html Analiza el código de un documento html.

tidy -m fichero.html Corrige modificando el código del fichero html.

tidy -m -asxml fichero.html Convierte el fichero html a xml.

tidy -m -asxhtml fichero.html Convierte el fichero html a xhtml.

tidy -m -ashtml fichero.xhtml Convierte un fichero xhtml a html.

pdftops fichero.pdf fichero.ps Convierte un fichero pdf a ps.

C.10 Instalación de software

dpkg -i paquete Instala un paquete.

dpkg -r paquete Desinstala un paquete.

dpkg -purge paquete Desinstala un paquete y sus archivos de configuración.

dpkg -force -r paquete Fuerza la desinstalación de un paquete.

dpkg -force-all -r paquete Fuerza aun mas la desinstalación de un paquete (Puede comprometer el sistema).

- dpkg -c paquete*** Muestra el contenido de un paquete.
- dpkg -L paquete*** Muestra todos los ficheros que se instalaron con un paquete.
- dpkg -S fichero*** Muestra a que paquete pertenece un fichero.
- dpkg --get-selections*** Muestra un listado con todos los paquetes instalados.
- dpkg-reconfigure paquete*** Reconfigura el paquete.
- aptitude update*** Actualiza la lista de paquetes.
- aptitude upgrade*** Actualiza el sistema (no instala ni elimina paquetes).
- aptitude dist-upgrade*** Actualiza el sistema eliminando e instalando paquetes si fuera necesario.
- aptitude install [paquetes]*** Instala los paquetes indicados.
- aptitude reinstall [paquetes]*** Reinstala los paquetes indicados.
- aptitude remove [paquetes]*** Elimina los paquetes indicados.

aptitude purge [paquetes] Elimina los paquetes y sus ficheros de configuración.

aptitude download [paquetes] Descarga los paquetes en el directorio actual.

aptitude hold [paquetes] Bloquea los paquetes indicados.

aptitude unhold [paquetes] Desbloquea los paquetes seleccionados.

aptitude unmarkauto [paquetes] Desmarca paquetes como instalados manualmente.

Markauto Marca paquetes como instalados manualmente.

aptitude search [expresion] Busca un paquete por nombre o expresión.

aptitude show [paquete] Muestra información detallada de un paquete.

aptitude clean Elimina los paquetes .deb descargados.

C.11 Audio.

lame -b 192 -m j tema.wav Convierte una canción wav a mp3 con bitrate de 192 (Este valor puede sustituirse, la opción -h indica máxima calidad).

lame -h -m j -nogap *.wav

Convierte todos los archivos wav a mp3.

`lame -h --decode tema.mp3 tema.wav`

Convierte un archivo mp3 a wav.

`oggenc -b 128 -q 5 tema.wav` Convierte un archivo wav a ogg (-q 5 indica la calidad de 0 a 10).

`oggenc *.wav` Convierte todos los wav en un unico fichero ogg

`oggenc -a -l -t *.wav` Convierte todos los wav en sus respectivos ogg

`oggdec tema.ogg` Convierte un archivo ogg a wav

`oggdec *.ogg` Convierte todos los ogg a wav

`mplayer -ao pcm fichero.asf` Convierte un archivo asf o wma a wav

`play canción` Reproduce una canción en la terminal.

C.12 Comandos en background

Linux, como cualquier sistema Unix, puede ejecutar varias tareas al mismo tiempo. En sistemas monoprocesador, se asigna un determinado tiempo a cada tarea de manera que, al usuario, le parece que se ejecutan al mismo tiempo.

Para ejecutar un programa en background, basta con poner el signo ampersand (&) al término de la línea de comandos. Por ejemplo, si se quisiera copiar el directorio.

/usr/src/linux al directorio */tmp*:

```
#cp -r /usr/src/linux /tmp &  
#
```

Cuando ha terminado la ejecución del programa, el sistema lo reporta mediante un mensaje:

```
#  
[Done] cp -r /usr/src/linux /tmp  
#
```

Si se hubiese ejecutado el programa y no se hubiese puesto el ampersand, se podría pasarlo a background de la siguiente manera:

1. Se suspende la ejecución del programa, pulsando Ctrl+Z.
2. Se ejecutamos la siguiente orden: `bg`

D. Intérprete de comandos: Shell

El intérprete de comandos es el programa que recibe lo que se escribe en la terminal y lo convierte en instrucciones para el sistema operativo.

En otras palabras el objetivo de cualquier intérprete de comandos es ejecutar los programas que el usuario teclea en el *prompt* del mismo. El *prompt* es una indicación que muestra el intérprete para anunciar que espera una orden del usuario. Cuando el usuario escribe una orden, el intérprete ejecuta dicha orden. En dicha orden, puede haber programas internos o externos: Los programas internos son aquellos que vienen incorporados en el propio intérprete, mientras que los externos son programas separados

(ej: aplicaciones de */bin,/usr/bin,...*).

En el mundo Linux/Unix existen tres grandes familias de Shells como se muestra en la tabla a continuación. Estas se diferencian entre sí básicamente en la sintaxis de sus comandos y en la interacción con el usuario.

Tipo de Shell	Shell estándar	Clones libres
AT&T Bourne Shell	Sh	ash, bash, bash2
Berkeley "C" Shell	Csh	Tcsh
AT&T Korn Shell	Ksh	pdksh, zsh
Otros interpretes	--	esh, gush, nwsh

D.1 Redireccionamiento de E/S

La filosofía de Linux/Unix es en extremo modular. Se prefieren las herramientas pequeñas con tareas puntuales a las meta-herramientas que realizan todo. Para hacer el modelo completo es necesario proveer el medio para ensamblar estas herramientas en estructuras más complejas. Esto se realiza por medio del redireccionamiento de las entradas y las salidas.

Redirección de Entrada y Salidas

`fig_redirect width=5cm images/standard_io.eps`

Todos los programas tienen por defecto una entrada estándar (teclado) y dos salidas: la salida estándar (pantalla) y la salida de error (pantalla). En ellos se puede sustituir la entrada y salidas estándar por otro dispositivo utilizando los caracteres ``"y ``, es decir, hacer que se lea un archivo que contenga las opciones a ejecutar y un archivo de salida, respectivamente. Por ejemplo:

Entrada: Se desea realizar una transferencia de archivos por ftp automática. Para ello se va a utilizar el programa *ncftp* con unas determinadas instrucciones preestablecidas.

Se crea un archivo *entrada* con dichas instrucciones:

```
open linuxcol.uniandes.edu.co
cd /pub/linux/utils
get *
quit
```

y se ejecuta el programa: `ncftp < entrada .`

Salida: Se quiere saber los archivos que empiezan por *i* o *I* y almacenarlo en un archivo:

```
ls [iI]* > listado.txt
```

Es importante resaltar que el carácter de redirección de salida ```` destruirá el archivo al cual apunta, si este existe, para ser reemplazado por uno nuevo con los resultados del proceso. Si se desea anexar la información a uno ya existente debe usarse doble carácter ````:

D.2 Tuberías o pipes

La filosofía de Linux/Unix es en extremo modular. Se prefieren las herramientas pequeñas con tareas puntuales a las meta-herramientas que realizan todo. Para hacer el modelo completo es necesario proveer el medio para ensamblar estas herramientas en estructuras más complejas. Esto se realiza por medio del redireccionamiento de las entradas y las salidas.

Redirección de Entrada y Salidas

fig_redirect width=5cmimages/standard_io.eps

Todos los programas tiene por defecto una entrada estándar (teclado) y dos salidas: la salida estándar (pantalla) y la salida de error (pantalla). En ellos se puede sustituir la entrada y salidas estándar por otro dispositivo utilizando los caracteres ``"y ```", es decir, hacer que se lea un archivo que contenga las opciones a ejecutar y un archivo de salida, respectivamente. Por ejemplo:

Entrada:

Se desea realizar una transferencia de archivos por ftp automática. Para ello se va a utilizar el programa *ncftp* con unas determinadas instrucciones preestablecidas.

Se crea un archivo *entrada* con dichas instrucciones:

```
open linuxcol.uniandes.edu.co
cd /pub/linux/utills
get *
quit
```

y se ejecuta el programa: `ncftp < entrada .`

Salida:

Se quiere saber los archivos que empiezan por i o l y almacenarlo en un archivo:

```
ls [il]* > listado.txt
```

Es importante resaltar que el carácter de redirección de salida ``"destruirá el archivo al cual apunta, si este existe, para ser reemplazado por uno nuevo con los resultados del proceso. Si se

desea anexar la información a uno ya existente debe usarse doble carácter ``":

Bifurcación o T (comando tee)

A veces interesa que la salida de un comando, además de redirigirse a un determinado fichero, se bifurque también hacia la terminal, con objeto de observar inmediatamente el resultado. Esto se consigue con el operador **tee**, que podría emplearse de la siguiente forma:

ls | tee file

la salida de **ls** se bifurca hacia la terminal y hacia **file**.

Si quisiéramos que la salida de este comando se añadiera al final de **file**, deberíamos utilizar la opción **-a**,

ls | tee -a file

D.3 Programación shell

La programación del shell es una de las herramientas mas apreciadas por todos los administradores y muchos usuarios de Linux/Unix ya que permite automatizar tareas complejas, comandos repetitivos y ejecutarlas con un solo llamado al *script* o hacerlo automáticamente a horas escogidas sin intervención de personas. La programación *shell* en Unix/Linux es, en cierto sentido, equivalente a crear archivos *.BAT* en DOS. La diferencia es que en Unix/Linux es mucho más potente. Estos *scripts* pueden usar un sinnúmero de herramientas como:

- Comandos del sistema Linux/Unix (ejm: ls, cut)

- Funciones intrínsecas del shell (ejm: kill, nice)
- Lenguaje de programación del shell (ejm: if/then/else/fi) (ver tabla de comandos)
- Programas y/o lenguajes de procesamiento en línea. (ejm: awk, sed, Perl)
- Programas propios del usuario escritos en cualquier lenguaje.

El lenguaje de programación de cada shell provee de una amplia gama de estructuras de control como se muestra en la tabla de comandos de la shell

- for name [in word;] do list ; done
- select name [in word ;] do list ; done
- case word in [pattern [| pattern]\dots) list ;;]\dots esac
- if list then list [elif list then list]\dots [else list] fi
- \$while list do list done
- \$until list do list done
- [function] name () { list; }

Instrucciones *bash* para programación *shell* tbl_instr_bash

Por ejemplo para realizar un backup de solo ciertos directorios (prog_dir1 y prog_dir2), luego comprimirlos usando bzip2 y enviarlos a un area de almacenamiento (digamos una unidad ZIP previamente montada en /mnt/zipdrive), y además con que el nombre del archivo contenga la fecha del día. Suena difícil? Realmente no lo es.

Se crea un archivo texto con cualquier nombre, por ejemplo *mibackup* que contenga las instrucciones que se desea ejecutar.

```
#!/bin/sh

#
echo "----- Captura fecha -----"
fecha='date +%Y%m%d'

#
echo "----- Haciendo Tar -----"
tar cvf backup$fecha.tar prog_dir1 prog_dir2

#
echo "----- Comprimiendo -----"
bzip2 backup$fecha.tar

#
echo "----- Enviándolos a zip -----"
cp ./backup$fecha.tar /mnt/zipdrive

#
echo "----- Limpiando -----"
rm -f ./backup$fecha.tar

#
echo "----- Final -----"

Luego, se le asigna permisos de ejecución con el comando
chmod +x mibackup
```

y esta listo para ser ejecutado.

En el *script* aquí mostrado es importante resaltar varios principios importantes: la primera línea determina el shell que se esta usando (sh o bash); las variables no se declaran solo se asignan; su valor es retornado usando el símbolo \$.

Si desea mas información acerca de programación en shell se puede consultar los manuales en línea del shell: *bash* o *tcsh*

D.4 Re-utilización de comandos

El shell almacena una historia de los comandos que el usuario ha escrito. Por medio de esta historia es posible volver a ejecutar una orden que ya se ha escrito anteriormente sin tener que escribirla de nuevo.

El comando `history` muestra la secuencia de comandos, con un número a su izquierda.

Con este número es posible llamar de nuevo el comando utilizando el carácter admiración

```!";` Por ejemplo `history` retorna

1 `history`

2 `ls`

3 `cd public_html`

4 `ls`

5 `rm *.bak`

6 `history`

y para ejecutar nuevamente el comando `rm *.bak` solo es necesario escribir `!5`. También

se puede pedir el último ```rm"` que se ha ejecutado escribiendo `!rm`.

El último comando se repite con doble admiración ```!!"`. Es posible también editar el último comando utilizando el carácter ```^"` pero este conocimiento se está volviendo poco útil, ya que los nuevos

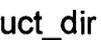
shells permiten viajar por la "historia" y editar los comandos usando únicamente las flechas del teclado.

## E. Sistema de Archivos

### E.1 Organización de los directorios

Linux organiza la información en archivos, los cuales están contenidos en directorios. Un directorio puede contener subdirectorios, teniendo así una estructura jerárquica, como en cualquier otro sistema operativo.

Las nuevas versiones de Linux (incluido Red Hat) siguen el estándar FSSTND (*Linux Filesystem Standard*) el cual estipula los nombres, la ubicación y la función de la mayoría de los directorios y los archivos del sistema. La siguiente tabla muestra la estructura básica del sistema de archivos de Linux como es definida por FSSTND.

Estructura de directorios de Linux según FSSTND 

width=10cmimages/struct\_dir.eps

Conociendo esta estructura básica, el usuario/administrador podrá moverse más fácilmente por los directorios, ya que la mayoría de éstos, tienen un determinado uso. En la siguiente tabla se tiene la descripción de los directorios más comunes.

Directorio	Descripción
/	Raíz ( <i>root</i> ), forma la base del sistema de archivos.
<i>/boot</i>	Archivos del kernel (compilados).
<i>/bin</i>	Archivos ejecutables esenciales para todos los usuarios.
<i>/dev</i>	Archivos de dispositivos.
<i>/etc</i>	Archivos de configuración.

<i>/etc/rc.d</i>	Archivos de inicialización (Red Hat).
<i>/home</i>	Generalmente, directorios de los usuarios.
<i>/home/ftp</i>	Contenido del servidor FTP.
<i>/home/httpd</i>	Contenido del servidor <u>WWW</u> .
<i>/lib</i>	Librerías esenciales y módulos del kernel.
<i>/mnt</i>	Directorios donde ``montar" diversos dispositivos
<i>/mnt/cdrom</i>	Directorio donde se ``monta" el CD-ROM.
<i>/mnt/floppy</i>	Directorio donde se ``monta" el disquete.
<i>/proc</i>	Información sobre partes del sistema.
<i>/root</i>	Directorio del usuario principal del sistema.
<i>/sbin</i>	Archivos ejecutables para tareas de administración.
<i>/tmp</i>	Temporal.
<i>/usr</i>	Programas, documentación, fuentes,...compartidos por todo el sistema
<i>/var</i>	Archivos variables del sistema, bitácoras, temporales,...

### Directorios de Linux más frecuentes

La tabla muestra los principales subdirectorios del directorio *usr*.

Directorio	Descripción
<i>/usr/X11R6</i>	Paquete XFree86 (X-Windows) Release 6.
<i>/usr/bin</i>	Archivos ejecutables para usuarios.
<i>/usr/dict</i>	Listados de palabras (diccionarios).
<i>/usr/doc</i>	Documentación.
<i>/usr/doc/FAQ</i>	F.A.Q. (o P.U.F.).
<i>/usr/doc/HOWTO</i>	HOWTO's.
<i>/usr/etc</i>	Archivos de configuración del sistema.
<i>/usr/games</i>	Juegos.
<i>/usr/include</i>	Archivos de encabezado.
<i>/usr/info</i>	Sistema de información GNU info.

<i>/usr/lib</i>	Librerías
<i>/usr/local</i>	Jerarquía de archivos locales.
<i>/usr/man</i>	Manuales.
<i>/usr/sbin</i>	Archivos ejecutables de administración no vitales.
<i>/usr/share</i>	Datos independientes de la arquitectura.
<i>/usr/src</i>	Código fuente.
<i>/usr/src/linux</i>	Código fuente del <i>kernel</i> de Linux.

### Subdirectorios de *usr*

La tabla muestra los principales subdirectorios del directorio *var*.

Directorio	Descripción
<i>/var/catman</i>	Manuales formateados localmente.
<i>/var/lib</i>	Información del estado de aplicaciones.
<i>/var/local</i>	Variables de aplicaciones en <i>/usr/local</i> .
<i>/var/lock</i>	Archivos de cerrojo.
<i>/var/log</i>	Bitácoras del sistema.
<i>/var/named</i>	Archivos del DNS.
<i>/var/nis</i>	Base de datos para NIS (Network Inf. Service).
<i>/var/preserve</i>	Archivos de respaldo después de una caída para <i>vi</i> o <i>ex</i> .
<i>/var/run</i>	Archivos relevantes a programas corriendo.
<i>/var/spool</i>	Colas de trabajos para realizar mas tarde.
<i>/var/spool/at</i>	Archivos creados por comando <i>at</i> .
<i>/var/spool/cron</i>	Archivos creados por comando <i>crontab</i> .
<i>/var/spool/lpd</i>	Archivos de impresora.
<i>/var/spool/mail</i>	Archivos de correo de cada usuario.
<i>/var/spool/mqueue</i>	Archivos de correo de salida.
<i>/var/spool/news</i>	Archivos de noticias de salida.
<i>/var/spool/smail</i>	Archivos de correo de <i>smail</i> .

<i>/var/tmp</i>	Temporal.
-----------------	-----------

Subdirectorios de var

## E.2 Permisos

Linux, como cualquier sistema Unix, es multiusuario, por lo que, los permisos de los archivos están orientados a dicho sistema. Los permisos de cualquier archivo tienen tres partes: permisos del propietario, permisos del grupo y permisos del resto. Así, se ve que un archivo pertenece a un determinado propietario y a un determinado grupo y, dependiendo de los permisos que tenga asociado dicho archivo, se podrá tener acceso a él o no.

Los permisos son de lectura (r), escritura (w) y ejecución (x). Estos se definen mediante letras (parecido al comando *attrib* de DOS). Con el signo `+` añadimos un permiso y con el signo `-` se lo quitamos. Además, los permisos pueden ser generales o no, es decir, si se pone sería permiso de ejecución a todos, sin embargo, si se pone sólo el propietario podría ejecutarlo. De este modo, se tiene: para propietario, para grupo y para el resto.

Ejemplo: Se tiene una serie de archivos después de listar con `ls -l` el cual muestra el propietario (skina), el grupo (users) y los permisos de izquierda a derecha: propietario, grupo y el resto.

```
[]$ ls -l
-rw-r--r-- 1 skina users 17680 Nov 29 16:52 GNU-GPL.tex
-rw-r--r-- 1 skina users 2573 Nov 30 19:52 Makefile
-rw-r--r-- 1 skina users 1562 Nov 29 13:47 autorizacion.txt
-rw-r--r-- 1 skina users 461 Oct 24 21:43 biblio.tex
drwxr-xr-x 2 skina users 1024 Nov 23 01:02 bin/
-rw-r--r-- 1 skina users 949 Nov 30 19:26 creditos.tex
-rw-r--r-- 1 skina users 550 Nov 30 19:48 curso_linux.tex
drwxr-xr-x 2 skina users 3072 Nov 30 22:55 images/
drwxr-xr-x 3 skina users 1024 Nov 30 00:09 install/
```

```

-rw-r--r-- 1 skina users 61566 Oct 26 22:29
lista_paquetes_mdk.tex
-rw-r--r-- 1 skina users 53227 Nov 23 01:08
lista_paquetes_rh.tex
-rw-r--r-- 1 skina users 3864 Nov 30 19:56 partel.tex
parte3_sistemas_archivos.tex
[]$

```

Estos permisos llevan "asociado" un número: el cuatro para lectura, el dos para la escritura y el uno para la ejecución. De esta manera, un archivo tiene tres números asignados: propietario, grupo y resto. Por ejemplo, si tenemos un fichero con los permisos 644 correspondería a: el propietario puede leer/escribir, el grupo sólo puede leer y el resto sólo puede leer. Vemos que, para asignar lectura y escritura, basta con sumar  $lectura(4)+escritura(2)$ .

El comando para modificar los permisos es `chmod` y tiene la siguiente sintaxis: `chmod permisos archivo(s)`. Por ejemplo se desea que todas las personas puedan ver escribir sobre el archivo `creditos.tex`, entonces

```

chmod a+w creditos.tex
o su equivalente en números
chmod 666 creditos.tex

```

### E.3 Montaje de un sistema de archivos

Linux accede a los dispositivos mediante archivos (directorios de `/dev`), y, por este motivo, en Linux no hay el concepto de unidades, ya que todo está bajo el directorio principal. En Linux no se accede a la primera disquetera mediante la orden

A: como en DOS sino que hay que "montarla".

De este modo, tenemos dos conceptos nuevos:

### “montar”

Decirle a Linux que se va a utilizar un determinado dispositivo con un determinado sistema de archivos y estará en un directorio especificado. En la siguiente tabla se muestran los sistemas de archivos más comunes en Linux.

Tipo	Descripción
<i>ext2</i>	Sistema de archivos de Linux.
<i>msdos</i>	Sistema de archivos de DOS.
<i>vfat</i>	Sistema de archivos de Windows 9X (nombres largos).
<i>iso9660</i>	Sistema de archivos de CD-ROM.
<i>nfs</i>	Sistema de archivos compartido por red (“exportado”).

Sistemas de archivos más comunes

### “desmontar”

Decirle a Linux que se ha dejado de utilizar un determinado dispositivo.

Para “montar” un determinado sistema de archivos de un dispositivo, se utiliza el comando *mount*. La sintaxis es la siguiente:

```
mount -t sistema_archivos dispositivo directorio [-o opciones]
```

Donde: *sistema\_archivos* puede ser cualquiera de los que aparece en la tabla anterior; *dispositivo* puede ser cualquier dispositivo del directorio */dev* o, en el caso de *nfs*, un directorio de otro ordenador; *directorio* es el directorio donde estará el contenido del dispositivo y *opciones* pueden ser cualquiera de la tabla siguiente, en el caso de no poner ninguna opción, *mount*

utilizará las opciones por defecto. Una vez ``montado" el dispositivo, si no se va a volver utilizar se puede ``desmontarlo" con el comando *umount* con la siguiente sintaxis:

```
umount directorio
```

Siempre, después de utilizar un dispositivo hay que ``desmontarlo", para que se almacenen correctamente los datos en dicho dispositivo. Un ejemplo de ello, es el hecho de que, un lector de CD-ROM, que haya sido ``montado", no se abrirá hasta que no se ``desmunte"

Opción	Descripción
<i>rw</i>	Lectura/escritura.
<i>ro</i>	Sólo lectura.
<i>exec</i>	Se permite ejecución.
<i>user</i>	Los usuarios pueden ``montar"/``desmontar".
<i>suid</i>	Tiene efecto los identificadores de propietario y del grupo.
<i>auto</i>	Se puede montar automáticamente.
<i>async</i>	Modo asíncrono.
<i>sync</i>	Modo síncrono.
<i>dev</i>	Supone que es un dispositivo de caracteres o bloques.

Opciones del comando *mount*

Ejemplos:

1. Disquete de DOS:

```
mount -t msdos /dev/fd0 /mnt/floppy
-o rw,noexec umount /mnt/floppy
```

2. Disquete de Windows 9X:

```
mount -t vfat /dev/fd0 /mnt/floppy
-o user,rw umount /mnt/floppy
```

### 3. CD-ROM:

```
mount -t iso9660 /dev/cdrom
/mnt/cdrom -o ro umount
/mnt/cdrom
```

### 4. Directorio exportado de host2:

```
mount -t nfs host2:/tmp
/mnt/host2 umount
/mnt/host2
```

### ***/etc/fstab***

En ocasiones, cuando se tienen varios dispositivos que se suelen "montar", se puede ahorrar tener que escribir continuamente la oportuna orden *mount*, simplemente incluyendo una línea en el archivo */etc/fstab*.

El archivo */etc/fstab* contiene líneas donde se indica qué dispositivo debe "montar", el lugar donde "montarlo", así como el sistema de archivos y las opciones (en este archivo, se pueden poner dos opciones más: *auto* y *noauto*, que indican si se debe "montar" automáticamente al arrancar el sistema o no, respectivamente).

Un ejemplo de */etc/fstab* puede ser:

```
Dispositivo Directorio FS Opciones
/dev/hda1 / ext2 defaults 1 1
/dev/hda2 /home ext2 defaults 1 2
/dev/hda3 /tmp ext2 defaults,noexec
```

```

/dev/hda4 none swap defaults
none /proc proc defaults
/dev/fd0 /mnt/floppy ext2 noauto,user,noexec,rw
/dev/fd0 /mnt/msdos vfat noauto,user,noexec,rw
/dev/cdrom /mnt/cdrom iso9660 noauto,user,noexec,ro

/dev/sda4 /mnt/iomegazip vfat noauto,user,noexec,rw
host2:/tmp /mnt/host2 nfs defaults

```

Con un archivo */etc/fstab* como el anterior, cualquier usuario podría hacer:

