UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

CENTRO DE TECNOLOGÍA DE INFORMACIÓN DE LA FACULTAD DE INGENIERÍA

TESIS PROFESIONAL
QUE PARA OBTENER EL TÍTULO DE
INGENIERO EN COMPUTACIÓN
P R E S E N T A :

IGNACIO RAMSES MENDOZA GAYOSSO

DIRECTOR DE TESIS:
ING. FCO. JAVIER MONTOYA CERVANTES

CO-DIRECTOR DE TESIS:
M. EN. I. CESAR ENRIQUE BENITEZ JOYNER

CIUDAD UNIVERSITARIA **2006**

AGRADECIMIENTOS

Solo me resta agradecer a Dios, a mis Padres, a mis Amigos
a mi Director y Co-Director de Tesis, a mis Profesores, a mi Universidad
y a todos aquellos que directa o indirectamente aportaron un granito
de arena para que yo lograra convertirme en la persona que soy.

Siempre les estaré profundamente agradecido.

IGNACIO RAMSES MENDOZA GAYOSSO

SIEMPRE HAY QUE TENER LA FUERZA Y LA ESPERANZA
PARA LLEGAR HASTA EL FINAL…

ÍNDICE TEMÁTICO:

INTRODUCCIÓN

En la actualidad, la tecnología de la información avanza a la velocidad de Internet y los cambios en los medios tecnológicos e informáticos son sorprendentemente drásticos, lo que ha obligado a las instituciones educativas de nivel medio y superior a mantenerse en constante evolución en lo referente a las herramientas con las que los alumnos y académicos pueden acceder a esa información.

Un **C**entro de **T**ecnología de **I**nformación (CTI) involucra la integración de aspectos técnicos, conocimientos administrativos, conceptos informáticos y experiencias teóricas y prácticas. El objetivo de un CTI es hacer que las tareas en donde se involucra un equipo de cómputo se realicen de manera más óptima, sencilla y en menor tiempo gracias a los recursos de software y hardware con que se dispone.

Así, un CTI busca brindar servicio y apoyo a las distintas áreas independientemente de donde esté albergado, esto, con la intención de proporcionar nuevas técnicas y herramientas que permitan enfrentar el futuro con nuevas expectativas.

La operación de un CTI debe llevarse a cabo de acuerdo con las funciones que a cada departamento o área correspondan y éstas a su vez deben ser delegadas por el administrador del mismo. La actividad prioritaria a realizar en el CTI, es la investigación, realización de proyectos académicos y consultas en la Web, así como el uso del correo electrónico, entre otros servicios de Internet.

El presente trabajo busca documentar e implementar los procesos y actividades necesarios para la planificación, organización y mantenimiento del **C**entro de **T**ecnología de **I**nformación, CTI, en la Facultad de Ingeniería que dispondrá de una red inalámbrica.
Con el propósito de cubrir estas necesidades, se realizó una investigación bibliográfica y de campo en las diversas áreas especializadas en CTI´s, con el afán de alcanzar los objetivos planteados en este trabajo.

En el **Capítulo 1** se plantean los antecedentes, el objetivo y los alcances pretendidos para este proyecto, así como exponer cuál será la estructura con respecto a la organización del CTI. En el **Capítulo 2,** se determinan los requerimientos fundamentales para el funcionamiento de un CTI, así como el análisis de instalaciones recomendables y requisitos primordiales de hardware y software. La selección del equipo de cómputo y periféricos se trata en el **Capítulo 3**, tomando en cuenta para ello el tipo de usuarios que harán uso de este equipo. En el **Capítulo 4,** se hace referencia a los parámetros de configuración, haciendo énfasis en la red inalámbrica a implementarse en el CTI, pasando además, por la configuración del resto de los elementos de cómputo; la seguridad informática es analizada en el **Capítulo 5,** considerando la prevención recomendable contra diversas amenazas como son virus y hackers y realizando un análisis de las medidas físicas y lógicas que se deben seguir para prevenir un ataque informático. De esta manera, se considera presentar en el **Capítulo 6,** lo concerniente al mantenimiento preventivo y correctivo (tanto físico, como lógico) que se deberá aplicar a todos los equipos de manera periódica. Para el **Capítulo 7,** la administración de todos los servicios que se imparten serán analizados, así como también la relación que mantendrá el CTI con la **Unidad de Servicios de Cómputo Académico,** que estará a cargo del centro.

Finalmente como resultado principal, se pretende elaborar un manual de procedimientos idóneo que facilite la implementación y administración de un Centro de Tecnología de Información para su aplicación en alguna otra área dentro o fuera de la Facultad de Ingeniería.

OBJETIVOS

El objetivo principal de este trabajo de tesis es documentar e implementar los procesos y actividades necesarios para la planificación, organización y mantenimiento del Centro de Tecnología de Información (CTI) de la Facultad de Ingeniería, en el área de Posgrado, que dispondrá de una red inalámbrica.

Al efecto, la Unidad de Servicios de Cómputo Académico (UNICA), que será la encargada de administrar el CTI cuenta con tres salas de atención a usuarios, una en el Edificio Principal (Edificio Norte) y dos en la División de Ciencias Básicas (Edificio Sur) pero, dada la gran demanda en las mismas, se requiere contar con una nueva sala de cómputo para el servicio a los alumnos de Licenciatura y Posgrado.

En cuanto a organización se refiere, es necesario crear una estructura fija que permita desarrollar y mantener los procedimientos para un funcionamiento óptimo del centro. Tanto la planificación como la organización involucran el alcance del proyecto, el cual debido a las condiciones iniciales principalmente en cuestión de recursos se contará con 30 equipos de cómputo para el uso de los alumnos de Licenciatura y Posgrado, pero se tiene contemplado en el proyecto que el número de equipos se incremente en fechas posteriores.

El alcance de este tema de tesis se centra en contar con los procedimientos, técnicas y herramientas fundamentales para la instalación y funcionamiento óptimo del Centro de Tecnología de Información o como era conocido con anterioridad, centro de cómputo, tomando en cuenta los requisitos principales como son:

- Tipo de instalaciones
- Software y hardware
- Parámetros de configuración
- Administración del lugar y los equipos
- Seguridad Informática
- Seguridad en equipos de cómputo e instalaciones

ANTECEDENTES

1.1 Generalidades

La computación es una de las áreas de mayor interés en los diversos campos del conocimiento humano, y que se ha desarrollado tecnológica y científicamente, caracterizándose por estar bien definida y con gran integración en otras disciplinas técnicas, económico-administrativas, ciencias físico-matemáticas y socioeconómicas. La utilización de las ciencias computacionales facilita en gran medida el manejo de grandes volúmenes de información desde varios puntos de vista.

Además, los campos o áreas en los que se están empleando cubren un número infinito de aplicaciones como lo son: sistemas bancarios, análisis y diseño de sistemas físicos de alta complejidad en Ingeniería, manejo de datos estadísticos experimentales en ciencias puras como la biología, física, ciencias de la salud y las ciencias sociales, aplicaciones en sistemas expertos, inteligencia artificial, robótica y manufactura flexible.

La tecnología de la computación ha modificado de manera importante la forma de trabajar de toda la humanidad. La dependencia que tenemos en la actualidad de las computadoras es evidente. Sin embargo, los sucesos han ocurrido con tal rapidez que se requiere de un análisis formal para comprobar la magnitud de esa dependencia. Una manera drástica, pero muy objetiva de ilustrarla, sería imaginar lo que podría suceder si de un momento a otro se desconectaran todas las computadoras en el mundo. Los efectos serían más graves que los causados por una guerra.

De ahí la importancia que tienen las computadoras en nuestras vidas, por tal razón es conveniente conocer y analizar los sitios en donde por lo general se albergan estos equipos. En los últimos tiempos, el auge que han alcanzado la computación y la aplicación de nuevas tecnologías en el manejo de la información, a través de sistemas de cómputo en los distintos campos de la docencia, investigación y administración, deben vincularse con las actividades académicas y de investigación de los alumnos, profesionales e investigadores de la Facultad de Ingeniería.

Concretamente un **Centro de Tecnología de Información (CTI) se refiere al conjunto de recursos físicos, lógicos y humanos necesarios para la organización, realización y control de las actividades informáticas de un lugar**. Con anterioridad se indicaba un local que alojaba equipo de cómputo y personal que operaba tales equipos; este concepto se ha renovado con apego a los tiempos que se viven, en donde los cambios en los medios informáticos y de Internet nos llevan a un paso por demás acelerado.

Comúnmente se piensa que en un CTI sólo existen computadoras que están a disposición de los diversos usuarios que hacen uso de éstas, pero en realidad en un CTI, se prestan otros servicios como lo son:

- El desarrollo y mantenimiento de sistemas informáticos
- Vigilar que el sistema computarizado se mantenga funcionando apropiadamente detectando y corrigiendo fallas en el mismo.
- Manejo de grandes volúmenes de información
- Realización de copias de respaldo
- Comunicación vía Internet
- Administración de recursos en el rubro de hardware y software
- Incorporación de acciones correctivas conforme a las fallas que se detecta en el equipo de cómputo y paquetería instalada.
- Llevar registros de fallas, problemas, soluciones, acciones desarrolladas, respaldos, recuperaciones y trabajos realizados.
- Realizar labores de mantenimiento y limpieza de los equipos del CTI
- Aplicar en forma estricta las normas de seguridad y control establecidas
- Cumplir con las normas, reglamentos y procedimientos establecidos para el desarrollo y funcionamiento del lugar.

La importancia que tiene un CTI lo sitúa en una posición que influye incluso en gran medida en

la toma de decisiones administrativas y de proyección de las empresas u organizaciones, debido a la información que se maneja a través de éste; su administración involucra el control tanto físico como económico y del buen funcionamiento del software y hardware, así como el desempeño del personal que labora en él.

Si estos conceptos se manejan estrictamente, la fluidez de la información de entrada y salida, el mantenimiento del equipo y personal idóneo, estarán cumpliendo con las condiciones necesarias para que funcione correctamente el CTI. El desarrollo tecnológico ha permitido que la computadora sea introducida en una gran cantidad de organizaciones, las cuales concentran la función informática en Departamentos, Unidades o Centros de Procesamiento de Datos que se encargan de proporcionar los servicios de cómputo necesarios para la organización.

Un CTI representa una entidad dentro de una organización, que tiene como objetivo satisfacer las necesidades de información, de manera veraz, oportuna y óptima. Su función primordial es apoyar la labor de la institución académica mediante la aplicación y ayuda de un conjunto de recursos de software y hardware para hacerla más segura, fluida, simplificada y competitiva en esta era de la computación.

1.2 Estructura de un CTI

Dentro de las instituciones académicas, existen varias tendencias para implementar un CTI, pero ninguna de éstas puede ser tomada como modelo, ya que la misma institución buscará la que más le convenga, de acuerdo con:

- **Tipo de organización** que se pretende manejar en el CTI en función de las capacidades y recursos con que se cuenta.
- **Capacidad del personal** con respecto a habilidades y conocimientos que se aplicarán en el lugar.
- **Tipo de administración** comprendida en función de la organización, el personal, las instalaciones, los recursos y el equipo de cómputo.

A una mayor escala, un CTI está compuesto por un conjunto de áreas en las que se reparten

todas las actividades que se desarrollan dentro de éste, estas áreas se presentan en el siguiente diagrama:

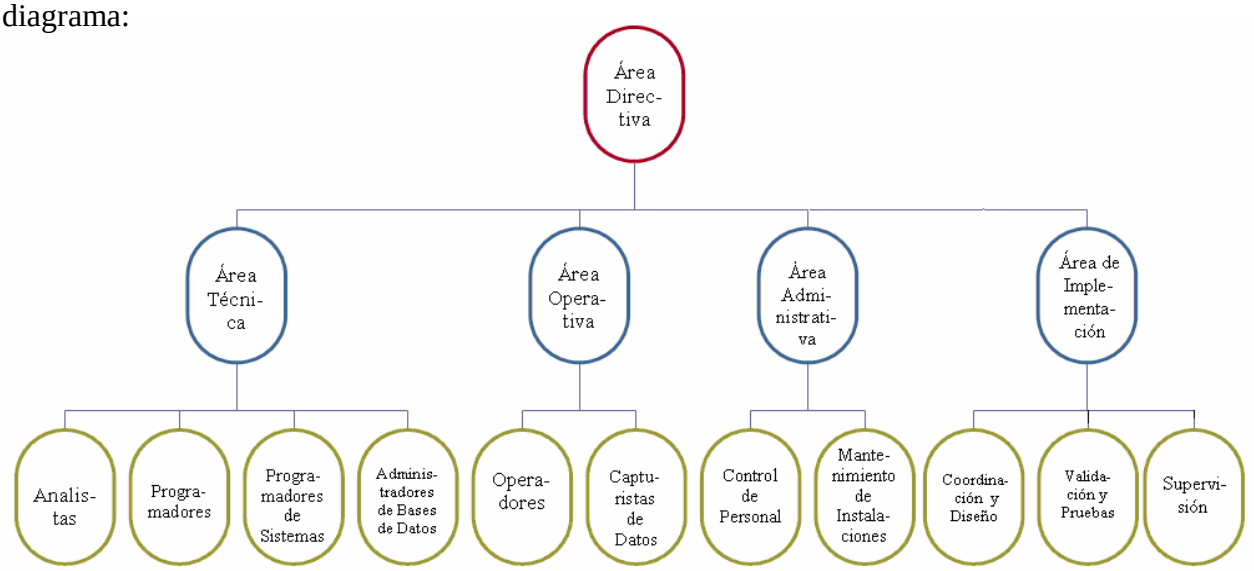

Figura 1.1 Organigrama organizacional sobre un CTI

Dentro de las actividades que se desarrollan en la **Unidad de Servicios de Cómputo Académico (UNICA)**, están contempladas las áreas descritas en la figura 1.1; en su conjunto, la Unidad ofrece los servicios siguientes:

- Correo electrónico
- Cursos de cómputo
- Préstamo de equipo de cómputo
- Internet
- Inventario del equipo de cómputo
- Plan de formación de becarios
- Servicio de base de datos
- Servicio de impresión
- Servicio social
- Asesorías y apoyo técnico en las salas de cómputo
- Desarrollo de sistemas
- Estadísticas

Estos servicios abarcan todas las áreas que componen la estructura organizacional del CTI.

Con el propósito de implementar el alcance previsto para el CTI, son requeridas sólo algunas áreas del diagrama organizacional mostrado en la figura 1.1 y son las siguientes:

- **Área Directiva:** Contiene las funciones de planeación, organización, administración de personal y control, además de coordinar las actividades de las áreas que dependen de ella. Un CTI es una unidad, que proporciona servicios a toda una organización y su área directiva es el enlace principal con las otras áreas y el centro mismo.

- **Área Operativa:** Es la encargada de operar y manipular los sistemas y el equipo con que cuenta el CTI; en otras palabras el software y el hardware; vigilar además que los elementos que componen los diversos sistemas funcionen adecuadamente.

Quedando con esto pendientes el resto de las áreas funcionales para un crecimiento a largo plazo del CTI:

- **Área Técnica:** Esta área esta integrada por expertos en informática y su principal función es brindar el soporte técnico especializado que se requiere en las actividades de cómputo, esta área esta conformada por analistas, programadores, programadores de Sistemas y administradores de base de datos.

- **Área Administrativa:** El área administrativa esta encargada de controlar los recursos económicos para el abastecimiento de materiales especializados tales como: equipo, cintas magnéticas, discos removibles, formas continuas y manuales para el funcionamiento del centro. También tiene el control sobre lo referente al personal y mantenimiento de las instalaciones.

- **Área de Implementación:** Con respecto a esta área, se maneja lo concerniente a la etapa final de los proyectos que son generados por el Centro, es aquí donde se realizan las pruebas finales, la validación definitiva del proyecto así como la supervisión en donde el proyecto se este desenvolviendo.

Muchas instituciones académicas se ven en la necesidad de instalar un CTI para poder brindar un

servicio cada vez más indispensable. Para ello hay que tener presente el diagrama mostrado en la Figura 1.1 en donde se plantea la estructura óptima para montar un CTI que cuente con las áreas principales, cubriendo con ello todas y cada una de sus necesidades y requerimientos.

1.3 Objetivo

La vertiginosa evolución de los medios informáticos en los últimos años, hace imprescindible dotar al futuro profesional del manejo de herramientas primordiales de computación, no como un usuario de una caja negra, sino con una formación suficiente, que le permita tomar decisiones sobre la conveniencia o no de su utilización; es decir, comprender las ventajas y desventajas de cada una de las aplicaciones para hacer un buen uso y obtener un mayor beneficio del capital que se invierte, y de los recursos con que se dispone.

El objetivo principal de este trabajo es **documentar** e **implementar los procesos y actividades** necesarios para la **planificación**, **organización** y **mantenimiento** del CTI que dispondrá de una red inalámbrica.

Debido a la naturaleza de un CTI, son diversos y complejos los problemas que lo aquejan, por tal motivo al alcanzar el objetivo propuesto se minimizan los problemas que puedan surgir, causados por personas (trabajadores de la organización o usuarios); problemas en las máquinas y en los programas, ya sean paquetes informáticos utilizados o los programas que se elaboran para los usuarios, citando como ejemplo la aplicación para controlar el acceso de los usuarios al CTI, o bien aplicaciones que controlan la distribución de alumnos que toman algún curso sobre un paquete informático y mediante el cual se reserva un espacio para la impartición del mismo; además de los problemas relacionados con la estructura interna de las computadoras, donde las fallas más comunes se deben a descomposturas en componentes, sean por desgaste, largas jornadas de funcionamiento o antigüedad del equipo.

Los objetivos son las metas propuestas que se deben de realizar en un periodo de tiempo necesario con un avance determinado. Es un resultado por alcanzar dentro de un campo específico que no se agota y que le da sentido a la actividad de una persona o de un grupo de personas. Normalmente los objetivos globales de una organización son expresados en términos de

logros en áreas funcionales específicas, y no determinan la información necesaria para lograr esas metas. Los objetivos deberían ser reexaminados y expresados a la luz de la información para su realización. Estos al ser permanentes, facilitan la integración en el tiempo de las diferentes etapas recorridas.

En líneas generales la planificación de los objetivos planteados hacen alusión a un término llamado ***Efectividad Operativa***, significa que debe existir una evolución práctica de los sistemas por parte de los usuarios o empleados que van a manejar dichos sistemas para el cumplimiento de las metas, es decir, la comprobación de que se realizan correctamente y se cumplan los objetivos planteados enfocados a la utilización del sistema.

Por otra parte, la computadora como herramienta de solución para problemas de cálculo de operaciones, investigación de procesos, enseñanza, entre otros, establece las bases para determinar el objetivo de un CTI, como es el de prestar servicios a diferentes áreas dentro de una institución educativa.

1.4 Alcances y ámbito del proyecto

Cuando se pretende cuantificar el alcance de algún proyecto el primer paso a considerar antes de desarrollarlo o resolverlo, es enfocar a los objetivos planteados, ya que desviarse de este contexto sería contraproducente, pues el tiempo que está usando podría utilizarse para resolver otro problema. Se puede afirmar que el CTI reclama que los mecanismos operativos de la organización estén claramente establecidos, a fin de tener seguridad para sus datos y equipo dedicado al procesamiento de los mismos, y seguir estándares y procedimientos, y cuando se dé el caso poder salir avante recuperando todo lo posible en caso de un desastre. Aún así, si estos mecanismos no estuvieran claramente definidos, el CTI debe estar preparado para colaborar a fin de establecerlos. En otras palabras, el **CTI debe predicar la buena administración**.

1.4.1 Etapas de planeación

Con respecto al alcance pretendido en este trabajo de tesis es pertinente tomar consideración en la etapa de planeación en donde se obtiene una visión del futuro, siendo posible determinar y lograr

los objetivos**,** mediante la elección de un curso de acción. Para cumplir con el objetivo planteado, se contemplan cinco niveles de planeación, conformados por:

- Planeación estratégica
- Planeación de recursos
- Planeación operativa
- Planeación de personal
- Planeación de instalaciones físicas

Estas áreas de planeación se describen a continuación:

- **Planeación estratégica:** En todo CTI existen variables para su planeación estratégica y es que debe haber áreas de trabajo para cada una de las funciones que se realizan dentro de las cuales podemos mencionar:

- **Supervisor de red:** Puesto dentro del área que trata de administrar, ejecutar y desarrollar las funciones que tienen que ver con las instalaciones de la red (en este caso una red inalámbrica).

- **Área de análisis:** Aquí se analizan los problemas del entorno para darle una solución sistematizada.

- **Área de captura:** Lugar donde se almacena la información en los equipos de cómputo para su procesamiento.

- **Planeación de recursos:** En esta etapa de la planeación, el jefe, coordinador o administrador del centro de tecnología, organiza los recursos económicos con que se cuenta, es decir, destina la cantidad de recursos necesarios para la subsistencia de cada departamento o área.

- **Planeación operativa:** Es la manera de organizar al personal de acuerdo con sus capacidades y funciones asignadas dentro de su departamento o área.

- **Planeación de personal:** En esta etapa de la planeación, el administrador del CTI debe seleccionar al personal que se requiere para la operación del mismo de acuerdo con su perfil profesional, su preparación y su experiencia en el ámbito laboral.

- **Planeación de instalaciones físicas:** Esta etapa de la planeación se refiere a todo lo que tiene que ver con el equipo requerido y necesario para el CTI.

El considerar una buena y adecuada planeación ahorrará una considerable carga de trabajo que puede ser evitada si se tiene en mente lo que se desea lograr y con que medios se cuenta para alcanzar ese objetivo.

DETERMINACIÓN DE LOS REQUERIMIENTOS PARA EL FUNCIONAMIENTO DEL CTI

2.1 Requerimientos generales

La mejor estrategia consiste siempre en **aprovechar los puntos fuertes** de un lugar para convertirlos así, en **zonas de oportunidad**. Es precisamente desde esta perspectiva donde se debe iniciar cualquier análisis trascendental, sin descuidar, los puntos débiles y las carencias del CTI, ni los problemas y amenazas del entorno.

Para hacer una planeación eficaz, lo primero que se requiere es obtener información general sobre la organización y sobre las funciones a evaluar, como lo son, el tipo de servicio que se proporcionará y los diversos tipos de usuarios que harán uso del lugar; con base en ello se determinarán los requerimientos en cuanto a instalaciones, así como hardware, software y la red inalámbrica. Para ello es preciso hacer una investigación preliminar y de ahí, planear el programa de trabajo, donde se deberá incluir tiempo, costo y personal necesario, así como documentos auxiliares a solicitar o formular durante el desarrollo de la misma.

El primer parámetro que generalmente se considera es el económico, ya que el CTI representa una cuantiosa inversión, dicho desembolso está lejos de ser el problema fundamental. Se trata de una condición previa necesaria, ya que ninguna institución educativa debe montar un sitio de este tipo sin satisfacer las siguientes condiciones:

- Realizar un estudio de factibilidad
- Disponer de los fondos necesarios para la instalación
- Contratar un jefe o director de proyecto

En este caso el director de proyecto debe contar con un buen currículo y dedicarse de tiempo completo a su cometido. Deberá asumir todos los aspectos de elección, planificación e

implementación del equipo central, periféricos elegidos e instalaciones. Tiene también que integrar un equipo coherente y efectivo con el diferente personal que se requiere para diseñar y mantener un CTI.

El administrador del CTI, hasta cierto punto es análogo a un administrador de negocios, pero mientras que en un negocio uno administra para obtener mayor ganancia económica, en este CTI uno administrará para brindar un servicio óptimo y de alta calidad para los usuarios.

El factor humano es fundamental en la creación o modificación de un CTI. Sólo gracias a una estrecha coordinación y colaboración entre todas aquellas personas que intervienen es posible efectuar la compleja planeación requerida.

Una vez cubierto este punto, la instalación física se ajustará a este procedimiento:

- Decidir cuáles serán las funciones que realizará el CTI
- Seleccionar el lugar, ya sea un edificio existente o un lugar donde construir uno
- Planear la distribución de las áreas de trabajo, así como el equipo
- Instalación del equipo
- Configuración de la red inalámbrica
- Puesta en marcha

2.2 Recopilación de información

En lo concerniente a la investigación preliminar para detectar los requerimientos necesarios, se deberá observar el estado general, su situación dentro del área de posgrado, que es donde se encontrará físicamente el lugar, contemplando para ello, que el servicio brindado será tanto para alumnos de licenciatura, como para personas que actualmente se encuentren cursando un posgrado.

Si bien es cierto que cada CTI tiene un mundo propio y particular, se ha tratado de estandarizar ciertos procedimientos y funciones que son aplicables dentro de cualquier lugar de este tipo, por

ello, las decisiones que se tomen con respecto a la correcta administración son una labor del responsable del CTI. La operación del centro se debe llevar a cabo de acuerdo con las funciones vistas en la planeación y éstas a su vez deben ser delegadas por el administrador del lugar.

Las formas de operar y administrar un CTI son consideradas por varios autores como simples restricciones, es decir, el administrador debe decidir (de acuerdo con las jerarquías existentes) quienes tendrán acceso a todo tipo de información o de recursos y quienes no lo tendrán, esto, con respecto a las actividades que realizarán los usuarios dentro del lugar.

2.2.1 Conflictos más comunes para la puesta en marcha de un CTI

Los problemas comunes dentro de un CTI se clasifican en cuatro principales géneros:

- Conflictos de hardware
- Conflictos de software
- Conflictos de recursos humanos
- Conflictos de instalaciones físicas

2.2.1.1 Conflictos de hardware

- **Vandalismo:** Destrucción del equipo por parte de usuarios, principalmente se ha visto que los alumnos de primer ingreso son los que tienden a descuidar un poco más el equipo y no conservarlo en óptimas condiciones.

- **Obsolescencia de equipos:** El acelerado paso en la innovación de los equipos, es de particular importancia para los propietarios de los CTI´s, ya que es necesario estar actualizando tanto el software como el hardware, así también, se necesitan discos duros más veloces y de mayor capacidad, impresoras con mayor nitidez, etc.

- **Consumibles:** La colocación estratégica y el suministro adecuado de los recursos que requieren las computadoras para su funcionamiento, son de vital importancia y se vuelve

un problema -sobre todo de tiempo- cuando no están disponibles en el momento y en el lugar requerido, toner, cartuchos, disquetes, etc.

- **Mantenimiento inadecuado**, deben existir programas de mantenimiento y cumplirse al pie de la letra, ya que el retraso en las actividades de limpieza en los equipos por lo general da como resultado daños en los mismos.

- **Defectos de fabricación** y/o daños físicos que puedan tener los componentes internos tanto de los equipos de cómputo como de los periféricos.

- **Manuales de uso y operación** de los equipos que se encuentren en otro idioma ajeno al que se maneja.

- Cuando se trabaja con una **conexión a red**, es muy común que por falta de conocimiento se den órdenes al sistema que puedan bloquear o provocar una falla, sobre todo para el caso de una red inalámbrica, donde los parámetros de configuración deben de ser los correctos para evitar fallas en la conexión o intrusiones de usuarios no deseados.

2.2.1.2 Conflictos de software

- **Accesos no autorizados:** La información, como recurso valioso de una organización, está expuesta a actos tanto intencionales como accidentales, de violación de su confidencialidad, alteración, borrados y copiado, por lo que se hace necesario que el usuario, propietario de esa información, adopte medidas de protección contra accesos no autorizados.

Las siguientes recomendaciones, ofrecen la posibilidad de habilitar cierto grado de protección con los medios actualmente disponibles.

- **Clave de autorización de encendido:** Este es un recurso de protección disponible en todos los computadores, se habilita al momento de configurar el equipo y es una clave que será solicitada como primer paso de inicialización después de encender el equipo.

- **Copias de respaldo:** Así como se protege la información contra accesos no autorizados y como complemento a las copias periódicas que los administradores realizan sobre la información, ya sea paquetería almacenada en los servidores o inventario de los equipos y periféricos, es también importante mantener en un lugar seguro y externo al sitio de trabajo, con el fin de garantizar la oportuna recuperación de datos y programas en caso de perdidas o daños en las computadoras.

- **Protección contra virus:** Dentro de la infinidad de virus detectados en el mundo entero y fácilmente reproducidos por el uso y copia de software "pirata", utilización de disquetes ya "infectados" o vía E-Mail.

- Algunas **órdenes, comandos u operaciones** son muy complejos y puede producir que al darlas de manera equivoca bloquee el equipo.

- El conflicto principal y más común que puede ser causa de otros a su vez es la **falta de experiencia** y la ignorancia en el manejo del equipo de cómputo.

2.2.1.3 Conflictos de recursos humanos

El principal factor que provoca ineficiencia proviene de **una mala administración** del CTI, en otras palabras, los administradores no tienen una formación adecuada para mantener en óptimas condiciones el flujo de las actividades llevadas a cabo.

Básicamente en este rubro se hace referencia a los problemas que se generan por carecer de programas de capacitación adecuados para el personal que labora en el centro, el abandono de empleo y la falta de una adecuada supervisión de las actividades desarrolladas por el personal.

Todos estos factores influyen notablemente en la productividad de un CTI y las soluciones a los mismos pueden concretarse por simple deducción. Aunque en menor escala -no por ello debe olvidarse- la sustracción no autorizada de dispositivos ya sean periféricos o partes de la máquina.

2.2.1.4 Conflictos en torno a las instalaciones físicas

Dentro de este punto se contempla y realiza un análisis de riesgos, en donde se identifican, evalúan y seleccionan los posibles riesgos a ser controlados dentro del entorno de un CTI.

Categorías de riesgos:

- **Desastres naturales:** Inundaciones, temblores, tormentas eléctricas, entre otros
- **Accidentes:** Descuidos, falta de prevención, falta de precaución, entre otros
- **Vandalismo:** Destrucción en contra del CTI afectando, instalaciones, equipo, programas, datos, documentación
- **Robo:** De información, de equipo, de periféricos
- Guías para el **control de errores**
- Asignación de **personal responsable**
- Definir **estándares y procedimientos** en medidas de seguridad y prevención de accidentes
- **Objetivo de cada paso** o procedimiento descritos en el punto anterior
- Establecer **restricciones** para los diversos grupos de usuarios que harán uso de las instalaciones, tanto personal interno como usuarios externos

2.3 Análisis de requerimientos sobre instalaciones

Posiblemente una decisión tan crucial como la **selección de equipo**, es la elección del **lugar dónde se va a instalar físicamente el CTI**, una elección equivocada de este punto será muy difícil remediar, por lo mismo debe tenerse especial cuidado al elegir. Existen diversos parámetros a analizar con respecto a la selección del local y las instalaciones, entre las que se mencionan:

2.3.1 Selección del edificio

- Las normas de construcción y planos de remodelación que afecten al inmueble.

- Se deben estudiar las características arquitectónicas del edificio
- Tener una buena accesibilidad del lugar
- Disponibilidad y requerimientos de la fuerza eléctrica adecuada
- Espacio para el equipo de aire acondicionado
- Normas de seguridad y protección contra incendios
- Facilidad de comunicación interior y exterior con los restantes servicios del edificio

2.3.2 Ubicación física

El lugar donde debe estar ubicado el CTI debe de cumplir una serie de requisitos de entre los cuales podemos mencionar a los siguientes:

- Estar situado en un lugar donde no pueda acceder personal no autorizado
- Acondicionado para que no entre mucha luz natural
- Debe haber aire acondicionado
- No debe haber entradas de aire natural
- Extintores
- Ruta de evacuación
- Prever una salida de emergencia

2.3.3 Equipo contra incendios

Situación en el área del equipo de cómputo:

- El área del equipo de cómputo debe estar en un edificio o habitación que sea resistente al fuego.
- El lugar deberá contar con puertas de emergencia.
- La sala donde se encuentre el equipo de cómputo no debe situarse encima, debajo o adyacente a un área donde se procesen, fabriquen o almacenen materiales flamables o peligrosos.

2.3.4 Seguridad en la estructura del edificio

- Las paredes del CTI deben ser de material incombustible. Si el área del equipo tiene una o más paredes exteriores adyacentes a un edificio que sea susceptible de incendio, la instalación de ventanas irrompibles mejorará la seguridad del personal y del equipo contra los escombros y el agua.

- Todas las canalizaciones y materiales aislantes deben ser de materiales incombustibles y que no desprendan polvo.

- Debe existir señalizaciones adecuadas en cuanto a la ubicación de los equipos contra incendios, así como una guía rápida sobre su correcto funcionamiento en caso de un incendio.

- Dentro de las instalaciones se debe contar con avisos o guías qué expliquen que hacer en caso de incendios o sismos, con todas las instrucciones necesarias para la evacuación y salvaguarda de las personas y las instalaciones.

2.3.5 Instalación eléctrica

- Con el proveedor del equipo de cómputo se comprobarán los voltajes de trabajo del mismo equipo.

- La tolerancia en tensión no deberá ser mayor de 10 % ni menor de 8 % de la tensión nominal que especifique el fabricante del equipo de cómputo.

- Habrá una red de enchufes o contactos auxiliares monofásicos a 117 [V] distribuidos a lo largo de la sala, preferentemente sacados de otra alimentación eléctrica, diferente de la del equipo de cómputo.

- Es indispensable que la alimentación a los equipos de cómputo sea mediante energía eléctrica regulada; para ello, y dependiendo de las condiciones, deberá considerarse:

- A través de un sistema de energía ininterrumpible, respaldado por un tablero de control.

- A través de un regulador de voltaje, el cual puede tener dispositivos que eliminen ciertas armónicas perjudiciales al equipo de cómputo.

- Para equipos de cómputo pequeños, como PC´s, a través de un multicontacto que permita eliminar armónicas y conectado a un regulador de voltaje individual o de mayor capacidad o conectado a un equipo no-break con regulador de voltaje.

2.3.6 Iluminación

La iluminación dentro del lugar ya sea natural o artificial es importante y deben mantenerse controladas, para ello, es necesario contar con persianas plegables y corredizas de manera que, cuando los ventanales permanezcan abiertos, éstas puedan correrse para permitir la entrada de aire pero cuando la luz solar penetre directamente éstas puedan cerrarse. En cuanto a la luz artificial, en el área debe mantenerse un promedio mínimo de 450 [luxes] a 70 [cm] del suelo. La iluminación no se alimentará de la misma acometida que el equipo eléctrico.

2.3.7 Aire acondicionado

En un lugar donde existe una cantidad considerable de equipos de cómputo, es común que exista un control de la temperatura ambiental, debido a que tanto los equipos como las personas irradian calor, por consiguiente deben contemplarse los siguientes elementos concernientes al aire acondicionado del lugar:

- Disipación térmica de las máquinas
- Disipación térmica de las personas
- Aire de renovación
- Pérdidas por puertas y ventanas
- Transmisión de paredes, suelos y techos
- Disipación de otros aparatos

- Las cargas caloríficas del equipo de cómputo y sus periféricos las proporcionará el proveedor, por lo común deben especificarse en [BTU/hr] o en [Kcal/hr].
- El proveedor del equipo también proporcionará la cantidad de aire que requieren los ventiladores de los diferentes dispositivos de cómputo.

2.4 Análisis de requerimientos de hardware y software

Los criterios para seleccionar software se componen en dos niveles principales:

- **Básico:** Sistema Operativo (seleccionar por estándar mundial)
- **Soporte:** Base de datos (seleccionar por estándar mundial)
- **Proveedor:** Las características que debe tener el proveedor de informática son:
  - Reconocido prestigio mundial y nacional
  - Soporte técnico en instalación
  - Ayuda en problemas y tiempo de atención
  - Personal especializado
  - Comunicación rápida
  - Servicios de capacitación: cursos, material, expositor, costos
  - Documentación: facilidad de uso
- **Costos:** Se considerará lo siguiente:
  - Condición de pago
  - Local
  - Inclusión de entrenamiento
  - Costos de mantenimiento

Los criterios para la selección de hardware son con respecto a:

- **Equipos:**
  - La configuración debe ser acorde a la carga de procesamiento de los datos

  - Debe tener una capacidad de crecimiento vertical (en el mismo equipo) y horizontal (con otros equipos)
  - Fabricante de calidad reconocido con prestigio mundial
  - Tiempo de garantía
  - Tecnología de "punta"

- **Proveedor:** Debe tener las siguientes características:
  - Reconocido prestigio local
  - Soporte de mantenimiento: personal especializado, stock de repuestos
  - Tiempo de atención, local apropiado, comunicación rápida
  - Cartera de clientes con equipos equivalentes a los adquiridos
  - Tiempo de entrega oportuno

- **Precios:** Se debe considerar lo siguiente:
  - Condiciones de pago
  - Detallado por componentes de la configuración
  - Descuentos por volumen
  - Costo de mantenimiento

2.4.1 Adquisición de software

El software para computadoras se puede clasificar en los siguientes tipos:

- **Paquete de sistemas aplicativos:** En los que a diferencia de los paquetes de usuario final, el usuario es simplemente quien los usa. La programación y el desarrollo son etapas complejas, realizadas por el Departamento de Sistemas del la Unidad de Servicios de Cómputo Académico (UNICA), por ejemplo, el Sistema de Control de Inventarios (SICI), Sistema de Evaluación de Cursos de Computación (SECC), Sistema de Control de Salas de UNICA (SCOSU), etc.
- **Sistema operacional:** Es el conjunto de programas que controla las actividades operativas de cada computadora y de la red.

- **Paquete de usuario final:** Mediante los cuales el usuario de una manera sencilla elabora sus procesos, por ejemplo, hojas de cálculo, manejadores de bases de datos, procesadores de palabras, etc.

- **Software autorizado:** Se considera como software autorizado, tanto a los sistemas operacionales como aquellos paquetes de usuario final y de sistemas aplicativos, que el administrador de sistemas ha instalado, previo visto bueno para su adquisición y con la autorización legal del proveedor para su uso.

2.4.2 Adquisición de hardware

El proceso de selección del hardware está diseñado de manera tal que, la adquisición del mismo sea una acción fácil de realizar y consta de los mismos pasos que el proceso de selección del software. La selección del modelo y capacidades del hardware requerido, debe ir de acuerdo con el plan estratégico de sistemas y sustentado por un estudio elaborado por el área directiva, en el que se enfatizan las características y volumen de información que ameritan sistematización y diferencian los tipos de equipos que se adjudican a las diversas áreas usuarias.