```

$ mount /mnt/msdos+
$ umount /mnt/msdos+

```

Para "montar" y "desmontar" un disquete, respectivamente. Sin embargo, sólo el administrador podría "montar" y "desmontar" el directorio */mnt/host2*

#### E.4 Uso de mtools

El hecho de tener que "montar" y "desmontar" puede ser un poco engorroso a la hora de utilizar determinados dispositivos (comúnmente, la disquetera). Por ello, se dispone de herramientas como *mtools* (ver tabla siguiente). Dichas herramientas, utilizan los dispositivos sin tener que "montar" y "desmontar"; y su sintaxis es parecida a la de los programas de DOS.

Comando	Descripción
<i>mdir</i>	Muestra el contenido del dispositivo <i>dir</i> .
<i>mcopy</i>	Copia archivos <i>copy</i> .
<i>mdel</i>	Borra archivos <i>del</i> .
<i>mformat</i>	Formatea la unidad <i>format</i> .

mcd	Cambia de directorio <i>cd</i> .
mmd	Crea un directorio <i>md</i> .
mrd	Borra un directorio <i>rd</i> .

Herramientas *mtools*

## 2.2.2 CENTRO DE TECNOLOGÍA DE INFORMACIÓN O CENTRO DE PROCESAMIENTO DE DATOS.

Se denomina **centro de procesamiento de datos** (CPD) a aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización. También se conoce como *centro de cómputo* o **centro de datos** por su equivalente en inglés *data center*.

Dichos recursos consisten esencialmente en unas dependencias debidamente acondicionadas, computadoras y redes de comunicaciones.

### 2.2.2 Centro de Tecnología de Información - Data Center- Clasificación

#### A. Según la forma de procesamiento son:

**Centralizados:** Aquellos que poseen un núcleo que comanda todos los demás, sin la activación de este los demás nodos no pueden efectuar ningún proceso.

**Descentralizados:** Aquellos en que el mando no depende de un solo núcleo, ya que se encuentre dividido en varios subsistemas. Además posee subsistemas de reserva que funcionan en caso que estos subsistemas de mando no funcionen.

**Mixtos o distribuidos:** Aquellos en que se juntan de los dos anteriores, los procesos se ejecutan de manera centralizada o descentralizada dependiendo de que se crea más conveniente.

Centralizados	Descentralizados
<ol style="list-style-type: none"> <li>1. Mayor tendencia a la especialización.</li> <li>2. Mayor dependencia técnica hacia el centro.</li> <li>3. Se procesan grandes volúmenes de información.</li> <li>4. Hay mayor gasto en cuanto a recursos humanos.</li> <li>5. Tiempo de respuesta al usuario es lento.</li> <li>6. Menos recursos de equipamiento.</li> </ol>	<ol style="list-style-type: none"> <li>1. Personal especializado reducido.</li> <li>2. Acceso inmediato a la información.</li> <li>3. Mayor dependencia del usuario en el uso del sistema en manejo de recursos.</li> <li>4. Tendencia a tener problemas técnicos específicos.</li> <li>5. Se pierde el control de las aplicaciones</li> <li>6. Hay mayor gasto en cuanto a recursos materiales.</li> </ol>

**B. Según el nivel de disponibilidad:**

El diseño de centros de datos no siempre siguió estándares establecidos, recién en Abril de 2005, la TIA (Telecommunications Industry Association)

lanzó el primer estándar que apuntaba a la infraestructura del centro de dato, el TIA-942 (o ANSI/TIA-942), que cubría cuestiones como el espacio físico y el trazado, la infraestructura de cableado, la confiabilidad en capas y las consideraciones ambientales. La norma establece capas (o tiers) para caracterizar los distintos tipos de datacenters

No hay un requerimiento mínimo para un datacenter, el Tier 1 realmente puede ser muy básico: un par de racks, una UPS, un aire acondicionado y cableado. En los niveles superiores empiezan los requerimientos.

**Tier 1: Centro de datos Básico: Disponibilidad del 99,671%.**

- El servicio puede interrumpirse por actividades planeadas o no planeadas.
- No hay componentes redundantes en la distribución eléctrica y de refrigeración.
- Puede o no puede tener suelos elevados, generadores auxiliares o UPS.
- Tiempo medio de implementación, 3 meses
- La infraestructura del datacenter deberá apagarse para realizar mantenimiento preventivo.

**Tier 2: Centro de datos con Componentes Redundantes:  
Disponibilidad del 99,741%.**

- Menos susceptible a interrupciones por actividades planeadas o no planeadas.
- Componentes redundantes (N+1).
- Tiene suelos elevados, generadores auxiliares y UPS.
- Conectados a una única línea de distribución eléctrica y de refrigeración.
- Se implementa en 3 a 6 meses.

- El mantenimiento relacionado con la alimentación o de otras partes de la infraestructura requiere una interrupción de las servicio.

**Tier 3: Centro de datos Concurrentemente Mantenibles: Disponibilidad del 99,982%.**

- Permite planificar actividades de mantenimiento sin afectar al servicio de computación, pero eventos no planeados pueden causar paradas no planificadas.
- Componentes redundantes (N+1).
- Conectados a múltiples líneas de distribución eléctrica y de refrigeración, pero únicamente con una activa.
- Incluye piso elevado y suficiente capacidad y distribución para soportar carga en una línea mientras se realiza mantenimiento en la otra.
- Downtime anual de 1,6 horas.
- De 15 a 20 meses para implementar.

**Tier 4: Centro de datos Tolerante a Fallos: Disponibilidad del 99,995%.**

- Permite planificar actividades de mantenimiento sin afectar al servicio de computación críticos, y es capaz de soportar por lo menos un evento no Planificado del tipo 'peor escenario' sin impacto crítico en la carga.
- Conectados múltiples líneas de distribución eléctrica y de refrigeración con múltiples componentes redundantes  $2(N+1)$ , que significa, por ejemplo 2 UPS con redundancia N+1.
- Downtime anual de 0,4 horas.

- De 15 a 20 meses para implementar.

Además de TIA y ANSI (American National Standards Institute), existen otras insituciones que dictan normas para centros de datos, como EIA (Energy Information Administration), NFPA (National Fire Protection Association), USGBC (U.S. Green Building Council), RoHS (Restriction of Hazardous Substances), ASHRAE (American Society of Heating, Refrigerating and Air Conditioning Engineers), IRAM (Instituto Argentino de Normalización y Certificación), IEC (International Electrotechnical Comisión), IEEE (Institute of Electrical and Electronic Engineers) y CENELEC (Comité Europé de Normalisation Electrotechnique), BICSI (Building Industry Consulting Service International), entre otras. Una sumamente respetada es el Uptime Institute.

### **C Según su ubicación:**

1. **Corporativos:** Aquellos que alojan los servidores y equipos de comunicación de una organización.
2. **Hosting :** Aquellos que alojan a servidores de terceros.

### **2.2.2.1 CTIs Centralizados a Distribuidos**

#### **A Grillas computacionales**

¿Qué es una grid computing? De acuerdo con IBM : " La computación grid es un acercamiento a la computación distribuida que abarca no sólo los lugares sino también las organizaciones, las arquitecturas de máquinas y los límites de software para proporcionar un poder ilimitado, la colaboración y el acceso a la información a todo el mundo conectado a una red. "

Un grid computacional es una red de computadoras conectadas para llevar a cabo la computación grid. En una red computacional, una tarea computacional grande se divide entre las distintas máquinas, que se ejecutan los cálculos en paralelo y luego devolver los resultados al equipo original. Estas máquinas individuales son nodos de una red, que puede abarcar múltiples dominios administrativos y pueden estar geográficamente distantes. Cada uno de los nodos puede ser considerado como un sistema discreto que puede realizar el trabajo y tiene acceso a una red. Redes computacionales son a menudo más rentable que los superordenadores de potencia de cálculo equivalente.

## **B Cloud Computing**

### **Comienzos**

El concepto de la computación en la nube empezó en proveedores de servicio de Internet a gran escala, como Google, Amazon AWS, Microsoft, y otros que construyeron su propia infraestructura. De entre todos ellos emergió una arquitectura: un sistema de recursos distribuidos horizontalmente, introducidos como servicios virtuales de TI escalados masivamente y manejados como recursos configurados y mancomunados de manera continua. Este modelo de arquitectura fue inmortalizado por George Gilder<sup>5</sup>. Las granjas de servidores, sobre las que escribió Gilder, eran similares en su arquitectura al procesamiento "grid" (red, parrilla), pero mientras que las grillas, redes se utilizan para aplicaciones de procesamiento técnico débilmente acoplados (loosely coupled), un sistema compuesto de subsistemas con cierta autonomía de acción, que mantienen una interrelación continua entre ellos), este nuevo modelo de nube se estaba aplicando a los servicios de Internet.

---

<sup>5</sup> Artículo: "Las fábricas de información" de octubre 2006 en la revista Wired.

En este tipo de computación todo lo que puede ofrecer un sistema informático se ofrece como servicio, de modo que los usuarios puedan acceder a los servicios disponibles "en la nube de Internet" sin conocimientos (o, al menos sin ser expertos) en la gestión de los recursos que usan. Según el IEEE Computer Society, es un paradigma en el que la información se almacena de manera permanente en servidores de Internet y se envía a cachés temporales de cliente, lo que incluye equipos de escritorio, centros de ocio, portátiles, etc.

"Cloud computing" es un nuevo modelo de prestación de servicios de negocio y tecnología, permite al usuario acceder a un catálogo de servicios estandarizados y cubrir las necesidades del negocio, de forma flexible y adaptativa, en caso de demandas no previsibles o de picos de trabajo, pagando únicamente por el consumo efectuado.

El cambio paradigmático que ofrece computación en nube es que permite aumentar el número de servicios basados en la red. Esto genera beneficios tanto para los proveedores, que pueden ofrecer un mayor número de servicios de forma más rápida y eficiente, como para los usuarios que tienen la posibilidad de acceder a ellos, disfrutando de la 'transparencia' e inmediatez del sistema y de un modelo de pago por consumo.

### **¿Qué es Cloud Computing?**

Es una forma computación compartida, donde los requerimientos informáticos se prestan cómo un servicio.

Normalmente, estos servicios están localizados en los centros de datos (Cloud o nubes), permitiendo el acceso a los servicios sin necesidad de contar localmente con la infraestructura requerida (poder de cómputo,

capacidad de almacenamiento, etc.), y, normalmente, también sin requerir que el usuario tenga el conocimiento o la experiencia para utilizar estos servicios.

El Cloud Computing (también conocido -y a veces confundido- con los nombres de grid computing, utility computing, computing on-demand o en español "Nube de cómputo") es un término del cual se ha estado hablando por más de 10 años, pero es ahora cuando está tomando mayor fuerza.

En una de sus formas, se trata de un concepto general que incorpora al software como un servicio, por ejemplo muchos servicios Web 2.0 usan esta tendencia, y el Web 3.0 la potenciará aún más. En estos casos, lo único que necesitan los usuarios para poder acceder al servicio es una conexión a internet. Un ejemplo muy claro es Google Apps que proporciona aplicaciones de negocios en línea a las que se accede desde un navegador web, mientras que el software y los datos se almacenan en los servidores de Google.

"Cloud Computing estaría cambiando en "commodities" ciertos servicios informáticos para el usuario"<sup>6</sup>. Es decir, que para contar con muchos de estos servicios no será necesario poseer localmente los equipos y software requeridos, pudiendo recibirlos en línea, ya sea pagando por la cantidad que usamos (como la electricidad) o de forma gratuita (como muchos servicios que ofrecen actualmente Google, MSN, etc.).

---

<sup>6</sup> "The Big Switch" - Nicholas Carr

Algunos consideran que Cloud Computing es un concepto que aplica igualmente en LAN como en WAN, pero otros asumen que solo se refiere a su uso en el ámbito de la internet.

La Computación Nube es una tecnología que permite ofrecer servicios de computación a través de Internet. En este tipo de computación todo lo que puede ofrecer un sistema informático se ofrece como servicio, de modo que los usuarios puedan acceder a los servicios disponibles "en la nube de Internet" sin conocimientos (o, al menos sin ser expertos) en la gestión de los recursos que usan.

La Computación Nube es un concepto general que incorpora el software como servicio, tal como la Web 2.0 y otros recientes, también conocidos como tendencias tecnológicas, donde el tema en común es la confianza sobre el Internet para satisfacer las necesidades de cómputo de los usuarios. Por ejemplo, Google Apps provee aplicaciones comunes de negocios en línea que son accesadas desde un navegador web, mientras el software y los datos son almacenados en los servidores.

### **Beneficios**

- Integración probada de servicios Red. Por su naturaleza, la tecnología de "Cloud Computing" se puede integrar con mucha mayor facilidad y rapidez con el resto de sus aplicaciones empresariales (tanto software tradicional como Cloud Computing basado en infraestructuras), ya sean desarrolladas de manera interna o externa.
- Prestación de servicios a nivel mundial. Las infraestructuras de "Cloud Computing" proporcionan mayor capacidad de adaptación, recuperación de desastres completa y reducción al mínimo de los tiempos de inactividad.

## **Ventajas y Desventajas**

### **Ventajas:**

⚡ Aumente y reduzca la capacidad según se precise, sin necesidad de tener que adquirir todos los recursos que se necesitarían cuando la demanda está en su punto álgido.

⚡ Acceso a capacidad durante períodos breves sin necesidad de grandes inversiones de capital.

⚡ Reduce los gastos que implica construir una infraestructura de gran tamaño para un futuro incierto y mantener infraestructuras redundantes.

⚡ Transición a un papel de proveedor de servicios interno. Capacidad de generar informes que permitan distribuir mejor los gastos de los servicios de TI compartidos, con el respaldo de acuerdos de nivel de servicio.

### **Desventajas:**

La centralización de las aplicaciones y el almacenamiento de los datos origina una interdependencia de los proveedores de servicios.

La disponibilidad de las aplicaciones está ligada a la disponibilidad de acceso a Internet.

Los datos "sensibles" del negocio no residen en las instalaciones de las empresas por lo que podría generar un contexto de alta vulnerabilidad para la sustracción o robo de información.

La confiabilidad de los servicios depende de la "salud" tecnológica y Financiera de los proveedores de servicios en nube. Empresas

emergentes o alianzas entre empresas podrían crear un ambiente propicio para el monopolio y el crecimiento exagerado en los servicios.

La disponibilidad de servicios altamente especializados podría tardar meses o incluso años para que sean factibles de ser desplegados en la red.

La madurez funcional de las aplicaciones hace que continuamente estén modificando sus interfaces, por lo cual la curva de aprendizaje en empresas de orientación no tecnológica tenga unas pendientes significativas, así como su consumo automático por aplicaciones.

Seguridad. La información de la empresa debe recorrer diferentes nodos para llegar a su destino, cada uno de ellos (y sus canales) son un foco de inseguridad. Si se utilizan protocolos seguros, HTTPS por ejemplo, la velocidad total disminuye debido a la sobrecarga que estos requieren.

Escalabilidad a largo plazo. A medida que más usuarios empiecen a compartir la infraestructura de la nube, la sobrecarga en los servidores de los proveedores aumentará, si la empresa no posee un esquema de crecimiento óptimo puede llevar a degradaciones en el servicio o jitter altos.

### **Tipos de nubes**

- Las nubes públicas se manejan por terceras partes, y los trabajos de muchos clientes diferentes pueden estar mezclados en los servidores, los sistemas de almacenamiento y otras infraestructuras de la nube. Los usuarios finales no conocen qué trabajos de otros clientes pueden estar corriendo en el mismo servidor, red, discos como los suyos propios.

- Las nubes privadas son una buena opción para las compañías que necesitan alta protección de datos y ediciones a nivel de servicio. Las nubes privadas están en una infraestructura en-demanda manejada por un solo cliente que controla qué aplicaciones debe correr y dónde. Son propietarios del servidor, red, y disco y pueden decidir qué usuarios están autorizados a utilizar la infraestructura.
- Las nubes híbridas combinan los modelos de nubes públicas y privadas. Usted es propietario de unas partes y comparte otras, aunque de una manera controlada. Las nubes híbridas ofrecen la promesa del escalado aprovisionada externamente, en-demanda, pero añaden la complejidad de determinar cómo distribuir las aplicaciones a través de estos ambientes diferentes. Las empresas pueden sentir cierta atracción por la promesa de una nube híbrida, pero esta opción, al menos inicialmente, estará probablemente reservada a aplicaciones simples sin condicionantes, que no requieran de ninguna sincronización o necesiten bases de datos complejas.

Richard Stallman, fundador de la Free Software Foundation, cree que la computación en nube pone en peligro las libertades de los usuarios, porque éstos dejan su privacidad y datos personales en manos de terceros. Ha afirmado que la computación en nube es "simplemente una trampa destinada a obligar a más gente a adquirir sistemas propietarios, bloqueados, que les costarán más y más conforme pase el tiempo."

Se podría resumir que el cloud computing es la capacidad de consumir servicios IT de forma ágil y flexible. Podríamos considerar servicio a todo aquello que realice IT y que se pueda empaquetar para ser consumido por distintos tipos de clientes o usuarios. Para que un servicio se pueda considerar como Cloud Computing debe cumplir con las siguientes afirmaciones:

- ✦ Pago por uso
- ✦ Debe permitir agregar o decrementar recursos de forma sencilla y rápida.
- ✦ Debe ser escalable
- ✦ Debe proporcionar herramientas de autoservicio al usuario.

### **Pago por uso**

Este es el principal atractivo ya que el usuario solo tendrá que abonar los recursos que haya consumido con su servicio, ahorrando así en implantaciones on-premise y reduciendo el riesgo inicial de los proyectos.

### **Flexibilidad en recursos**

Consiste en la capacidad de poder agregar o disminuir nuevos recursos o los que tuviéramos ya disponibles en nuestro servicio. Un ejemplo sería el de poder aumentar o reducir la RAM utilizada por nuestro aplicativo web.

### **Escalabilidad**

Los proveedores de Cloud computing deben proporcionar plataformas que permitan aumentar el número de instancias del servicio para poder responder a una mayor demanda de usuarios o peticiones.

Además debe permitir mecanismo para mover el servicio entre los distintos servidores y los distintos centros de datos que disponga el proveedor.

## **Herramientas de autoservicio**

Se deben proporcionar herramientas que permitan al propio usuario (o un responsable) contratar los servicios que desea consumir y ajustar los recursos destinados a esos servicios.

En una primera aproximación se podría pensar que el Cloud computing es algo similar que un hosting, pero estaríamos equivocados por varios motivos:

- El hosting se paga por cuotas de recursos y no por uso.
- El hosting no permite modificar los recursos disponibles de forma sencilla y automatizada.
- No todos los Hosters permiten funcionalidades de escalado.

En definitiva se podría decir que un hosting es un subconjunto del Cloud computing o que el cloud computing es una evolución del hosting.

Los distintos servicios que se pueden ofrecer en modo Cloud computing se agrupan en: IaaS (Infraestructura como servicio), PaaS (Plataforma como servicio) y SaaS (Software como servicio).

- El IaaS ofrece a los usuarios la posibilidad de utilizar distintos tipos de infraestructura como un servicio. Por ejemplo Amazon EC2 permite crear instancias de máquinas virtuales pudiendo ajustar la memoria RAM, el tamaño de los discos, el SO.
- El PaaS proporciona características adicionales al IaaS como pueden ser: despliegue automatizado de aplicaciones, sistemas de gestión de autenticación, sistemas de comunicación de colas o mensajes, sistemas

de monitorización, Un ejemplo podría ser el rol web de Azure que permite desplegar una aplicación web

sin necesidad de configurar el SO ni el IIS y sin necesidad de conocer las máquinas desde donde se ejecutan la aplicación.

- El SaaS permite utilizar como servicio un software existente sin realizar instalaciones ni configuraciones. Como ejemplo: CRM Online es una versión del CRM de Microsoft en modo cloud computing con el que los clientes contratan desde una web el número de usuarios y en unos instantes disponen de la funcionalidad de CRM sin realizar ninguna instalación.

### **Para quién está pensado el Cloud computing**

Se podría decir que el cloud computing no está pensado para un tipo de cliente específico sino para un tipo de proyecto o aplicativo que quiera aprovecharse de las características que se han mencionado anteriormente. Las pequeñas empresas por ejemplo podrán utilizar aplicativos sin necesidad de adquirir una infraestructura que le supondría un coste muy alto en hardware, licencias y mantenimiento.

Las grandes o medianas empresas pueden adquirir una flexibilidad a la hora de desplegar servicios que les permitirán ser más competitivos y podrán ahorrar en costes en IT.

El cloud computing no vale para todas las soluciones, pero si es una opción a tener en cuenta que habrá que plantearse en aquellos escenarios en los que necesitemos de las prestaciones del cloud computing.

## **Cloud Computing es un ahorro en costes en IT**

El poder disponer de un servicio en cualquier momento sin necesidad de provisionar nuevas infraestructuras y de pagar por su uso, permite a las empresas plantear soluciones más escalables, con menor mantenimiento por parte del departamento de IT y con un menor coste en infraestructuras y licencias.

Con el Cloud Computing se puede abordar nuevos tipos de proyectos y reducir el coste en infraestructuras, licencias y mantenimiento, siendo más ágiles a la hora de crear nuevos servicios y más competitivos a la hora de plantear soluciones.

El Cloud computing se encuentra en una de sus primeras fases que dará paso en breve a su siguiente generación de nubes y servicios. El ritmo al que avanzan los proveedores de Cloud Computing es muy superior al de nuestros negocios o Infraestructuras, cuanto antes abordemos este tipo de servicios más rápidos podremos adaptarnos a las futuras versiones.

Esperar dos años para empezar a virtualizar nuestros entornos o calcular el coste de nuestras infraestructuras puede hacer que cuando queramos abordarlo nuestros competidos ya lo hayan hecho mucho antes y tengan muchas más experiencia que nosotros.

### **2.2.2.2 Niveles de disponibilidad de un Data Center - Norma ANSI/TIA 942 ORGANIZACION REGULATORIA -UPTIME INSTITUTE<sup>7</sup>**

Consortio de empresas que le ayuda a sus miembros a evitar tiempos caídos (downtime); optimizar la inversión de infraestructura del sitio y obtener un nivel de profesionalismo más alto en operaciones y

---

<sup>7</sup> <http://www.upsite.com/TUIpages/tuihome.html>

prácticas para asegurar el funcionamiento continuo (uptime) de sus instalaciones.

- ⊙ El Uptime Institute ha definido un sistema de clasificación y certificación de centros de datos basado en cuatro niveles (TIERS).
- ⊙ Conforme más alto sea el “tier”, mayor es la confiabilidad del centro de datos.
- ⊙ <http://www.uptime.com/TUIpages/tuihome.html>

⊙ Generalidades Clasificación Tier

	<b>Tier I</b>	<b>Tier II</b>	<b>Tier III</b>	<b>Tier IV</b>
<b>Downtime anual</b>	28.8 hrs	22.0 hrs	1.6 hrs	0.8 hrs
<b>Disponibilidad</b>	99.671%	99.741%	99.982%	99.995%

**Clasificación de tiers**

Manera de describir: Disponibilidad, Confiabilidad, Costos, estimados de construcción y mantenimiento. Entre mayor el número más confiable el sistema

- ⊙ Clasificación Tier
  - Tier I: Infraestructura básica
  - Tier II: Infraestructura con componentes redundantes
  - Tier III: Infraestructura con Mantenimiento simultáneo
  - Tier IV: Infraestructura Tolerante a Fallas

## ⊙ Tier I

### **Infraestructura Básica**

- Componentes no redundantes
- Unica vía de distribución no redundante
- Una falla en un componente o en la distribución impactará el funcionamiento de los sistemas de cómputo
- Infraestructura susceptible a interrupciones por cualquier evento planeado o no planeada

## ⊙ Aplicación

- Aplicable para negocios pequeños
- Infraestructura de TI solo para procesos internos
- Compañías hacen uso de la Web como una herramienta de mercadeo
- Compañías que basan su negocio en Internet pero que no requieren calidad en sus servicios

## ⊙ Tier II

### **Componentes Redundantes**

- Componentes redundantes
- Unica vía de distribución no redundante

- Infraestructura susceptible a interrupciones por cualquier evento planeado o no planeada
- Requiere Generador y UPS redundantes

◎ **Aplicación**

- Aplicable a negocios pequeños
- Uso de TI limitado a las horas normales de trabajo
- Compañías de software que no ofrecen servicios “online” o “real-time”
- Compañías que basan su negocio en Internet pero que no requieren calidad en sus servicios

◎ **Tier III**

**Mantenimiento simultáneo**

- Componentes redundantes
- Vías de distribución redundantes (una activa y otras pasivas)
- Los componentes pueden ser removidos durante un evento planeado sin generar interrupciones en el sistema
- Susceptible a actividades no planeadas
- Alto riesgo de interrupción durante mantenimientos

◎ **Aplicación**

- Para compañías que dan soporte 24/7 como centros de servicio y información

- Negocios donde los recursos de TI dan soporte a procesos automatizados
- Compañías que manejan múltiples zonas horarias

⊙ **Tier IV**

**Tolerante a fallas**

- ⊙ Componentes redundantes
- ⊙ Múltiples vías de distribución activas y redundantes
- ⊙ Los componentes pueden ser removidos durante un evento planeado sin generar interrupciones en el sistema
- ⊙ No susceptible a interrupciones por un evento no planeado
- ⊙ Posibles causas de interrupción: Alarma incendio, supresión de incendios o EPO (Emergency Power Off)

⊙ **Aplicación**

- Compañías con presencia en el mercado internacional
- Servicios 24x365 en un mercado altamente competitivo
- Compañías basadas en el comercio electrónico
- Acceso a procesos y transacciones Online
- Entidades financieras

⊙ **Aplicación de los TIER**

- A nivel de Arquitectura
- A nivel de Telecomunicaciones

- A nivel de Eléctrico
- A nivel de Mecánico

### ◎ **Arquitectónico**

Tier1: Sin protección eventos físicos, naturales o intencionales.

Tier2: Protección mínima a eventos críticos, Puertas de seguridad

Tier3: Acceso controlado, Muros exteriores sin ventanas, Seguridad perimetral, CCTV

Tier4: Protección desastres naturales, sismos, inundaciones, huracanes, Edificio separado, Cercanía a lugares públicos (Aeropuertos, Líneas Ferreas), Requerimientos antisísmicos según la zona,

### **Telecomunicaciones**

- Tier 1: Un solo proveedor, una sola ruta de cableado.
- Tier 2: Redundancia en equipos críticos, fuentes de poder, procesadores
- Tier 3: Dos proveedores, dos cuartos de entrada de servicio, Rutas y áreas redundantes
- Tier 4: Áreas aisladas

### ◎ **Eléctrico**

Tier 1:

- Piso falso, UPS y generador (opcionales) sin redundancia.
- Única vía de distribución
- UPS simple o paralelas por capacidad. Debe contar con bypass para mantenimiento

- PDUs y paneles de distribución utilizados para distribución de la carga
- Sistemas de tierra: requerimientos mínimos
- Monitoreo de los sistemas es opcional

#### Tier 2:

- UPS redundante N+1
- Un generador redundante
- PDUs redundantes, preferiblemente alimentados de sistemas UPS separados
- Gabinetes deben de contar con dos circuitos eléctricos dedicados de 20A/120V.
- Emergency Power Off System (EPO)

#### Tier 3:

- Al menos redundancia N+1 en el generador, UPS y sistema de distribución.
- Dos vías de distribución (una activa y otra alterna)
- Sistema de aterrizaje y sistema de protección para alumbrado.
- Sistema de Control y Monitoreo para monitorear la mayoría de los equipos eléctricos.
- Servidor redundante para asegurar monitoreo y control continuo.

#### Tier 4:

- Diseño 2(N+1)

- UPS deben contar con bypass manual para mantenimiento o falla.
- Un sistema de monitoreo de baterías.
- Data Center debe contar con una entrada de servicios dedicada, aislada de otras facilidades críticas.
- Al menos dos distribuciones de diferentes subestaciones (2 activas simultáneamente)
- Detección y transferencia automática

### © Mecánico

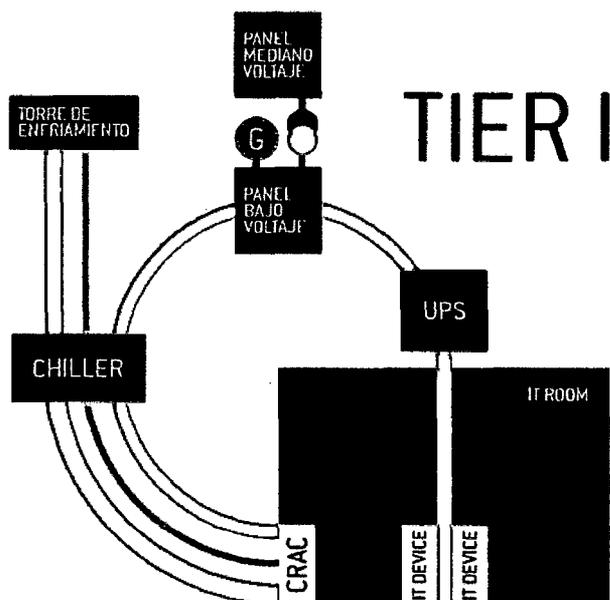
- Tier 1: Una o varias unidades de aire acondicionado sin redundancia. Tuberías con una sola ruta
- Tier 2: Capacidad de enfriamiento combinada, temperatura y humedad, 7 x 24 x 365
- Tier 3: Múltiples unidades de aire acondicionado
- Tuberías y bombas duales, Detección de derrames
- Tier 4: Soporta fallas en un tablero de alimentación, Fuentes de agua alternas

### **Instalación eléctrica Tier 1: Básica**

Una instalación eléctrica tipo Tier 1 se muestra en la figura 1 (GE es el grupo electrógeno, o gmg). La misma provee los requerimientos mínimos necesarios para un CPD. El elemento representado como CPD son los equipos críticos.

Tal como se puede observar, la instalación eléctrica prevé el uso de un grupo electrógeno (gmg) como forma de respaldo ante un corte del suministro de la energía eléctrica pública (UTE, en general, en nuestro país).

Para brindar energía durante el lapso de tiempo en que demora en encender el gmg se usa una UPS, que alimenta a su salida un PDU (Panel Distribution Unit, en inglés), o lo que es lo mismo, el tablero de distribución de las cargas críticas.



**Figura 1: esquema ilustrativo de una instalación eléctrica para un CPD Tier 1.**

De la figura se observa la alimentación eléctrica de los equipos de acondicionamiento térmico (aire acondicionado), responsable de disipar el calor generado dentro del CPD y mantener una temperatura adecuada en la sala.

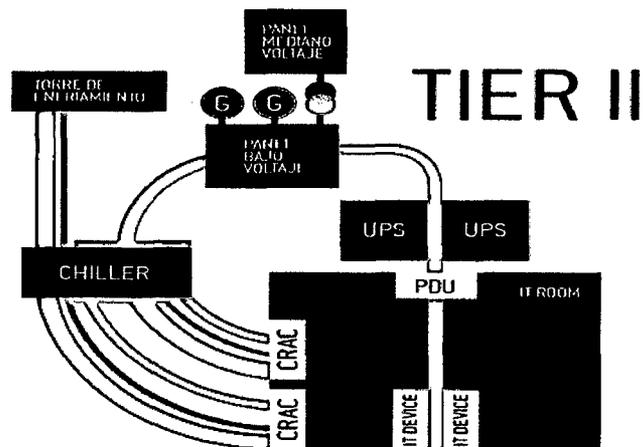
Del diagrama se observa que el desperfecto de cualquier componente (UPS, línea de distribución, o equipo de aire acondicionado) afectará el servicio del CPD.

Si es necesario realizar un trabajo programado en el tablero de salida de la UPS, o en el PDU, o en el aire acondicionado, se precisará coordinar previamente un corte de los equipos del CPD dado que estos se verán afectados (un CPD saldrá de servicio al cabo de 1 hora, aproximadamente, por alta temperatura, si su equipo de aire acondicionado no funciona).

El sistema también es susceptible ante fallas inesperadas (ejemplo: una falla de encendido del gmg cuando exista corte de la energía pública, la falla de un interruptor automático en el PDU, etc.) dado que existen varios puntos simples de falla.

### **Instalación eléctrica Tier 2: Sistema redundante**

Una instalación eléctrica nivel Tier 2 se muestra en la figura 2. Se caracteriza por poseer redundancia a nivel de los componentes principales de respaldo de energía (UPS y gmg) y en el sistema de aire acondicionado, pero la distribución de energía no es redundante (un solo camino).



**Figura 2: esquema ilustrativo de una instalación eléctrica para un CPD Tier 2**

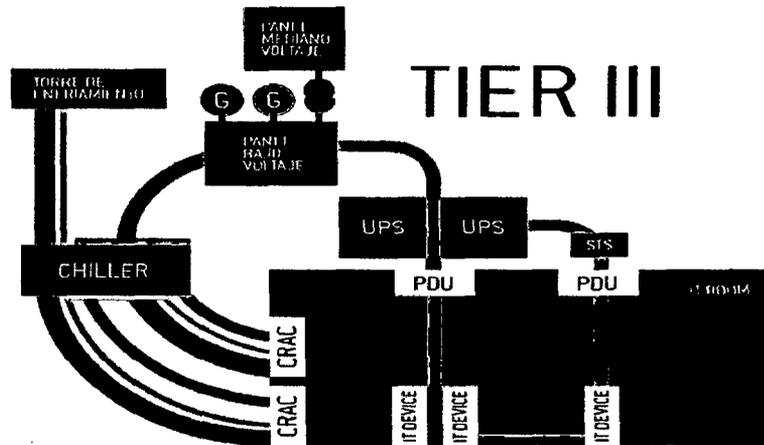
Del diagrama se observa que el desperfecto de cualquier línea de distribución de energía afectará el servicio del CPD. Si es necesario realizar un trabajo programado en el tablero de salida de UPS se precisará realizar un corte de los equipos del CPD, aunque sí se puede hacer en el tablero general (encendiendo los gmg).

El sistema también es susceptible ante fallas inesperadas, aunque menos que en un Tier1, dado que siguen existiendo varios puntos simples de falla.

### **Instalación eléctrica Tier 3: Mantenimiento con servicio**

Una instalación eléctrica nivel Tier 3 se muestra en la figura 3. Posee redundancia N+1 en los componentes de respaldo de energía, transformadores de la subestación y múltiples caminos de distribución de energía. En general, uno solo de los caminos estará activo, siendo el otro de respaldo.

La redundancia debe permitir que cualquier trabajo de mantenimiento pueda ser realizado sin afectar los equipos críticos. Todos los equipos del CPD deben admitir doble entrada de alimentación y a los que no lo admitan se les deberá alimentar a través de una llave estática de transferencia de 2 entradas y 1 salida.



**Figura 3: esquema ilustrativo de una instalación eléctrica para un CPD Tier 3.**

La norma ANSI/TIA 942 admite que en este nivel una falla inesperada afecte el servicio a los equipos críticos, pero exige que toda actividad prevista de mantenimiento pueda ser efectuada de forma segura para el operario (aislando eléctricamente la zona de trabajo) sin afectar el servicio al CPD (esto no se refleja en el diagrama de la figura 3).

Entre las muchas cosas que deben ser consideradas en este nivel, algunas son: doble batería de arranque con cargadores individuales en los gmg, autonomía en combustible de 72hs para los gmg, los sistemas de control de los equipos de refrigeración alimentados de UPS, doble banco de baterías para las UPS, doble entrada de alimentación eléctrica (aunque se admite que la misma sea una sola si procede de un sistema de media tensión en anillo).

**Instalación eléctrica Tier 4: Tolerante a fallas inesperadas**

Una instalación eléctrica nivel Tier 4 se muestra en la figura 4. Posee redundancia  $2x(N+1)$  en los componentes de respaldo de energía y múltiples caminos de distribución de energía activos. Dichos cableados



significa que si vamos a tener una subestación propia con los dos transformadores, entonces deberemos contratarle a UTE el tendido de 2 líneas exclusivas de MT desde estaciones de transformación distintas.

Con este artículo hemos querido mostrar las bases para encarar la instalación eléctrica de un centro de datos simple, hasta de uno de exigencias extremas.

### **2.2.3 Virtualización**

El término "virtualización" se viene usando desde 1960, y ha sido aplicado a diferentes aspectos y ámbitos de la informática, desde sistemas computacionales completos, hasta capacidades o componentes individuales.

Virtualización es la creación -a través de software- de una versión virtual de algún recurso tecnológico, como puede ser una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento u otros recursos de red. En los ámbitos de habla inglesa, este término se suele conocer por el numerónimo "**v11n**".

Dicho de otra manera, se refiere a la abstracción de los recursos de una computadora, llamada Hypervisor o VMM (Virtual Machine Monitor) que crea una capa de abstracción entre el hardware de la máquina física (host) y el sistema operativo de la máquina virtual (virtual machine, guest), dividiéndose el recurso en uno o más entornos de ejecución.

Esta capa de software (VMM) maneja, gestiona y arbitra los cuatro recursos principales de una computadora (CPU, Memoria,

Almacenamiento y Conexiones de Red) y así podrá repartir dinámicamente dichos recursos entre todas las máquinas virtuales definidas en el computador central. Esto hace que se puedan tener varios ordenadores virtuales ejecutándose en el mismo ordenador físico.

La virtualización se encarga de crear una interfaz externa que encapsula una implementación subyacente mediante la combinación de recursos en localizaciones físicas diferentes, o por medio de la simplificación del sistema de control. Un avanzado desarrollo de nuevas plataformas y tecnologías de virtualización ha hecho que en los últimos años se haya vuelto a prestar atención a este concepto.

La máquina virtual en general simula una plataforma de hardware autónoma incluyendo un sistema operativo completo que se ejecuta como si estuviera instalado. Típicamente varias máquinas virtuales operan en un computador central. Para que el sistema operativo "guest" funcione, la simulación debe ser lo suficientemente grande (siempre dependiendo del tipo de virtualización).

Existen diferentes formas de virtualización: es posible virtualizar el hardware de servidor, el software de servidor, virtualizar sesiones de usuario, virtualizar aplicaciones y también se pueden crear máquinas virtuales en una computadora de escritorio.

Entre los principales proveedores de software que han desarrollado tecnologías de virtualización integrales (que abarcan todas las instancias: servidor, aplicaciones, escritorio) se encuentran, por ejemplo VMware y Microsoft. Estas compañías han diseñado soluciones específicas para virtualización, como VMware Server y Windows Server 2008 Hyper-V para la virtualización de servidores. Si

bien la virtualización no es un invento reciente, con la consolidación del modelo de la Computación en la nube, la virtualización ha pasado a ser uno de los componentes fundamentales, especialmente en lo que se denomina infraestructura de nube privada.

### **Ventajas de la Virtualización**

- Reutilización de hardware existente (para utilizar software más moderno) y optimizar el aprovechamiento de todos los recursos de hardware.
- Rápida incorporación de nuevos recursos para los servidores virtualizados.
- Reducción de los costes de espacio y consumo necesario de forma proporcional al índice de consolidación logrado (Estimación media 10:1).
- Administración global centralizada y simplificada.
- Nos permite gestionar nuestro CPD como un pool de recursos o agrupación de toda la capacidad de procesamiento, memoria, red y almacenamiento disponible en nuestra infraestructura
- Mejora en los procesos de clonación y copia de sistemas: Mayor facilidad para la creación de entornos de test que permiten poner en marcha nuevas aplicaciones sin impactar a la producción, agilizando el proceso de las pruebas.
- Aislamiento: un fallo general de sistema de una máquina virtual no afecta al resto de máquinas virtuales.
- Mejora de TCO y ROI.
- No sólo aporta el beneficio directo en la reducción del hardware necesario, sino también los costes asociados.
- Reduce los tiempos de parada.

- Migración en caliente de máquinas virtuales (sin pérdida de servicio) de un servidor físico a otro, eliminando la necesidad de paradas planificadas por mantenimiento de los servidores físicos.
- Balanceo dinámico de máquinas virtuales entre los servidores físicos que componen el pool de recursos, garantizando que cada máquina virtual ejecute en el servidor físico más adecuado y proporcionando un consumo de recursos homogéneo y óptimo en toda la infraestructura.
- Contribución al medio ambiente -Green IT- por menor consumo de energía en servidores físicos.

### **Diferencias entre virtualizar un Sistema operativo e instalarlo**

Virtualizar el sistema operativo es una opción interesante si no queremos instalar dos sistemas operativos en el mismo ordenador, pero si por el contrario lo que hacemos es instalarlo, todos los sistemas operativos que tengamos instalados funcionarían de la misma manera que si estuvieran instalados en distintos ordenadores.

El único y pequeño inconveniente es que se necesita un gestor de arranque que al encender el ordenador dé la opción de elegir qué sistema operativo se quiere utilizar, lo que conlleva que si por ejemplo se está utilizando Windows y se quiere cambiar a GNU/Linux se debería reiniciar el ordenador. La virtualización por el contrario permite cambiar de sistema operativo como si se tratase de cualquier otro programa, sin embargo, esta agilidad tiene la desventaja de que un sistema operativo virtualizado no es tan potente como uno que ya estuviera instalado.

## **Retos de la Virtualización**

- **Índices de utilización más altos** — Antes de la virtualización, los índices de utilización del servidor y almacenamiento en los centros de datos de la empresa rondaban menos del 50% (de hecho, del 10% al 15% de los índices de utilización fueron los más comunes). A través de la virtualización, las cargas de trabajo pueden ser encapsuladas y transferidas a los sistemas inactivos o sin uso — lo cual significa que los sistemas existentes pueden ser consolidados, así que las compras de capacidad adicional del servidor pueden ser retrasadas o evitadas.
- **Consolidación de Recursos** — La virtualización permite la consolidación de múltiples recursos de TI. Más allá de la consolidación de almacenamiento, la virtualización proporciona una oportunidad para consolidar la arquitectura de sistemas, infraestructura de aplicación, datos y base de datos, interfaces, redes, escritorios, e incluso procesos de negocios, resultando en ahorros de costo y mayor eficiencia.
- **Uso/costo menor energía** — La electricidad requerida para que funcionen los centros de datos de clase empresarial ya no está disponible en suministros ilimitados, y el costo está en una espiral ascendente. Por cada dólar gastado en un servidor hardware, un dólar adicional es gastado en energía (incluyendo el costo de los servidores en función y los enfriadores). Utilizando virtualización para consolidar hace posible cortar el consumo total de energía y ahorrar dinero de una manera significativa.
- **Ahorros de espacio** — La extensión del servidor permanece como un serio problema en la mayoría de los centros de datos empresariales, pero la expansión del centro de datos no es siempre una opción, con los costos de construcción promediando miles de dólares por pie cuadrado. La virtualización puede aliviar la tensión mediante la

consolidación de muchos sistemas virtuales en menos sistemas físicos.

- Recuperación de desastre/continuidad del negocio — La virtualización puede incrementar la disponibilidad de los índices del nivel de servicio en general y proporcionar nuevas opciones de soluciones para la recuperación de desastre.

Costos de operación reducidos — La empresa promedio gasta \$8 dólares en mantenimiento por cada \$1 dólar invertido en nueva infraestructura. La virtualización puede cambiar el radio de servicio-a-administración reducir la carga total de trabajo administrativo, y cortar el total de costos de operación

### **2.2.3.1 Tipos de Virtualización**

La virtualización se puede hacer desde un sistema operativo Windows, ya sea XP, Vista u otra versión que sea compatible con el programa que utilicemos, en el que virtualizamos otro sistema operativo como Linux o viceversa, que tengamos instalado Linux y queramos virtualizar una versión de Windows.

#### **Infraestructura Virtual**

Una infraestructura virtual consiste en el mapping dinámico de recursos físicos en función de las necesidades de la empresa. Una máquina virtual representa los recursos físicos de un único ordenador, mientras que una infraestructura virtual representa los recursos físicos de la totalidad del entorno de TI, aglutinando ordenadores x86, así como su red y almacenamiento asociados, en un pool unificado de recursos de TI.

Estructuralmente, una infraestructura virtual consta de los siguientes componentes:

- Hipervisor de un solo nodo para hacer posible la virtualización de todos los ordenadores x86.
- Un conjunto de servicios de infraestructura de sistemas distribuida basada en la virtualización, como gestión de recursos, para optimizar los recursos disponibles entre las máquinas virtuales.
- Soluciones de automatización que proporcionen capacidades especiales para optimizar un proceso de TI concreto, como provisioning o recuperación ante desastres. Mediante la separación de la totalidad del entorno de software de su infraestructura de hardware subyacente, la virtualización hace posible la reunión de varios servidores, estructuras de almacenamiento y redes en pools compartidos de recursos que se pueden asignar de forma dinámica, segura y fiable a las aplicaciones según sea necesario. Este enfoque innovador permite a las organizaciones crear una infraestructura informática con altos niveles de utilización, disponibilidad, automatización y flexibilidad utilizando componentes básicos de servidores económicos y estándar del sector.

### **Virtualización por (Hardware)**

Virtualización asistida por Hardware son extensiones introducidas en la arquitectura de procesador x86 para facilitar las tareas de virtualización al software ejecutándose sobre el sistema. Si cuatro son los niveles de privilegio o anillos de ejecución en esta arquitectura, desde el cero o de mayor privilegio, que se destina a las operaciones del kernel de SO, al tres, con privilegios menores que es el utilizado por los procesos de usuario, en esta nueva arquitectura se introduce un anillo interior o ring - 1 que será el que un hypervisor o Virtual Machine Monitor usará para aislar todas las capas superiores de software de las operaciones de virtualización.

## **La virtualización de almacenamiento**

Se refiere al proceso de abstraer el almacenamiento lógico del almacenamiento físico, y es comúnmente usado en SANs ("Storage Area Network" Red de área de almacenamiento). Los recursos de almacenamiento físicos son agregados al "storage pool" (almacén de almacenamiento), del cual es creado el almacenamiento lógico.

## **Particionamiento**

Es la división de un solo recurso (casi siempre grande), como en espacio de disco o ancho de banda de la red, en un número más pequeño y con recursos del mismo tipo que son más fáciles de utilizar. Esto es muchas veces llamado "zoning", especialmente en almacenamiento de red.

## **Máquina virtual**

Es un sistema de virtualización, denominado "virtualización de servidores", que dependiendo de la función que esta deba de desempeñar en la organización, todas ellas dependen del hardware y dispositivos físicos, pero casi siempre trabajan como modelos totalmente independientes de este. Cada una de ellas con sus propias CPUs virtuales, tarjetas de red, discos etc. Lo cual podría especificarse como una compartición de recursos locales físicos entre varios dispositivos virtuales.

## **Hypervisor de almacenamiento**

Es un pack portátil de gestión centralizada, utilizado para mejorar el valor combinado de los sistemas de disco de almacenamiento múltiples, incluyendo los modelos diferentes e incompatibles, complementando sus capacidades individuales con el aprovisionamiento extendido, la réplica y

la aceleración del rendimiento del servicio. Su completo conjunto de funciones de control y monitorización del almacenamiento, operan como una capa virtual transparente entre los pools de disco consolidados para mejorar su disponibilidad, velocidad y utilización.

### **Virtualización relacionada con el Green IT**

En estudios realizados, basados en el ahorro de energía que genera la empresa para sus clientes, muestra que las soluciones de virtualización reducen los costos económicos y emisiones de CO<sub>2</sub>.

Esto se puede llevar acabo fusionando varias máquinas en un solo servidor, con lo que disminuyendo el consumo energético y los costos; ahorrando 7.000 kilovatios hora o cuatro toneladas de emisiones de CO<sub>2</sub> al año. Los PCs virtualizados pueden reducir el consumo de energía y los costos en un 35 por ciento. hoy en día, la mayor parte consumen entre un 70 y un 80% de su energía estimada. Otra medida es la desconexión de los servidores y desktops durante los períodos de inactividad, como por la noche o los fines de semana, con lo que se puede ahorrar aproximadamente un 25 por ciento en su consumo energético. Las empresas hoy en día son las más interesadas en el tema de la virtualización, ya que para ellas es muy importante reducir costos y energía principalmente.

#### **2.2.3.2 Aplicaciones para Virtualización**

Ejecutar 2 o más Sistemas Operativos en un mismo equipo es ya algo habitual. Como usuarios de GNU/Linux se encontra a disposición abundante información sobre el uso de aplicaciones de virtualización como, por ejemplo, VirtualBox o VMware. Sin embargo, existen otras

opciones en este campo de las que, con GNU/Linux como sistema anfitrión, podemos sacar ventaja y elegir de acuerdo a las necesidades y/o gustos. Entre estas opciones se tiene: VirtualBox y VMware, KVM, Qemu, OpenVZ, Linux-VServer y Xen.

## **VirtualBox**

Se trata, probablemente, de la aplicación más utilizada a nivel de escritorio. Resulta sencilla de utilizar y cuenta con una interfaz de configuración fácil de entender y usar, incluso para no expertos.

La compañía que está detrás de VirtualBox es Oracle, una de las mayores compañías de software del mundo.

Esta aplicación ofrece soporte tanto para plataforma de 32 como 64 bits, tanto en sistema anfitrión como cliente. Se encuentra disponible para descarga la opción OSE (*Open Source Edition*) y la opción gratuita, bajo licencia *Personal Use and Evaluation License*.

Como sistema anfitrión, VirtualBox está disponible para GNU/Linux, Mac OS X y Windows. Como cliente, ofrece soporte para sistemas GNU/Linux, Solaris, Windows, OpenSolaris, DOS, OS/2, \*BSD, QNX, Haiku y ReactOS.

Con VB se puede emplear los puertos paralelos, serie y usb del equipo, así como usar imágenes de otras aplicaciones de virtualización como VMware y compartir directorios entre el sistema cliente y servidor. Además, tiene soporte para aceleración 3D.

Se encuentra VB en los repositorios de numerosas distribuciones.

Homesite: [virtualbox.org](http://virtualbox.org).

## **VMware Player**

Otra de las opciones muy utilizadas en este campo. Tanto VMware Player como VMware Server se ofrece para descarga gratuitamente.

Ofrece soporte, tanto en SO cliente como servidor, para plataforma de 32 y 64 bits. Los sistemas clientes pueden ser GNU/Linux, Windows, Solaris, OpenSolaris, DOS, OS/2, \*BSD, QNX, Haiku y ReactOS. Al igual que VirtualBox, pueden usarse los puertos paralelo, usb y serie, tiene soporte para aceleración 3D y puede compartir carpetas con el sistema anfitrión.

Homesite: [vmware.com](http://vmware.com).

## **QEMU**

Se trata de una opción libre que, a diferencia de los anteriores, no dispone de una interfaz gráfica por defecto con las opciones de configuración. Sin embargo, para los usuarios de GNU/Linux se dispone de la opción de instalar Qemu launcher para acceder a una interfaz básica del programa.

Ofrece soporte tanto para plataforma x86 como x86-64 y viene con un servidor VNC integrado para control remoto.

Al igual que VB, se puede encontrar Qemu vía los repositorios de numerosas distribuciones.

Homesite: [wiki.qemu.org](http://wiki.qemu.org).

## **KVM**

*“Kernel-based Virtual Machine”*. Se trata de una aplicación libre y sólo disponible para plataforma Linux (como anfitrión) con la que podremos

usar sistemas cliente basados en Linux, sistemas Windows, Solaris, OpenSolaris, DOS, OS/2, \*BSD, QNX, Haiku y ReactOS.

Al igual que las otras opciones, ofrece soporte para plataformas de 32 y 64 bits y se puede usar los puertos usb, paralelo y serial de los equipos.

Homesite: [linux-kvm.org](http://linux-kvm.org).

### **OpenVZ**

Otra opción para virtualizar sistemas operativos que, como indica su nombre, es open source.

OpenVZ se mueve sólo entre sistemas GNU/Linux, es decir, no se puede usar para tener como sistema cliente sistemas Windows, por ejemplo. Sin embargo, la virtualización en el nivel de sistema operativo de OpenVZ proporciona mejor rendimiento, escalabilidad, densidad, administración de recursos dinámicos, y facilidad de administración que las alternativas.

Tanto para la creación como para el manejo de los sistemas instalados vía OpenVZ y de los parámetros de esta aplicación, se puede hacer uso de las órdenes en terminal o usar una interfaz gráfica como EasyVZ, una solución libre que puede facilitar el trabajo a los no habituados a la línea de comandos.

Homesite: [wiki.openvz.org](http://wiki.openvz.org).

### **Linux-VServer**

Al igual que la opción anterior, se trata de una aplicación libre y con soporte únicamente de sistemas basados en Linux. No se debe confundir esta aplicación con Linux Virtual Server, solución para gestionar balance de carga en sistemas Linux.

Puede usarse también sobre plataformas 64 bits (como anfitrión).

Homesite: [linux-vserver.org](http://linux-vserver.org).

## **Xen**

Es una aplicación libre para virtualización de sistemas basados en Linux, Solaris, Windows, OpenSolaris, DOS, OS/2, BSD, QNX, Haiku o ReactOS, usando un sistema GNU/Linux como anfitrión.

Como la anterior opción, puede ser usada en un sistema anfitrión de 64 bits y también puede correr sistemas clientes de la misma plataforma. También se puede usar los puertos usb, serie y paralelo del equipo. Xen también ofrece soporte de aceleración 3D.

No se trata de una aplicación sencilla de configurar para los no entendidos pero es la opción elegida por muchos administradores por su buen rendimiento gracias a la técnica de virtualización usada por Xen<sup>8</sup>.

## **2.3 Marco Teórico**

### **2.3.1 Virtualización de escritorios**

El proceso de separación entre el escritorio, que engloba los datos y programas que utilizan los usuarios para trabajar, de la máquina física. El escritorio "virtualizado" es almacenado remotamente en un servidor central en lugar de en el disco duro del ordenador personal. Es decir, cuando los usuarios trabajan en su escritorio desde su portátil u ordenador personal, todos sus programas, aplicaciones, procesos y datos se almacenan y ejecutan centralmente, permitiendo a los usuarios acceder remotamente a sus escritorios desde cualquier dispositivo capaz

---

<sup>8</sup> Homesite: [www.xen.org](http://www.xen.org).

de conectarse remotamente al escritorio, tales como un portátil, PC, smartphone o cliente ligero.

La virtualización de escritorio es encapsular y entregar bien el acceso a la totalidad de un entorno de un sistema de información o del entorno en sí a un dispositivo remoto. Este dispositivo puede estar basado en una arquitectura de hardware completamente diferente a la utilizada por el entorno de escritorio proyectado. También puede tener como base un sistema operativo totalmente diferente.

La virtualización de escritorio es el uso de máquinas virtuales para permitir que los múltiples usuarios de la red mantengan sus escritorios individuales en un único servidor u ordenador central. El equipo central puede estar localizado en una residencia, en la empresa o en un centro de datos. Los usuarios pueden estar geográficamente dispersos y estar conectados al equipo central mediante una red de área local (LAN), una red de área extensa (WAN) o mediante Internet.

La virtualización de escritorio ofrece ventajas con respecto al modelo tradicional, en el que cada ordenador funciona como una unidad completa y autónoma con su propio sistema operativo, periféricos y aplicaciones. En general los gastos se reducen porque los recursos pueden ser compartidos y se asignan a los usuarios en función de sus necesidades. La integridad de la información del usuario se mejora por que todos los datos se almacenan y se guardan copias de seguridad en el centro de datos. Los conflictos en el software se minimizan mediante la reducción del número total de los programas almacenados en los equipos.

A pesar de la distribución de los recursos, todos los usuarios pueden personalizar y modificar sus equipos de escritorio para satisfacer sus

necesidades específicas. De esta manera, la virtualización de escritorio ofrece una mayor flexibilidad en comparación con la paradigma cliente / servidor.

Las limitaciones que tiene la virtualización de escritorios son los riesgos de seguridad que se generan si la red no está bien gestionada, conlleva una pérdida de autonomía y privacidad del usuario, los desafíos en la creación y el mantenimiento de los controladores para las impresoras y otros periféricos, dificultad en la gestión de complejas aplicaciones como las multimedia y problemas de mantenimiento de direcciones de los usuarios de máquinas virtuales en correspondencia con los del centro de datos.

### **2.3.2 Linux Terminal Server Project - LTSP**

Son un conjunto de aplicaciones servidores que proporcionan la capacidad de ejecutar Linux en computadores de pocas prestaciones de velocidad o de bajo costo, permitiendo reutilizar equipos que actualmente resultan obsoletos debido a la alta performance requerida por otros sistemas operativos. LTSP se distribuye bajo licencia GNU GPL de software libre.

El sistema de funcionamiento de **LTSP** consiste en repartir por medio de la red el núcleo de Linux que es ejecutado por los clientes y que posteriormente ejecutarán secuencias de scripts típicos de una mini distribución. Los clientes podrán acceder a las aplicaciones por medio de una consola textual o por un servidor gráfico que se comparte utilizando el protocolo XDMCP.

Cuando un servidor X corre en un X terminal independiente, muestra una lista de clientes conectables (un **XDMCP Chooser**). Esta lista puede estar compuesta por:

- Una lista predefinida de máquinas y sus direcciones de red respectivas.
- Una lista que el XDMCP de turno obtiene mediante una petición broadcast, la cual normalmente coincide con la lista de las máquinas locales TCP/IP.

Es común que el servidor XDMCP se muestre a sí mismo en la lista. Cuando el usuario selecciona una máquina de la lista, el servidor X que corre en la máquina local se conecta al administrador de pantalla X de la máquina remota.

Entre los beneficios se tiene:

- El sistema operativo es Linux, libre de licenciamiento.
- Comprando un equipo con prestaciones estándar es posible reciclar 10 ordenadores obsoletos.
- Una aplicación instalada en el servidor está disponible para todos los clientes.
- Todo se guarda en el servidor, lo que facilita el trabajo en grupo de red.

## **XDMCP**

Siglas de "X Display Manager Control Protocol", "Protocolo de Control de Administrador de la Pantalla X". Es un protocolo utilizado en redes para comunicar un ordenador servidor que ejecuta un sistema operativo con un gestor de ventanas basado en X-Window con el resto de clientes que se conectarán a éste con propósitos interactivos.

## **Display Manager**

Administrador de pantalla X, mantiene los procesos del servidor X activos en él, conectándolo a una pantalla física y proporcionando un cuadro de diálogo que permita iniciar sesión en el mismo a todos los ordenadores que lo requieran. Escucha el User Datagram Protocol (UDP) en el puerto 177 y responde a peticiones de tipo QUERY y BROADCAST\_QUERY enviando un paquete tipo WILLING al equipo que le contactó.

Actualmente uno de los campos donde se utiliza bastante LTSP es en la educación, debido a su bajo costo de implantación que suele tener.

LTSP ha servido de base para varias Distribuciones Linux, la más destacada es K12LTSP (basada en Fedora Core), también se encuentran Deworks, Edubuntu, Skolelinux y Trisquel GNU/Linux en su versión para educación.

Actualmente, la compatibilidad de este servidor de terminales se ha extendido a todas las plataformas Linux de uso común, y su rendimiento y capacidad ha mejorado con la última versión.

Otro uso, aunque con mayor complejidad de implantación, es para el manejo y gestión de estaciones de trabajo de ofimática para empresas u otras aplicaciones que no se basen en artes gráficas o cualquier aplicación que requiera alto rendimiento gráfico.

- **Métodos de Arranque**

Etherboot PXE RPL

la línea de comandos del kernel opciones

CustomLtspKernels

WirelessLtsp

BootingFromLocalDevice

- **Configuración**

Casi la totalidad de la configuración del cliente para LTSP se realiza en el archivo lts.conf.

- **Hardware**

Tarjetas de red, tarjetas de vídeo tarjetas de sonido Ratones InputDevices arquitecturas de CPU Clientes Teclados Scanners Eproms.

- **Aplicaciones Locales**

Las aplicaciones suelen ejecutarse en el servidor, y se muestran los resultados en la pantalla de cliente ligero. Con LTSP, es posible ejecutar una aplicación en el cliente ligero, con lo que la utilización de más de los recursos locales y poniendo menos de una carga en el servidor. A esto lo llamamos aplicaciones locales .

- **Secuencias de comandos de la pantalla**

Las secuencias de comandos de la pantalla son algo así como aplicaciones locales. Hacen algo para ejecutar de forma local. Usamos las secuencias de comandos de la pantalla para iniciar el servidor X, una sesión de Telnet, o una sesión de rdesktop. En esos ejemplos, se inicia un proceso a nivel local, para ayudar a conectarse a un servidor en la red.

- **Dispositivos locales**

Sonido Impresoras medios de comunicación locales

- **Protocolos y Servicios**

DHCP TFTP NFS XDMCP XFS VNC RDP LDAP Sonido Intercambio de Syslog Puertos utilizados por los servicios de LTSP.

### **2.3.3 Fases de Implementación de un CTI-Centros de Datos**

#### **I. Planificación**

- Preparar