Todo estudio determina una configuración mínima para las computadoras y los aditamentos o dispositivos electrónicos anexos como unidades externas, impresoras, elementos de red (alámbricos e inalámbricos) para comunicaciones, de acuerdo con las necesidades del usuario, así como una evaluación del costo aproximado de la inversión.

2.4.3 Consideraciones generales para la adquisición de software y hardware

Para realizar cualquier adquisición de Software o Hardware, se deberán considerar los siguientes puntos:

- **Solicitud de propuesta.** Todo sistema se origina con base en una solicitud que hace el usuario al CTI, intentando satisfacer una necesidad específica.

- Los **parámetros** sobre los que debe medirse dicha solicitud son los objetivos y las políticas de uso, los cuales debe fijar el usuario, aunque puede ser que el administrador del CTI le brinde ayuda en su clarificación. Ambos parámetros deben quedar establecidos por escrito.

- **Evaluación de propuesta**. Previamente debe llevarse a cabo una investigación con el propósito de establecer con seguridad el tipo de software y hardware requerido para su implementación, posteriormente se integra toda la información obtenida de dicha investigación, y así poder establecer la operatividad de los sistemas a adquirirse.

- **Financiamiento.** Las fuentes de financiamiento pueden ser principalmente instituciones bancarias a través de créditos. Para el caso de centros de cómputo destinados a la educación pública no existen fuentes de financiamiento, a menos que la institución educativa cuente con un área destinada a la producción de software para empresas privadas, entonces la misma empresa puede ser el origen del financiamiento.

- **Negociación de Contrato.** La negociación de contrato debe incluir todos los aspectos de operación del software y del hardware a implementarse. Aspectos tales como: actualizaciones, innovaciones, capacitación, asesoría técnica, etc.

2.4.4 Elementos que intervienen en la solicitud de software y hardware

La solicitud de propuesta deberá realizarse mediante las requisiciones que deberán incluir:

- Información general
- Objetivo
- Propósito
- Fecha límite de entrega
- Fecha límite de aclaraciones
- Cobertura de requerimientos
  - Mínimos
  - Deseables

- Solicitud de descripción detallada del producto o servicio
- Solicitar especificaciones detalladas de servicios de soporte de usuario

Evaluación de propuesta:

Para llevar a cabo una buena evaluación de las propuestas presentadas deberán tomarse en cuenta los siguientes términos:

- Verificar lo que ofrece el proveedor (credibilidad de propuesta)
- Analizar propuesta
- Costo
- Disponibilidad
- Calidad de diseño
- Soporte y mantenimiento
- Expansión
- Configuración
- Ambiente de software
- Documentación

Y posteriormente se deberá verificar con terceros la información sobre los productos o servicios ofrecidos por el proveedor.

Negociación de contrato con el proveedor

La negociación del contrato deberá contemplar entre otros los siguientes puntos:

- Obtener un contrato justo
- Puntos de negociación
- Precios
- Costo
- Capacitación
- Penalizaciones
- Posibles problemas que se puedan presentar
- Contrato a favor del proveedor

- Vendedor profesional, comprador amateur o principiante
- Convenios no incorporados en cláusulas
- Ausencia de penalizaciones
- Cláusulas integradoras (dejar sin validez cualquier acuerdo previo)

2.5 Identificación de usuarios del CTI

Al ponerse en marcha el CTI se tienen contemplados dos grupos principales de usuarios, el primero, alumnos que cursan alguna de las 12 licenciaturas en la Facultad de Ingeniería, esto, sin importar el semestre que actualmente estén cursando; el segundo, para alumnos de la Facultad que se encuentren estudiando un posgrado.

Eventualmente se lleva a cabo un programa de intercambio académico entre la Universidad Nacional Autónoma de México y universidades de otros países. La Facultad de Ingeniería tiene contemplado este programa, por tal motivo, los alumnos provenientes de universidades en el extranjero podrán hacer uso de los equipos e instalaciones del CTI, previa entrevista con el administrador para que éste les explique el reglamento vigente dentro del lugar, así como para expedirles un comprobante, con el qué podrán acceder al CTI.

SELECCIÓN DEL EQUIPO DE CÓMPUTO

3.1 Características acordes a los tipos de usuarios

En función de los tipos de usuarios especificados en el capítulo anterior, a quienes se les brindará el servicio, se definirán ciertos parámetros que servirán para determinar las características más adecuadas y acordes con respecto a los mismos.

Un punto importante a considerar al momento de implementar un CTI enfocado al área académica es de los usuarios, debido a que el servicio está encaminado hacia ellos, por tal motivo es imprescindible planear que tipo de personas harán uso de las instalaciones.

Dado que los usuarios son alumnos de la Facultad de Ingeniería, tanto de **licenciatura**, como aquellos que cursan un **posgrado**, la paquetería que se instalará, así como el tipo de equipos deben estar en función con los requerimientos y exigencias de los mismos.

3.2 Elementos que intervienen en la selección del equipo de cómputo

El problema al momento de elegir el equipo de cómputo para el CTI tiene contrastes muy subjetivos, a fin de poder realizar una selección lo más objetiva posible, hay que seguir una secuencia de parámetros que nos llevarán a una selección mucho más adecuada. Tales parámetros a considerar son los siguientes:

3.2.1 Factores financieros

- **Precio de compra:** Como ventaja se puede pagar a crédito, en pagos predeterminados en períodos fijos, no necesariamente se tienen que efectuar pagos elevados y se puede disponer del equipo a la hora que se quiera. Como desventaja es una decisión irrevocable, se requiere capital inicial mayor, así como el riesgo a la obsolescencia.

- **Precio de alquiler:** Las ventajas son que tenemos un alto nivel de flexibilidad, no se requieren pagos altos y elevados, y a corto plazo es más económico alquilar que comprar. Como desventajas, a la larga puede resultar más costoso que comprar el equipo y además podemos tener limitaciones en cuanto a uso, éste es un aspecto muy poco utilizado, ya que el equipo no suele alquilarse, debido a las condiciones del lugar.

- **Precio de renta con opción a compra:** Modalidad similar a la manejada en el punto anterior, en este caso el equipo se adquiere a renta, pero con el objetivo de comprarse en un futuro.

- **Depreciación prevista del equipo por obsolescencia:** Siempre hay que tener en cuenta que el equipo se vuelve obsoleto, por tanto va perdiendo su valor monetario.

3.2.2 Determinación del tamaño y requerimientos de capacidad

La velocidad de procesamiento, así como el espacio de almacenamiento estarán en función de la software requerido a instalar, ya que dependiendo de los programas que se usarán se ocupará espacio en disco duro y recursos del sistema para ejecutarlos.

3.2.3 Evaluación y medición de la computadora

Es común que se efectúen comparaciones entre los diferentes sistemas de cómputo basándose en el **desarrollo y desempeño real de los datos que operan**, así como de los procesos que ejecutan, estas evaluaciones ayudan a elegir el equipo más eficiente y óptimo de acuerdo con dos factores muy importantes:

- El valor de compra del equipo en función de las innovaciones tecnológicas que posea
- Aquel que ofrezca el mejor rendimiento de acuerdo con uso que se le dé

3.2.4 Compatibilidad

Por cuestiones económicas se considera factible la compra de equipo llamado **compatible**. La ventaja de este equipo es un menor costo que el original, pero debe tenerse cuidado con los siguientes puntos:

- Nivel de calidad
- Desempeño igual al original
- Garantías y acuerdos de servicio

3.2.5 Mantenimiento y soporte técnico

- **Fuente de mantenimiento:** Una vez que el sistema se ha entregado e instalado, existe un período de garantía en el que la unidad de ventas que efectuó la operación tiene la responsabilidad del mantenimiento, después de este tiempo el comprador puede adquirir mantenimiento de varias fuentes.

- **Términos de mantenimiento:** El contrato puede redactarse de manera tal que, cubra tanto la mano de obra como las piezas que se hayan necesitado en el mantenimiento, o bien mano de obra y piezas por separado.

- **Servicio y respuesta:** El apoyo de mantenimiento es útil si se encuentra disponible cuando se requiere. Dos puntos de interés son el tiempo de respuesta y las horas en las que se puede obtener el apoyo.

Existen muchas opciones que pueden elegirse al realizar una compra pero siempre debe considerarse en cuestión de elementos internos de los equipos de cómputo lo siguiente:

- Tamaño interno de la memoria y velocidad de procesamiento
- Tipos y números de dispositivos de almacenamiento
- Software que se proporciona en conjunto con los sistemas desarrollados disponibles

3.2.6 Apoyos del proveedor

- Frecuencia del mantenimiento
- Servicios que se incluyen en el pago
- Saber si se incrementa el costo del mantenimiento
- Horarios disponibles de servicio
- Saber si tienen servicio de emergencia

3.3 Descripción de los equipos de escritorio (desktop)

Los equipos desktop a adquirir para el CTI son de la marca ***Dell***, específicamente de la serie ***OptiPlex,*** (véase figura 3.1 y 3.2), estos equipos están diseñados para instituciones educativas que necesitan sistemas estables, de fácil mantenimiento, administración y altamente confiables en ambientes de red. Accesible e ideal para las necesidades de computo básicas. Con las características de un sistema de este tipo, el soporte y servicio que *Dell* ofrece, la ***Dell OptiPlex GX270*** es el sistema que ofrece el mayor valor en su clase, es ideal para la gente que busca un balance entre un precio accesible, desempeño y expansibilidad básica.

Figura 3.1 Vista frontal equipo Dell OptiPlex GX 270

Figura 3.2 Vista trasera equipo Dell OptiPlex GX 270

Las características de los equipos *Dell OptiPlex GX270* se enlistan a continuación:

Sistema:

Sistema operativo	Microsoft Windows XP Professional
Service Pack del Sistema Operativo	Service Pack 2
Internet Explorer	6.0.2900.2180

Placa base:

Tipo de procesador	Intel Pentium 4A, 2800 MHz (3.5 x 800)
Nombre de la Placa Base	Dell Computer Corporation OptiPlex GX270
Chipset de la Placa Base	Intel Springdale-G i865G
Memoria del Sistema	256 MB (DDR SDRAM)
Tipo de BIOS	Phoenix (05/17/04)
Puerto de comunicación	Puerto de comunicaciones (COM1)
Puerto de comunicación	Puerto de impresora ECP (LPT1)

Monitor:

Tarjeta gráfica	Intel(R) 82865G Graphics Controller (64 MB)
Acelerador 3D	Intel Extreme Graphics 2
Monitor	
	Monitor Plug and Play [NoDB] (X378244JB52F)

Multimedia:

Tarjeta de sonido	Intel 82801EB ICH5 - AC'97 Audio Controller

Almacenamiento:

Disquetera de 3 1/2	Unidad de disquete
Disco duro	ST340014A (40 GB, 7200 RPM, Ultra-ATA/100)
Lector óptico	HL-DT-ST CD-RW GCE-8483B

Dispositivos de entrada:

Teclado	Teclado estándar de 101/102 teclas PS/2 Keyboard
Ratón	Mouse compatible PS/2

Red:

Tarjeta de Red Alámbrica	Intel(R) PRO/1000 MT Network Connection
Tarjeta de Red Inalámbrica	3COM 3CRDAG75 Wireless LAN PCI adapter

Dispositivos:

Dispositivos USB	Dispositivo de almacenamiento masivo USB

Garantía:

Estándar: 1 año de partes en sitio, 1 año de mano de obra, 1 año soporte técnico
Opcional: 2 años de partes en sitio, 2 años de mano de obra, 2 años soporte técnico
Opcional: 3 años de partes en sitio, mano de obra y soporte técnico por el término de su garantía

Para la configuración antes mencionada, el costo aproximado del equipo asciende a **$ 7,829.51**, éste es el precio que brinda el distribuidor autorizado Dell, el precio está dado en pesos mexicanos, con la característica de que incluye el flete de transportación así como los impuestos de importación; este costo no incluye el 15% de IVA.

Figura. 3.3 Vista interna equipo Dell OptiPlex GX 270

3.4 Descripción del servidor

En cuanto al tipo de servidor que se manejará en el CTI, se tiene pensado el modelo ***PowerEdge 420SC***, igualmente de la compañía *Dell (véase figura 3.4)*, este equipo es ideal para empresas y centros pequeños que necesitan pasar de un software de servidor en una PC a un servidor accesible para tareas en general.

El servidor ofrece un bus de 800 Mhz e incluye una memoria que corrige errores de bit simples para alta disponibilidad de los datos, una ventaja importante para una PC que utiliza software de servidor. Además, el servidor *PowerEdge* aborda aquellos temas sobre la disponibilidad con RAID (arreglo redundante de discos independientes) basado en software y diagnóstico en línea.

El equipo está diseñado para ofrecer a entornos pequeños las capacidades de servidor que se necesitan hoy en día, así como la flexibilidad de expandirse a medida que el lugar que administra crezca, sin invertir más dinero en las funciones que se necesitan.

Las características del equipo PowerEdge 420SC se enlistan a continuación:

Placa base:

Procesador	Intel Pentium 4 de hasta 3,6 GHz
Bus frontal	533 MHz o 800 MHz
Caché	Hasta 1 MB L2
Chipset	Intel E7221
Memoria	256 MB / 4 GB ECC DDR2
Disponibilidad Memoria	ECC; RAID de software; unidad de cinta (opcional)

Sistema:

Administración de sistemas	Asistente de servidor de Dell para servidores PowerEdge SC
Sistemas operativos	Microsoft Windows Server 2003; Microsoft Windows Small Business Server 2003; Red Hat Linux ES 3.0

Almacenamiento:

Almacenamiento interno máximo	Hasta 292 GB SCSI o hasta 500 GB SATA
Unidades de disco rígido	36 GB, 73 GB y 146 GB Ultra 320 SCSI con controlador PCI opcional (o) 40 GB, 80 GB, 160 GB y 250 GB SATA
Rendimiento de almacenamiento interno	Unidades de 10K RPM SCSI; unidades de 7.2K RPM SATA
Unidades de disco	Unidades SATA o SCSI de 2 x 1”; sin conexión en caliente
	Soporte de cinta Unidad de copia de seguridad de cinta Travan TR-40 (opcional)

Dispositivos de E/S:

Canales de E/S	Cinco en total: dos ranuras PCI ExpressTM (conector de 1 x 8 y conector de 1 x 1); tres ranuras PCI (32-bit / 33 MHz)
Controlador de unidad	Canal doble incorporado SATA; Ultra320 SCSI (opcional) Controlador RAID CERC SATA 2s, RAID de software 1 SCSI

Red:

Tarjeta de interfaz de red Incorporado simple Gigabit NIC

Figura 3.4 Vista frontal Servidor Dell PowerEdge 420SC

Para la configuración antes mencionada, el costo aproximado del equipo asciende a **$ 27,973.47**, éste es el precio que brinda el distribuidor autorizado Dell, el precio está dado en pesos mexicanos, con la característica de que incluye el flete de transportación, así como los impuestos de importación; este costo no incluye el 15% de IVA.

3.5 Descripción del servidor de impresión

Dentro del CTI está contemplado un servidor de impresión, este equipo cuenta con las mismas características de configuración que los equipos de escritorio ya descritos; debido a las condiciones de uso del equipo, los usuarios no pueden realizar alguna actividad diferente a la de impresión de sus trabajos, la paquetería instalada en este equipo es la misma que la instalada en los equipos de escritorio (desktop).

Para el caso de la impresora, se prevé contar con un equipo **HP LaserJet modelo 4050,** (véase figura 3.5) fácil de usar y de gran rendimiento, que permita trabajar a una velocidad de impresión considerable, debido al número elevado de usuarios que atenderá y que contará con las características siguientes:

Velocidad de impresión:

Negro, calidad de borrador, A4: 43 ppm
Negro, calidad normal, A4: Hasta 33 ppm
Negro, calidad óptima, A4: Hasta 20 ppm

Velocidad del procesador:

460 MHz

Tecnología de impresión:

Láser monocromo

Calidad de impresión (negro, calidad óptima):

Hasta 1.200 x 1.200 ppp

Capacidad:

De entrada estándar	Hasta 600 páginas
Máxima de entrada	Hasta 3.100 páginas
De salida de serie	Hasta 300: 250 boca abajo y 50 boca arriba

Opciones de impresión a doble cara:

Automática (opcional)

Memoria estándar:

48 MB

Ranuras de memoria:

Dos ranuras DIMM DDR de 100 conectores

Tipos de letra:

80 juegos de tipos de letra HP (además de griego, hebreo, cirílico y árabe)

Lenguajes de impresora estándar:

HP PCL 6
HP PCL 5e
Emulación HP Postscript nivel 3
PDF 1.3

Conectividad estándar:

Puerto paralelo homologado IEEE 1284 B
2 ranuras, 1 puerto Hi Speed USB (compatible con las especificaciones USB 2.0)

Sistemas operativos de red compatibles:

Microsoft Windows 98, Me, NT 4.0, 2000, XP, XP de 64 bits, Server 2003
Novell NetWare 3.2, 4.2, 5.x, 6.x
Apple Mac OS 8.6 y posteriores
Red Hat Linux 6.x, SuSE Linux 6.x y posteriores
Solaris 2.5 y posteriores
IBM AIX 3.2.5 y posteriores

Requisitos mínimos del sistema:

Windows 98: procesador 33Mhz, 16 MB de RAM, unidad de CD ROM
Windows Me: procesador 66 Mhz, 32 MB de RAM, unidad de CD ROM
Windows NT 4.0: procesador 66 Mhz, 32 MB de RAM, unidad de CD ROM
Windows 2000: procesador a 133 MHz, 64 MB de RAM, unidad de CD ROM
Windows XP: procesador a 233 MHz, 64 MB de RAM, unidad de CD ROM
Windows Server 2003: procesador a 550 MHz, 128 MB de RAM, unidad de CD ROM o conexión a Internet, puerto paralelo bidireccional homologado IEEE 1284, USB 1.1, USB (compatible con las especificaciones 2.0)

Garantía:

1 año a domicilio.
Servicios HP Care Pack opcionales disponibles

El costo de la impresora asciende a **$ 6,700.00** pesos mexicanos, de acuerdo con la tabla de precios del distribuidor HP.

Figura. 3.5 Impresora Láser jet HP 4050

3.6 Descripción de las tarjetas de red inalámbricas

Con los nuevos estándares en la industria, mayores tarifas de rendimiento de procesamiento, y las continuas bajas de costos, se ha vuelto más fácil justificar implementaciones de tecnología de red inalámbrica. El caso de negocio para implementaciones de redes inalámbricas depende de la aplicación específica para la cual se implementa. En algunos casos, puede verse un claro valor monetario al adoptar redes inalámbricas. En otros, los beneficios son más cualitativos.

Al contar con una red inalámbrica, los equipos de cómputo poseerán independientemente de la tarjeta de red convencional, una tarjeta de red inalámbrica, para ello se pensó en que el proveedor tanto del Punto de Acceso como de las tarjetas fuera **3COM**, debido al prestigio y seguridad que ofrece la marca con respecto a estos componentes.

Con respecto a la tarjeta inalámbrica, este modelo (**3Com Wireless 11a/b/g PCI Adapter**) ofrece una completa cobertura inalámbrica efectiva, (véase figura 3.6) soporta los tres estándares de **IEEE 802.11** existentes **- 11a, 11b, y 11g -** por lo que los usuarios se pueden conectar a cualquier red inalámbrica **Wi-Fi** [1].

[1] Wireless Fidelity

El control de acceso de red IEEE 802.1x, así como su autenticación, soportan las últimas y más efectivas técnicas para deshacerse de los intrusos y simplificar así, la administración de red.

La encriptación **WPA** [2] y **AES** [3] de 128 bits, y la encriptación **WEP** [4] por clave compartida de 40/64, 128, y 152 bits (para clientes legacy) ayudan a mantener la privacidad de las transmisiones inalámbricas.

Los usuarios de computadoras de escritorio pueden acceder a los recursos de la red, a Internet, y al correo electrónico a velocidades de hasta 54 Mbps o 108 Mbps en modo turbo, lo que resulta ideal para aplicaciones multimedia.

En tanto que la certificación Wi-Fi, ayuda a garantizar la interoperabilidad con los productos de otros fabricantes con certificación WiFi. La tarjeta inalámbrica PCI Adapter, soporta la encriptación WPA, AES, y WEP para proteger los datos inalámbricos. La autenticación MD5, 802.1x, y EAP protege contra los accesos no autorizados a la red.

El costo de las tarjetas de red inalámbricas es de **$ 1,003.21** pesos mexicanos, precio unitario más IVA, establecido por el distribuidor 3COM.

Figura 3.6 Tarjeta de red inalámbrica 3Com 11a/b/g Wireless PCI Adapter

[2] Wi-Fi Protected Access
[3] Advanced Encryption Standard
[4] Wireless Equivalent Privacy

3.7 Descripción del punto de acceso

En un panorama general, dentro de una configuración típica de **LAN** [5] sin cableado, los puntos de acceso (transceiver) conectan la red cableada de un lugar fijo mediante cableado normalizado. EL punto de acceso recibe la información, la almacena y transmite entre la **WLAN** [6] y la LAN cableada.

Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos. El punto de acceso (o la antena conectada al punto de acceso) es normalmente colocado en alto, pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

Las características del punto de acceso modelo **3COM Wireless LAN Access Point 8750** requerido son las siguientes:

- Soporta hasta **253 usuarios simultáneos** a velocidades de hasta **54 Mbps** y distancias de hasta 100 [m] radiales (328 [ft]).

- **Clear Channel Select** escoge el canal menos traficado para brindar conexiones sin problemas.

- La conexión automática a la red y los cambios dinámicos de velocidad hacen que las conexiones a la red estén continuamente disponibles modificando las velocidades de conexión automáticamente, a medida que las condiciones cambian y los usuarios móviles se desplazan a través del área de cobertura de la red.

- El punto de acceso recibe corriente por medio de **cables Ethernet** existentes, resultando en instalaciones más simples y flexibles, no se requiere un suministro de potencia adicional.

[5] Local Area Network
[6] Wireless Local Area Network

- Una antena de radio diversa provee rendimiento y cobertura excelentes en ambientes de altas trayectorias múltiples tales como oficinas, bodegas y otras instalaciones internas.

- Las opciones de antenas externas extienden el alcance de la conexión inalámbrica 802.11g a hasta **305 metros** (1,000 pies).

- Se distribuye como punto de acceso 802.11g a 2.4 GHz de una sola modalidad de **54 Mbps** con una ranura abierta de radio intercambiable.

- Soporta a usuarios inalámbricos **11g** y **11b**, preservando sus inversiones inalámbricas existentes.

- La encriptación **WEP de clave compartida** de 40/64 bits y 128/54 bits, y la **encriptación avanzada WPA** AES de 256 bits, asegura la privacidad de todas las transmisiones inalámbricas.

- El enlace dinámico de seguridad automáticamente asigna claves de encriptación específicas para cada usuario de 128 bits en las sesiones inalámbricas.

- Las listas de control de acceso de direcciones **MAC**[7]**,** controlan el acceso a los recursos de la red.

- Las funciones de filtración "cliente a cliente" y de uplinks (clientes externos) dirigen las comunicaciones entre otros usuarios inalámbricos asociados a los puntos de acceso.

- Las herramientas Wireless Infrastructure Device Manager (Gerente Inalámbrico de Infraestructura de Dispositivos) y Wireless LAN Device Discovery (Descubrimiento de Dispositivos en LAN´s Inalámbricas) permiten configurar parámetros, ejecutar diagnósticos y supervisar el rendimiento desde cualquier punto en la red, usando un navegador Web.

[7] Dirección de control de acceso al medio. Es una dirección asociada con un dispositivo de red en partícular.

Especificaciones del producto:

Usuarios Soportados:

Hasta 253 usuarios simultáneos

Cumplimiento con estándares:

Certificación Wi Fi, IEEE 802.11g, IEEE 802.11a (con kit de actualización)

Velocidades de datos:

54, 48, 36, 24, 18, 11, 9, 5.5, 2, 1 Mbps

Banda de frecuencia:

2.4 GHz

Medio inalámbrico:

Codificación para proveer compatibilidad con el estándar 802.11b

Protocolo de Acceso de Medios:

CSMA/CA

Alcance operativo:

Hasta 100 metros (328 pies) de transmisión y recepción

Configuraciones de potencia de transmisión:

17 [dBm] dependiendo de la velocidad en bits

Consumo:

7,1W de media, 8,4W máximo

Sensibilidad de recepción:

1 Mbps: -96 dBm 2 Mbps: -94 dBm 5.5 Mbps: -92 dBm 11 Mbps: -88 dBm 12 Mbps: -86 dBm 24 Mbps: -85 dBm 36 Mbps: -80 dBm 54 Mbps: -73 dBm

Seguridad:

Encriptación WEP de 40/64 y 128/154 bits
Encriptación WPA AES de 256 bits
Autentificación EAP-MD5, EAP-TLS, EAP-TTLS y PEAP
ESSID broadcast control, autentificación MAC local
Asignación dinámica VLAN, filtración cliente a cliente y uplink

Alcance de operación ambiental:

Temperatura de operación: 0°C a 40°C (32°F a 105°F); Humedad: 5-95% no-condensación

Requisitos del sistema:

Para ejecutar las aplicaciones de administración, se necesita una computadora con CD-ROM que opere con Windows XP/2000/Me/98/95b+/NT 4.0/Linux/Open Bsd

El costo aproximado del Punto de Acceso (véase figura 3.7) es de **$ 5,057.00** pesos mexicanos más IVA, establecido por el distribuidor 3COM.

Figura 3.7 Punto de Acceso 3Com Wireless LAN Access Point 8750

3.8 Tecnologías de vanguardia

En el amplio campo de la informática, los avances tecnológicos se desarrollan con una velocidad impresionante, día con día estos avances nos sorprenden con nuevas tecnologías, capaces de superar en algún aspecto a sus antecesores mediante desarrollos más potentes, mucho más óptimos o desarrollados a un costo menor, éstos, son algunos de los avances más significativos en cuanto a equipos de cómputo y tecnologías informáticas se refiere:

3.8.1 Procesadores que van desde los Mega Hertz a los Giga Hertz

La compañía **Intel** ha mostrado por primera vez en mucho tiempo muestras de flaqueza al desechar oficialmente el lanzamiento de un microprocesador a 4 Ghz. No sucedía nada similar desde el histórico Athlon a 1 Ghz le ganó la batalla a su competidor de entonces, el Pentium III, un hecho que, sin duda, marcó un antes y después en esta batalla por el CPU más veloz.

Pocos días después del sorprendente anuncio por parte de los responsables de esta plataforma,

AMD lanzaba sus últimos productos estrella: el Athlón 64 FX-55 y el Athlon 64 4000+. Mientras que el primero alcanza los 2.6 Ghz. de frecuencia real, el segundo es, en realidad un FX-53 (2.4 Ghz.) al que se le han aplicado algunas limitaciones.

Puede que la batalla por los megahertz se halla acabado, máxime cuando las metodologías para la nomenclatura de los microprocesadores cada vez son más extrañas (como el nuevo modelo seguido por Intel con su empaquetado LGA775).

Las tecnologías de fabricación, la densidad de integración, la potencia disipada y la comunicación con otros componentes suponen cada vez un handicap más serio para los grandes de este mercado. Sin embargo, ya se está investigando en las tecnologías de 0.65 micras (65 nanómetros), y el margen de actuación que aún tienen las plataformas de 64 bits, con la compañía AMD al frente.

3.8.2 Equipos con una misma característica, un Giga Byte en memoria RAM

Analizando algunas de las computadoras que representan el actual estado del mercado informático actual, se puede afirmar, por ejemplo, que ha habido un cierto equilibrio entre algunas máquinas Atlhon 64, frente a algunas Pentium 4 similares. Sin embargo, llama la atención el hecho de que, como ha sido habitual con los productos AMD, los equipos revisados están fundamentalmente dirigidos a juegos, ocio y multimedia. Entre los Pentium 4, aunque también se encuentran propuestas similares, salta a la vista el modelo de Dell diseñado para reducir el espacio de los escritorios, incluso HP lanza una computadora de altas prestaciones dirigida a un usuario residencial que busca lo mejor, pero sin más preocupaciones que desembalar el producto y empezar a trabajar con él.

Algunas similitudes que presentan estos equipos es que, en general, presentan de serie 1 Gigabyte de RAM, la segunda cuestión es la velocidad de los procesadores, ya que resulta complicado encontrar modelos con parámetros reales o relativos inferiores a los 3 Ghz.

Ello nos da una idea del progreso en prestaciones y capacidad de cálculo que poseen las PC´s que están llegando últimamente al mercado de una forma masiva. Un equipo que sobresale es el modelo Dell SX280, (véase figura 3.8), una solución para entornos pequeños de oficina donde el espacio es reducido o limitado, al tiempo que un diseño elegante son alicientes para la compra. Esta PC, además de ofrecer un tamaño reducido sin renunciar a lo último en tecnología, cuenta con dos posibles formas de instalación.

La primera, como se aprecia en la figura 3.4, es en formato horizontal o vertical, dependiendo de nuestras necesidades, la segunda, echando mano de un soporte que incluye la propia base en su parte trasera, y que permite ensamblar la diminuta caja del monitor. De esta forma, además de lograr una solución de alta integración visual y reducir el número de cables, se gana mucho más espacio.

Figura 3.8 Equipo Dell SX280

3.8.3 Comunicación inalámbrica

Los cables han pasado a la historia. Los dispositivos inalámbricos han mejorado sustancialmente nuestra calidad de vida en la última década. Teléfonos móviles y computadoras portátiles, entre otros ingenios, nos mantienen conectados allá donde estemos, brindándonos la posibilidad de disfrutar de una libertad otrora impensable.

A pesar de que el ser humano es curioso por naturaleza, en muchas ocasiones nos conformamos con saber para qué sirve algo sin preguntarnos por el principio de su funcionamiento. Afortunadamente, la tecnología no es tan compleja como puede parecer. La popularidad de las redes inalámbricas se incrementa continuamente, en gran parte debido a la estandarización de los elementos en el proceso de comunicación.

Por un lado, los principales proveedores de servicios de acceso a Internet de banda ancha ofrecen a sus clientes la posibilidad de utilizar en sus instalaciones puntos de acceso para comunicaciones inalámbricas a precios extraordinariamente competitivos; de hecho, en ocasiones no superan el costo de los routers y módems convencionales.

Figura 3.9 Tarjeta de Red Inalámbrica

Por otra parte, la tecnología WiFi ha contado desde un principio con el respaldo de las firmas de gran peso específico en la industria, como es el caso específico de Intel. Por ejemplo, para que un dispositivo portátil pueda lucir en su carcasa el logotipo Centrino de Intel, debe incorporar en su interior tres elementos: un microprocesador Pentium M, un *chipset* perteneciente a la familia 855 y una controladora para redes inalámbricas Intel Pro Wireless 2100/2100A/2200BG, (véase figura 3.9).

3.8.4 Accesos WiFi

El método utilizado hace algunos años para encontrar un punto de acceso wireless era tan variado

como la cantidad de tarjetas inalámbricas. Algunos se ponían en marcha cuando se topaban con fuertes señales complejas, mientras que otras simplemente mostraban un icono de conexión.

Frente al pasado, hoy en día, solo hay que "toquetear" en la instalación de red. Se debe dar clic en el icono de la esquina inferior derecha del monitor para acceder a las distintas conexiones y elegir el identificador de la infraestructura inalámbrica, posteriormente, recorrer las distintas opciones hasta encontrar la lista de redes wireless disponibles. Todo lo que hay que saber sobre un punto de acceso es que tan fuerte es la señal. Eso, y si podemos disfrutar de ella. El detector no puede ayudarnos a descubrir si está abierto o pertenece a una red empresarial con las medidas de seguridad pertinentes, pero puede decirnos dónde se encuentra.

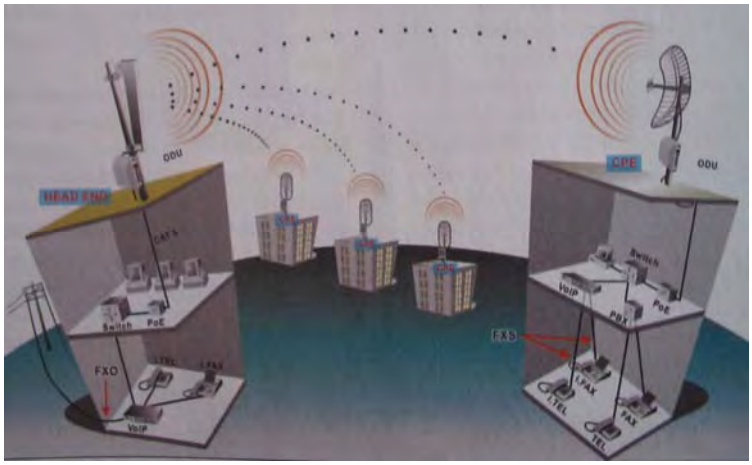

Figura. 3.10 En la imagen se puede apreciar el funcionamiento de una serie de antenas direccionales, diseñadas para comunicar vía inalámbrica diferentes edificios entre sí

Esta información es importante por dos razones. En primer lugar, si muestra que la señal proviene de una solución emplazada en la misma habitación en la que nos encontramos, y miramos y ahí está, sabremos que es la correcta, en segundo lugar, cuanto más cerca estemos, el sistema se pondrá más rápidamente en marcha y menos interferencias con otras redes soportaremos. Las redes WiFi son una verdadera maravilla a la hora de comunicar múltiples dispositivos sin necesidad de utilizar cables y a una velocidad medianamente razonable para los usos a los que comúnmente se les destina. Sin embrago, deben superar generalmente dos problemas en una gran parte de entornos en los que son instalados: la seguridad y el área de cobertura.

PARÁMETROS DE CONFIGURACIÓN

4.1 Sistema Operativo y software de aplicaciones

La selección de las instalaciones y la selección del equipo de cómputo, es tan importante como la **selección del software** que llevarán instaladas todas las computadoras dentro del CTI.

Si bien es cierto que los equipos de cómputo elegidos poseen características que los hacen veloces y eficientes en el procesamiento de información, hay que tomar en cuenta el no saturar estos equipos con paquetería que quizás, no sea la más adecuada para las necesidades que tienen los usuarios, sin olvidar que se trata de alumnos de la Facultad de Ingeniería y por ende, los paquetes de cómputo deben de apegarse a sus necesidades.

Los programas o software, son el conjunto de instrucciones que le dicen a la computadora qué debe hacer, sin ellos, la computadora es una máquina inútil. Hay diferentes clases de programas. Las dos principales categorías son las de los **sistemas operativos** y el **software de aplicaciones**.

El sistema operativo es el programa más importante, porque controla el funcionamiento de la computadora y los demás programas. Las aplicaciones son todos los programas que permiten al usuario:

- Realizar tareas de administración
- Procesar texto para documentos
- Juegos para divertirse
- Hojas de cálculo para trabajo financiero
- Browsers para navegar por la red, entre otros

El sistema operativo establece las reglas y parámetros para que el software aplicativo interactúe

con la computadora, ya que en lugar de comunicarse directamente con el hardware[1], las aplicaciones interactúan con el sistema operativo y este actúa como su intérprete.

4.1.1 Software de aplicaciones mínimos requeridos

A continuación se muestra una lista con la paquetería mínima requerida para los equipos de cómputo **(clientes)**:

- **Sistema Operativo:** Es el conjunto de programas que controla las actividades operativas de la computadora. El sistema operativo para los equipos de cómputo será Windows XP de Microsoft, ya que los equipos a adquirir son de la marca Dell, y como se sabe, está compañía tiene un convenio con la compañía Microsoft, por lo que se aprovechará el mismo.

- **Office de Microsoft:** Conjunto de programas para oficina, el cual esta compuesto generalmente, por un procesador de textos (**Word**), una hoja de cálculo (**Excel**) y un programa de gráficos de presentación (**PowerPoint**); este grupo de aplicaciones de productividad se ha convertido en el estándar en la mayoría de las computadoras utilizadas por instituciones de casi cualquier tipo.

- **Winzip:** Ésta es una aplicación diseñada para comprimir diversos tipos de archivos y con ello reducir el espacio de almacenamiento de los mismos; ofrece una interfaz de visualización, extracción, compresión y borrado de archivos **ZIP**.

- **Acrobat Reader:** Es un sistema de publicación de documentos electrónicos de uso estándar a nivel mundial. El documento es un **archivo PDF, (Poscript Document Format)**, tal documento posee todas sus características (tipos de fuente, espaciados, imágenes, viñetas, etc.) pero con el valor agregado que permite abrirlo de nuevo en cualquier otra computadora, idéntico al original.
- **Antivirus:** Programa cuya finalidad es prevenir las infecciones producidas por los virus informáticos, así como curar las ya producidas. Para que sean realmente efectivos, dada la gran cantidad de virus que se crean continuamente, estos programas deben actualizarse

[1] Elementos físicos que componen la computadora

periódicamente; debido al enorme número de virus que se generan día con día, han surgido un incontable número de antivirus, de entre los que se encuentran las versiones de **Norton** de Symantec, **Panda** de Panda Software **y McAffe** entre otros.

Lo anterior es para el caso de los equipos **clientes,** con respecto al **servidor** se detalla lo siguiente:

- **Sistema Operativo:** En este caso se eligió la versión **Windows 2000 Server de Microsoft** por ser una solución ideal para servidores de archivos, impresión y comunicaciones, además de ser un sistema operativo estable, confiable y robusto; mediante este sistema operativo se puede tener acceso a archivos, impresoras y recursos de red, esto, gracias a la creación de un dominio que controlará los recursos compartidos de los equipos clientes.

4.1.2 Software de aplicaciones específicos para alumnos de la Facultad de Ingeniería

Con respecto a la paquetería enfocada a las diversas ramas de la ingeniería, se enlistan algunos de los programas que más requieren los alumnos de esta Facultad.

- **Autocad:** Es una avanzada aplicación que permite trabajar con un elevado nivel de eficacia y productividad en la elaboración de planos. Es una plataforma de diseño $2D^2$ que automatiza las tareas de diseño y proporciona herramientas digitales de modo que las tareas se puedan enfocar en el diseño y no en la herramienta de trabajo. Es el software personalizable y ampliable líder de **CAD**[3] para dibujo y documentación de diseño en 2D, y diseño básico en $3D^2$.

- **Matlab:** Es un entorno de computación y desarrollo de aplicaciones totalmente integrado, orientado para llevar a cabo proyectos en donde se encuentren implicados elevados cálculos matemáticos y la visualización gráfica de los mismos.

  Matlab integra análisis numérico, cálculo matricial, proceso de señales en un entorno completo; dispone también en la actualidad de un amplio abanico de programas de apoyo especializados,

[2] 2D - 2 dimensiones. 3D – 3 dimensiones
[3] Diseño Asistido por Computadora

denominados **toolboxes**, que extienden el número de funciones incorporadas en el programa principal, cubren prácticamente casi todas las áreas principales de la ingeniería y la simulación, destacando entre ellos los "toolboxes" de proceso de imágenes, señal, control robusto, estadística, análisis financiero, matemáticas simbólicas, redes neuronales, lógica difusa, identificación de sistemas, simulación de sistemas dinámicos, etc.

- **Electronic Workbench:** Es un programa que permite la simulación de circuitos electrónicos además de una poderosa herramienta de simulación que incluye una completa y totalmente integrada versión de **Multicap,** para el diseño desde la entrada hasta la simulación de los circuitos electrónicos.

- **PSpice: (**Simulation Program with Integrated Circuits Emphasis) es un completo simulador para diseños analógicos, de propósito general que permite analizar circuitos analógicos sin necesidad de montarlos físicamente. Con sus sofisticados modelos internos, puede simular diseños de alta frecuencia, diseños de circuitos integrados de baja potencia y circuitos de potencia. **Spice** está considerado como el estándar en análisis electrónico, es referencia y base de numerosos simuladores del mercado.

- **Max Plus II:** Es un entorno integrado para el diseño de circuitos digitales sobre lógica programable. Soporta todas las familias de dispositivos programables de Altera, en los entornos Windows y UNIX.

- **Visual Basic:** Es un lenguaje de programación que se ha diseñado para facilitar el desarrollo de aplicaciones en un entorno gráfico. Es un diseñador de entorno de datos, genera de manera automática, conectividad entre controles y datos mediante la acción de arrastrar y colocar sobre formularios o informes. Es un conjunto de aplicaciones completo para la creación tanto de aplicaciones de escritorio como de aplicaciones Web. Aparte de generar aplicaciones de escritorio de alto rendimiento, se pueden utilizar las eficaces herramientas de desarrollo basado en componentes y otras tecnologías de Visual Studio para simplificar el diseño, desarrollo e implementación en equipo de soluciones.

- **Mathematica:** Es un programa en donde se pueden realizar todos los cálculos simbólicos y numéricos necesarios, se pueden preparar reportes científicos en un corto tiempo, pueden

realizarse gráficas de datos y funciones en 2D y 3D, así como analizar datos, gráficas y sonido provenientes de archivos con estándares distintos, se puede incluso publicar el trabajo realizado en la Web.

- **Maple:** Es un programa interactivo diseñado para resolver, de forma simbólica, problemas en las áreas de ciencias e ingeniería. Herramienta de cálculo analítico, capaz de generar código para Matlab y Visual Basic.

- **Flash:** Es una herramienta de creación de contenidos para Internet de última generación, es la forma más rápida de crear aplicaciones y contenido de animaciones para Internet. Las características de Flash permiten usar potentes videos, multimedia y desarrollar aplicaciones que se traducen en un mayor dinamismo en las interfaces de usuario.

- **Dreamweaver:** Es un editor HTML profesional para diseñar, codificar y desarrollar sitios, páginas y aplicaciones Web. Las funciones de edición visual de Dreamweaver permiten crear páginas de forma rápida, sin escribir una sola línea de código. Puede ver todos los elementos pasivos o activos del sitio y arrastrarlos desde un panel fácil de usar directamente hasta un documento. Puede agilizar el flujo de trabajo de desarrollo mediante la creación y edición de imágenes en **Macromedia Fireworks** o en otra aplicación de gráficos y su posterior importación directa a **Dreamweaver**, o bien añadir objetos **Macromedia Flash.**

  Dreamweaver también ofrece un entorno de codificación con todas las funciones, que incluye herramientas para la edición de código (tales como coloreado de código y terminación automática de etiquetas) y material de referencia sobre HTML, hojas de estilos en cascada (CSS), JavaScript, ColdFusion Markup Language (CFML), Microsoft Active Server Pages (ASP) y JavaServer Pages (JSP).

- **C++ :** En la actualidad, el C++ es un lenguaje versátil, potente y general. Su éxito entre los programadores profesionales le ha llevado a ocupar el primer puesto como herramienta de desarrollo de aplicaciones. El C++ mantiene las ventajas del C en cuanto a riqueza de operadores y expresiones, flexibilidad, concisión y eficiencia. Además, ha eliminado algunas de

las dificultades y limitaciones del C original. La evolución de C++ ha continuado con la aparición de Java, un lenguaje creado simplificando algunas cosas de C++ y añadiendo otras, que se utiliza para realizar aplicaciones en Internet.

4.2 Software autorizado

Se considera como software autorizado, tanto los **sistemas operacionales** como aquellos **paquetes de usuario final** y de **sistemas aplicativos**, que se hayan instalado, previo visto bueno para su adquisición y con la autorización legal del proveedor para su uso.

4.2.1 Permisos y licencias

El uso de Software no autorizado o adquirido ilegalmente, se considera como ***"pirata"*** y constituye una violación a los derechos de autor. El uso de hardware y de software autorizado esta regulado por las siguientes normas:

- Toda dependencia podrá utilizar **UNICAMENTE** el hardware y el software que el administrador o el personal autorizado haya instalado y oficializado mediante un "Acta de entrega de equipos y/o software".

- Tanto el hardware y software, como los datos, son propiedad del CTI, su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias del CTI, será sancionada de acuerdo con las normas y reglamento interno del lugar.

- El administrador o el personal autorizado llevará el control del hardware y el software instalado, basándose en el número de serie que contiene cada uno.

- Los discos compactos que contienen el software original de cada paquete serán administrados y almacenados por el administrador del CTI.

- Toda necesidad de hardware y/o software adicional debe ser solicitada por escrito al administrador, quien justificará o no dicho requerimiento, mediante un estudio evaluativo.

- El administrador proveerá al personal una copia del software original en caso de requerirse la reinstalación de un paquete determinado.

- Periódicamente, el administrador o el personal autorizado efectuarán revisiones para verificar el software utilizado. Por lo tanto, el detectar software no registrado por el responsable, será considerado como una violación a las normas internas del CTI.

- El administrador o el personal autorizado instalarán el software original, previo registro, en cada computadora y facilitarán a los usuarios, los manuales pertinentes los cuales quedarán bajo la responsabilidad del encargado del CTI.

- La prueba, instalación y puesta en marcha de los equipos y/o dispositivos, serán realizada por el personal autorizado por el administrador, quien una vez que compruebe el correcto funcionamiento, oficializará su entrega mediante un **"Acta de Entrega de Equipos y/o Software"**.

- El coordinador del CTI mantendrá actualizada la relación de los equipos de cómputo, en cuanto a número de serie y ubicación, con el fin de que este mismo verifique, por lo menos una vez por semestre su correcta destinación.

- El coordinador del CTI actualizará el software comprado cada vez que una nueva versión salga al mercado, a fin de aprovechar las mejoras realizadas a los programas, siempre y cuando se justifique esta actualización.

4.2.2 Derechos de autor y licencia de uso de software

El **Copyright**, o los **derechos de autor**, son el **sistema de protección jurídica** concebido para titular las obras originales de autoría determinada, expresadas a través de cualquier medio tangible o intangible.

Los programas de computación, las bases de datos y las infracciones derivadas de su uso ilícito se encuentran reguladas en la **Ley Federal del Derecho de Autor** del 24 de diciembre de 1996, que entró en vigor el 24 de marzo de 1997. En este orden, esta **Ley regula todo lo relativo a la**

protección de los programas de computación, a las bases de datos y a los derechos autorales relacionados con ambos.

Se contempla dentro de esta Ley la protección de los programas de computación, sus derechos patrimoniales, de arrendamiento, casos en los que el usuario podrá realizar copias del programa que autorice el autor del mismo. Las facultades de autorizar o prohibir la reproducción, la autorización del acceso a la información de carácter privado relativa a las personas contenida en las bases de datos, la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, establece las infracciones y sanciones que en materia de derecho de autor deben ser aplicadas cuando ocurren ilícitos relacionados con los citados programas y las bases de datos, etc. En este sentido, se considera importante la mención de los artículos **102**[4] y **231**[5].

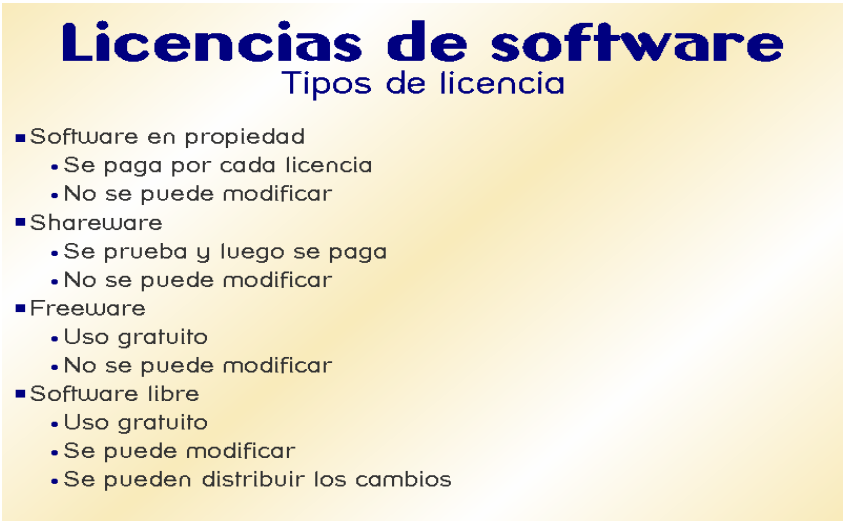

Figura 4.1 Tipos de licencias de software

El tipo de licencia que será utilizada en el CTI será básicamente, un tipo de **licencia por servidor** para ese equipo, **licencias** independientes **para los Sistemas Operativos** de los equipos de escritorio (Windows XP Professional) y **licencias para la paquetería** que así lo requiera.

[4] Regula la protección de los programas de computación y señala además que aquellos que tengan por objeto causar efectos nocivos a otros programas o equipos, lógicamente no serán protegidos.

[5] En su fracción V sanciona el comercio de programas de dispositivos o sistemas cuya finalidad sea desactivar dispositivos electrónicos de protección de un programa de cómputo. En las fracciones II y VII contemplan dentro de las infracciones de comercio el "producir, fabricar, almacenar, distribuir, transportar o comercializar copias ilícitas de obras protegidas por la Ley" y "usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular".

4.3 Red inalámbrica

Entre las innovaciones con las que cuenta el CTI se encuentra la más importante, la red inalámbrica; dentro de la UNAM y más específicamente, en la Facultad de Ingeniería, existen diversas redes inalámbricas que poseen características distintas a las de este CTI, tales como la cantidad de usuarios a las que prestan el servicio o el fin por el que prestan ese servicio; la principal característica que distingue a este lugar con respecto a la red inalámbrica, es en cuanto a la capacidad de conexiones, ya que la mayoría de las redes inalámbricas en la Facultad soportan un número reducido de usuarios.

Se tiene contemplado brindar inicialmente el servicio para **30 usuarios**, dado que es el número de equipos de cómputo (computadoras de escritorio fijas) que estarán en funcionamiento dentro del CTI, posteriormente el servicio se brindará también a usuarios de **equipos portátiles (laptops)** que podrán trabajar en espacios específicos al interior del CTI, o bien, en los alrededores próximos al lugar, aprovechando con esto el potencial que brindará la conexión inalámbrica.

El servicio para **equipos portátiles** se brindará tiempo después de que el CTI se encuentre operando, pensando primero en la difusión de la sala y los servicios con los que cuenta, una ves logrado lo anterior, se establecerá el servicio para laptops.

Para poder ofrecer este servicio se dispondrá de una cantidad inicial de **100 direcciones IP** [6] que serán asignadas a cada uno de los equipos portátiles que requieran del servicio. Para tener un control sobre este servicio y asegurar el fin para el cual se brinda, el usuario tendrá que llenar una forma en la cual proporcione sus datos personales así como datos característicos del equipo, tales como modelo y dirección **MAC**[7]**,** aunado a esto, se le proporcionará una guía para la configuración de la tarjeta de red inalámbrica y el reglamento específico a acatar para este servicio. La vigencia de la dirección IP será por un semestre y el usuario tendrá la opción de renovar el servicio para el semestre siguiente o liberar la dirección, permitiendo con esto la continuidad del servicio para nuevos usuarios.

[6] Secuencia de números que se utilizan para asignar una ubicación a nivel electrónico. Identifica una computadora determinada dentro de una red.
[7] Identificador único para una computadora a nivel mundial.

4.3.1 Ventajas de la conexión inalámbrica

La tecnología inalámbrica proporciona al usuario las siguientes ventajas:

- Movilidad
- Opciones de instalación simple y flexible
- Costo reducido de adquisición (no genera gastos de cableado o mantenimiento)
- Excelente adaptabilidad para soportar equipos de cómputo adicionales

En la configuración inalámbrica típica, un Punto de Acceso (transceiver) se conecta a una red de alambre con cableado estándar. El Punto de Acceso soporta hasta **253 usuarios** localizados a 25 [m] de distancia del equipo, hasta un máximo de **100 [m] radiales**. Los usuarios tienen acceso a la WLAN vía la tarjeta inalámbrica instalada en sus equipos portátiles o de escritorio. La tarjeta inalámbrica crea la interfase entre el sistema operativo de la red y el radio vía una antena (el propio Punto de Acceso).

La tecnología inalámbrica proporciona mayor **comodidad** y **movilidad** con total **funcionalidad** en cualquier lugar. Pero para que tenga aceptación entre los usuarios, esta funcionalidad debe garantizarse cualquiera que sea la plataforma.

Con los nuevos estándares en la industria, mayores tarifas de rendimiento de procesamiento, y las continuas bajas de costos, se ha vuelto más fácil justificar implementaciones de tecnología de red inalámbrica, además de que podremos contar con una serie de elementos que elevarán la productividad de la sala, tales como:

- **Movilidad:** Ninguna conexión física de red permite la mobilidad de trasladarse virtualmente a cualquier parte del CTI, dentro o fuera del mismo.

- **Productividad:** Es posible trabajar en cualquier lugar próximo al CTI sin perder la conexión. Velocidades de rendimiento comparable o mejor que las redes cableadas **10BaseT** [8], las cuales ofrecen acceso confiable a e-mail, Internet, archivos compartidos y otros recursos de la red.

[8] Estándar Ethernet para transmisión sobre par de cobre a 10 Mbps.

- **Flexibilidad:** A pesar de que el CTI contará a su vez con una instalación de red física, con la red inalámbrica no hay necesidad de preocuparse por el cableado. Las redes inalámbricas son fáciles de instalar y ofrecen beneficios en los lugares donde el cableado es difícil de desplegar.

- **Portabilidad:** Cuando hay que cambiar de espacio de trabajo y se cuenta con un equipo portátil, tan sólo hay que llevar el equipo y seguir disfrutando de la conexión.

- **Ahorro de costo/tiempo:** Una costosa y tardada instalación de cable puede ser reemplazada, crecida, o expandida con una solución de red inalámbrica; en el caso específico del CTI, además de contar con la red inalámbrica, se contará también con una instalación de red cableada, asegurando con esto que si por algún motivo la red inalámbrica llegase a fallar, los equipos podrán conectarse a la red cableada, manteniendo así el servicio sin interrupción alguna. Para ello, basta con realizar un simple arreglo en los equipos de cómputo en donde se active la opción en las **conexiones de red** para que se establezca una conexión dependiendo del tipo de red disponible, sea alámbrica o inalámbrica.

- **Facilidad de instalación:** Agregar más computadoras de escritorio y portátiles a una red requiere de un mínimo de tiempo y esfuerzo.

4.3.2 Funcionamiento de las WLAN

WLAN son las siglas en inglés de **W**ireless **L**ocal **A**rea **N**etwork. Es un sistema de comunicación de datos flexible muy utilizado como alternativa a la LAN cableada o como una extensión de ésta. Utiliza tecnología de radio frecuencia que permite mayor movilidad a los usuarios al minimizarse las conexiones cableadas. Las WLAN han adquirido importancia en muchos campos incluido el de la medicina. **Se utilizan ondas de radio para llevar la información de un punto a otro sin necesidad de un medio físico,** como se muestra en la figura 4.2**.** Las ondas de radio son normalmente referidas a portadoras de radio, ya que éstas únicamente realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final.

Esto es llamado **modulación de la portadora** por la información que está siendo transmitida. De este modo, la señal ocupa más ancho de banda que una sola frecuencia. **Varias portadoras**

pueden existir en igual tiempo y espacio sin interferir entre ellas, si las ondas son transmitidas a distintas frecuencias de radio. Para extraer los datos el receptor se sitúa en una determinada frecuencia ignorando el resto. El punto de acceso recibe la información, la almacena y transmite entre la WLAN y la LAN cableada. **Un único punto de acceso puede soportar un pequeño grupo de usuarios** y puede funcionar en un rango de al menos treinta metros y hasta varios cientos.

Figura 4.2 Método de propagación de la señal en una red inalámbrica

4.3.3 Tipos de instalaciones inalámbricas

Las redes inalámbricas se construyen utilizando diferentes topologías básicas. Estas topologías se llaman de distintas formas:

- **Red punto a punto:** Instalando un Punto de Acceso se puede doblar el rango al que los dispositivos pueden comunicarse, pues actúan como repetidores. Cada punto de acceso puede servir a varios clientes, según la naturaleza y número de transmisiones que tienen lugar.

- **Topología de infraestructura:** Es una red que amplía una red cableada existente a dispositivos inalámbricos, proporcionando una estación base (llamada punto de acceso). El punto de acceso se une a las redes inalámbricas y cableadas, actuando como un controlador central para la red inalámbrica.

  El punto de acceso coordina la transmisión y la recepción de múltiples dispositivos

inalámbricos dentro de un rango específico. El rango y cantidad de dispositivos dependen del estándar inalámbrico que se utilice y el producto del proveedor. En la infraestructura puede haber varios puntos de acceso para cubrir una gran área o sólo un punto único de acceso para un área pequeña, como por ejemplo una casa o un edificio pequeño.

- **Topología ad-hoc:** Es una en la cual se crea una red WLAN únicamente por los dispositivos inalámbricos mismos, sin controlador central o punto de acceso. Cada dispositivo se comunica directamente con los demás dispositivos en la red, en lugar de que sea a través de un controlador central. Esto es útil en lugares en donde pequeños grupos de computadoras pueden congregarse y no se necesita acceso a otra red. Por ejemplo, un hogar sin una red cableada o un cuarto de conferencia en donde se reúnen regularmente equipos para intercambiar ideas, son ejemplos en los que puede ser útil una red inalámbrica ad-hoc.

Una vez que se ha explicado la operación básica de la modalidad de infraestructura, se puede explicar la modalidad ad-hoc, la configuración más simple de una WLAN conecta un conjunto de computadoras con adaptadores inalámbricos. Cuando dos o más de estos equipos están dentro del rango de alcance de sus adaptadores pueden establecer una red independiente. Estas redes generalmente no requieren administración o preconfiguración alguna.

En este tipo de redes, varios puntos de acceso enlazan la WLAN con la red alambrada, de esta forma, éstos también fungen como mediadores de tráfico hacia el vecindario inmediato. La cobertura inalámbrica puede ser extendida en un edifico completo, si así se requiere.

- En la configuración **cliente – punto de acceso**, los puntos de acceso tienen un rango finito, del orden de 150 [m] en lugares cerrados y 300 [m] en zonas abiertas. En zonas grandes como por ejemplo un campus universitario o un edificio es probablemente necesario más de un punto de acceso. La meta es cubrir el área con células que envuelvan la zona de modo que los clientes puedan moverse sin cortes entre un grupo de puntos de acceso, esto es llamado "roaming".

- Para resolver problemas particulares de topología, el diseñador de la red puede elegir usar un **Punto de Extensión (EP)** para aumentar el número de puntos de acceso a la red, de

modo que funcionan como tal pero no estén enganchados a la red cableada como los puntos de acceso. Los puntos de extensión pueden encadenarse para pasar mensajes entre un punto de acceso y clientes lejanos de modo que se construye un "puente" entre ambos.

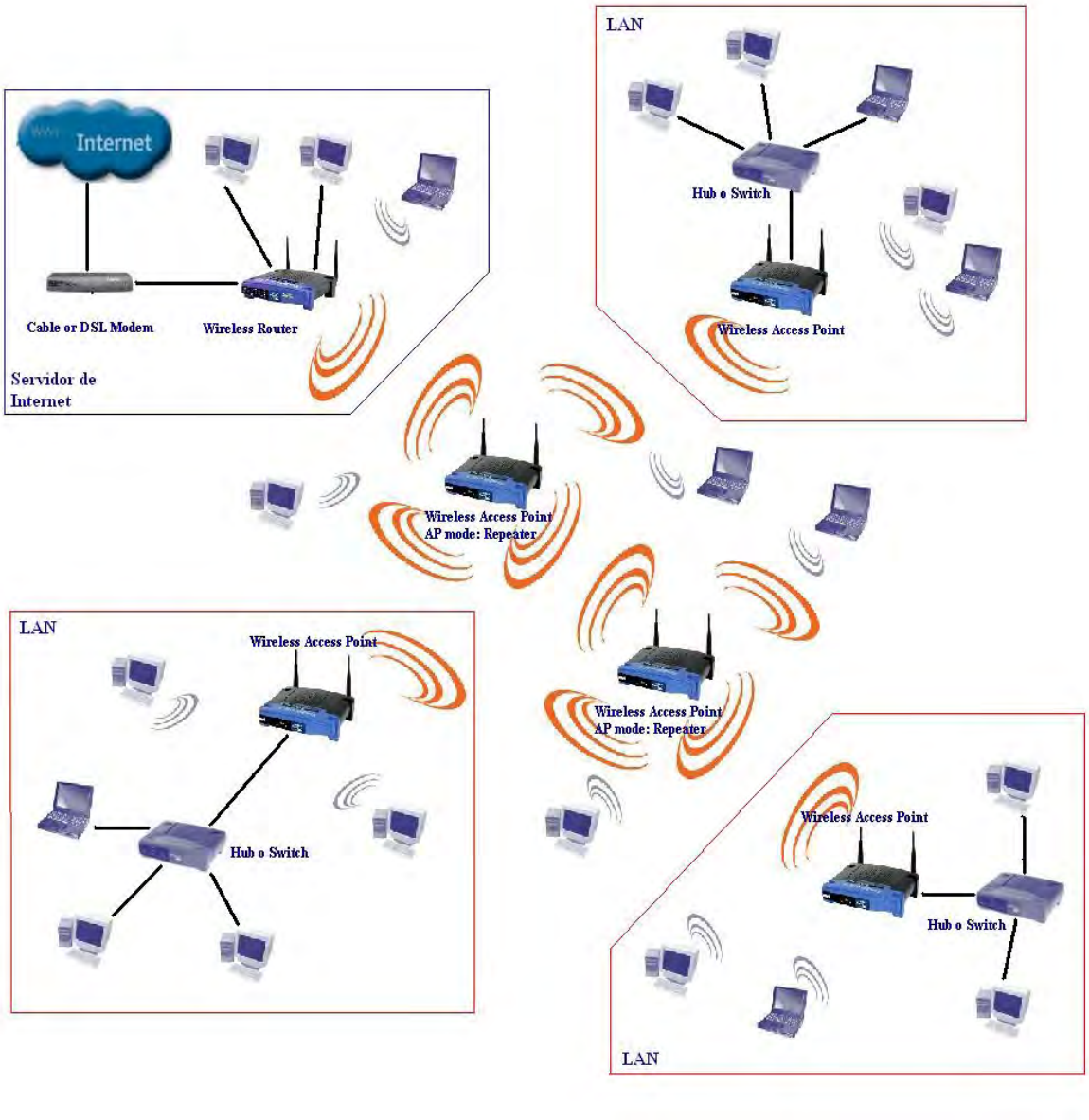

Figura 4.3 En la figura se muestra una topología en donde el proveedor de Internet comparte su conexión a través de un Módem o Cable DSL (Línea Segura Digital) con un Hub o Switch si es que se cuenta con un número considerable de equipos, de aquí, al Router Inalámbrico.

También están los Puntos de Acceso Inalámbricos, AP mode: Repetidores. Estos servirían para ampliar la red a zonas más grandes. A continuación se encuentran las LAN's, con su respectivo Punto de Acceso Inalámbrico, que serviría como puente entre la LAN local y la red inalámbrica. También esta el Hub o Switch para las conexión de las computadoras que no tienen la tarjeta de red inalámbrica.

Uno de los últimos componentes a considerar en el equipo de una WLAN es la antena direccional. Por ejemplo, se requiere una WLAN sin cable a otro edificio a 1 [Km] de distancia. Una solución puede ser instalar una antena en cada edificio con línea de visión directa. La antena del primer edificio está conectada a la red cableada mediante un punto de acceso. Igualmente en el segundo edificio se conecta un punto de acceso, lo cuál permite una conexión sin cable en esta aplicación.

4.3.4 Cobertura

La distancia que pueden alcanzar las **Ondas de Radiofrecuencia (RF)** está en función del diseño del producto y del camino de propagación, especialmente en lugares cerrados. Las interacciones con objetos, paredes, metales, e incluso la gente, afectan a la propagación de la energía. Los objetos sólidos bloquean las señales, esto impone límites adicionales.

La mayor parte de los sistemas de redes inalámbricas usan RF porque pueden penetrar la mayor parte de lugares cerrados y obstáculos. El rango de cobertura de una WLAN típica va de 30 a 100 [m] aproximadamente. Puede extenderse y tener posibilidad de alto grado de libertad y movilidad utilizando puntos de acceso (micro células) que permiten "navegar" por la WLAN.

4.3.5 Rendimiento

El rendimiento así como la eficacia de la red inalámbrica, dependen de diversos factores:

- La puesta a punto de los productos así como del número de usuarios
- Los factores de propagación (cobertura, diversos caminos de propagación)
- Tipo de sistema inalámbrico utilizado, que a su vez depende de:
    - Retardo de la señal
    - Los cuellos de botella de la parte cableada de la red

Para la más comercial de las redes inalámbricas, los datos que se tienen hablan de un rango de 1.6 Mbps. Los usuarios de Ethernet no experimentan generalmente gran diferencia en el funcionamiento cuando utilizan una red inalámbrica. La mayor parte de las redes WLAN

proporcionan un estándar de interconexión con redes cableadas como **Ethernet** [9] o **Token Ring**[10].

Los nodos de la red inalámbrica son soportados por el sistema de la red de la misma manera que cualquier otro nodo de una red LAN, aunque con los discos apropiados. Una vez instalado, la red trata los nodos inalámbricos igual que cualquier otro componente de la red.

Las WLAN son un medio compartido, lo que significa que incluso en despliegues pequeños, ciertos usuarios o aplicaciones podrían "colapsar" todo el ancho de banda y alentar al máximo la red, para prevenir ello, conviene tomar en cuenta el diseño del tráfico, incluyendo la asignación de prioridades, y la gestión del ancho de banda para el tráfico entrante y saliente, lo que permita a cada usuario, grupo de usuarios o servicio se le asigne una cantidad adecuada del ancho de banda disponible.

4.3.6 Estándares 802.11

En 1997, un grupo de ingenieros del **IEEE**[11] se unió para crear un estándar para las LAN inalámbricas. El primer protocolo, ***802.11*** (véase Tabla 4.1), fue ratificado por la organización en ese mismo año y permitía abordar la transferencia de datos a un máximo de 2 Mbps; se puso de manifiesto que estas velocidades de transferencia de datos eran demasiado lentas para soportar la mayoría de las aplicaciones generales de las empresas.

Dos años después se presentó la versión ***802.11b***, también conocido como ***802.11*** **de Alta Velocidad** (de entre 5.5 Mbps y 11 Mbps), a la que siguieron las especificaciones ***802.11g***, (véase Tabla 4.2) y ***802.11a***, (ambas a 54 Mbps).

Con lo anterior se pretende que el Punto de Acceso a utilizar cubra los estándares **802.11 b** y **g** ya que con esto, se podrá trabajar a una buena velocidad y sobretodo ser compatibles con otros estándares, con respecto a las tarjetas de red inalámbricas que utilicen los usuarios.

[9] Es una red con topología tipo bus, con protocolo CSMA/CD, que trabaja en banda base y es capaz de transmitir a 10 MBit/s, emplea codificación Manchester.
[10] Es un sistema utilizado cuando varios ordenadores están conectados a una red configurada en forma de anillo o de estrella, para evitar la colisión de los datos de dos ordenadores si estos envían sus mensajes a la red al mismo tiempo.
[11] Institute of Electrical and Electronics Engineers

ESPECIFICACIONES DE LOS ESTÁNDARES DE COMUNICACIÓN INALÁMBRICA *802.11*										
Estándar	**Año de lanzamiento**	**Tasa de transferencia máxima [Mbits/s]**	**Banda de radio [GHz]**	**Ancho de banda del canal [MHz]**	**Potencia de emisión [mW]**	**Cobertura aprox. en interior/exterior [m]**	**Modulación utilizada**	**Compatibilidad**	**Ventajas**	**Inconvenientes**
802.11	1997	2	2.4	obsoleto	obsoleto	obsoleto	DBPSK (Differential Binary Phase Shift Keying)	Estándar original	Universal y compatible en todo el mundo	Lento
802.11b	1999	11	2.4	22	100	100 / 300	CCK (Complementary Code Keying)	Compatible con productos que satisfagan el estándar 802.11g	Universal y compatible en todo el mundo	Lento, propicio a interferencia y soporta pocos clientes simultáneos
802.11a	2001	54	5	25	200	50 / 150	OFDM (Orthogonal Frecuency Division Multiplexing)	Compatible con productos que satisfagan el estándar 802.11a	Rápido y admite un mayor número de clientes simultáneos	Caro y poco extendido
802.11g	2003	54	2.4	22	100	100 / 300	OFDM o CCK	Compatible con productos que satisfagan el estándar 802.11b	Económico, rápido y cada vez más extendido	Propicio a interferencias

Tabla 4.1 Estándares principales de comunicación inalámbrica

En julio de 1999, los líderes de la industria inalámbrica se unieron para crear la Alianza para la **Compatibilidad Ethernet Inalámbrica (WECA)**. La misión de la WECA es la de certificar la interfuncionalidad y compatibilidad de los productos de redes inalámbricas IEEE *802.11b* y promover este estándar para la empresa, las universidades, los pequeños negocios y el hogar.

Entre los miembros de la WECA se incluyen fabricantes y proveedores de semiconductores WLAN, fabricantes de sistemas informáticos y desarrolladores de software. La misión de este organismo es certificar la interfuncionalidad de los productos WiFi, así como promoverlo como el estándar global para WLAN en todos los segmentos del mercado.

Estándar	Descripción
802.11	Estándar WLAN original. Soporta de 1 a 2 Mbps.
802.11a	Estándar WLAN de alta velocidad en la banda de los 5 GHz. Soporta hasta 54 Mbps.
802.11b	Estándar WLAN para la banda de 2.4 GHz. Soporta 11 Mbps.
802.11e	Está dirigido a los requerimientos de calidad de servicio para todas las interfaces IEEE WLAN de radio.
802.11f	Define la comunicación entre puntos de acceso para facilitar redes WLAN de diferentes proveedores.
802.11g	Establece una técnica de modulación adicional para la banda de los 2.4 GHz. Dirigido a proporcionar velocidades de hasta 54 Mbps.
802.11h	Define la administración del espectro de la banda de los 5 GHz para su uso en Europa y en Asia Pacífico.
802.11i	Está dirigido a abatir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1X, TKIP (Protocolo de Llaves Integras –Seguras– Temporales), y AES (Estándar de Encriptación Avanzado).

Tabla 4.2 Estándares existentes de comunicación inalámbrica

4.3.7 La seguridad en redes WLAN

Aunque parezca mentira a estas alturas, aun hay muchos usuarios que preparan la infraestructura necesaria para montar una red inalámbrica sin preocuparse en lo más mínimo por la seguridad de sus equipos. Basta darse una vuelta con una computadora portátil equipada con una tarjeta de red inalámbrica por una zona urbanizada o comercial para descubrir una multitud de redes totalmente abiertas y listas para que cualquier persona haga uso de ellas.

Para poder realizar lo anterior, basta contar con una computadora portátil, que cuente con una tarjeta de red inalámbrica de buena calidad y potencia ya que mientras mejor sea la tarjeta, mejor captación habrá de las redes disponibles. Al transitar por una zona comercial donde se crea existen tecnologías inalámbricas, el equipo captará las diversas redes existentes, si se requiere una localización exacta de los puntos de acceso, basta utilizar un localizador **GPS**[12] que ubique la posición exacta de estos y una aplicación que distinga los diversos tipos de redes inalámbricas existentes, como lo son:

- **Redes abiertas:** Accesibles para cualquier usuario
- **Redes protegidas:** Accesibles solo con contraseña
- **Redes públicas con acceso mediante contraseña:** Accesibles a través de contraseñas distribuidas por el proveedor del servicio de red inalámbrico
- **Redes cerradas:** Redes no accesibles para equipos ajenos a los configurados en el punto de acceso.

Al localizar una **red abierta,** basta con seleccionarla de entre todas las redes disponibles y automáticamente el equipo contará con salida a Internet. En los inicios de la tecnología inalámbrica, los procedimientos y mecanismos de seguridad eran tan débiles que podía ganarse acceso con relativa facilidad hacia redes WLAN de compañías desde la calle. Existe el término **"wardriving"**, que se refiere a la acción de recorrer una lugar para buscar la existencia de redes inalámbricas y tener acceso a ellas. En la actualidad, existen técnicas más sofisticadas y complejas, las cuales fortalecen los inconvenientes de los mecanismos WLAN y ayudan a mantener la confidencialidad y resistencia ante los ataques dirigidos hacia este tipo de redes.

El estándar inalámbrico 802.11 original incorpora encriptación y autenticación **WEP**[13]. Sin embargo, en el 2001 se publicaron artículos que comunicaban las deficiencias que enfrentaba dicho mecanismo. Al interceptar y decodificar los datos transmitidos en el aire, y en cuestión de horas en una red WLAN con tráfico intenso, la clave WEP puede ser deducida y se puede ganar acceso no autorizado. Esta situación desencadenó una serie de acciones por parte del IEEE y de la industria para mejorar la seguridad en las redes de tecnología inalámbrica.

[12] Global Position System - Sistema de Posicionamiento Global.
[13] Wireless Equivalent Privacy - Privacidad Alterna en redes inalámbricas.

La seguridad WLAN abarca dos elementos: El **acceso a la red** y la **protección de los datos** (autenticación y encriptación, respectivamente). Las violaciones a la seguridad de la red inalámbrica, generalmente, vienen de los puntos de acceso **no autorizados**, aquéllos instalados sin el conocimiento de los administradores de la red, o que operan con las funcionalidades de protección deshabilitadas (que es la configuración por omisión en los dispositivos inalámbricos).

Estos "hoyos" en la seguridad, pueden ser aprovechados por personal no autorizado (hackers), que en caso de que logren asociarse con el punto de acceso, ponen en riesgo no únicamente la infraestructura inalámbrica, sino también la WLAN a la cual se conecta. A continuación se mencionan los mecanismos de seguridad usados en redes WLAN, así como las ventajas y desventajas de cada uno de ellos. En el terreno de la seguridad de las redes WLAN, aparecen multitud de acrónimos que vienen a identificar otros tantos protocolos, algunos de los cuales resultan familiares a los administradores de estas redes:

- ***EAP*** (**E**xtensible **A**uthentication **P**rotocol): Autenticación de un cliente mediante un protocolo
- ***LEAP*** (**L**ightweigth **EAP**): Emplea un esquema de nombre de usuario y contraseña, soporta claves de usuario dinámicas
- ***WEP*** *(**W**ireless **E**ncryption **P**rotocol o **W**ireless **E**quivalent **P**rivacy):* Preserva la privacidad de los datos transferidos en una WLAN
- ***TKIP*** (**T**emporal **K**ey **I**ntegrity **P**rotocol): Se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo
- ***WPA*** (**W**i-Fi **P**rotected **A**ccess): Este estándar subsana los problemas de WEP, mejora el cifrado de los datos y obtiene un mecanismo de autentificación

Son en definitiva, eficaces herramientas, capaces de proporcionarnos en cierta medida la seguridad pretendida. Para conseguir la fiabilidad que necesitamos en una red inalámbrica debemos contemplar un factor esencial: Hay que decidir quien debe tener acceso a nuestra WLAN, esto lo resolvemos mediante los mecanismos de autenticación. El estándar ***802.11*** preserva la privacidad de los datos transferidos gracias al algoritmo WEP, además, estipula dos mecanismos de identificación de clientes netamente diferenciados: **autenticación abierta (*Open authentication*)** y por **clave compartida (Shared key authentication)**.

4.3.8 Retos de la seguridad en redes inalámbricas

Con una red cableada existe una seguridad inherente en el hecho de que un ladrón potencial de datos tiene que tener acceso a la red a través de una conexión cableada, lo que normalmente quiere decir que necesita un acceso físico a la planta de cables de la red. Además de este acceso físico, se pueden estratificar otros mecanismos de seguridad.

Cuando la red ya no está formada por cables, la libertad adquirida por los usuarios de la red también puede ampliarse al robo potencial de datos. Ahora, la red puede estar disponible en los pasillos, áreas inseguras de espera, hasta afuera de un edificio. En un ambiente doméstico (en casa), la red puede ampliarse a las casas de los vecinos si esta no adopta mecanismos adecuados de seguridad o si no se usa apropiadamente.