- Diseñar

#### **II. Construir**

- Adquirir
- Implementar.

#### **III. Operación**

#### **IV. Administración**

## **PLANIFICACIÓN**

El proceso de planificación es el talón de aquiles de un proyecto de infraestructura de "Data center", errores de planificación pueden magnificarse en la etapa de construcción, provocando retrasos, sobrecostos, tiempo desperdiciado y últimamente un sistema deficiente.

Las principales tareas que involucra son:

- Determinar los parámetros de IT (Servidores, Telecomunicaciones, etc.)
- Desarrollar el concepto del Sistema (Estándares, etc.)
- Determinar requerimientos de usuarios (área soporte, operación, seguridad, etc.,)
- Generar especificaciones (escribir).
- Generar un Diseño detallado.

## **Planeamiento de un CTI: Centro de Datos**

Los centros de datos, ya sea para mantener las necesidades de una sola empresa o alojar decenas de miles de sitios de Internet de clientes, son esenciales para el tráfico, procesamiento y almacenamiento de información, es por esto que deben ser extremadamente confiables y seguros al tiempo que deben ser capaces de adaptarse al crecimiento y la reconfiguración.

Para diseñar un centro de datos se deben tener en cuenta varios factores más allá del tamaño y la cantidad de equipos de procesamiento/almacenamiento de datos que éste debiera albergar. Establecer el lugar físico, acceso a la energía, nivel de redundancia, cantidad de refrigeración, rigurosa seguridad y tipo de cableado son sólo algunos de los varios factores que entran en juego en una instalación exitosa o ampliación de un centro de datos.

- Disponibilidad y Redundancia del Centro de Datos
- La necesidad de disponibilidad para el centro de datos depende de varios factores. La ubicación, el acceso a la energía y a las comunicaciones, que otras industrias estén ubicadas en el mismo vecindario, todo esto está relacionado con la confiabilidad. Dentro del centro de datos, la disponibilidad se controla por la redundancia de la infraestructura del servicio.

Los centros de datos concentran gran cantidad de equipos electrónicos en un área reducida, por esto es que requieren organización para manejar el crecimiento y la reconfiguración. Los temas incluyen la disposición de las entradas de electricidad y telecomunicaciones a las salas, HVAC (calefacción, ventilación y

aire acondicionado- a veces llamado el equipo “mecánico”), un centro de operaciones de red, una sala de telecomunicaciones, oficinas para el personal, energía redundante y por su puesto sala de cómputos. Otros temas incluyen la colocación de racks, gabinetes y equipos para una óptima refrigeración, agrupándolos por eficiencia y apartándolos por seguridad.

❖ **Sistemas Eléctricos del Centro de Datos**

La entrada de energía necesita estar condicionada y “ruteada”. Las tecnologías de energía redundante (UPS – Sistema de Energía Ininterrumpida [SEI] y generadores) se discuten como también la importancia de la puesta a tierra.

❖ **Presentación del cableado de datos**

Varios tipos de cables y sistemas se describirán y compararán con consejos sobre cómo hacer el mejor uso de ellos.

❖ **Cableado del centro de cómputos**

Los métodos, medios (cable de par trenzado de cobre y fibra óptica) y terminación del cableado estructurado se trazan y comparan.

❖ **Monitoreo y control del centro de datos**

Los sistemas de monitoreo automático ayudan a mantener el centro de datos y la sala de cómputos funcionando con su máxima eficiencia.

❖ **Seguridad Física y Lógica del centro de datos**

Las normas de seguridad contra incendios y la seguridad eléctrica (NFPA –Asociación Nacional de Protección contra Incendio- y NEC –Código Nacional de Electricidad-, etc.) se tratan aquí así como también asuntos de seguridad lógica tales como el control al

acceso y el monitores por CCTV (circuito cerrado de televisión, conocido también como video de seguridad).

#### ❖ Tipos y Topología del Centro de Datos

En términos generales, la definición de un centro de datos es una sala o red de salas que alberga el procesamiento, almacenamiento y comunicaciones de datos de los activos interconectados de una o más empresas. El centro de datos puede ser una sala dentro de un edificio o bien ocupar un edificio completo para este fin.

El propósito del centro de datos es albergar información de activos en un ambiente que enfrenta sus necesidades para energía, HVAC, telecomunicaciones, redundancia y seguridad lógica. Estos bienes incluyen rack o gabinete montado con equipo activo y un sistema de cableado estructurado para interconectarlos.

Los parámetros para los centros de datos se definen bajo las normas TIA-942 (norteamericana), EN 50173-5.200X (europea) y el Proyecto ISO/IEC 24764 (internacional). TIA-942 se desarrolla bajo las normas de cableado estructurado más los requerimientos de energía eléctrica, ventilación del aire, distribución de los equipos, entre otras. El propósito de esta presentación es colaborar en el planeamiento del centro de datos y proporcionar asesoramiento para la instalación.

#### ❖ El centro de datos corporativo

Brinda comunicación y servicio de datos a una sola compañía o empresa. Un centro de datos de una empresa es el núcleo para la red de información de la empresa así como lo es su acceso a Internet y la telefonía. Los servidores de páginas web, los concentradores de Intranet, equipos de almacenamiento de red

(NAS= network attached storage) y otros, por lo general se ubican aquí.

El centro de hosting es propiedad del proveedor del servicio que vende información y servicios de Internet (tales como el hosting web o de Red Privada Virtual [VPN]) a varios clientes. Mientras los dos tipos de centro de datos utilizan la misma clase de equipos e infraestructura de cableado, el centro de datos de hosting necesita una línea de delimitación adicional y seguridad. Por ejemplo, un cliente grande puede instalar o colocar sus propios equipos en el sitio de hospedaje. Estos equipos pueden estar apartados en áreas cerradas con acceso controlado.

Un centro de datos típico se organiza como se muestra a continuación. Podría decirse que un centro de datos consiste en una sala de cómputos y los espacios que necesita.

- ❖ El Área de Distribución Principal (MDA) es el concentrador del sistema de cableado y está dentro de la sala de cómputos. En el caso de que un centro de datos se encuentre en varios pisos, las MDA actúan como punto de colección. IMPORTANTE: En un ambiente compartido entre varias empresas, el MDA puede estar en una zona apartada por seguridad. El MDA incluye la conexión cruzada principal y puede incluir conexiones cruzadas horizontales si el equipo que los utiliza está cerca (ver HDA).
- ❖ El MDA puede albergar los ruteadores y los switches Red de Área Local (LAN -Local Área Network)/Red de Área de Almacenamiento (SAN- Storage Área Network) de núcleo. A veces, el equipo proveedor del servicio (como multiplexores) está contenido en el MDA de manera que no se excedan las distancias especificadas del circuito.

- ❖ El Área de Distribución Horizontal (HDA) es donde se encuentra la conexión cruzada horizontal si el centro de datos es relativamente amplio. En centros de datos más pequeños, el HDA está incorporado al MDA. Como el MDA, el HDA puede estar apartado por seguridad. Esto incluye los switches de LAN/SAN y los switches para Teclado/Video/Mouse (KVMKeyboard/ Video/Mouse) para el equipo.
- ❖ La Sala de Almacenamiento es un área segura para albergar las piezas de reposición y cableado además de otros materiales necesarios para el correcto funcionamiento. El acceso a un puerto de carga es muy práctico.
- ❖ Las Salas eléctrica/mecánica albergan los servicios primarios, los circuitos de distribución y los equipos para manipulación de aire destinado a esos servicios. Para lograr un rendimiento del 100% de disponibilidad son esenciales tener líneas filtrada con contingencia (UPS, batería o generadores) y un sistema de HCAV amplio y confiable.
- ❖ La Sala de telecomunicaciones, mantiene los equipos que abastecen los datos locales, video y voz necesarios para las oficinas de soporte de las operaciones del centro de datos y otras áreas de trabajo.
- ❖ El centro de operaciones, es el lugar en el cual se monitorea el centro de datos. Dependiendo de la medida del centro de datos, el centro de operaciones puede albergar docenas de técnicos que monitorean las redes en pantallas amplias montadas en la pared así como también en pantallas de escritorio.
- ❖ La sala de entrada es la interfase entre el proveedor de acceso y el cableado estructurado del centro de datos. Es la sala que delimita con los equipos. **IMPORTANTE:** Algunas veces se usa una boca de entrada (un espacio afuera del centro de datos) como punto de

ingreso para los proveedores de acceso. La sala de entrada se encuentra afuera de la sala de cómputos por cuestiones de seguridad.

- ❖ Debería haber más de una sala de entrada dependiendo del nivel de la redundancia y el Nivel para el acceso secundario a proveedores de servicio. En caso de que el centro de datos sea muy amplio, puede ser necesaria otra sala de entrada para acercar los proveedores del servicio al equipo como para no superar la extensión máxima del circuito (por ejemplo, los 100 m de longitud del canal para los cables de par trenzados- ver Sección 6.0).
- ❖ Las Áreas de Distribución de los Equipos (EDA) son los racks y gabinetes que contienen los módulos de computación y almacenamiento.
- ❖ La sala de cómputos es un espacio de ambiente controlado y seguro donde se encuentran los equipos de datos y telecomunicaciones y el cableado. Está dividido en áreas de distribución que son los puntos de conexión para el sistema de cableado estructurado. Los equipos de racks/gabinetes están en un piso más elevado. La refrigeración y el cableado (para datos y electricidad) por lo general se pasan por debajo. La norma TIA-942 maneja específicamente temas como el acceso a la manipulación de aire, la iluminación, la contingencia de energía, la densidad del equipamiento, y otras funciones.
- ❖ El Área de Distribución Zonal (ZDA) se utiliza en amplias salas de cómputos que necesitan flexibilidad de configuración adicional entre el HDA y los equipos. Las ZDA albergan sólo los equipos pasivos y debe estar al menos 49 pies (15 metros) distante del HDA.

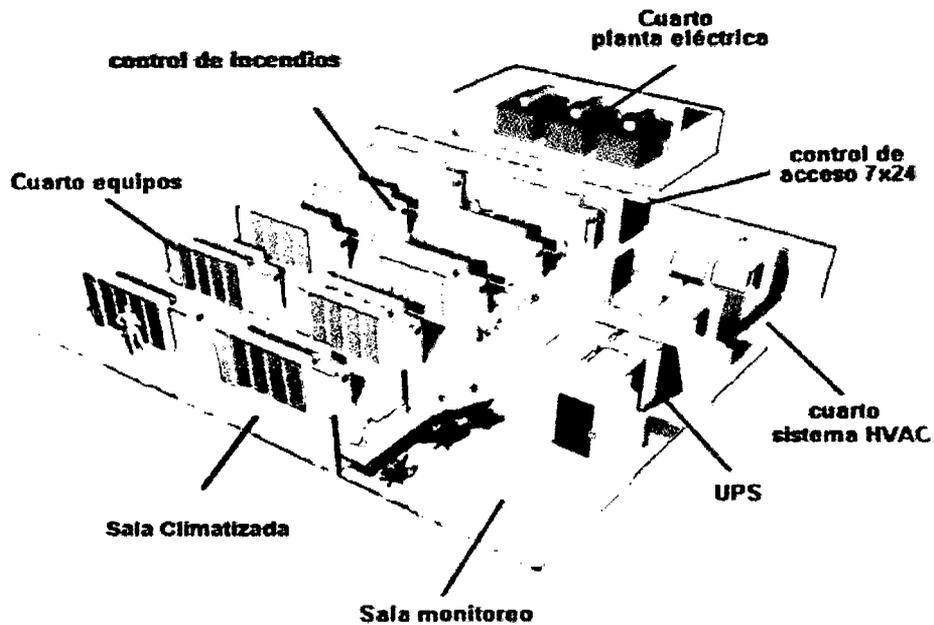


Fig. 2.2 Infraestructura del centro de datos

## Redundancia y Disponibilidad

La expectativa de un centro de datos con disponibilidad del 100% es lo ideal. Sin embargo, todos los centros de datos, sin importar cuán cuidadosamente hayan sido planificados, construidos y manejados, sufrirán un tiempo de indisponibilidad, sea intencional (mantenimiento planificado) o no intencional. La indisponibilidad se minimiza a través de la creación de sistemas de redundantes para posibles puntos únicos de falla. Una empresa necesita considerar cuidadosamente el tiempo de caídas que ésta pueda tolerar cuando diseña su centro de datos.

La redundancia proviene de la eliminación de los puntos únicos de falla. Un servicio sin un SEI o un generador hace que la energía eléctrica sea su punto único de falla. Para los sistemas de infraestructura (telecomunicaciones, electricidad, HVAC y arquitectura/estructura), TIA-942 traza cuatro niveles de redundancia, llamados "tiers" (niveles). En el nivel (tiers) más alto, las infraestructuras son menos susceptibles a la interrupción. Un centro de datos se define por su nivel más bajo para el sistema de infraestructura; un centro de datos con acceso a la

electricidad de Nivel III y de Nivel II en acceso a las comunicaciones tiene una redundancia de Nivel II.

### **Energía**

Dentro del rack o gabinete se colocan enchufes múltiples los cuales deben suministrar 20A 120V (o 16A 230V) de energía. Cada rack/gabinete deberá tener su propio circuito protegido por un interruptor. Las unidades de distribución de potencia (PDU) condicionan y manejan la energía dentro de la sala de cómputos. Las unidades SAI de hasta 100 kVA se pueden ubicar en la sala de cómputos mientras no sean del tipo de batería de plomo ácido inundada. Todos los sistemas de infraestructura (iluminación, seguridad, HVAC, etc.) deberían tener sus propios circuitos eléctricos separados.

### **Aire Acondicionado**

Los equipos modernos de computación generan grandes cantidades de calor, tanto como 500 watts cada pié cuadrado (30cm<sup>2</sup>) de la sala de cómputos. La energía en constante crecimiento de los equipos y la velocidad de las conexiones se están convirtiendo en temas serios de calentamiento.

Los centros de datos deben mantener un HVAC durante las 24 horas que genera una temperatura de bulbo seco de entre 20 y 25°C; se prefiere una temperatura de 22°C, la humedad debería estar entre un 40 y 55% con un punto de rocío no mayor a 21°C.

Para optimizar la refrigeración, los racks/gabinetes se deben de colocar en pasillos fríos y calientes con el equipamiento instalado frente a frente / fondo con fondo. El frente de los equipos dan al pasillo "frío".

Como los gabinetes tienen puertas, un espacio libre de al menos 4 pulgadas (100 mm) debería haber entre las puertas y el interior de los equipos para el cableado de energía y comunicaciones.

Los cortes de los mosaicos para el acceso de los cables no debe ser mayor de lo necesario. Se deben instalar humedecedores o escobillas para bloquear el aire que circula por los cortes. En cualquiera de los casos, el corte debe estar cubierto con bordes para evitar que los cables sean dañados durante linstalación.

### **Cielorraso e iluminación**

TIA-942 recomienda luz fluorescente con una iluminación de 500 lux (50 bujías-pie) en el plano horizontal y200 lux (20 bujías-pie) en el plano vertical medidos desde 3.3 pies (1 m) por encima del piso terminado en cada pasillo. Las luces y cualquier otro obstáculo (como roscas para rociadores) deben estar al menos a 8.5 pies (2.6 m) por encima del piso falso.

Racks/gabinetes más altos de 7 pies (2.13 m) necesitarán un cielorraso más elevado para mantener un espacio mínimo de 18 pulgadas (460 mm) entre el borde superior de la cabina de los equipos y el sistema de rociadores. Los rociadores deben ser del tipo pre- acción, que no llenan las cañerías hasta que detecta el humo.

### **Monitoreo y Control del Centro de Datos**

#### **Automatización del edificio**

Junto con las actividades del centro de cómputos, un centro de datos tiene docenas de sistemas separados igual que cualquier otra estructura comercial. Estos incluyen protección contra incendios, iluminación, sistema de calefacción, ventilación y aire acondicionado (HVAC-Heating,

Ventilation and Air Conditioner Equipment), seguridad, circuito cerrado de televisión (Close Circuit Television-CCTV) y control de acceso, que son sólo algunos de los tantos sistemas que necesitan ser monitoreados y controlados. Una solución de cableado integrado para respaldar los sistemas de automatización del edificio (building automation systems - BAS) pueden no sólo ofrecer el control central sino también los ahorros de costos que brinda la integración. La norma del cableado TIA-862 tiene requisitos para el cableado utilizado en sistemas de automatización de edificios. **IMPORTANTE** la protección contra incendios y circuitos de alarmas pueden ser requeridas por el código local para tener sus propios circuitos. Los códigos locales tiene prioridad.

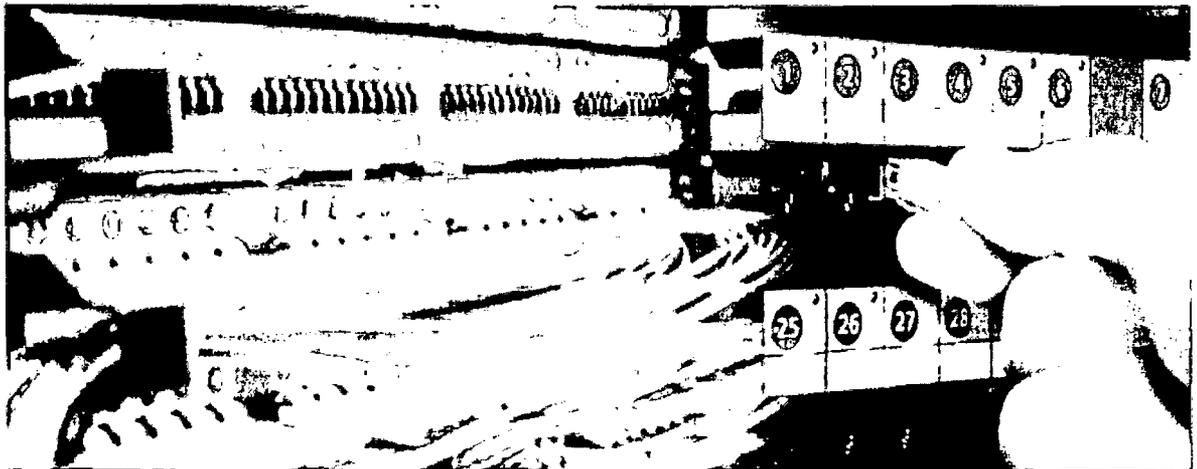
### **Monitoreo de la red**

La infraestructura del cableado de datos puede también ser monitoreada electrónicamente. El sistema de Patch Inteligente ofrece a los administradores control en tiempo real interactivo sobre las conexiones de cobre y fibra. Esto se hace instalando un sistema de manejo de infraestructura en tiempo real con paneles inteligentes que se unen al software inteligente en funcionamiento en el centro de operaciones.

El Patch Inteligente dice a los administradores del sistema el estado de cada conexión en la red. El monitoreo en tiempo real de conectividad física y descubrimiento de dispositivo permite solucionar los problemas más rápido en la red que maneja. La actualización automática del estado de circuito de la red asegura la última información y el trabajo electrónico ordena minimizar los errores humanos. También ayuda en la de desastre brindando un mapa virtual del circuito.

Si se necesita que se provea un servicio, o un circuito necesita ser quitado o agregado, el Patch Inteligente calcula la mejor forma de

implementarlo y generar un orden de trabajo electrónico. Los paneles LCD pantalla de cristal líquido (Liquid Crystal Display) en cada panel inteligente visualizan las instrucciones. Luces en cada puerto individual muestran qué conexiones se necesitan hacer. Los resultados son una administración de red con mejor respuesta y mejor seguridad. El sistema también reduce costos integrando procesos de workflow, automatizando las tareas de rutina y ayudando a los técnicos a cumplir órdenes de trabajo y abastecimiento de servicio. Como resultado, la productividad aumenta y los administradores logran un uso más eficiente de los recursos y control de costos.

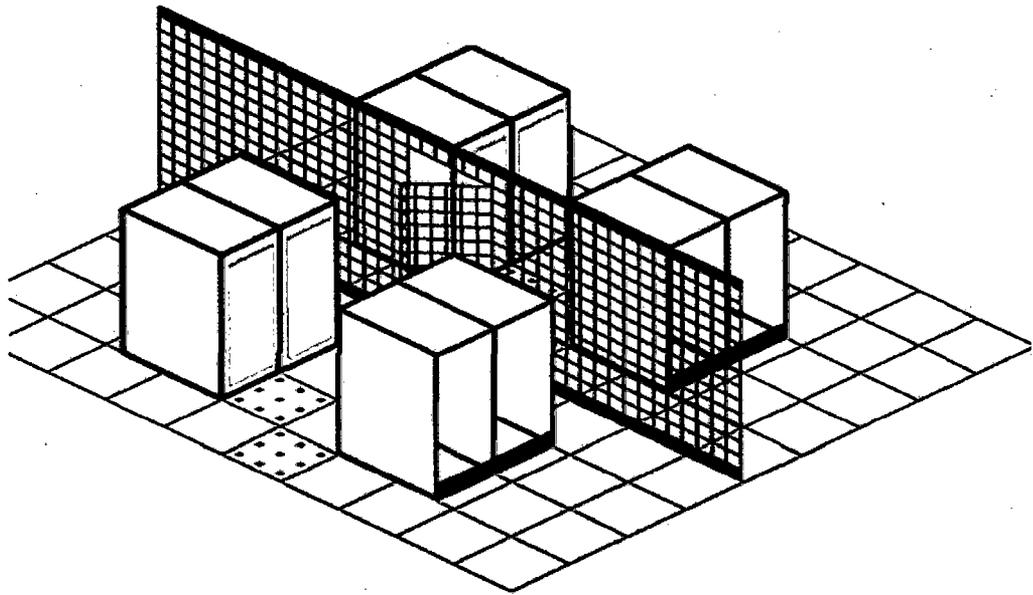


### **Seguridad Física y Lógica**

Los centros de datos representan una parte considerable de los recursos de una compañía. Lo más importante es que son el depósito de la información de una empresa. Este valiosísimo commodity debe ser protegido contra daño, destrucción y robo.

Debe hacerse lo posible para aislar las condiciones ambientales de la sala de cómputos. Las paredes deben ser sólidas y seguras y alcanzar las

normas de incendio de dos/cuatro horas. Las barreras de vapor deben instalarse para ayudar a mantener niveles de humedad aceptables. Todas las aberturas en las paredes por la entrada del cableado deben ser contra incendios. Cualquiera de los equipos grandes, como los generadores de contingencia, deben montarse sobre aislantes para que los racks y las gabinetes no sufran vibraciones.



Toda infraestructura que es mantenida por personal externo debe hacerlo fuera de la sala de cómputos. La entrada del centro de datos debe ser monitoreada (CCTV) y controlada por acceso autenticados (tarjetas magnéticas, biometría, etc.). La entrada del centro de cómputos debe estar construida de manera que se prevenga entradas superpuestas (más de una persona entrando al mismo tiempo). Se deben considerar las medidas de los cercos exteriores o portón de acceso al estacionamiento.

Dentro del centro de datos, los gabinetes con puertas que se pueden cerrar con llave previenen el acceso no autorizado a los equipos. Las cabinas previenen el acceso a los equipos ya ubicados o a los equipos que almacena información confidencial.

## **DISEÑO DE CENTRO DE DATOS**

El diseño de todo CPD conlleva un análisis de necesidades futuras y una planificación de alto nivel. Cualquier error en el diseño, sería irreversible, ya que podría implicar una limitación en las prestaciones o crecimiento futuro del mismo.

Coordinar todos los aspectos de un centro de datos es crítico, lo cual puede incluir:

- Sistema de cableado de telecomunicaciones
- Plano de piso del equipamiento
- Planos eléctricos
- Plano arquitectural
- HVAC
- Seguridad
- Sistema para rayos

### **Principios del Diseño de la Infraestructura de un Centro de Datos**

#### **1. Ahorro de espacio:**

Maximizar los recursos de espacio es un aspecto crítico del diseño de un centro de datos.

#### **2. Confiabilidad:**

Diseños redundantes, prueba de fallas para máximo “uptime” (tiempo de actividad u operación).

#### **3. Administrabilidad:**

Principio clave para optimizar el Centro de Datos,

Se diseña la infraestructura para ser un servicio altamente confiable y flexible para adecuar todo desde upgrades y modificaciones hasta recuperación de desastres.

**Proceso de Diseño recomendado:**

- Estimar necesidades a full capacidad para todo el equipamiento.
- Anticipar crecimiento futuro sobre la vida del centro de datos.
- Proveer todos los requerimientos a ingenieros y arquitectos.
- Crear un plano de piso del equipamiento.
- Diseñar el sistema de cableado de telecomunicaciones.

**2.3.3.1 ESTÁNDARES RELACIONADOS AL DISEÑO DE CENTROS DE DATOS**

**La TIA/EIA-568-B, define para el diseño de un Centro de Datos:**

- Instalación de entrada
- Cuarto de equipos
- Cuarto de Telecomunicaciones
- Punto de consolidación
- Área de trabajo

**La norma TIA-942, respecto al Diseño de Cableado, establece que hay 6 pasos para este proceso:**

- **Evaluar las necesidades** de espacio, telecomunicaciones, electricidad, refrigeración y redundancia en su plena capacidad, luego reservar un lugar para el crecimiento.

Los cálculos variarán de acuerdo con la puesta en práctica en sí, pero un 25 % para el crecimiento es un buen comienzo.

- **Contactar diseñadores profesionales** y proveerlos de las necesidades para la protección del área, la electricidad, la refrigeración, la seguridad, la carga del piso, la puesta a tierra y la eléctrica para la sala de cómputos. Proveerlos de las necesidades para las áreas de soporte del centro de datos.
- **Coordinar los planos preliminares** de los diseñadores y modificar lo necesario.
- **Crear un plano del ambiente para el equipamiento** con la distribución de las salas principales y áreas de distribución. Incluir las necesidades de electricidad esperada, telecomunicaciones, refrigeración y carga del piso.
- **Obtener un plano actualizado** por parte de los diseñadores con rutas de telecomunicación, equipamiento eléctrico y equipamiento mecánico añadido a la capacidad total del plano del ambiente del centro de datos.
- **Diseñar el sistema de cableado estructurado** basado en las necesidades del equipamiento del centro de datos.

### **La Norma ICREA Std-131-2009**

Establece los componentes de un ambiente de Tecnología de la Información:

- Electricidad
- Aire acondicionado
- Seguridad
- Comunicaciones

- Environment
- Gobernabilidad, Administración y Mantenimiento
- Consideraciones Green

#### **Nivel de Disponibilidad en Data Centers:**

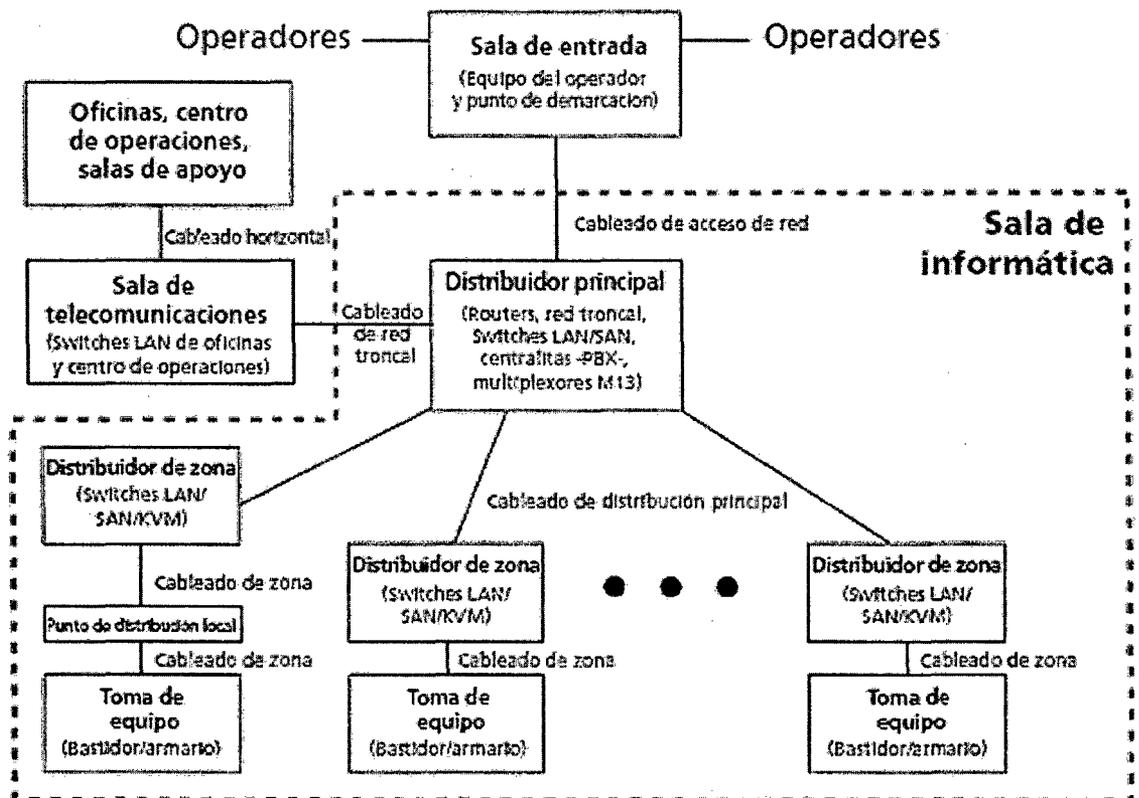
- **Nivel 1: QADC (18 Días)**  
Quality Assurance Data Center (95%)
- **Nivel 2: WCQA (88 Horas)**  
World Class Quality Assurance Data Center (99%)
- **Nivel 3: S-WCQA (9 Hrs)**  
Safety World Class Quality Assurance Data Center (99.9%)
- **Nivel 4: HS-WCQA (52 min)**  
High Security World Class Quality Assurance Data Center (99.99%)
- **Nivel: 5: HSHA-WCQA (5 min)**  
High Security High Available World Class Quality Assurance Data Center (99.998%)

#### **La norma CENELEC-EN50173-5**

De acuerdo con la norma, un centro de datos debería incluir los siguientes elementos funcionales clave:

- Una o más salas de acceso
- Distribuidor principal

- Distribuidor de zona
- Punto de distribución local
- Sala de datos



Centro de datos conforme con la norma EN 50173-5

### © Sala de acceso

La sala de acceso aloja el equipo del operador y el punto de demarcación. Puede estar dentro de la sala de ordenadores, pero la norma recomienda una sala separada por razones de seguridad. Si está alojada en la sala de ordenadores, debería consolidarse dentro del área principal de distribución.

### © Distribuidor principal

El distribuidor principal (MD) aloja la conexión cruzada principal, el punto central de distribución para el sistema de cableado estructurado del centro de datos. Este área debería situarse de forma central para evitar superar las distancias de cableado recomendadas y puede incluir una conexión cruzada horizontal para un área de distribución de equipo adyacente. La norma especifica bastidores separados para fibra óptica, par trenzado y cable coaxial.

### © Distribuidor de zona

El distribuidor de zona (ZD) es la ubicación de las conexiones cruzadas horizontales, el punto de distribución para las áreas de distribución del cableado al equipo. Puede haber un ZD o varios, dependiendo del tamaño del centro de datos y de los requisitos de cableado. Como orientación, un solo ZD tiene un máximo de 2.000 terminaciones de cables de 4 pares o coaxiales. Como la MD, la norma especifica bastidores separados para fibra óptica, par trenzado y cable coaxial.

### © Punto de distribución local

Éste es el área de cableado estructurado para equipos que están sobre el suelo y no admiten paneles de conexión (por ejemplo, algunos ordenadores centrales y servidores).

### © Sala de datos

Éste es la ubicación de los armarios y bastidores de equipos. La norma especifica que los armarios y bastidores deben configurarse de tal forma que exista una circulación de aire caliente/frío para disipar con eficacia el calor de los componentes electrónicos.

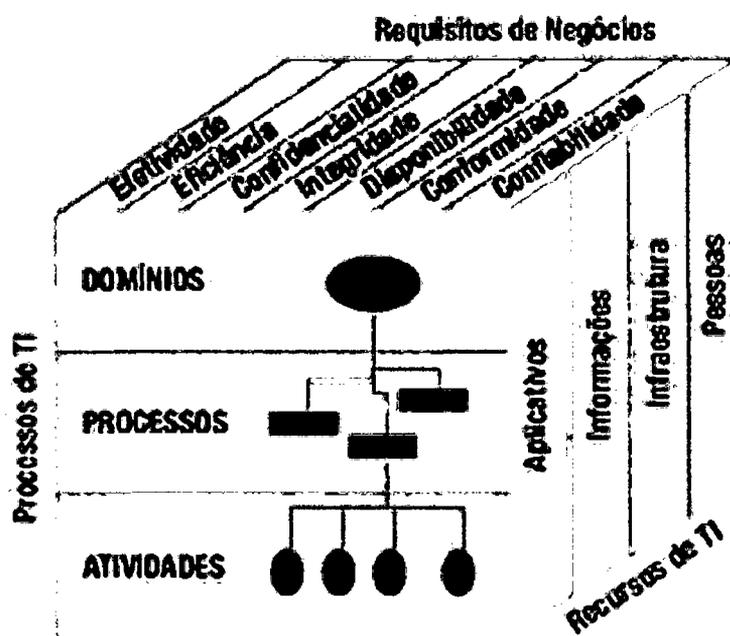
### **2.3.4 COBIT 4.1**

COBIT es un marco de trabajo y un conjunto de herramientas de Gobierno de Tecnología de Información (TI) que permite a la Gerencia cerrar la brecha entre los requerimientos de control, aspectos técnicos y riesgos de negocios. COBIT habilita el desarrollo de políticas claras y buenas prácticas para el control de TI a lo largo de las organizaciones. COBIT fue publicado por primera vez por ITGI en abril de 1996. La versión COBIT® 4.1 hace énfasis en el cumplimiento reglamentario, ayudando a la organizaciones a incrementar el valor de TI, destacando los vínculos entre los objetivos del negocio y TI, y simplificando la implementación del marco de trabajo COBIT. Este marco de trabajo es la base para diferentes entes reguladores a nivel mundial, con la finalidad de lograr que las entidades reguladas optimicen sus inversiones de TI y administren adecuadamente sus riesgos tecnológicos.

#### **2.3.4.1 Criterios de Información de COBIT**

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio. Con base en los requerimientos más amplios de calidad, fiduciarios y de seguridad, se definieron los siguientes siete criterios de información:

## CUADRO N° 8: CUBO DE COBIT



Fuente: COBIT 4.1 IT GOVERNANCE INSTITUTE [Pag. 25]

1. La efectividad tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.
2. La eficiencia consiste en que la información sea generada con el óptimo (más productivo y económico) uso de los recursos.
3. La confidencialidad se refiere a la protección de información sensible contra revelación no autorizada.
4. La integridad está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.
5. La disponibilidad se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.

6. El cumplimiento tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.

7. La confiabilidad se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.

#### **2.3.4.2 Recursos de TI**

Los recursos de TI identificados en COBIT se pueden definir como sigue:

1. Las **aplicaciones** incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.

2. La **información** son los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información, en cualquier forma en que sean utilizados por el negocio.

3. La **infraestructura** es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.

4. Las **personas** son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran.

Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados. Normalmente se ordenan dentro de dominios de responsabilidad de plan, construir, ejecutar y Monitorear. COBIT define las actividades de TI en un modelo de 34 procesos genéricos agrupados en 4 dominios:

- **Planear y Organizar (PO)** Estrategias y tácticas. Identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio. Proporciona dirección para la entrega de soluciones (AI) y la entrega de servicio (DS).
- **Adquirir e Implementar (AI)** Identificación de soluciones, desarrollo o adquisición, cambios y/o mantenimiento de sistemas existentes. Proporciona las soluciones y las pasa para convertirlas en servicios.
- **Entregar y Dar Soporte (DS)** Cubre la entrega de los servicios requeridos. Incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales. Recibe las soluciones y las hace utilizables por los usuarios finales.
- **Monitorear y Evaluar (ME)** Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno. Monitorear todos los procesos para asegurar que se sigue la dirección provista.

Los dominios se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear. A lo largo de estos cuatro dominios, COBIT ha identificado 34 procesos de TI generalmente usados. Mientras la mayoría de las empresas ha definido las responsabilidades de planear, construir, ejecutar y monitorear para TI, y la mayoría tienen los mismos procesos clave, pocas tienen la misma estructura de procesos o le aplicaran todos los 34 procesos de COBIT. COBIT proporciona una lista completa de procesos que puede ser utilizada para verificar que se completan las actividades y responsabilidades; sin embargo, no es necesario que apliquen todas, y, aun más, se pueden combinar como se necesite por cada empresa. Para cada uno de estos 34 procesos, tiene

un enlace a las metas de negocio y TI que soporta. Información de cómo se pueden medir las metas, también se proporcionan cuales son sus actividades clave y entregables principales, y quién es el responsable de ellas. COBIT proporciona un modelo de procesos de referencia y un lenguaje común para que cada uno en la empresa visualice y administre las actividades de TI. La incorporación de un modelo operacional y un lenguaje común para todas las partes de un negocio involucradas en TI es uno de los pasos iniciales más importantes hacia un buen gobierno. También brinda un marco de trabajo para la **medición y monitoreo** del desempeño de TI, comunicándose con los proveedores de servicios e integrando las mejores prácticas administrativas. Un modelo de procesos fomenta la propiedad de los procesos, permitiendo que se definan las responsabilidades. Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados. Éstos se pueden resumir como sigue:

#### **2.3.4.3 Los procesos requieren Controles**

**Control:** Políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos.

**Objetivos de Control:** Requerimientos mínimos para un control efectivo de cada proceso de IT. Gerencia usa los procesos para organizar y administrar las actividades de TI en curso. Cada proceso de TI de COBIT tiene un objetivo de control de alto nivel y un número de objetivos de control detallados. Además de los objetivos de control detallados, cada proceso COBIT tiene requerimientos de control genéricos que se identifican con PCn, que significa número de control de proceso:

**PC1 Dueño del proceso:** Asignar un dueño para cada proceso COBIT de tal manera que la responsabilidad sea clara.

**PC2 Reiterativo:** Definir cada proceso COBIT de tal forma que sea repetitivo.

**PC3 Metas y objetivos:** Establecer metas y objetivos claros para cada proceso COBIT para una ejecución efectiva.

**PC4 Roles y responsabilidades:** Definir roles, actividades y responsabilidades claros en cada proceso COBIT para una ejecución eficiente.

**PC5 Desempeño del proceso:** Medir el desempeño de cada proceso COBIT en comparación con sus metas.

**PC6 Políticas, planes y procedimientos:** Documentar, revisar, actualizar, formalizar y comunicar a todas las partes involucradas cualquier política, plan ó procedimiento que impulse un proceso COBIT. Los propietarios de procesos deben entender qué entradas requieren de otros procesos y que requieren otros de sus procesos.

**Roles y responsabilidades documentados:** Clave para un gobierno efectivo. Gráfica **RACI** (quién es responsable, quién rinde cuentas, quién es consultado y quien informado) para cada proceso.

**Rendir cuentas:** La persona que provee autorización y direccionamiento a una actividad.

**Responsabilidad:** la persona que realiza la actividad. Consultado e Informado Garantizan que todas las personas que son requeridas están involucradas y dan soporte al proceso.

#### **2.3.4.4 Controles del Negocio y Controles de TI**

□ **Objetivos de negocio:** Se fijan a nivel de dirección ejecutiva. Se establecen políticas y se toman decisiones de cómo aplicar y administrar los recursos empresariales para ejecutar la estrategia de la compañía. Los controles TI se guían por este conjunto de objetivos y políticas de alto nivel.

□ **Controles de negocio:** A nivel de procesos de negocio. Son controles para actividades específicas del negocio. La mayoría de los procesos de negocio están automatizados e integrados con los sistemas aplicativos de TI muchos de los controles a este nivel estén automatizados [**controles de las aplicaciones**]. P.e.: Integridad, precisión, validez, autorización, segregación de funciones...

Otros controles como procedimientos manuales (autorización de transacciones, separación de funciones conciliaciones manuales...) [**controles manuales**].

□ **Servicios TI:** Proporcionados para soportar los procesos de negocio. Suelen estar compartidos por varios procesos de negocio. A estos servicios se también aplican controles [**controles generales de TI**]. P.e.: desarrollo de sistemas, administración de cambios, seguridad, operaciones del computador.

#### **2.3.4.5 Generadores de Mediciones**

Las empresas deben medir dónde se encuentran y dónde se requieren mejoras, e implementar un juego de herramientas gerenciales para

monitorear esta mejora. ¿Hasta dónde debemos ir? ¿Está justificado el costo por el beneficio? Para responder a esto COBIT utiliza:

- Modelos de madurez** que facilitan la evaluación por medio de benchmarking y la identificación de las mejoras necesarias en la capacidad
- Metas y mediciones** de desempeño para los procesos de TI cómo los procesos satisfacen las necesidades del negocio y de TI, y cómo se usan para medir el desempeño de los procesos internos
- Metas de actividades** para facilitar el desempeño efectivo de los procesos

Usando los procesos de madurez desarrollados para cada uno de los 34 procesos TI la administración podrá identificar:

- El desempeño real de la empresa—Dónde se encuentra la empresa hoy
- El estatus actual de la industria—La comparación
- El objetivo de mejora de la empresa—Dónde desea estar la empresa

**Modelo genérico de madurez 0 No existente.** Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.

**1 Inicial.** Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques *ad hoc* que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

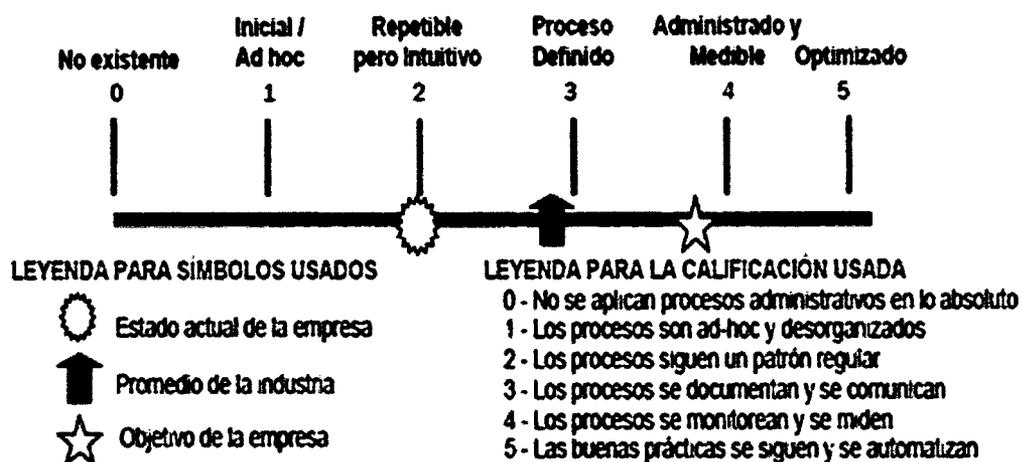
**2 Repetible.** Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

**3 Definido.** Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

**4 Administrado.** Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

**5 Optimizado.** Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de **mejoras continuas** y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

## CUADRO N° 9: NIVEL DE MADUREZ DE LOS PROCESOS SEGÚN EL MARCO DE TRABAJO DE COBIT



Fuente: COBIT 4.1 [Pag.18]

### 2.3.4.6 Medición del Desempeño

Se definen **metas** a nivel de Negocio, TI, Proceso y Actividad. Se definen **métricas** a nivel de negocio, de TI y de proceso. Se utilizan dos tipos de métrica:

- Indicadores clave de metas (KGI) □□ indican (después del hecho) si un proceso ha alcanzado o no sus requerimientos de negocio.
- Indicadores clave de desempeño (KPI) □□ indican cómo se está desempeñando un proceso (si será factible o no alcanzar la meta).

### 2.3.4.7 Marco de Trabajo General de COBIT:

El modelo de procesos de COBIT compuesto de 4 dominios que contienen 34 procesos genéricos, administrando los **recursos** de TI para proporcionar **información** al negocio de acuerdo con los requerimientos del negocio y de gobierno. MONITOREAR Y EVALUAR ME1 Monitorear y evaluar el desempeño de TI. ME2 Monitorear y evaluar el control interno ME3 Garantizar cumplimiento regulatorio. ME4 Proporcionar

gobierno de TI. PLANEAR Y ORGANIZAR PO1 Definir el plan estratégico de TI. PO2 Definir la arquitectura de la información PO3 Determinar la dirección tecnológica. PO4 Definir procesos, organización y relaciones de TI. PO5 Administrar la inversión en TI. PO6 Comunicar las aspiraciones y la dirección de la gerencia. PO7 Administrar recursos humanos de TI.

PO8 Administrar calidad. PO9 Evaluar y administrar riesgos de TI PO10 Administrar proyectos. ADQUIRIR E IMPLANTAR AI1 Identificar soluciones automatizadas. AI2 Adquirir y mantener el software aplicativo. AI3 Adquirir y mantener la infraestructura tecnológica AI4 Facilitar la operación y el uso. AI5 Adquirir recursos de TI. AI6 Administrar cambios. AI7 Instalar y acreditar soluciones y cambios.

ENTREGAR Y DAR SOPORTE DS1 Definir y administrar niveles de servicio. DS2 Administrar servicios de terceros. DS3 Administrar desempeño y capacidad. DS4 Garantizar la continuidad del servicio. DS5 Garantizar la seguridad de los sistemas. DS6 Identificar y asignar costos. DS7 Educar y entrenar a los usuarios. DS8 Administrar la mesa de servicio y los incidentes. DS9 Administrar la configuración. DS10 Administrar los problemas. DS11 Administrar los datos. DS12 Administrar el ambiente físico. DS13 Administrar las operaciones.

## **2.4 Método de Costeo ABC**

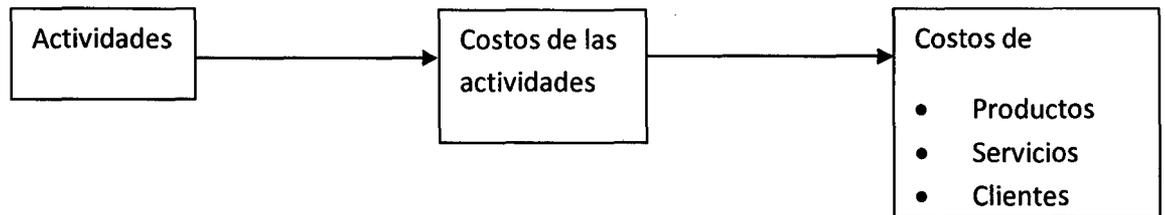
### **2.4.1 Sistema De Costeo Basados en Actividades (ABC)**

Una de las mejores herramientas para el mejoramiento de un sistema de costeo es el costeo basado en actividades. El costeo basado en actividades (ABC) mejorará un sistema de costeo al identificar las actividades individuales como los objetos de costos fundamentales. Una actividad es un evento, una tarea o una unidad de trabajo que tiene un propósito especificado, por ejemplo el diseño de productos, la

configuración de las máquinas, la operación de las máquinas y la distribución de productos. De una manera más informal, las actividades son verbos: Algo que hace una empresa. Para ayudar a la toma de decisiones estratégicas, los sistemas ABC identifican las actividades de todas las funciones de la cadena de valor, calculan los costos de las actividades individuales y asignan los costos a los objetos de costos, como productos y servicios, con base en la mezcla de actividades necesarias para producir cada producto o servicio.

Objetos de costos fundamentales

Asignación a otros objetos de costos



***Fuente: Contabilidad de costo; Charles T. Horngren;Srikant M. Datar;Madhav V.Rajan;Décima edición[pag 147]***

Consideraciones en la implementación de los sistemas de costos basados en actividades

Los gerentes eligen el nivel de detalle que habrán de usar en un sistema de costos mediante la evaluación de los costos esperados del sistema, contra los beneficios proyectados que resultarían por mejores decisiones. Hay signos reveladores acerca de cuándo es probable que un sistema ABC proporcione los mayores beneficios. A continuación se presentan algunos de tales signos:

- Se aplican cantidades significativas de costos indirectos usando uno o dos grupos comunes de costos.

- Todos los costos indirectos o la mayoría de ellos se identifican como costos a nivel de unidades de producción (un número pequeño de costos indirectos se describen como costos a nivel de lote, costos de mantenimiento del producto, o costos de mantenimiento de las instalaciones).
- Los productos ejercen exigencias diversas sobre los recursos debido a las diferencias en volumen, pasos del proceso, tamaño de los lotes o complejidad.
- Los productos que una compañía está bien preparada para elaborar y vender muestran utilidades pequeñas; en tanto que los productos que una compañía está menos preparada para elaborar y vender muestran utilidades significativas..
- El personal de operaciones tiene un desacuerdo sustancial con los costos reportados para la manufactura y la comercialización de los bienes y los servicios.

Cuando una compañía decide implementar un sistema ABC, tiene que hacer importantes elecciones en relación con el nivel de detalle que se usará. ¿Debería elegir muchos generadores de costos, actividades y grupos comunes de costos especificados de una manera detallada, o sería suficiente con unos cuantos?

Los costos y las limitaciones principales de un sistema ABC son las mediciones que se necesitan para implementarlo. Los sistemas ABC requieren que la administración estime los costos de los grupos comunes de actividades, y que identifique y mida los generadores de costos para que estos grupos comunes sirvan como base de aplicación de los costos. Incluso los sistemas ABC básicos requieren de muchos cálculos para determinar los costos de los productos y los servicios. Estas mediciones son costosas. Las tasas de los costos de las actividades también necesitan actualizarse con regularidad.

A medida que los sistemas ABC se vuelven más detallados y se crean más grupos comunes de costos, se requieren más aplicaciones para calcular los costos de las actividades en cada uno de los grupos. Ello aumenta las probabilidades de identificar incorrectamente los costos de diferentes grupos comunes de costos de las actividades. Por ejemplo, los supervisores son más proclives a identificar incorrectamente el tiempo que utilizan en diferentes actividades, cuando tienen que asignar su tiempo a cinco actividades en vez únicamente a dos.

En ocasiones, las compañías también se ven obligadas a usar ciertas bases de aplicación para las cuales los datos son fáciles de obtener, en vez de utilizar la base de aplicación que les hubiera gustado. Por ejemplo, una compañía podría verse obligada a usar el número de cargas desplazadas, en vez del grado de dificultad y la distancia de las diferentes cargas que se han movilizadas, como la base aplicación para los costos por el manejo de materiales, dado que los datos acerca del grado de dificultad y las distancias de las movilizaciones son difíciles de obtener.

Cuando se usan bases erróneas para la aplicación de los costos, la información de los costos de las actividades quizá resulte engañosa. Si el costo por carga movilizada disminuye, por ejemplo, una empresa concluirá que se ha vuelto más eficiente en sus operaciones de manejo de materiales. De hecho, el costo más bajo por carga movilizada podría haber sido resultado únicamente del hecho de desplazar cargas más ligeras a lo largo de distancias más cortas.

#### **2.4.2 Conceptos en Acción Defensa Exitosa De un Sistema Abc**

La implementación exitosa de los sistemas ABC requiere más que tan solo comprender los detalles técnicos. La implementación de un sistema

ABC representa a menudo un cambio significativo en un sistema de costeo y, como se indica se requiere que un gerente haga elecciones importantes en cuanto a la definición de las actividades y nivel de detalle.

#### Requisitos para una Sistema ABC

¿Cuáles son algunas de las cuestiones del comportamiento ante las cuales el contador administrativo debería mostrarse sensible?

1. Obtención del apoyo de alta gerencia y creación de un sentido de urgencia para el esfuerzo del sistema ABC. Esto requiere que los contadores administrativos desarrollen visión para el proyecto ABC y que comuniquen con claridad sus beneficios estratégicos (por ejemplo, los mejoramientos resultantes en el diseño del producto y del proceso).

También requiere que se venda la idea a los usuarios finales y que se trabaje con miembros de otros departamentos como asociados de negocios de los gerentes, en las diversas áreas afectadas por el proyecto ABC. En el USAA Federal Savings Bank, por ejemplo, los gerentes de proyectos demostraron la manera en que la información obtenida del sistema ABC daría luz acerca de la deficiencia de las operaciones bancarias, lo cual no estaba disponible anteriormente. Ahora, el área de finanzas se comunica de manera regular con las operaciones acerca de los nuevos reportes y los cambios propuestos al paquete de información financiera que los gerentes reciben.

2. Creación de una coalición de gerentes orientada a lo largo de toda la cadena de valor en favor del esfuerzo ABC. Los sistemas ABC miden la manera en que se utilizan los recursos de una organización. Los gerentes son responsables de estos recursos, tienen el mejor conocimiento acerca de las actividades y de los generadores de costos. Lograr que los gerentes cooperen y que tomen la iniciativa para la

implementación de un sistema ABC es esencial para obtener el talento requerido, la credibilidad adecuada y el liderazgo necesario.

La obtención de una mayor participación de los gerentes tiene otros beneficios. Es probable que los gerentes que se sienten más implicados en el proceso comprometan más tiempo al esfuerzo ABC y que sean menos escépticos ante el mismo. La intervención de los gerentes a lo largo de toda la cadena de valor también crean mayores oportunidades de coordinación y de cooperación en las diferentes funciones, como por ejemplo, diseño y manufactura.

3. Educación y Capacitación de los empleados en el Sistema ABC como base para la delegación de autoridad (empowerment) entre los empleados. La diseminación de la información acerca de un sistema ABC por toda la organización permite que los trabajadores de todas las áreas de una empresa usen sus conocimientos de los sistemas ABC para realizar mejoras. Por ejemplo, WS Industries, un fabricante de aislantes con sede en la India, no solamente compartió la información ABC con sus trabajadores, sino que también estableció un plan de incentivos que daba a los empleados un porcentaje de los ahorros en costos. Los resultados fueron espectaculares porque los empleados se les delegó autoridad y se les motivó para implementar diversos proyectos para obtener ahorros en costos.

4. Búsqueda de pequeños éxitos a corto plazo, como prueba de que la implementación del sistema ABC está dando resultados. Con demasiada frecuencia, los gerentes y los contadores administrativos buscan resultados notorios y cambios importantes con demasiada rapidez. En muchas situaciones, es difícil lograr un cambio significativo de la noche a la mañana. Sin embargo, el hecho de mostrar la manera en que la información ABC ha ayudado a mejorar un proceso y ahorrar en costos,

aunque sea tan solo de una forma modesta, alienta al equipo a permanecer en el rumbo correcto y ganar impulso. La credibilidad que se logra gracias a las pequeñas victorias conduce a mejoramientos adicionales y más grandes, donde intervienen un mayor número de individuos de diferentes áreas de la organización. Finalmente, el ABC y el ABM (activity based management) quedan arraigados en la cultura de la organización. Compartir con los demás los éxitos a corto plazo ayuda a motivar a los empleados para que sean innovadores.

5. Reconocimiento de que la información ABC no es perfecta, ya que dicha información equilibra la necesidad de una mejor información contra los costos por crear un sistema complejo que pocos gerentes y empleados logran entender. El contador administrativo debe ayudar a los gerentes a reconocer tanto el valor como las limitaciones del sistema ABC y no debe intentar venderlo sobrevaluado. Una comunicación abierta y honesta acerca de un sistema ABC asegura que los gerentes lo usen de una manera juiciosa para tomar buenas decisiones. De este modo, se podrían hacer juicios trascendentales sin incurrir en controversias, así como formular preguntas desafiantes para ayudar a impulsar mejores decisiones sobre el sistema.

## CAPITULO III

### **METODOS Y PROCEDIMIENTOS**

#### **3.1 Tipo y Diseño de la Investigación**

La presente investigación es de tipo aplicada, por cuanto se utilizó la tecnología de software libre LTSP en un conjunto de equipos de cómputo. El diseño del estudio es de tipo cuasi-experimental con dos grupos equivalentes. Se ha seleccionado este tipo de diseño porque esta investigación se desarrolló en una institución educativa, donde no se puede tener un control total de las condiciones experimentales. Siendo recomendable el uso de diseño cuasi-experimentales por haber contado con grupos intactos, no elegidos al azar.

Grupo experimental:	O1	X	O2
Grupo control :	O3	X	O4

El diseño planteado consistió en una pre-evaluación de la variable dependiente a ambos grupos (O1 y O3), luego en el Centro de Tecnología de Información - laboratorio experimental se aplicó el tratamiento experimental y en el otro laboratorio se mantuvo su infraestructura tecnológica tradicional. Al final se aplicó una post-evaluación a ambos laboratorios.

El trabajo realizado en el Centro de Tecnología de Información -laboratorio experimental consistió en la instalación, configuración e implantación de la tecnología LTSP, por un periodo de tres (03) meses se llevó un seguimiento de los costos asociados al trabajo de instalación y administración.

En el laboratorio de control no se efectuó ningún cambio en su configuración.

### **3.2 Población y muestra**

La Población está conformada por:

1500 estudiantes de la Carrera Profesional de Ingeniería de Sistemas.

5 Laboratorios de cómputo operativos con un total de 150 computadoras y 1 laboratorio de 20 equipos que fueron dados de baja.

La muestra de estudiantes fue tomada de los alumnos que estuvieron matriculados en el curso de sistemas operativos (20 alumnos).

Respecto a la muestra de equipos informáticos, se tomaron 20 equipos Pentium IV, los mismos que fueron separados en dos grupos:

**Grupo 1 :** 10 equipos en los que se aplicó LTSP

**Grupo 2:** 10 equipos en los que se mantuvo una configuración tradicional de Computadoras de escritorio con procesamiento independientes.

### **3.3 Técnicas e Instrumentos de Recolección de Datos**

- Encuestas
- Monitoreo
- Reportes de soporte técnico
- Documental: Flujo de Caja

## CAPITULO IV

### RESULTADOS DE LA INVESTIGACIÓN

#### 4.1 Benchmarking entre LTSP y un centro de cómputo tradicional

##### A. Ahorro de costos en software.

LTSP es gratuito, lo que supone un ahorro importante de costes en licencias. De este modo, no se tuvo que efectuar pago alguno por dicho concepto, del mismo modo el sistema operativo y aplicaciones que incluyen las distribuciones de Linux Ubuntu.

Asimismo, incorporando LTSP a los escritorios es posible añadir una gran cantidad de aplicaciones para un entorno académico, profesional o doméstico sin coste económico.

---

##### B Ahorro de costos en hardware

LTSP, al estar especialmente ideado para el aprovechamiento de ordenadores que, con los sistemas operativos y aplicaciones actuales, han quedado obsoletos. Permitió además la incorporación de terminales especialmente diseñados para este tipo de arquitecturas. Estos equipos suponen un ahorro que oscila entre el 50% y el 60% respecto del coste de un PC normal promedio.

A esto hay que unir el hecho de que los requerimientos técnicos del servidor son superiores a los de otros respecto a la memoria RAM. No obstante, el coste global del servidor es mucho menor que en sistemas

tradicionales de servicios centralizados usando software propietario, ya que este tipo de software tradicionalmente requiere más recursos o que el funcionamiento de un Centro de Tecnología de Información que funciona de manera tradicional.

---

### **C La administración centralizada del sistema**

Puesto que los procesos no se ejecutan en los terminales sino en el servidor, que además alberga el software y los datos, la administración de un sistema LTSP se reduce a la administración de un sólo equipo: "el servidor". En tal sentido el número de horas que debe dedicarse al mantenimiento y configuraciones desciende drásticamente, se simplifica la administración del sistema y de los datos, y se aumenta el control en todos los sentidos. Si a las ventajas anteriores sumamos el ahorro en mano de obra cualificada por este concepto, así como las mejoras en simplicidad y seguridad.

### **D Código Fuente**

GNU/Linux y el proyecto LTSP ofrecen su código fuente en todo momento, lo cual posibilita que si alguien desea aportar con el proyecto o si requiere corregir algún error, lo podrá hacer sin necesidad de tener que comprar ninguna licencia. Lo contrario pasa con Windows en sus versiones Cliente / Servidor, porque aun se adquiriese el licenciamiento, no se podrá tener acceso al código fuente.

### **E Compatibilidad de Sistema de Archivos**

Windows solo puede montar particiones con sistemas de archivos Microsoft, al respecto se tendría que instalar software adicional que permita hacerlo, en cambio con Linux no es necesario, toda vez que reconoce diferentes sistemas de archivos.

## **F Continuidad de Servicio**

Con la plataforma Linux - LSTP no se reportaron incidentes con virus informáticos por parte de los usuarios, por el contrario el sistema operativo les permitió detectar y eliminar directamente los virus de sus dispositivos externos, diferentes particiones y unidades de red.

Al realizar un análisis económico se verificó claramente que el sistema LTSP es más óptimo que el sistema actual tanto el corto como en el largo plazo.

## **G Compatibilidad con los sistemas propietarios**

LTSP hace posible desde cada terminal realizar conexiones a servidores de diversas plataformas, como pueden ser Windows 2003 o Solaris. Por tanto, es posible utilizar LTSP para trabajar con aplicaciones bajo esas y otras plataformas. Dicho de otro modo, se trata de una tecnología ideal para entornos multiplataforma.

---

## **H Movilidad y accesibilidad**

La sencillez en la configuración de red de un sistema de terminales permite a los usuarios acceder a su espacio de trabajo desde cualquier terminal de la red, puesto que sus datos, al igual que el propio sistema, se encuentran centralizados en el servidor. Esto evita tener que configurar soluciones de directorio o sistemas de almacenamiento centralizados en entornos de bajo requerimiento técnico e inversión reducida.

---

## **I Soporte y mantenimiento**

Puesto que el sistema es altamente centralizado, es posible dar un soporte y mantenimiento remoto de alta calidad sin que los costes se disparen. Así, tanto la cantidad de horas que debe dedicarse a esta labor como su escasa complejidad, hacen factible, desde el punto de vista económico y técnico, externalizar el servicio de soporte y mantenimiento.

## **J Multitud de aplicaciones disponibles**

Existen infinidad de aplicaciones libres en el mercado que satisfacen las necesidades de la mayor parte de los usuarios en entornos laborales. En caso de necesitar una aplicación propietaria que funcione bajo otra plataforma, debido a lo comentado con anterioridad, es posible que, usando LTSP, todos los usuarios puedan acceder a ella. Por tanto, es factible disponer de multitud de nuevas aplicaciones libres sin renunciar a aplicaciones propietarias de otras plataformas.

---

## **K Escalabilidad**

Los sistemas LTSP son altamente escalables. Aumentando el número de servidores o la potencia de los mismos, es posible aumentar drásticamente el número de clientes. Se han desarrollado soluciones de clústering (granjas de servidores que funcionan "como uno sólo") para escalar el sistema asegurando su fiabilidad. Es posible incorporar portátiles a la infraestructura y equipos conectados a través de redes inalámbricas. Asimismo, ya existen protocolos que permiten conexiones WAN (externas, desde puntos lejanos) al sistema.

---

## **L Seguridad**

Gracias a las ventajas que ofrece GNU/Linux, los usuarios tienen pocas posibilidades de alterar el software más allá de sus propios datos y configuraciones. Esto implica que el sistema es estable frente a errores o acciones nocivas provocadas. Los usuarios no podrán instalar aplicaciones o alterar archivos de compañeros, por ejemplo. Además, los sistemas linux son inmunes a virus, por lo que se reduce a cero una de las principales causas de fallos. Todo esto implica un mayor ahorro en costes de mantenimiento.

---

## **M Fiabilidad frente a fallos**

LTSP puede configurarse como sistema de alta disponibilidad con sencillez. Esto tiene tres ventajas:

1. Se obtienen fuertes mejoras de prestaciones sin disparar el precio.
2. En caso de fallo, la reparación es menos costosa.
3. En caso de fallo, el sistema permanece en producción con prestaciones cercanas al 100% de manera automática, sin intervención técnica.

De esta manera, podemos establecer periodos de respuesta a fallos realmente cortos, con lo que la fiabilidad del sistema es muy superior a la de sistemas con arquitectura tradicional basada en PC.

---

## **N Personalización**

Otra de las ventajas importantes, inherente del software libre, es la posibilidad de personalización extrema. Así, el aspecto visual y usabilidad del entorno puede definirse a gusto del cliente, es posible establecer entornos personalizados en función del perfil del usuario (diferentes tamaños, colores, iconos, entorno gráfico, escritorio, etc.). Son conocidos los entornos diseñados para niños pequeños o para personas con deficiencias visuales.

---

## **O Extensa documentación**

Si hay algo que caracteriza a los sistemas GNU/Linux es la gran oferta y gratuidad de los manuales y guías para usuarios y técnicos. Existe documentación de cualquier aplicación o utilidad que incorporemos al sistema (gran parte en inglés, eso sí).

---

## P Sistema plurilingüe

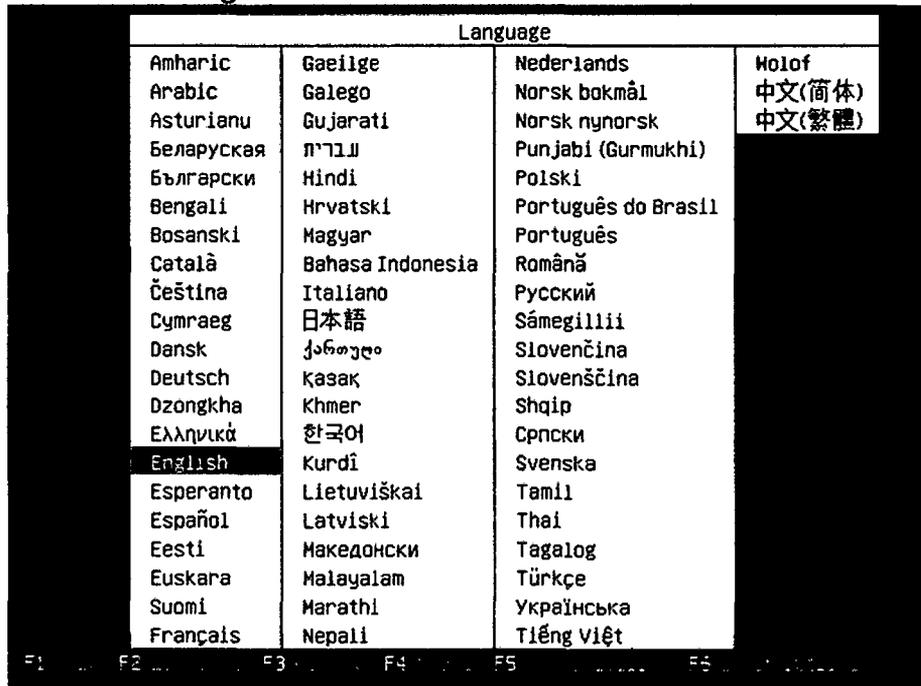
Especial mención debe realizarse sobre la elección del idioma, puesto que los sistemas GNU/Linux permiten que el usuario elija el idioma del escritorio y las aplicaciones fácilmente. De este modo, el entorno puede convertirse en plurilingüe. Allí donde trabajen personas que hablen diferente lengua, como aulas de informática de colegios o centros de acceso libre, GNU/Linux representa una ventaja competitiva determinante.

### 4.2 Implantación de LTSP

Procedimiento efectuado para la instalación de Ubuntu LTSP

Procedimiento efectuado para la instalación de Ubuntu LTSP

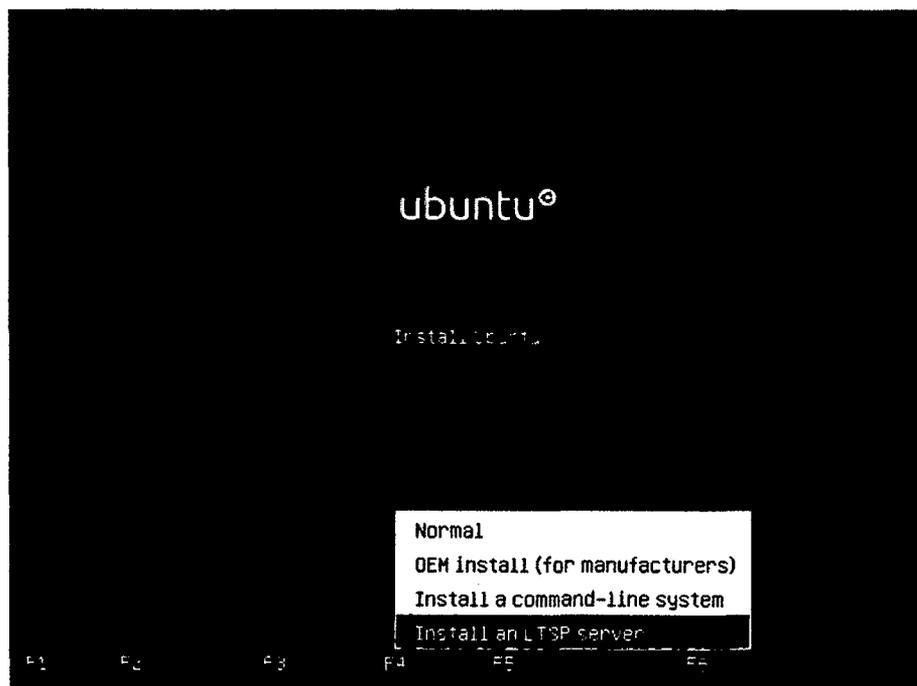
1. Descargar el "Alternate Install CD" de la versión seleccionada de Ubuntu. En este caso se ha utilizado Ubuntu 10.04.
2. Iniciar el servidor desde el CD descargado. La primera pantalla obtenida es la siguiente:



3. Seleccionar el idioma y dar "Enter"



4. Usando la tecla F4, entrar a la lista de Modos de instalación:
5. Seleccionar "Install an LTSP Server" y dar enter.



6. Dar "Enter" en "Install Ubuntu" y esperar que inicie

## 7. Seleccionar el idioma a instalar y dar "Enter":

[!] Choose language

Please choose the language used for the installation process. This language will be the default language for the final system.

Choose a language:

C	- No localization	↑
Albanian	- Shqip	
Arabic	- عربي	
Asturian	- Asturianu	
Basque	- Euskara	
Belarusian	- Беларуская	
Bosnian	- Bosanski	
Bulgarian	- Български	
Catalan	- Català	
Chinese (Simplified)	- 中文(简体)	
Chinese (Traditional)	- 中文(繁體)	
Croatian	- Hrvatski	
Czech	- Čeština	
Danish	- Dansk	
Dutch	- Nederlands	↓

<Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons

## 8. Seleccionar el país y dar "Enter":

[!] Choose language

Based on your language, you are probably located in one of these countries or regions.

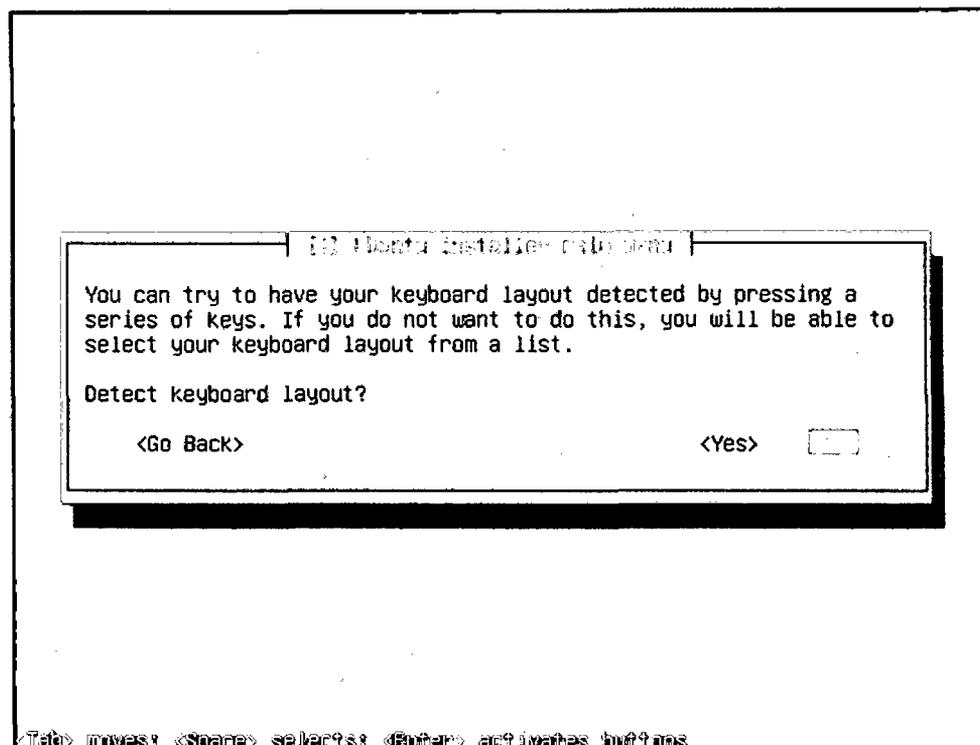
Choose a country, territory or area:

- Antigua and Barbuda
- Australia
- Botswana
- Canada
- Hong Kong
- India
- Ireland
- New Zealand
- Nigeria
- Philippines
- Singapore
- South Africa
- United Kingdom
- Zimbabwe
- other

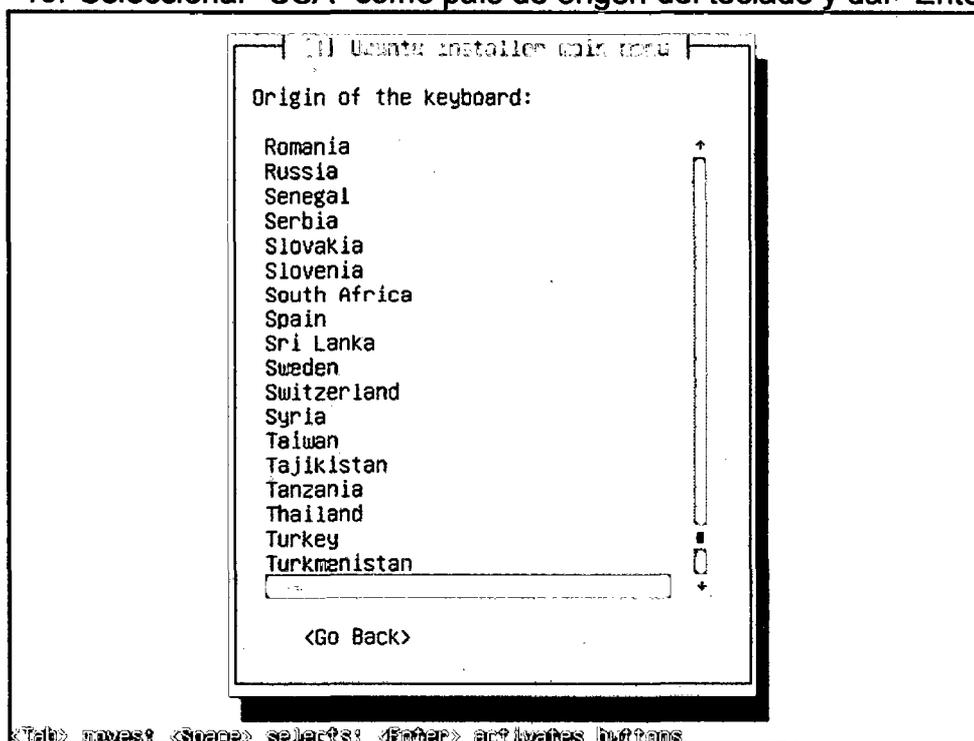
<Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons

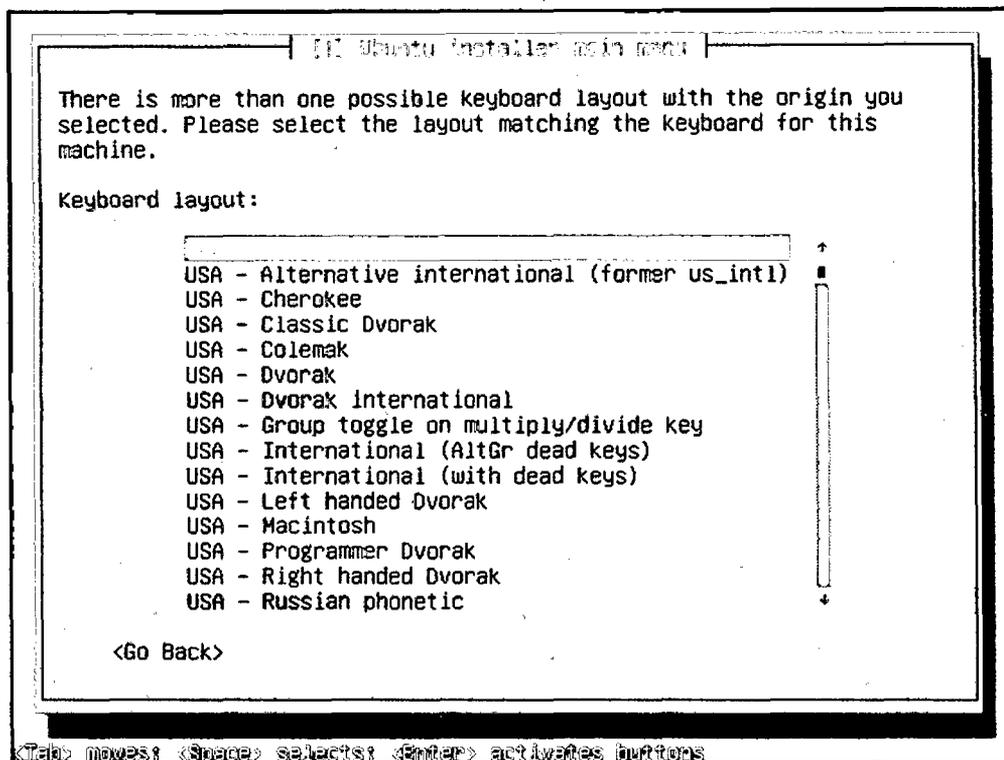
## 9. Indicar que no detecte distribución del teclado, ya que realmente no es necesario para el servidor y dar "Enter":



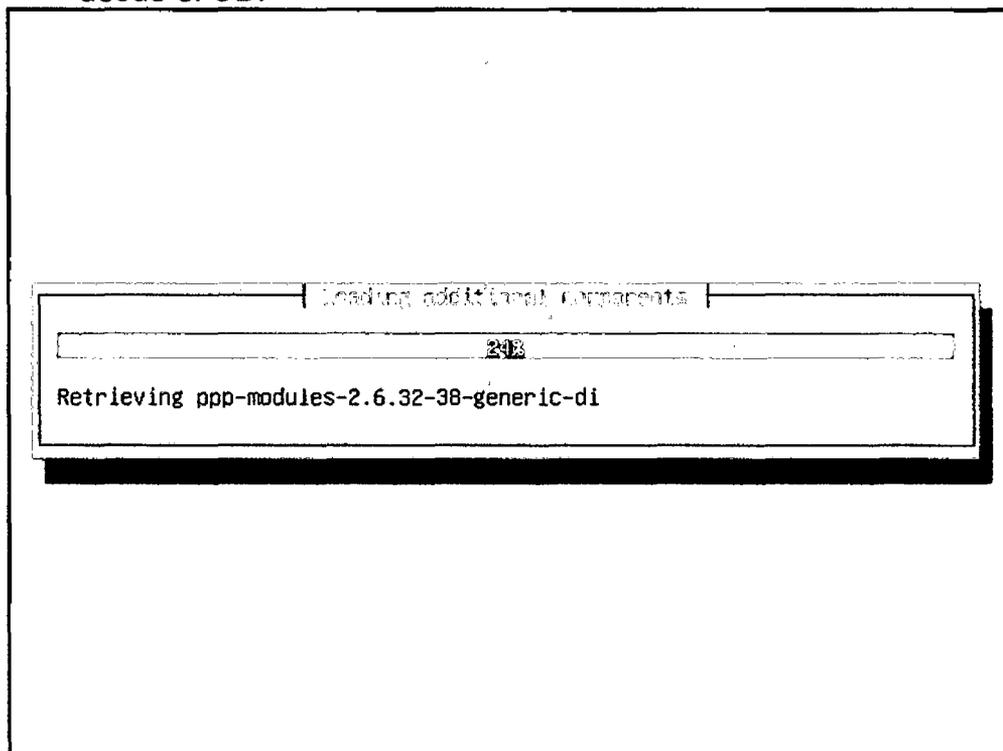
10. Seleccionar "USA" como país de origen del teclado y dar "Enter":



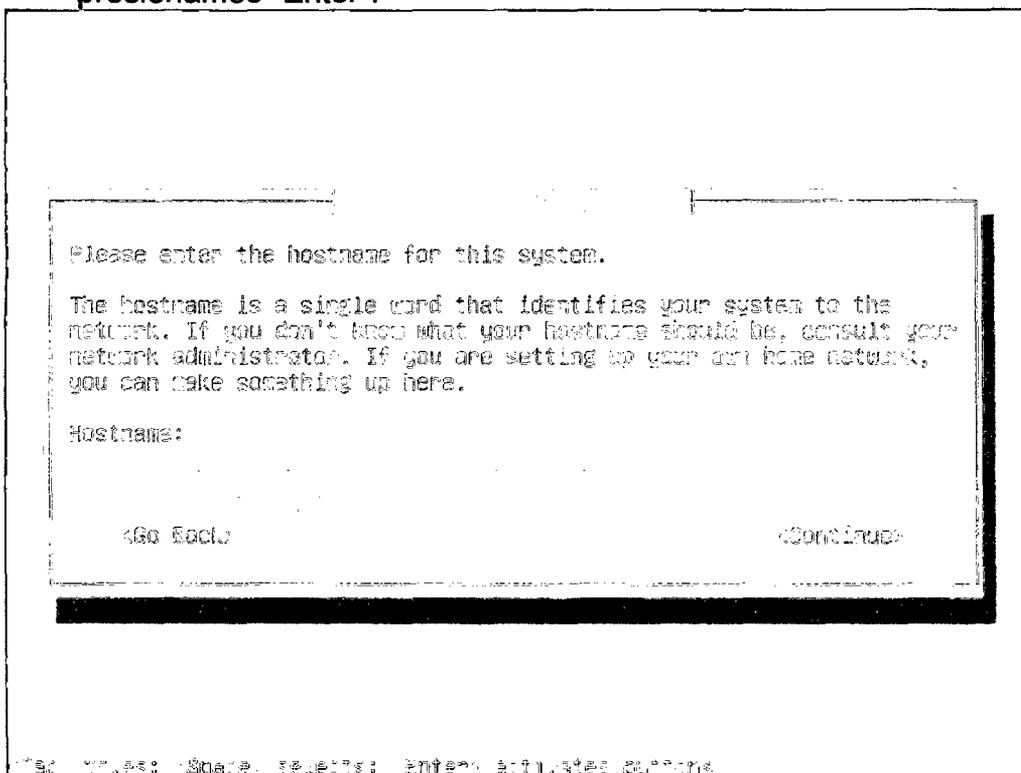
11. Seleccionar la distribución del teclado predeterminada y dar "Enter":



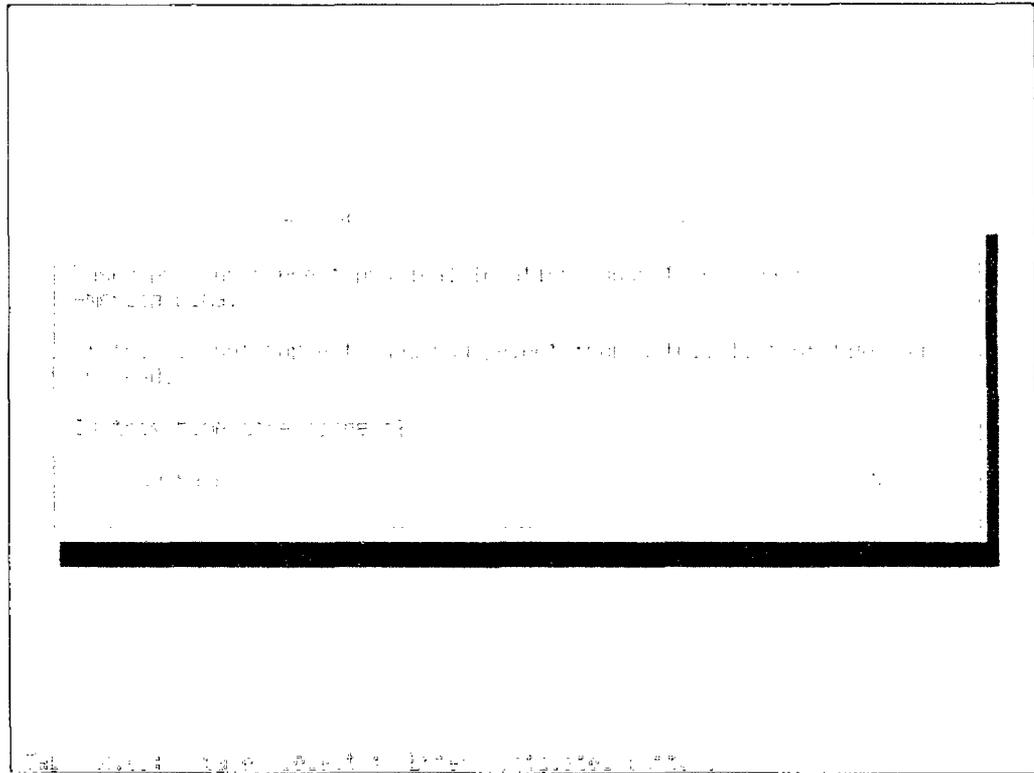
12. El sistema comienza a detectar hardware y cargar listado de paquetes desde el CD:



13. Después de unos momentos, ingresamos el nombre del host y presionamos "Enter":



14. El instalador ahora nos sugiere la zona horaria en la que nos encontramos. Usualmente es la correcta, así que seleccionamos "Yes" y damos "Enter":



15. Ahora nos toca seleccionar como queremos particionar el disco. Este es un tema bastante extenso, pero para este ejemplo, seleccionamos "Guided – Use entire disk" y damos "Enter":

[1] Partition disks

The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.

Partitioning method:

Guided - use entire disk and set up LVM  
 Guided - use entire disk and set up encrypted LVM  
 Manual

<Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons

**16. Seleccionamos el disco donde vamos a instalar y damos "Enter":**

[1] Partition disks

Note that all data on the disk you select will be erased, but not before you have confirmed that you really want to make the changes.

Select disk to partition:

...

<Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons

17. Aceptamos la propuesta de particionamiento seleccionado "Yes" y dando "Enter":