Desde su creación, el protocolo **802.11** ha proporcionado algunos mecanismos básicos de seguridad para que esta mayor libertad no sea una amenaza potencial. Por ejemplo, los puntos de acceso de 802.11 (o conjuntos de puntos de acceso) se pueden configurar con un identificador de conjunto de servicios.

Si bien puede haber otros problemas con este esquema, esto ya es suficiente para no detener a ninguno de los piratas más inexpertos. Se proporciona seguridad adicional a través de las especificaciones 802.11 por medio del algoritmo WEP. El protocolo anterior proporciona 802.11 con servicios de autenticación y encriptación. **El algoritmo WEP** define el uso de una clave secreta de 40 bits para autenticación y encriptación y muchas implementaciones, IEEE 802.11 también permiten claves secretas de 104 bits. Este algoritmo proporciona la mayor protección contra peligros y cuenta con atributos físicos de seguridad comparables con los de una red cableada.

4.4 Configuración del servidor

Como se describió en el capítulo 4.1.1, el servidor dispondrá del sistema operativo **Windows 2000 Server de Microsoft,** que es el centro vital que controla los parámetros de administración de recursos, usuarios, aplicaciones y dispositivos así como las directivas de seguridad correspondientes para proteger los elementos anteriores.

El proceso de instalación del sistema operativo se basa en la aplicación de un conjunto de elementos de análisis y configuración. En la siguiente tabla se enumeran los tipos de información que deben recopilarse antes de iniciar el programa de instalación:

Adaptador	Información para recopilar
Vídeo	Tipo de conjunto de chips o de adaptador y cuántos adaptadores de vídeo
Red	IRQ, dirección de E/S, tipo de conector DMA (si se utiliza), por ejemplo BNC o par trenzado, y tipo de bus
Controlador SCSI	Modelo de adaptador o conjunto de chips, IRQ y tipo de bus
Mouse	Tipo de mouse y puerto (COM1, COM2, bus o PS/2) o USB
Puerto de E/S	IRQ, dirección de E/S y DMA (si se utiliza) para cada puerto de E/S
Adaptador de sonido	IRQ, dirección de E/S y DMA
Bus serie universal (USB)	Dispositivos y concentradores conectados
PC Card	Qué adaptadores se han insertado y en qué ranuras
Plug and Play	Si está habilitado o deshabilitado en el BIOS
Configuración del BIOS	Fecha y versión del BIOS
Módem externo	Conexiones de puerto COM (COM1, COM2, etc.)
Módem interno	Conexiones de puerto COM; para configuraciones no estándar, IRQ y direcciones de E/S
Configuración avanzada e interfaz de energía (ACPI); Opciones de energía	Habilitada o deshabilitada; configuración actual
PCI	Qué adaptadores PCI se han insertado y en qué ranuras

Tabla 4.3 Información necesaria antes de la instalación

4.4.1 Requisitos del sistema y compatibilidad de hardware

Para garantizar un rendimiento adecuado, hay que asegurarse de que los equipos en los que va a instalar Windows 2000 Server cumplen los siguientes requisitos:

- Unidad central de proceso (CPU) Pentium a 133 MHz o superior.
- Se recomienda 256 MB de RAM como mínimo (128 MB es el mínimo admitido; 4 GB es el máximo).

- Una partición de disco duro con suficiente espacio libre para permitir el proceso de instalación. El espacio mínimo necesario será aproximadamente 1 GB. Es posible que necesite más espacio, dependiendo de los factores siguientes:

    - Los componentes que vaya a instalar: Cuantos más componentes, más espacio se necesitará.
    - El sistema de archivos que se utiliza: FAT[14] requiere entre 100 y 200 MB más de espacio libre en disco que otros sistemas de archivos.
    - El método utilizado para la instalación: Si va a instalar a través de una red, necesitará entre 100 y 200 MB más de espacio que si instala desde el disco compacto. (Es necesario tener disponibles más archivos de controladores durante la instalación a través de una red).

El programa de instalación de Windows 2000 comprueba automáticamente el hardware y el software e informa de los conflictos posibles. No obstante, para garantizar una instalación correcta hay que asegurarse de que el hardware del equipo es compatible con Windows 2000 Server antes de iniciar el programa de instalación.

4.4.2 Modo de licencia

Windows 2000 Server acepta dos modos de licencia: **Por puesto** y **por servidor**. El modo **por puesto** requiere una Licencia de Acceso de Cliente (CAL) independiente por cada equipo que tenga acceso a Windows 2000 Server. El modo Por servidor requiere una CAL independiente para cada conexión simultánea a este servidor.

Por el contrario, la licencia **por servidor** significa que cada conexión simultánea a este servidor requiere una CAL independiente. Es decir, en un momento dado, Windows 2000 Server puede admitir un número fijo de conexiones. Por ejemplo, si selecciona el modo de licencia de cliente Por servidor y cinco conexiones simultáneas, este servidor que ejecuta Windows 2000 Server puede tener cinco equipos (clientes) conectados a la vez.

[14] Tabla de asignación de archivos

Esos equipos no necesitarían licencias adicionales. **La licencia por servidor será el tipo de licencia elegido para el servidor de este CTI.**

4.4.3 Elección de más de un Sistema Operativo en un equipo

Es posible configurar un equipo de manera que cada vez que se reinicie sea posible elegir entre varios sistemas operativos diferentes. Durante el reinicio, puede aparecer una pantalla durante un número especificado de segundos, lo que le permitirá seleccionar entre los sistemas operativos. Puede especificar un sistema operativo predeterminado que se ejecutará si no se realiza ninguna selección durante el proceso de reinicio. La razón para configurar un equipo de manera que pueda elegir entre dos o más sistemas operativos al iniciar dicho equipo, es permitir el uso de aplicaciones que únicamente se ejecutan en un determinado sistema operativo.

4.4.4 Sistema de archivos

Los sistemas de archivos entre los que puede elegir son **NTFS**[15], **FAT**[16] y **FAT32**. NTFS siempre ha sido un sistema de archivos más eficaz que FAT y FAT32. Windows 2000 Server incluye una versión nueva de NTFS, con compatibilidad para una gran variedad de características, incluido **Active Directory**[17], que es necesario para los dominios, cuentas de usuario y otras características de seguridad importantes. Sin embargo, puede ser necesario tener una partición FAT o FAT32 en situaciones en las que debe configurar un equipo de manera que unas veces ejecute Windows 2000 y otras veces ejecute un sistema operativo anterior.

4.4.5 Planeación de las particiones de disco para nuevas instalaciones

La partición de disco es una manera de dividir el disco físico para que cada sección funcione como una unidad independiente. Al crear particiones, divide el disco en una o más áreas a las que se pueden dar formato para su uso por parte de un sistema de archivos, como FAT o NTFS. Las diferentes particiones suelen tener distintas letras de unidad (por ejemplo, C: y D:).

[15] Nueva Tecnología de Sistema de Archivos.
[16] FAT (File Allocation Table o "tabla de ubicación de archivos") es el principal sistema de archivos desarrollado para MS-DOS y Windows.
[17] Aplicación que forma parte de la instalación del Sistema Operativo de servidor, controla todos los elementos de configuración del equipo.

Una **partición principal**, o partición de sistema, es una partición en la que es posible instalar los archivos necesarios para cargar un sistema operativo, como Windows 2000. Cuando realice una instalación nueva de Windows 2000 Server, podrá seleccionar la partición en la que desea llevar a cabo la instalación. Si especifica una partición en la que ya existe otro sistema operativo, se le pedirá que confirme su elección.

4.4.6 Selección de componentes para instalar

Windows 2000 Server incluye una gran variedad de componentes principales, incluidas numerosas herramientas administrativas. Además, puede elegir entre un gran número de componentes opcionales que amplían la funcionalidad. Se puede instalar estos componentes durante la instalación o agregarlos después **(con agregar o quitar programas del Panel de control)**. Cuantos más componentes se elijan, más posibilidades se ofrecerán en el servidor. Sin embargo, se debe elegir únicamente los componentes que se necesite, ya que cada componente requiere espacio adicional en el disco.

Servidor DHCP, DNS o WINS (en una red TCP/IP)	Protocolo de configuración dinámica de host (DHCP), DNS o el Servicio de nombres Internet de Windows (WINS); todos forman parte de los Servicios de red.
Administración centralizada de redes	Herramientas de administración y supervisión Servicios de instalación remota Servicios de Terminal Server (modo de administración remota)
Autenticación y comunicación segura	Servicio de autenticación Internet (parte de los Servicios de red) Servicios de Certificate Server
Acceso a archivos	Servicio de Index Server Almacenamiento remoto Otros servicios de archivos e impresión en red (compatibilidad con sistemas operativos Macintosh y UNIX)
Acceso a impresión	Otros servicios de impresión y archivos de red (compatibilidad con sistemas operativos Macintosh y UNIX)
Servicios de Terminal Server	Servicios de Terminal Server (modo de servidor de aplicaciones); Licencias de Servicios de Terminal Server
Compatibilidad con aplicaciones	Message Queue Server Control de admisión QoS (parte de los Servicios de red)
Infraestructura de Internet (Web)	Servicios de Internet Information Server Servicio ILS de Site Server (parte de los Servicios de red)
Compatibilidad con acceso telefónico	Kit de administración de Connection Manager y Servicios de punto de conexión (parte de las Herramientas de administración y supervisión). Tenga en cuenta que el Servicio de enrutamiento y acceso remoto se incluye como elemento principal de Windows 2000 y no es necesario instalarlo como componente.
Comunicaciones multimedia	Servicios de Windows Media

Tabla 4.4 Componentes opcionales de configuración

4.4.7 Red TCP/IP, Direcciones IP y resolución de nombres

TCP/IP es el **protocolo de red que proporciona acceso a Internet**. Es el protocolo que se utiliza en la mayor parte de los servidores, aunque también puede utilizarse en adaptadores de redes diferentes o adicionales. Para utilizar TCP/IP, hay que asegurarse de que el servidor dispone de una **dirección IP**, ya sea dirección **dinámica** o automática proporcionada mediante software, o una dirección **estática** obtenida y establecida por el usuario.

4.4.8 Elección entre grupos de trabajo y dominios

Los dominios son una característica importante de Windows 2000 Server. Un ***dominio*** es una agrupación de cuentas y recursos de red bajo un mismo nombre y límite de seguridad. Un ***grupo de trabajo*** es más básico y está diseñado únicamente para ayudar a los usuarios a encontrar elementos como impresoras y carpetas compartidas dentro del grupo.

Los dominios facilitan al administrador el control del acceso a los recursos y el seguimiento de los usuarios. Por tal motivo en el CTI se contará con el correspondiente dominio que administrará los recursos informáticos.

El elemento principal dentro del sistema operativo que controla los componentes anteriores es llamado **Active Directory** e incluye las características siguientes:

- **Administración simplificada** de información de los recursos de red y de usuario.
- **Directiva de grupo**, que se puede utilizar para establecer directivas que se aplican en un sitio, un dominio o una unidad organizativa dada de Active Directory.
- **Directivas de seguridad y de autenticación**, donde el objetivo de las directivas de seguridad es definir los procedimientos de configuración y administración de la seguridad del entorno.
- **Consolidación de directorios**, mediante la que puede organizar y simplificar la administración de usuarios, equipos, aplicaciones y dispositivos, así como facilitar a los usuarios la búsqueda de la información que necesitan.

Ya instalado el sistema operativo, después de seguir los pasos descritos anteriormente, se procede a crear el dominio respectivo e instalar el **active directory**, esto, mediante la ejecución del comando **dcpromo** que realizará el proceso anterior mediante una guía paso a paso:

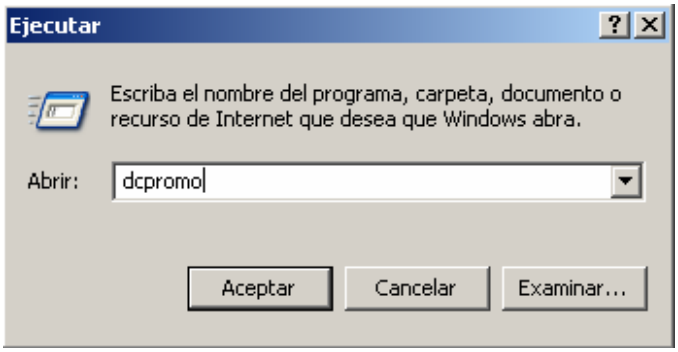

Figura 4.4 Promoción del dominio e instalación del active directory

Una vez instalado el **active directory**, se podrá acceder mediante el **botón de inicio** en el escritorio a las **herramientas administrativas,** que contienen los parámetros de configuración:

Figura 4.5 Herramientas administrativas de Windows 2000 Server

La configuración completa del servidor se puede realizar mediante un proceso que guía **paso a paso** sobre cada uno de los elementos de administración, este se encuentra dentro de las **herramientas administrativas** y contiene los siguientes elementos:

Figura 4.6 Configuración del servidor

4.4.9 Antivirus para Servidores

En el caso del **antivirus** se contempla uno llamado **NOD32,** se eligió por ser es un antivirus de calidad y eficacia realmente impresionantes, con una certeza prácticamente absoluta de que en cada uno de sus análisis detectará cualquier virus conocido y, mediante una heurística compleja, analiza todo tipo de archivos.

En conjunto se trata de un antivirus de primera calidad, compitiendo entre los mejores en la mayoría de herramientas que posee, aunque en la velocidad y la total detección basa toda su potencia, destacando del resto. Entre las nuevas características de esta versión se encuentra la detección de aplicaciones spyware, un mejor análisis de archivos auto-extraíbles, compatibilidad con mayor número de versiones de Outlook, poder pausar y reanudar un análisis, entre otras tantas más.

En la imagen siguiente se presenta la configuración del antivirus, en este caso se seleccionan el(los) disco(s) duro(s) que el sistema analizará automáticamente:

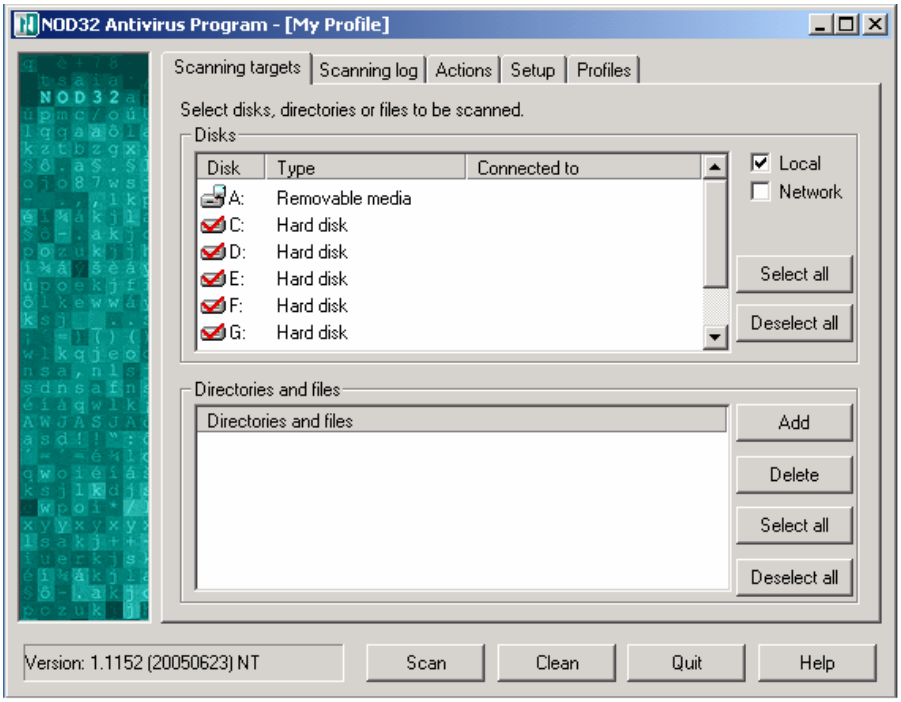

Figura 4.7 Configuración del antivirus

En la siguiente figura se presenta los objetos a diagnosticar, así como los métodos de escaneo:

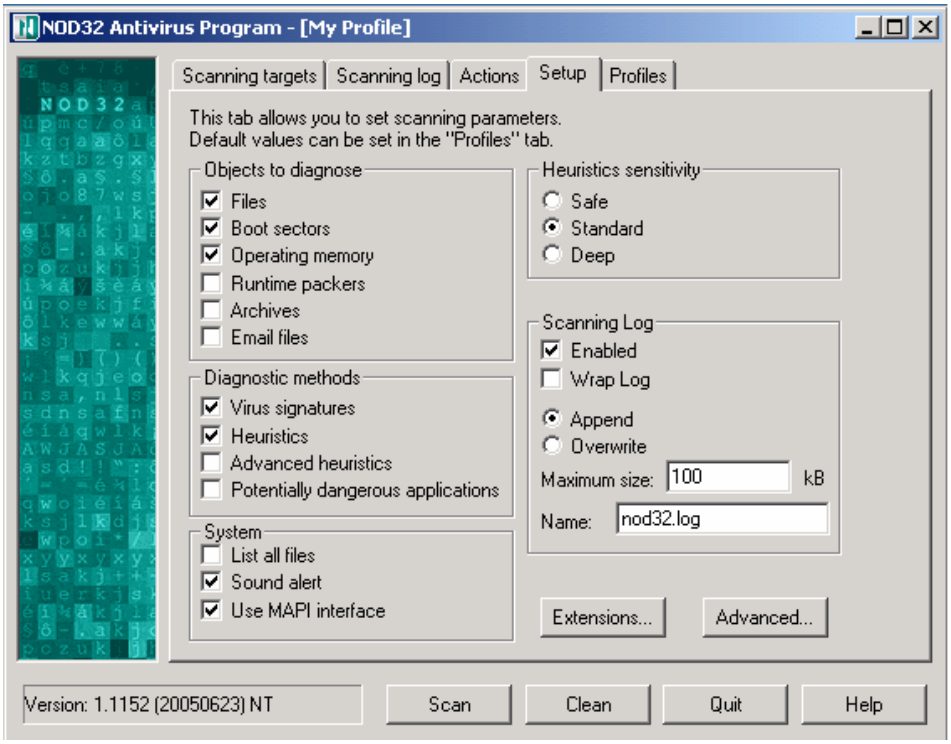

Figura 4.8 Configuración del antivirus

4.5 Configuración de los equipos desktop

En la siguiente gráfica se puede ver una lista con la paquetería mencionada al principio de este capítulo, está paquetería se instalará en todos los equipos desktop; para los fines de este trabajo de tesis, se omitirá la explicación sobre la instalación de cada una de las aplicaciones para pasar con la configuración interna de los equipos.

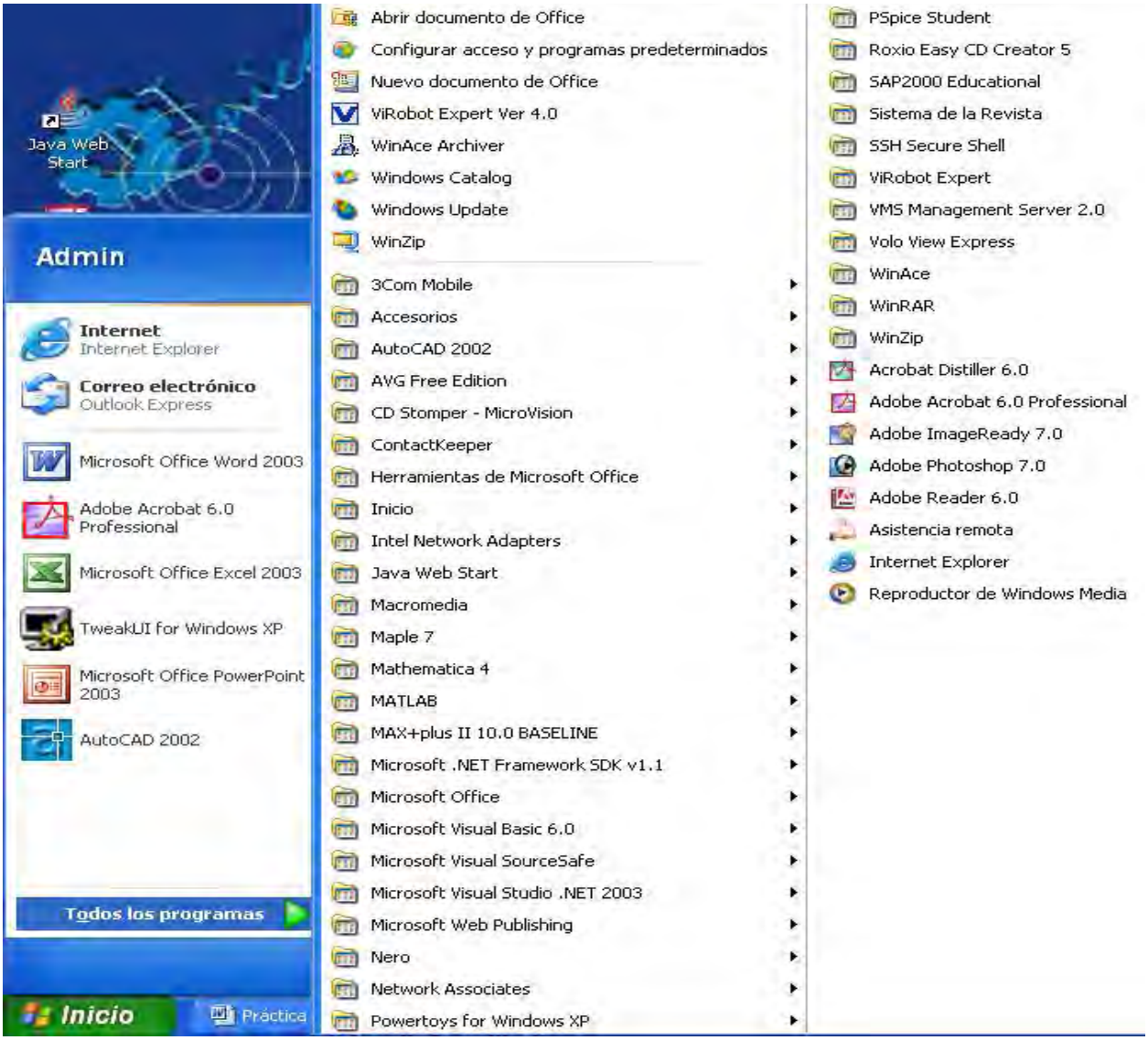

Figura 4.9 Paquetería instalada en los equipos de escritorio

Dado que los equipos contarán con el sistema operativo preinstalado, bastará con instalar la paquetería requerida con anterioridad.

4.5.1 Tipos de cuentas de usuario

Estas se configuran en el apartado de **cuentas de usuario** dentro del **panel de control**. Se contará con **2 cuentas** principales, la primera que es de **administración** para personal exclusivo del CTI y una segunda cuenta que tendrá privilegios de **usuario avanzado**, la que permite a los usuarios trabajar perfectamente pero evita que realicen cambios en la configuración de los equipos.

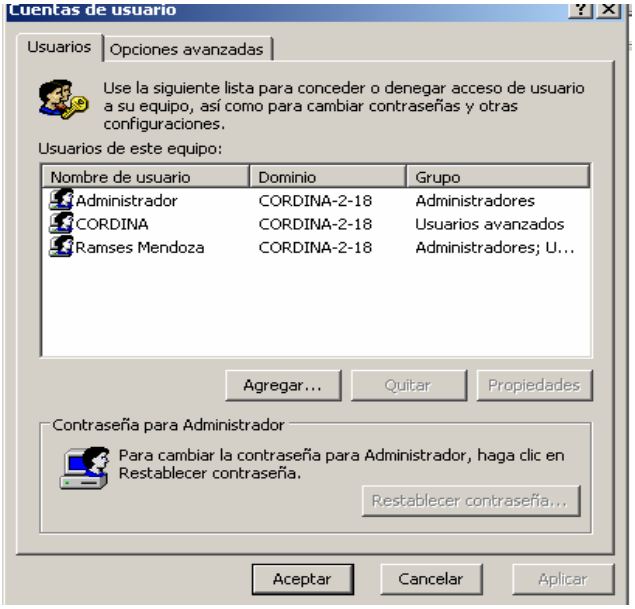

Figura 4.10 Apartado para creación de cuentas de usuario

4.5.2 Antivirus para clientes

Los equipos clientes contarán con un antivirus propio para equipos desktop, se eligió el antivirus **AVG** debido a que brinda una combinación única de rápidos métodos de detección y máxima protección en múltiples niveles.

Figura 4.11 Programa antivirus

Después de que el programa haya copiado todos los archivos de instalación, comenzará de forma automática un asistente para completar la configuración básica del mismo, con el fin de adaptarlo a las preferencias y necesidades del CTI.

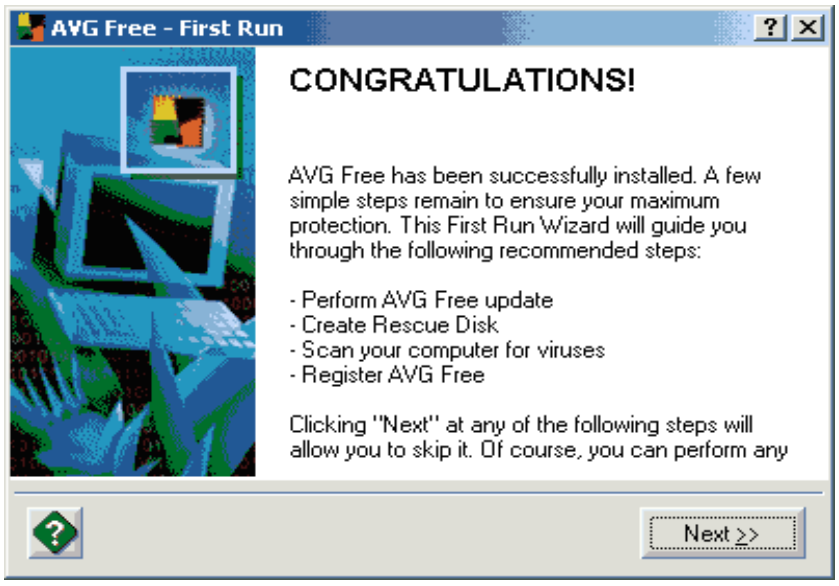

Figura 4.12 Configuración del antivirus

Lo primero es la actualización de la definición de virus, el programa nos sugiere conectarnos al servidor para comprobar si hay disponible una última versión de actualización. El programa pregunta si el archivo de actualización debe obtenerlo desde Internet o desde una carpeta local del disco duro. El programa conectará, mostrará las versiones encontradas y por último al dar clic en **UPDATE**. Se vera la siguiente ventana de actualización.

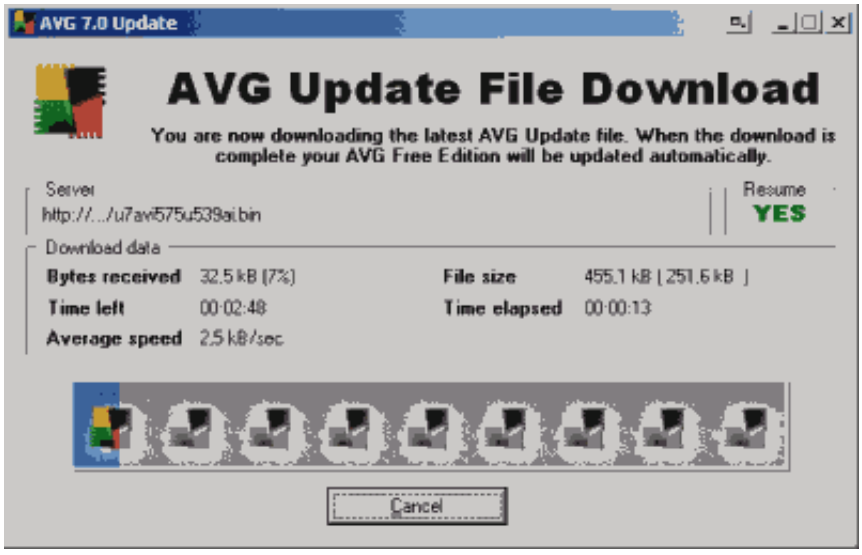

Figura 4.13 Actualización de la lista de definiciones de virus

Es muy recomendable tener un disco de rescate en caso de infección de virus. El disco ayudará a eliminarlo y recuperar el control del sistema. La creación del mismo es automática y es preferible crear el disco de inicio en este punto.

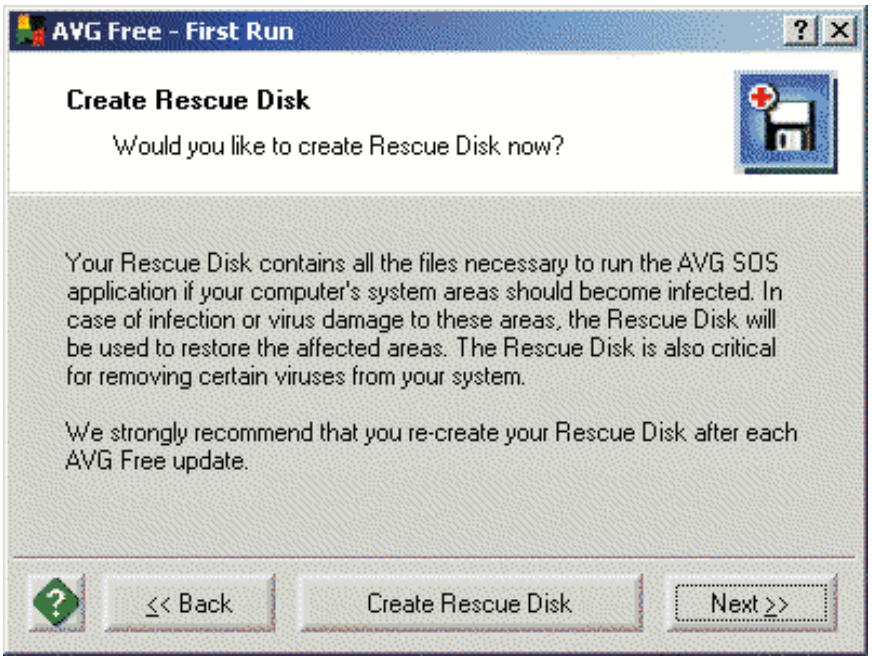

Figura 4.14 Creación del disco de rescate

La siguiente ventana sugiere realizar un escaneo de la computadora completo, es decir, buscar posibles virus en todas las unidades.

Figura 4.15 Escaneo en búsqueda de virus

4.5.3 Firewall para equipos cliente

Todos los equipos clientes contarán con un **firewall del tipo lógico** (mediante software), este firewall forma parte del sistema operativo (Windows XP) ya que se instala junto con una actualización crítica del sistema llamada **Service Pack 2 para XP**, para acceder el mismo, hay que abrir el panel de control y acceder al **centro de seguridad** como es mostrado en la gráfica siguiente:

Figura 4.16 Centro de seguridad de Windows XP

El centro de seguridad de Windows, controla el **funcionamiento y configuración del firewall**, manejando todas aquellas restricciones o permisos de acceso para todos los programas que tienen interacción con Internet, también se establece la periodicidad de descarga de las **actualizaciones automáticas** del sistema operativo y finalmente, se gestiona el control de la protección antivirus para el caso de que el equipo no cuente con un programa antivirus independiente.

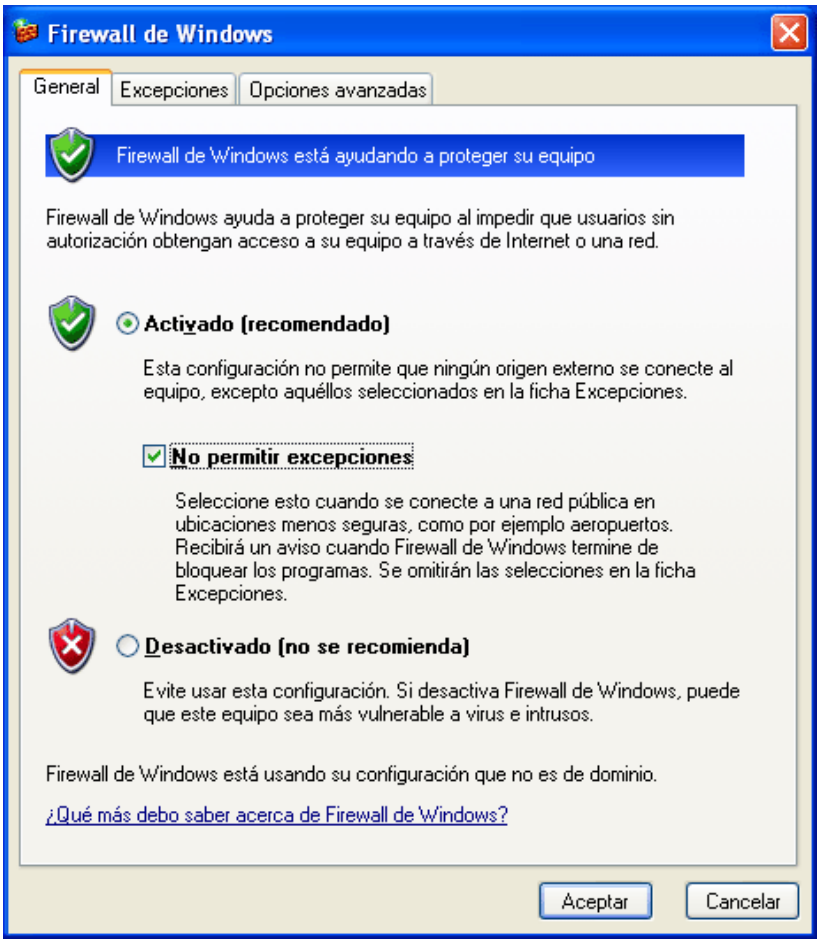

Figura 4.17 Muro de Fuego incluido en el Sistema Operativo

La protección es exactamente la misma para todos los equipos de escritorio y poseerán tanto la misma paquetería como la misma configuración.

4.5.4 Configuración de la red local

Para que los equipos tengan salida a Internet deberán de estar conectados por su tarjeta de red, sea esta alámbrica (a un conector RJ45) o inalámbrica (a un punto de acceso), una vez realizado lo anterior, se asignará una dirección IP distinta a cada uno de los equipos, manejando claro esta, un adecuado control y registro de las direcciones IP, con esto se evitará que exista un conflicto con direcciones repetidas que eviten que los equipos puedan tener conexión a Internet o compartir ciertos recursos de red.

El método para asignar una dirección IP consiste en abrir la ventana de **conexiones de red** que se encuentra en el **panel de control**, dando doble click en el icono de la **conexión de área local**, aparecerán las **propiedades de la conexión** mostrada en la siguiente ventana:

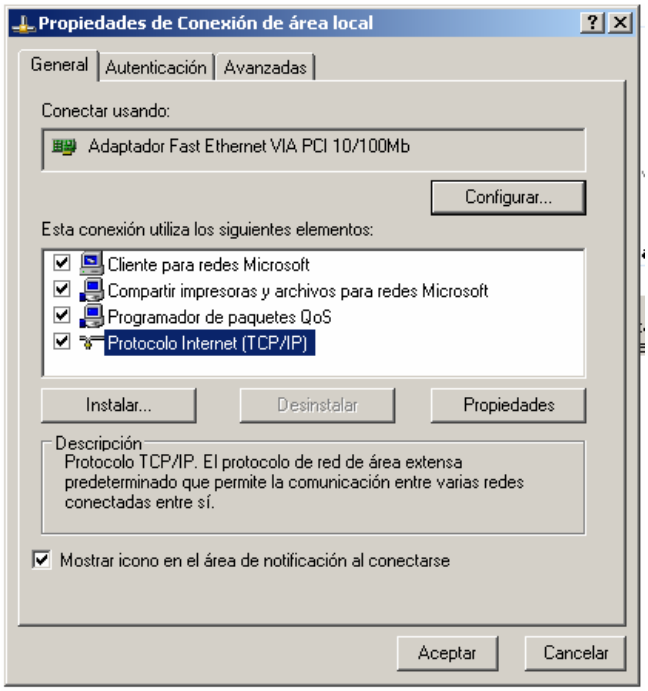

Figura 4.18 Propiedades de la conexión de área local

Se seleccionarán las **propiedades** del **protocolo de Internet (TCP/IP),** con lo que aparecerá la ventana siguiente:

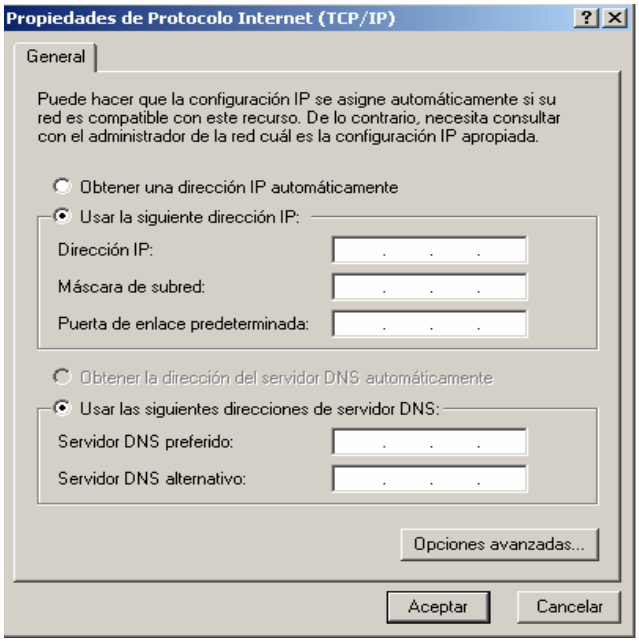

Figura 4.19 Propiedades del protocolo de Internet (TCP/IP)

La asignación de la dirección IP, así como los demás elementos de red (mascara de subred, puerta de enlace, servidor DNS, etc.) serán fijados por el administrador del lugar.

4.5.5 Salida a Internet

La salida a Internet para el CTI será provista por **DGSCA**[18]**,** la cuál, mediante un cable de fibra óptica llega a un nodo en la zona de posgrado de la Facultad de Ingeniería, a partir de este nodo, la señal se distribuye a los diferentes edificios de la zona por medio de cable RJ45 a través de un Router, uno de estos cables de red es dirigido al CTI, contando con una toma principal de la señal, esta se distribuye al Punto de Acceso y a los diferentes equipos por medio de la instalación de red cableada que se encontrará a la espera en el caso de que la red inalámbrica no funcione.

4.6 Configuración del servidor de impresión

Un servidor de impresión es una computadora de aplicación específica que gestiona las impresoras y solicitudes de servicios de impresión, además, permite que múltiples usuarios compartan una impresora en red.

Para ahorrar recursos y sacar el máximo provecho de la red local se instalará una impresora para brindar el servicio de impresión, para esto, se acondicionará un equipo de escritorio con las mismas características, referentes a configuración, paquetería y directivas de seguridad que los equipos destinados para uso de los usuarios, con la única diferencia que en este equipo no se podrán realizar tareas más allá que la de imprimir los trabajos exclusivos del usuario y con fines académicos.

El primer paso a realizar es conectar la impresora al equipo de cómputo mediante un cable al puerto LPT de la impresora, encender el equipo e instalar el controlador correspondiente para que exista comunicación entre ambos elementos para llegar a la pantalla mostrada a continuación:

[18] Dirección de Servicios de Cómputo Académico, UNAM

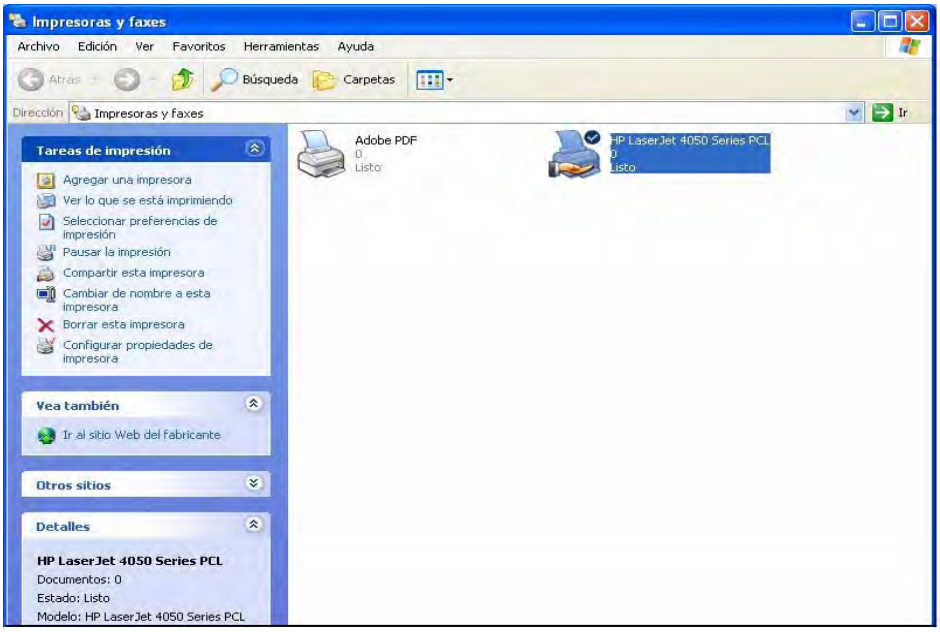

Figura 4.20 Instalación de la impresora en el servidor de impresión

A continuación se deben configurar ciertos parámetros, como la disponibilidad de tiempo para imprimir, prioridad con la cola de impresión y algunas opciones extras:

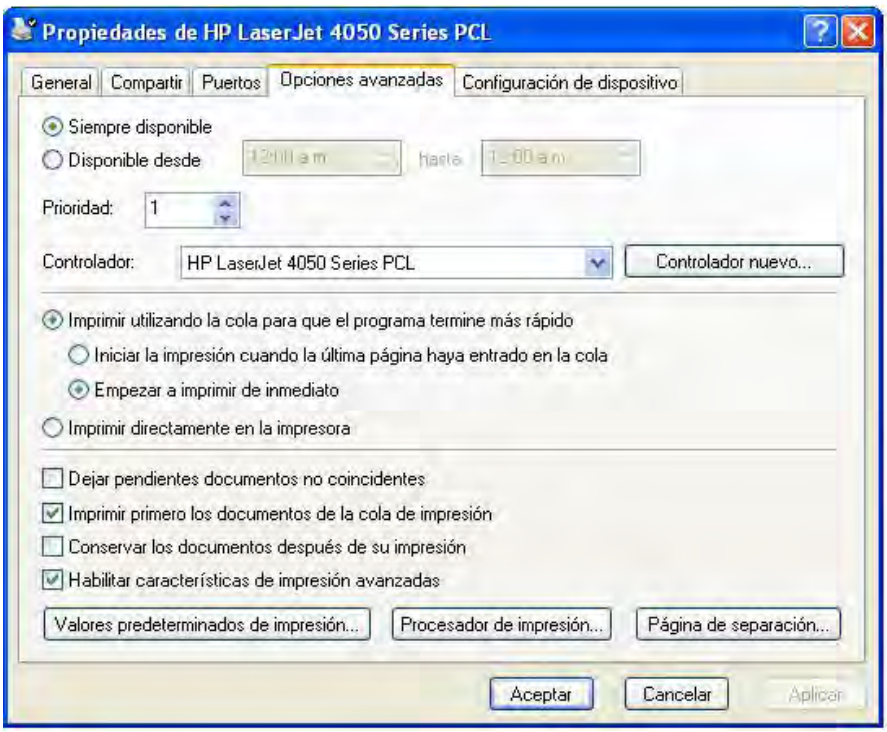

Figura 4.21 Parámetros de configuración de la impresora

Finalmente para los usuarios de equipos portátiles se brindará la opción de imprimir desde sus propios equipos, para ello, la impresora se encontrará dentro de un recurso compartido de la red local permitiendo que sólo usuarios de laptops puedan imprimir sus trabajos con tan sólo conectarse al servidor de impresión que se encontrará dentro de un grupo de trabajo definido.

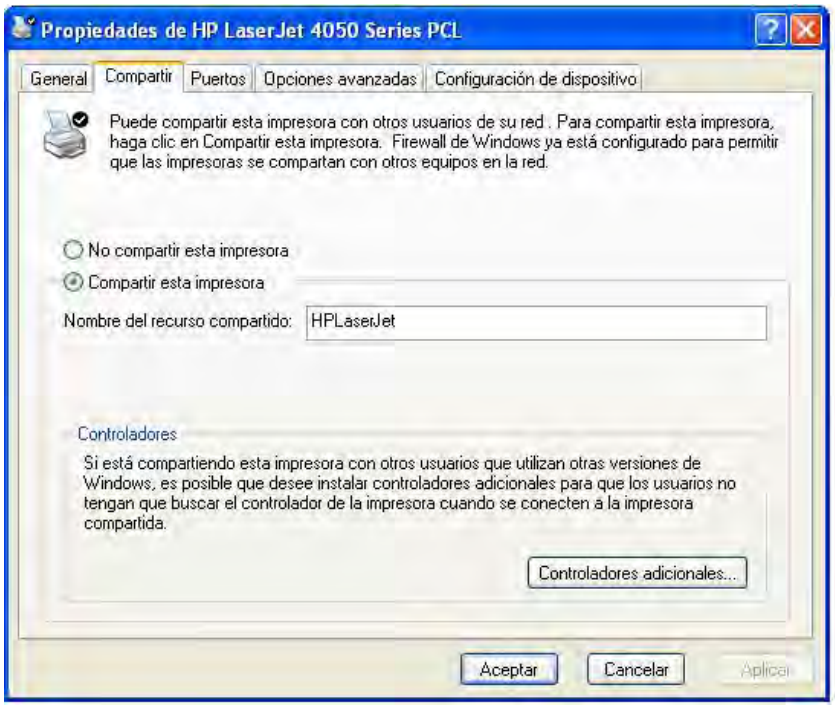

Figura 4.22 Propiedades para compartir una impresora en red

Los usuarios que deseen imprimir y se encuentren utilizando un equipo de escritorio, deberán desocupar el equipo y notificar al personal la necesidad de imprimir un documento para poder hacer uso del equipo de impresión.

4.7 Configuración del punto de acceso

El Punto de Acceso es el dispositivo que brinda la señal de Internet, así como la comunicación entre todos los medios de la red local, el dispositivo se encontrará en un lugar elevado dentro del CTI para poder recibir y transmitir una señal apropiada hacia las antenas de las tarjetas de red inalámbricas. El Punto de Acceso estará conectado por una parte a una **toma de corriente** y por otro lado a un equipo de cómputo mediante un **cable RJ45 a la tarjeta de red** del mismo que administra todos los aspectos de configuración y seguridad.

El sistema operativo que posee el equipo de cómputo se trata de un sistema tipo **Libre UNIX** descendiente del **BSD** UNIX de Berkeley que ha evolucionado para convertirse en uno de los sistemas UNIX más seguros de la actualidad. Las claves de **OpenBSD**[19] son: portabilidad, cumplimiento de normas y regulaciones, corrección del código, seguridad proactiva y criptografía integrada.

Para montar un Punto de Acceso no son necesarias máquinas potentes ni de última generación. Básicamente tendremos que asegurarnos que se cumplan los requisitos mínimos para hacer funcionar la tarjeta de red. La configuración del Punto de Acceso brinda ciertos parámetros a la tarjeta de red y pone en marcha el demonio ***DHCP***[20] que acompaña a la instalación base de OpenBSD.

Hay una serie de valores que serán variables en cada instalación. Los definimos a continuación:

- $IP: Dirección de red del nodo
- $NET: Dirección de la red del nodo
- $MASK: Máscara de red del nodo
- $SSID: Identificador para la red wireless
- $CHAN: Canal (dependiendo del país puede haber restricciones)
- $NAME: Nobre del nodo
- $TX: Tasa de transmisión

En cada instalación se reemplazarán estas variables por su valor correspondiente. La tarjeta de red puede configurarse en la instalación como una tarjeta de red normal, con lo que posteriormente tendremos que añadir parámetros extra por ser una tarjeta WLAN. Los parámetros de configuración concernientes a la seguridad brindada por el Punto de Acceso son exclusivos del administrador del CTI, por lo que hay que tener en mente el no olvidar este importante paso en el establecimiento de algún CTI con estas características.

[19] BSD son las iniciales de Berkeley Software Distribution (en español, Versión de Software Berkeley) y se utiliza para identificar un sistema operativo derivado del sistema Unix nacido a partir de las aportaciones realizadas a ese sistema por la Universidad de California en Berkeley.

[20] Protocolo de Configuración Dinámica de Host. Servidor que asigna direcciones IP de manera automática de entre un conjunto de direcciones disponibles.

4.8 Configuración de las tarjetas de red

PASO # 1

Apague el equipo e instale la tarjeta de red, teniendo cuidado con la antena, conéctela en un slot o ranura libre en el equipo. Hay que fijar la antena en la base que tiene y colocarla en un lugar propicio para recibir la señal. Al encender el equipo, este detectará la tarjeta e indicará que hay un hardware desconocido, mediante el CD-ROM se instalará el software correspondiente, en donde se seleccionará la segunda opción presentada en la pantalla siguiente:

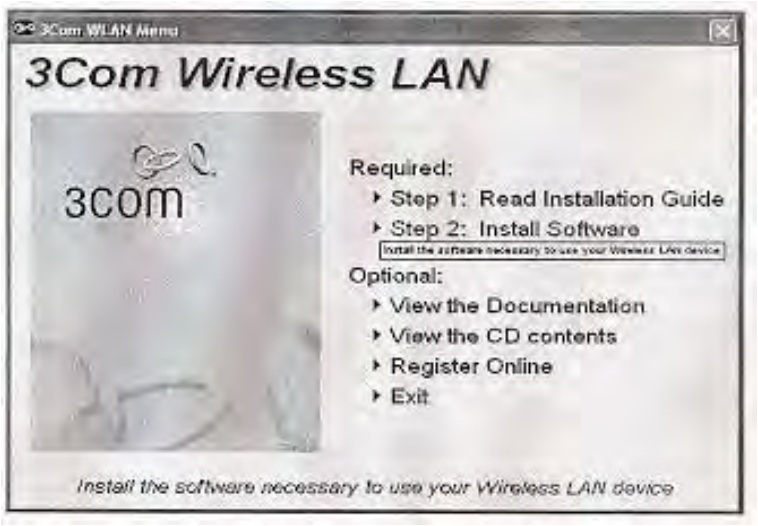

Figura 4.23 Menú de opciones de 3COM

PASO # 2

Después de la instalación del software deberá aparecer un icono con el logotipo de la compañía que fabricó el componente (dar doble click), este icono aparece en la barra de inicio, en el área de notificación y en el escritorio:

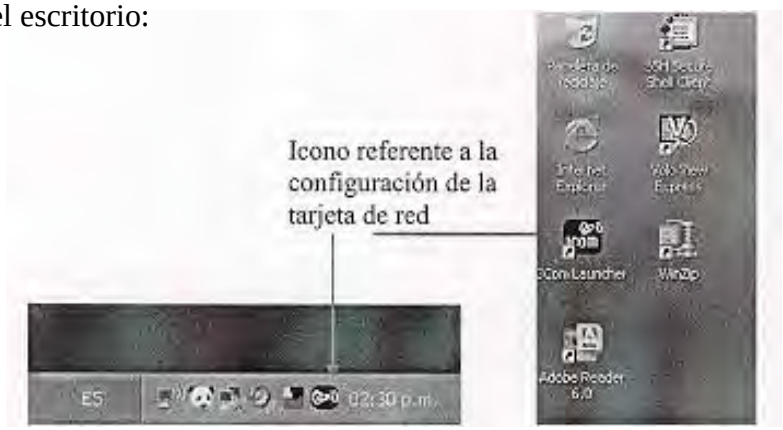

Figura 4.24 Iconos de la tarjeta de red

PASO # 3

Se pueden encontrar errores en la configuración del país, por lo que al instalar se podrá ver la siguiente pantalla en donde tenemos que seleccionar como país a México:

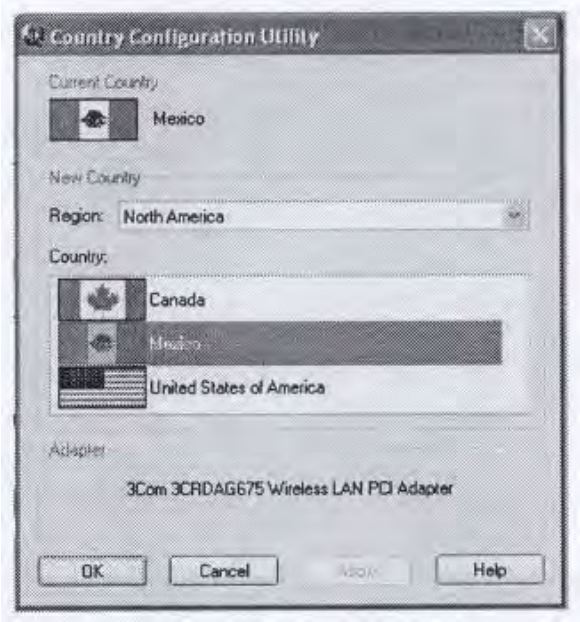

Figura 4.25 Utilería para la selección del país

PASO # 4

Al abrir la aplicación se verá una pantalla como la siguiente:

Figura 4.26 Aplicación para configurar el Punto de Acceso

Se creará un nuevo perfil de red, para ello presionaremos el botón ***"Create New Conecction":***

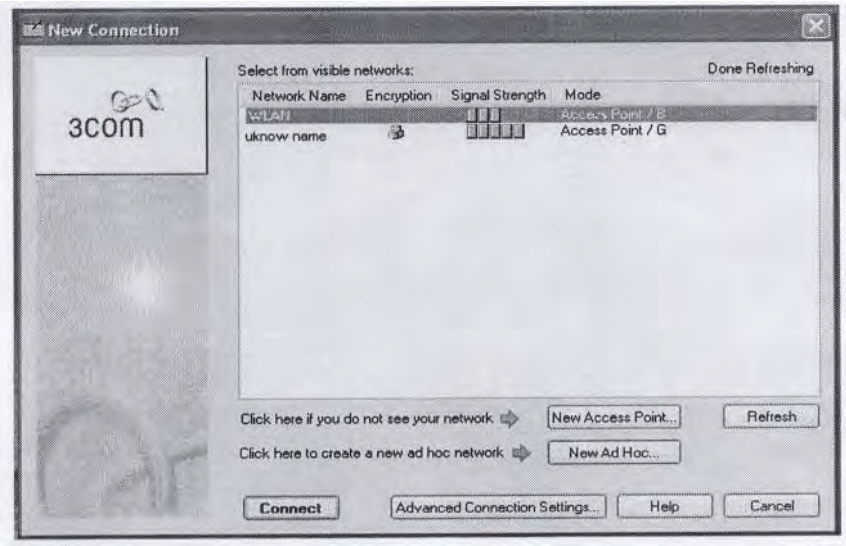

Figura 4.27 Creación de una conexión nueva

Se seleccionará la que posee la leyenda de ***"unknow name"*** ya que posee la señal más alta y corresponde a nuestra red.

PASO # 5

Seleccionaremos el renglón de ***"unknow name"*** y se dará clic en el botón de ***"Advanced Conecctions Settings"*** con lo que aparecerá la siguiente pantalla para dar un nombre a la red:

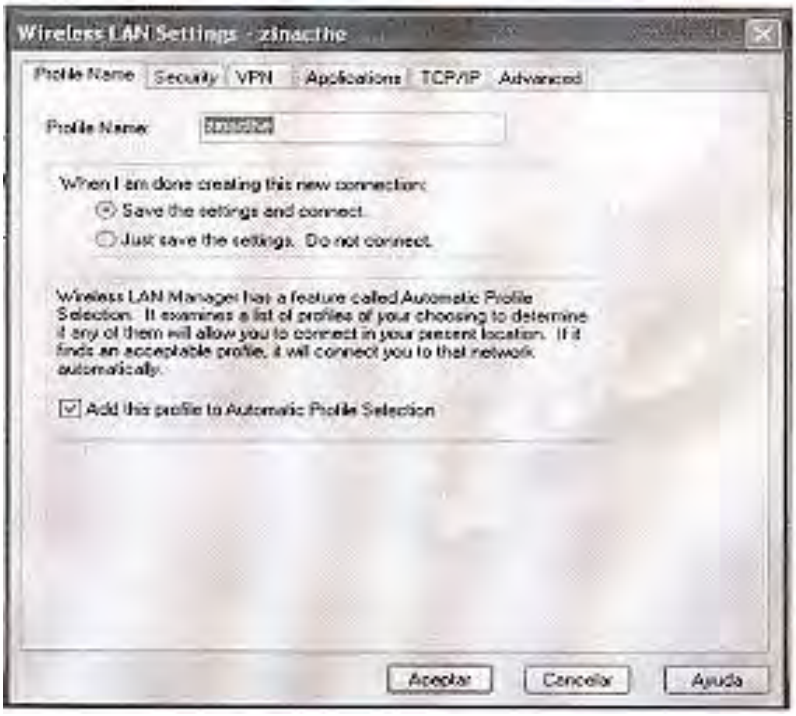

Figura 4.28 Perfil propio de la red inalámbrica

PASO # 6

En la pestaña de seguridad se configurará el grado de seguridad de la red, donde ingresaremos la información que se muestra en pantalla:

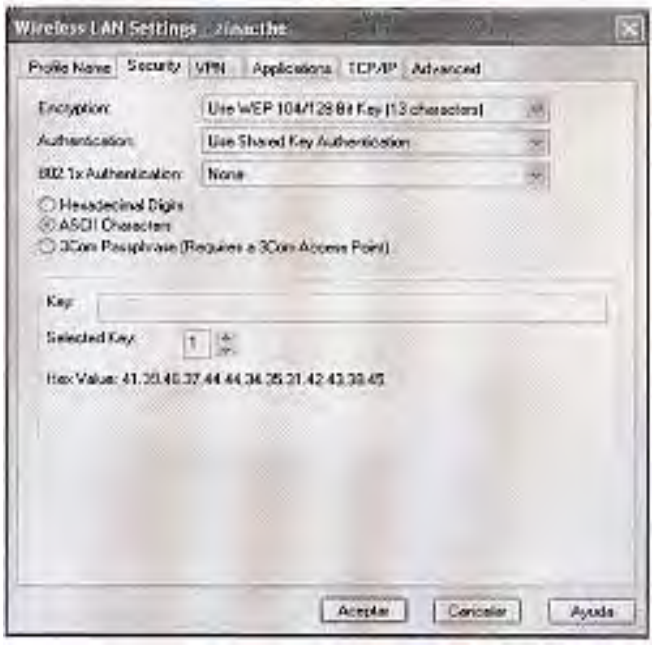

Figura 4.29 Tipo de seguridad otorgado a la red inalámbrica

NOTA: el campo **key** en donde se ingresa la llave de encriptación, es un elemento de seguridad.

PASO # 7

En la pestaña TCP/IP, se debe deseleccionar el radio: ***This network uses a DHCP Server.***

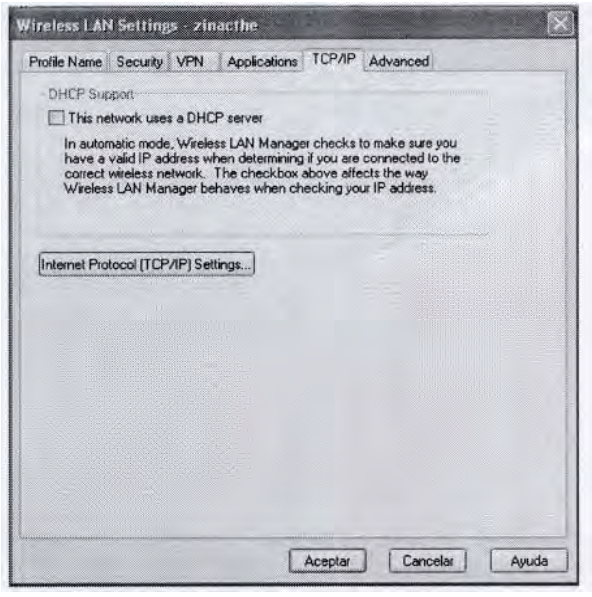

Figura 4.30 Configuración del DHCP

Presionar el botón ***Internet Protocol (TCP/IP) Settings…,*** para que aparezca la siguiente pantalla y verificar que se encuentre de la forma:

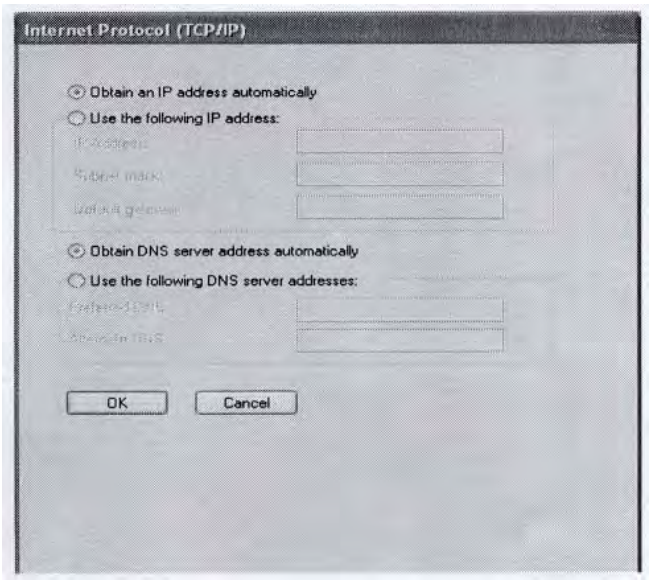

Figura 4.31 Protocolos TCP/IP

PASO # 8

Al dar clic en ***Ok*** en la ventana de ***Internet Protocol (TCP/IP)*** y aceptar en la ventana de ***Wireless LAN Settings,*** se mostrará la siguiente pantalla:

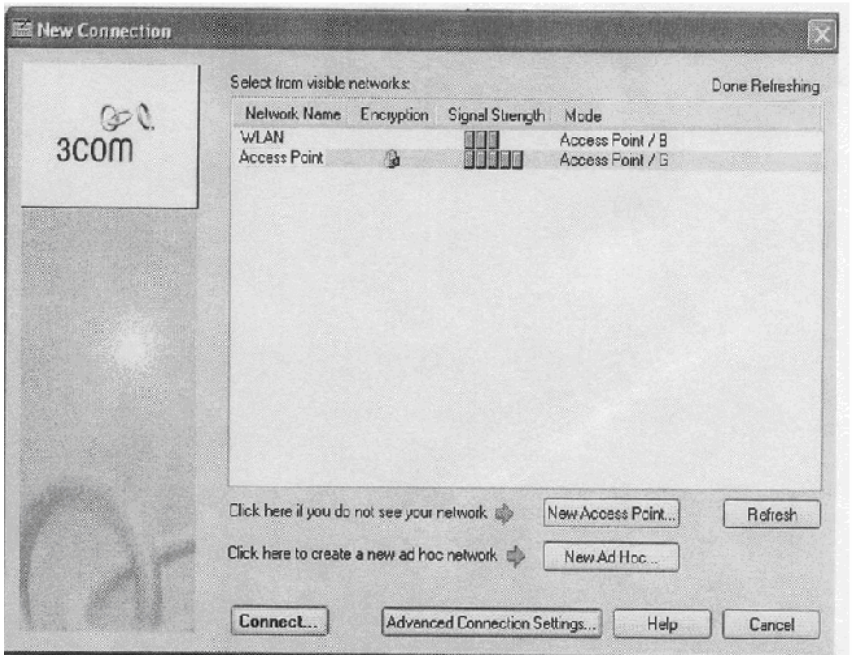

Figura 4.32 Red inalámbrica configurada

Cuando presionamos el botón ***Connect…,*** comenzará la búsqueda del perfil que se dio de alta, una vez realizado esto, se tendrá salida a Internet. Conjuntamente se debe configurar y verificar que la red predeterminada corresponda al perfil que se creo, para ello se abrirá el ***Profile Manager:***

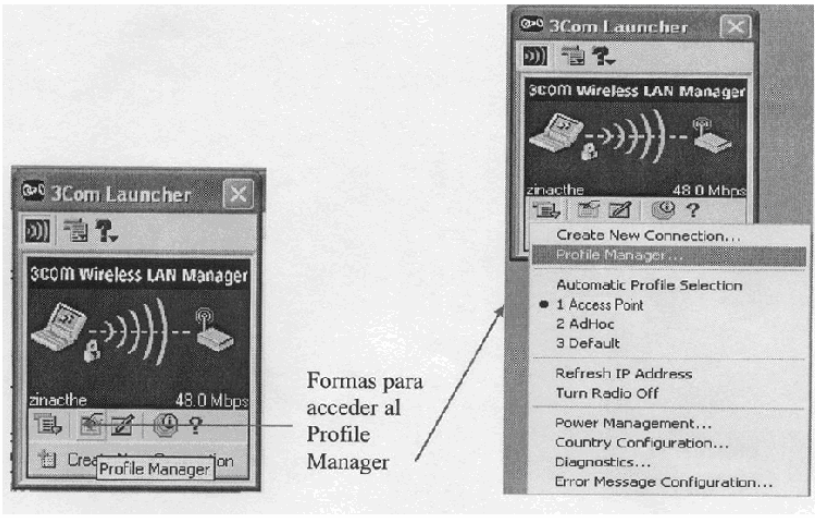

Figura 4.33 Acceso a la ventana de configuración

Seleccionar *la red que se utilizará* y deseleccionar ***Default*** que está seleccionada por defecto:

Figura 4.34 Selección de la red inalámbrica deseada

4.9 Configuración de las computadoras portátiles (Laptops)

Cuando un usuario requiera del servicio que brinda el CTI y se de el caso de que este lleve su equipo portátil se realizará el proceso descrito en el **punto 4.3** que habla sobre la red inalámbrica, en el equipo se configurará la conexión de red inalámbrica:

Figura 4.35 Conexiones de red en un equipo de cómputo portátil

Dentro de las conexiones de red y dependiendo del tipo de tarjeta inalámbrica que posean los equipos, se podrán detectar los diversos puntos de acceso disponibles en el área:

Figura 4.36 Conexiones inalámbricas detectadas por una tarjeta de red

Sólo bastará con seleccionar la red específica para el CTI, corroborando junto con un administrador del CTI que la configuración sea la adecuada y conectar el equipo como se muestra en las figuras siguientes:

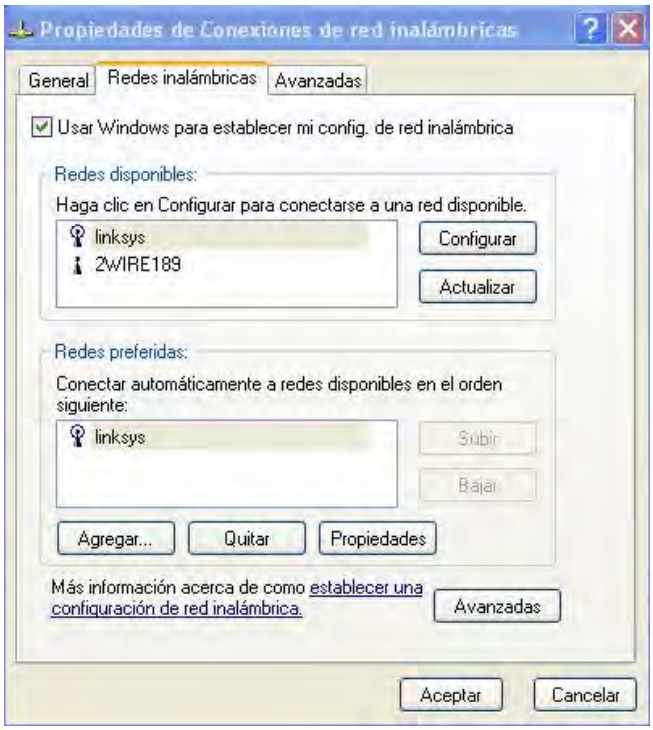

Figura 4.37 Propiedades de conexión de redes inalámbricas

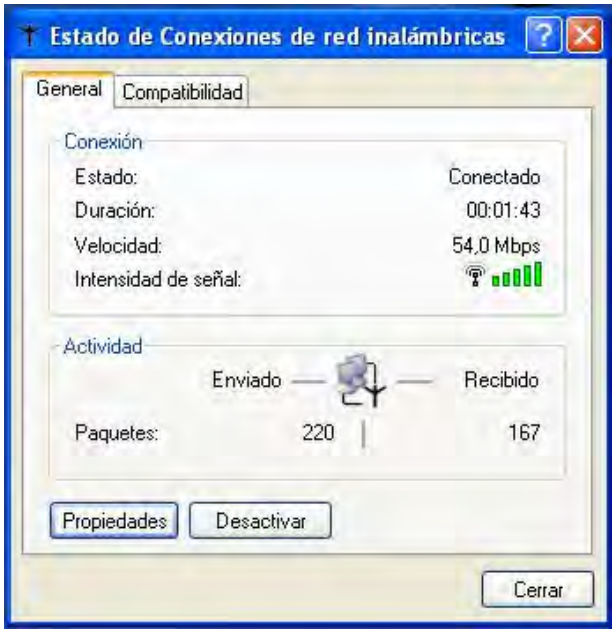

Figura 4.38 Estado de la conexión inalámbrica

4.10 Directivas de configuración y seguridad para equipos desktop

En un lugar con las características con las que contará este CTI, en donde los equipos de cómputo se encontrarán a disposición de todo tipo de personas, una medida de seguridad y prevención de los equipos son las directivas de configuración. La función principal de estas directivas es la de restringir configuraciones y accesos específicos de los equipos, básicamente, recursos a los que sólo un administrador puede tener acceso para mantener los equipos de cómputo en óptimas condiciones.

Existe un gran número de programas diseñados específicamente para administrar las directivas de configuración de los equipos de cómputo, entre ellos se encuentra una aplicación llamada **TweakUI**.[21]

Para poder acceder a los servicios disponibles para esta aplicación, basta con instalar el programa en cada uno de los equipos de cómputo, una vez instalado, se podrá acceder al mismo, desde el menú de inicio o dando doble clic en el icono en el escritorio, siempre y cuando se maneje desde una cuenta con privilegios de administrador, con lo anterior aparecerá la siguiente ventana:

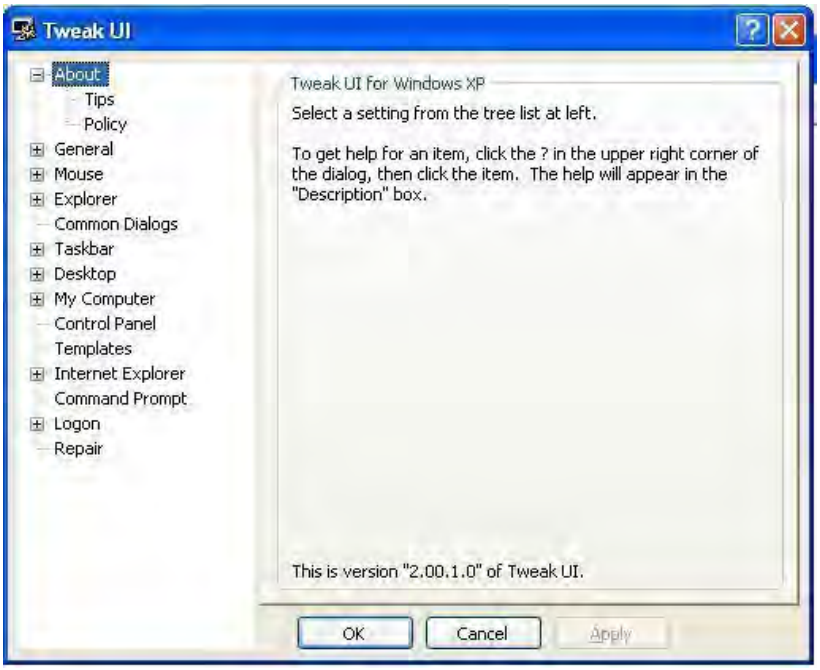

Figura 4.39 Pantalla inicial de la aplicación

[21] Aplicación que permite configurar parámetros ocultos de Windows, y que además de ser gratuito, tiene muchas opciones de restricción de parámetros.