```
If you continue, the changes listed below will be written to the
disks. Otherwise, you will be able to make further changes manually.

The partition tables of the following devices are changed:
SCSI3 (0,0,0) (sda)

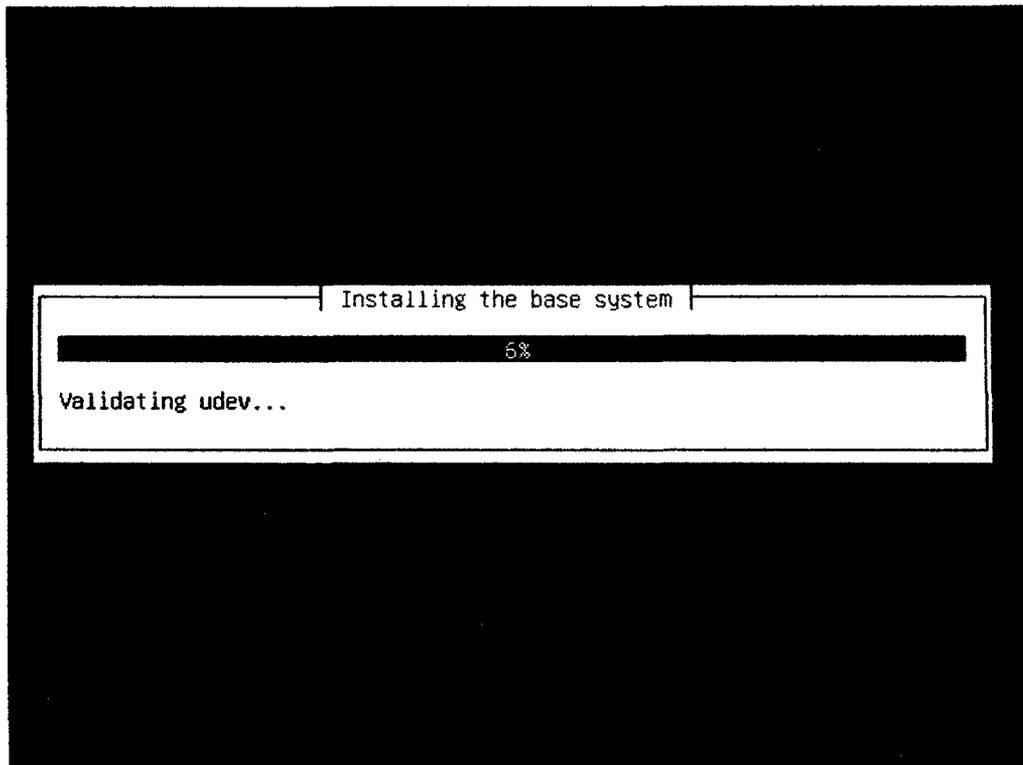
The following partitions are going to be formatted:
partition #1 of SCSI3 (0,0,0) (sda) as ext4
partition #5 of SCSI3 (0,0,0) (sda) as swap

Write the changes to disks?

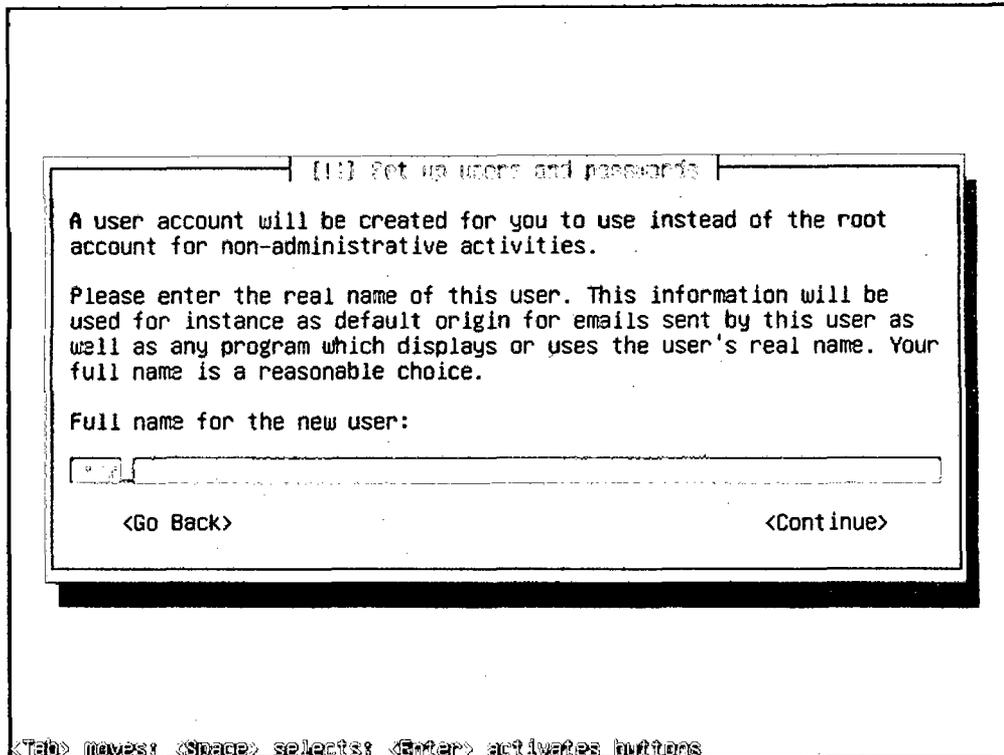
<Y>
```

Tab: Home: Ctrl + PageUp: Enter: Alt+Ctrl+PageUp

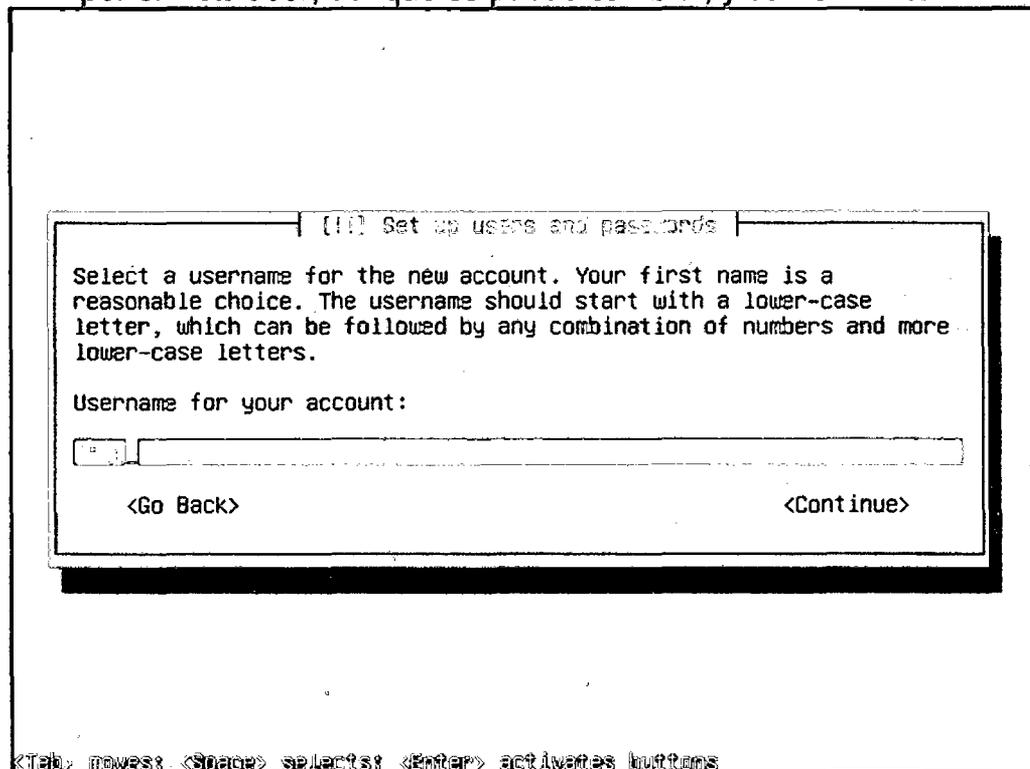
18. Luego de unos segundos creando las particiones, el instalador va a instalar el sistema base. Solo esperamos a que termine:



19. Luego de terminado de instalar el sistema base, el instalador nos pide el nombre de un usuario a crear. Para este ejemplo le ponemos "ltsp" y damos "Enter":



20. Luego ingresamos el username de ese usuario, usualmente lo sugerido por el instalador, aunque se puede cambiar, y damos "Enter":



21. Ingresamos el password que deseamos y damos "Enter":

[1] Set up users and passwords

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

Choose a password for the new user:

<Tab> moves; <Space> selects; <Enter> activates buttons

22. Ingresamos nuevamente el password para verificar que lo escribimos correctazos y le damos "Enter":

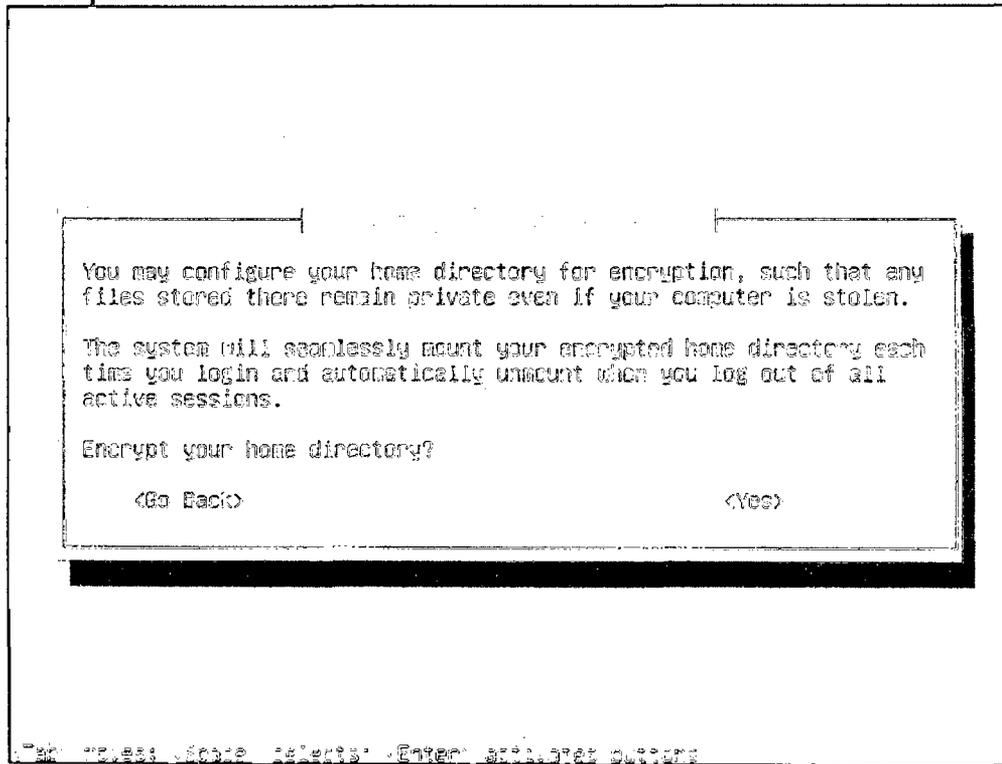
[1] Set up users and passwords

Please enter the same user password again to verify you have typed it correctly.

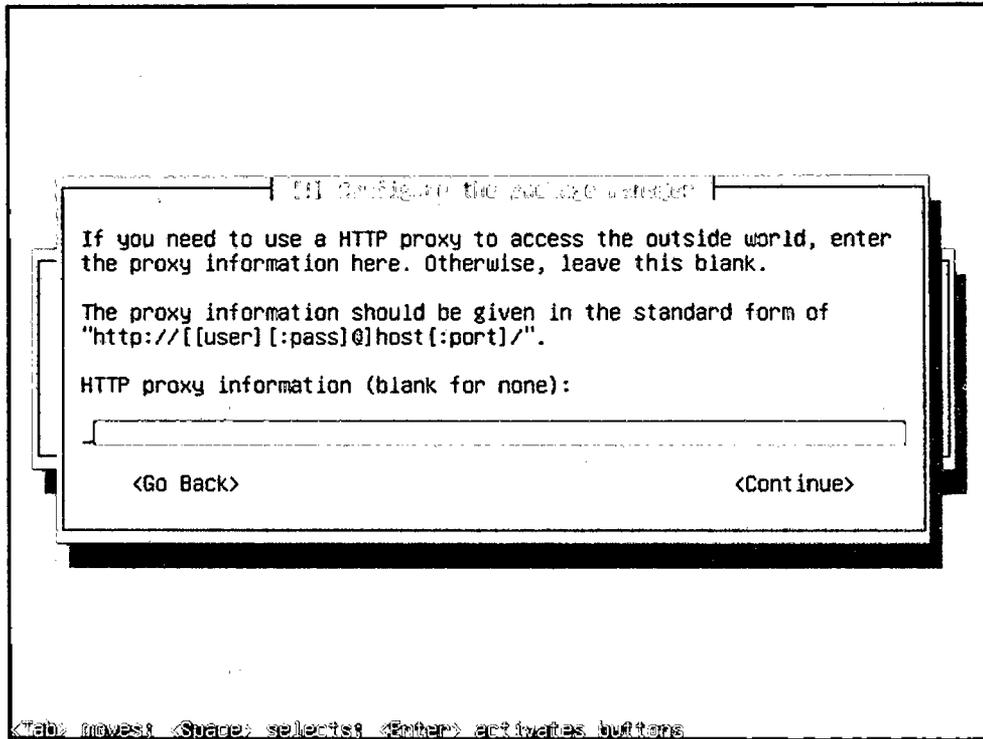
Re-enter password to verify:

<Tab> moves; <Space> selects; <Enter> activates buttons

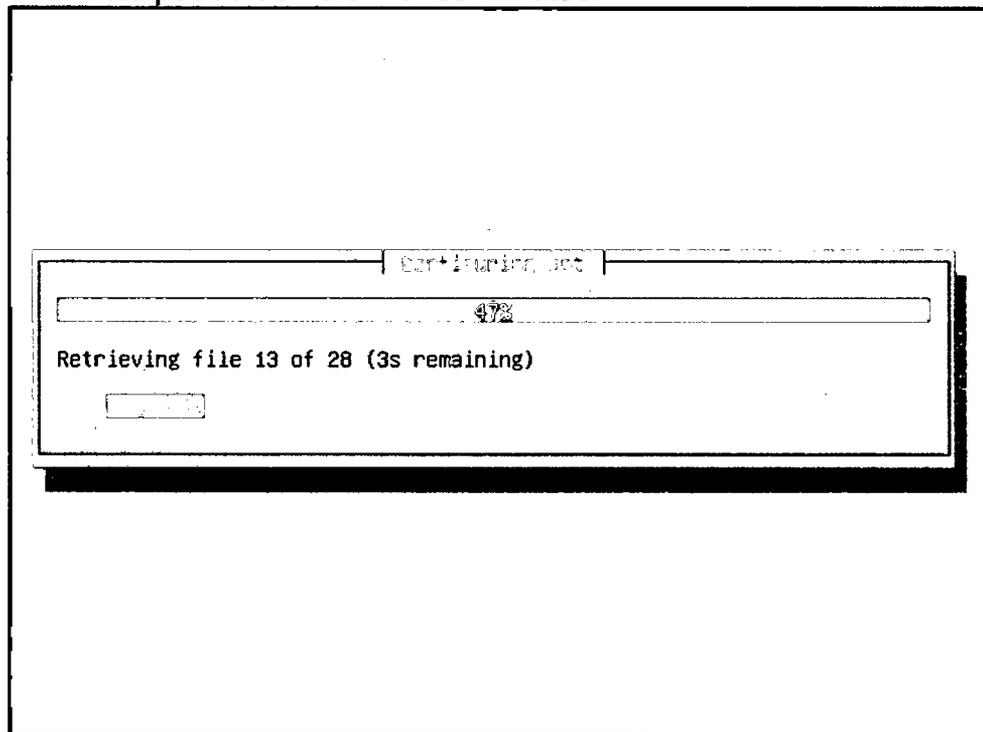
23. A la pregunta de si desea encriptar el directorio home, le respondamos que no:



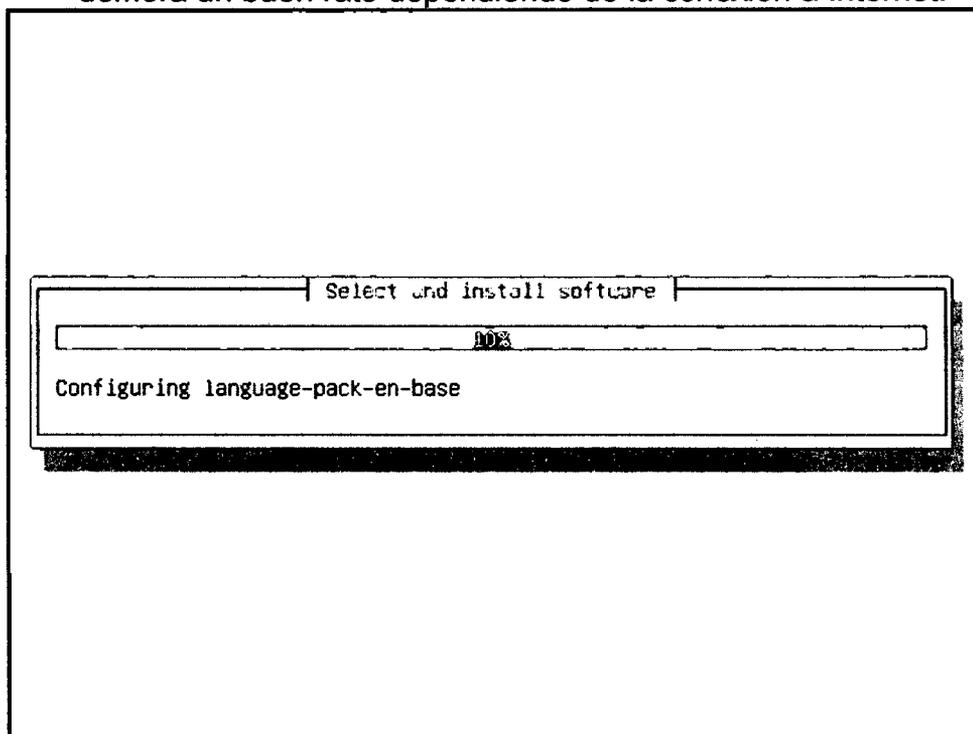
24. El instalador ahora nos pide si deseamos utilizar un servidor Proxy. Normalmente no es el caso y lo dejamos en blanco y damos "Enter":



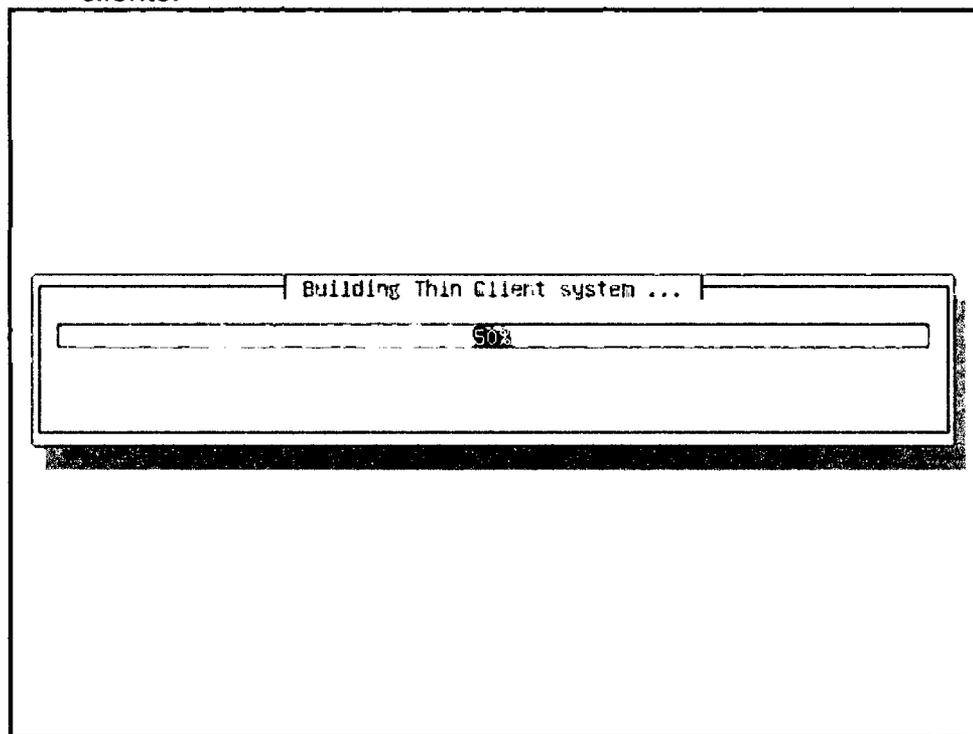
25. El instalador comienza a descargar la lista de paquetes desde Internet. Esto puede demorar varios minutos:



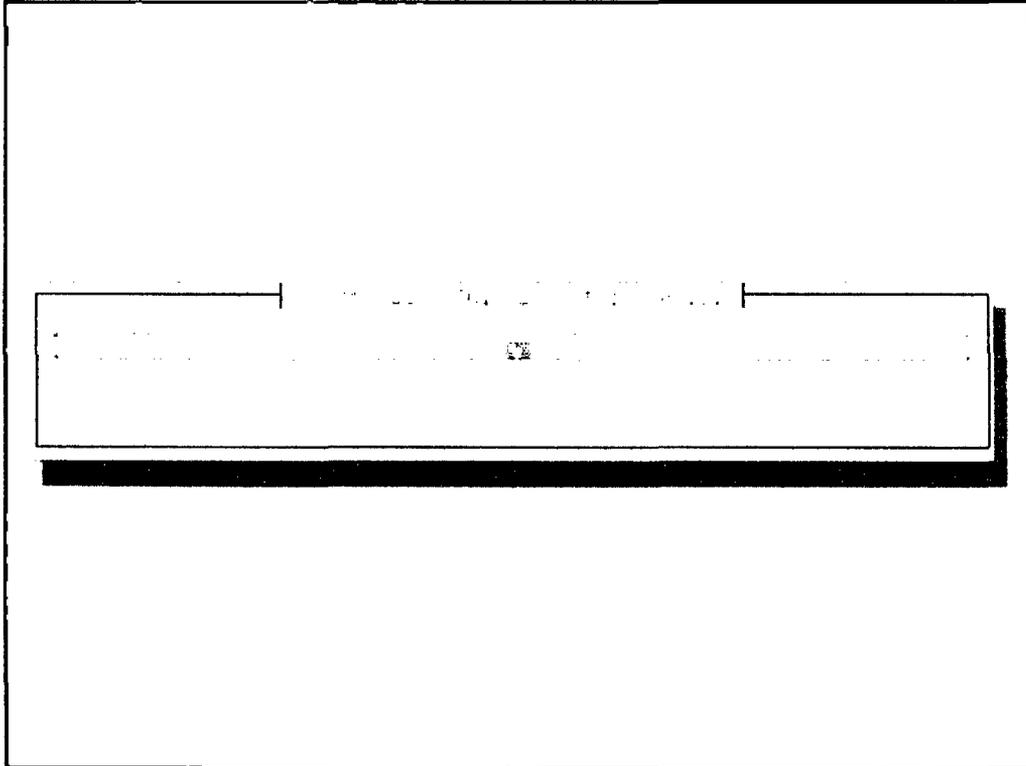
26. Luego el instalador comienza a instalar paquetes desde Internet. Esto si demora un buen rato dependiendo de la conexión a Internet:



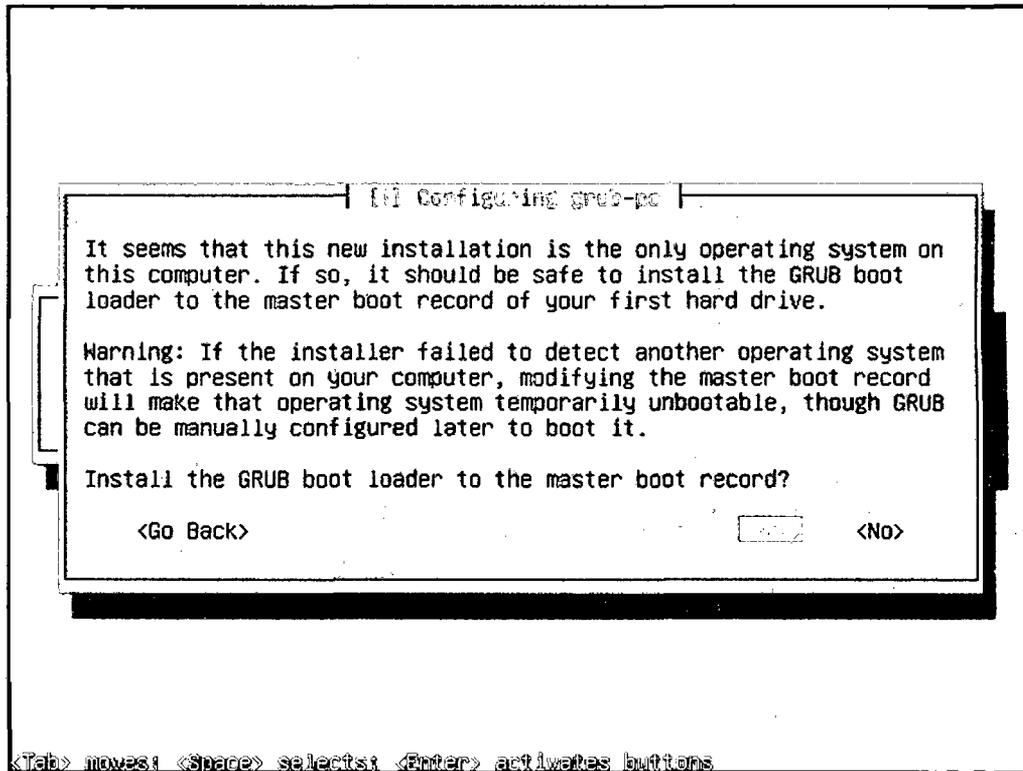
27. Una vez terminado esto, el instalador crea el sistema para los thin-clients:



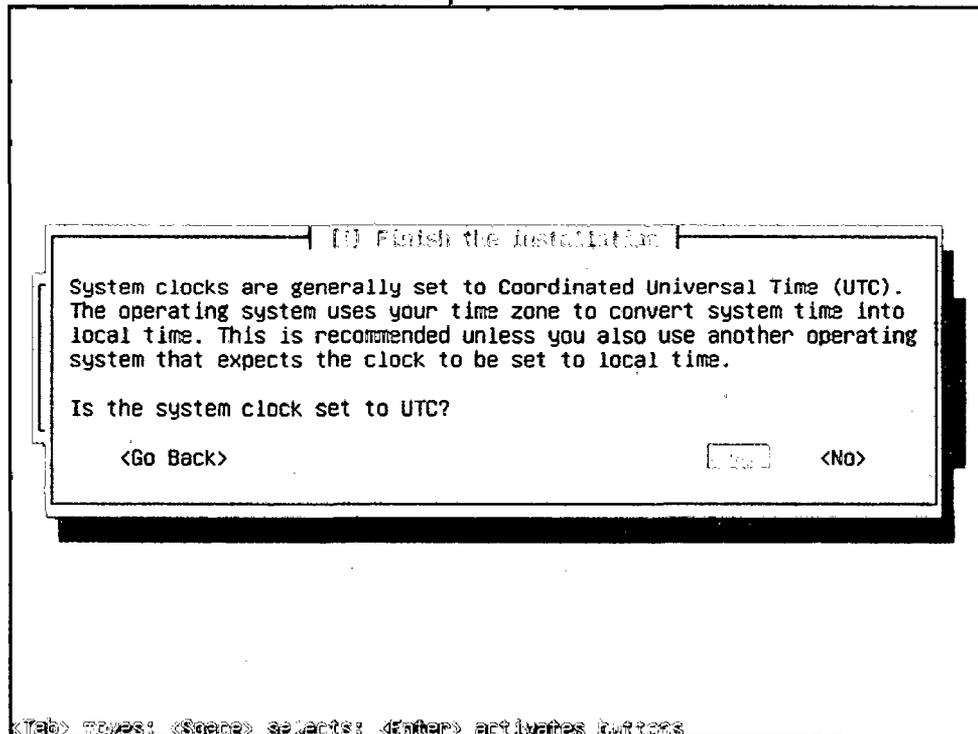
28. Luego sale la siguiente pantalla:



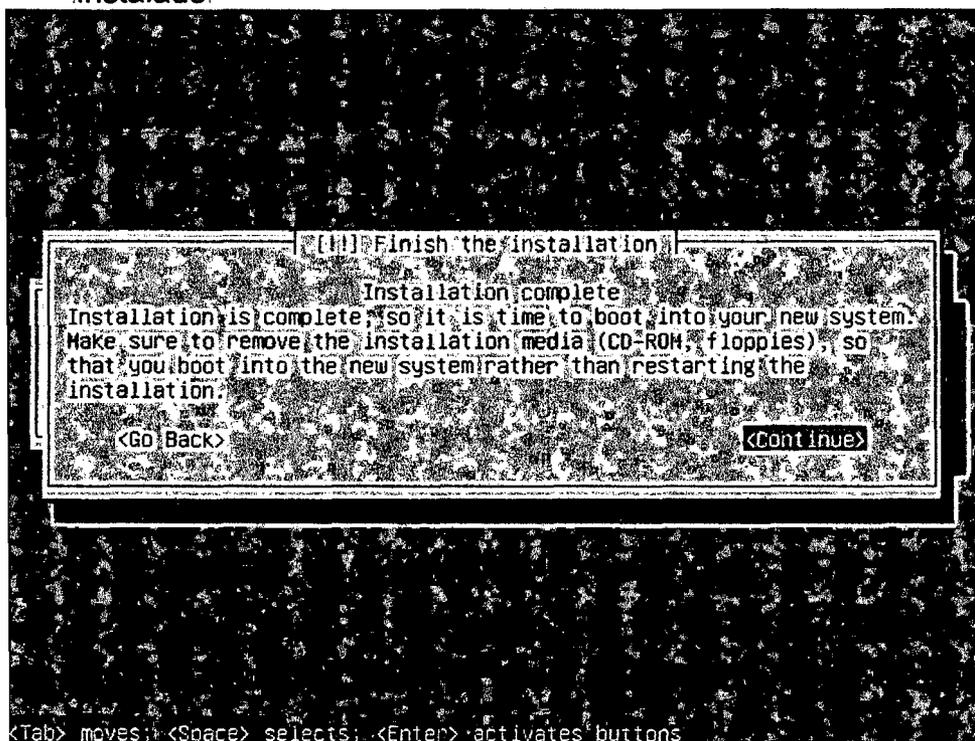
29. Luego nos sale una pantalla donde nos pregunta si deseamos instalar GRUB en el MBR, le respondemos "Yes":



30. El instalador nos pregunta si el reloj de la máquina está configurado en UTC. Normalmente la respuesta es "No".



31. Instalación finalizada! Solo se le da 'Continue' y reinicia al servidor ya instalado.



## Ficheros de configuración asociados a los servicios de LTSP

### **/etc/ltsp/dhcpd.conf**

```
#
Default LTSP dhcpd.conf config file.
#
authoritative;

subnet 192.168.0.0 netmask 255.255.255.0 {
 range 192.168.0.20 192.168.0.250;
 option domain-name "example.com";
 option domain-name-servers 192.168.0.1;
 option broadcast-address 192.168.0.255;
 option routers 192.168.0.1;
next-server 192.168.0.1;
get-lease-hostnames true;
 option subnet-mask 255.255.255.0;
 option root-path "/opt/ltsp/amd64.tmp";
 if substring(option vendor-class-identifier, 0, 9) = "PXEClient" {
 filename "/ltsp/amd64.tmp/pxelinux.0";
 } else {
 filename "/ltsp/amd64.tmp/nbi.img";
 }
}
```

### **/etc/inetd.conf**

```
/etc/inetd.conf: see inetd(8) for further informations.
#
Internet superserver configuration database
#
#
Lines starting with "#:LABEL:" or "#<off>#" should not
be changed unless you know what you are doing!
#
If you want to disable an entry so it isn't touched during
package updates just comment it out with a single '#' character.
#
Packages should modify this file by using update-inetd(8)
#
<service_name> <sock_type> <proto> <flags> <user> <server_path> <args>
#
#:INTERNAL: Internal services
#discard stream tcp nowait root internal
#discard dgram udp wait root internal
#daytime stream tcp nowait root internal
```

```

#time stream tcp nowait root internal

#STANDARD: These are standard services.

#BSD: Shell, login, exec and talk are BSD protocols.

#MAIL: Mail, news and uucp services.

#INFO: Info services

#BOOT: TFTP service is provided primarily for booting. Most sites
run this only on machines acting as "boot servers."