Mediante esta ventana, se podrá ingresar a dos parámetros principales, el primero, acceder a las directivas de configuración, segundo, a la opción para seleccionar con que cuenta iniciará la computadora (en el caso de que exista alguna otra, aparte de la cuenta de administración); si ingresamos a la opción de "policy", al dar clic en el boton "Run Group Policy Editor" nos adentraremos en las directivas de configuración del equipo:

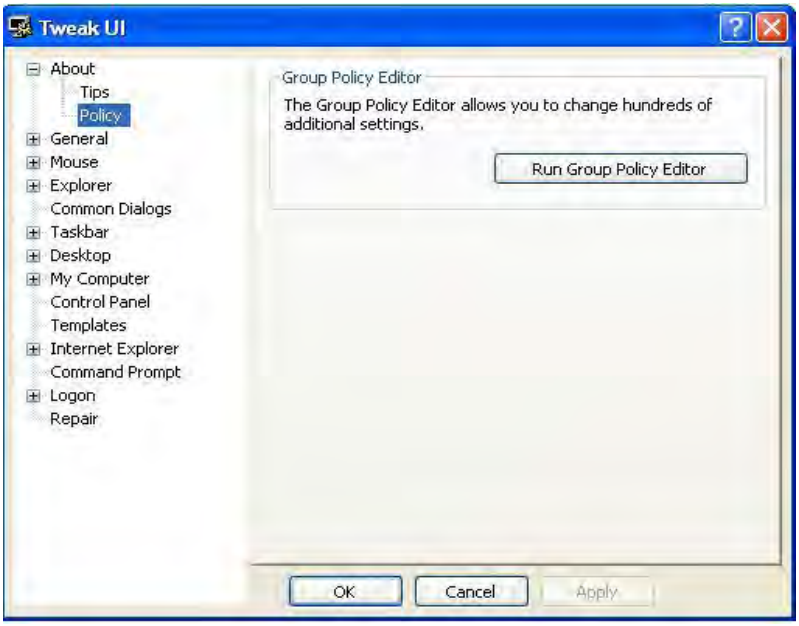

Figura 4.40 Ejecución del grupo de políticas de seguridad

En la siguiente ventana se encontrarán todos los parámetros del equipo que sean configurables para el tipo de usuario que hará uso de las computadoras:

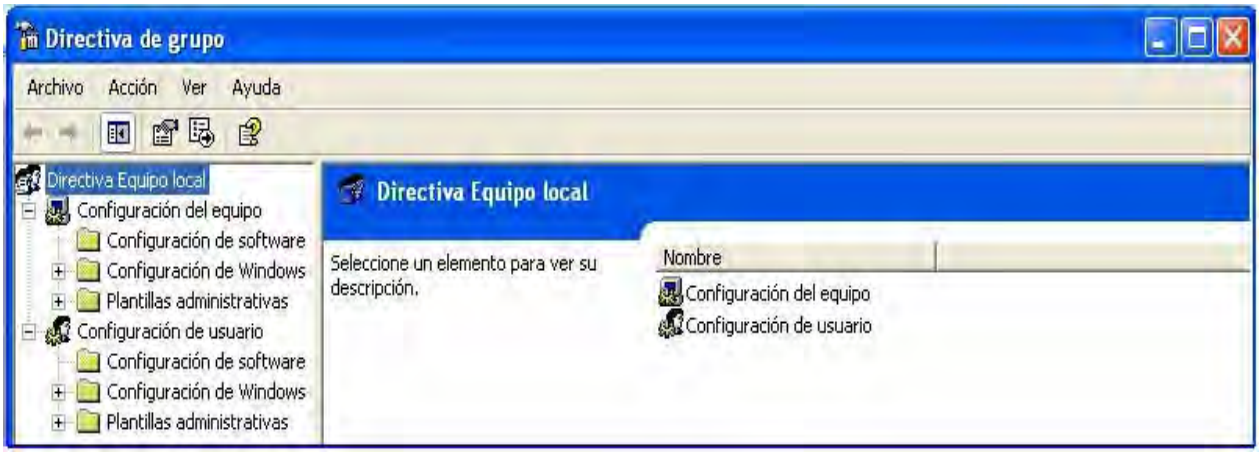

Figura 4.41 Ventana propia de las directivas de seguridad

Por lo general, en un CTI con estas características, los servicios a los que se impiden el acceso son, los componentes de Windows, acceso a los comandos del sistema, protocolos de red y servicios de impresión:

Figura 4.42 Directivas sobre plantillas administrativas

En cuanto al acceso y directivas para el uso de Internet, también se contemplan un conjunto de políticas que se enfocan al Internet Explorer (navegador de Internet para el sistema operativo Windows), de entre las que se desprenden las siguientes:

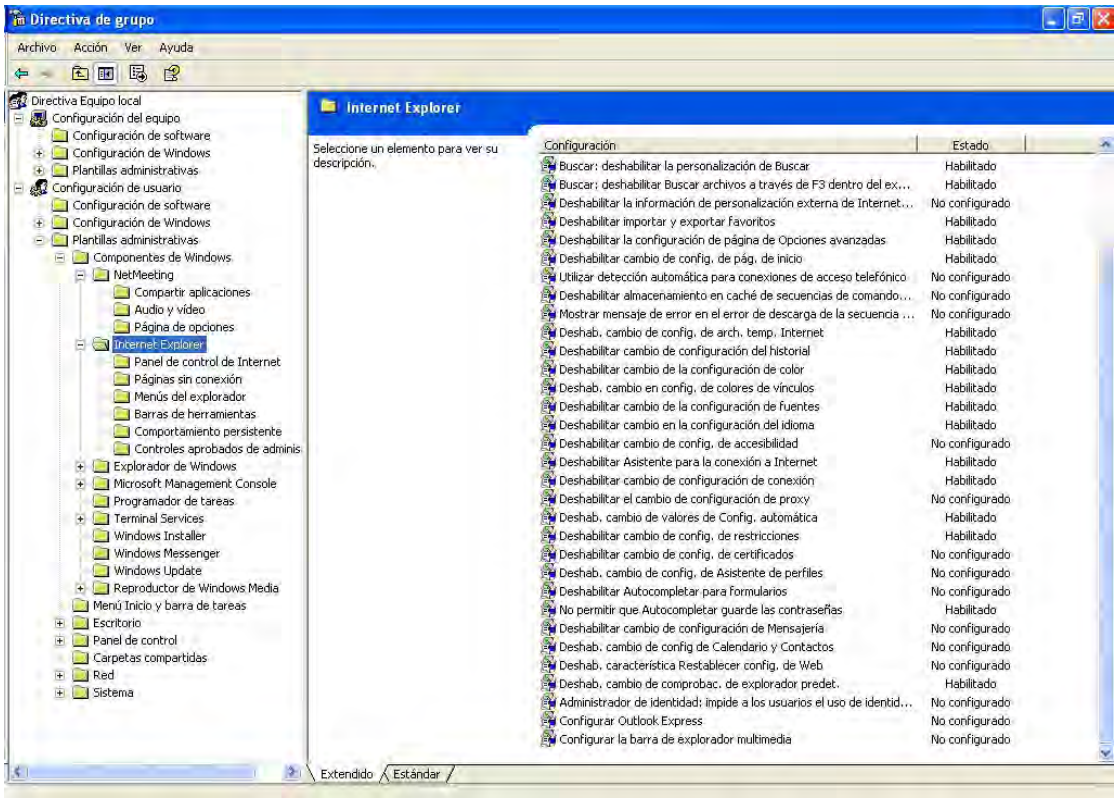

Figura 4.43 Directivas para el Internet Explorer

Por consiguiente, para el explorador de archivos de Windows, también se contemplan un conjunto de políticas, concerniente a la manipulación y administración de archivos, accesos al Panel de Control, unidades de sistemas ocultos, etc:

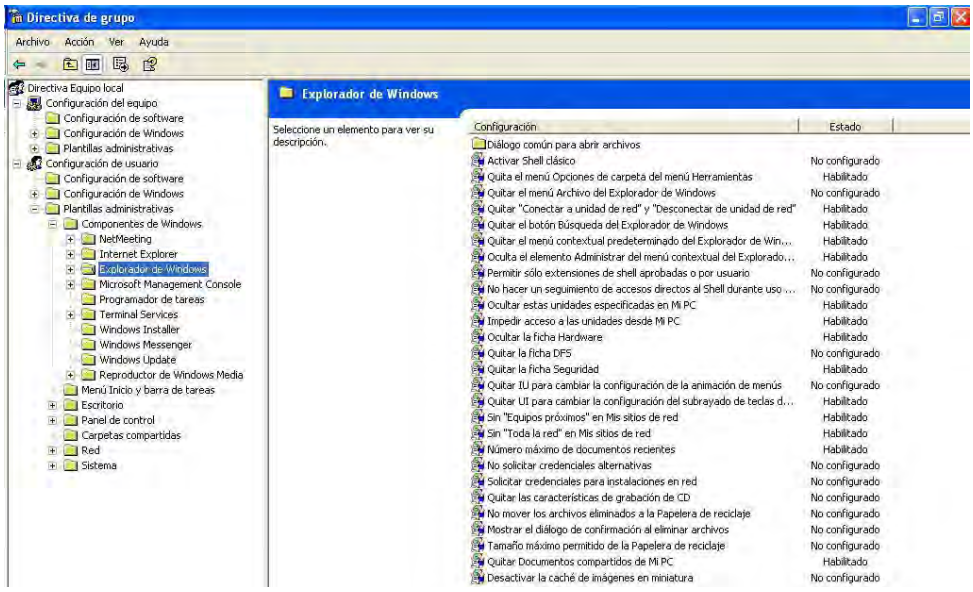

Figura 4.44 Directivas para el Explorador de Windows

Directivas acerca del menú de inicio y la barra de tareas de Windows:

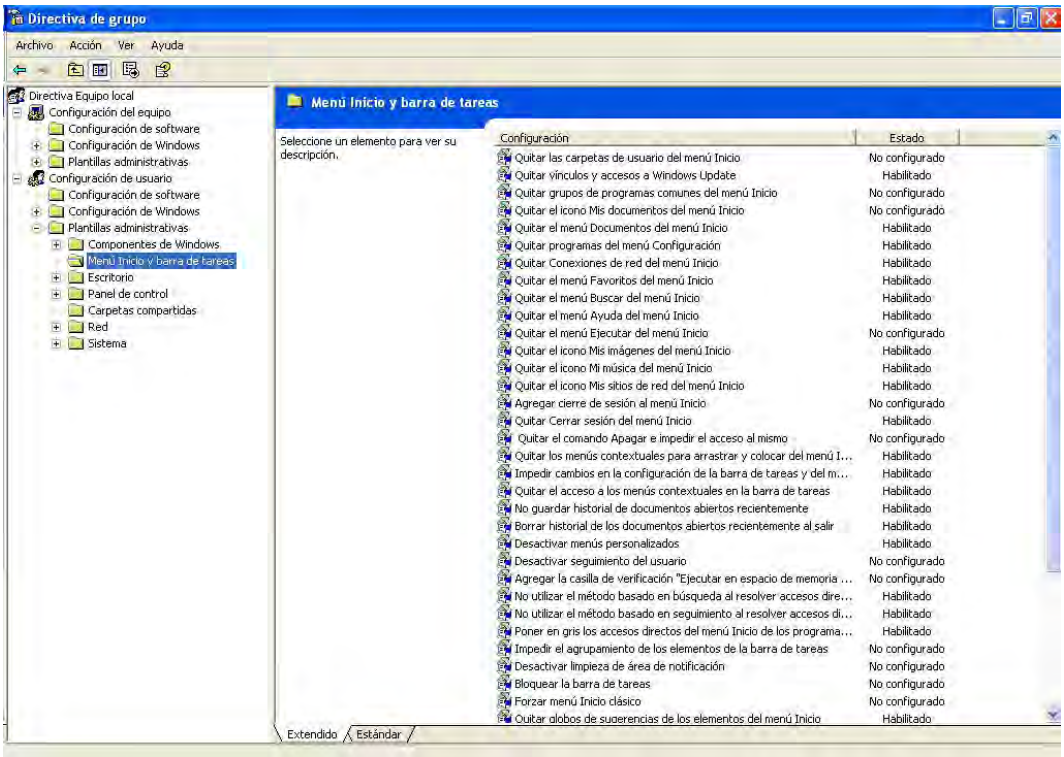

Figura 4.45 Directivas para el Menú de Inicio y la barra de tareas

Un punto importante en esta ventana es la activación y desactivación de los parámetros de configuración, a lo cual se podrá acceder habilitando o deshabilitando las directivas de grupo:

Figura 4.46 Ventana de activación y desactivación de las directivas de seguridad

Las directivas de configuración y seguridad se aplican a todas las cuentas existentes en los equipos, pero sólo pueden ser activadas o desactivadas en la cuenta de administrador de los mismos.

4.11 El Modelo OSI

El modelo de referencia **OSI**[22] es la arquitectura de red actual más prominente. El objetivo de éste es el de desarrollar estándares para la interconexión de sistemas abiertos (Open System Interconnection).

El término OSI es el nombre dado a un conjunto de estándares para las comunicaciones entre computadoras, terminales y redes. OSI es un modelo de 7 capas, donde cada capa define los procedimientos y las reglas (protocolos normalizados) que los subsistemas de comunicaciones deben seguir, para poder comunicarse con sus procesos correspondientes de los otros sistemas.

[22] Modelo de Referencia implantado por ISO, Internacional Standard Organization

Esto permite que un proceso que se ejecuta en una computadora, pueda comunicarse con un proceso similar en otra computadora, si tienen implementados los mismos protocolos de comunicaciones de capas OSI. El modelo OSI está conformado por los siguientes niveles:

Nivel de aplicación. Se definen una serie de aplicaciones para la comunicación entre distintos sistemas, las que gestionan:

- Transferencia de archivos (FTP)
- Intercambio de mensajes (correo electrónico)

Nivel de presentación. En esta capa se realizan las siguientes funciones:

- Da formato a la información para visualizarla o imprimirla
- Se interpretan los códigos que estén en los datos (conversión de código)
- Gestiona la encriptación de datos
- Realiza la compresión de datos

Nivel de sesión. Provee mecanismos para organizar y estructurar diálogos entre procesos de aplicación. Actúa como un elemento moderador capaz de coordinar y controlar el intercambio de los datos. Algunas de las funciones que realiza son las siguientes:

- Establecimiento de la conexión de sesión
- Intercambio de datos
- Liberación de la conexión de sesión
- Sincronización y administración de la sesión
- Controla la integridad y el flujo de los datos en ambos sentidos

Nivel de transporte. Esta capa asegura que se reciban todos los datos y en el orden adecuado. Realiza un control de extremo a extremo. Algunas de las funciones realizadas son:

- Acepta los datos del nivel de sesión, fragmentándolos en unidades más pequeñas y los pasa al nivel de red
- Multiplexaje
- Regula el control de flujo del tráfico de extremo a extremo
- Reconoce los paquetes duplicados

Nivel de red. En esta capa se determina el establecimiento de la ruta.

- Esta capa mira las direcciones del paquete para determinar los métodos de conmutación y enrutamiento
- Realiza control de congestión

Nivel de enlace. Aquí es donde se comunican y controlan los datos, realizando las funciones de:

- Detección y control de errores
- Control de secuencia y flujo
- Control de enlace lógico
- Control de acceso al medio
- Sincronización de la trama

Nivel físico. Esta etapa define las características:

- Físicas (componentes y conectores mecánicos)
- Eléctricas (niveles de tensión)
- Funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico)

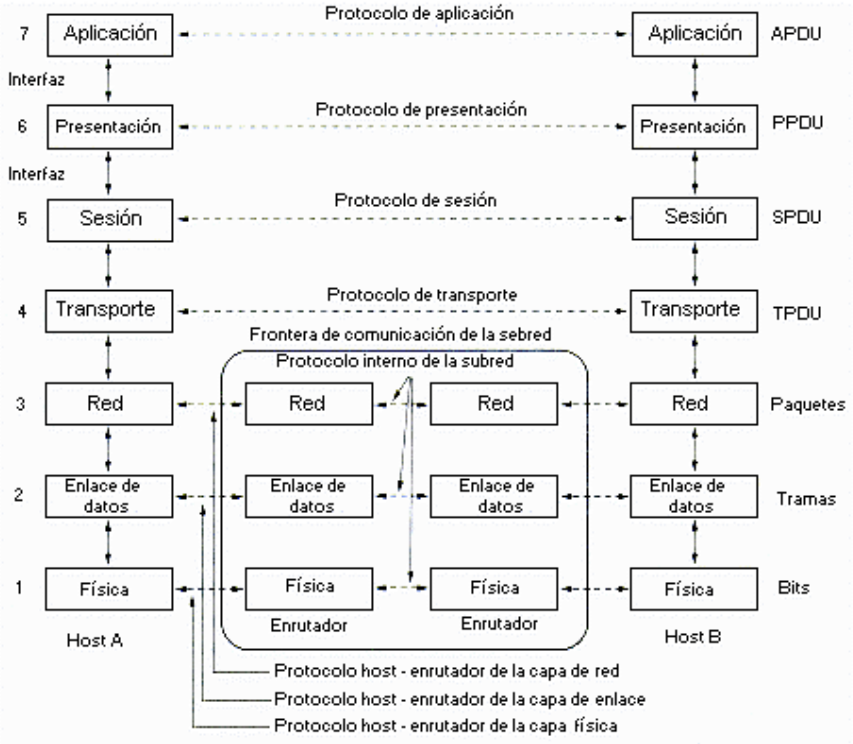

Figura 4.47 Capas, interfaces y protocolos del modelo OSI

La norma **IEEE 802.11** fue diseñada para sustituir a la **capa física y MAC** (**capa 2 del modelo de OSI**) de la norma 802.3 (Ethernet), así, la única diferencia entre ambas es la manera en la que los dispositivos acceden a la red, por lo que ambas normas son perfectamente compatibles. WEP opera a nivel 2 del modelo OSI (capa de enlace) y es soportado por la gran mayoría de fabricantes de soluciones inalámbricas.

El estándar **802.11b abarca las capas física y de enlace del modelo OSI**. A nivel físico el estándar 802.11b trabaja en la banda de los 2.4 GHz, 802.11b proporciona para la capa MAC mecanismos de control de acceso y de encriptación denominado WEP (Wired Equivalent Privacy)

Cabe recordar que **un protocolo no es más que un conjunto de reglas o convenciones** (algoritmos, formatos de mensajes, interfaces, etc.) perfectamente conocidas por los dispositivos que intercambian información a través de una red de comunicaciones. Cada protocolo responde a un propósito concreto, razón por la que lo habitual es que en una red de comunicaciones intervengan varios de distinta índole.

Estos conjuntos de reglas suelen agruparse en niveles o capas de distinta funcionalidad, de forma que cada uno de ellos se apoya en los servicios que le ofrece el inmediatamente inferior, y al mismo tiempo brinda al nivel superior nuevas opciones.

Los protocolos de un nivel ocultan la forma en que han sido implementados los servicios ofrecidos a la capa superior lo que, por una parte, materializa una arquitectura modular que facilita la evolución de cualquier componente sin que esto conlleve modificaciones en el resto y, por otra, permite abstraerse de la complejidad inherente a la resolución de toda la infraestructura de comunicaciones.

No obstante esto no significa que se este abordando un proceso de transferencia física de datos entre ambas capas en distintos equipos. Los paquetes de datos solo se transfieren entre niveles adyacentes de cada máquina vinculada al proceso de comunicación, para lo que se usan las

interfaces entre niveles. Por ello, los paquetes de datos se envían a través de la capa física, uno de los niveles definidos en la arquitectura de red.

Este capítulo por si sólo es contemplado como un pilar fundamental en la elaboración de este trabajo de Tesis, ya que dentro de la información recabada se contempla tanto la configuración a **nivel software** como la configuración de la **red inalámbrica.**

El Centro de Tecnología de Información sobre el que se realiza la presente documentación, es **uno de los primeros en su tipo dentro del campus universitario**, innovando con nuevas tecnologías y brindando así, un servicio óptimo y eficiente para los alumnos de la Facultad de Ingeniería, motivo por el cuál, la configuración correcta de todos los servicios que se ofrecerán dentro del CTI es de vital importancia dentro de la administración que deberá llevar el lugar.

SEGURIDAD INFORMÁTICA

La utilización masiva de las computadoras y redes como medios para almacenar, transferir y procesar información se ha incrementado espectacularmente en los últimos años, al grado de convertirse en un elemento indispensable para el funcionamiento de la sociedad actual.

Como consecuencia, la información en todas sus formas y estados se ha convertido en un activo de altísimo valor, el cual se debe proteger y asegurar para garantizar su integridad, confidencialidad y disponibilidad, entre otros servicios de seguridad.

5.1 Antecedentes de seguridad informática

El objetivo de la seguridad informática será mantener los siguientes elementos, referente a la información manejada por los equipos de cómputo:

- **Integridad de la información:** Es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias.
- **Disponibilidad de la información:** Es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.
- **Privacidad:** Es la necesidad de que la información sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la información puede provocar severos daños a su dueño o volverse obsoleta.
- **Control sobre la información:** Permite asegurar que sólo los usuarios autorizados pueden decidir cuándo y cómo permitir el acceso a la misma.

- **Autenticidad:** Permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución, esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades.

Cuando se desea mantener algo controlado, lo primero que debe de hacerse es conocer aquello que pueda dañarlo, algo que represente una **amenaza**[1] para un dispositivo o entorno. Las amenazas pueden ser analizadas en tres momentos: **antes** del ataque, **durante** y **después** del mismo. Estos mecanismos conformarán políticas que garantizarán la seguridad de cualquier sistema informático.

Las amenazas que pueden aquejar a la seguridad de cualquier tipo de sistema informático se clasifican en los tipos mostrados en el diagrama siguiente:

Figura 5.1 Amenazas para la seguridad

Comprender y conocer de seguridad ayudará a llevar a cabo un análisis sobre los **riesgos**, las **vulnerabilidades, amenazas** y **contramedidas**; evaluar las ventajas o desventajas de la situación; a decidir medidas técnicas y tácticas metodológicas, físicas e informáticas, con base en las necesidades de seguridad. Contrario a lo que se piensa, el concepto de seguridad informática no es nuevo y nació con los grandes centros de cómputo. Con el pasar de los años, las computadoras pasaron de ser monstruos, que ocupaban salas enteras, a pequeños elementos de trabajos perfectamente ubicables sobre un escritorio de oficina.

[1] Cabe definir **Amenaza,** en el entorno informático, como cualquier elemento que comprometa a un sistema.

En este proceso de digitalización y miniaturización llamada **"downsizing"** la característica más importante que se perdió fue la seguridad. Los especialistas de **Seguridad Informática** de hoy se basan en principios de aquellos antiguos MainFrames (grandes computadoras).

5.1.1 Intrusos informáticos

Se llama **Intruso** o **Atacante** a la persona que accede (o intenta acceder) sin autorización a un sistema ajeno, ya sea en forma intencional o no. Los diversos tipos de intrusos se pueden caracterizar desde el punto de vista del nivel de conocimiento, formando una pirámide[2]:

1. **Clase A:** El 80% en la base, son los nuevos intrusos que bajan programas de Internet y prueban, a manera de juego.
2. **Clase B:** Es el 12% son más peligrosos, saben compilar programas, aunque no saben programar. Prueban programas, conocen como detectar que sistema operativo está usando la victima, analizan las vulnerabilidades del mismo e ingresan por ellas.
3. **Clase C:** Es el 5%, es gente que sabe, que conoce y define sus objetivos, a partir de aquí buscan todos los accesos remotos e intentan ingresar al sistema.
4. **Clase D:** El 3% restante. Cuando entran a determinados sistemas buscan información que necesitan.

Para llegar desde la base hasta el último nivel se tardan desde cuatro hasta seis años, por el nivel de conocimiento que se requiere asimilar.

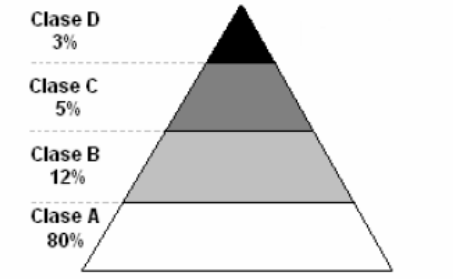

Figura 5.2 Tipos de Intrusos

[2] Fuente: CybSec S.A. http://www.cybsec.com

5.1.2 ¿Qué Debemos Proteger?

En cualquier sistema informático existen tres elementos básicos a proteger: El **hardware**[3]**,** el **software**[4] y los **datos**[5]**.** Además, se habla de un cuarto elemento llamado **fungible**; que son aquellos que se gastan o desgastan con el uso continuo: papel, tonner, tinta, disquetes, discos, etc.

De los cuatro, los datos que manejan los sistemas, son los más importantes, ya que son el resultado del trabajo realizado. Si existiera daño del hardware, software o de los elementos fungibles, éstos pueden adquirirse nuevamente desde su medio original; pero los datos obtenidos en el transcurso del tiempo por el sistema son imposibles de recuperar.

Para cualquiera de los elementos descritos existen multitud de amenazas y ataques que se les puede clasificar en:

1. **Ataques pasivos:** El atacante no altera la comunicación, sino que únicamente la "escucha" para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico.

2. **Ataques activos:** Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos. Generalmente son realizados por hackers, piratas informáticos o intrusos remunerados y se les puede subdividir en cinco categorías:

    - **Interrupción:** Si hace que un objeto del sistema se pierda, quede inutilizable o no disponible.
    - **Intercepción:** Si un elemento no autorizado consigue el acceso a un determinado objeto del sistema.

[3] Conjunto de todos los sistemas físicos del sistema: CPU, cableado, impresoras, CD-ROM, componentes de comunicación, etc.
[4] Elementos lógicos que hacen funcional al hardware: sistema operativo, aplicaciones, programas, etc.
[5] Conjunto de información lógica que maneja el software y el hardware: bases de datos, documentos, archivos, etc.

- **Modificación:** Si además de conseguir el acceso, consigue modificar el objeto
- **Fabricación:** Se consigue un objeto similar al original de forma que es difícil distinguirlos entre sí
- **Destrucción:** Es una modificación que inutiliza el objeto

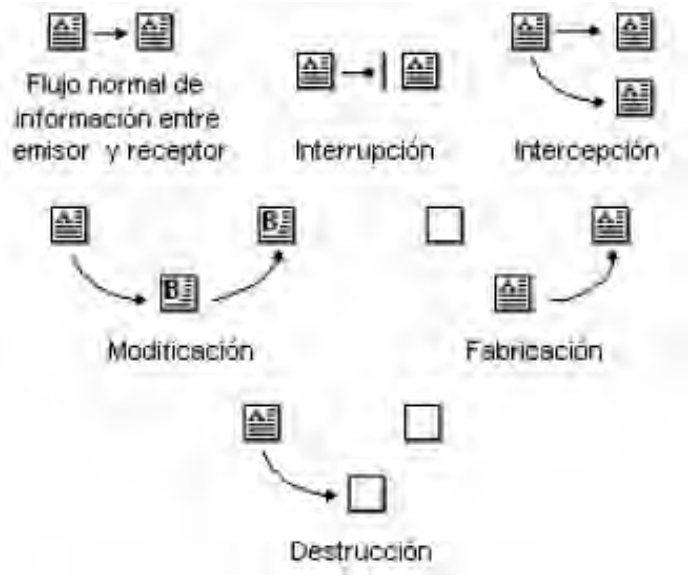

Figura 5.3 Tipos de Ataques Activos[6]

5.2 Seguridad Física

La seguridad física consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial"[7]. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del CTI, así como medios de acceso remoto a éste y desde él mismo; implementados para proteger el hardware y los medios de almacenamiento de datos.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro. Las

[6] HOWARD, John D. Tesis: Análisis de la seguridad en el Internet. Instituto de Tecnología de Carnegie. 1995. EE.UU.
[7] HUERTA, Antonio Villalón. "Seguridad en UNIX y Redes". Versión 1.2 Digital. 2 de Octubre de 2000

principales amenazas que se advierten en la seguridad física son:

1. Desastres naturales, incendios accidentales, tormentas e inundaciones
2. Amenazas ocasionadas por el hombre
3. Disturbios, sabotajes internos y externos deliberados

5.2.1 Medidas físicas de prevención

Evaluar y controlar permanentemente la seguridad física del CTI es la base para comenzar a integrar la seguridad como una función primordial dentro de cualquier organismo. Tener controlado el ambiente y acceso físico permite:

- Disminuir siniestros
- Trabajar mejor manteniendo la sensación de seguridad
- Descartar falsas hipótesis si se produjeran incidentes
- Tener los medios para luchar contra incidentes

5.3 Seguridad lógica

La seguridad lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo. Existe un viejo dicho en la seguridad informática que dicta que **“todo lo que no está permitido debe estar prohibido”** y esto es lo que debe asegurar la seguridad lógica.

5.3.1 Controles de acceso

Los objetivos que se plantean serán:

1. Restringir el acceso a los programas y archivos

2. Asegurar que los usuarios puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan
3. Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en un paquete específico de seguridad o en cualquier otro utilitario. Estos, constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información y para resguardar la información confidencial de accesos no autorizados.

La seguridad informática se basa, en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos. Esta administración abarca:

1. Proceso de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios, tanto en las cuentas provistas para los equipos de cómputo como en las cuentas creadas en el servidor. Es necesario considerar que la solicitud de habilitación de un permiso de acceso para un usuario determinado, debe provenir de su superior y, de acuerdo con sus requerimientos específicos de acceso, debe generarse el perfil en el sistema de seguridad, en el sistema operativo o en la aplicación según corresponda.
2. La identificación de los usuarios debe definirse de acuerdo con una norma homogénea para toda la organización.
3. Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos.
4. Las revisiones deben orientarse a verificar la adecuación de los permisos de acceso de cada individuo de acuerdo con sus necesidades operativas, la actividad de las cuentas de usuarios o la autorización de cada habilitación de acceso. Para esto,

deben analizarse las cuentas en busca de períodos de inactividad o cualquier otro aspecto anormal que permita una redefinición de la necesidad de acceso.

5.3.2 Modalidad de acceso

Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser:

- **Lectura:** El usuario puede únicamente leer o visualizar la información, pero no alterarla. Debe considerarse que la información puede ser copiada o impresa
- **Escritura:** Este tipo de acceso permite agregar datos, modificar o borrar información
- **Ejecución:** Este acceso otorga al usuario el privilegio de ejecutar programas
- **Borrado:** Permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación

Además existen otras modalidades de acceso especiales, que generalmente se incluyen en los sistemas de aplicación:

- **Creación:** Permite al usuario crear nuevos archivos, registros o campos
- **Búsqueda:** Permite listar los archivos de un directorio determinado

5.3.3 Políticas de seguridad básicas

Dentro de las políticas generales de seguridad aplicables a un centro u organización, se deben tener en mente las directivas básicas a implementar en un CTI, como las siguientes:

- Los administradores de red y usuarios de estaciones de trabajo deberán actualizar en forma permanente los últimos parches de los sistemas operativos.
- Es imperativo tener instalado un buen software antivirus y actualizar su registro de virus diariamente.

- Usar claves de acceso que no estén asociadas a datos comunes del usuario, tales como la fecha de nacimiento, apelativos, nombres de familiares, etc.
- Cambiar de clave de acceso por lo menos cada tres meses, aunque lo ideal es hacerlo mensualmente.
- Las carpetas compartidas, dentro de una Red, deben tener una clave de acceso, la misma que deberá ser cambiada periódicamente.
- No ejecutar ningún archivo contenido en un mensaje de correo no solicitado o enviado por un remitente desconocido, así ofrezca atractivos premios o temas provocativos.
- Verificar cualquier software que haya sido instalado, asegurándose que provenga de fuentes conocidas y seguras.
- No instalar copias de software sin su respectiva licencia de uso. Además de transgredir la Ley, pueden contener virus, **spyware**[8] o archivos de sistema incompatibles con el del usuario, lo cual provocará su inestabilidad.
- Instalar un Firewall de software o cualquier sistema seguro para controlar los puertos del sistema.
- Tomar precauciones con los contenidos **applets**[9] de Java, **JavaScripts**[10] y Controles **ActiveX**[11], durante la navegación, así como los **certificados de seguridad**. Es recomendable configurar el navegador desactivando la ejecución automática de estos contenidos, ya que mediante estos se pueden ejecutar virus o aplicaciones que puedan dañar el software o la información contenida en los equipos.
- No emplear los máximos privilegios en tareas para las que no sean estrictamente necesarios.
- No almacenar información importante en su sistema. Si un intruso la captura, puede borrar esos archivos y eliminar toda prueba, para posteriormente usar los datos

[8] Son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas.
[9] Pequeña aplicación en línea desarrollada con Java. Son descargados automáticamente desde la Red y ejecutados en el ordenador de usuario.
[10] Es un lenguaje de scripts creado por Netscape, y que permite la programación para cualquier plataforma (al igual que el lenguaje JAVA) de eventos, objetos y acciones que pueden ser utilizados en páginas HTML, estándar.
[11] Componentes software de Microsoft. Activan el sonido, las aplicaciones Java y las animaciones que se desea integrar en una página Web.

obtenidos. Es recomendable mantener esta información en discos compactos o en un zip drive.

- No se debe confiar en los archivos gratuitos que se descargan de sitios Web desconocidos, ya que son una potencial vía de propagación de virus.
- Configurar el sistema para que muestre las extensiones de todos los archivos.
- La aparición y desaparición de archivos, incluso temporales injustificadamente, lentitud del sistema, bloqueos o re-inicios continuos, desconexiones de Internet, inicialización o finalización de programas o procesos sin justificación, la bandeja del CD/DVD se abre y cierra sin motivo alguno, el teclado, mouse u otro periférico dejan de funcionar, son evidencias de que el equipo está siendo controlado por un hacker que ha ingresado al sistema con un virus troyano/backdoor.
- Borrar constantemente las **cookies**[12], archivos temporales e historial, en la opción herramientas, opciones de Internet, del navegador de Internet.

5.4 Delitos informáticos

El desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La cuantía de los perjuicios así ocasionados es a menudo muy superior a la usual en la delincuencia tradicional y también son mucho más elevadas las posibilidades de que no lleguen a descubrirse o castigarse.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que "entra" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes. Para el caso del CTI, se tienen pensadas las directivas de seguridad en los equipos, pensando en el uso que se les pueda dar a los mismos por los usuarios, ya sea para ejecutar acciones indebidas al exterior mediante Internet o bien, para ejecutar acciones indebidas en los propios equipos.

[12] Pequeños archivos de texto que un servidor Web almacena en la computadora del usuario, para guardar información sobre éste, como un número de identificación, una contraseña, sus preferencias o cuántas veces ha visitado el sitio el usuario.

5.4.1 Definición de hacker

Un **hacker** es una persona que está siempre en una continua búsqueda de información, vive para aprender y todo para él es un reto; no existen barreras, y lucha por la difusión libre de información, distribución de software sin costo, y la globalización de la comunicación. El concepto de Hacker, generalmente es confundido erróneamente con los mitos que existen acerca de este tema:

- Un hacker es pirata. Esto no es así ya que los piratas comercian con la información que obtienen, entre otras cosas y un verdadero hacker sólo obtiene esa información para uso personal.
- Un hacker es el que entra en los sistemas ajenos y se dedica a destruir la información almacenada en ellos. El error consiste en que el que destruye información y sistemas ajenos, no es el Hacker sino el **cracker**.
- Un verdadero hacker no se mete en el sistema para borrarlo todo o para vender lo que consiga. Quiere aprender y satisfacer su curiosidad.

5.4.2 Definición de cracker

Los **cracker**, en realidad, son Hackers cuyas intenciones van más allá de la investigación. Es una persona que tiene fines maliciosos o de venganza, quiere demostrar sus habilidades, pero de la manera equivocada o simplemente personas que hacen daño sólo por diversión.

En algunos casos los alumnos de la carrera de Ingeniero en Computación, llevan sus conocimientos al punto de dañar más que adentrarse en sistemas no permitidos, esto a manera de reto; pensando en los ataques de éste tipo que se puedan recibir, se contemplan las **directivas de seguridad**, el **firewall** y el **antivirus** en todos los equipos de cómputo.

5.5 Amenazas internas

Las amenazas a la seguridad de un CTI, pueden provenir del personal propio al lugar, rara vez es tomada en cuenta esta posibilidad porque siempre se supone un ámbito de confianza

muchas veces inexistente. Generalmente, estos ataques son accidentes por desconocimiento o inexistencia de las normas básicas de seguridad; pero también pueden ser del tipo intencional.

Es de destacar que un simple electricista puede ser más dañino que el más peligroso de los piratas informáticos, ya que un corte de energía puede causar un desastre en los datos almacenados por los usuarios en los equipos de cómputo del CTI. Al evaluar la situación, se verá que aquí el daño no es intencionado pero ello no esta en discusión; el daño existió y esto es lo que compete a la seguridad informática.

Para prevenir un siniestro con estas características se tiene pensado el uso de un pequeño generador que provea de energía eléctrica a los equipos por algunos minutos, con la finalidad de que los usuarios respalden la información ya sea en los equipos o en medios de almacenamiento extraíbles, por otro lado esta acción daría el tiempo suficiente al personal del CTI de apagar los equipos de manera correcta y no esperar a que se apaguen automáticamente por la falta de energía, previniendo con ello un daño innecesario en los mismos.

5.5.1 Curiosos

Suelen ser los atacantes más habituales de un CTI enfocado al área educativa. Son personas que tienen un alto grado de interés en las nuevas tecnologías, pero no tienen los conocimientos ni experiencia básicos para considerarlos hackers o crackers. En la mayoría de los casos son estudiantes intentando penetrar los servidores de su facultad o empleados consiguiendo privilegios para obtener información para ellos restringida. Generalmente no se trata de ataques de daño, pero afectan el entorno de fiabilidad en el lugar.

5.5.2 Políticas de seguridad informática

Hoy es imposible hablar de un sistema 100 % seguro, sencillamente porque el costo de la seguridad total es muy alto. Por eso las empresas, en general, asumen riesgos, deben optar

por perder un negocio o arriesgarse a ser “hackeadas”.

Las **P**olíticas de **S**eguridad **I**nformática **(PSI),** surgen como una herramienta organizacional para concienciar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos.

“Una política de seguridad es un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales que está y que no está permitido en el área de seguridad durante la operación general del sistema.”[13]

Una norma básica dentro del marco de las políticas de seguridad, sería la de verificar a cada aspirante a ser nuevo empleado; aunque tampoco debemos olvidar a los usuarios que son el principal foco de ataque a las instalaciones. Para minimizar el daño que un atacante interno puede causar se pueden seguir estos principios fundamentales:

- **Necesidad de conocimiento:** Comúnmente llamado *mínimo privilegio.* Cada usuario debe tener el mínimo privilegio que necesite para desempeñar correctamente su función, es decir, que sólo se le debe permitir que sepa lo necesario para realizar su trabajo.
- **Rotación de funciones:** La mayor amenaza del conocimiento parcial de tareas es la complicidad de dos responsables, de forma tal, que se pueda ocultar sendas violaciones de seguridad. Para evitar el problema, una forma común es rotar (dentro de ciertos límites) a las personas a lo largo de diferentes responsabilidades, para establecer una vigilancia mutua.
- **Conocimiento parcial:** Las actividades más delicadas dentro del CTI deben ser realizadas por dos personas competentes, de forma que si uno comete un error en las políticas de seguridad, el otro pueda subsanarlo.
- **Separación de funciones:** Es necesario que definan y separen correctamente las funciones de cada persona, de forma que alguien cuya tarea es velar por la seguridad

[13] HUERTA, Antonio Villalón. Seguridad en Unix y redes. Versión 1.2

del lugar o sistema no posea la capacidad para violarla sin que nadie se percate de ello.

- **Cancelación inmediata de cuenta:** Cuando un empleado abandona la organización se debe cancelar inmediatamente el acceso a sus antiguos recursos y cambiar las claves que el usuario conocía.

En estos puntos se encuentran las mayores vulnerabilidades de un sistema, como, por ejemplo, suelen encontrarse claves de usuario que hace años que no se utilizan y por ende tampoco se han cambiado sus contraseñas.

Si bien estas normas pueden aplicarse a las organizaciones, no se podrán hacer del todo en instituciones como una Universidad, donde la mayoría de los atacantes son alumnos y no podrán verificarse los antecedentes de miles de alumnos (y tampoco ético prohibir su acceso por ser estos dudosos).

De esta forma, en estos casos deberá ceñirse a otros mecanismos de control en donde casi siempre se opta por las sanciones a todos aquellos que utilicen el CTI para cometer delitos informáticos. Un método utilizado para el control de los equipos se basa en la configuración para que cada una de las computadoras que utilizarán los usuarios inicien con una sesión específica con privilegios no administrativos, de esta manera cuando el equipo se enciende al comienzo del día la máquina inicia automáticamente en una **sesión de usuarios** en la cual el usuario puede trabajar pero no puede modificar los parámetros de configuración del equipo.

5.6 Amenazas lógicas

La seguridad de un sistema es tan fuerte como su punto más débil, la seguridad total no existe pero si la mínima seguridad. Bajo la etiqueta de **amenazas lógicas** encontramos todo tipo de programas, que de una forma u otra, pueden dañar a los sistemas, creados de forma intencionada para ello (*software* malicioso, también conocido como *malware*) o simplemente por error (*bugs* o agujeros).

5.6.1 Identificación de las amenazas

La identificación de amenazas requiere conocer los tipos de ataques, el tipo de acceso, la forma operacional y el objetivo del atacante. Las consecuencias de los ataques se podrían clasificar en:

- **Corrupción de datos:** La información que no contenía defectos pasa a tenerlos
- **Negación de servicios (DoS):** Servicios que deberían estar disponibles no lo están
- **Leakage:** Los datos llegan a destinos a los que no deberían llegar

Desde 1990 hasta nuestros días, el **CERT**[14] viene desarrollando una serie de estadísticas que demuestran que cada día se registran más ataques informáticos, y estos son cada vez más sofisticados, automáticos y difíciles de rastrear.

La Tabla 5.1 detalla el tipo de atacante, las herramientas utilizadas, en que fase se realiza el ataque, los tipos de procesos atacados, los resultados esperados y/u obtenidos y los objetivos perseguidos por los intrusos:

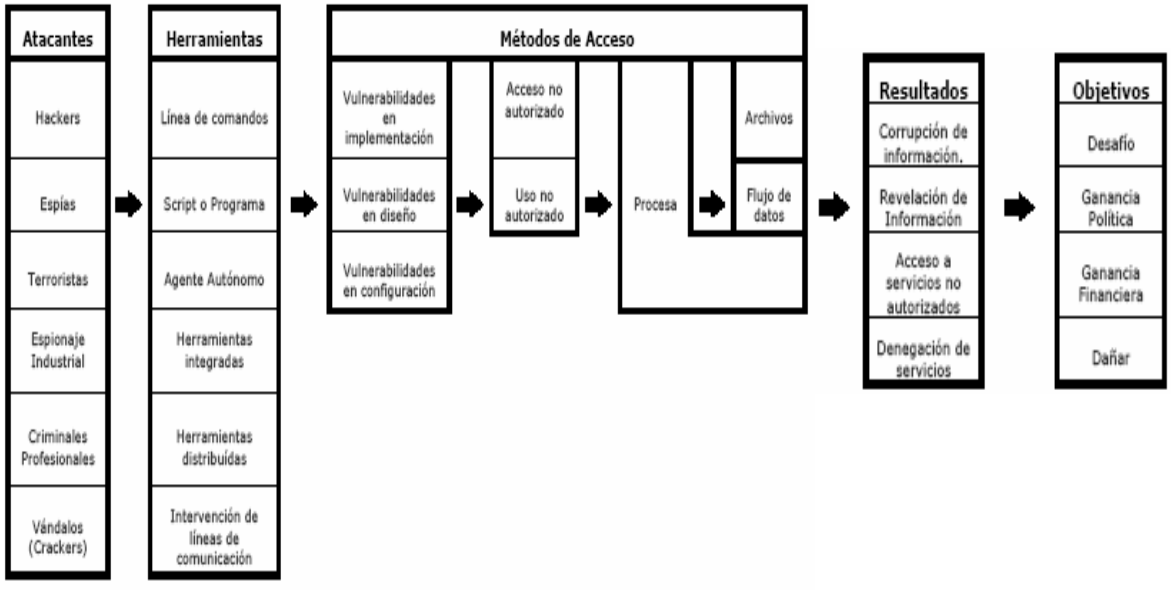

Tabla 5.1 Detalle de Ataques. Fuente: HOWARD, John D. Thesis: An Analysis of security on the Internet. 1989-1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU.

[14] CERT: Computer Emergency Response Team. Grupo de Seguridad Internacional especializado en dar respuesta a las empresas y organizaciones que denuncian ataques informáticos a sus sistemas de información. *http://www.cert.org*

5.6.2 Tipos de ataques

En los primeros tiempos, los ataques involucraban poca sofisticación técnica. Los operadores, programadores y capturistas utilizaban sus permisos para alterar archivos o registros, en tanto que otro tipo de personas ingresaban a la red simplemente averiguando una clave o contraseña válidas. A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explorar "agujeros" en el diseño, configuración y operación de los sistemas, de entre los cuales se mencionan los siguientes elementos:

- **Herramientas de seguridad:** Éstas representan un arma de doble filo, ya que de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos.

  Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar ciertos programas en los sistemas habituales de autentificación del programa o del núcleo que se está diseñando. A estos atajos se les denomina **puertas traseras**, y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos.

- **Bombas lógicas:** Son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que sean activadas; en ese punto, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial.

- **Virus:** Es una secuencia de código que se inserta en un archivo ejecutable (denominado **huésped**), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.

- **Gusano:** Es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando errores en los sistemas a los que se conecta para dañarlos. Al ser difíciles de programar su número no es muy elevado, pero el daño que pueden causar es muy grande.

- **Caballos de troya:** Son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas (generalmente en detrimento de la seguridad) sin el conocimiento del usuario.

- **Programas conejo o bacterias:** Bajo este nombre se conoce a los programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco...), produciendo una negación de servicio.

5.7 Protección

Una vez conocidas las vulnerabilidades y ataques a las que está expuesto un sistema, es necesario **conocer los recursos disponibles para protegerlo**. Mientras algunas técnicas son evidentes (seguridad física por ejemplo) otras pautas no lo son tanto e incluso algunas pueden ocasionar una sensación de falsa seguridad.

Muchas de las vulnerabilidades estudiadas son el resultado de **implementación incorrecta de tecnologías**, otras consecuencias de la **falta de planeación** de las mismas pero, como ya se ha mencionado, la mayoría de los agujeros de seguridad son ocasionados por los usuarios de dichos sistemas y es responsabilidad del administrador detectarlos y encontrar la mejor manera de cerrarlos.

5.7.1 Administración de la seguridad

Los intrusos utilizan diversas técnicas para quebrar los sistemas de seguridad de una red. Básicamente utilizan los puntos débiles del sistema para poder colarse en ella. El trabajo de los administradores no difiere mucho de ello. Los intrusos cuentan con grandes herramientas como los **scanners**, los **crackeadores de contraseñas**, **software de análisis de vulnerabilidades**, etc.

Un administrador cuenta con todas ellas empleadas para bien, los **sistemas de detección de**

intrusos o los **sistemas de rastreo de intrusiones** son una prueba de ello. Al conjunto de técnicas que se utilizan para evaluar y probar la seguridad de una red se le conoce como **penetration testing**, uno de los recursos más poderosos con los que se cuenta hoy para generar barreras cada vez más eficaces.

Un test está totalmente relacionado con el tipo de información que se maneja en cada organización. Por consiguiente, según la información que deba ser protegida, se determinan la estructura y las herramientas de seguridad; **no a la inversa.**

El software y el hardware utilizados son una parte importante, pero no la única. A ella se agrega lo que se denomina **"políticas de seguridad internas"** que cada organización debe generar para implementar.

Es posible dividir las tareas de administración de seguridad en tres grandes grupos:

- **Autenticar:** Se refiere a establecer las entidades que pueden tener acceso al universo de recursos de cómputo que cierto medio ambiente puede ofrecer.
- **Autorización:** Es el hecho de que las entidades autorizadas a tener acceso a los recursos de cómputo, tengan acceso únicamente a las áreas de trabajo sobre las cuales ellas deben tener dominio.
- **Auditoría:** Se refiere a la continua vigilancia de los servicios en producción. Entra dentro de este grupo el mantener estadísticas de acceso, estadísticas de uso y políticas de acceso físico a los recursos.

Por lo general, las políticas son el primer paso que se dispone para entrar en un ambiente de seguridad, puesto que reflejan la voluntad de hacer algo que permita detener un posible ataque antes de que éste suceda. En el CTI se analizan todas aquellas medidas de seguridad que deban aplicarse para mantener a los equipos aislados de un ataque o de un mal uso por parte de los usuarios o algún otro tipo de persona, en estos casos la verdadera seguridad radica en una buena organización y estructuración de las políticas de seguridad.

A continuación se citan algunos de los métodos de protección más comúnmente empleados.

1. **Sistemas de detección de intrusos:** Son sistemas que permiten analizar las bitácoras de los sistemas en busca de patrones o eventos que puedan considerarse sospechosos, sobre la base de la información con la que han sido previamente alimentados, pueden considerarse como monitores.

2. **Sistemas orientados a conexión de red:** Monitorizan las conexiones que se intentan establecer en una red o equipo en particular, siendo capaces de efectuar una acción sobre la base de métricas como: origen y destino de la conexión, servicio solicitado, permisos, etc.

   Las acciones que pueden emprender suelen ir desde el rechazo de la conexión hasta alerta al administrador. En esta categoría están los cortafuegos (**Firewalls**).

3. **Sistemas de análisis de vulnerabilidades:** Analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. La desventaja de estos sistemas es que pueden ser utilizados tanto por personas autorizadas como por personas que buscan acceso no autorizado al sistema.

4. **Sistemas de protección a la integridad de información:** Sistemas que mediante criptografía o sumas de verificación tratan de asegurar que no ha habido alteraciones indeseadas en la información que se intenta proteger.

Un modelo de seguridad debe estar formado por múltiples componentes o capas que pueden ser incorporadas de manera progresiva al modelo global de seguridad en el CTI, logrando así el método más efectivo para disuadir el uso no autorizado de sistemas y servicios de red.

5.7.2 Firewalls

Quizá uno de los elementos más publicados a la hora de establecer seguridad, sean estos elementos. Aunque deben ser uno de los principales sistemas a los que más se debe prestar

atención, distan mucho de ser la solución final a los problemas de seguridad.

Un **Firewall** es un sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce la política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet).

Como puede observarse, el **muro cortafuegos**, solo sirve de defensa perimetral de las redes, no defiende de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa. Algunos Firewalls aprovechan esta capacidad de que toda la información entrante y saliente debe pasar a través de ellos para proveer servicios de seguridad adicionales como la encriptación del tráfico en la red.

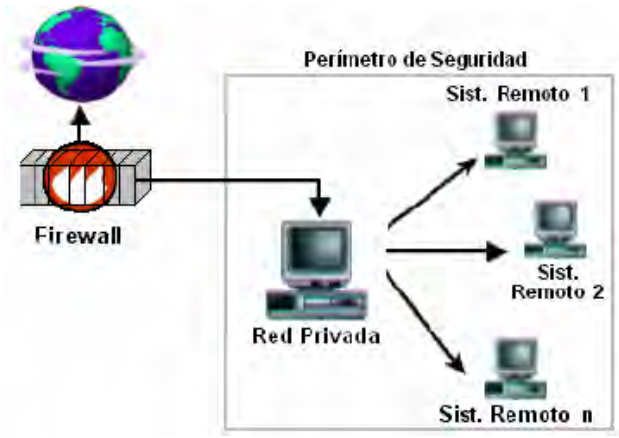

Figura 5.4 Funcionamiento de un Firewall

Debido a su funcionamiento y estructura basada en el filtrado de direcciones y puertos, trabajan en los **niveles** de **transporte** y de **red** del **modelo OSI** y están conectados a ambos perímetros (interior y exterior) de la red. Tienen la ventaja de ser económicos, tienen un alto desempeño y son transparentes para los usuarios conectados a la red. Sin embargo presenta debilidades como:

- No protege las capas superiores a nivel OSI
- Las aplicaciones son difíciles de traducir como filtros de protocolos y puertos

- No son capaces de esconder la topología de redes privadas, por lo que exponen la red al mundo exterior
- No soportan políticas de seguridad complejas como la autentificación de usuarios y control de accesos con horarios predefinidos

Otra causa que ha hecho que el uso de firewalls se halla convertido en uso casi imperativo es el hecho que en los últimos años en Internet han entrado en crisis el número disponible de direcciones IP, esto ha hecho que las intranets adopten direcciones sin clase, las cuales salen a Internet por medio de un "**traductor de direcciones**", el cual puede alojarse en el firewall.

Finalmente, un firewall es vulnerable, el **NO** protege de la gente que está dentro de la red interna. El firewall trabaja mejor si se complementa con una defensa interna. Cuanto mayor sea el tráfico de entrada y salida permitido por el Firewall, menos será la resistencia contra los paquetes externos.

5.7.3 Normas para la elección de claves de seguridad

Se deben tener en cuenta los siguientes consejos:

- No utilizar contraseñas que sean palabras (aunque sean extranjeras), o nombres (el del usuario, personajes de ficción, miembros de la familia, mascotas, marcas, ciudades, lugares u otro relacionado).
- No usar contraseñas completamente numéricas con algún significado (teléfonos, fechas de nacimiento, números de alguna cuenta).
- Elegir una contraseña que mezcle caracteres alfabéticos (mayúsculas y minúsculas) y numéricos.
- Deben ser largas, de ocho caracteres o más.
- Tener contraseñas diferentes en máquinas diferentes. Es posible usar una contraseña base y ciertas variaciones lógicas de la misma para distintas máquinas.

- Deben ser fáciles de recordar para no verse obligado a escribirlas.

La aplicación del conjunto total de las políticas de seguridad usadas en cada uno de los equipos de cómputo se analiza de manera gráfica a través de la aplicación específica llamada TweakUI en el capítulo 4.10 de este trabajo de Tesis.

5.7.4 Normas para proteger claves de seguridad

La protección de las contraseñas recae tanto sobre el administrador del sistema como sobre el usuario. Al comprometer una cuenta se puede estar comprometiendo todo el sistema. Coloquialmente existe una frase que resume algunas de las reglas básicas del uso de una contraseña: “Un password debe ser como un cepillo de dientes. Úsalo cada día, cámbialo regularmente y NO lo compartas con tus amigos”.

Algunos consejos a seguir:

- No permitir ninguna cuenta sin contraseña. Si se es administrador del sistema, repasar este hecho periódicamente
- No mantener la contraseña por defecto del sistema
- Nunca compartir con nadie la contraseña. Si se hace cambiarla inmediatamente
- No escribir la contraseña en ningún sitio. Si se escribe, no debe identificarse como tal y no debe identificarse al propietario en el mismo lugar
- No teclear la contraseña si hay alguien mirando. Es una norma táctica de buen usuario no mirar el teclado mientras alguien teclea su contraseña
- No enviar la contraseña por correo electrónico ni mencionarla en una conversación. Si se debe mencionar no hacerlo explícitamente diciendo: “mi clave es…”
- No mantener una contraseña indefinidamente. Cambiarla regularmente. Disponer de una lista de contraseñas que puedan usarse cíclicamente

Muchos sistemas incorporan ya algunas medidas de gestión y protección de las contraseñas. Entre ellas podemos citar las siguientes:

1. **Número de intentos limitados:** Tras un número de intentos fallidos, pueden tomarse distintas medidas:
    - Obligar a reescribir el nombre de usuario
    - Bloquear el acceso durante un tiempo
    - Enviar un mensaje al administrador y/o mantener un registro especial
2. **Longitud mínima:** Las contraseñas deben tener un número mínimo de caracteres
3. **Restricciones de formato:** Las contraseñas deben combinar un mínimo de letras y números, no pueden contener el nombre de usuario, no ser en blanco
4. **Envejecimiento y expiración de contraseñas:** Cada cierto tiempo se fuerza a cambiar la contraseña
5. **Ataque preventivo:** Muchos administradores utilizan “crakeadores” para intentar atacar las contraseñas de su propio sistema en busca de debilidades

Existen infinidad de métodos (en diversas ocasiones plasmados en herramientas) que permiten violar un sistema o servicio. El profesional cuenta con la misma tecnología para la evaluación de la seguridad del bien a proteger y otras pensadas para la protección como fin, esto hace que muchas veces, la seguridad, sea asunto de la capacidad del profesional.

Ciertamente la **seguridad** requiere un nivel de protección que realmente no existe, y de hecho dudo que algún día exista, pero los riesgos deben y pueden ser manejables. Es importante comprender que la seguridad consiste en **tecnología y políticas de seguridad**, es decir, que la combinación de la tecnología y su forma de utilización determina cuan seguros son los sistemas o los servicios y la mejor manera para obtener un mayor beneficio es integrar todas aquellas soluciones que se encuentren a nuestro alcance tales como aplicaciones informáticas completas en donde se contemplen todas aquellas directivas de seguridad que el personal considere necesarias para salvaguardar la integridad tanto software como de hardware en el CTI.

MANTENIMIENTO PREVENTIVO Y CORRECTIVO

6.1 Medidas Preventivas y Correctivas al Equipo de Cómputo

La puesta en marcha del CTI no sólo consiste en la compra del equipo de cómputo, ni la ubicación del mismo; tampoco implica instalar la paquetería requerida por los usuarios adecuando los parámetros de configuración y seguridad.

El establecer un centro de esta magnitud, implica por sobre todas las cosas el llevar una adecuada administración y principalmente mantener en correcto funcionamiento a todos los elementos que conforman en su conjunto al CTI. Mantener en óptimas condiciones un gran número de equipos de cómputo es una tarea que requiere de ciertas habilidades, sobretodo por un aspecto que siempre se hace presente: **El tiempo**.

Una vez en funcionamiento el CTI, el tiempo se convertirá en un factor primordial para su buena marcha, en centros de cómputo con características similares y tomando en cuenta la población estudiantil de la Facultad de Ingeniería se ha registrado una afluencia de usuarios de aproximadamente ***4000*** **personas**[1], por tal motivo, los equipos de cómputo deben trabajar en óptimas condiciones y de manera ininterrumpida.

En estos casos lo que puede afectar la productividad del CTI en mayor medida, es cuando se presenta una falla, específicamente en los equipos de cómputo dado que el préstamo de estos equipos es el principal servicio prestado a los alumnos de la Facultad. Considerando que los equipos son nuevos se contempla la aplicación en un futuro de un programa de mantenimiento que ha sido exitosamente aplicado en el resto de las salas de cómputo de UNICA.

6.2 Mantenimiento físico preventivo al equipo de cómputo

La finalidad del mantenimiento físico preventivo a los equipos es **prolongar la vida útil** de los mismos, así como **prevenir posibles fallas de hardware**, esto, mediante la

[1] Estadísticas realizadas por UNICA con una afluencia de usuarios diaria en los 3 centros de cómputo con alrededor de 250 equipos de cómputo.

aplicación de un programa que garantice que los equipos de cómputo no serán dañados en sus componentes por los factores ambientales en los que se desempeñan; y de esta forma mantenerlos en condiciones óptimas de funcionamiento, de acuerdo a las especificaciones técnicas de cada fabricante.

Este tipo de mantenimiento es necesario para prevenir fallas mecánicas o eléctricas en los periféricos del equipo de cómputo **(limpieza, lubricación, verificación y ajuste)** al menos cada **6 ó 12 meses** dependiendo de las necesidades del equipo.

6.2.1 Elementos de un equipo de cómputo que requieren servicio

Primeramente se analizarán los elementos principales de un equipo de cómputo que deben someterse a algún tipo de mantenimiento, así como la descripción de la metodología más adecuada para mantener en buen estado todos y cada uno de los componentes que forman parte de los equipos que se utilizan dentro del CTI.

Los equipos se someten a un **proceso de aspirado, sopleteado y rociado de componentes electrónicos** con líquidos dieléctricos y antiestáticos, esto en CPU; además de limpieza de mouse y teclado, limpieza de cabezas de unidades de diskette, lubricación de partes y limpieza de superficies. Detección y corrección de defectos mecánicos en elementos tales como los engranes que permiten la movilidad de la charola de las unidades de disco compacto.

La electricidad estática es un aspecto importante a considerar, ya que el cuerpo humano es conductor de esta electricidad, no muy bueno, pero con la suficiente capacidad para dañar dispositivos electrónicos. Además, las partículas de grasa y aceite que pueda contener el aire del ambiente se mezclan con el polvo, creando una espesa capa aislante que refleja el calor hacia los demás componentes, con lo cual se reduce la vida útil del sistema en general.

Para un mantenimiento más detallado se contempla la tabla siguiente:

DISPOSITIVO	CUIDADOS
Disco duro	Nunca se debe de aplicar ningún tipo de limpiador que no sea de componentes electrónicos, y sólo retirar la acumulación de polvo. Es recomendable que por ningún motivo se abra un disco duro.
Memoria RAM	Aplicar sólo limpiador de componentes electrónicos, no tocar los contactos de cobre que son los que hacen contacto con la tarjeta madre, y siempre insertar los módulos de memoria correctamente, en caso contrario no arrancará la máquina.
Tarjeta madre	Sólo se deberá de cepillar y aspirar el polvo depositado en su superficie, y aplicar limpiador de componentes electrónicos en las ranuras de expansión para evitar falsos contactos.
Tarjetas de expansión	Es necesario cepillar el polvo, aplicar limpiador de componentes electrónicos, limpiar los contactos de cobre y evitar con el cepillado, si es el caso, retirar puentes (jumper) por no tener suficiente cuidado.
Unidades lectoras de disco flexible	Primero retirar el polvo depositado en la superficie externa, después aspirar el polvo que llegase a tener la unidad en el interior; al final utilizar un limpiador de cabezas que se puede adquirir en cualquier tienda de equipo de cómputo.

Tabla 6.1 Recomendaciones para el mantenimiento de hardware

6.2.2 Área de trabajo para el mantenimiento

Con referencia al área de trabajo recomendable para realizar el mantenimiento a los diversos dispositivos se tiene lo siguiente:

	DESCRIPCIÓN
Mesa	De superficie lisa, sin perforaciones y amplia, para evitar que se extravíen o caigan piezas pequeñas.
Iluminación	Buena y suficiente para poder tener una buena visibilidad, en caso necesario tener una lámpara sorda (lámpara de pilas).
Energía eléctrica	Se debe de contar con conexiones eléctricas a la mano por si hay que utilizar algún dispositivo de limpieza eléctrico.

Tabla 6.2 Características del área de trabajo

6.2.3 Materiales que se requieren para limpiar el CPU

- Cepillos de cerdas duras
- Brochas, de preferencia antiestática
- Trapos, favorablemente que no suelten pelusa
- Isopos de algodón
- Limpiador de aplicación en espuma
- Limpiador de componentes electrónicos dieléctrico
- Aire comprimido
- Aspiradora
- Limpiador de unidades lectoras de 3 ½ pulgadas

6.2.4 Limpieza externa del CPU

Una vez que se cuenta con el **espacio adecuado** y los **utensilios necesarios** para trabajar, se procede a **limpiar de forma externa el CPU**, para lo cual se deberán de seguir los siguientes pasos:

1. Apagar el equipo y desconectarlo de la toma eléctrica
2. Eliminar el exceso de polvo con un cepillo de cerdas duras, cepillando de arriba hacia abajo
3. Aplicación de espuma limpiadora
    - **Directa:** cuando la superficie sea lisa y sin perforaciones, la espuma se aplicará de forma directa al CPU
    - **Indirecta:** se aplica la espuma a un trapo para que éste se humedezca y se procede a limpiar las ranuras del CPU

Figura 6.1 Limpieza del CPU

La **mezcla del polvo** con el **ambiente húmedo** en casos extremos ocasiona que éste pueda ser un magnífico **conductor eléctrico** provocando pequeñas fallas en los componentes electrónicos de una computadora; además de que la acumulación del mismo reduce la eficiencia de los ventiladores de enfriamiento, por otra parte, el polvo cuando se acumula de forma uniforme sobre los circuitos integrados forma **un manto aislante** el cual retiene el calor provocando que los circuitos disminuyan su rendimiento.

6.2.5 Limpieza de las tarjetas de expansión

Para realizar **la limpieza de las tarjetas de expansión** se seguirán los pasos que a continuación se indican:

1. Retirar el tornillo que fija la tarjeta de expansión al mueble de la computadora
2. Tener cuidado de no tomar la tarjeta por el costado donde están los contactos de bronce, ya que se pueden ensuciar con la grasa o polvo de los dedos
3. Con una brocha se procede a retirar el polvo que se encuentre depositado en la superficie de la tarjeta, hay que cepillar el polvo de arriba hacia abajo y por todos los costados
4. Después de retirar el polvo, limpiar las terminales de bronce con una goma para eliminar impurezas que se hallan depositado en ellas
5. Por último, aplicar un producto de limpieza para componentes electrónicos, para que la tarjeta quede lista

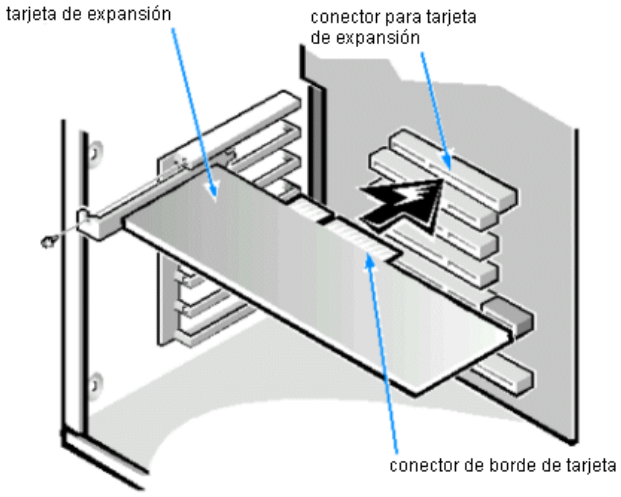

Figura 6.2 Tarjeta de expansión

6.2.6 Limpieza de la fuente de poder

Así como se explicó, se deberá de proceder con todas las tarjetas de expansión. Por su parte, la **limpieza de la fuente de poder** se lleva a cabo en el siguiente orden:

1. Nunca abrir la fuente de poder, toda limpieza deberá ser externa
2. Cepillar el polvo para removerlo de las aspas del ventilador y de la superficie externa de la fuente de poder
3. Bloquear el ventilador para que no gire mientras se aspira el polvo, es necesario tener cuidado de no utilizar objetos pequeños que se puedan quedar atrapados dentro de la fuente
4. Aspirar el polvo de la fuente procurando absorber la máxima cantidad de polvo depositada en ella

Figura 6.3 Fuente de poder

6.2.7 Limpieza de la tarjeta madre

La limpieza de este dispositivo es muy importante ya que en él se encuentran el procesador y los circuitos principales del CPU, son los siguientes:

Figura 6.4 Tarjeta Madre (Mother Board)

1. Para darle limpieza no es necesario desmontarla del chasis del CPU
2. Cepillar toda la superficie de arriba hacia abajo, para que todo el polvo se deposite en la parte inferior, hay que tener cuidado que con el cepillado no se remuevan de su lugar los puentes que tiene la tarjeta madre
3. Con una aspiradora remover todo el polvo depositado en la parte inferior y el que todavía pueda estar depositado en cualquier otra parte del chasis del CPU
4. Aplicar limpiador de componentes electrónicos en la tarjeta madre, incluyendo las ranuras

6.2.8 Limpieza del monitor

Para realizar la limpieza se necesitan seguir los siguientes pasos:

1. Nunca tratar de abrir el monitor para limpiarlo por dentro, ya que se puede sufrir una descarga eléctrica.
2. Con un cepillo de cerdas firmes retirar el polvo depositado en la superficie de la carcaza del monitor.
3. Para completar el paso anterior, pasar un trapo limpio sobre la superficie de la carcaza y la pantalla del monitor.
4. Para lograr una limpieza excelente se tendrá que aplicar espuma limpiadora. Como el monitor tiene ranuras para ventilación, la aplicación de la espuma se realizará de forma indirecta.
5. Una vez que se ha terminado con la carcaza del monitor, hay que limpiar la pantalla, para lo cual se pueden ocupar productos de limpieza de cristal, sólo hay que recordar que la aplicación también debe de llevarse a cabo de forma indirecta.

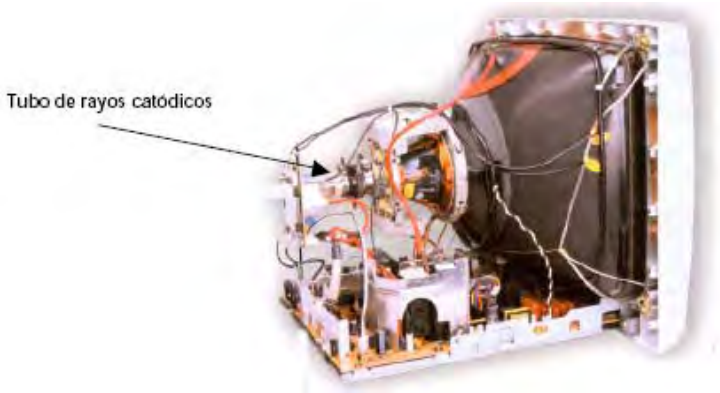

Figura 6.5 Monitor de rayos catódicos

6.2.9 Limpieza del teclado

Una vez terminada la limpieza del monitor se continúa con la del teclado, que es un medio de entrada para el CPU. La limpieza del teclado se puede clasificar en dos tipos:

- **Limpieza superficial** que se hace siguiendo los pasos que a continuación se listan:
  1. Retirar el polvo depositado en la superficie externa del teclado y con una brocha el depositado entre las teclas.
  2. Aplicar aire comprimido para complementar el paso anterior, sobre todo entre las teclas.
  3. Se ocupa espuma limpiadora para limpiar la superficie y teclas. La aplicación deberá ser de forma indirecta. Para las superficies grandes utilizar un trapo y en el caso de las teclas, aplicadores de algodón.

- **Limpieza profunda** que se hará cuando se ha derramado algún líquido sobre el teclado (agua, café, refresco, etc.), se recomienda en este caso acudir con un técnico especializado, ya que se podría dañar o lastimar las membranas del teclado si no se toman las medidas de cuidado necesarias.

Figura 6.6 Teclado ergonómico

6.2.10 Limpieza del ratón

Los pasos a seguir para la limpieza del ratón son los siguientes:

1. Retirar la tapa que retiene la bola de tracción en el interior del ratón

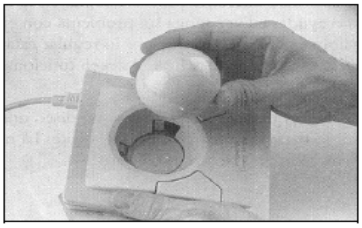

Figura 6.7 Bola de tracción del ratón

2. Identificar y limpiar los rodillos de tracción, esto se hace utilizando un aplicador de algodón humedecido con espuma limpiadora

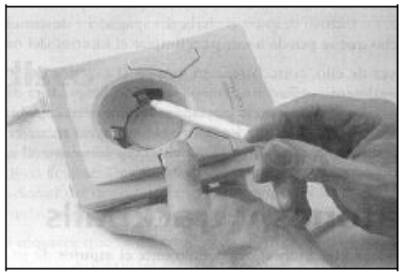

Figura 6.8 Limpieza de rodillos de tracción

6.2.11 Limpieza de la impresora

Con respecto a este punto se procede con el aspirado y sopleteado, lubricación, ajuste de partes y limpieza de superficies. Así como el equipo de cómputo requiere de mantenimiento, las impresoras acumulan del medio ambiente polvo, residuos de tinta o papel y partículas que dañan su funcionamiento, el propio uso genera el desajuste de las piezas y partes que impiden impresiones de calidad. En virtud de lo anterior es recomendable realizar un mantenimiento preventivo cuando menos **una vez al año.**

Figura 6.9 Mantenimiento de impresoras

6.2.12 Limpieza del hub[2]

Para realizar la limpieza a este dispositivo es preciso desconectarlo de la toma de corriente eléctrica además de los conectores de red conectados al mismo, realizar una limpieza directa en toda su superficie con espuma limpiadora.

[2] Dispositivo en una red que conecta múltiples computadoras para conformar una red LAN

La limpieza debe realizarse teniendo cuidado con las terminales a donde se conectan los cables de red.

Figura 6.10 Hub

El mantenimiento preventivo es recomendable que se le proporcione a cada equipo de cómputo en promedio **cuatro veces al año**, aunque hay que tener en cuenta el sitio donde éste se encuentre instalado puesto que podría llegar a necesitarlo hasta **una o dos veces más**.

La administración apropiada de un programa de mantenimiento preventivo recompensa por sí mismo mucho más tiempo de uso del equipo de cómputo libre de problemas, información perdida, componentes dañados y además ofrece la seguridad de una larga vida para el sistema.

6.3 Mantenimiento lógico preventivo al equipo de cómputo

También es necesario darle mantenimiento al software o programas de cómputo, esencialmente para fines de optimización de espacio lógico y uso de recursos del sistema operativo, ya que el continuo uso genera una serie de cambios en la configuración original del sistema, causando bajas en el rendimiento que al acumularse con el tiempo pueden generar problemas serios. Actualmente también es indispensable mantener actualizada la protección contra virus informáticos.

6.3.1 Revisiones al sistema y limpieza de archivos

La computadora trabaja más de lo que se cree, está constantemente dando prioridad a las tareas, ejecutando órdenes y distribuyendo la memoria. Es realmente sorprendente la eficacia de estos equipos, sin embargo, con el tiempo ocurren errores en el disco duro, los datos se desorganizan y las referencias se vuelven obsoletas.

Estos problemas se acumulan y reducen la eficiencia del sistema operativo, las fallas del sistema y software ocurren con más frecuencia y las operaciones de encendido y apagado se demoran más. Para que el sistema funcione adecuadamente e incluso para que sobre todo reduzca el rendimiento, es necesario programar un horario de mantenimiento mensual. Asegurarse además de incluir las siguientes labores en la rutina:

- **Explorar** el disco duro para saber si tienen errores y solucionar los sectores alterados
- **Desfragmentar** el disco duro
- **Eliminar** las entradas de registro inválidas y los accesos directos dañados

Para garantizar una experiencia informática eficaz y placentera, hay que mantener la computadora limpia y bien organizada y para ello es recomendable seguir las siguientes recomendaciones:

- Eliminar los **programas antiguos** y **archivos temporales**
- Eliminar la **información obsoleta**
- Asegurarse de guardar de manera segura la información privada y si es el caso, financiera

Las fallas de los sistemas suceden así como los cortes de energía eléctrica. Y algunas veces, no importa qué tanto cuidado se tenga, inadvertidamente por este y otros motivos se borran diversos tipos de archivos. Para prevenir esto, hay que hacer lo siguiente:

- Hacer **copias de respaldo** de la información mensualmente
- Guardar las copias de respaldo en dos lugares diferentes
- Crear un **disco para el sistema de emergencia** y guardarlo en un lugar seguro

Desde el punto de vista del rendimiento y la seguridad, la **actualización del software** y sistema operativo es tan importante como mantenerlos limpios. La próxima vez que se realice el mantenimiento ordinario del sistema, agregar estos aspectos en la lista es importante:

- **Actualizar el software y sistema operativo**, prestando especial atención a los **parches de seguridad**

- Renovar los servicios de **suscripciones** vencidas **de software**
- Asegurarse de actualizar el software más utilizado con la **última versión**

Ahora más que nunca, se debe incluir un control exhaustivo a la seguridad en la rutina de mantenimiento. El control de seguridad debe por lo menos hacer una **exploración antivirus y una actualización de las definiciones de virus**. También debe revisar que la **configuración del software de seguridad** esté activada y funcionando de manera adecuada.

Casi todas las partes de la computadora requieren desde la desfragmentación del disco duro, hasta el análisis de la seguridad y limpieza del monitor y ratón. Si realizamos periódicamente las tareas anteriores, el resultado será **una computadora en buen estado, confiable y segura**.

6.4 Mantenimiento correctivo al equipo de cómputo

Consiste en la reparación de alguno de los componentes de la computadora, puede ser una soldadura pequeña, el cambio total de una tarjeta (sonido, video, SIMMS de memoria, entre otras), o el cambio total de algún dispositivo periférico como el ratón, teclado, monitor, etc.

Resulta mucho más barato cambiar algún dispositivo que el tratar de repararlo pues muchas veces nos vemos limitados de tiempo y con sobre carga de trabajo, además de que se necesitan aparatos especiales para probar algunos dispositivos.

Asimismo, para realizar el mantenimiento debe considerarse lo siguiente:

- En el ámbito operativo, la reconfiguración de la computadora y los principales programas que utiliza
- Revisión de los recursos del sistema, memoria, procesador y disco duro
- Optimización de la velocidad de desempeño de la computadora
- Revisión de la instalación eléctrica (sólo para especialistas)
- Un completo reporte del mantenimiento realizado a cada equipo
- Observaciones que puedan mejorar el ambiente de funcionamiento

6.4.1 Tipos de mantenimiento correctivo

Dentro de las características concernientes al mantenimiento correctivo a equipos de cómputo se encuentran las siguientes:

- **No planificado:** Corrección de las averías o fallas, cuando éstas se presentan, y no planificadamente, al contrario del caso de mantenimiento preventivo. Esta forma de mantenimiento impide el diagnóstico fiable de las causas que provocan la falla, pues se ignora si falló por mal trato, por abandono, por desconocimiento del manejo, por desgaste natural, etc. El ejemplo de este tipo de mantenimiento correctivo no planificado es la habitual reparación urgente tras una avería que obligó a detener el equipo o máquina dañada.

- **Planificado:** El mantenimiento correctivo planificado consiste en la reparación de un equipo o máquina, cuando se dispone del personal, repuestos y documentos técnicos necesarios para efectuarlo.

Los **costos de mantenimiento correctivo** son aquellos originados, cuando el equipo falla o no puede ser operado a un costo razonable: éstos incluyen también el tiempo de operación perdido, el costo de reparación en sí y en algunos casos el costo de reembolso de equipos, los cuales con mejor mantenimiento pudiesen haberse salvado.

6.5 Consideraciones finales

- No exponer al equipo de cómputo a los rayos del sol
- No colocar al equipo de cómputo en lugares húmedos
- Mantener el equipo de cómputo alejado de equipos electrónicos o bocinas que produzcan campos magnéticos ya que pueden dañar la información
- No fumar cerca del equipo de cómputo
- Evitar comer y beber cuando se esté usando el equipo
- Usar “No-Break” para regular la energía eléctrica y por si la energía se corta que haya tiempo de guardar la información
- Cuando se deje de usar el equipo, esperar a que se enfríe el monitor y ponerle una funda protectora, así como al teclado y al chasis del CPU

6.6 Mantenimiento en periodos intersemestrales

Durante los periodos intersemestrales que es cuando el CTI se encontrará cerrado a los alumnos de la Facultad, se dará un mantenimiento general a los equipos en su totalidad, con esto se logrará que para el siguiente semestre el servicio no se vea interrumpido por alguna falla en los mismos.

En ocasiones el número de equipos que requieren un mantenimiento correctivo en el periodo intersemestral es considerado en estos casos se opta por utilizar una técnica en donde se copia la información y configuración de un equipo en buen estado al equipo en mal funcionamiento.

Este método también llamado **instalación de imagen** consiste específicamente en copiar a discos compactos la información de paquetería y configuración específica de un equipo modelo que se encuentra en óptimas condiciones de funcionamiento, esto, mediante un software llamado **Partition Manager**.

Una vez copiada la información a los discos compactos, estos se instalan en los equipos de cómputo que lo requieran, una vez que la información ha sido copiada, solo resta configurar datos propios del equipo, tales como el nombre de equipo, la dirección IP y las contraseñas de acceso de las diversas cuentas que se manejarán.