#RPC: RPC based services

#HAM-RADIO: amateur-radio services

#OTHER: Other services

9571 stream tcp nowait nobody /usr/sbin/tcpd /usr/sbin/ldminfod
9572 stream tcp nowait nobody /usr/sbin/tcpd
/usr/sbin/nbdswapd
2000 stream tcp nowait nobody /usr/sbin/tcpd /usr/sbin/nbdrootd
/opt/ltsp/images/amd64.img

```

### **/etc/ltsp/ltsp-update-image.conf**

```

Configuration file for ltsp-update-image

By default, do not compress the image
as it's reported to make it unstable
NO_COMP="-noF -noD -noI -no-exports"

```

### **/var/lib/tftpboot/ltsp/amd64/pxelinux.cfg/default**

```

default ltsp
label ltsp
kernel vmlinuz
append ro initrd=initrd.img quiet splash nbdport=2000

```

#### 4.3 Evaluación de Resultados (Económica)

##### CUADRO N° 4: COSTO DE IMPLEMENTACIÓN Y ADMINISTRACIÓN DE UN LABORATORIO DE 15 COMPUTADORAS BAJO LTSP.

Cantidad	Detalle	C. Unitario \$	C.Total \$
15	Equipo de cómputo P4 con 256 MB de RAM, con tarjeta de red sin disco duro	100.00	1500.00
1	Servidor IBM 3200Dual Core con 4GB de RAM y un disco duro de 200GB	800.00	800.00
	Costo de Licencia de Sistema Operativo	0.00	0.00
<b>TOTAL \$</b>			<b>2300.00</b>

*Fuente: Elaboración propia en base a cotizaciones del mercado*

#### ANÁLISIS COMPARATIVO ENTRE SISTEMAS EXISTENTES Y EL SISTEMA PROPUESTO

El costo de implementación de un Centro de Cómputo convencional es el siguiente:

##### CUADRO N° 5: INVERSIÓN REQUERIDA EN CASO SE OPTE POR TECNOLOGÍAS LIBRES EN CENTROS DE CÓMPUTO

Cantidad	Detalle	C. Unitario \$	C. Total \$
15	Computador Core2Duo de 3.00 con 2GB de RAM y un disco duro de 160GB	700.00	10500.00
15	Licencia del Sistema Operativo Windows	100.00	1500.00
<b>TOTAL \$</b>			<b>12000.00</b>

*Fuente: Elaboración propia en base a cotizaciones del mercado*

**CUADRO N° 6: FLUJO DE CAJA SEGÚN SISTEMAS CONVENCIONALES  
(Periodo de 6 meses)**

<b>Detalle</b>	<b>0</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
Computador Core2Duo de 3.00 con 2GB de RAM y un disco duro de 160GB	-700.00					
Licencia de Software del Sistema Operativo Windows	-15000.00	0.00	0.00	0.00	0.00	0.00
Costo de soporte técnico a nivel de software		-1500.00	1500.00	1500.00	1500.00	1500.00
<b>FLUJO DE CAJA \$</b>	<b>-15700.00</b>	<b>-1500.00</b>	<b>1500.00</b>	<b>1500.00</b>	<b>1500.00</b>	<b>1500.00</b>

*Fuente: Elaboración propia en base a cotizaciones del mercado y Cuadro N° 5.*

**CUADRO N° 7: FLUJO DE CAJA DE SISTEMA PROPUESTO (Periodo de 6 meses)**

Detalle	0	1	2	3	4	5
Costo de Licencia de Software (*)		0.00	0.00	0.00	0.00	0.00
10 Equipos reciclados	-1500.00					
1 Servidor IBM 3200 DualCore con 4GB de RAM , Disco Duro de 200 GB	-800.00					
Costo de soporte técnico a nivel de software (**)		- 1000.00	- 1000.00	- 1000.00	- 1000.00	- 1000.00
<b>FLUJO DE CAJA \$.</b>	<b>-2300.00</b>	<b>1000.00</b>	<b>1000.00</b>	<b>1000.00</b>	<b>1000.00</b>	<b>1000.00</b>

**Fuente: Elaboración propia en base a cotizaciones del mercado y Cuadros N°4.**

(\*) El costo por licencias de software no está presente dado que el software libre no requiere la adquisición de licencias de uso.

(\*\*)El costo de soporte es menor debido a la reducción de horas hombre de soporte en tareas de reinstalación de equipos.

## CONCLUSIONES Y RECOMENDACIONES

### CONCLUSIONES

1. Se ha demostrado que el proyecto propuesto es económicamente viable. Asimismo promoverá la utilización de software libre en la Universidad Peruana de Ciencias e Informática, hecho que permitirá expandir la visión de los estudiantes respecto a la investigación en esta área de conocimiento.
2. En relación a la comparación de rendimiento a nivel de sistema operativo la velocidad de procesamiento entre un CTI basado en LTSP con un CTI con equipos independientes Core2Duo con sistema Operativo Windows7, es similar; de la comparación efectuada a la velocidad de procesamiento de la Suit ofimática OpenOffice, se comprobó que dicho software es más eficiente bajo la tecnología LTSP.
3. La administración de un CTI basado en LTSP es más efectiva que la administración de un CTI convencional, el tiempo y costo asociado al trabajo del personal de soporte en efectuar tareas de reinstalación de equipos es 0, no se tiene problemas con virus informáticos, se proporciona a los docentes una herramienta que les permite monitorear y controlar remotamente el manejo que se haga en las terminales.

4. Existe incompatibilidad de con software propietario que solo corre sobre plataforma Windows, las empresa desarrolladoras de software CopyRight mantienen un monopolio del software que desarrollan, lo cual limita a la comunidad a ser simples usuarios finales.

## **RECOMENDACIONES**

1. Todo cambio requiere un proceso de adaptación, una migración es un proceso cuyo éxito depende de la capacitación inicial y el seguimiento que se haga hasta que los usuarios están familiarizados.
2. Se debería formar una Comunidad de Software Libre en la Universidad Peruana de Ciencias e Informática con la finalidad de poder capacitar e involucrar a más estudiantes y personal que labora en dicha casa de estudios, con al finalidad de concientizarlos sobre las ventajas de trabajar con tecnologías libres.
3. Se debería implementar un arreglo de discos duros con RAID en el servidor LTSP como buena práctica de seguridad de la información, con la finalidad de asegurar la continuidad del servicio en caso se presentes fallas físicas en el disco duro.
4. Es recomendable que las máquinas cliente tengan la misma arquitectura.

## BIBLIOGRAFÍA

1. **Mauricio Arregoces**, "Data Center Fundamentals " Macmillan Technical Pub , Hardcover;2003.
2. **Howard Schaeffer**, "Data center operations: a guide to effective planning, processing, and performance" Prentice-Hall, 1981.
3. **Eric Maillé y René Francois Mennecier**, "VMware vSphere 5 en el seno del Datacenter ", Eni Ediciones; 2012.
4. **Martin Graef, Reinald Greiller**, "Organization and management of a computer center", 2da Edición, Macmillan, 1985.
5. **Jesús Javier Estepa Nieto**, Investigación, "Software Libre en países envías de Desarrollo",2008,Madrid.
6. **García Valcárcel, Ignacio**,E-business colaborativo: cómo implantar Software Libre, Servicios Web y el Grid Computing para ahorrar costes y mejorar las comunicaciones en su empresa, 283 p. Madrid: Fundación Confemetal, 2003
7. **Wayner, Peter**, La ofensiva del software libre; como Linux y el movimiento del software libre se impusieron frente a los titanes de la alta tecnología , 239 p. Barcelona : Granica, 2001.
8. **Raya Cabrera, José Luis**, Guía de campo: máquinas virtuales 1a ed. , 239 p. México D. F. : Alfaomega, 2010.
9. **Ramos, Antonio Ángel**, Instala, administra, securiza y virtualiza entornos Linux 1a ed.
10. **Mena Ponce, Gustavo Eduardo**, Implementación de tecnologías de la información basadas en Linux para PyMEs.

11. **Bovet, Daniel P.** , Understanding the Linux Kernel 3a ed.
12. **aya González, Laura**, Sistemas informáticos multiusuario y en red.
13. **Martin, Michel**, De Windows a Linux : para distribuciones Red Hat y SuSE.
14. **O'Reilly**, Linux in a Windows World, O'Reilly Media, Inc. All rights reserved; 2005
15. **William E. Shotts, Jr.** "The Linux Command Line"; 2000-2012.
16. **Keir Thomas Ubuntu**, "Pocket Guide and Reference", © Copyright 2008 Ubuntu is a trademark of Canonical Ltd
17. **Machtelt Garrels**, "Bash Guide for Beginners" Garrels BVBA, Copyright (c); 2002-2007.
18. COBIT 4.1, **IT GOVERNANCE INSTITUTE**, [en línea].ISACA <[www.isaca.org](http://www.isaca.org)>
19. **Charles T. Horngren;Srikant, M. Datar;Madhav y V.Rajan**, Contabilidad de Costos; Décima Edición
20. <http://www.ltsp.org/> (2012,2011)
21. <http://www.k12linux.org/> (2011)
22. <http://en.opensuse.org/LTSP> (2010,2011,2013)
23. <https://help.ubuntu.com/community/UbuntuLTSP> (2012,2011)
24. <https://help.ubuntu.com/community/ThinClientHowto> (2012,2011)

## APÉNDICE 01

### Encuesta a estudiantes de la Carrera Profesional de Ingeniería de Sistemas de Informática, 2011-II

#### ENCUESTA A LOS USUARIOS DE LOS CTIs (LABORATORIOS) DE LA UPCI

1. La cantidad de horas de laboratorio asignadas por curso es adecuada?  
Si ( )                      No ( )
  
2. Durante el semestre ha tenido que compartir horas de laboratorio con otro grupo de alumnos (alumnos de otro curso) en el mismo horario?  
Si ( )                      No ( )
  
3. Se han producido cruces de horario para el uso del laboratorio?  
Si ( )                      No ( )
  
4. Durante el uso de los laboratorio ha tenido algún tipo de inconveniente:  
Virus Informático ( )  
Los aplicativos requeridos no están instalados oportunamente ( )  
Los equipos de cómputo presentan fallas a nivel de hardware ( )  
Los equipos presentan fallas a nivel de sistema operativo ( )  
Otros:  
.....

## APÉNDICE 02

### Entrevista realizada al personal de soporte técnico de los laboratorios de cómputo de la Universidad Peruana de Ciencias e Informática, 2011-II

#### ENTREVISTA EFECTUADA A LOS ADMINISTRADORES DE LOS CTI (LABORATORIOS) DE LA UPCI

1. Los usuarios reportan que los laboratorios no están disponibles cuando se los requiere; al respecto, indique, cuáles son los problemas que afectan la operatividad de los equipos de cómputo en los laboratorios?

Virus Informático ( )

Los aplicativos requeridos no están instalados oportunamente ( )

Los equipos de cómputo presentan fallas a nivel de hardware ( )

Los equipos presentan fallas a nivel de sistema operativo ( )

Otros:

.....  
.....

2. Durante el semestre ha observado que más de un grupo de alumnos (un curso) tenga asignado un mismo laboratorio a la vez?

Si ( )      No ( )

3. Durante el horario de clases: Lunes a viernes (6:00 pm a 10:30 pm) y sábados (2:00 pm a 8:00 pm) se tienen horas en las que los laboratorios no estén siendo utilizados?

Si ( )      No ( )

**APÉNDICE 03: Establecimiento de los Procesos de TI que requieren ser mejorados a partir de las Metas de TI, basado en el marco de trabajo de COBIT 4.1**

**CUADRO N° 01: ENLACE DE LAS METAS DE NEGOCIO A METAS DE TI**

Balance ScoreCard	Metas de Negocio	Metas de TI										Criterios de Información de COBIT					
		2	14	17	18	19	20	21	22	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiable	
PERSPECTIVA FINANCIERA	2 Gestionar los riesgos de TI que afecten al negocio.	2	14	17	18	19	20	21	22		x						
PERSPECTIVA DEL CLIENTE	4 Mejorar la orientación y servicio al cliente	3	23							x							
	6 Establecer continuidad y disponibilidad de servicios.	10	16	22	23					x			x				
PERSPECTIVA INTERNA	8 Lograr optimizar el coste de entrega de servicios	7	8	10	24						x						
	10 Mejorar y mantener funcionalidad de procesos de negocio	6	7	11						x	x						
	11 Reducir el coste de los procesos	7	8	13	15	24					x						
	14 Gestionar los cambios del Negocio.	1	5	6	11	28				x	x						
PERSPECTIVA DE APRENDIZAJE Y CRECIMIENTO	15 Mejorar y Mantener productividad operacional y de persona	7	8	11	13					x	x						
	16 Gestionar productos e innovación de negocios	5	25	28						x	x						

Fuente: Construcción propia en base a l diagnóstico y COBIT 4.1: Apéndice 4 Tablas entre Metas y Procesos

**APÉNDICE 04: Determinación de las Metas de TI a partir de las Metas del Negocio, basado en el marco de trabajo de COBIT 4.1**

*Criterios de Información*

Metas de TI		Procesos de TI											Criterios de Información			
		PO1	PO2	PO4	PO10	AI1	AI6	AI7	DS1	DS3	ME1	P	P	S	S	
1	Asegurar la satisfacción del usuario final con la oferta de servicio y niveles de servicio	PO1	PO2	PO4	PO10	AI1	AI6	AI7	DS1	DS3	ME1	P	P	S	S	
3	Asegurar la satisfacción del usuario final con la oferta de servicio y niveles de servicio	PO8	AI4	DS1	DS2	DS7	DS8	DS10	DS13			P	P	S	S	
5	Crear agilidad de TI	PO2	PO4	PO7	AI3							P	P	S		
6	Definir como la funcionalidad de negocio y requerimientos de control se traslada en soluciones efecticiennemente automatizada	AI1	AI2	AI6												
7	Adquirir y mantener sistemas de aplicación integrados y estandarizados	PO3	AI2	AI5								P	P		S	
8	Adquirir y mantener una infraestructura de TI integrada y estandarizada	AI3	AI5									S	P			
11	Asegurar la integración sin fisuras de las aplicaciones dentro de los procesos del negocio.	PO2	AI4	AI7								P	P	S	S	
12	Asegurar la transparencia y compromiso de costes de TI, beneficios, estrategias, políticas y niveles de servicio.	PO5	PO6	DS1	DS2	DS6	ME1	ME4				P	P		S	
13	Asegurar el uso apropiado y desempeño de las soluciones de aplicación y tecnología	AI6	AI4	AI7	DS7	DS8						P	S			
15	Optimizar la infraestructura, recursos y capacidades de TI	PO3	AI3	DS3	DS7	DS9						S	P			
20	Asegurar que las transacciones de negocio automatizadas y los cambios a la información son confiables.	PO6	AI6	DS5	DS12							P		P	S	
22	Asegurar el mínimo impacto de negocio en caso de una interrupción de servicios de TI o cambios en el negocio.	PO8	AI7	DS4								P	S	S	P	
23	Estar seguros que los servicios de TI están disponibles según se requiere	DS3	DS4	DS8	DS13							P	P		P	
24	Mejorar la eficiencia de costos de TI y sus contribuciones a la rentabilidad del negocio	PO5	DS8									S	P		S	
25	Entregar proyectos a tiempo y sobre presupuesto, reuniendo los estándares de calidad	PO8	PO10									P	P	S	S	
28	Asegurar que TI demuestra la eficiencia de costos de la calidad de servicio, mejora continua y disposición para cambios futuros	PO5	DS6	ME1	ME4							P	P		P	

Fuente: Construcción propia en base a diagnóstico y COBIT 4.1: Apéndice I: Equivalencias entre Metas de TI con los Procesos de TI de COBIT, y los criterios de información sobre los cuales se basa la meta de TI.

**APÉNDICE N° 05**  
**MATRIZ DE CONSISTENCIA**

FORMULACIÓN DEL PROBLEMA	OBJETIVOS DE LA INVESTIGACIÓN	HIPÓTESIS
<p><b>Problema General</b></p> <p>¿En qué medida la utilización software libre minimiza los costos asociados a la implementación y administración de un Centro de Tecnología de Información en una universidad peruana?</p>	<p><b>Objetivo general</b></p> <p>Utilizar software libre para minimizar los costos asociados a una adecuada a la implementación y administración de un Centro de Tecnología de Información utilizando Software Libre en la Universidad Peruana de Ciencias e Informática.</p>	<p><b>Hipótesis General</b></p> <ul style="list-style-type: none"> <li>• El uso de software libre minimiza los costos de funcionamiento de un Centro Tecnológico de Información en la Universidad Peruana de Ciencias e Informática.</li> </ul>
<p><b>Problemas Específicos</b></p> <ul style="list-style-type: none"> <li>• ¿E s Posible prolongar el tiempo de vida útil de equipos de cómputo de escritorio con el empleo de software libre?</li> <li>• ¿De qué manera se puede cuantificar los beneficios de utilizar software libre en la implementación y administración de un Centro de Tecnología de Información?</li> </ul>	<p><b>Objetivos específicos</b></p> <ul style="list-style-type: none"> <li>• Aplicar la tecnología LTSP para reutilizar equipos de cómputo de baja performance.</li> <li>• Elaborar un benchmarking entre el funcionamiento de equipos y costos asociados antes y después de la implementación de software libre en un Centro de Tecnología de información en una universidad peruana.</li> </ul>	<p><b>Hipótesis Específicas</b></p> <ul style="list-style-type: none"> <li>• La aplicación del Software Libre-LTSP, posibilita reutilizar equipos de cómputo de baja performance.</li> <li>• Es factible efectuar un benchmarking del funcionamiento y costo de implementación de software libre en un Centro de Tecnología de información de la Universidad Peruana de Ciencias e Informática.</li> </ul>

**Anexo 01**  
**Librerías de trabajo de COBIT versiones 4.1 y 5**

# APÉNDICE I

## TABLA DE ENLACES ENTRE METAS Y PROCEDIMIENTOS.

Este apéndice brinda una visión global de cómo se relacionan las metas genéricas del negocio con las metas de TI con los procesos de TI y con los criterios de información. Se proporcionan tres tablas:

1. La primera tabla muestra las equivalencias de las metas del negocio, de acuerdo al balanced scorecard, con las metas de TI y con los criterios de información<sup>1</sup>. Esto ayuda a mostrar, para una meta genérica de negocios determinada, las metas de TI que por lo general dan soporte a esta meta, y los criterios de información de COBIT que se relacionan con la meta del negocio.
2. La segunda tabla muestra las equivalencias de las metas de TI con los procesos de TI de COBIT, así como los criterios de información sobre los cuales se basa la meta de TI<sup>2</sup>.
3. La tercera tabla proporciona un mapeo inverso que muestra para cada proceso de TI, las metas de TI que son soportadas.

Las tablas ayudan a demostrar el alcance de COBIT y la relación general de negocio entre COBIT y los impulsores del negocio, permitiendo así establecer la equivalencia entre las metas típicas de negocio, por medio de las metas de TI, y los procesos de TI requeridos para darles soporte. Las tablas se basan en metas orgánicas y, por lo tanto, se deben usar como guía y adaptarse a la empresa determinada.

Para proporcionar una liga hacia los criterios de información usados para los requisitos de negocio de la 3ª edición de COBIT, las tablas también contienen una indicación de los criterios de información más importantes soportados por el negocio y por las metas de TI.

---

### Notas:

<sup>1</sup> Los criterios de información contenidos en la gráfica de metas de negocio se basan en un agregado de los criterios para las metas de TI relacionadas y en una evaluación subjetiva de aquellos que son más relevantes para la meta del negocio. No se hizo el intento para indicar si son primarios o secundarios. Estos son tan solo indicativos y los usuarios pueden seguir un proceso similar al evaluar sus propias metas de negocio

<sup>2</sup> Las referencias primarias y secundarias de los criterios de información en la gráfica de metas de TI se basan en un agregado de los criterios para cada proceso de TI y en una evaluación subjetiva de qué es primario y qué es secundario para la meta de TI., debido a que algunos procesos tienen mayor impacto en la meta de TI que otros. Estos son tan solo indicativos y los usuarios pueden seguir un proceso similar al evaluar sus propias metas de TI

# Apendice I – Tablas de Enlace Entre Metas y Procesos

## ENLACE DE LAS METAS DE NEGOCIO A PROCESOS DE TI

Criteria de Información de COBIT

	Metas de Negocio	Metas de TI										Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiablez
		24	28															
<b>Perspectiva Financiera</b>	1 Proporcionar un buen retorno de inversión de TI-permitiendo inversión en negocio	24	28										✓					
	2 Gestionar los riesgos de TI que afecten a negocio	2	14	17	18	19	20	21	22				✓	✓	✓			
	3 Mejorar gobierno corporativo y transparencia	2	18															✓
<b>Perspectiva del cliente</b>	4 Mejorar la orientación y servicio al cliente	3	23										✓					
	5 Ofrecer productos y servicios competitivos.	5	24										✓	✓				
	6 Establecer continuidad y disponibilidad de servicios	10	16	22	23								✓			✓		
	7 Crear agilidad en la respuesta a los cambios de los requerimientos de negocio	1	5	25									✓	✓				
	8 Lograr optimización de costes de la entrega de servicios	7	8	10	24									✓				
	9 Obtener información fiable y útil para tomar decisiones estratégicas	2	4	12	20	26							✓			✓		✓
<b>Perspectiva Interna</b>	10 Mejorar y mantener funcionalidad de procesos de negocio	6	7	11									✓	✓				
	11 Reducir el coste de los procesos	7	8	13	15	24								✓				
	12 Proporcionar cumplimiento con leyes externas, regulaciones y contratos	2	19	20	21	22	26	27							✓			✓
	13 Proporcionar cumplimiento con políticas internas	2	13												✓			✓
	14 Gestionar cambios de negocio	1	5	6	11	28							✓	✓				
	15 Mejorar y mantener productividad operacional y de personal	7	8	11	13									✓	✓			
<b>Perspectiva de Aprendizaje y Crecimiento</b>	16 Gestionar productos e innovación de negocio.	5	25	28									✓	✓				
	17 Adquirir y mantener personal cualificado y motivado	9											✓	✓				

ENLACE DE LAS METAS DE TI A PROCESOS DE TI

Criterios de Información de CobIT

Metas de TI	Procesos											Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiablez
	P01	P02	P04	P010	AI1	AI6	AI7	DS1	DS3	ME1								
1 Responder a requerimientos de negocio alineado con la estrategia de negocio	P01	P02	P04	P010	AI1	AI6	AI7	DS1	DS3	ME1		P	P	S	S			
2 Responder a los requerimientos de gobierno en línea con la dirección ejecutiva	P01	P04	P010	ME1	ME4							P	P					
3 Asegurar la satisfacción del usuario final con la oferta de servicios y niveles de servicio	P08	AI4	DS1	DS2	DS7	DS8	DS10	DS13				P	P	S	S			
4 Optimizar el uso de la información	P02	DS11										S	P			S		
5 Crear agilidad de TI	P02	P04	P07	AI3								P	P	S				
6 Definir como la funcionalidad de negocio y requerimientos de control se trasladan en soluciones efectivas y	AI1	AI2	AI6									P	P			S		
7 Adquirir y mantener sistemas de aplicación integrados y estandarizados	P03	AI2	AI5									P	P			S		
8 Adquirir y mantener una infraestructura de TI integrada y estandarizada	AI3	AI5										S	P					
9 Adquirir y mantener habilidades de TI que responden a la estrategia de TI	P07	AI5										P	P					
10 Asegurar la satisfacción mutua de relaciones con terceras partes	DS2											P	P	S	S	S	S	
11 Asegurar la integración sin fisuras de las aplicaciones dentro de los procesos del negocio	P02	AI4	AI7									P	P	S	S			
12 Asegurar la transparencia y comprensión de costes de TI, beneficios, estrategia, políticas y niveles de servicio	P05	P06	DS1	DS2	DS6	ME1	ME4					P	P			S	S	
13 Asegurar el uso apropiado y desempeño de las soluciones de aplicación y tecnológica	P06	AI4	AI7	DS7	DS8							P	S					
14 Tener en cuenta y proteger todos los activos de TI	P09	DS5	DS9	DS12	ME2							S	S	P	P	P	S	
15 Optimizar la infraestructura, recursos y capacidades de TI	P03	AI3	DS3	DS7	DS9							S	P					
16 Reducir los defectos de la solución y entrega de servicio y reelaborar	P08	AI4	AI6	AI7	DS10							P	P	S	S			
17 Proteger el logro de los objetivos de TI	P09	DS10	ME2									P	P	S	S	S	S	
18 Establecer la claridad del impacto de negocio de los riesgos a los objetivos y recursos de TI	P09											S	S	P	P	P	S	
19 Asegurar que la información crítica y confidencial se retiene a aquellos que no deben tener acceso	P06	DS5	DS11	DS12									P	P	S	S	S	
20 Asegurar que las transacciones de negocio automatizadas y los cambios a la información son confiables	P06	AI7	DS5									P		P	S	S		
21 Asegurar que los servicios de TI y la infraestructura pueden resistir apropiadamente y recuperar de fallos debidos a errores, ataques deliberados o desastres.	P06	AI7	DS4	DS5	DS12	DS13	ME2					P	S	S	P			
22 Asegurar el mínimo impacto de negocio en caso de una interrupción de servicios de TI o cambios	P06	AI6	DS4	DS12								P	S	S	P			
23 Estar seguros que los servicios de TI están disponibles según se requiere	DS3	DS4	DS8	DS13								P	P		P			
24 Mejorar la eficiencia de costes de TI y sus contribuciones a la rentabilidad de negocio	P05	DS6										S	P			S		
25 Entregar proyectos a tiempo y sobre presupuesto, reuniendo los estándares de calidad	P08	P010										P	P	S		S		
26 Mantener la integridad de la información e infraestructura de procesamiento	AI6	DS5										P	P	P	P	S		
27 Asegurar que TI cumple con la legislación, regulación y contratos	DS11	ME2	ME3	ME4										S	S	P	S	
28 Asegurar que TI demuestra la eficiencia de costes de la calidad de servicios, mejora continua y disposición para cambios futuros	P05	DS6	ME1	ME4								P	P				P	

# APÉNDICE I

# COBIT 4.1

199

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
<b>Planear y Organizar</b>																												
PO1 Definir un plan estratégico de TI	V	V																										
PO2 Definir la arquitectura de la información	V			V	V						V																	
PO3 Determinar la dirección tecnológica								V								V												
PO4 Definir los procesos, organización y relaciones de TI	V	V			V																							
PO5 Administrar la inversión en TI												V																
PO6 Comunicar las aspiraciones y la dirección de la gerencia												V	V						V	V	V	V			V			V
PO7 Administrar recursos humanos de TI					V				V			V	V															
PO8 Administrar la calidad				V												V												
PO9 Evaluar y administrar los riesgos de TI														V			V	V							V			
PO10 Administrar proyectos	V	V																								V		
<b>Adquirir e Implementar</b>																												
A11 Identificar soluciones automatizadas	V					V																						
A12 Adquirir y mantener software aplicativo						V	V																					
A13 Adquirir y mantener infraestructura tecnológica					V			V																				
A14 Facilitar la operación y el uso				V							V																	
A15 Adquirir recursos de TI							V	V	V							V												
A16 Administrar cambios	V					V										V						V				V		
A17 Instalar y acreditar soluciones y cambios	V										V		V			V					V	V						
<b>Entregar y Dar Soporte</b>																												
DS1 Definir y administrar los niveles de servicio	V		V									V																
DS2 Administrar los servicios de terceros			V							V		V																
DS3 Administrar el desempeño y la capacidad	V										V					V												
DS4 Garantizar la continuidad del servicio																												
DS5 Garantizar la seguridad de los sistemas																												
DS6 Identificar y asignar costos												V							V	V	V	V	V					V
DS7 Educar y entrenar a los usuarios				V								V																
DS8 Administrar la mesa de servicio y los incidentes				V								V																
DS9 Administrar la configuración																												
DS10 Administrar los problemas				V												V	V											
DS11 Administrar los datos					V												V	V										
DS12 Administrar el ambiente físico																			V			V	V					
DS13 Administrar las operaciones				V																		V	V	V				
<b>Monitorear y Evaluar</b>																												
ME1 Monitorear y evaluar el desempeño de TI	V	V										V																V
ME2 Monitorear y evaluar el control interno															V						V							V
ME3 Garantizar el cumplimiento regulatorio																												V
ME4 Proporcionar gobierno de TI		V										V																V

1 Responder a requerimientos de negocio alineado con la estrategia de negocio  
 2 Responder a los requerimientos de gobierno en línea con la dirección de servicio  
 3 Asegurar la satisfacción del usuario final con la oferta de servicios y niveles de servicio  
 4 Optimizar el uso de la información  
 5 Crear agilidad de TI  
 6 Definir como la funcionalidad de negocio y requerimientos de control se traducen en soluciones efectivas y eficientes para el negocio  
 7 Adquirir y mantener sistemas de aplicación integrados y estandarizados  
 8 Adquirir y mantener una infraestructura de TI integrada y estandarizada  
 9 Adquirir y mantener habilidades de TI que respondan a la estrategia de TI  
 10 Asegurar la satisfacción mutua de relaciones con actores partes  
 11 Asegurar la integración en flujos en las aplicaciones de los procesos del negocio  
 12 Asegurar la transparencia y comprensión de costos de los entornos, políticas y niveles de servicio  
 13 Asegurar el uso apropiado y mantenimiento de costos de TI, beneficios tecnológicos  
 14 Tener en cuenta y proteger todos los activos de aplicación y datos  
 15 Optimizar la infraestructura, recursos y capacidades de TI  
 16 Reducir los riesgos de la solución y entrega de servicio y relacionar  
 17 Proteger el valor de los objetivos de TI  
 18 Estrategia de clientes del impacto de negocio de los riesgos a los objetivos y recursos de TI  
 19 Asegurar que la información crítica y confidencial se relate a los objetivos de negocio y se maneje de manera adecuada  
 20 Asegurar que las transacciones de negocio automatizadas y los cambios de configuración se manejen de manera adecuada  
 21 Asegurar que los servicios de TI, la infraestructura puedan manejar los cambios de configuración de los recursos de negocio a través de los servicios de TI o cambios de configuración de negocio en caso de una interrupción de servicio  
 22 Estar seguros que los servicios de TI están disponibles según se requiere de negocio  
 23 Mejorar la evidencia de costos de TI y sus contribuciones a la rentabilidad de negocio  
 24 Entregar proyectos a tiempo y sobre presupuesto, siguiendo los estándares de calidad  
 25 Mantener la integridad de la información e infraestructura de negocio  
 26 Asegurar que TI cumple con la legislación, regulada y contratos  
 27 Asegurar que TI contribuya a la evidencia de costos de la calidad de los servicios, mejora continua y disposición para cambios futuros

## APÉNDICE II

# MAPEO ENTRE LOS PROCESOS DE TI Y LAS ÁREAS FOCALES DE GOBIERNO DE TI, COSO, LOS RECURSOS TI DE COBIT Y LOS CRITERIOS DE INFORMACIÓN DE COBIT

Este apéndice proporciona las equivalencias entre los procesos de TI de COBIT y las cinco áreas focales del gobierno de TI, los recursos de TI y los criterios de información. La tabla también contiene un indicador de importancia relativa (alta, media y baja), con base en la evaluación por comparación (benchmarking) vía COBIT ONLINE. Esta matriz en una página, y a alto nivel como el marco de trabajo de COBIT resuelve los requisitos de gobierno de TI y de COSO, y muestra la relación entre los procesos de TI, los recursos y criterios de información de TI. La P se usa cuando hay una relación primaria y la S cuando solamente existe una relación secundaria. El hecho de que no exista una P ni una S no significa que no exista relación, sólo que es menos importante o marginal. Los valores de importancia se basan en una encuesta y en la opinión de expertos, y se incluyen sólo como una guía. Los usuarios deben considerar qué procesos son importantes dentro de sus propias organizaciones.

# Apendice II – Mapeo de Procesos de TI a las Areas Focales de Gobierno TI, COSO, Recursos de TI de CobiT y Criterios de Información de CobiT

	IMPORTANCIA	Áreas de enfoque de Gobierno TI				COSO				Recursos TI de CobiT			Criterios de información de CobiT						
		Alineación estratégica	Entrega de valor	Administración de	Medición del desempeño	Entorno de Control	Evaluación de riesgos	Actividades de control	Información y Monitoreo	Aplicación	Infraestructura	Personas	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiablez
<b>Planear y Organizar</b>																			
PD1 Definir un plan estratégico de TI	A	P	S	S			P	S	S				P	S					
PD2 Definir la arquitectura de la información	B	P	S	P	S			P	P				S	P	S	P			
PD3 Determinar la dirección tecnológica	M	S	S	P	S			S	P	S			P	P					
PD4 Definir los procesos, organización y relaciones de TI	B	S		P	P			P	P	S			P	P					S
PD5 Administrar la inversión en TI	M	S	P	S	S	S			S	P			P	P					
PD6 Comunicar las aspiraciones y la dirección de la gerencia	M	P		P	P			P		P									S
PD7 Administrar recursos humanos de TI	B	P		P	S	S		P		S			P	P					
PD8 Administrar la calidad	M	P	S		P			P	P	S	P		P	P	S				S
PD9 Evaluar y administrar los riesgos de TI	A	P			P			P	P				S	S	P	P	P	S	S
PD10 Administrar proyectos	A	P	S	S	S	S		S	S	P	S		P	P					
<b>Adquirir e Implementar</b>																			
A11 Identificar soluciones automatizadas	M	P	P	S	S				P				P	S					
A12 Adquirir y mantener software aplicativo	M	P	P	P	S				P				P	P	S				S
A13 Adquirir y mantener infraestructura tecnológica	B			P					P				S	P	S	S			
A14 Facilitar la operación y el uso	B	S	P	S	S				P	S			P	P	S	S	S	S	
A15 Adquirir recursos de TI	M		S	P					P				S	P					
A16 Administrar cambios	A		P	S					S	P	S		P	P					S
A17 Instalar y acreditar soluciones y cambios	M	S	P	S	S	S			P	S	S		P	S	S				
<b>Entregar y Dar Soporte</b>																			
DS1 Definir y administrar los niveles de servicio	M	P	P	P	P			S	P	S	S		P	P	S	S	S	S	S
DS2 Administrar los servicios de terceros	B		P	S	P	S		P	S	P	S		P	P	S	S	S	S	S
DS3 Administrar el desempeño y la capacidad	B	S	S	P	S	S			P		S		P	P					
DS4 Garantizar la continuidad del servicio	M	S	P	S	P	S		S	P	S			P	S					
DS5 Garantizar la seguridad de los sistemas	A			P					P	S	S			P	P	S	S	S	
DS6 Identificar y asignar costos	B		S	P	P	S			P				P						P
DS7 Educar y entrenar a los usuarios	B	S	P	S	S			P		S			P	S					
DS8 Administrar la mesa de servicio y los incidentes	B		P		S			S	P	P	P		P	P					
DS9 Administrar la configuración	M		P	P	S				P				P	S					S
DS10 Administrar los problemas	M		P		S	S			P	S	S		P	P					S
DS11 Administrar los datos	A		P	P	P				P										P
DS12 Administrar el ambiente físico	B			S	P				S	P									P
DS13 Administrar las operaciones	B			P					P	S				P	P	S	S		
<b>Monitorear y Evaluar</b>																			
ME1 Monitorear y evaluar el desempeño de TI	A	S	S	S	S	P				S	P		P	P	S	S	S	S	S
ME2 Monitorear y evaluar el control interno	M		P		P						P		P	P	S	S	S	S	S
ME3 Garantizar el cumplimiento regulatorio	A	P			P				P	S	S								P
ME4 Proporcionar gobierno de TI	A	P	P	P	P	P			P	S	S	P		P	P	S	S	S	S

(P=Primario, S=Secundario).

**Nota:** El mapeo COSO esta basado sobre el marco original COSO. El mapeo también aplica sobre el ultimo COSO Administración de Riesgos Empresarial - Marco Integrado, que expande sobre los controles internos proporcionando un enfoque mas robusto y extensivo sobre el sujeto de la gestión de riesgos de la empresa. Mientras ni intenta ni reemplaza el marco de control interno COSO, sino mas bien incorpora el marco de control interno dentro, los usuarios de CobiT pueden elegir referir a ambos marcos de gestión de riesgos de la empresa para satisfacer sus necesidades de control interno y moverse a través de un proceso de gestión de riesgos mas completo.

# APÉNDICE III

## MODELO DE MADUREZ PARA EL CONTROL INTERNO

Este apéndice muestra un modelo genérico de madurez que describe el estatus del ambiente de control interno y el establecimiento de controles internos en una empresa. Muestra cómo la administración del control interno, y la conciencia de la necesidad de establecer mejores controles internos, por lo general evoluciona de algo *ad hoc*, hasta un nivel optimizado. El modelo brinda una guía de alto nivel para ayudar a los usuarios de COBIT a apreciar lo que se requiere para un control interno efectivo en TI y ayudar a posicionar a su empresa en la escala de madurez.

## APÉNDICE III – MODELO DE MADUREZ PARA EL CONTROL INTERNO

Nivel de Madurez	Estado del Entorno de Control Interno	Establecimiento de Control Interno
0 No existente	No se reconoce la necesidad del control interno. El control no es parte de la cultura o misión organizacional. Existe un alto riesgo de deficiencias e incidentes de control.	No existe la intención de evaluar la necesidad del control interno. Los incidentes se manejan conforme van surgiendo.
1 Inicial / <i>ad hoc</i>	Se reconoce algo de la necesidad del control interno. El enfoque hacia los requerimientos de riesgo y control es <i>ad hoc</i> y desorganizado, sin comunicación o supervisión. No se identifican las deficiencias. Los empleados no están concientes de sus responsabilidades.	No existe la conciencia de la necesidad de evaluar lo que se necesita en términos de controles de TI. Cuando se llevan a cabo, son solamente de forma <i>ad hoc</i> , a alto nivel y como reacción a incidentes significativos. La evaluación sólo se enfoca al incidente presente.
2 Repetible pero Intuitivo	Existen controles pero no están documentados. Su operación depende del conocimiento y motivación de los individuos. La efectividad no se evalúa de forma adecuada. Existen muchas debilidades de control y no se resuelven de forma apropiada; el impacto puede ser severo. Las medidas de la gerencia para resolver problemas de control no son consistentes ni tienen prioridades. Los empleados pueden no estar concientes de sus responsabilidades.	La evaluación de la necesidad de control sucede solo cuando se necesita para ciertos procesos seleccionados de TI para determinar el nivel actual de madurez del control, el nivel meta que debe ser alcanzado, y las brechas existentes. Se utiliza un enfoque de taller informal, que involucra a los gerentes de TI y al equipo interesado en el proceso, para definir un enfoque adecuado hacia el control para los procesos, y para generar un plan de acción acordado.
3 Definido	Existen controles y están documentados de forma adecuada. Se evalúa la efectividad operativa de forma periódica y existe un número promedio de problemas. Sin embargo, el proceso de evaluación no está documentado. Aunque la gerencia puede manejar la mayoría de los problemas de control de forma predecible, algunas debilidades de control persisten y los impactos pueden ser severos. Los empleados están concientes de sus responsabilidades de control.	Los procesos críticos de TI se identifican con base en impulsores de valor y de riesgo. Se realiza un análisis detallado para identificar requisitos de control y la causa raíz de las brechas, así como para desarrollar oportunidades de mejora. Además de facilitar talleres, se usan herramientas y se realizan entrevistas para apoyar el análisis y garantizar que los dueños de los procesos de TI son realmente los dueños e impulsan al proceso de evaluación y mejora.
4 Administrado y Medible	Existe un ambiente efectivo de control interno y de administración de riesgos. La evaluación formal y documentada de los controles ocurre de forma periódica. Muchos controles están automatizados y se realizan de forma periódica. Es probable que la gerencia detecte la mayoría de los problemas de control, aunque no todos los problemas se identifican de forma rutinaria. Hay un seguimiento consistente para manejar las debilidades de control identificadas. Se aplica un uso de la tecnología táctico y limitado a los controles automatizados.	Se define de forma periódica qué tan críticos son los procesos de TI con el apoyo y acuerdo completo por parte de los dueños de los procesos correspondientes. La evaluación de los requisitos de control se basa en las políticas y en la madurez real de estos procesos, siguiendo un análisis meticuloso y medido, involucrando a los Interesados (Stakeholders) clave. La rendición de cuentas sobre estas evaluaciones es clara y está reforzada. Las estrategias de mejora están apoyadas en casos de negocio. El desempeño para lograr los resultados deseados se supervisa de forma periódica. Se organizan de forma ocasional revisiones externas de control.
5 Optimizado	Un programa organizacional de riesgo y control proporciona la solución continua y efectiva a problemas de control y riesgo. El control interno y la administración de riesgos se integran a las prácticas empresariales, apoyadas con una supervisión en tiempo real, y una rendición de cuentas completa para la vigilancia de los controles, administración de riesgos, e implantación del cumplimiento. La evaluación del control es continua y se basa en auto-evaluaciones y en análisis de brechas y de causas raíz. Los empleados se involucran de forma pro-activa en las mejoras de control.	Los cambios en el negocio toman en cuenta que tan críticos son los procesos de TI, y cubren cualquier necesidad de re-evaluar la capacidad del control de los procesos. Los dueños de los procesos realizan auto-evaluaciones de forma periódica para confirmar que los controles se encuentran en el nivel correcto de madurez para satisfacer las necesidades del negocio, y toman en cuenta los atributos de madurez para encontrar maneras de hacer que los controles sean más eficientes y efectivos. La organización evalúa por comparación con las mejoras prácticas externas y busca asesoría externa sobre la efectividad de los controles internos. Para procesos críticos, se realizan evaluaciones independientes para proporcionar seguridad de que los controles se encuentran al nivel deseado de madurez y funcionan como fue planeado.

# CAPÍTULO 8

## EL MODELO DE CAPACIDAD DE LOS PROCESOS DE COBIT 5

### Introducción

Los usuarios de COBIT 4.1, Risk IT y Val IT están familiarizados con los modelos de madurez de procesos incluidos en esos marcos. Estos modelos se utilizan para medir la madurez actual o en el estado en que se encuentran ('as-is') los procesos relacionados con las TI de una empresa, para definir un estado de madurez requerido ('to-be'), y para determinar la brecha entre ellos y la forma de mejorar el proceso para alcanzar el nivel de madurez deseado.

El conjunto de productos de COBIT 5 incluye un modelo de capacidad de procesos, basado en la norma internacionalmente reconocida ISO / IEC 15504 de Ingeniería de Software-Evaluación de Procesos. Este modelo alcanzará los mismos objetivos generales de evaluación de procesos y apoyo a la mejora de procesos, es decir, que proporcionará un medio para medir el desempeño de cualquiera de los procesos de gobierno (basado en EDM) o de gestión (basado en PBRM), y permitirá identificar áreas de mejora.

Sin embargo, el nuevo modelo es diferente del modelo de madurez de COBIT 4.1 en su diseño y uso, y por esa razón, se tratan los temas siguientes:

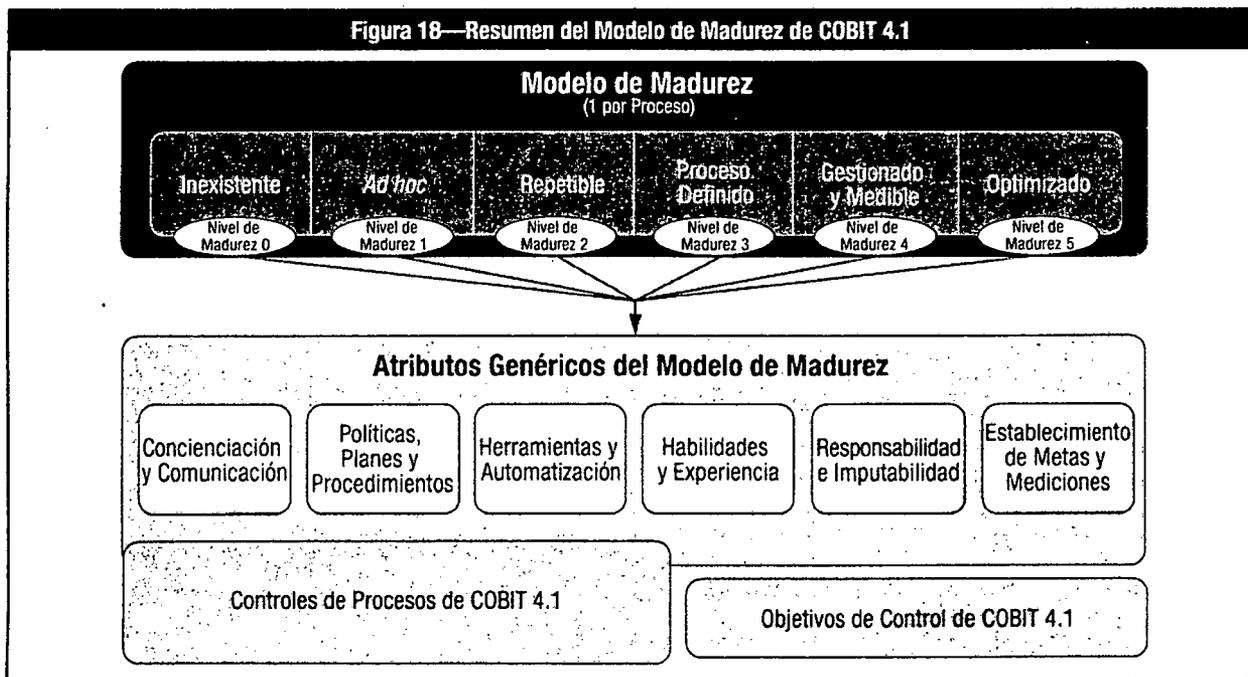
- Diferencias entre los modelos de COBIT 5 y de COBIT 4.1
- Beneficios del modelo COBIT 5
- Resumen de las diferencias que los usuarios de COBIT 5 encontrarán en la práctica.
- Llevar a cabo una evaluación de la capacidad COBIT 5

Los detalles del enfoque de evaluación de la capacidad basada en COBIT 5 están incluidos en la publicación de ISACA *COBIT® Process Assessment Model (PAM): Using COBIT® 4.1*.<sup>11</sup>

Aunque este enfoque proporcionará información valiosa sobre el estado de los procesos, estos procesos son solo uno de los siete catalizadores del gobierno y la gestión. Consecuentemente, las evaluaciones de los procesos no proporcionarán una imagen completa sobre el estado del gobierno en una empresa. Es por esto que también se necesita evaluar los otros catalizadores.

### Diferencias Entre el Modelo de Madurez de COBIT 4.1 y el Modelo de Capacidad de los Procesos de COBIT 5

Los elementos del enfoque del modelo de madurez de COBIT 4.1 se muestran en la figura 18.

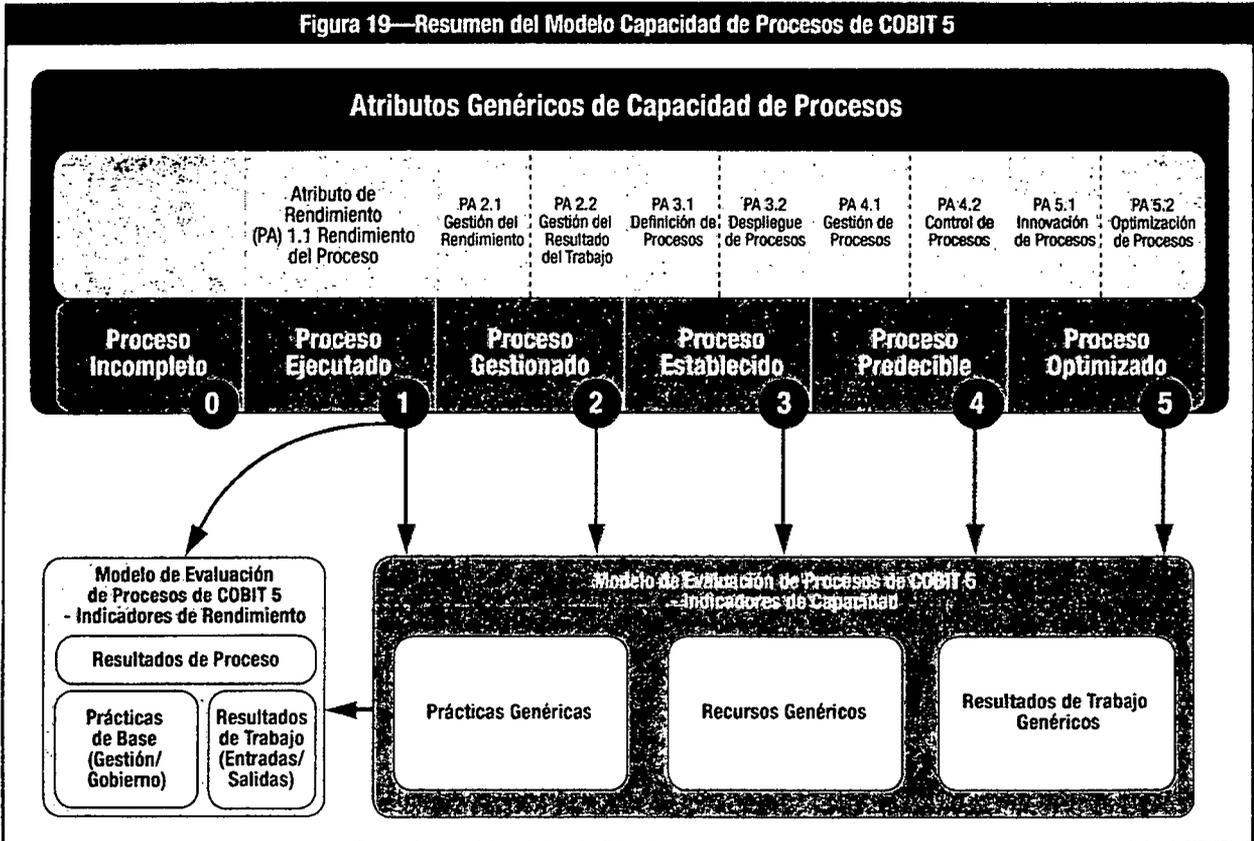


<sup>11</sup> [www.isaca.org/cobit-pam](http://www.isaca.org/cobit-pam)

Usar el modelo de madurez de COBIT 4.1 para la mejora de procesos - evaluar la madurez de un proceso, definir nivel objetivo de madurez e identificar las deficiencias- requería utilizar los siguientes componentes de COBIT 4.1:

- Primero, era necesario hacer un análisis para comprobar si los objetivos de control de los procesos se cumplían.
- Después, el modelo de madurez incluido en la guía de gestión para cada proceso podía ser utilizada para obtener un perfil de madurez del proceso.
- Además, el modelo de madurez genérico de COBIT 4.1 proporcionaba seis atributos diferentes que eran de aplicación a cada proceso y ayudaban en la obtención de una perspectiva más detallada del nivel de madurez del proceso.
- Los controles de proceso son objetivos de control genéricos – también necesitaban ser revisados cuando se llevaba a cabo un análisis de proceso. Los controles de procesos se solapan parcialmente con los atributos genéricos del modelo de madurez.

El enfoque de COBIT 5 de capacidad de los procesos se puede resumir como se muestra en la figura 19.



Existen seis niveles de capacidad que se pueden alcanzar por un proceso, incluida la designación de “proceso incompleto” si las prácticas definidas en el proceso no alcanzan la finalidad prevista:

- **0 Proceso incompleto**—El proceso no está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso.
- **1 Proceso ejecutado** (un atributo) -- El proceso implementado alcanza su propósito.
- **2 Proceso gestionado** (dos atributos) – El proceso ejecutado descrito anteriormente está ya implementado de forma gestionada (planificado, supervisado y ajustado) y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.
- **3 Proceso establecido** (dos atributos) – El proceso gestionado descrito anteriormente está ahora implementado usando un proceso definido que es capaz de alcanzar sus resultados de proceso.
- **4 Proceso predecible** (dos atributos) – El proceso establecido descrito anteriormente ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso.
- **5 Proceso optimizado** (dos atributos) – El proceso predecible descrito anteriormente es mejorado de forma continua para cumplir con los metas empresariales presentes y futuros.

Cada nivel de capacidad puede ser alcanzado sólo cuando el nivel inferior se ha alcanzado por completo. Por ejemplo, un nivel 3 de capacidad de proceso (establecido) requiere que los atributos de definición y despliegue del proceso se hayan alcanzado ampliamente, sobre la consecución completa de los atributos del nivel 2 de madurez de procesos (proceso gestionado).

Existe una diferencia significativa entre el nivel 1 de capacidad de procesos y los niveles superiores. Alcanzar el nivel 1 requiere que el atributo de rendimiento sea alcanzado ampliamente, lo que significa que el proceso se ejecuta con éxito y la organización obtiene los resultados esperados. Es entonces cuando los niveles de capacidad superiores añaden diferentes atributos al proceso. En este esquema de evaluación, alcanzar un nivel 1 de capacidad, incluso en una escala de 5, es ya un logro importante para la organización. Ha de tenerse en cuenta que (basándose en motivos de viabilidad y coste-beneficio) cada empresa de forma individual deberá elegir su objetivo o nivel deseado, que raramente será uno de los más altos.

Las diferencias más importantes entre un análisis de capacidad de procesos basado en la norma ISO/IEC 15504 y el modelo de madurez actual de COBIT 4.1 (y los modelos similares de ValIT y RiskIT basados en dominios) se pueden resumir como sigue:

- La nomenclatura y significado de los niveles definidos en la ISO/IEC 15504 son muy diferentes de aquellos de COBIT 4.1.
- En la norma ISO/IEC 15504 los niveles de capacidad se definen por un conjunto de nueve atributos de proceso. Estos atributos cubren algo del terreno cubierto por los atributos de madurez COBIT 4.1 y/o los controles de proceso, pero solo en cierta medida y de forma distinta.

Los requisitos para un modelo de referencia para procesos compatible con la norma ISO/IEC 15504.2 prescriben que en la descripción de cualquier proceso que se vaya a analizar, por ejemplo cualquier proceso de gobierno o gestión de COBIT 5:

- El proceso está descrito en términos de su propósito y resultados.
- La descripción del proceso no debe contener ningún aspecto del marco de medición por debajo del nivel 1, lo que significa que cualquier característica del atributo de un proceso no puede aparecer dentro de la descripción del proceso. Si un proceso es supervisado y medido, o si está formalmente descrito, etc., no puede ser parte de la descripción del proceso o cualquiera de las actividades o prácticas inferiores. Esto implica que las descripciones del proceso- como se incluyen en *COBIT 5: Procesos Catalizadores*- contienen solamente los pasos necesarios para alcanzar el propósito y las metas reales del proceso.
- Siguiendo los puntos anteriores, los atributos comunes aplicables a todos los procesos de la empresa, los cuales produjeron la duplicación de objetivos de control en la publicación de *COBIT 3ª Edición* y se agruparon en los objetivos de control de procesos (PC) en COBIT 4.1, están ahora definidos en los niveles 2 a 5 del modelo de evaluación.

## Diferencias en la Práctica<sup>12</sup>

De las descripciones previas, está claro que hay algunas diferencias prácticas asociadas con el cambio en los modelos de evaluación de procesos. Los usuarios han de ser conscientes de estos cambios y tenerlos en cuenta en sus planes de acción.

Los principales cambios a considerar incluyen:

- Aunque es tentador comparar los resultados entre COBIT 4.1 y COBIT 5 debido a la aparente similitud de las escalas numéricas y las palabras usadas para describirlas, tal comparación es difícil por las diferencias de ámbito de aplicación, foco e intención, tal y como se ilustra en la **figura 20**.
- En general, los resultados de la evaluación serán menores al usar el modelo de capacidad de procesos de COBIT 5, tal y como se muestra en la **figura 20**. En el modelo de madurez de COBIT 4.1, un proceso podía alcanzar un nivel 1 ó 2 sin alcanzar completamente todos los objetivos del proceso; con los niveles de la capacidad de procesos de COBIT 5, esto implicaría un resultado inferior, entre 0 y 1.

Las escalas de capacidad de COBIT 4.1 y COBIT 5 se pueden considerar “mapeadas” como se muestra en la **figura 20**.

- Ya no se incluye dentro de los contenidos detallados de un proceso en COBIT 5 un modelo específico de madurez para cada proceso. Esto es porque el enfoque de la norma ISO/IEC 15504 para la evaluación de la capacidad de procesos no lo requiere, incluso lo prohíbe. En cambio, el enfoque de la norma define la información requerida en el “modelo de referencia de procesos” (el modelo de procesos que debe ser usado en la evaluación):
  - Descripción del proceso, con la declaración de propósitos.
  - Prácticas base, que son las equivalentes a prácticas de gestión o de gobierno en COBIT 5.
  - Productos de trabajo, que son el equivalente a las entradas y salidas en términos de COBIT 5.
- El modelo de madurez de COBIT 4.1 producía un perfil de madurez de la empresa. El principal propósito de este perfil era identificar en qué dimensión o para qué atributos había debilidades específicas que necesitaban mejoras. Este enfoque era usado por las empresas cuando había un enfoque hacia la mejora más que para obtener un número de madurez para incluirlo en un informe. En COBIT 5 el modelo de evaluación proporciona una escala de medida para cada atributo de capacidad y guía sobre cómo aplicarlo, por lo que por cada proceso se puede hacer un análisis para cada uno de los nueve atributos de capacidad.
- Los atributos de madurez de COBIT 4.1 y los atributos de capacidad de los procesos de COBIT 5 no son idénticos. Estos se solapan/mapean hasta cierto punto, tal y como se muestra en la **figura 21**. Las empresas que hayan utilizado el enfoque de atributos del modelo de madurez de COBIT 4.1 pueden reutilizar los datos de sus evaluaciones existentes y reclasificarlos según las evaluaciones de atributos de COBIT 5 basado en la **figura 21**.

<sup>12</sup> Puede encontrar más información sobre el nuevo Programa de Evaluación COBIT basado en ISO/IEC 15504 en [www.isaca.org/cobit-assessment-programme](http://www.isaca.org/cobit-assessment-programme).

**Figura 20—Tabla de Comparación de los Niveles de Madurez (COBIT 4.1) y los Niveles de Capacidad de Procesos (COBIT 5)**

Nivel del Modelo de Madurez de Cobit 4.1	Capacidad del Proceso basada en ISO/IEC 15504	Contexto
<b>5 Optimizado</b> —Los procesos han sido refinados a nivel de buena práctica, sobre la base de los resultados de mejora continua y de modelado de madurez con otras empresas. Las TI se usan de forma integrada para automatizar los flujos de trabajo, proporcionando herramientas para mejorar la calidad y la efectividad, haciendo a la empresa rápida para adaptarse.	<b>Nivel 5: Proceso optimizado</b> —El proceso predecible del nivel 4 es mejorado continuamente para alcanzar metas de negocio actuales y futuros.	<b>Punto de Vista de la Empresa— Conocimiento Corporativo</b>
<b>4 Gestionado y medible</b> — Los responsables de la gestión monitorizan y miden el cumplimiento con procedimientos y llevan a cabo acciones donde los procesos parecen no estar funcionando con efectividad. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Automatización y herramientas son usadas de forma limitada o fragmentada.	<b>Nivel 4: Proceso establecido</b> —El proceso establecido del nivel 3 es operado ahora dentro de unos límites definidos para alcanzar sus resultados.	
<b>3 Procesos definidos</b> — Se han estandarizado, documentado y comunicado los procedimientos mediante formación. Es obligatorio seguir estos procedimientos, sin embargo es poco probable que se detecten desviaciones. Los procedimientos no son sofisticados en sí mismos, pero sí la formalización de las prácticas existentes.	<b>Nivel 3: Procesos establecidos</b> —El proceso gestionado del nivel 2 se implementa usando un proceso definido que es capaz de alcanzar sus objetivos.	
	<b>Nivel 2: Proceso gestionado</b> —El proceso ejecutado del nivel 1 es implementado de forma gestionada (planificado, supervisado y ajustado) y sus resultados son debidamente establecidos, controlados y mantenidos.	<b>Punto de Vista de la Instancia— Conocimiento Individual</b>
<b>2 Repetible pero intuitivo</b> — Los procesos están desarrollados hasta el punto que procedimientos similares son seguidos por personas diferentes ejecutando la misma tarea. No hay formación formal o comunicación de los procedimientos estándar, y la responsabilidad se deja a la persona de forma individual. Hay un alto grado de dependencia en el conocimiento individual y, por lo tanto, los errores son probables.	<b>Nivel 1: Proceso ejecutado</b> —El proceso implementado alcanza su objetivo.  <b>Comentario: Es posible que algunos procesos clasificados como nivel 1 del Modelo de Madurez sean clasificados nivel 0 por ISO/IEC 15504 si los objetivos no son alcanzados.</b>	
<b>1 Inicial/Ad hoc</b> —Hay evidencia de que la empresa reconoce que existe el problema y que hay que abordarlo. Sin embargo, no hay procesos estandarizados. En su lugar hay enfoques <i>ad hoc</i> que tienden a aplicarse de forma individual o caso por caso. La aproximación general a la gestión es desorganizada.		
<b>0 Inexistente</b> —Ausencia completa de cualquier proceso reconocible. La empresa ni siquiera ha reconocido que hay un problema que gestionar.	<b>Nivel 0: Proceso incompleto</b> —El proceso no está implantado o no alcanza sus objetivos.	

**Figura 21—Tabla de Comparación de los Atributos de Madurez (COBIT 4.1) y los Atributos de Proceso (COBIT 5)**

Atributo de Madurez de COBIT 4.1	Atributo de Capacidad de Procesos de COBIT 5								
	Rendimiento del Proceso	Gestión del Rendimiento	Gestión de los Resultados	Definición de Procesos	Despliegue de Procesos	Gestión de Procesos	Control de Procesos	Innovación de Procesos	Optimización de Procesos
Concienciación y Comunicación									
Políticas, planes y procedimientos									
Herramientas y automatización									
Conocimientos y experiencia									
Responsabilidad e imputabilidad									
Establecimiento y medición de metas									

### Beneficios de los Cambios

Los beneficios del modelo de capacidad de los procesos de COBIT 5, comparados con los modelos de madurez de COBIT 4.1, incluyen:

- Enfoque mejorado en los procesos en ejecución, para confirmar que se está realmente consiguiendo su objetivo y que está entregando los resultados esperados.

- Contenido simplificado a través de la eliminación de duplicados, porque la evaluación del modelo de madurez de COBIT 4.1 requería el uso de un número de componentes específicos, incluido el modelo de madurez genérico, los modelos de madurez de los procesos, objetivos de control y controles de procesos para apoyar las evaluaciones de los procesos.
- Confiabilidad y repetitividad mejorada de las actividades y valoraciones de la evaluación de la capacidad de los procesos, reduciendo discusiones y falta de acuerdo entre las partes interesadas sobre los resultados de la evaluación.
- Incremento de la utilidad de los resultados de la evaluación de la capacidad de los procesos, ya que el nuevo modelo establece una base para que se lleven a cabo evaluaciones más formales y rigurosas, tanto para propósitos internos como externos.
- Cumplimiento con un estándar de evaluación de procesos generalmente aceptado y de esta forma con un fuerte soporte al enfoque de evaluación de procesos por el mercado.

## Realizando Evaluaciones de Capacidad de Procesos en COBIT 5

El estándar ISO/IEC 15504 especifica que la evaluación de la capacidad de los procesos puede llevarse a cabo para varios propósitos y con varios grados de rigor. Los objetivos pueden ser internos, con un foco en las comparaciones entre áreas de la empresa y/o mejoras de procesos para el beneficio interno, o pueden ser externos enfocados a evaluaciones formales, informes y certificaciones.

El enfoque de la evaluación basada en COBIT 5 y la norma ISO/IEC 15504 continua facilitando los siguientes objetivos que han sido claves para el enfoque COBIT desde el 2000 para:

- Habilitar al órgano de gobierno y de gestión para establecer un punto de referencia para la evaluación de la capacidad.
- Habilitar chequeos sobre “el estado en que se encuentran” (“as-is”) y “el estado objetivo” (“to-be”) de alto nivel para asistir al órgano de gobierno y a la gestión de la empresa en la toma de decisiones de inversiones relativas a la mejora de procesos.
- Proporcionar análisis de carencias e información sobre la planificación de mejoras para apoyar la definición de proyectos de mejora justificables.
- Proporcionar al órgano de gobierno y de gestión de la empresa con ratios de evaluación para medir y monitorizar la capacidad actual.

Esta sección describe como se puede llevar a cabo una evaluación a alto nivel con el modelo de capacidad de los procesos de COBIT 5 para alcanzar esos objetivos.

La evaluación distingue entre evaluar el nivel 1 de capacidad y los niveles superiores. De hecho, como se describió anteriormente, el nivel 1 de capacidad de procesos describe si un proceso alcanza su objetivo establecido, y es por tanto un nivel a alcanzar muy importante - así como la base para hacer alcanzables los niveles de capacidad superiores.

Evaluar si el proceso alcanza sus objetivos—o, en otras palabras, alcanza el nivel de capacidad 1—puede hacerse por:

1. Revisión de los resultados del proceso tal y como se describen para cada proceso en sus descripciones detalladas, y usando las escalas y ratios de la ISO/IEC 15504 para asignar un ratio para el grado en el que cada objetivo es alcanzado. Esta escala consiste en los siguientes ratios:
  - **N** (No alcanzado)—Hay muy poca o ninguna evidencia de que se alcanza el atributo definido en el proceso de evaluación. (0 al 15 por ciento de logro)
  - **P** (Parcialmente alcanzado)—Hay alguna evidencia de aproximación a, y algún logro del atributo definido en el proceso evaluado. Algunos aspectos del logro del atributo pueden ser impredecibles. (15 a 30 por ciento de logro)
  - **L** (Ampliamente alcanzado)—Hay evidencias de un enfoque sistemático y de un logro significativo del atributo definido en el proceso evaluado. Pueden encontrarse algunas debilidades relacionadas con el atributo en el proceso evaluado. (50 a 85 por ciento de logro)
  - **F** (Completamente alcanzado)—Existe evidencia de un completo y sistemático enfoque y un logro completo del atributo definido en el proceso evaluado. No existen debilidades significativas relacionadas con el atributo en el proceso evaluado. (85 a 100 por ciento de logro)
2. Además, las prácticas del proceso (de gobierno o de gestión) pueden ser evaluadas usando la misma escala de puntuación, expresando el punto hasta el que se aplican las prácticas de base.
3. Para afinar la evaluación más allá, los productos del trabajo pueden ser considerados para determinar el grado al que un atributo de evaluación específico ha sido alcanzado.

Aunque depende de cada empresa decidir los objetivos de niveles de capacidad, muchas empresas tendrán la ambición de que sus procesos alcancen el nivel 1. (De otro modo, ¿cuál sería el propósito de tener esos procesos?) Si no se alcanza este nivel, las razones por las que no se ha alcanzado son inmediatamente obvias a partir del enfoque explicado anteriormente y se puede definir un plan de mejora:

1. Si el resultado requerido de un proceso no se alcanza de manera continuada, el proceso no alcanza su objetivo y necesita ser mejorado.
2. La evaluación de las prácticas del proceso revelará qué prácticas faltan o están fallando, habilitando la implementación y/o la mejora de esas prácticas y permitiendo alcanzar todos los objetivos de los procesos.

Para niveles de capacidad de los procesos superiores se utilizan las prácticas genéricas tomadas del estándar ISO/IEC 15504:2. Éstas proporcionan descripciones genéricas para cada uno de los niveles de capacidad.

## APÉNDICE B

# MAPEO DETALLADO DE LAS METAS DE EMPRESA Y LAS METAS RELACIONADAS CON LAS TI

En el capítulo 2 se detallan las metas en cascada de COBIT 5.

El propósito de la tabla de mapeo de la **figura 22** es mostrar cómo las metas empresariales son soportadas (o se traducen) en objetivos relacionados con TI. Por este motivo, la tabla contiene la siguiente información:

- Las columnas contienen, agrupados por dimensión del CMI, los 17 objetivos genéricos corporativos de COBIT 5.
- En horizontal, los 17 objetivos relacionados con TI, igualmente agrupados por dimensión del CMI.
- El mapeo de cómo cada objetivo corporativo es soportado por los objetivos TI relacionados. Este mapeo se expresa usando la siguiente escala:
  - ‘P’ para principal, cuando hay una importante relación, es decir, las metas relacionadas con TI que son el pilar imprescindible para conseguir los objetivos de la empresa.
  - ‘S’ para secundario, cuando todavía hay un vínculo fuerte, pero menos importante, es decir, las metas relacionadas con TI son un soporte secundario para los objetivos de la empresa.

### EJEMPLO 7-TABLA DE MAPEO

La tabla de correspondencias sugiere lo que normalmente se podría esperar:

- Meta corporativa 7. La continuidad y disponibilidad del servicio de negocio:
  - Dependerá principalmente de la consecución de los siguientes metas relativas a TI:
    - 04 Riesgos de negocio relacionados con las TI gestionados
    - 10 Seguridad de la información, infraestructura de procesamiento y aplicaciones.
    - 14 Disponibilidad de información útil y relevante para la toma de decisiones.
  - También dependerá, pero en un menor grado, de la consecución de las siguientes metas relativas a TI:
    - 01 Alineamiento de TI con la estrategia de negocio.
    - 07 Entrega de los servicios de TI de acuerdo a los requisitos de negocio.
    - 08 Uso adecuado de las aplicaciones, la información y las soluciones tecnológicas.
- Usando la tabla en sentido contrario, la consecución del objetivo de TI 09. La Agilidad de las TI contribuirá a la consecución de las siguientes metas corporativas:
  - Principalmente, a las metas corporativas:
    - 2. Cartera de productos y servicios competitivos.
    - 8. Respuesta ágil a un entorno de negocio cambiante.
    - 11. Optimización de la funcionalidad del proceso de negocio.
    - 17. Cultura de innovación del producto y del negocio.
  - En un grado menor, a los objetivos empresariales:
    - 1. Valor para las partes interesadas de las inversiones realizadas en el negocio.
    - 3. Riesgos de negocio gestionados (salvaguarda de activos).
    - 6. Cultura de servicio orientada al cliente.
    - 13. Programas gestionados de cambios en el negocio.
    - 14. Productividad operacional y de los empleados.
    - 16. Personas preparadas y motivadas

La tabla fue creada con las siguientes aportaciones:

- Estudio realizado por el Instituto de Investigación en Alineamiento TI y Gobierno de la Escuela de Dirección de Empresas de la Universidad de Amberes
- Revisiones adicionales y opiniones de expertos obtenidas durante el proceso de desarrollo y revisión de COBIT 5

Por favor, cuando use la tabla de la figura 22, tenga en cuenta las recomendaciones hechas en el capítulo 2 relativas al uso de metas en cascada de COBIT 5.

**Figura 22—Mapeo entre las Metas Corporativas de COBIT 5 y las Metas Relacionadas con las TI**

		Meta corporativa																
		Valor para las partes interesadas de las Inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activo)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basadas en información	Optimización de costes de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas internas	Personas preparadas y motivadas	Cultura de innovación del producto y del negocio
		1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
Meta relacionada con las TI		Financiera					Cliente					Interna					Apre- ndizaje y Creci- miento	
Financiera	01 Alineamiento de TI y la estrategia de negocio	P	P	S			P	S	P	P	S	P	S	P			S	S
	02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas			S	P											P		
	03 Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S				S	S		S		P				S	S
	04 Riesgos de negocio relacionados con las TI gestionados			P	S		P	S		P		S		S		S	S	
	05 Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	P	P			S		S		S	S	P		S			S	
	06 Transparencia de los costes, beneficios y riesgos de las TI	S		S		P			S	P		P						
Cliente	07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S		P	S	P	S		P	S	S			S	S
	08 Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S	S	S	P	S		P			S	S
Interna	09 Agilidad de las TI	S	P	S			S		P		P		S	S			S	P
	10 Seguridad de la información, infraestructuras de procesamiento y aplicaciones			P	P		P									P		
	11 Optimización de activos, recursos y capacidades de las TI	P	S					S		P	S	P	S	S			S	
	12 Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	S	P	S			S		S		S	P	S	S			S	
	13 Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	P	S	S			S				S		S	P				
	14 Disponibilidad de información útil y relevante para la toma de decisiones	S	S	S			P		P		S							
15 Cumplimiento de TI con las políticas internas			S												P			
Apre- ndizaje y Crecimiento	16 Personal del negocio y de las TI competente y motivado	S	S	P			S							P		P	S	
	17 Conocimiento, experiencia e iniciativas para la innovación de negocio	S	P					P	S		S						S	P

## APÉNDICE C

### MAPEO DETALLADO DE LAS METAS RELACIONADAS CON LAS TI Y LOS PROCESOS RELACIONADOS CON LAS TI

Este apéndice contiene la tabla de mapeo entre las metas relacionadas con TI y cómo son apoyadas por los procesos relativos a TI, como parte de las metas en cascada explicados en el capítulo 2.

La **figura 23** contiene:

- En columnas, las 17 metas genéricas relacionadas con TI definidas en el capítulo 2, agrupadas por las dimensiones del CMI.
- En filas, los 37 procesos de COBIT 5, agrupados por dominios.
- Un mapeo de cómo cada meta relacionada con TI es soportada por procesos de COBIT 5. Este mapeo se muestra usando la siguiente escala:
  - “P” indica principal, cuando hay una relación importante. Por ejemplo, el proceso de COBIT 5 proporciona un soporte imprescindible para conseguir las metas relacionadas con TI.
  - “S” indica secundario, cuando todavía hay un vínculo fuerte, pero menos importante. Por ejemplo, el proceso de COBIT 5 es un apoyo secundario para los procesos relativos a TI.

#### EJEMPLO 8-AP013 GESTIÓN DE LA SEGURIDAD

El proceso AP013 *Gestión de la Seguridad* contribuirá:

- Principalmente, a la consecución de las siguientes metas relacionadas con TI:
  - 02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
  - 04 Riesgos de negocio relacionados con las TI gestionados
  - 06 Transparencia de los costes , beneficios y riesgos de TI
  - 10 Seguridad de la Información, infraestructura para el procesamiento y aplicaciones
  - 14 Disponibilidad de información útil y relevante para la toma de decisiones
- En un menor grado, a la consecución de las siguientes metas relacionadas con TI:
  - 07 Entrega de los servicios de TI de acuerdo a los requisitos de negocio
  - 08 Uso adecuado de aplicaciones, información y soluciones tecnológicas

Esta tabla fue creada basándose en las siguientes aportaciones:

- Estudio realizado por el Instituto de Investigación en Alineamiento TI y Gobernanza de la Escuela de Dirección de Empresas de la Universidad de Amberes.
- Revisiones adicionales y opiniones de expertos obtenidas durante el proceso de desarrollo y revisión de COBIT 5.

Por favor, cuando use la tabla de la figura 23 tenga en cuenta las recomendaciones hechas en el capítulo 2 relativas al uso de metas de COBIT 5 en cascada.

**Figura 23—Mapeo entre las Metas Relacionadas con las TI de COBIT 5 y los Procesos**

Procesos de COBIT 5		Meta relacionada con las TI																
		Alineamiento de TI y la estrategia de negocio Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI Riesgos de negocio relacionados con las TI gestionados Realización de beneficios del portafolio de inversiones y Servicios relacionados con las TI Transparencia de los costos, beneficios y riesgos de las TI Entrega de servicios de TI de acuerdo a los requisitos del negocio Uso adecuado de aplicaciones, información y soluciones tecnológicas Agilidad de las TI Seguridad de la información, infraestructura de procesamiento y aplicaciones Optimización de activos, recursos y capacidades de las TI Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad. Disponibilidad de información útil y relevante para la toma de decisiones Cumplimiento de las políticas internas por parte de las TI Personal del negocio y de las TI competente y motivado Conocimiento, experiencia e iniciativas para la innovación de negocio																
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
		Financiera					Cliente				Interna						Aprendizaje y Crecimiento	
Evaluar, Orientar y Supervisar	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	P	S	P	S	S	P		S	S	S	S	S	S	S	S	
	EDM02	Asegurar la Entrega de Beneficios	P		S		P	P	P	S			S	S		S	P	
	EDM03	Asegurar la Optimización del Riesgo	S	S	S	P		P	S	S		P			S	S	P	
	EDM04	Asegurar la Optimización de los Recursos	S		S	S	S	S	S	S	P		P		S		P	
	EDM05	Asegurar la Transparencia hacia las partes interesadas	S	S	P			P	P					S	S	S	S	
Alinear, Planificar y Organizar	APO01	Gestionar el Marco de Gestión de TI	P	P	S	S			S		P	S	P	S	S	S	P	
	APO02	Gestionar la Estrategia	P		S	S	S		P	S	S		S	S	S	S	S	
	APO03	Gestionar la Arquitectura Empresarial	P		S	S	S	S	S	S	P	S	P	S		S	S	
	APO04	Gestionar la Innovación	S			S	P			P	P		P	S		S		
	APO05	Gestionar el portafolio	P		S	S	P	S	S	S		S			P		S	
	APO06	Gestionar el Presupuesto y los Costes	S		S	S	P	P	S	S			S		S			
	APO07	Gestionar los Recursos Humanos	P	S	S	S			S		S	S	P		P	S	P	
	APO08	Gestionar las Relaciones	P		S	S	S	S		P	S		S	P	S	S	P	
	APO09	Gestionar los Acuerdos de Servicio	S			S	S	S	P	S	S	S	S		S	P	S	
	APO10	Gestionar los Proveedores		S		P	S	S		P	S	P	S		S	S	S	
	APO11	Gestionar la Calidad	S	S		S	P		P	S	S		S		P	S	S	
	APO12	Gestionar el Riesgo		P		P		P	S	S	S	P			P	S	S	
	APO13	Gestionar la Seguridad		P		P		P	S	S		P			P			

# MAPEO DETALLADO DE LAS METAS RELACIONADAS CON LAS TI Y LOS PROCESOS RELACIONADOS CON LAS TI

**Figura 23—Mapeo entre las Metas Relacionadas con las TI de COBIT 5 y los Procesos (cont.)**

		Meta relacionada con las TI																
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
		Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
		Financiera					Cliente			Interna							Aprendizaje y Crecimiento	
Construcción, Adquisición e Implementación	BAI01	P	S	P	P	S	S	S	S	S	S	P	S	S	S	S	S	
	BAI02	P	S	S	S	S	S	P	S	S	S	S	P	S	S	S	S	
	BAI03	S	S	S	S	S	S	P	S	S	S	S	S	S	S	S	S	
	BAI04	S	S	S	S	S	P	S	S	S	P	S	S	P	S	S	S	
	BAI05	S	S	S	S	S	S	P	S	S	S	S	P	S	S	S	P	
	BAI06	S	S	P	S	S	P	S	S	P	S	S	S	S	S	S	S	
	BAI07	S	S	S	S	S	S	P	S	S	S	P	S	S	S	S	S	
	BAI08	S	S	S	S	S	S	S	P	S	S	S	S	S	S	S	P	
	BAI09	S	S	S	S	P	S	S	S	S	P	S	S	S	S	S	S	
	BAI10	P	S	S	S	S	S	S	S	S	P	S	S	P	S	S	S	
Entregar, dar Servicio y Soporte	DSS01	S	S	P	S	S	P	S	S	S	P	S	S	S	S	S	S	
	DSS02	S	S	P	S	S	P	S	S	S	S	S	S	S	S	S	S	
	DSS03	S	S	P	S	S	P	S	S	P	S	S	P	S	S	S	S	
	DSS04	S	S	P	S	S	P	S	S	S	S	S	P	S	S	S	S	
	DSS05	S	P	P	S	S	S	S	S	P	S	S	S	S	S	S	S	
	DSS06	S	S	P	S	S	P	S	S	S	S	S	S	S	S	S	S	
Supervisión, Evaluación y Verificación	MEA01	S	S	S	P	S	S	P	S	S	S	P	S	S	P	S	S	
	MEA02	P	S	P	S	S	S	S	S	S	S	S	S	S	P	S	S	
	MEA03	P	S	P	S	S	S	S	S	S	S	S	S	S	S	S	S	

## APÉNDICE D

### NECESIDADES DE LAS PARTES INTERESADAS (SOCIOS, ACCIONISTAS, ETC.) Y METAS EMPRESARIALES

En el Capítulo 4 se explicaron los diferentes pasos de las metas en cascada, comenzando por las necesidades de los interesados hasta llegar a las metas de los catalizadores. En el Capítulo 2 se incluía una tabla con las típicas cuestiones de gobierno y gestión sobre TI. Desde el punto de vista de las partes interesadas, es interesante conocer cuáles de estas cuestiones competen a las metas empresariales. Por tal motivo, se incluye la **figura 24** que muestra como una lista de las necesidades de las partes interesadas internas puede ser vinculada con las metas empresariales.

Esta tabla se puede usar para establecer y priorizar metas corporativas específicas o relacionadas con TI, basadas en las necesidades de las partes interesadas. Deben tomarse las mismas precauciones cuando se usen estas tablas que cuando se usen las otras tablas de metas en cascada, es decir, la situación de cada empresa es diferente y no deben usarse estas tablas de forma mecánica, sino sólo como sugerencia de un conjunto genérico de relaciones. En la **figura 24**, la intersección entre la necesidad de un interesado y una meta corporativa está coloreada si esa necesidad debe ser considerada para esa meta.

**Figura 24—Mapeo entre las Metas Corporativas de COBIT 5 y las Preguntas del Gobierno y la Gestión**

NECESIDADES DE LAS PARTES INTERESADAS	Valor para los Interesados de las Inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activos)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basada en información	Optimización de los costes de los procesos de negocio	Optimización de la funcionalidad de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas internas	Cumplimiento con políticas internas	Personas preparadas y motivadas	Cultura de Innovación de producto y negocio
	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
¿Cómo se consigue valor mediante el uso de TI? ¿Está el usuario final satisfecho con la calidad del servicio de TI?																	
¿Cómo se gestiona el rendimiento de TI?																	
¿Cómo se puede explotar mejor la tecnología de red para conseguir nuevas oportunidades estratégicas?																	
¿Cómo puedo construir y estructurar mejor mi departamento de TI?																	
¿Cuánto dependo de mis proveedores externos? ¿Cómo de bien están siendo gestionados los acuerdos de externalización de TI? ¿Cómo puedo verificarlos sobre proveedores externos?																	
¿Cuáles son los requisitos (de control) para la información?																	
¿He contemplado todo los riesgos relacionados con TI?																	
¿Estoy ejecutando una operación de TI eficiente y robusta?																	
¿Cómo se controla el coste de TI? ¿Cómo se usan los recursos de TI en la manera más efectiva y eficiente? ¿Cuáles son las opciones de aprovisionamiento más efectivas y eficientes?																	

Figura 24—Mapeo entre las Metas Corporativas de COBIT 5 y las Preguntas del Gobierno y la Gestión (cont.)

NECESIDADES DE LAS PARTES INTERESADAS	Valor para los Interesados de las Inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activos)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basada en Información	Optimización de los costes de los procesos de negocio	Optimización de la funcionalidad de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas internas	Cumplimiento con políticas internas	Personas preparadas y motivadas	Cultura de innovación de producto y negocio
	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
¿Tengo suficiente personal para TI? ¿Cómo puedo desarrollar y mantener sus habilidades y cómo gestiono su rendimiento?																	
¿Cómo consigo confianza sobre TI?																	
¿Está bien securizada la información que se está procesando?																	
¿Cómo se puede mejorar la capacidad de respuesta del negocio mediante un entorno de IT más flexible?																	
¿Fracasan los proyectos de TI en proporcionar lo que habian prometido? Si es así, ¿por qué permanece la TI en el camino de ejecutar la estrategia de negocio?																	
¿Cómo es de crítica la TI para para la sostenibilidad de la empresa? ¿Qué pasaría si la TI no estuviera disponible?																	
¿Qué procesos de negocio críticos dependen de TI y cuáles son los requerimientos de los procesos de negocio?																	
¿En cuánto han excedido de media los presupuestos de operación de TI? ¿Con qué frecuencia y cuánto se salen del presupuesto los proyectos de TI?																	
¿Qué parte del esfuerzo de TI se dedica a apagar fuegos en lugar de facilitar las mejoras del negocio?																	
¿Son suficientes los recursos y la infraestructura de TI disponibles para conseguir los objetivos estratégicos de empresa requeridos?																	
¿Cuánto se tarda en la toma de decisiones importantes de TI?																	
¿Son transparentes el esfuerzo y las inversiones totales en TI?																	
¿Respalda TI a la empresa en el cumplimiento de la normativa y los niveles de servicio? ¿Cómo puedo saber si se cumple con todas las normas aplicables?																	

## Anexo 02

### Instalación y configuración del servicio DHCP en Linux Ubuntu

El protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol) es un estándar TCP/IP diseñado para simplificar la administración de la configuración IP de los equipos de nuestra red.

Si se dispone de un servidor DHCP, la configuración IP de los PCs puede hacerse de forma automática sin necesidad de hacerlo manualmente.

Un servidor DHCP es un servidor que recibe peticiones de clientes solicitando una configuración de red IP. El servidor responderá a dichas peticiones proporcionando los parámetros que permitan a los clientes autoconfigurarse. Para que un PC solicite la configuración a un servidor, en la configuración de red de los PCs hay que seleccionar la opción 'Obtener dirección IP automáticamente'.

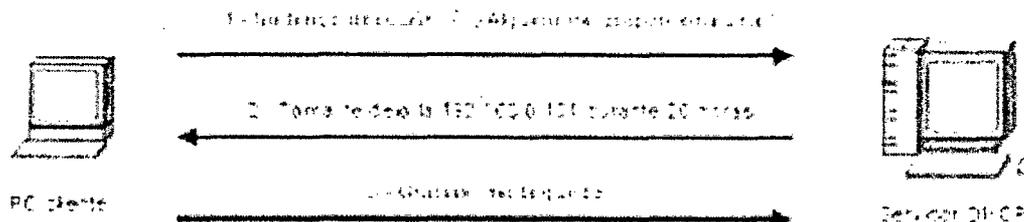
El servidor proporcionará al cliente al menos los siguientes parámetros:

- Dirección IP
- Máscara de subred

Opcionalmente, el servidor DHCP podrá proporcionar otros parámetros de configuración tales como:

- Puerta de enlace
- Servidores DNS
- Muchos otros parámetros más

El servidor DHCP proporciona una configuración de red TCP/IP segura y evita conflictos de direcciones repetidas. Utiliza un modelo cliente-servidor en el que el servidor DHCP mantiene una administración centralizada de las direcciones IP utilizadas en la red. Los clientes podrán solicitar al servidor una dirección IP y así poder integrarse en la red.



## Instalación del servidor DHCP

Para instalar los archivos necesarios del servidor DHCP se puede utilizar apt-get desde una consola de root:

```
// Instalación del servidor DHCP
apt-get install dhcp3-server
```

## Configuración del servidor DHCP

Al igual que todas las aplicaciones en Linux, el servidor DHCP dispone de su propio archivo de configuración. Se trata del archivo:

```
// Archivo de configuración del servidor DHCP
/etc/dhcp3/dhcpd.conf
```

Este archivo de configuración consta de una primera parte principal donde se especifican los parámetros generales que definen el 'alquiler' y los parámetros adicionales que se proporcionarán al cliente.

Los rangos de direcciones IP se especifican en secciones que empiezan con la palabra clave 'subnet' seguido de la dirección de red de la subred, continua con la palabra 'netmask' seguido de la máscara de red. A continuación estará la lista de parámetros para dicha sección encerrados entre llaves.

Si además de proporcionar al cliente la dirección IP y la máscara deseamos que le proporcione también la dirección de la puerta de enlace y las direcciones de dos servidores DNS para que pueda navegar por Internet, la sección subnet que debemos crear será:

```
// Rango de cesión y parámetros adicionales
subnet 192.168.1.0 netmask 255.255.255.0 {
option routers 192.168.1.254;
option domain-name-servers 80.58.0.33, 80.58.32.97;
range 192.168.1.60 192.168.1.90;
}
```

También se pueden hacer reservas de IP para un determinado equipo, en función de la MAC de su tarjeta de red. Para establecer una configuración de equipo es necesario crear una sección host. Ejemplo, si deseamos que el cliente cuya dirección MAC sea 00:0c:29:c9:46:80 se configure siempre (reserva de dirección IP) con la dirección IP 192.168.1.50 y puerta de enlace 192.168.1.254, que su nombre de dominio sea "ieslapaloma.com" y el servidor de nombres netbios sea "192.168.1.250" la sección host que debemos crear será:

```
// Crear una reserva de dirección IP
host Profesor5 {
hardware ethernet 00:0c:29:c9:46:80;
fixed-address 192.168.1.50;
option routers 192.168.1.254;
option domain.name "ieslapaloma.com";
option netbios-name-servers 192.168.1.250;
}
```

Cuando el PC cuya dirección MAC sea '00:0c:29:c9:46:80' solicite una dirección IP al servidor DHCP, recibirá la 192.168.1.50.

### Archivo dhcpd.conf comentado

A continuación mostramos un sencillo archivo dhcpd.conf comentado línea por línea: (Todas las líneas que comienzan por almoadilla (#) son líneas de comentarios y son ignoradas por el servidor dhcp. Todas las líneas que especifican parámetros deben terminar en punto y coma ';')

```
// Ejemplo de archivo dhcp.conf
Sample configuration file for ISC dhcpd for Debian
$Id: dhcpd.conf,v 1.4.2.2 2002/07/10 03:50:33 peloy Exp $

Opciones de cliente y de dhcp aplicables por defecto a todas las secciones

Estas opciones pueden ser sobreescritas por otras en cada sección

option domain-name-servers 195.53.123.57; # DNS para los clientes (atenea)
option domain-name "ieslapaloma.com"; # Nombre de dominio para los clientes
option subnet-mask 255.255.255.0; # Máscara por defecto para los clientes
```

```
default-lease-time 600; # Tiempo en segundos del 'alquiler'
max-lease-time 7200; # Máximo tiempo en segundos que durará el 'alquiler'
```

---

```
Especificación de un rango
subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.1.60 192.168.1.80; # Rango de la 60 a la 80 inclusive
option broadcast-address 192.168.1.255; # Dirección de difusión
option routers 192.168.1.254; # Puerta de enlace
option domain-name-servers 80.58.0.33; # DNS (ej: el de telefónica)
default-lease-time 6000; # Tiempo
}
```

---

```
Configuración particular para un equipo
host aula5pc6 {
hardware ethernet 00:0c:29:1e:88:1d; # Dirección MAC en cuestión
fixed-address 192.168.1.59; # IP a asignar (siempre la misma)
}
```

Si se desea consultar las concesiones de direcciones en nuestra red podemos consultar el fichero `/var/lib/dhcp3/dhcpd.leases` del servidor dónde podrás encontrar algo similar a:

```
All times in this file are in UTC (GMT), not your local timezone. This is
not a bug, so please don't ask about it. There is no portable way to
store leases in the local timezone, so please don't request this as a
feature. If this is inconvenient or confusing to you, we sincerely
apologize. Seriously, though - don't ask.
The format of this file is documented in the dhcpd.leases(5) manual page.
This lease file was written by isc-dhcp-V3.0.6
```

```
lease 172.16.15.239 {
starts 2 2008/10/21 19:01:21;
ends 2 2008/10/21 19:11:21;
tstp 2 2008/10/21 19:11:21;
binding state free;
hardware ethernet 00:0c:29:ba:40:2f;
}
lease 172.16.15.240 {
starts 2 2008/10/21 19:17:29;
ends 2 2008/10/21 19:27:29;
tstp 2 2008/10/21 19:27:29;
binding state free;
hardware ethernet 00:0c:29:24:0d:dc;
}
lease 172.16.15.239 {
starts 2 2008/10/21 19:35:29;
```

```
ends 2 2008/10/21 19:45:29;
binding state active;
next binding state free;
hardware ethernet 00:0c:29:ba:40:2f;
client-hostname "profe-desktop";
}
```

Fuente:

Página del isftic :

Curso: Redes de Área Local. Aplicaciones y servicios en Linux.

Curso: Redes de Área Local. Aplicaciones y servicios en Linux.

[http://www.isftic.mepsyd.es/formacion/enred/index\\_formacion.php](http://www.isftic.mepsyd.es/formacion/enred/index_formacion.php)

## Anexo 03

### Instalación y configuración del servicio TFTP en Linux Ubuntu

TFTP (Trivial file transfer Protocol), se trata de un protocolo de transferencia de ficheros bastante básico y que es utilizado principalmente para transferir pequeños archivos entre equipos... En nuestro caso, este protocolo nos sera muy útil a la hora de virtualizar dispositivos CISCO en GNS3, ya que tendremos que cargar ciertos ficheros en estos dispositivo mediante la utilización de un servidor tftp... Pero esto ya es otra historia que veremos en un futuro... de momento vamos a centrarnos en instalar y poner en marcha un servidor tftp en Ubuntu.

Lo primero que tenemos que hacer es instalar el servidor tftp, para ello utilizamos el siguiente comando:

```
apt-get install tftpd-hpa
```

Una vez hecho esto, se edita el fichero de configuración:

```
nano /etc/default/tftpd-hpa
```

Según muestra la imagen:

```
root@alberto-ubuntu: ~
GNU nano 2.2.6 Archivo: /etc/default/tftpd-hpa Modificado
/etc/default/tftpd-hpa
TFTP_USERNAME="tftp"
TFTP_DIRECTORY="/var/lib/tftpboot"
TFTP_ADDRESS="0.0.0.0:69"
TFTP_OPTIONS="--secure"
RUN_DAEMON="yes"
OPTIONS="-c -l -s /var/lib/tftpboot"
^G Ver ayuda ^O Guardar ^R Leer Fich ^Y Repág. ^K Cortar Tex ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^V Pág. Sig. ^U PegarTxt ^I Ortografía
```

Luego se dan permisos para acceder al directorio raíz del servidor tftp:

```
chmod 777 /var/lib/tftpboot
```

Y por último, iniciamos el servicio:

```
start tftpd-hpa
```

Y con esto ya tenemos funcional nuestro servidor tftp.

## Anexo 04

### Instalación y configuración del servicio NTFS en Linux Ubuntu

**NFS (Network File System)**, es un popular protocolo utilizado para compartir sistemas de archivos de manera transparente entre anfitriones dentro de una red de área local. Es utilizado para sistemas de archivos distribuido.

Fue desarrollado en 1984 por Sun Microsystems, teniendo en mente la independencia del anfitrión, sistema operativo, protocolo de transporte. Funciona a través de los protocolos **XDR** (nivel de presentación del modelo OSI de TCP/IP) y **ONC RPC** (nivel de sesión del modelo OSI de TCP/IP).

Es muy popular entre sistemas basados sobre el estándar POSIX y viene incluido en la mayoría de éstos de modo predeterminado. Es muy fácil de configurar y utilizar, sin embargo cabe señalar que hay quienes denominan *cariñosamente* a **NFS** como "*No File Security*", pues carece de soporte para validar usuarios por contraseñas, como lo hacen otras alternativas como Samba. Su seguridad se basa sobre listas de de control de acceso compuestas por direcciones IP o nombres de anfitrión. Es por ésto que es importante que el administrador de la red de área local comprenda que un servidor NFS puede ser un serio problema de seguridad, si éste es configurado incorrectamente.

Existen tres versiones de NFS que se utilizan hoy en día:

- **NFSv2**: Es la versión más antigua y mejor soportada.
- **NFSv3**: Tiene más características que NFSv2, como el manejo de archivos de tamaño variable y mejores informes de errores. Sólo es parcialmente compatible con los clientes para NFSv2.

- **NFSv4:** Es la versión más moderna, y, entre otras cosas, incluye soporte para seguridad a través de Kerberos, soporte para ACL y utiliza operaciones con descripción del estado.

Salvo que se trate de directorios de acceso público, se recomienda utilizar **NFS** sólo dentro de una red de área local detrás de un muro contrafuegos y que sólo se permita el acceso a los anfitriones que integren la red de área local y evitar compartir sistemas de archivos con información sensible a través de Internet

### Procedimiento de Instalación de un servidor NFS

```
apt-get install nfs-kernel-server nfs-common portmap
Editar el fichero /etc/exports
/etc/exports: the access control list for filesystems which may be exported
to NFS clients. See exports(5).
##
Example for NFSv2 and NFSv3:
/srv/homes hostname1(rw, sync) hostname2(ro, sync)
##
Example for NFSv4:
/srv/nfs4 gss/krb5i(rw, sync, fsid=0, crossmnt)
/srv/nfs4/homes gss/krb5i(rw, sync)
##
especificar la ruta donde se encuentra el contenido del CD-ROM de Ubuntu
7.04
##
Y se indica que red (192.168.5.0) tiene permisos para acceder a dicha carpeta
/
tftpboot/ubuntu-desktop 192.168.5.0/255.255.255.0(sync)
Reiniciar el servidor NFS.
/etc/init.d/nfs-kernel-server restart
Editamos el fichero /etc/hosts.allow
/etc/hosts.allow: list of hosts that are allowed to access the system.
See the manual pages hosts_access(5), hosts_options(5)
and /usr/doc/netbase/portmapper.txt.gz
##
Example: ALL: LOCAL @some_netgroup
ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
##
If you're going to protect the portmapper use the name "portmap" for the
daemon name. Remember that you can only use the keyword "ALL" and IP
```

# addresses (NOT host or domain names) for the portmapper, as well as for  
# rpc.mountd (the NFS mount daemon). See portmap(8), rpc.mountd(8) and  
# /usr/share/doc/portmap/portmapper.txt.gz for further information.

##

Indicar la red que tiene permisos para acceder a NFS

#

ALL: 192.168.5.0/255.255.255.0

## **Anexo 05**

### **Instalación y configuración del servicio XDMCP en Linux**

XDMCP es un estándar del Open Group el «protocolo de control de administración de la pantalla X» (X Display Manager Control Protocol). Se utiliza para configurar las conexiones entre sistemas remotos a través de la red.

XDMCP es práctico en situaciones multiusuario en las que existen usuarios con estaciones de trabajo y un servidor muy potente que puede proporcionar los recursos para ejecutar múltiples sesiones X. Por ejemplo, XDMCP es una buena forma de reutilizar viejos ordenadores -un Pentium e incluso un 486 con 16Mb de RAM es suficiente para ejecutar las X y utilizar XDMCP como un ordenador que puede ejecutar sesiones del moderno KDE en el servidor. Por parte del servidor, una vez que se está ejecutando una sesión de KDE (u otro entorno), ejecutar otra necesitará pocos recursos extra.

Sin embargo, permitir otros métodos de acceso a su máquina, obviamente, tiene implicaciones de seguridad. Debería ejecutar este servicio únicamente si necesitase permitir el acceso a servidores X remotos para que inicien sesiones de acceso en su sistema. Los usuarios con un sencillo ordenador con UNIX® no necesitan ejecutar esto.

#### **Control de acceso XDMCP**

El archivo especificado en la opción AccessFile proporciona información que kdm utiliza para controlar el acceso a la petición de servicios a través de XDMCP. El archivo contiene cuatro tipos de entrada: Las entradas que controlan la respuesta a peticiones «Direct» y «Broadcast», entradas que responden a peticiones «Indirect», macro definiciones para las entradas «Indirect», y las entradas que controlan en qué interfaz de red escucha kdm las peticiones de XDMCP. Las líneas en blanco se ignoran, # se trata como un delimitador de comentario provocando que el resto de la línea se ignore, y \ provoca que se ignore el salto de línea, lo que permite utilizar varias líneas para definir listas de servidores.

El formato de las entradas «Direct» es sencilla, bien el nombre del servidor o bien un patrón, se comparan con el nombre del servidor del dispositivo de visualización. Los patrones se distinguen de los nombres de servidor por la

inclusión de uno o más meta caracteres. \* coincide con una secuencia de 0 o más caracteres, y ? coincide con cualquier caracter individual. Si la entrada es un nombre de servidor, todas las comparaciones se hacen utilizando las direcciones de red, por tanto, se utilizará cualquier nombre que pueda convertirse en una dirección de red. Para los patrones, únicamente se utilizan nombres de servidor canónicos en la comparación, para asegurarse de que no van a coincidir con los alias. Los nombres de servidor de las peticiones XDMCP siempre contendrán un nombre de dominio local incluso si la búsqueda inversa devuelve un nombre corto, por tanto, podrá utilizar patrones para el dominio local. Si está precedido de un caracter ! esta entrada se excluirá. Precedido de un = no tendrá efecto, aunque se requiere cuando se especifica una macro para distinguir la entrada de la definición de la macro. La única respuesta a las peticiones «Direct» para un servidor o patrón, podrá ser seguida de la palabra clave opcional NOBROADCAST. Esto se utiliza para evitar que se haga visible un servidor kdm en los menús que se basa en peticiones «Broadcast».

Una entrada «Indirect» también puede contener un nombre de servidor o un patrón, pero seguido de una lista de servidores o macros que las peticiones deberían seguir. Las entradas «Indirect» también pueden ser excluidas en el caso de que se proporcione un nombre de un servidor ficticio (válido) para hacer la entrada diferenciable de un entrada «Direct». Si está compilado con soporte IPv6, se puede incluir el envío a varias direcciones de grupos de red en la lista de direcciones de las peticiones que se hagan. Si el servidor indirect contiene la palabra CHOOSER, las peticiones «Indirect» no se reenvían y en su lugar se muestra el diálogo selector de servidores de kdm. El selector enviará una petición «Direct» a cada uno de los restantes nombres de servidor de la lista y ofrecerá un menú con todos los servidores que hayan respondido. La lista de servidores puede contener la palabra clave BROADCAST, para hacer que el selector envíe una petición «Broadcast». Tenga en cuenta que en algunos sistemas operativos los paquetes UDP no se pueden distribuir y en este caso esta característica no funcionará.

Cuando se está probando el acceso a un servidor de visualización particular, se comprueba cada entrada y la primera entrada que coincide determina la respuesta. Las entradas «Direct» y «Broadcast» se ignoran cuando se está buscando una entrada «Indirect» y viceversa.

Una macrodefinición contiene un nombre de la macro y una lista de los nombres de los servidores y de otras macros que la macro expande. Para distinguir las macros de los nombres de servidor, los nombres de las macros comienzan por un caracter %.

El último tipo de entrada es la directiva LISTEN. La sintaxis formal es

## **LISTEN [*interfaz* [*lista multicast*]]**

Si se especifican una o más líneas LISTEN, kdm escucha las peticiones XDMCP únicamente en los interfaces especificados. *interfaz* puede ser un nombre de servidor o una dirección IP que represente una interfaz de red en esta máquina, o el comodín \* para representar todas las interfaces de red disponibles. Si se lista un grupo multicast en una línea LISTEN, kdm une los grupos multicast a las interfaces dadas. Para el multicast en IPv6, el IANA tiene asignado ff0X:0:0:0:0:0:0:12b como el rango de direcciones multicast asignados de forma permanente para XDMCP. La X puede ser reemplazada por cualquier identificador de ámbito válido, como 1 para el nodo local, 2 para el enlace local, 5 para el sitio local, y así sucesivamente (véa IETF RFC 2373 o su reemplazo para ver las definiciones y detalles más amplios). kdm escucha de forma predeterminada en la dirección de ámbito local ff02:0:0:0:0:0:0:12b que es la más parecida en cuanto al comportamiento para broadcast en subredes IPv4. Sino se proporcionan líneas LISTEN, kdm escuchará en todos los interfaces y se une al grupo multicast predeterminado IPv6 para XDMCP (cuando se compila con soporte IPv6). Para desactivar por completo la escucha para las peticiones XDMCP, se puede especificar una línea LISTEN sin direcciones, aunque es preferible utilizar la opción

## 1. Introducción.

Linux es un sistema operativo de la familia Unix, gratuito, creado mediante la política de "código abierto" <sup>[viii]</sup>. Estas características implican un gran ahorro en los costes de instalación de los equipos, pero también una mayor especialización por parte del personal informático.

En todo sistema Unix existe un usuario administrador (**root**), que controla el funcionamiento completo del sistema, tiene acceso universal y puede realizar cualquier operación con los datos y los dispositivos de la máquina.

Este curso se ofrece originalmente en el Plan de Formación para personal informático de la Universidad de Sevilla <sup>[ix]</sup> y va dirigido principalmente a personas que, habiendo trabajado con el sistema operativo Linux y teniendo nociones esenciales de programación en BASH, se interesen por la realización de labores administrativas básicas en el sistema.

### 1.1. Tareas del administrador.

El administrador de cualquier tipo de servidor debe ser una persona especializada, que conozca lo mejor posible sus equipos, sus aplicaciones y sus usuarios; manteniéndose al día en los avances tecnológicos, en las revisiones y parches de los programas instalados y en las necesidades de su empresa.

#### 1.1.1. Planificación y previsión de necesidades.

Una de las funciones principales en la administración de sistemas informáticos es la planificación detallada de las tareas de gestión, lo que puede evitar sorpresas desagradables en el momento de ejecutarlas.

El analista de sistemas tiene la obligación de asesorar al personal administrativo de su empresa sobre las necesidades tecnológicas en la adquisición de material informático, estimando los recursos que precisen los usuarios, en relación con las posibilidades económicas de la empresa.

Una vez recibido el equipo debe realizarse un plan de instalación, en el que se incluya, al menos la siguiente información:

- Documentación y estudio de los recursos disponibles.
- Previsión de posibles ampliaciones.
- Relleno de solicitud de alta en la red informática corporativa y activación de los parámetros de conexión.

- Documentación de necesidades del entorno de operación (SAI, aire acondicionado, etc.).
- Documentación sobre registro, configuración, instalación y actualización del sistema operativo, de las aplicaciones requeridos y de los programas propios, de acuerdo con los servicios que debe prestar el nuevo equipo.
- Creación y publicación de solicitudes de apertura y modificación de cuentas de usuarios, de instalación de programas, de mejora de recursos, etc.

### **1.1.2. Documentación.**

El responsable del sistema se compromete a realizar también documentación interna para el Centro de Cálculo, que debe describir las siguientes necesidades:

- Registro actualizado de los usuarios y grupos del sistema.
- Políticas de utilización y permisos para cada grupo de usuarios.
- Descripción de los procedimientos comunes que deben ejecutar los operadores del sistema (copias de seguridad, gestión de cuentas, informes, etc.).
- Registro completo y actualizado de los cambios en la configuración del servidor (sistema operativo, aplicaciones, ficheros, etc.).
- Recogida periódica y archivado de datos sobre el rendimiento del sistema y de sus componentes.

### **1.1.3. Automatización.**

El personal informático de una empresa ha de ejecutar periódicamente las funciones definidas en el plan de actuación. El programador necesita automatizar la mayoría de estos procedimientos repetitivos para evitar errores tipográficos o conceptuales, y para mejorar el tratamiento general de las aplicaciones.

En cada servidor deben automatizarse, al menos, las siguientes tareas:

- Comprobación del espacio libre en los discos.
- Gestión de cuentas de usuarios y revisión periódica de las cuotas de disco.
- Procedimientos para crear, comprobar y restaurar copias de seguridad, según el plan de actuación.
- Comprobación y registro del rendimiento general del sistema y de la red informática.

- Trabajos específicos (informes, gestión de servicios, creación de documentación, etc.).
- Creación de alertas de seguridad (comprobación de cambios, detección de intrusos, etc.).

#### **1.1.4. Informar a los usuarios.**

El administrador de sistema debe también mantener informados a sus usuarios y darles unas guías de operación y buen uso, lo que puede evitar errores provocados por desconocimiento.

También es necesario informar sobre los cambios que pueden afectar a cada grupo de usuarios, indicando la siguiente información <sup>[1]</sup>:

- La naturaleza de los cambios que van a realizarse en el sistema y su evolución temporal.
- Cuándo se realizará cada modificación.
- Qué resultados se esperan obtener con la operación y cuáles son los obtenidos.
- Tiempo estimado y tiempo real de la duración de la operación.
- Impacto posible sobre los usuarios (nueva configuración, parada del sistema, etc.).
- Información de contacto para recoger dudas y consultas.

Por otro lado, el encargado del sistema tiene la obligación de conocer profundamente el comportamiento general de sus usuarios, registrando sus consultas, sus sugerencias y los datos de rendimiento y utilización de recursos. Esto permite ofrecer una mejor calidad en los servicios ofertados.

#### **1.1.5. Control de la seguridad del sistema.**

Dependiendo del tipo de información tratada por el sistema, el administrador debe definir sus políticas de seguridad, tanto para el servidor, como para la red corporativa, ya que los usuarios tienen derecho a la privacidad e integridad de sus datos.

Deben ponerse los medios para evitar posibles ataques o fallos informáticos que afecten –o incluso paralicen– el funcionamiento normal de la máquina.

Nunca hay que tener la presunción de que un sistema es completamente seguro o de que sólo puede ser atacado desde fuera. Por ello, el *superusuario* debe realizar las siguientes operaciones:

- Activar y revisar los registros históricos de incidencias.

- Realizar revisiones periódicas sobre posibles cambios no deseados en el sistema.
- Instalar aplicaciones y dispositivos que protejan a los servidores y a la red informática (sistemas de detección de intrusos, cortafuegos, filtros, lectores de tarjetas de acceso, etc.)..

### **1.1.6. Previsión de fallos.**

Por último, la empresa debe poner los medios físicos necesarios para prevenir y corregir los posibles fallos informáticos.

Por otra parte, los cambios ambientales (eléctricos, temperatura, humedad, ...) son algunos de los aspectos más importantes y costosos en la prevención de errores

. Debe hacerse hincapié en los siguientes temas:

- Tener una correcta instalación eléctrica, que evite caídas y subidas inesperadas de tensión, así como instalar sistemas de alimentación ininterrumpida (SAI) que protejan los servicios críticos de la empresa (armarios de comunicaciones, servidores, etc.).
- Tener un adecuado sistema de aire acondicionado, que filtre y regule la temperatura y la humedad del ambiente, sin que afecte a la salud de los operadores.
- Contar con un alumbrado adecuado, que no afecte al tendido eléctrico informático.
- Mantener una adecuada infraestructura en la red informática, con acceso cómodo y restringido a los dispositivos de comunicaciones.

Otras posibles causas de fallos más difíciles de prever son:

- Saturación o fallo de los recursos del sistema (procesadores, memoria, discos, etc.). Hay que sopesar la necesidad de solicitar la ampliación o sustitución de los componentes afectados.
- Fallos de programación, tanto en el S.O., como en las aplicaciones instaladas o en los programas propios. El administrador debe mantenerse informado sobre las actualizaciones y parches que instalar.
- Errores humanos del propio administrador, de los operadores, del servicio técnico o de los usuarios finales.

## 2. Usuarios y grupos.

Un usuario Unix representa tanto a una persona (**usuario real**) como a una entidad que gestiona algún servicio o aplicación (**usuario lógico o ficticio**) <sup>[2]</sup>.

Todo usuario definido en el sistema se corresponde con un identificador único (**UID**) y con una **cuenta**, donde se almacenan sus datos personales en una zona de disco reservada.

Un **grupo** es una construcción lógica –con un nombre y un identificador (**GID**) únicos– usada para conjuntar varias cuentas en un propósito común <sup>[1]</sup>, compartiendo los mismos permisos de acceso en algunos recursos. Cada cuenta debe estar incluida como mínimo en un grupo de usuarios, conocido como **grupo primario** o **grupo principal**.

### 2.1. Características generales de una cuenta.

Las características que definen la cuenta de un usuario son:

- Tiene un nombre y un identificador de usuario (UID) únicos en el sistema.
- Pertenece a un grupo principal.
- Puede pertenecer a otros grupos de usuarios.
- Puede definirse una información asociada con la persona propietaria de la cuenta.
- Tiene asociado un directorio personal para los datos del usuario.
- El usuario utiliza en su conexión un determinado intérprete de mandatos, donde podrá ejecutar sus aplicaciones y las utilidades del sistema operativo.
- Debe contar con una clave de acceso personal y difícil de averiguar por parte de un impostor.
- Tiene un perfil de entrada propio, donde se definen las características iniciales de su entorno de operación.
- Puede tener una fecha de caducidad.
- Pueden definirse cuotas de disco para cada sistema de archivos.
- Es posible contar con un sistema de auditoria que registre las operaciones realizadas por el usuario.

## 2.2. Ficheros del sistema.

Linux proporciona varios métodos para la definir los usuarios que pueden conectarse al sistema. Lo típico es definir localmente en cada servidor las cuentas de los usuarios y grupos, aunque también pueden usarse métodos externos de autenticación, que permiten que varias máquinas compartan las mismas definiciones para sus usuarios comunes.

La siguiente tabla muestra los ficheros del sistema involucrados en el proceso de definición de los usuarios locales.

Formato	Descripción
<b>/etc/passwd</b>	
<i>Usuario:x:UID:GID:Descrip:Direct:Shell</i> ...	Fichero principal de descripción de usuarios locales. Sus campos son: <ol style="list-style-type: none"><li>1. Nombre de usuario.</li><li>2. No usado (antiguamente, clave).</li><li>3. Identificador de usuario (UID).</li><li>4. Identificador del grupo primario.</li><li>5. Descripción o nombre completo de la persona que representa dicho usuario.</li><li>6. Directorio personal.</li><li>7. Intérprete de mandatos.</li></ol>
<b>/etc/shadow</b>	
<i>Usuario:clave:F1:N1:N2:N3:N4:Caduc:</i> ...	Fichero oculto que incluye la codificación y las restricciones de las claves de acceso a las cuentas. Sus campos son: <ol style="list-style-type: none"><li>1. Nombre de usuario.</li><li>2. Clave codificada.</li><li>3. Fecha del último cambio de clave.</li><li>4. Días hasta que la clave pueda ser cambiada.</li><li>5. Días para pedir otro cambio de clave.</li><li>6. Días para avisar del cambio de la clave.</li></ol>

	<p>7. Días para deshabilitar la cuenta tras su caducidad.</p> <p>8. Fecha de caducidad.</p> <p>9. Reservado (normalmente ignorado).</p> <p>Nota: Las fechas se expresan como el nº de días desde el 1/1/1.970.</p>
<b>/etc/group</b>	
<p><i>Grupo:x:GID:Usuarios</i></p> <p>...</p>	<p>Contiene la definición de los grupos de usuarios. Sus campos son:</p> <ol style="list-style-type: none"> <li>1. Nombre del grupo.</li> <li>2. No usado (antiguamente, clave del grupo).</li> <li>3. Identificador del grupo (GID).</li> <li>4. Lista de miembros (separada por comas).</li> </ol>
<b>/etc/gshadow</b>	
<p><i>Grupo:Clave:Admins:Usuarios</i></p> <p>...</p>	<p>Fichero oculto y opcional que contiene las claves de grupos privados. Sus campos son:</p> <ol style="list-style-type: none"> <li>1. Nombre del grupo.</li> <li>2. Clave codificada (opcional).</li> <li>3. Lista de usuarios administradores.</li> <li>4. Lista de usuarios normales.</li> </ol>

### 2.3. Usuarios y grupos predefinidos.

En todos los "dialectos" Unix existen algunos usuarios y grupos predefinidos por el sistema operativo, que se utilizan para la gestión y el control de los distintos servicios ofrecidos por el ordenador.

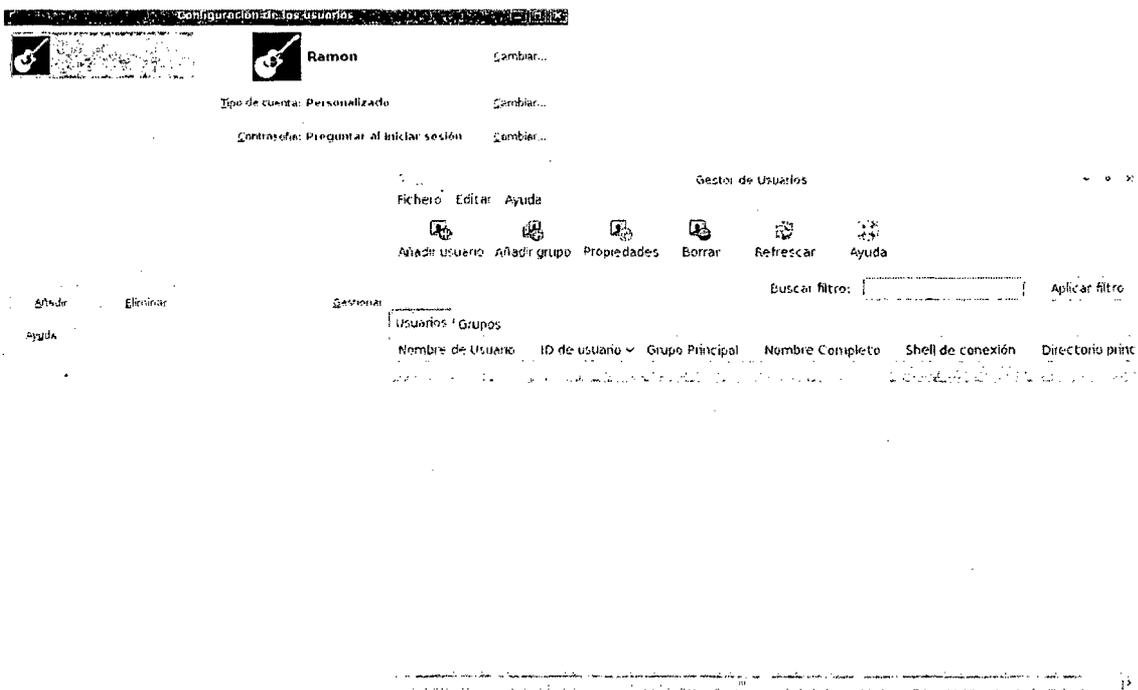
En especial el **usuario** root -con **UID 0**- es el administrador de la máquina, con un control total sobre el sistema. Existe también un **grupo** root -con **GID 0**- con características administrativas, al que pertenece el citado usuario.

Como ejemplo, la siguiente tabla lista algunos de los usuarios y grupos predefinidos en Fedora 13<sup>(1)</sup> y en Ubuntu 10.04 Lucid<sup>(2)</sup>, indicando también las posibles diferencias.

<b>Usuario</b>	<b>UID<sup>(1)</sup></b>	<b>UID<sup>(2)</sup></b>	<b>Descripción</b>
root	0	0	Administrador con control total.
bin	1	2	Propietario de las utilidades del sistema operativo.
daemon	2	1	Gestor de servicios generales.
adm	3		Propietario de los archivos de registros históricos y administrativos.
sys		3	
lp	4	7	Administrador de los servicios de impresión.
nobody	99	65534	Gestor de servicios varios.
ftp	14	50	Controlador del acceso al árbol del servicio FTP anónimo..
sshd	74	123	Usuario ficticio gestor del servicio SSH.
apache	48		Propietario de los ficheros y directorios del servicio de hipertexto Apache.
www-data		33	
squid	23		Controlador del servicio de representación Squid.
proxy		13	
<b>Grupo</b>	<b>GID<sup>(1)</sup></b>	<b>GID<sup>(2)</sup></b>	<b>Descripción</b>
root	0	0	Administradores con control total.
bin	1	2	Binarios del sistema.
daemon	2	1	Servicios generales.
sys	3	3	Control del sistema.
adm	4	4	Ficheros históricos y administrativos.
tty	5	5	Acceso a la consola.
lp	7	7	Servicio de impresión.
kmem	9	15	Control de memoria del núcleo de Linux.

cdrom	11	24	Acceso a discos extraíbles (CD-ROM, DVD).
man	15	12	Páginas de manuales.
admin		123	Administradores que pueden ejecutar la orden sudo.
apache	488		Servicio de hipertexto HTTP.
www-data		33	
sshd	484		Servicio de conexión segura SSH.
ssh		111	
users	100	100	Usuarios normales.
nobody	99	65534	Control de servicios.
squid	23		Servicio representante.
proxy		13	

El gráfico siguiente muestra la ejecución de herramientas para gestión básica de usuarios como **users-admin** del entorno GNOME 2.30 bajo Ubuntu 10.04 Lucid (izquierda) y **system-config-users** de Fedora 13 (derecha).



Los usuarios ficticios, que gestionan los servicios ofrecidos por el ordenador, deben tener su cuenta deshabilitada para evitar una posible puerta de entrada para los intrusos. Esto se consigue bloqueando la clave de acceso y asignando `/sbin/nologin` como intérprete de mandatos de la cuenta.

### 2.3.1. El usuario root definido por defecto.

Ubuntu y Fedora establecen en sus programas de instalación distintas políticas para definir la forma de trabajar por defecto con la cuenta de superusuario (root).

Como se puede comprobar en el apartado anterior, en ambos casos la cuenta tiene el mismo nombre y los mismos parámetros de UID y GID. Sin embargo, el programa de instalación de Fedora pide establecer una clave para dicho usuario, mientras que el de Ubuntu no la solicita.

Ubuntu no permite conectarse directamente al sistema como `root` y sólo los usuarios que pertenecen al grupo `admin` pueden ejecutar órdenes con privilegios usando la orden `sudo` e introduciendo su propia clave.

La siguiente tabla muestra un resumen de las diferencias entre ambos sistemas operativos definiendo la cuenta `root`.

Característica	Ubuntu 10.04	Fedora 13
Clave de acceso	Sin clave	Definida en la instalación
Acceso al sistema	Sin acceso	Con acceso
Un usuario puede ejecutar órdenes como <code>root</code>	Orden <code>sudo</code> (miembros del grupo <code>admin</code> )	Orden <code>sudo</code> sin configurar
Un usuario puede ejecutar el intérprete de <code>root</code>	<code>sudo su</code> (miembros del grupo <code>admin</code> )	<code>su</code> (cualquier usuario)

### 2.4. Clave de acceso.

Como se ha indicado anteriormente, las claves de los usuarios locales de Linux se guardan codificadas en el fichero inaccesible `/etc/shadow`.

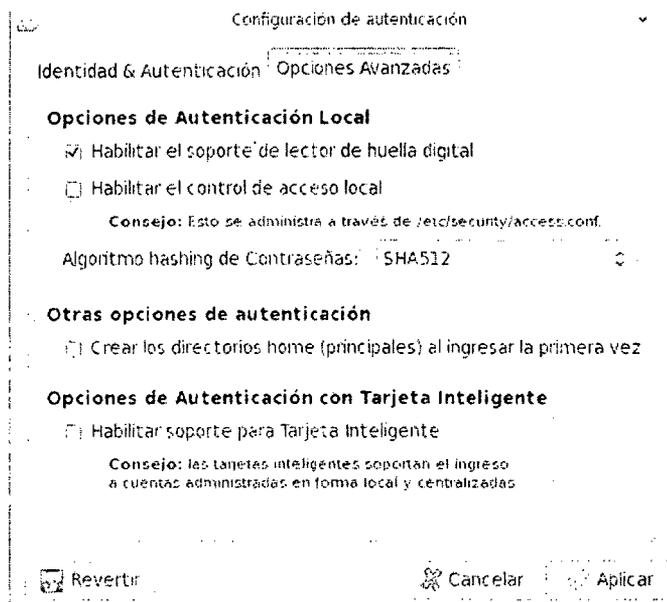
Los algoritmos de codificación de las claves son "de sentido único", o sea que impiden la descodificación directa de las claves. Por lo tanto, cuando un usuario entra en el sistema, se le codifica la clave y se compara con la

clave válida encriptada. Si el resultado es correcto, el usuario puede conectarse.

Linux puede utilizar el algoritmo de codificación **Crypt**, usado en los antiguos sistemas Unix y llamado así por la función del lenguaje C que realiza los cálculos. Este método es inseguro porque usa claves de codificación débiles de 56 bits y las contraseñas sólo pueden tener un máximo de 8 caracteres.

Los nuevos Linux también soportan algoritmos de codificación más potentes como **MD5 o SHA**, mucho más robustos y que permiten claves más extensas y difíciles de averiguar. El algoritmo MD5 usa claves de 128 bits, mientras que SHA512 –por defecto en Fedora 13 y en Ubuntu 10.04– aumenta dicha longitud hasta los 512 bits.

La siguiente figura muestra la pestaña de opciones de la aplicación gráfica **system-config-authentication**, para gestión de autenticación en Fedora 13.



### 2.4.1. Restricciones para tener claves seguras.

El administrador debe recomendar a sus usuarios que creen claves que puedan resultar difíciles de averiguar para un pirata informático.

También debe hacer que el sistema cree dificultades al intruso, usando codificaciones complejas y creando restricciones que comprometan al usuario con la seguridad del sistema.

Todos los usuarios del sistema han de tener en cuenta las siguientes recomendaciones con sus claves:

- No usar palabras comunes o números asociados a la persona.

- No repetir las claves en distintas máquinas.
- Usar claves de 8 caracteres como mínimo, con al menos 2 caracteres no alfabéticos.
- No usar secuencias de teclado.
- Cambiar la clave periódicamente y no repetir claves anteriores.
- No dejar ni anotar la clave.
- Evitar que otra persona vea teclear la clave.

## 2.5. Permisos.

Uno de los elementos principales de la seguridad en Unix es el buen uso de los permisos para acceder a ficheros y directorios. Todo usuario -no sólo el administrador- debe tener claros los conceptos más básicos para evitar que otro usuario lea, modifique o incluso borre datos de interés <sup>[4]</sup>.

El usuario administrador -al tener el control completo del sistema- también puede realizar operaciones sobre los ficheros y directorios de cualquier usuario (técnica que puede ser utilizada para evitar que un usuario pueda acceder a su propio directorio personal).

Este hecho hace imprescindible que los responsables de la máquina tengan especial cuidado cuando utilicen la cuenta del usuario **root**.

Los permisos de acceso se dividen principalmente en dos categorías:

- permisos normales,
- permisos especiales.

Por otro lado, los permisos también se subdividen en tres grupos:

- permisos para el propietario,
- permisos para su grupo de usuarios,
- permisos para el resto de usuarios del sistema,

Las **listas de control de acceso (ACL)** permiten asignar permisos de forma específica a conjuntos de usuarios y grupos.

### 2.5.1. Permisos normales.

Cada usuario tiene un nombre de conexión único en el ordenador y pertenecerá a uno o varios grupos de usuarios. El propietario de un fichero o directorio puede seleccionar qué permisos desea activar y cuales deshabilitar.

Para comprobarlo de manera más clara, tómesese el primer grupo de valores obtenidos con el mandato `ls -l`, que permitirá observar los permisos. Estos 11 caracteres indican:

- 1 carácter mostrando el tipo: fichero (-), directorio (d), enlace (l), tubería (p), enlace simbólico (L), etc.
- 3 caracteres para los permisos del propietario.
- 3 caracteres para los permisos de otros usuarios del grupo.
- 3 caracteres para los permisos del resto de usuario.
- 1 carácter opcional que indica si hay definida una ACL.

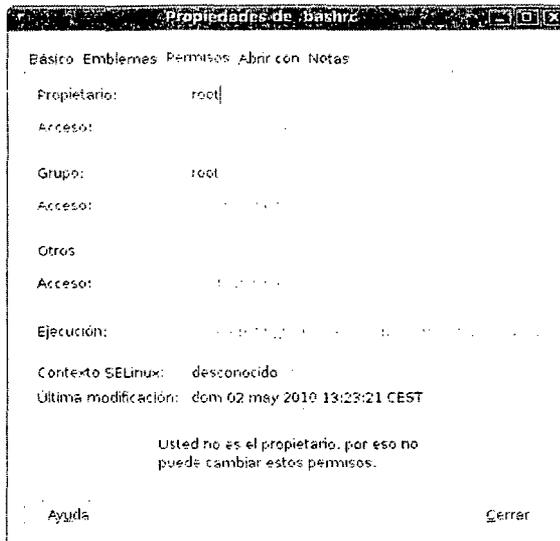
Según el tipo de entrada del directorio, los caracteres de permisos normales pueden variar de significado:

<b>Ficheros:</b>	<b>Lectura (r):</b> el usuario puede leer el fichero. <b>Escritura (w):</b> el usuario puede escribir en el fichero. <b>Ejecución (x):</b> el usuario puede ejecutar el fichero (siempre que sea un ejecutable o un guión de intérprete de mandatos).
<b>Directorios:</b>	<b>Lectura (r):</b> el usuario puede leer el contenido del directorio. <b>Escritura (w):</b> el usuario puede crear, modificar y borrar entradas del directorio. <b>Acceso (x):</b> el usuario puede acceder al directorio y puede usarlo como directorio actual (ejecutando la orden <code>cd</code> ). Este permiso posibilita proteger cierta información de un directorio padre y, sin embargo, acceder a la información de los directorios hijos.

El ejemplo siguiente muestra la ejecución de una orden `ls` para ver el contenido y los permisos del directorio `/etc/skel` definido por defecto en Ubuntu 10.04 Lucid.

```
$ ls -al /etc/skel
total 32
drwxr-xr-x 2 root root 4096 2010-05-02 20:26 .
drwxr-xr-x 186 root root 12288 2010-05-30 13:49 ..
-rw-r--r-- 1 root root 220 2008-05-12 20:49 .bash_logout
-rw-r--r-- 1 root root 3103 2010-04-19 04:15 .bashrc
-rw-r--r-- 1 root root 179 2010-03-26 13:31 examples.desktop
-rw-r--r-- 1 root root 675 2008-05-12 20:49 .profile
```

Asimismo, el ejemplo muestra la pestaña “Permisos” del cuadro de propiedades del navegador de archivos propio del entorno GNOME 2.30 bajo Ubuntu 10.04, mostrando los datos del fichero `.bashrc` del directorio anterior.



La siguiente tabla muestra los permisos necesarios para poder ejecutar algunos mandatos <sup>[4]</sup>.

<b>Mandato</b>	<b>Permisos directorio origen</b>	<b>Permisos fichero</b>	<b>Permisos directorio destino</b>
cd	X	No aplicable	No aplicable
ls	R	No aplicable	No aplicable
mkdir	W, X	No aplicable	No aplicable
rmdir	W, X	No aplicable	No aplicable
cat	X	R	No aplicable
rm	W, X	-	No aplicable
cp	X	R	W, X
mv	W, X	-	W, X

### 2.5.2. Permisos especiales.

Los permisos especiales complementan al conjunto de permisos normales, potencian la seguridad del sistema y se utilizan para soportar ciertas operaciones específicas.

Al igual que en el punto anterior, dependiendo del tipo de entrada del directorio, los caracteres de permisos especiales representados por `ls -l` son <sup>[4]</sup>:

<b>Ficheros:</b>	<p><b>Identificador de usuario activo (s para el propietario):</b> un programa ejecutable puede activar el identificador de usuario (<b>SUID</b>), lo cual permite que durante la ejecución del programa un usuario se convierta en el usuario propietario del fichero. Por ejemplo, el mandato <code>passwd</code> accede a ficheros que sólo puede modificar el usuario <code>root</code>. Dicho mandato tiene activo el SUID para que durante la ejecución del programa otro usuario sea por algún momento <code>root</code> y pueda cambiar su clave. Hay que tener especial cuidado con estos ejecutables, porque usuarios no autorizados pueden tomar privilegios.</p> <p><b>Identificador de grupo activo (s para el grupo):</b> al igual que en el caso anterior, un programa ejecutable puede activar el identificador de grupo (<b>SGID</b>) para que un usuario pueda realizar operaciones propias del grupo al que pertenece el fichero. Por ejemplo, el mandato <code>mail</code> activa el SGID para que cualquier usuario pueda acceder a su buzón de correo sin posibilidad de leer correo de cualquier otro usuario.</p>
<b>Directorios:</b>	<p><b>Directorio de intercambio (t en el resto de usuarios):</b> permite que en directorios compartidos los ficheros sólo puedan ser modificados por el propietario (suele usarse en directorios para ficheros temporales como <code>/tmp</code>).</p> <p><b>Identificador de grupo activo (s para el grupo):</b> los ficheros que se creen en dicho directorio tendrán el mismo grupo que el del propio directorio, en vez del grupo del propietario.</p>

El administrador debe catalogar todos los ficheros y directorios creados tras la instalación del sistema operativo o de cualquier aplicación, y que contengan permisos especiales. Periódicamente debe comprobar el estado de dichos archivos y verificar que no han sido modificados.

### 2.5.3. Notaciones simbólica y octal.

La orden `chmod` se utiliza para modificar los permisos de acceso descritos anteriormente y soporta dos tipos de notaciones: simbólica y numérica en formato octal.

La siguiente tabla muestra la forma de asignar permisos en ambas notaciones.

<b>Permisos normales</b>		<b>Valor octal</b>	<b>Notación simbólica</b>
Propietario:	Lectura	400	u+r
	Escritura	200	u+w
	Ejecución / Acceso	100	u+x
Grupo:	Lectura	40	g+r
	Escritura	20	g+w
	Ejecución / Acceso	10	g+x
Resto de usuarios:	Lectura	4	o+r
	Escritura	2	o+w
	Ejecución / Acceso	1	o+x
<b>Permisos especiales</b>		<b>Valor octal</b>	<b>Notación simbólica</b>
Propietario:	Usuario activo (SUID)	4000	u+s
Grupo:	Grupo activo (SGID)	2000	g+s
Resto de usuarios:	Directorio de intercambio	1000	+t

La notación simbólica se utiliza para añadir (+), quitar (-) o asignar (=) permisos agrupados según su tipo.

La notación numérica en formato octal sirve para asignar todos los permisos a la vez, aplicando una operación lógica O para obtener el resultado.

Véase un ejemplo. Si el usuario tiene permiso de modificación en el directorio y si es propietario de los archivos, se ejecutarán las siguientes modificaciones:

- A fichero1 se le asignan los permisos de lectura y escritura para el propietario y el grupo asociado, y se le quitan (si existen) los de escritura y ejecución para otros usuarios.
- A fichero2 se le asignan directamente los permisos de lectura y escritura para el propietario y de lectura para su grupo. El resto de usuarios no tiene ningún permiso.

```
$ chmod ug=rw,o-wx fichero1
$ chmod 640 fichero2
```

## 2.5.4. Listas de Control de Acceso (ACL)

La distribución básica de permisos de Linux es bastante rígida, sin embargo, las **Listas de Control de Acceso (ACL)** se implementan como una extensión al sistema de archivos para definir distintos conjuntos de permisos para usuarios y grupos de forma individualizada.

Una ACL consta de una lista de entradas en la que se especifica la asignación de los 3 permisos básicos de Unix: lectura (r), escritura (w) o ejecución/acceso (x), en este orden; la ausencia de un determinado permiso se denota por un guión (-). El siguiente cuadro muestra el formato genérico de una ACL.

```
[Tipo]:[Calificador]:ListaPermisos[,...]
```

La existencia de una ACL definida sobre un fichero se denota cuando el carácter número 11 de la salida de permisos de la orden `ls -l` es un signo más (+). La siguiente tabla describe las órdenes principales para gestión de ACL.

Mandato	Descripción
<code>getfacl</code>	Devuelve la lista de control de acceso a un fichero o directorio.
<code>setfacl</code>	Asigna, modifica o elimina una lista de control de acceso.

En el siguiente ejemplo, el propietario del fichero asigna permiso de lectura y escritura a un usuario determinado que no pertenece a su grupo.

```
$ ls -l fich1.txt
-rw-r----- 1 usu1 grup01 11776 2010-01-27 19:20 fich1.txt
$ group usu2
usu2 : grupo2
$ setfacl -m user:usu2:rw fich1.txt
$ ls -l fich1.txt
-rw-r-----+ 1 usu1 grup01 11776 2010-01-27 19:20 fich1.txt
$ getfacl fich1.txt
file: fich1.txt
owner: usu1
group: grup01
user::rw-
user:usu2:rw-
group::r--
other::r--
```

En este otro ejemplo se utiliza una orden compuesta para copiar la ACL de un fichero a otro.

```
getfacl fich1 | setfacl --set-file=- fich2
```

## **2.6. Configuración del entorno.**

El intérprete de mandados de cada cuenta de usuario tiene un entorno de operación propio, en el que se incluyen una serie de variables de configuración.

El administrador del sistema asignará unas variables para el entorno de ejecución comunes a cada grupo de usuarios, o a todos ellos; mientras que cada usuario puede personalizar algunas de estas características en su perfil de entrada, añadiendo o modificando aquellas variables que el gestor no haya definido como de sólo lectura.

Para crear el entorno global, el administrador crea un perfil de entrada común para todos los usuarios (archivo `/etc/bashrc` en el caso de BASH), donde -entre otros cometidos- se definen las variables del sistema y se ejecutan los ficheros de configuración propios para cada aplicación.

Estos pequeños programas se sitúan en el subdirectorio `/etc/profile.d`; debiendo existir ficheros propios de los intérpretes de mandatos basados en el de Bourne (BSH, BASH, PDKSH, etc.), con extensión `.sh`, y otros para los basados en el intérprete C (CSH, TCSH, etc.), con extensión `.csh`.

El proceso de conexión del usuario se completa con la ejecución del perfil de entrada personal del usuario (archivo `~/.bash_profile` para BASH). Aunque el administrador debe suministrar un perfil válido, el usuario puede retocarlo a su conveniencia.

El lector puede dirigirse a la documentación de los cursos de formación sobre Programación Avanzada en Shell para obtener más información sobre las variables de entorno más importantes <sup>[3]</sup>.

## **2.7. Gestión de cuentas.**

Los sistemas Linux modernos (y los entornos de escritorio) ofrecen herramientas gráficas de gestión para realizar las tareas comunes de administración del sistema, incluyendo su propio conjunto de aplicaciones para la gestión usuarios y grupos.

Con este tipo de programas se pueden ejecutar las operaciones más sencillas de revisión y control, pero resultan bastante pobres para realizar una administración automatizada y avanzada de las cuentas de los usuarios.

El sistema operativo ofrece también una serie de mandatos de gestión, que deben ser usados para personalizar y automatizar el proceso de

creación, revisión y eliminación de usuarios y grupos. La siguiente tabla describe dichas funciones.

<b>Mandato</b>	<b>Descripción</b>
<b>useradd</b>	Crea una nueva cuenta de usuario.
<b>usermod</b>	Modifica los parámetros de una cuenta.
<b>userdel</b>	Borra una cuenta de usuario.
<b>passwd</b>	Modifica la clave de acceso a una cuenta.
<b>chpasswd</b>	Cambia la clave a varios usuarios usando un fichero de entrada de datos.
<b>chage</b>	Cambia las restricciones temporales de una cuenta.
<b>chfn</b>	Cambia la descripción del usuario.
<b>chsh</b>	Cambia el intérprete de mandatos de la cuenta.
<b>groupadd</b>	Crea un nuevo grupo de usuarios.
<b>groupmod</b>	Modifica los parámetros de un grupo de usuarios.
<b>groupdel</b>	Elimina un grupo de usuarios.
<b>gpasswd</b>	Cambia la clave de acceso a un grupo privado.

### **2.7.1. Planificación.**

La gestión de las cuentas de los usuarios es uno de los aspectos más importantes dentro de las tareas administrativas, por ello deben planificarse detalladamente las características y las necesidades de los usuarios y de los grupos que vayan a darse de alta en el sistema.

Fundamentalmente, deben realizarse las siguientes operaciones previas antes de crear cualquier cuenta:

- Crear los distintos grupos de usuarios, uno para cada conjunto de tareas que vayan a ejecutar los usuarios, o uno por cada rol administrativo.
- Definir los parámetros globales del sistema, tales como: restricciones para la creación de claves, método principal de acceso, posibilidad de almacenamiento remoto de las cuentas, etc.
- Crear la estructura de directorios básica para las cuentas, separando los subdirectorios de cada grupo principal. Asignando los permisos

adecuados, puede evitarse que usuarios con menor privilegio accedan a zonas reservadas de otros grupos.

- Definir listas privadas donde el administrador pueda comprobar la identidad de cada usuario, almacenando los datos básicos de cada persona y de su cuenta asociada.
- Crear los programas para la gestión de las cuentas, generando ficheros de configuración que automaticen los procesos de creación, modificación, revisión, caducidad y borrado de usuarios.

### 2.7.2. Ejemplo: servidor de prácticas universitarias.

Para ilustrar el proceso de gestión de cuentas, la siguiente tabla describe en resumen una estructura que puede usarse en un servidor de prácticas universitarias, relativamente parecida a la existente en el Centro de Cálculo de la E.T.S. de Ingeniería Informática de la Universidad de Sevilla.

<b>Restricciones generales para claves:</b>	Las definidas anteriormente en este capítulo.
<b>Creación de grupos de usuarios:</b>	<p>Crear grupos para administradores, alumnos normales, alumnos de proyectos fin de carrera y profesores.</p> <p>Un grupo para cada departamento.</p> <p>Definir grupos para alumnos por curso.</p>
<b>Estructura de directorios:</b>	<p>Directorio privado para el grupo de administradores.</p> <p>Directorio privado para profesores con subdirectorios privados para cada departamento.</p> <p>Directorios para alumnos normales agrupados por cursos y para alumnos de proyectos.</p> <p>Directorio para apuntes, con permisos de escritura para profesores y de lectura para alumnos.</p>
<b>Crear listas de usuarios:</b>	Generar una lista distinta para cada grupo de usuarios..
<b>Programas de gestión:</b>	<p>Creación de perfiles de configuración para los programas, donde se almacena información por defecto para cada tipo de usuarios y para la generación de los menús de selección.</p> <p>Creación interactiva de cuentas usando dichos perfiles.</p> <p>Creación automática de varias cuentas usando un fichero de datos de entrada.</p>

Comprobación de datos de usuarios; mostrando el contenido de la lista correspondiente, la entrada del fichero `/etc/passwd`, el directorio de la cuenta, la fecha de caducidad y la cuota de disco.

Comprobación de concordancia entre los datos de las listas de usuarios y las cuentas creadas.

Registro de cuotas de disco y comprobación semanal de su estado.

Comprobación de la caducidad de las cuentas.

Renovación automática de cuentas.

Eliminación automática de cuentas caducadas.

Borrado interactivo de cuentas y sus directorios.

Registro de incidencias sobre bloqueo y desbloqueo de cuentas.

Cambio automático de claves.

### 3. Sistemas de archivos.

La gestión adecuada del acceso a disco es otro de los aspectos importantes en el proceso de administración de sistemas operativos multiusuario y multitarea y es imprescindible mantener una estructura básica con un cierto nivel organizativo. El sistema operativo interactúa con los usuarios y las aplicaciones, y se hace necesario un modelo de seguridad dependiente de la forma en que se almacenan los ficheros en los dispositivos.

Un sistema de archivos puede verse desde dos categorías lógicas de ficheros <sup>[7]</sup>:

- Archivos locales no compartibles o compartibles con otras máquinas.
- Archivos estáticos o variables.

Por lo tanto, un **sistema de archivos** es un subárbol de directorios con un directorio raíz -que debe tener unos permisos acordes con las necesidades de acceso a sus archivos-, una estructura lógica de almacenamiento y un punto de montaje adecuado en el árbol de directorios global del servidor.

#### 3.1. Normas para la Jerarquía de Sistemas de Archivos (FHS).

Las **Normas para la Jerarquía de Sistemas de Archivos (FHS)** <sup>[v]</sup> describen un conjunto de reglas que permiten, tanto a los usuarios como a los programas, predecir la localización de los ficheros y directorios instalados en el sistema.

La siguiente tabla describe brevemente los subdirectorios de la jerarquía principal, ordenados alfabéticamente <sup>[7]</sup>.

Directorio	Descripción
/bin	Binarios básicos para todos los usuarios del sistema.
/boot	Ficheros estáticos del cargador de arranque.
/dev	Sus entradas representan los dispositivos del sistema (conviene recordar que "en Unix todo es un archivo").
/etc	Configuración local del sistema.

<b>/home</b>	Cuentas de usuarios (si se define, debe ser un sistema de archivos independiente).
<b>/lib</b>	Bibliotecas compartidas del sistema y módulos fundamentales del núcleo.
<b>/lib32</b> <b>/lib64</b>	Bibliotecas específicas para arquitecturas de 32 o 64 bits.
<b>/media</b>	Puntos de montaje para dispositivos extraíbles (disquete, CDs/DVDs, conexiones USB, etc.).
<b>/mnt</b>	Puntos de montaje para sistemas de archivos temporales.
<b>/opt</b>	Área compartida para paquetes de grandes aplicaciones (puede ser un sistema de archivos independiente con una jerarquía propia).
<b>/proc</b>	Sistema de archivos virtual con información sobre procesos y el núcleo.
<b>/root</b>	Cuenta del usuario administrador <code>root</code> (opcional).
<b>/sbin</b>	Binarios del sistema.
<b>/srv</b>	Datos de los servicios suministrados por el sistema.
<b>/usr</b>	Jerarquía secundaria similar a la principal, con información que puede ser compartida por otros ordenadores con acceso de sólo lectura (debe ser un sistema de archivos independiente en servidores).
<b>/usr/local</b>	Jerarquía para programas locales (debe ser un sistema de archivos independiente).
<b>/tmp</b>	Zona compartida para ficheros temporales.
<b>/var</b>	Información variable, incluyendo ficheros históricos, de estado, de bloqueos, de recuperación, de colas de trabajos, etc.

### **3.2. Discos y particiones.**

Todos los sistemas Unix -y, por lo tanto, todos los "dialectos" Linux- utilizan ficheros de dispositivos para acceder a los recursos de la máquina, almacenados en el directorio `/dev`. Sin embargo, cada dialecto Unix tiene una notación diferente para identificar cada dispositivo de almacenamiento.

Tanto Fedora 13 como Ubuntu 10.04 Lucid identifican los ficheros controladores de particiones para discos sencillos con el siguiente formato:

- Tipo de dispositivo (sd para discos normales).
- Unidad (a para el dispositivo 1, b para el 2, etc.).
- Número de partición.

En caso de usar discos redundantes por *hardware*, el fichero del dispositivo se encuentra en un subdirectorio con el nombre del controlador RAID (por ejemplo, cciss para HP Smart Array) y su nombre tiene el siguiente formato:

- cN (nº de controlador, empezando por 0).
- dN (nº de disco, empezando por 0).
- pN (nº de partición, empezando por 1)..

Una **partición** es cada una de las subdivisiones que el gestor del sistema define en una unidad de disco del sistema, donde se almacena un determinado sistema de archivos o un espacio de paginación.

Siguiendo las normas descritas en el apartado anterior, el administrador debe definir los distintos sistemas de archivos de su sistema, creando particiones en cada disco, teniendo en cuenta los recursos disponibles y la utilización principal que los usuarios harán de ellos.

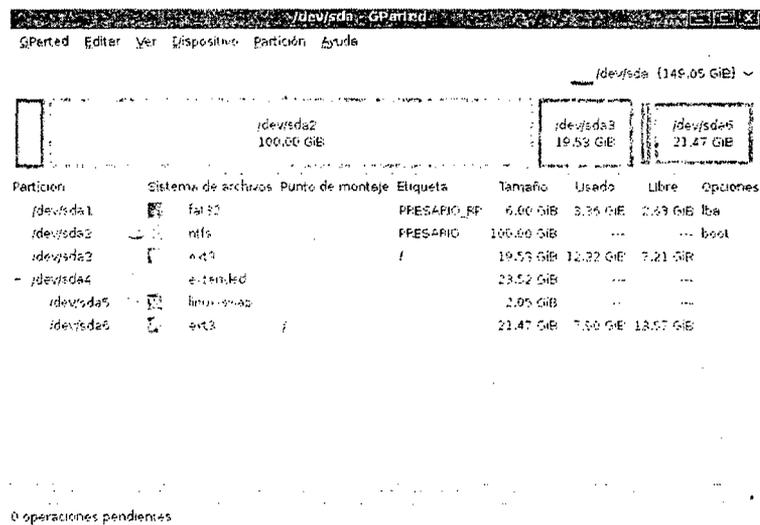
El proceso de crear los sistemas de archivos básicos suele realizarse durante la instalación de la máquina, aunque pueden añadirse y ampliarse posteriormente. La siguiente tabla define una distribución típica e indica algunas recomendaciones.

Sistema de archivos	Recomendaciones
/	Es necesario para trabajar, no tiene por qué ser de gran tamaño.
/proc	Es necesario para trabajar y debe ocupar entre la mitad y el doble de la memoria física, inversamente al tamaño de ésta.
/usr	Contiene el sistema operativo, su tamaño depende de los paquetes que deban instalarse y de las previsiones de ampliación.
/tmp	Espacio para ficheros temporales, depende del número de usuarios que se definirán y del espacio estimado para sus trabajos.
/var	Contará con ficheros que crecen, debe preverse un tamaño suficiente, pero sin desperdiciar el espacio de disco.
/boot	Puede usarse para almacenar el gestor de arranque; se usa cuando es necesario cargar algún controlador para localizar el sistema de archivos raíz.

/home	Cuentas de usuarios; puede ser recomendable usar un disco independiente, cuyo tamaño dependerá del número de usuarios y de la capacidad estimada de sus cuentas.
/usr/local	Debe tener un tamaño suficientemente grande para almacenar las utilidades y aplicaciones instaladas; es recomendable usar un disco independiente.

Aunque las distribuciones Linux suelen incluir herramientas gráficas que ayudan a gestionar el espacio de almacenamiento, tanto durante el periodo de instalación como de ejecución normal, pueden incluirse ciertas aplicaciones que tienen una apariencia independiente.

El siguiente gráfico describe la utilidad de creación de sistemas **GParted**, instalada en un sistema con 2 discos SATA. Se muestra el particionado del primer disco, con sistemas de archivos de Windwos (1 FAT y 1 NTFS) y de Linux (2 Ext3 y 1 de paginación).



### 3.3. Sistemas de archivos Ext3 y Ext4.

Linux soporta el montaje de distintos sistemas de archivos, tanto locales como remotos, ya que se ha programado una interfaz entre ellos y el núcleo, conocida como **Sistema de Archivos Virtual (VFS)**.

El sistema de archivos más utilizado hasta hace algunos años en Linux era el conocido como **Sistema de Archivos Extendido 2 (Ext2)**, que aumentaba las prestaciones de la primera versión, pero que seguía presentando problemas ante una caída inesperada del sistema, ya que necesitaba un largo proceso de comprobación y corrección.

Las modernas distribuciones Linux usan el **Sistema de Archivos Extendido 3 (Ext3)**, el cual incluye las siguientes mejoras:

- El diario de registros es la característica más importante, que mejora los procesos de revisión de integridad, ya que sólo se requiere la comprobación de dicho diario.
- Soporta mayores niveles de integridad de datos para evitar la corrupción del sistema de archivos, permitiendo elegir el tipo y el nivel de protección.
- Mayor flujo y mayor velocidad de accesos repetidos a datos.
- Fácil transición entre ext2 y ext3, sin necesidad de volver a formatear las particiones.

El núcleo de Linux incluye soporte para el **Sistema de Archivos Extendido 4 (Ext4)** a partir de la versión 2.6.30; por lo tanto, Ext4 está incorporado por defecto en las instalaciones nuevas de Fedora 13 y de Ubuntu 10.04 Lucid.

El sistema de archivos Ext4 incluye las siguientes mejoras con respecto a Ext3<sup>[ix]</sup>:

- Mayor tamaño del sistema de archivos (hasta 1 EB = 2<sup>20</sup> TB).
- Sin restricciones en el número de subdirectorios.
- Mayor velocidad de tratamiento de ficheros grandes mediante "extents".
- Asignación previa de disco o asignación retardada.
- Comprobación del registro del sistema de archivos.
- Desfragmentación en directo sin necesidad de desmontar el sistema de archivos.
- Recuperación de ficheros borrados.
- Comprobaciones más rápidas del estado del sistema de archivos.
- Las marcas de tiempo cuentan con precisión de nanosegundos.
- Actualizable desde Ext3 (puede volverse a Ext3 perdiendo los "extents").

La configuración permanente de los sistemas de archivos montados en un servidor se define en el fichero `/etc/fstab`, incluyendo datos sobre el dispositivo origen, el punto de montaje, el tipo del sistema de archivos, así como el conjunto de opciones de montaje, depuración y comprobación de la consistencia de los datos.

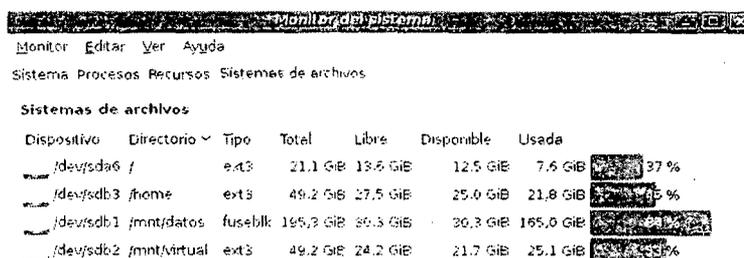
Las siguiente tabla describe el formato general del fichero de configuración `/etc/fstab`.

Formato	Descripción
<b>/etc/fstab</b>	
<i>Etiq Montaje Tipo Opciones Volc NOrden</i> ...	Fichero de descripción de sistemas de archivos. Sus campos son: <ol style="list-style-type: none"> <li>1. Etiqueta o UUID de la partición, dispositivo o directorio remoto.</li> <li>2. Punto de montaje local.</li> <li>3. Tipo de sistema de archivos (ext3, ext4, swap, vfat, ntfs, nfs, cifs, etc.).</li> <li>4. Opciones de montaje (dependen del tipo de sistema de archivos).</li> <li>5. Control de volcado automático de seguridad ante caídas del sistema.</li> <li>6. Orden de comprobación de consistencia de datos durante el arranque del servidor (1 para /, incrementar en sistemas de archivos de distintos discos).</li> </ol>

Asimismo, a continuación se describen brevemente los mandatos más habituales en la gestión de sistemas de archivos.

Mandato	Descripción
<b>fdisk</b> <b>sfdisk</b>	Manipulación de la tabla de particiones de un disco.
<b>parted</b>	Gestión de particiones y sistemas de archivos.
<b>mkfs</b>	Formatea una nueva partición.
<b>mount</b>	Monta un sistema de archivos en el árbol global de directorios.
<b>umount</b>	Desmonta un sistema de archivos.
<b>tune2fs</b>	Convertor entre sistemas de archivos <b>ext2</b> , <b>ext3</b> y <b>ext4</b> .

El siguiente gráfico muestra un ejemplo de la ejecución de la pestaña “Sistemas de archivos” de la aplicación **gnome-system-monitor**, incluida en GNOME 2.30 bajo Ubuntu 10.04.



Dispositivo	Directorio	Tipo	Total	Libre	Disponible	Usada	
/dev/sda6	/	ext3	21.1 GIB	13.6 GIB	12.5 GIB	7.6 GIB	37 %
/dev/sdb3	/home	ext3	49.2 GIB	27.5 GIB	25.0 GIB	21.8 GIB	45 %
/dev/sdb1	/mnt/datos	fuseblk	155.3 GIB	29.3 GIB	26.3 GIB	155.0 GIB	100 %
/dev/sdb2	/mnt/virtual	ext3	49.2 GIB	24.2 GIB	21.7 GIB	25.1 GIB	51 %

## 3.4. Paginación y procesos.

### 3.4.1. Espacios de paginación.

Un sistema operativo multiusuario y multitarea como Linux necesita una gran cantidad de memoria física para poder ejecutar todos los procesos. Los **espacios de paginación** son particiones de disco que permiten ampliar virtualmente la memoria del sistema, guardando el estado de los procesos que en un determinado momento están a la espera de ser ejecutados, si la memoria física está agotada.

Los factores principales que deben determinar el tamaño del espacio total de paginación son:

- La cantidad de memoria y de disco del sistema.
- El número de usuarios que tendrán acceso a la máquina.
- El número previsto de procesos/usuario.
- El número de servicios activos en el sistema.
- El número estimado de clientes/servicio.

Debido al crecimiento de la memoria en los nuevos servidores, la regla general es utilizar para paginación entre la mitad y el doble de la memoria física instalada. Ante casos de necesidad, el administrador puede ampliar la cantidad de paginación usando ficheros de disco que pueden ser posteriormente eliminados.

La siguiente tabla describe las órdenes Linux usadas para manipular los espacios de paginación.

Mandato	Descripción
<b>fdisk</b>	Gestor de discos usado para definir particiones.
<b>mkswap</b>	Crea particiones o ficheros de paginación.
<b>swapon</b>	Activa una partición o un fichero de paginación.
<b>swapoff</b>	Desactiva una partición o un fichero de paginación.

### 3.4.2. Sistemas de archivos virtuales /proc y /sys.

Los sistemas de archivos virtuales montados en /proc y en /sys están almacenados en memoria y contienen una jerarquía de ficheros y directorios especiales que mantienen el estado actual del núcleo del sistema Linux, recopilando información sobre los dispositivos y los procesos en ejecución.

El siguiente cuadro muestra el formato típico de la definición de ambos sistemas de archivos en el fichero /etc/fstab.

<b>sysfs</b>	<b>/sys</b>	<b>sysfs</b>	<b>defaults</b>	<b>0 0</b>
<b>proc</b>	<b>/proc</b>	<b>proc</b>	<b>defaults</b>	<b>0 0</b>

La mayoría de los ficheros virtuales de /proc aparecen con longitud 0, aunque pueden ser revisados como si fueran archivos de texto, algunos de ellos con gran cantidad de información <sup>[2]</sup>.

En /proc hay una serie de directorios especiales que describen el estado actual de cada proceso en ejecución -denotados por el identificador del proceso (PID)-, incluyendo datos como: la línea de la orden ejecutada, los directorio raíz y de trabajo del proceso, estados de la memoria, de ejecución y de uso de los procesadores, las variables de entorno, etc.

Otros ficheros y directorios de interés son los que informan sobre procesadores, memoria, interrupciones, dispositivos, particiones, puntos de montaje, módulos del núcleo, parámetros de red, etc.

El directorio especial /proc/sys contiene ficheros que sólo pueden ser modificados por el administrador para realizar cambios de configuración en el núcleo, habilitando o desactivando ciertas características operativas.

Debe tenerse gran precaución en la modificación de los archivos virtuales de /proc/sys.
-----------------------------------------------------------------------------------------

La siguiente tabla describe el contenido de dicho directorio /proc/sys.

Directorio	Descripción
/proc/sys/dev	Información sobre dispositivos especiales (CD-ROM, discos RAID, etc.).
/proc/sys/fs	Parámetros de sistemas de archivos (límites de ficheros e i-nodos abiertos, cuotas, etc.).
/proc/sys/kernel	Configuración del núcleo (contabilidad de procesos, nombre del sistema, parada por consola, módulos, colas de mensajes, etc.).
/proc/sys/net	Parámetros de conexión para cada tipo de red (IPv4, IPv6, Token Ring, local (loopback), etc.).
/proc/sys/vm	Configuración de la memoria virtual (páginas usadas, tamaño mínimo que la memoria debe quedar libre, etc.).

La información completa sobre el sistema de archivos virtual `/proc` puede encontrarse en el paquete del código fuente del núcleo, que suele encontrarse en el subdirectorio `/usr/src/VersiónNúcleo/Documentation`.

Por su parte, el núcleo de Linux utiliza el sistema de archivos `/sys` para informar a las aplicaciones de usuario respecto de los objetos gestionados por el Kernel y las relaciones de dependencia entre ellos.

La estructura principal de `/sys` agrupa información sobre las clases de dispositivos registrados, los buses físicos, los dispositivos conectados, los controladores y los módulos del núcleo.

### 3.5. Discos redundantes (RAID).

La **Matriz Redundante de Discos Independientes (RAID)** representa un conjunto de técnicas válidas para ahorrar costes o mejorar las prestaciones y la seguridad del acceso al almacenamiento masivo, combinando múltiples discos en un único dispositivo lógico <sup>[21]</sup>.

El concepto principal de RAID es dividir los datos en ciertos trozos y distribuirlos en los dispositivos de la matriz, según el nivel de necesidad. Durante el proceso de lectura se sigue un algoritmo inverso de reconstrucción.

Las principales características del uso de discos en RAID son:

- Aumentar la velocidad de acceso a los datos.
- Incrementar la capacidad de almacenamiento, combinando discos de menor capacidad en un único disco lógico mayor.

- Mejorar la tolerancia a fallos de los discos.

Existen dispositivos y controladores preparados para realizar técnicas RAID en su propio *hardware*, lo que aumenta las prestaciones y el precio final de la máquina. Los nuevos sistemas operativos son aptos para realizar este cometido bajo *software*.

La siguiente tabla describe los niveles RAID más usados.

<b>RAID 0:</b>	<p>Los datos se dividen en bandas, escribiendo cada una de ellas en un disco.</p> <p>Se mejora las prestaciones de acceso.</p> <p>La capacidad total es la suma de las capacidades de cada disco.</p>
<b>RAID 1:</b>	<p>Los datos se almacenan en espejo, repitiendo la misma escritura en cada disco.</p> <p>Se incrementa la seguridad y la tolerancia a fallos del sistema, porque puede sustituirse un disco defectuoso sin afectar al funcionamiento de la máquina.</p> <p>La capacidad total corresponde a la de cualquier disco (todos deben ser iguales).</p>
<b>RAID 5:</b>	<p>Se usan más de 2 discos para distribuir los trozos de datos y sus paridades. Cada disco contiene una banda de datos y la paridad de las bandas de otros datos.</p> <p>Se incrementan la seguridad, las prestaciones y los costes.</p> <p>La capacidad total es, aproximadamente, la suma total de la capacidad de los discos menos 1.</p>
<b>RAID 6:</b>	<p>Es un RAID 5 con 2 bandas de comprobación.</p> <p>Aumenta aún más la seguridad del sistema y sus costes.</p> <p>Se disminuye en algo la capacidad total con respecto al RAID 5.</p>
<b>RAID lineal:</b>	<p>Los discos se agrupan secuencialmente para formar un disco lógico mayor.</p> <p>No se incrementan ni las prestaciones ni la seguridad, sólo la capacidad.</p>

Si las particiones que vayan a utilizarse para el RAID por *software* van a montarse sobre sistemas de archivos esenciales para Linux, deben definirse durante el proceso de instalación del sistema operativo. Utilidades como **Disk Druid** (usada en Fedora y Red Hat Enterprise) permiten definir particiones RAID, asociarles el nivel de redundancia y generar el disco lógico (**metadispositivo**).

La definición de la matriz se encuentra en el fichero `/etc/raidtab`. El siguiente ejemplo muestra la configuración de un metadispositivo `md0` de tipo RAID 1 (espejo) formado por las particiones `sda1` y `sdb1` de 2 discos, que contienen un sistema de archivos de tipo Ext3 montado sobre el directorio raíz.