Aunque parezca algo obvia la información presentada en este capítulo, siempre es bueno contar con una serie de herramientas o caminos que nos guíen para mantener todos los elementos que componen al CTI en óptimas condiciones, si seguimos lo antes citado y mantenemos una cultura del mantenimiento, nos ahorraremos muchos problemas que son originados por el uso, adecuado o no, que se le den a estos equipos.

ADMINISTRACIÓN DEL CTI

La administración se define como el **proceso de crear, diseñar y mantener un ambiente** en el que las personas a laborar o trabajar en grupos, alcancen con eficiencia metas seleccionadas. Las personas realizan funciones administrativas de planeación, organización, integración de personal, dirección y control.

- La administración se aprovecha en todo tipo de corporación
- Es aplicable a los administradores en todos los niveles de la corporación
- La administración se ocupa del rendimiento; esto implica eficacia y eficiencia

7.1 Unidad de Servicios de Cómputo Académico (UNICA)

El CTI formará parte de La Unidad de Servicios de Cómputo Académico que será la encargada de administrarlo, por tal motivo es conveniente conocer un poco acerca de la historia de esta Unidad y de las actividades que se realizan.

7.1.1 Historia

Surge en el año de 1994 cuando se decide seccionar el Centro de Cálculo, con la finalidad de proporcionar una mayor eficiencia en el desempeño del personal. Con base a esto, se crean dos Unidades para desempeñar el trabajo que realizaba el Centro de Cálculo. La **Unidad de Servicios de Cómputo Académico (UNICA)** y la **Unidad de Servicios de Cálculo Administrativo (USECAD)**, son las dos unidades creadas para llevar a cabo las tareas Académicas y Administrativas de la Facultad de Ingeniería.

La excelencia de UNICA se debe a que una de sus principales actividades es brindar el mejor servicio a los usuarios para ayudar en su formación como futuros profesionistas, en base a esta premisa es que se planeó contar con una nueva sala de cómputo para los alumnos de la Facultad, no solo de licenciatura sino también, para los alumnos de Posgrado. En UNICA, uno de los objetivos fundamentales es cumplir con los requerimientos de los clientes en el área de cómputo, teniendo como meta elevar la calidad de sus productos y servicios, para ello hay un compromiso de mejora continua.

7.1.2 Organización

La Unidad se compone del Departamento de Servicios Académicos (DSA), el Departamento de Investigación y Desarrollo (DID), el Departamento de Redes y Operación de Servidores (DROS), la **Coordinación de Salas de Cómputo (CSC)** y el Departamento de Seguridad en Cómputo (DSC).

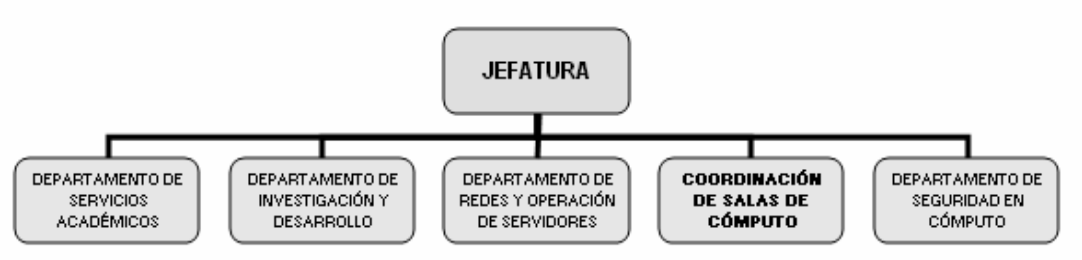

Figura 7.1 Organigrama de UNICA

La función principal de la **Coordinación de Salas de Cómputo (CSC)** es la de proporcionar el servicio de cómputo y de impresión a los alumnos de la Facultad, para que éstos puedan realizar sus trabajos y tareas de investigación, además proporciona servicio de correo electrónico, acceso a Internet y servicios varios de apoyo en material de cómputo.

Para ello se cuenta con **cuatro salas de atención a usuarios,** una en el edificio principal, dos en la División de Ciencias Básicas y una en el edificio de Posgrado; en las que se cuenta con un total de **253 computadoras personales**, **13 impresoras** y **5 estaciones de trabajo,** como equipo al servicio exclusivo de los alumnos, el que se complementa con 9 servidores y las computadoras necesarias para la administración y control del servicio.

El horario de servicio de las diferentes salas, así como del CTI es de **lunes a viernes**, de **9 de la mañana a 8:45 de la noche**, en módulos de dos horas al día.

7.1.3 Política de calidad

Misión

UNICA es una coordinación de la **Secretaría General** de la Facultad de Ingeniería,

cuya finalidad principal es la de **proporcionar, en el ámbito institucional, los servicios de apoyo en cómputo que la comunidad de la Facultad requiere**, recursos de cómputo comerciales y de alta especialización que el avance de la educación, en el desarrollo de la informática y el ejercicio profesional demanden.

Visión

Mantener el liderazgo y estar a la vanguardia en cómputo tanto dentro de la Facultad de Ingeniería como en el entorno universitario.

Otra de las funciones de la Unidad es la de proporcionar el servicio de cómputo y asesorías en el mismo rubro a los alumnos de la Facultad, para que éstos puedan realizar sus trabajos y tareas de investigación así como la de imprimir sus trabajos escolares.

7.2 Organización y división de las responsabilidades dentro del CTI

La **división de responsabilidades** permite lograr **la revisión y los balances sobre la calidad del trabajo**. Cada persona que labora en el CTI debe tener diferentes actividades dentro del lugar, de manera que se puedan organizar para que puedan dividirse las responsabilidades.

En el CTI se contemplan 3 puestos principales que desarrollan las siguientes actividades:

- **Prestadores de servicio social:** Como su nombre lo menciona, son personas que realizan el servicio social, contemplado como requisito dentro de todos los programas de las carreras de Ingeniero en la Facultad, estas personas reciben capacitación para desarrollar actividades sencillas pero fundamentales dentro del CTI.
- **Becarios:** Son personas que dentro de la Unidad de Servicios de Cómputo Académico, desarrollan proyectos académicos, además de impartir cursos y en el caso específico del CTI dar asesorías a los usuarios con respecto a la utilización del software de aplicaciones instalado en los equipos.
- **Coordinadores:** Son las personas encargadas de la administración del CTI, por

ende, este es el puesto de mayor responsabilidad, la labor de los coordinadores es la de supervisar y controlar la administración de los servidores, gestionar el acceso de los usuarios al interior del CTI, mantener en buen funcionamiento el equipo de cómputo, así como, dar cursos de computación. Considerando las dimensiones y el alcance del CTI dependerá su infraestructura y en consecuencia su organización.

7.3 Acceso y préstamo de equipos de cómputo

Al iniciar cada semestre, los alumnos de la Facultad de Ingeniería deberán registrarse para darse de alta en la base de datos del sistema y poder acceder a los servicios que prestará el CTI. Una vez dados de alta, recibirán un comprobante con la confirmación del alta del servicio, en el mismo se les proporcionará una cuenta de correo electrónico además de un nombre de usuario y contraseña para poder consultar dicho correo.

Ya registrados los usuarios, para que se le otorgue el préstamo de un equipo de cómputo deberán presentar a la entrada su credencial de alumno actualizada; para llevar un control sobre el préstamo de los equipos, se cuenta con una aplicación llamada **SCOSU**[1] es esta aplicación, como se muestra en la figura siguiente, se muestran bloques numerados que representan los equipos de cómputo a préstamo:

Figura 7.2 Distribución de equipos de cómputo

[1] Sistema de Control de Salas de UNICA, aplicación desarrollada para controlar la entrada y salida de usuarios a los que se les asigna un equipo en préstamo.

Los bloques en color gris significan equipos de cómputo libres, en tanto que los bloques mostrados con algún color implican un equipo de cómputo ya asignado a un alumno.
Para asignar un equipo a un usuario, basta con capturar, mediante el teclado o un lector de código de barras el número de cuenta que aparece en la credencial del alumno, con ello, en pantalla se mostrarán los siguientes datos:

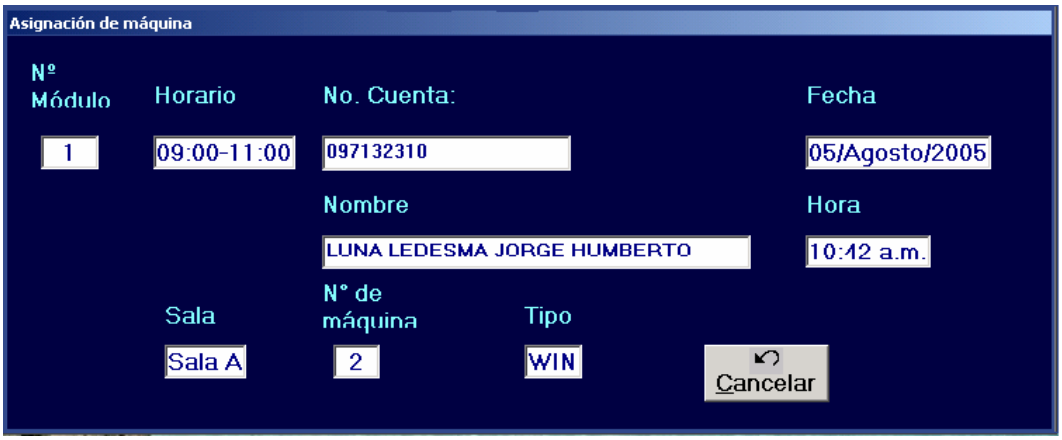

Figura 7.3 Asignación de equipo de cómputo

En la figura anterior se puede apreciar el número de cuenta así como el nombre del alumno, el horario en el que se le otorga el préstamo del equipo, así como el número de máquina que puede utilizar y en que sala se encuentra ubicado este equipo. El tiempo máximo del préstamo del equipo es de **2 horas diarias.**

7.4 Servicio de impresión

En el capítulo 4.6 se habló sobre la configuración del servidor de impresión así como la manera para que usuarios con equipos portátiles pudieran imprimir sus trabajos. Con respecto a la política de impresión esta contempla los siguientes puntos:

- Solo se podrán imprimir trabajos estrictamente académicos, correspondientes a la Facultad de Ingeniería
- El usuario deberá avisar a control de salas para poder imprimir
- Los trabajos deben ser personales, evitando imprimir trabajos de amigos o compañeros, aunque estos también sean alumnos de la Facultad
- Todos los trabajos se imprimirán en hojas tamaño carta, blancas por ambos lados, no se permite el uso de hojas de rehuso, hojas de color ni imprimir por

ambos lados de la hoja

- El tiempo máximo para el uso de impresión será de 5 minutos, esto con el fin de agilizar su uso
- No se podrá realizar ningún tipo de modificación a los trabajos en el servidor de impresión, si se requiere modificar será necesario el préstamo de un equipo

Las impresoras cuentan con una configuración predeterminada, razón por la cual es responsabilidad del usuario adaptar sus programas y trabajos, de modo que la impresión sea correcta. No esta permitido alterar la configuración de las impresoras. En caso de ser necesario y de proceder, deberá acudir al encargado del CTI para realizar el ajuste correspondiente.

Se considera que un usuario hace mal uso de la impresora si:

- Imprime archivos con fines no académicos o para otra(s) persona (s)
- Envía “basura” a la impresora, lo cual provoque que esta se bloquee
- Cambiar la configuración de las impresoras
- Imprimir en papel acerado (especial para impresoras de inyección de tinta)
- Imprimir acetatos
- Imprimir documentos voluminosos como manuales, tesis entre otros

7.5 Asesorías

UNICA ofrece el servicio de asesorías en horarios determinados en el CTI. Es indispensable que al acudir con un asesor, sea con una duda específica sobre problemas relacionados con el uso de los equipos. El asesor tiene la responsabilidad de resolver dudas específicas por lo tanto el usuario debe definir el problema y plantear su duda al asesor.

En esta actividad los asesores están al pendiente en dichas salas por si algún alumno tiene dificultades en algún software que en esos momentos esté utilizando, es entonces cuando ellos van a su lugar y se trata de aclarar sus dudas o resolverlas.

También cuando se llega a descomponer algún equipo o parte de éste, como los teclados, monitores o las unidades lectoras de discos de 3 ½, ellos colaboran ya sea cambiando o reparando la pieza afectada, también apoyan en cuanto al mantenimiento, actualizaciones y revisiones constantes no solo en el hardware sino también del software de dichas unidades.

El software de aplicaciones más usado por los estudiantes que ocupan estas salas son regularmente Word, Excel, Power Point, Linux, AutoCad, MatLab, Navegadores por Internet, correo electrónico, también lenguajes de programación como lenguaje C, C++, Java, Visual Basic, HTML, entre otros.

7.6 Cursos de cómputo

Existen varios tipos de cursos impartidos por UNICA:

Cursos semestrales

Estos cursos son abiertos al público en general, para los alumnos de la Facultad de Ingeniería no tendrán costo alguno. Los cursos semestrales se imparten en las siguientes fechas:

Enero-Febrero
Junio
Noviembre-Diciembre

Cursos intersemestrales

Estos cursos son abiertos al público en general y tienen una duración de dos semanas en sesiones de 3 horas. Los cursos intersemestrales tentativamente se imparten en el mes de septiembre

Cursos sábados y domingos

Los cursos sabatinos tienen una duración de dos a tres fines de semana según el curso, se imparten en sesiones de tres horas cada día y se imparten en las siguientes fechas:

Marzo-Abril
Septiembre

Cursos especiales

Son cursos impartidos a personal miembro de alguna dependencia de la Facultad de Ingeniería. Para poder llevar a cabo un curso de este tipo el personal interesado deberá acudir con el jefe de la dependencia a la que pertenecen, y él deberá solicitar en forma oficial a UNICA el curso.

Cursos externos

Son cursos impartidos a personal miembro de alguna empresa privada. Para poder llevar a cabo un curso de este tipo la empresa deberá solicitar en forma oficial a la Unidad la impartición del curso. La unidad le indicará a la empresa los requerimientos y costo del curso.

Cursos internos

Son cursos impartidos a personal miembro de UNICA y tienen como finalidad capacitar a su personal para mantenerlo a la vanguardia en el ámbito tecnológico.

A continuación se muestran los cursos que se imparten en la Unidad:

- 3D Studio Max
- Access
- Action Script (Flash)
- Administración de Servicios WEB con Apache
- Administración de Linux
- Administración Solaris
- Administración y Seguridad en WEB
- ASP
- Autocad Básico
- Autocad Avanzado
- Bases de Datos y SQL con ORACLE
- Computación para Niños
- Cristal Report
- Delphi 6.0 Básico
- Dreamweaver

- Excel
- Flash MX
- Fundamentos de JAVA.
- Fundamentos de MatLab
- HTML
- Internet
- Introducción a la Computación
- Introducción a Redes de Computadoras
- Introducción a Office 2000
- Java con Base de Datos
- JavaScript
- JSP con Bases de Datos
- Lenguaje C Básico
- Linux Básico
- Mantenimiento Preventivo de PC's
- Office 2000 para niños
- PERL
- PHP
- PL/SQL
- Programación en Linux con comandos Shell Script
- Redes Novell
- Solaris
- Visual Basic Básico y Avanzado
- Visual Basic con Bases de Datos
- Visual Basic Orientado a Objetos y Base de Datos con ODBC
- Visual Fox Pro 6.0 Básico
- Windows NT

7.7 Reglamento aplicable al CTI

Debido al tipo de servicio que prestará el CTI, las reglas para mantener un cierto control y orden son indispensables, por tanto el manejar un reglamento que delimite lo que los usuarios pueden o no hacer es muy importante.

UNICA proporciona servicios de cómputo a la comunidad de la Facultad de Ingeniería y es la encargada de coordinar el CTI. Una de las primeras reglas que los usuarios deben tener presentes menciona lo siguiente: El uso del equipo y de la información que se maneje es para uso **personal y exclusivo de los alumnos de licenciatura y posgrado de la Facultad de Ingeniería y con fines estrictamente académicos.**

Cualquier uso diferente al descrito anteriormente, tal como lucro, esparcimiento o el atentar contra la seguridad e integridad del equipo y los sistemas, será sancionado con la cancelación definitiva del servicio, o hasta con la remisión del problema al Tribunal Universitario.

7.7.1 Alta del servicio

Para hacer uso de los equipos, es necesario acudir al CTI y registrarse con la credencial vigente de la UNAM. Al realizar el registro como usuario, podrá hacer uso del equipo además del CTI, en cualquiera de las 3 salas restantes destinadas para su uso. Las claves para hacer uso del servicio son válidas a partir de la fecha de su expedición, hasta el último día de actividades del semestre escolar.[2]

Cabe resaltar que al realizar el registro como usuario, implica **la aceptación y cumplimiento incondicional del reglamento vigente.**

7.7.2 Procedimiento para solicitar el servicio

El interesado debe presentarse en control de salas, identificarse como alumno de la Facultad, con su credencial vigente y solicitar un equipo, impresión y/o asesorías. El usuario esta comprometido a usar sólo el equipo asignado. No se permitirá el acceso a más de una persona por equipo de cómputo. Una vez concluido el módulo de 2 horas de uso del equipo, el usuario deberá desocupar el mismo.

7.7.3 Disposiciones generales

Las actividades que desarrollen los usuarios dentro de las instalaciones, deben ser personales y de carácter académico, por lo cual queda estrictamente prohibido el uso de

[2] El semestre escolar incluye el periodo de exámenes finales.

juegos de computadora, imágenes, textos o dibujos que no cumplan con un fin específico dentro de las actividades académicas que desarrollen los usuarios.

- Está estrictamente prohibido fumar, introducir comida, bebidas o tirar basura dentro de las salas de trabajo.
- Cualquier actividad que ponga en peligro la integridad de las personas dentro de las instalaciones será sancionada severamente conforme a la Legislación Universitaria.
- Sólo tendrán acceso al CTI los usuarios que cuenten con equipo asignado así como usuarios que requieran de un espacio para utilizar sus equipos portátiles.
- Si un usuario detecta algún desperfecto en el equipo que se le asignó al inicio de su sesión, deberá reportarlo a control de salas.
- Si un usuario provoca un desperfecto, deliberadamente o por desconocimiento, será sancionado.
- Queda absolutamente prohibido ejecutar cualquier ejercicio, programa o actividad que por su naturaleza pudiera atentar contra la seguridad de los sistemas, aunque tales actividades tuvieran carácter académico.

A los usuarios que sean sorprendidos haciendo uso indebido de los equipos se les cancelará el servicio por el resto del semestre.

7.7.4 Sanciones

Dentro del reglamento están contempladas sanciones que aplican en casos en donde los usuarios hacen mal uso de los equipos o instalaciones:

- No esta permitido utilizar el equipo de cómputo para editar imágenes que no tengan relación con actividades académicas, ya que en caso de ser sorprendidos, se les cancelará el servicio permanentemente.
- A toda persona que sea sorprendida modificando, dañando o haciendo mal uso del equipo de hardware, software, red inalámbrica, o que viole los lineamientos establecidos en los reglamentos universitarios, se le cancelará el servicio

definitivamente. En el caso dado deberá restituir los bienes dañados, o será remitido ante las autoridades universitarias correspondientes.

- Queda estrictamente prohibido el uso del CHAT o cualquier software o página parecida, visitar páginas XXX o que no tengan un fin académico.
- No está permitido cambiar el papel tapiz, cambiar la configuración o instalar algún software.
- Está prohibido cambiarse de máquina o andar recorriendo el CTI.

En un panorama general, la Unidad de Servicios de Cómputo Académico, más que administrar el CTI y el resto de las salas de cómputo ofrece una gama de servicios que ayudan a los alumnos a desarrollar sus actividades; con todos los servicios descritos, los alumnos cuentan con las herramientas necesarias que apoyan el desarrollo y aprendizaje a lo largo de su formación profesional.

CONCLUSIONES

Es primordial la necesidad de poner en marcha una nueva sala de cómputo, no solo para satisfacer la demanda del servicio por parte de los usuarios sino para mantener el liderazgo y estar a la vanguardia en cómputo tanto en la Facultad de Ingeniería como en el entorno universitario.

Se cumplió el objetivo general ya que se documentaron los procesos y actividades necesarios para la planificación, organización y mantenimiento del Centro de Tecnología de Información contemplándose todos aquellos elementos como son:

- Tipo de instalaciones
- Determinación de requerimientos para el funcionamiento del CTI
- Selección del equipo de cómputo
- Tipo de software y hardware
- Parámetros de configuración
- Red inalámbrica
- Seguridad informática
- Seguridad en equipos de cómputo e instalaciones
- Mantenimiento preventivo y correctivo
- Administración de equipos de cómputo e instalaciones

En cuestión de **instalaciones físicas**, se logró optimizar la distribución de las áreas de trabajo de manera que se aprovecharan al máximo, también se establecieron planes y medidas de seguridad orientados a la prevención de accidentes. Se optó por adquirir equipos que fueran acordes al tipo de usuarios, contemplando siempre los factores financieros y el tiempo de vida de los mismos. Se definió que software de aplicaciones sería utilizado, así como una política sobre la instalación de software original y licencias de uso.

Uno de los principales logros alcanzados es la puesta en marcha de la **red inalámbrica,** este tipo de tecnología trajo consigo:

- Movilidad de conexión, principalmente con equipos portátiles
- Opciones de instalación simple y flexible
- Costo reducido de adquisición (no genera gastos de cableado o mantenimiento)
- Excelente adaptabilidad para soportar equipos de cómputo adicionales

Se documentaron los pasos a seguir para instalar y poner en funcionamiento los equipos clientes y servidor; el servidor de impresión, el firewall, la salida a Internet, el Punto de Acceso y las tarjetas de red inalámbrica y así como las directivas de configuración y seguridad para equipos desktop. Se estableció una metodología para el mantenimiento físico de equipos de cómputo y periféricos, a nivel preventivo y correctivo. Se documentó también el mantenimiento lógico a los sistemas.

En cuanto a la **administración del CTI** se definieron los servicios que se realizan en el resto de las salas de UNICA y que serán aplicadas al CTI, actividades como:

- Préstamo de equipos de cómputo
- Servicio de impresión
- Asesorías
- Cursos de cómputo

Claro esta, sin dejar pasar por alto el reglamento sobre el uso de equipos e instalaciones del CTI, aplicable a todas las salas de cómputo de UNICA.

APÉNDICES

Apéndice I

FIGURAS

CAPÍTULO 1

CAPÍTULO 3

CAPÍTULO 4

CAPÍTULO 5

CAPÍTULO 6

CAPÍTULO 7

Apéndice II

TABLAS

CAPÍTULO 4

CAPÍTULO 5

CAPÍTULO 6

GLOSARIO DE TÉRMINOS

- **802.11**

802.11, o IEEE 802.11, es un grupo de trabajo del IEEE que desarrolla distintos estándares para el uso de la tecnología de radiofrecuencia en las redes de área local (LAN).

- **ACCESS POINT**

Estación base o punto de acceso que conecta una red cableada con uno o más dispositivos de red inalámbricos. Existen muchos tipos de Access Point en el mercado, con diferentes capacidades: bridge, hubs, gateway, router, y las diferencias entre ellos muchas veces no están claras, porque las características de uno se pueden incluir en otro. Por ejemplo, un router puede hacer bridge, y un hub puede hacer switch.

- **ACTIVE DIRECTORY**

Aplicación que forma parte de la instalación del Sistema Operativo de servidor, controla todos los elementos de configuración del equipo.

- **ACTIVEX**

Componentes software de Microsoft. Activan el sonido, las aplicaciones Java y las animaciones que se desea integrar en una página Web.

- **AD-HOC, MODO**

Un tipo de topología de WLAN en la que sólo existen dispositivos clientes, sin la participación de ningún Access Point, de forma que los clientes se comunican de forma independiente punto a punto, peer-to-peer. Dado que no existe un dispositivo central, las señales pueden ocasionar mayores interferencias reduciendo las prestaciones de la red.

- **AMENAZA**

Cabe definir amenaza, en el entorno informático, como cualquier elemento que comprometa a un sistema.

- **ANILLO**

Topología de red que se basa en un cable que se origina y termina en el equipo central y que interconecta todos los nodos de una red.

- **ANTIVIRUS**

Es un programa que se ejecuta en la computadora para buscar indicios de virus. Si encuentra alguno, guía al usuario en los pasos a seguir para la remoción del mismo. El programa antivirus debe ser actualizado periódicamente con las nuevas definiciones de virus.

- **ATAQUE**

Es la realización de una amenaza.

- **ATAQUE PASIVO**

Es aquel que no causa modificación o cambio en la información o recurso; es decir únicamente lo observa, escucha, obtiene o monitorea mientras está siendo transmitida.

- **ATAQUE ACTIVO**

Es aquel que implica algún tipo de modificación de flujo de datos transmitido o la creación de un falso flujo de datos.

- **APPLET**

Pequeña aplicación en línea desarrollada con Java. Son descargados automáticamente desde la Red y ejecutados en el ordenador de usuario.

- **BASE T**

Estándar Ethernet para transmisión sobre par de cobre a 10 Mbps.

- **BIOS**

Basic **I**nput **O**utput **S**ystem. Sistema básico de entrada y salida. Es un *chip* (circuito integrado) que contiene un conjunto de instrucciones de software para activar los periféricos de la computadora.

- **BROWSER**

Aplicación para visualizar documentos WWW y navegar por el espacio Internet. En su forma más básica son aplicaciones de hipertexto que facilitan la navegación por los servidores de información Internet; los más avanzados cuentan con funcionalidades plenamente multimedia y permiten indistintamente la navegación por servidores WWW, FTP, Gopher, el acceso a grupos de noticias, la gestión del correo electrónico, etc.

- **C, C++**

Lenguaje de programación de alto nivel, utilizado para manejar la computadora a bajo nivel, tal como lo haría un ensamblador.

- **CABLE COAXIAL**

Cable de conexión eléctrica que comprende a la vez un conductor interior y otro exterior. Es utilizado por muchas compañías de televisión por cable y para suministrar conexión a Internet.

- **COOKIES**

Pequeños archivos de texto que un servidor Web almacena en la computadora del usuario, para guardar información sobre éste, como un número de identificación, una contraseña, sus preferencias o cuántas veces ha visitado el sitio el usuario.

- **COMPUTADORA**

Máquina de propósito general que procesa datos de acuerdo con las instrucciones almacenadas en un programa.

- **CONCENTRADOR**

Dispositivo que concentra todas las señales de los nodos y servidores de una red y las envía, una por una, a la computadora central y recibe de ésta la respuesta que envía al nodo correspondiente de acuerdo con un código de dirección.

- **CPU**

Control Processing Unit. Unidad Central de Procesamiento. Parte central de una computadora.

- **CRACKER**

Un "cracker" es una persona que intenta acceder a un sistema informático sin autorización. Estas personas tienen a menudo malas intenciones, en contraste con los "hackers", y suelen disponer de muchos medios para introducirse en un sistema.

- **DATOS**

Conjunto de información lógica que maneja el software y el hardware: bases de datos, documentos, archivos, etc.

- **DIRECCIÓN IP**

Secuencia de números que se utilizan para asignar una ubicación a nivel electrónico. Identifica una computadora determinada dentro de una red.

- **DHCP**

Protocolo de Configuración Dinámica de Host. Servidor que asigna direcciones IP de manera automática de entre un conjunto de direcciones disponibles.

- **DIRECCIÓN MAC**

Identificador único para una computadora a nivel mundial.

- **DISCO FLEXIBLE**

Floppy **D**isk. Disco flexible o disquete. Medio de almacenamiento de archivos, que es portátil y con capacidad para ser grabado y borrado cientos de veces.

- **DNS**

Domain Name System. Sistema de Nombres de Dominio. El DNS un servicio de búsqueda de datos de uso general, distribuido y multiplicado. Su utilidad principal es la búsqueda de direcciones IP de sistemas centrales ("hosts") basándose en los nombres de estos. El estilo de los nombres de "hosts" utilizado actualmente en Internet es llamado "nombre de dominio".

- **ETHERNET**

Es una red con topología tipo bus, con protocolo CSMA/CD, que trabaja en banda base y es capaz de transmitir a 10 MBit/s, emplea codificación Manchester.

- **FAT**

FAT (File Allocation Table o "tabla de ubicación de archivos") es el principal sistema de archivos desarrollado para MS-DOS y Windows.

- **FIREWALL**

Sistema que se coloca entre una red local e Internet. La regla básica es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autentificaron, etc.

- **FREEWARE**

Software que se distribuye sin ningún cargo y bajo ninguna condición. La propiedad la retiene el desarrollador que tiene el control de su distribución, incluyendo la capacidad de cambiar la siguiente versión del freeware a payware (software que se distribuye a cambio de dinero).

- **GATEWAY**

Hoy se utiliza el término "router" (direccionador) en lugar de la definición original de "gateway". Actualmente una pasarela es un programa o dispositivo de comunicaciones que transfiere datos entre redes que tienen funciones similares pero operativas diferentes.

- **GPS**

Global Position System - Sistema de Posicionamiento Global.

- **HACKER**

Pirata. Una persona que goza alcanzando un conocimiento profundo sobre el funcionamiento interno de un sistema, de un ordenador o de una red de ordenadores. Este término se suele utilizar indebidamente como peyorativo, cuando en este último sentido sería más correcto utilizar el término "cracker".

- **HARDWARE**

Conjunto de todos los sistemas físicos del sistema: CPU, cableado, impresoras, CD-ROM, componentes de comunicación, etc.

- **HUB**

Dispositivo en una red que conecta múltiples computadoras para conformar una red LAN.

- **IEEE**

Institute of Electrical and Electronics Engineers. Organización formada por ingenieros, científicos y estudiantes involucrados en el desarrollo de estándares para, entre otros campos, las comunicaciones. Este organismo utiliza los números y letras en una clasificación jerárquica para diferenciar grupo de trabajo y sus normas. Así, el subgrupo 802 se encarga de las redes LAN y WAN, y cuenta con la subsección 802.11 para las redes WLAN.

- **INFRAESTRUCTURA, MODO**

El modo de infraestructura es una topología de red inalámbrica en la que se requiere un Punto de Acceso. A diferencia del modo Ad-Hoc, toda la información pasa a través del Punto de Acceso, quien puede además proporcionar la conectividad con una red cableada y controlar el acceso a la propia red wireless.

- **INTRANET**

Red propia de una organización, diseñada y desarrollada siguiendo los protocolos propios de Internet, en particular el protocolo TCP/IP. Puede tratarse de una red aislada, es decir no conectada a Internet.

- **ISO**

International Organization for Standardization. (Organización Internacional para la Normalización). Organización de carácter voluntario fundada en 1946 que es responsable de la creación de estándares internacionales en muchas áreas, incluyendo la informática y las comunicaciones.

- **JAVASCRIPT**

Es un lenguaje de scripts creado por Netscape, y que permite la programación para cualquier plataforma (al igual que el lenguaje JAVA) de eventos, objetos y acciones que pueden ser utilizados en páginas HTML, estándar.

- **KBPS**

(Kilobits por segundo) Unidad de medida de la velocidad de transmisión por una línea de telecomunicación. Cada kilobit esta formado por mil bits.

- **LAN**

Local Area Network. (Red de Area Local). Red de datos para dar servicio a un área geográfica máxima de unos pocos kilómetros cuadrados, por lo cual pueden mejorar los protocolos de señal de la red para llegar a velocidades de transmisión de hasta 100 Mbps (100 millones de bits por segundo).

- **MAC**

Dirección de control de acceso al medio. En las redes wireless, el MAC es un protocolo de radiofrecuencia, corresponde al nivel de enlace (nivel 2) en el modelo ISO. Cada dispositivo wireless posee una dirección para este protocolo, denominada dirección

MAC, que consiste en un número de 48 bits: los primeros 24 bits identifican al fabricante de la tarjeta, mientras que los restantes 24, a la tarjeta en sí. Este modelo de direccionamiento es común con las redes Ethernet (802.3).

- **OPENBSD**

BSD son las iniciales de Berkeley Software Distribution (en español, Versión de Software Berkeley) y se utiliza para identificar un sistema operativo derivado del sistema Unix nacido a partir de las aportaciones realizadas a ese sistema por la Universidad de California en Berkeley.

- **OSI**

Modelo de Referencia implantado por ISO, Internacional Standard Organization.

- **PROTOCOLO**

Descripción formal de formatos de mensaje y de reglas que dos ordenadores deben seguir para intercambiar dichos mensajes. Un protocolo puede describir detalles de bajo nivel de las interfaces máquina-a-máquina o intercambios de alto nivel entre programas de asignación de recursos.

- **SCOSU**

Sistema de Control de Salas de UNICA, aplicación desarrollada para controlar la entrada y salida de usuarios a los que se les asigna un equipo en préstamo.

- **SOFTWARE**

Elementos lógicos que hacen funcional al hardware: sistema operativo, aplicaciones, programas, etc.

- **SPYWARE**

Son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas.

- **TOKEN RING**

Es un sistema utilizado cuando varios ordenadores están conectados a una red configurada en forma de anillo o de estrella, para evitar la colisión de los datos de dos ordenadores si estos envían sus mensajes a la red al mismo tiempo.

- **TWEAKUI**

Aplicación que permite configurar parámetros ocultos de Windows, y que además de ser gratuito, tiene muchas opciones de restricción de parámetros.

- **VIRUS**

Programa que se duplica a si mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas. Estos programas pueden causar problemas de diversa gravedad en los sistemas que los almacenan.

- **WAR DRIVING**

Localización y posible intrusión en redes wireless de forma no autorizada. Sólo se necesita un portátil, un adaptador wireless, el software adecuado y un medio de transporte.

- **WEP**

Wireless Equivalent Privacy. Privacidad Alterna en redes inalámbricas. Algoritmo de seguridad, de uso opcional, definido en el estándard 802.11. Basado en el algoritmo criptográfico RC4, utiliza una clave simétrica que debe configurarse en todos los equipos que participan en la red. Emplea claves de 40 y 104 bits, con un vector de inicialización de 24 bits. Se ha demostrado su vulnerabilidad y que su clave es fácilmente obtenible con software de libre distribución a partir de cierta cantidad de tráfico recogido de la red.

- **WI-FI**

Wíreles Fidelity. Nombre dado al protocolo 802.11b. Los dispositivos certificados como Wi-Fi son interoperables entre sí, como garantía para el usuario.

REFERENCIAS BIBLIOGRÁFICAS

- Feher, Kamilo.
  Wireless digital communications: Modulation and spread spectrum applications.
  Prentice-Hall PTR.
  Upper Saddle River, N.J., 1995.

- Fragoso Trejo, Héctor Manuel.
  Administración de la tecnología de redes inalámbricas.
  Ed. Iberoamericana.
  México, 2001.

- Huidobro Moya, José Manuel.
  Comunicaciones móviles.
  Ed. Paraninfo.
  Madrid, 2002.

- Stallings, William.
  Wireless communications and networking
  Prentice Hall.
  Upper Saddle River, N.J., 2002.

- Tanenbaum, Andrew S.
  Redes de computadoras.
  Ed. Prentice Hall.
  México, 1987.

- Gómez Ceja, Guillermo.
  Planeación y Organización de Empresas.
  Ed. McGraw Hill.
  México.

- Hernández Jiménez, Ricardo.
  Administración de centros de cómputo.
  Ed. Trillas.
  México.

- Boyce, Jim.
  Conozca y actualice su PC. Guía ilustrada.
  Prentice Hall Hispanoamericana SA.
  1998.

- Norton, Peter.
  Toda la PC.
  Prentice Hall Hispanoamericana SA.
  1994, Quinta edición.

PÁGINAS DE INTERNET

- **Precio Punto de Acceso**
  www.pcenlinea.com/sctg/WIRELESS.html

- **Descripción Punto de Acceso**
  www.3com.com/prod/es_LA_AMER/detail.jsp?tab=features&sku=3CRWE825075A

- **Soluciones wireless**
  http://www.technidata.com.mx

- **Definición de Matlab**
  http://www.monografias.com/trabajos5/matlab/matlab.shtml

- **Funcionamiento de las WLAN**
  http://www.uag.mx/servicios/red_wlan.htm

- **Historia de las redes inalámbricas**
  http://www.tecnotopia.com.mx/redes/redinalambricas.htm

- **Gráfica sobre topología**
  http://www.infoguia.net/foros/uploads/post-233-1064265911.jpg

- **Tecnología y topología de redes inalámbricas**
  http://www.microsoft.com/latam/technet/articulos/windowsxp/2008/default.asp

- **Estándares IEEE**
  http://standards.ieee.org/wireless/

- **Página sobre redes de la Facultad de Ingeniería**
  http://www.fi-b.unam.mx/pp/profesores/jaqui/

- **Amenazas lógicas de seguridad informática**
  http://es.tldp.org/Manuales-LuCAS/SEGUNIX/unixsec-2.1-html/node12.html

- **Mantenimiento de un switch**
  http://img2.insight.com/graphics/uk/products/lg/3cmna0382u_lg.jpg

- **Mantenimiento preventivo y correctivo a computadoras**

  http://www.i-kiosko.com.mx/mantenim.htm

  http://redescolar.ilce.edu.mx/redescolar/cursos/sepacomputo/manten.pdf

  http://redescolar.ilce.edu.mx/redescolar/cursos/sepacomputo/mantecuader.pdf

- **Configuración de Access Point con Openbsd**

  http://www.usebox.net/jjm/obsd-wifi/guia/obsd-wifi.html

- **Glosario wireless**

  http://www.gammainternet.com/tecnologia/wireless/glosario.html#802.11

- **Configuración de impresora Hp Laserjet 4050**

  http://h200002.www2.hp.com/bc/docs/support/SupportManual/bpl06884/bpl06884.pdf

- **Configuración de tarjeta de red**

  http://www.3com.com/prod/es_LA_AMER/detail.jsp?tab=features&sku=3CRDAG675

- **Información sobre la red UNAM**

  http://www.nic.unam.mx/

- **Página oficial de Dell**

  http://www.dell.com.mx

- **Página oficial de Hewlett Packart**

  http://www.hp.com.mx