```

$ cat /etc/raidtab
raiddev /dev/md0
raid-level 1
nr-raid-disks 2
chunk-size 64k
persistent-superblock 1
nr-spare-disks 0
 device /dev/sda1
 raid-disk 0
 device /dev/sdb1
 raid-disk 1
$ df -h /dev/md0
S.ficheros Tamaño Usado Disp Uso% Montado en
/dev/md0 40G 21,5G 19,5G 51% /

```

### 3.6. Volúmenes lógicos.

Los volúmenes lógicos son técnicas de gestión de almacenamiento disponibles a partir de la versión 2.4 del núcleo de Linux –heredadas del sistema operativo AIX, el dialecto Unix de IBM– que permiten redimensionar las particiones y distribuir las en varios discos.

En algunas distribuciones de Linux puede existir la restricción impuesta por el **Gestor de Volúmenes Lógicos (LVM)** de que el directorio `/boot` deba encontrarse en una partición real y no formar parte de ningún volumen lógico.

Es obligatorio definir los volúmenes lógicos en el proceso de instalación cuando éstos vayan a almacenar sistemas de archivos propios del sistema.

El Gestor de Volúmenes Lógicos consta de 3 elementos fundamentales:

<b>Volumen físico:</b>	estructura que representa a un disco físico.
<b>Volumen lógico:</b>	estructura equivalente a un sistema de archivos Linux.
<b>Grupo de volúmenes:</b>	conjunto de varios volúmenes lógicos que pueden almacenarse en varios volúmenes físicos. Así, un disco puede contener varios sistemas de archivos y un sistema de archivos puede estar grabado en varios discos.

El instalador del sistema debe seguir los siguientes pasos:

- Si la distribución de Linux es antigua, crear una partición normal de tipo Ext3 para el directorio /boot, ya sea incluido en el directorio raíz o en una partición propia.
- Definir un volumen físico en cada disco.
- Crear los grupos de volúmenes conjuntando adecuadamente los volúmenes físicos.
- Definir los volúmenes lógicos de cada grupo de volúmenes, asignando para cada uno de ellos su tamaño inicial y su punto de montaje.

Es recomendable dejar algún espacio sin asignar para poder ampliar las particiones que lo necesiten.

El sistema incluye una gran variedad de mandatos para gestionar cada uno de los componentes del gestor de volúmenes lógicos. La siguiente tabla describe la mayoría de estas instrucciones según su función.

Operación	Volumen físico	Grupo de volúmenes	Volumen lógico
Crear	<code>pvcreate</code>	<code>vgcreate</code>	<code>lvcreate</code>
Eliminar	<code>pvremove</code>	<code>vgremove</code>	<code>lvremove</code>
Comprobar estado	<code>pvscan</code>	<code>vgscan</code>	<code>lvscan</code>
Cambiar tamaño	<code>pvresize</code>	<code>vgresize</code> <code>vgextend</code> <code>vgreduce</code>	<code>lvresize</code> <code>lvextend</code> <code>lvreduce</code>
Mostrar información	<code>pvs</code>	<code>vgs</code>	<code>lvs</code>
Mostrar atributos	<code>pvdisplay</code>	<code>vgdisplay</code>	<code>lvdisplay</code>

El siguiente cuadro muestra un ejemplo real usado para definir un grupo de volúmenes `vg0` con 2 discos que usan un controlador RAID por *hardware*, en donde se definirán 3 volúmenes lógicos; posteriormente, el administrador podrá usar cada uno de ellos para montar los sistemas de archivos del servidor.

```
pvcreate /dev/cciss/cld0 /dev/cciss/cld1
pvs
PV VG Fmt Attr PSize PFree
/dev/cciss/cld0 lvm2 -- 1,36T 1,36T
/dev/cciss/cld1 lvm2 -- 698,56G 698,56G
vgcreate vg0 /dev/cciss/cld0 /dev/cciss/cld1
vgs
VG #PV #LV #SN Attr VSize VFree
vg0 2 0 0 wz--n- 2,05T 2,05T
```

```

lvcreate -L 300G vg0
lvcreate -L 700G vg0
lvcreate -L 700G vg0
lvs
LV VG Attr LSize Origin Snap% Move Log Copy%
lvol0 vg0 -wi-a- 300,00G
lvol1 vg0 -wi-a- 700,00G
lvol2 vg0 -wi-a- 700,00G
vgs
VG #PV #LV #SN Attr VSize VFree
vg0 2 3 0 wz--n- 2,05T 395,69G

```

### 3.7. Sistemas de archivos remotos.

La conexión remota a otros ordenadores supone una gran ventaja en el proceso de compartir información. Los sistemas de archivos remotos permiten almacenar la información en un único nodo central y hacerla accesible a los distintos clientes, posibilitando la movilidad del usuario.

Para finalizar este capítulo van a describirse los sistemas de archivos remotos más utilizados actualmente.

#### 3.7.1. NFS.

El **Sistema de Archivos en Red (NFS)** fue creado por Sun Microsystems para SunOS –su dialecto Unix–, usando las técnicas de **Llamadas a Procedimientos Remotos (RPC)**. NFS permite acceder a los archivos en nodos remotos exactamente en la misma manera que si fueran locales, de un modo completamente transparente al cliente e independientemente de la arquitectura del servidor <sup>[6]</sup>.

IETF <sup>[xi]</sup> especifica en su RFC 3530 la versión 4 de NFS (**NFSv4**), redefiniendo completamente el protocolo e incluyendo mejoras como bloqueo de uso de ficheros, negociación de seguridad, ACLs, interoperabilidad entre plataformas, internacionalización, etc.

La siguiente tabla describe los servicios que deben activarse en los ordenadores servidor y cliente NFS.

Servicio	Descripción
portmap	Servicio de control principal de RPC.
rpc.mountd	Control de montaje del cliente NFS.
rpc.nfsd	Servidor NFS.

<code>rpc.statd</code>	Monitor del Estado de la Red (NSM), que notifica el reinicio del servidor NFS.
<code>rpc.rquotad</code>	Provee información de cuotas para usuarios remotos.

El fichero `/etc/exports` contiene la configuración NFS en el servidor. La siguiente tabla describe el formato de las líneas del fichero, una para cada directorio exportado.

Formato	Descripción
<b><code>/etc/exports</code></b>	
<code>Directorio Cliente(Opciones) ...</code> ...	Fichero principal que describe los directorios que pueden exportarse por NFS. Sus campos son: <ul style="list-style-type: none"> <li>a) Directorio local a exportar.</li> <li>b) Nombre o IP del cliente (soporta comodines en nombre y en dominios).</li> <li>c) Opciones de exportación: sólo lectura (<code>ro</code>), lectura/escritura (<code>rw</code>), evitar acceso privilegiado para el <code>root</code> del cliente (<code>root_squash</code>), acceso privilegiado para <code>root</code> (<code>no_root_squash</code>), etc.</li> </ul>

El cliente NFS puede configurar la importación de directorios en su fichero `/etc/fstab` o montarlo directamente con la orden `mount`.

```
mount -t nfs4 Servidor:Directorio PuntoMontaje [Opciones]
```

### 3.7.2. SMB/CIFS.

El **Sistema de Archivos Común para Internet (CIFS)** provee una serie de mecanismos abiertos e independientes de la plataforma utilizada, para que sistemas clientes soliciten servicios de ficheros a otras máquinas a través de la red. Este protocolo es una implementación del conocido como **Bloque de Mensajes del Servidor (SMB)**, usado principalmente por ordenadores con Windows <sup>[12]</sup>.

Microsoft ha redefinido nuevos dialectos del protocolo (SMB2 lanzado con Windows Vista y SMB2.1 con Windows 7), para mejorar el rendimiento y reducir la complejidad de las comunicaciones.

Las características principales de CIFS son:

- Acceso a ficheros, permitiendo compartir información en lectura y escritura.
- Acceso bloqueado y desbloqueado tanto a ficheros como a registros.
- Notificación de cambios en ficheros y directorios.
- Inclusión de atributos extendidos.
- Independencia del protocolo de resolución de nombres.

Las **Extensiones de CIFS para UNIX** son normas de reciente creación y sólo están implementadas en las versiones 2.6 de los servicios de ficheros del núcleo de Linux, mientras que los antiguos necesitan ser recompilados o generar un módulo propio para la gestión de clientes CIFS, aunque soportan el montaje de sistemas de archivos SMBFS.

El servidor de ficheros puede ser una máquina con sistema operativo Windows (a partir de NT) o con Linux y el servicio **Samba** activado. En ambos casos, deben ser configurados los recursos que van a ser exportados.

Cada distribución de Linux incluye una serie de paquetes con las herramientas básicas para el control de sistemas de archivos CIFS/SMB, los clientes para acceso a los recursos o el servidor de ficheros Samba.

Ubuntu 10.04 Lucid distribuye la rama 3.4 de Samba, que incorpora compatibilidad inicial con la futura versión de Samba 4; mientras que Fedora 13 viene con la reversión 3.5, la cual incluye soporte experimental para SMB2.

La próxima tabla muestra los mandatos usados por el cliente Samba.

<b>Mandato</b>	<b>Descripción</b>
<b>smbclient</b>	Cliente Samba con interfaz similar al cliente FTP.
<b>smbpasswd</b>	Permite cambiar la clave remota del usuario..
<b>smbcquotas</b>	Gestiona las cuotas en recursos NTFS.
<b>smbcacls</b>	Gestiona la lista de control de accesos (ACL) a los ficheros.
<b>smbpool</b>	Envía un fichero a una cola de impresión remota.
<b>net</b>	Herramienta de administración de Samba y de servidores remotos.
<b>pdbedit</b>	Herramienta de de gestión la base de datos de usuarios de Samba.
<b>findsmb</b>	Lista las máquinas que responden a una petición SMB en una subred.
<b>mount.cifs</b>	Montador de sistemas de archivos CIFS.
<b>umount</b>	Desmontador general de sistemas de archivos.

El montaje de un sistema de archivos CIFS requiere autenticación mediante usuario y clave. El método más seguro es indicar en la orden de montaje un archivo donde se incluyan las credenciales del usuario (usuario, contraseña y dominio opcional de autenticación), con el siguiente el formato:

```
Username = UsuarioRemoto
Password = Clave
Domain = Dominio
```

El formato para montar un sistema de archivos CIFS es el siguiente:

```
mount -t cifs //Servidor/Recurso PuntoMontaje \
-o credentials=FichCredenciales[,Opción=Valor,...]
```

## 4. Configuración de la red.

La red informática es el medio por el cual el servidor puede comunicarse con los usuarios y con otras máquinas, tanto servidores como clientes, permitiendo el intercambio masivo de información entre ordenadores.

De acuerdo con la planificación efectuada, la empresa debe contar con una infraestructura adecuada para el intercambio de datos. Asimismo, los dispositivos de los servidores deben cumplir las necesidades previstas, ofreciendo un ancho de banda y una capacidad de procesamiento adecuados.

Existe una gran variedad de tipos de redes y protocolos de comunicaciones, sin embargo, este capítulo se centra en redes Ethernet con protocolos TCP/IP, los más usados en la conexión a Internet y en redes privadas.

### 4.1. Interfaces de red.

El ordenador necesita un dispositivo -conocido como **tarjeta de red**- que le permita conectarse a cada una de las subredes que tenga directamente a su disposición.

El sistema operativo Linux puede trabajar con una gran variedad de tipos de máquinas y periféricos. Para normalizar el acceso a la red, el sistema dispone de una serie de funciones básicas. El conjunto de estas funciones usadas en una arquitectura de comunicaciones determinada, se conoce como **interfaz de red**.

Por último, la interfaz de red dialoga con el dispositivo físico mediante un módulo específico del núcleo denominado **controlador de red**.

Las modernas versiones de Linux detectan automáticamente las tarjetas de red, cargan los módulos adecuados del núcleo y asignan los interfaces de red por defecto. El administrador puede establecer los parámetros de conexión durante el proceso de instalación del sistema.

Linux establece una nomenclatura para cada tipo de interfaz de red, añadiendo un número de orden para cada conector del mismo tipo (empezando por el número 0). La siguiente tabla describe la nomenclatura usada por Red Hat para los principales interfaces de red.

Interfaz	Descripción
lo	Interfaz virtual para pruebas (tiene asignada la dirección IP 127.0.0.1).
eth	Dispositivos Ethernet (también puede definir dispositivos ADSL y Ethernet .).

wlan	Dispositivos Ethernet inalámbricos.
tr	Redes en anillo de tipo Token Ring.
ppp	Conexión mediante módem o RDSI.
hdi	Dispositivo BlueTooth.

Cada dispositivo de red cuenta con una dirección física de acceso al medio (**dirección MAC**) única y diferente, asignada por el fabricante. Sin embargo, durante el proceso de activado del interfaz de red deben asignarse sus parámetros de conexión.

La dirección MAC de una tarjeta Ethernet está formada por 48 bits representados en 6 campos con 2 dígitos hexadecimales cada uno.

## 4.2. TCP/IP.

El protocolo de comunicaciones **TCP/IP** (*Transmission Control Protocol/Internet Protocol*) permite la localización y comunicación de todo tipo de máquinas conectadas a Internet. TCP/IP está constituido por un conjunto de protocolos basado en capas <sup>[4]</sup>:

- La capa de red -equivalente al nivel 3 de la norma OSI-, que establece el camino óptimo que deben seguir los paquetes de información que comunican varias máquinas. Utiliza el **Protocolo de Internet (IP)**.
- La capa de transporte -equivalente al nivel 4 de la pila de protocolos OSI-, que permite establecer una conexión entre nodos de la red. Existen 2 protocolos de transporte: el **Protocolo para el Control de la Transmisión (TCP)** -que realiza una comunicación síncrona y segura con recuperación de datos en caso de error- y el **Protocolo de Datagramas del Usuario (UDP)** -que permite una comunicación asíncrona basada en paquetes denominados **datagramas**.

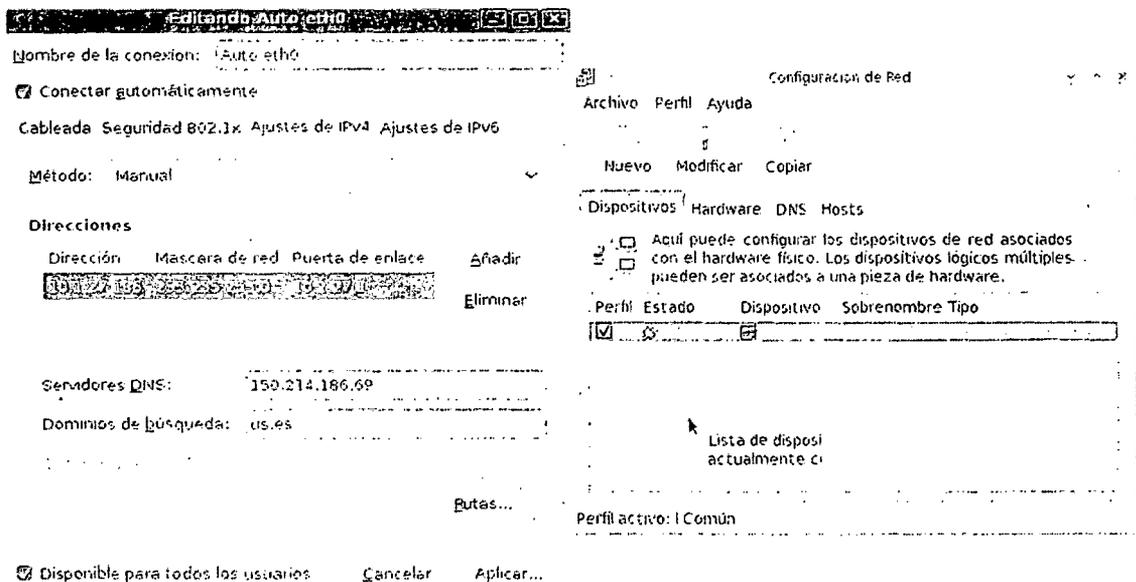
El conjunto de protocolos TCP/IP establece un mecanismo basado en direcciones y nombres que permite localizar inequívocamente cada máquina conectada a Internet. Las equivalencias entre direcciones IP y nombres de máquinas son realizadas por ordenadores especiales que atienden las consultas mediante el protocolo conocido como **Servicio de Nombres de Dominios (DNS)**.

El administrador del sistema tiene que establecer los parámetros para cada interfaz de red del sistema, bien mediante ficheros de configuración locales, bien generados por un servidor DHCP remoto, que puede asignar

los valores estática o dinámicamente. En ambos casos, deben especificarse los aspectos descritos en la siguiente tabla.

<b>Dirección IP del interfaz:</b>	Dirección única y diferenciada en toda Internet o en la red privada, formada por 32 bits en IPv4 o por 128 bits en IPv6.
<b>Máscara de red:</b>	Especifica mediante una operación lógica Y la porción de bits de la dirección IP común a todas las máquinas de la misma subred.
<b>Dirección de difusión de la red:</b>	Usada para enviar paquetes de información a todos los dispositivos de la misma subred.
<b>Nombre del nodo y nombre del dominio de red:</b>	Ambos valores en conjunto describen fácil y unívocamente una determinada máquina en toda Internet o en la red privada.
<b>Direcciones de los servidores de nombres:</b>	Servidores encargados de la resolución de nombres en Internet mediante el protocolo DNS. No suele usarse en redes privadas.

La siguiente figura muestra la pantalla de opciones de configuración de **NetworkManager**, incluida en GNOME 2.30 de Ubuntu 10.04 (izquierda), y la pantalla principal de **system-config-network**, suministrada con Fedora 13 (derecha); herramientas que pueden utilizarse en la configuración básica de las interfaces de red.



### 4.3. Configuración de la red.

Para terminar la instalación básica de la red, el responsable del sistema debe revisar –y en algunos casos modificar– los ficheros de configuración de los servicios esenciales del sistema. La siguiente tabla describe los formatos de estos ficheros.

<b>/etc/sysconfig/network</b>	
<b>Descripción:</b>	Usado en Fedora para establecer los valores de las variables básicas para el servicio de red (nombre, dominio, dirección del <i>encaminador</i> , etc).
<b>Formato:</b>	<i>Variable=Valor</i> ...
<b>/etc/sysconfig/network-scripts/ifcfg-Interfaz</b>	
<b>Descripción:</b>	Usado en Fedora para asignar los valores de las variables de red específicas para cada interfaz de red (recogida de valores de red mediante DHCP, BOOTP o local), dirección IP, máscara de red, dirección de difusión, etc.
<b>Formato:</b>	<i>Variable=Valor</i> ...
<b>/etc/network/interfaces</b>	
<b>Descripción:</b>	Fichero equivalente al anterior, usado en Ubuntu para configurar todas las interfaces de red del sistema.
<b>Formato:</b>	<i>[auto Interfaz]</i> <i>iface Interfaz Parámetros</i> <i>  [Variable Valor]</i> ... ...
<b>/etc/hosts</b>	
<b>Descripción:</b>	Almacena la asociación entre dirección IP, nombre y alias de ordenadores conocidos. Siempre debe estar presente la dirección 127.0.0.1.
<b>Formato:</b>	<i>DirecciónIP Nombre [Alias ...]</i> ...
<b>/etc/resolv.conf</b>	
<b>Descripción:</b>	Establece las bases para la resolución de nombres, indicando dominio del ordenador, dirección de los servidores de nombres y otros dominios de interés.
<b>Formato:</b>	<i>domain Dominio</i> <i>nameserver IPServidorDNS</i> ... <i>[search DominioBúsqueda ...]</i>

<b>/etc/nsswitch.conf</b>	
<b>Descripción:</b>	Indica el orden de búsqueda para ficheros de red.
<b>Formato:</b>	<i>TipoFichero TipoBúsqueda ...</i> ...
<b>Tipos de búsqueda:</b>	files: archivos locales. nis: NIS. nisplus: NIS+. ldap: servicio de directorios. dns: servicio de nombres.
<b>/etc/services</b>	
<b>Descripción:</b>	Indica el protocolo y el puerto utilizados por cada servicio de comunicaciones (este fichero no debe modificarse, ya que suele estar bien configurado).
<b>Formato:</b>	<i>Servicio Puerto/Protocolo [ Alias ... ]</i> ...

#### **4.4. Servicios de red.**

Los protocolos definidos para controlar cada servicio de comunicaciones utilizan una especie de punto de anclaje a los protocolos TCP o UDP. Este mecanismo es conocido como **puerto**.

Si una aplicación quiere ofrecer un cierto servicio, se engancha ella misma a un puerto y espera las peticiones de los clientes (escuchar en el puerto). Cuando un cliente quiere usar este servicio, el sistema le asigna un puerto libre en su nodo local y se conecta al puerto del servidor en el nodo remoto.

Un puerto del servidor puede ser abierto por diferentes máquinas, pero no existe la posibilidad de ser usado por más de una de ellas al mismo tiempo <sup>[6]</sup>. Por lo tanto, para atender las peticiones de múltiples clientes, el servidor puede delegarlas a subprocesos que las gestionan individualmente.

##### **4.4.1. Breve descripción de los principales servicios de red.**

Para finalizar el capítulo, la siguiente tabla presenta una sencilla descripción de los servicios de red más utilizados en Linux.

<b>dhcp</b>	
<b>Descripción:</b>	Servicio de asignación remota de parámetros de la red, tanto estática como dinámicamente; utiliza el protocolo DHCP, aunque también puede usar BOOTP.
<b>Fichero de configuración:</b>	/etc/dhcpd.conf
<b>ldap</b>	
<b>Descripción:</b>	Servicio de acceso a directorios mediante protocolo LDAP. Un directorio es un árbol donde se incluye todo tipo de recursos agrupados lógicamente.
<b>Fichero de configuración:</b>	/etc/openldap/slapd.conf
<b>Directorio de esquemas LDAP:</b>	/etc/openldap/schemas
<b>httpd, apache2</b>	
<b>Descripción:</b>	Servicio de acceso a la información mediante hipertexto, utilizando los protocolos HTTP.
<b>Fichero de configuración:</b>	/etc/Servicio/conf/httpd.conf, /etc/Servicio/conf.d/*
<b>squid</b>	
<b>Descripción:</b>	Servicio de acceso a la información mediante hipertexto, utilizando el protocolo HTTP.
<b>Fichero de configuración:</b>	/etc/squid/squid.conf
<b>samba</b>	
<b>Descripción:</b>	Servicio que permite compartir recursos (ficheros e impresoras) mediante los protocolos CISS o SMB.
<b>Fichero de configuración:</b>	/etc/samba/smb.conf
<b>ssh</b>	
<b>Descripción:</b>	Servicio para la conexión remota y segura al intérprete de mandatos del sistema mediante Secure Shell.
<b>Ficheros de configuración:</b>	/etc/ssh/sshd_config, /etc/ssh/ssh_config

## subversion

<b>Descripción:</b>	Servicio para el control y almacenamiento de versiones y revisiones de ficheros, soporta accesos SVN y WebDAV.
<b>Fichero de configuración:</b>	Configuración de acceso WebDAV mediante Apache.

## 5. Arranque y servicios.

### 5.1. Proceso de arranque.

Durante el proceso de arranque de la máquina se realizan las comprobaciones necesarias para configurar y activar todos los servicios definidos por el administrador del sistema. Es fundamental conocer este procedimiento y preparar los cambios necesarios según la planificación realizada para dicho ordenador.

El proceso de arranque de un servidor Linux basado en arquitectura x86 (Intel, AMD) comprende los siguientes pasos <sup>[2]</sup>:

- Tras comprobar los dispositivos de la máquina, el BIOS ejecuta el primer paso del cargador del sistema, situado en el sector de arranque del primer disco duro. GRUB es el cargador usado actualmente en Linux.
- El cargador de arranque ejecuta el segundo paso del proceso, situado en la partición `/boot`.
- El núcleo de Linux y sus módulos adicionales se cargan en memoria y se monta la partición raíz en modo de sólo lectura.
- El núcleo toma el control de la secuencia de arranque y ejecuta el proceso de inicio (`/sbin/init`).
- Este programa de iniciación carga todos los servicios definidos, ejecuta los programas de iniciación y configuración y monta las particiones definidas. `/sbin/init` lee la información de los ficheros de configuración (`/etc/inittab` en SysVinit de Fedora o `/etc/event.d/*` en Upstart de Ubuntu). El proceso carga en primer lugar los servicios básicos y luego los asociados al nivel de arranque elegido por el administrador.
- Se finaliza el arranque del sistema presentando al usuario el proceso de conexión (**login**) o el entorno gráfico (normalmente GNOME o KDE).

Evidentemente, por motivos de seguridad, todos los ficheros y mandatos de configuración tienen que estar completamente vetados para los usuarios normales del servidor y sólo pueden ser ejecutados o modificados por el usuario **root**.

**SysVinit**, implantado por defecto en Fedora y en muchas otras distribuciones Linux, es un proceso de arranque secuencial (basado en System V Init), que es lento y presenta ciertos problemas para usar nuevos dispositivos (como sistemas de archivos en USB).

Ubuntu utiliza **Upstart**, un proceso controlado por eventos que aún está en proceso de desarrollo y que puede emular el funcionamiento de SysVinit.

Existen también otras alternativas en desarrollo basadas métodos de arranque paralelo (**init-NG**) o dirigidas por eventos (**Solaris Service Management Facility** o **Apple launchd**).

## 5.2. El cargador GRUB.

Como se ha descrito en el apartado anterior, un programa cargador de arranque es el encargado de iniciar un sistema operativo.

Los principales cargadores usados por Linux soportan la definición de un menú de ejecución para los distintos sistemas operativos instalados en el ordenador e iniciarlos en determinados niveles de ejecución.

El **Cargador de Arranque Unificado de GNU (GRUB)** <sup>[1]</sup> permite al usuario elegir el sistema operativo y el núcleo con que desea trabajar.

GRUB tiene 2 modos de operación <sup>[2]</sup>:

- El **modo directo** se usa para cargar el núcleo de Linux sin ningún tipo de intermediarios.
- El **modo encadenado** se utiliza para cargar otros sistemas operativos y apunta al primer sector de arranque de la partición, donde se encuentran los ficheros de iniciación del sistema.

GRUB ofrece al usuario un entorno de operación válido para realizar configuraciones previas al inicio del sistema operativo, pudiendo acceder directamente a su fichero de control `/boot/grub/grub.conf` o `/boot/grub/menu.lst`.

Las órdenes para la configuración de GRUB definen las características del menú de arranque, indicando los distintas opciones de carga de sistemas, la opción por omisión, límites temporales, entorno gráfico, etc.

El siguiente ejemplo presenta la configuración de un menú para arrancar Ubuntu 10.04 Lucid con un núcleo versión 2.6.32-22 en la segunda partición del primer disco, y Windows XP en la primera partición.

```
boot=/dev/sda
default=0
timeout=5
title Ubuntu 10.04 LTS, kernel 2.6.32-22-generic
 kernel /boot/vmlinuz-2.6.32-22-generic root=/dev/sda2 ro quiet
 initrd /boot/initrd.img-2.6.32-22-generic
 quiet
title Windows XP SP3
 root (hd0,1)
 makeactive
 chainloader +1
```

Cuando se enciende la máquina, GRUB presenta al usuario un menú de selección y éste puede editar las distintas opciones antes de arrancar el sistema operativo correspondiente.

GRUB 2 es una versión en desarrollo, incluida en las nuevas distribuciones de Linux, que supone una redefinición del cargador, para permitir su uso en diferentes arquitecturas, acceder a los sistemas de ficheros locales, incluir un lenguaje de *scripts* complejo, etc.

### 5.3. El Núcleo.

Los sistemas operativos Unix se basan en una estructura de capas, donde las capas internas prestan servicios básicos a las externas. El **Núcleo** (*kernel*) es la parte principal del sistema operativo, realiza las funciones básicas de control y presta los servicios esenciales para gestionar el sistema operativo.

El núcleo de Linux consta principalmente de los componentes descritos en la siguiente tabla <sup>[10]</sup>.

<b>Gestor de memoria:</b>	Encargado de asignar áreas de memoria y de espacios de paginación a los procesos, a los módulos del núcleo y al área de <i>caché</i> .
<b>Gestor de procesos:</b>	Parte esencial que crea, activa y termina los procesos; implementa las reglas de la multitarea.
<b>Controladores de dispositivos:</b>	Gestionan la comunicación del sistema con cada uno de los dispositivos conectados. El núcleo se configura en el proceso de arranque para cargar los módulos necesarios para controlar los dispositivos específicos de cada máquina.
<b>Gestor del sistema de archivos virtual:</b>	Capa intermedia que permite acceder uniformemente a los sistemas de archivos, manteniendo un árbol de directorios homogéneo.
<b>Gestor de redes:</b>	Capa abstracta para el acceso general a la red informática, independientemente del tipo de dispositivos usado y de la arquitectura de la red.

Siendo Linux un sistema operativo basado en el código abierto, el administrador puede rehacer el núcleo, incluyendo o eliminando características operativas, según sus necesidades. El proceso para recompilar el núcleo de Linux es cada vez más sencillo de realizar, ya que se configura mediante menús con una gran cantidad de opciones.

Para aumentar las prestaciones del sistema, es conveniente contar con un núcleo pequeño, pero que pueda tratar todas las funciones básicas del sistema. La gestión de los dispositivos y de las funciones adicionales puede ser controlada por los módulos del núcleo.

### 5.3.1. Módulos.

Los módulos del núcleo de Linux son objetos compilados en lenguaje C que controlan elementos o funciones específicas.

Los módulos básicos para el control de los dispositivos conectados se cargan en el proceso de arranque del sistema operativo. El resto de módulos que el gestor del sistema considera necesarios deben enumerarse en los ficheros de configuración, así como los parámetros opcionales que éstos requieran para obtener un funcionamiento óptimo del servidor.

La versión 2.4 del núcleo de Linux usa un único fichero `/etc/modules.conf`, mientras que las distribuciones basadas en la versión 2.6 del núcleo localizan varios ficheros (uno por módulo o grupo de módulos) en el directorio `/etc/modprobe.d`.

En los ficheros de configuración se especifican las asociaciones (alias) entre módulos reales y virtuales. Los módulos virtuales son las interfaces entre el sistema y los módulos que controlan dispositivos reales; son los encargados, por ejemplo, de gestionar la red, los sistemas de archivos especiales, las capacidades exclusivas de tarjetas de sonido, etc.

La siguiente tabla describe las órdenes del sistema implicadas en la gestión de los módulos del núcleo.

Mandato	Descripción
<code>lsmod</code>	Lista los módulos cargados.
<code>modprobe</code>	Prueba un determinado módulo del sistema e indica si puede ser instalado.
<code>insmod</code>	Instala un nuevo módulo.
<code>rmod</code>	Desinstala un módulo cargado.

### 5.3.2. Parámetros de operación.

Las nuevas versiones de los núcleos de Linux soportan la configuración y personalización de sus parámetros de operación, que afectan a la conducta de sus componentes, tales como: incrementar el máximo

número de ficheros abiertos (`fs.file-max`) o activar la capacidad de reenviar paquetes para crear cortafuegos (`net.ipv4.ip_forward`).

Las modificaciones en el entorno predefinido para el núcleo se verán reflejadas en el fichero correspondiente a la característica modificada, situado en el sistema de archivos virtual `/proc/sys`.

El fichero de configuración de los parámetros operativos del núcleo es `/etc/sysctl.conf` y puede ser editado por el responsable del sistema para incluir los cambios en el próximo arranque del sistema. Asimismo, los cambios se activan automáticamente ejecutando la orden `sysctl -p`.

La siguiente tabla muestra el formato de las líneas del fichero `/etc/sysctl.conf`.

Formato	Descripción
<b><code>/etc/sysctl.conf</code></b>	
<code>Componente[.Subcomp].Parámetro = Valor</code> ...	Configuración de los parámetros del núcleo. Los campos son: <ol style="list-style-type: none"><li>1. Componente principal del núcleo: núcleo (<code>kernel</code>), memoria virtual (<code>vm</code>), sistema de archivos (<code>fs</code>) o red (<code>net</code>). Algunos de éstos pueden contar con grupos (directorios) de parámetros.</li><li>2. Parámetro de operación.</li><li>3. Valor asignado al parámetro.</li></ol>

Algunos programas pueden almacenar también ficheros de configuración de parámetros del núcleo en el directorio `/etc/sysctl.d`, los cuales utilizar una sintaxis similar a la del fichero principal.

Puede obtenerse una completa información sobre los parámetros de operación del Núcleo de Linux en la documentación del código fuente del Kernel y en su página de descarga<sup>[x]</sup>.

#### **5.4. Niveles de arranque en SysVinit.**

Muchas distribuciones Linux, como Fedora, utilizar un proceso de arranque secuencial heredado de Unix System V, conocido como **SysVinit**.

Los niveles de arranque sirven para que SysVinit pueda operar de distintas maneras según las necesidades del administrador. Simplemente

cambiando el nivel de arranque, el sistema operativo puede entrar en modo mantenimiento y posteriormente volver al modo multiusuario.

La siguiente tabla describe los niveles de ejecución soportados por SysVinit.

Nivel	Descripción
0	Parada del sistema.
1 o S	Nivel de mantenimiento para usuario privilegiado (monousuario).
2	Definido por el administrador en Fedora, por defecto en Ubuntu, multiusuario sin NFS en Solaris y AIX.
3	Nivel de multiusuario, definido por el administrador en Ubuntu.
4	Definido por el administrador o no usado.
5	Nivel de multiusuario con entorno gráfico, definido en Ubuntu.
6	Rearranque del sistema.

El nivel de arranque usado por defecto en el sistema se define en el fichero de configuración `/etc/inittab`. Sin embargo, la orden `init` permite modificar el nivel de ejecución de la máquina en cualquier momento.

El mandato `init` lee los guiones de configuración almacenados en el subdirectorio `/etc/rcN.d`, correspondiente al nivel de ejecución seleccionado. El modo de operación es el siguiente:

- Parar en secuencia los procesos correspondientes a los ficheros `KNNservicio`, siendo `NN` el orden de la secuencia (2 dígitos) para dicho servicio (se ejecuta: `/etc/rcN.d/KMMservicio stop`).
- Arrancar en orden secuencial los procesos de los ficheros `SNNservicio` (se ejecuta: `/etc/rcN.d/SMMservicio start`).

Los guiones de ejecución de servicios se encuentran normalmente en el directorio `/etc/init.d` y están enlazados simbólicamente a los *scripts* de cada nivel de ejecución. De esta manera, el administrador puede arrancar o parar servicios independientemente, ejecutando el *script* correspondiente o el orden `service` de Fedora:

```
service Servicio { start|stop|restart|reload|status }
```

La siguiente tabla describe algunos de los programas incluidos en Fedora 13 para la gestión de servicios ejecutados en el proceso de arranque del servidor.

Mandato	Descripción
chkconfig	Establece los enlaces simbólicos para incluir un servicio en los niveles de arranque indicados.
ntsysv	Menú para establecer los servicios que se ejecutarán en los niveles de multiusuario.
service	Arranca o para un determinado servicio.
system-config-services	Interfaz gráfica para la gestión de servicios, incluidos los dependientes de Inetd.
telinit	Cambia al nivel de ejecución especificado.

El siguiente gráfico muestra un ejemplo de arranque de una máquina con Fedora 13.

```

Máquina Dispositivos Ayuda
/dev/sda1: limpio, 36/128816 ficheros, 43791/512088 bloques
Remontando sistema de archivos raíz en modo de lectura y escritura [OK]
Montando sistema de archivos local: [OK]
Activando cuotas del sistema de archivos local: [OK]
Activando espacio swap de /etc/fstab: [OK]
Entrando en el inicio no interactivo
Starting monitoring for UG uy_fedora: 2 logical volume(s) in volume group "uy_
fedora" monitored
ip6tables: Aplicando las reglas del cortafuegos: [OK]
iptables: Aplicando reglas del cortafuegos: [OK]
Iniciando auditd: [OK]
Iniciando portreserve: [OK]
Iniciando logger del sistema: [OK]
Iniciando irqbalance: [OK]
Iniciando rpcbind: [OK]
Iniciando mdmmonitor: [OK]
Iniciando bus de mensajes del sistema: [OK]
Configurando parámetros de red... [OK]
Iniciando el demonio NetworkManager: [OK]
Iniciando demonio Avahi... [OK]
Uso de NFS statd: [OK]
Iniciando idmospd RPC: [OK]
Iniciando cups: [OK]

```

## 5.5. Trabajos en Upstart.

**Upstart** <sup>[viii]</sup> es un proceso de arranque no secuencial basado en eventos que ha sido incluido por defecto a partir de la versión 6.10 de Ubuntu.

Un trabajo es una tarea o un servicio que puede ser ejecutado o detenido cuando se dispara un evento, y que también puede generar nuevos eventos para gestionar otros trabajos que dependen de él.

Un sistema de arranque de este tipo tiene la ventaja de poder lanzar las tareas necesarias cuando el sistema reconoce los dispositivos correspondientes, sin necesidad de esperar a terminar la ejecución de tareas anteriores. Por lo tanto, puede definirse una especie de árbol de ejecución de tareas.

Upstart puede emular el modo de trabajar de SysVinit, definiendo niveles de ejecución para los servicios generales del sistema. Ubuntu 8.10 Intrepid

define por defecto el nivel 2, además de los niveles de mantenimiento (0, 1 y 6).

El siguiente ejemplo muestra el fichero `/etc/event.d/rc2`, que configura el trabajo para definir el nivel de ejecución 2.

```
start on runlevel 2
stop on runlevel [!2]
console output
script
 set $(runlevel --set 2 || true)
 exec /etc/init.d/rc 2
endscript
```

El administrador puede definir el orden de arranque de los servicios, de manera similar a SysVinit, incluyendo los enlaces simbólicos a los *scripts* correspondientes en el directorio `/etc/init.d/rcN.d` o ejecutando la orden **update-rc.d**.

El formato de ejecución para arrancar o parar un servicio es el siguiente:

```
/etc/init.d/Servicio { start|stop|restart|reload|status }
```

La tabla describe algunos de los mandatos de gestión de servicios y trabajos de arranque en Ubuntu 7.10.

Mandato	Descripción
<code>initctl</code>	Utilidad de control del proceso de arranque para ejecutar órdenes y lanzar eventos.
<code>start</code>	Arranca un trabajo
<code>status</code>	Muestra el estado de ejecución de un trabajo.
<code>stop</code>	Para un trabajo.
<code>telinit</code>	Cambia al nivel de ejecución especificado.
<code>update-rc.d</code>	Gestiona los enlaces para los <i>scripts</i> del tipo SysVinit.

## 5.6. Servicios.

Los servicios son programas cargados en un determinado nivel de ejecución, que suministran al usuario ciertas utilidades o beneficios. Cada servicio supone una posibilidad de conexión con la máquina, lo que también implica la posibilidad de sufrir ataques contra la seguridad del sistema.

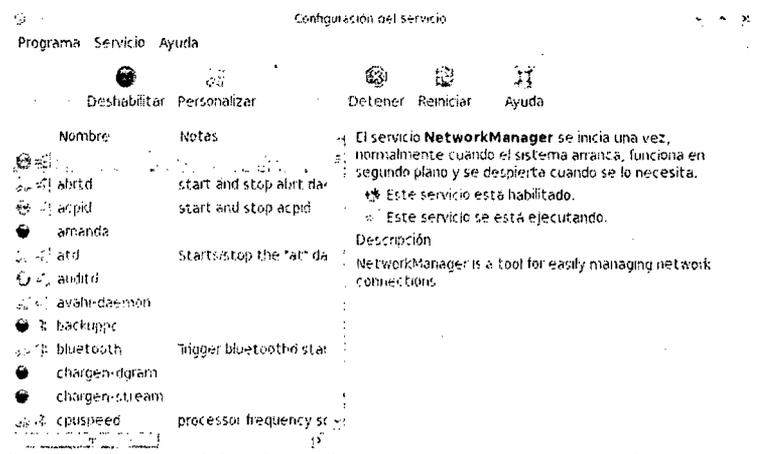
El administrador sólo debe activar los servicios estrictamente necesarios para su máquina.

La siguiente tabla describe de forma breve los servicios más usados en Linux.

<b>Servicio</b>	<b>Descripción</b>
<b>apmd</b>	Control de ahorro de energía.
<b>atd</b>	Planificador de tareas.
<b>avahi-daemon</b>	Cliente para descubrir servicios de configuración de red Zeroconf.
<b>bluetooth</b>	Control de conexiones Bluetooth.
<b>crond</b>	Ejecución cronológica de programas.
<b>cups, cupsys</b>	Servidor de impresión mediante protocolo IPP.
<b>dhcp</b>	Servicio DHCP para la asignación remota de parámetros de la red.
<b>httpd, apache2</b>	Servidor Apache para suministrar acceso a páginas <i>web</i> .
<b>inn</b>	Servicio de noticias.
<b>ldap</b>	Servicio de directorios LDAP.
<b>mailman</b>	Servidor de lista de distribución de correo con interfaz <i>web</i> .
<b>named</b>	Servidor de nombres de dominio (DNS).
<b>NetworkManager</b>	Servicio que mantiene activas las conexiones de red.
<b>nfs</b>	Acceso remoto a directorios mediante NFS.
<b>ntpd</b>	Servidor de sincronización horaria.
<b>postfix</b>	Servidor de correo electrónico.
<b>rsync</b>	Sincronización remota de contenido entre servidores.
<b>sendmail</b>	Servidor de correo electrónico.
<b>sockd</b>	Servidor representante ( <i>proxy</i> ) para aplicaciones.
<b>samba, smb</b>	Servicio para compartir ficheros y recursos, compatible con la red de Windows.

<b>squid</b>	Servidor representante ( <i>proxy</i> ) para accesos mediante HTTP y FTP.
<b>ssh</b>	Conexión segura.
<b>svnserve</b>	Servicio independiente de Subversion (sin Apache).
<b>syslogd</b>	Registro de anotaciones e incidencias.
<b>sysstat</b>	Recopilador de estadísticas de actividad del sistema.
<b>wu-ftp</b>	Servicio FTP para transferencia de ficheros.
<b>xinetd</b>	Metaservicio de red.
<b>ypserv</b>	Servicio principal para NIS o NIS+.

El siguiente gráfico muestra la aplicación para gestión de servicios **system-config-services** incluida en Fedora 13.



## 5.7. Control básico de procesos.

Puede entenderse por **proceso** todo programa o mandato en ejecución. Un proceso tiene las siguientes características:

- Cada proceso consta de zona de código, de datos y de pila.
- Los procesos existen en una jerarquía de árbol (varios hijos, un sólo padre).
- El sistema asigna un identificador de proceso (**PID**) único al iniciar el proceso.
- El planificador de tareas asigna un tiempo compartido para el proceso según su prioridad (sólo **root** puede aumentar la prioridad de un proceso).

- Cada proceso almacena su identificador (**PID**) el de su proceso padre (**PPID**), el propietario y grupo del proceso y las variables de entorno.

El *superusuario* debe mantener el control del sistema en todo momento, realizando revisiones periódicas de los procesos que se están ejecutando en el servidor, lo que puede evitar problemas y abusos que afecten el funcionamiento normal de la máquina.

La siguiente tabla describe los mandatos más usados para el control de procesos.

Mandato	Descripción
<b>ps</b>	Presenta una lista con los procesos activos en la máquina, indicando propietario, identificador del proceso (PID), identificador del proceso padre (PPID), mandato, etc.
<b>kill</b>	Manda una señal de interrupción a uno o a varios procesos. Suele usarse para finalizar su ejecución.
<b>pgrep</b>	Lista procesos que cumplan un cierto criterio.
<b>pkill</b>	Manda una señal a procesos que cumplan un cierto criterio (tener especial cuidado al ejecutar esta orden).
<b>nice</b>	Cambia la prioridad de los procesos. Suele usarse para bajar el tiempo de ejecución de procesos que saturan al sistema.
<b>top</b>	Presenta una lista actualizada de los procesos que consumen más recursos. También permite mandar señales y modificar la prioridad de ejecución.
<b>lsof</b>	Lista los ficheros y las conexiones de red abiertos por cada proceso, indicando además el propietario, PID, prioridad, mandato, etc.

El mandato **lsof** es una potente herramienta administrativa, ya que muestra todos los ficheros, tuberías con nombre, dispositivos y conexiones de red abiertos por cada proceso. Suele usarse para comprobar aquellos procesos sospechosos de crear problemas y para revisar las conexiones de red de cada servicio.

Por último, el siguiente gráfico muestra la ejecución de **KSysGuard** del entorno KDE 4.4 bajo Fedora 13, que puede usarse para realizar una gestión básica de los procesos del sistema.

Monitor del sistema

Tabla de procesos Carga del sistema

Nombre	Usuario	CPU %	Memoria	Comando	Título de la ventana
ksysguard	practica	0%	6.7 M	26.6 M	Monitor del sistema
plasma-desktop	practica		9.8 M	24.8 M	
systemsettings	practica		6.2 M	17.1 M	Preferencias d...
kwin	practica		5.6 M	16.1 M	Sin título - Alzate
ksysde	practica		4.7 M	13.5 M	practica: Sys...
ksysguardd	practica	2%	0.2 M	0.7 M	
valvesort	practica		24.4 M	6.6 M	
python	practica		12.6 M	22.0 M	
krnotify	practica		5.4 M	12.5 M	
kwin	practica		5.7 M	16.8 M	
nepermi.services	practica		4.2 M	11.6 M	
krumner	practica		4.2 M	12.2 M	
kdeife	practica		5.5 M	15.5 M	

136 procesos CPU: 28% Mem: 242.6 MB Interfaz: 0 B