



**UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO**

**FACULTAD DE ESTUDIOS SUPERIORES
ARAGÓN**

**CONTROL Y ADMINISTRACIÓN DEL
LABORATORIO DE TIC, ÁREA RyT DE LA
UNIVERSIDAD TECNOLÓGICA DE
NEZAHUALCÓYOTL**

**INFORME DEL EJERCICIO
PROFESIONAL**

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

JUAN ESTEBAN YÁÑEZ YÁÑEZ



**ASESOR:
MTRO. GASTALDI PÉREZ JUAN**

MEXICO, 2014



Universidad Nacional
Autónoma de México



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

Dedicatoria

*Quiero dedicar este trabajo de titulación a la persona que siempre
Creyó en mí y siempre me apoyo para continuar estudiando y
Seguir esforzándome cada día por ser mejor persona.
Gracias mamá por todo tu amor.*

*También quiero dedicar especialmente este trabajo
A la mujer que con su amor incondicional siempre
Me apoya y me ha dado una hermosa Familia.
Gracias Vero, te amare por siempre.*

*Por último, quiero dedicar este logro a mis
Hijos, los cuales son la luz de mi vida.
Liset y Carlos Yáñez Sandoval.*

Agradecimientos

*Quiero agradecer primero que nada a Dios,
Nuestro Señor Padre por su infinito Amor,
Gracias Dios mío por todo lo que me has dado.*

*Agradezco a mis Padres por su esfuerzo,
Por todo su Amor y Cariño incondicional.
Porque ustedes me han guiado por la Vida.*

*Gracias a todas las Personas que tienen la
Vocación para enseñar y han marcado mi
Camino y espero poder seguir sus pasos.*

Resumen

CONTROL Y ADMINISTRACIÓN DEL LABORATORIO DE TIC ÁREA RYT

El presente trabajo tiene como objetivo mostrar el desarrollo de un Plan estratégico de Control y Administración de los laboratorios de computo de la división académica de TIC, área Redes y Telecomunicaciones (RyT).

Dicho plan es el resultado de una investigación a través del método de FODA para obtener las mejores estrategias, además de los datos estadísticos que se obtuvieron durante los periodos del 2007-1 al 2009-3 de la aplicación del sistema de Grado de Satisfacción del Cliente (GRASC) donde uno de los puntos más críticos fue la infraestructura de los laboratorios, donde se pudo percatar que no existía un plan de control, ya que los usuarios muchas veces hacían un uso indebido de los laboratorios, por ejemplo instalar programas o juegos, además de desconfigurar los equipos de la red e infectarlos, ya que no se contaba con un antivirus corporativo con licenciamiento por ejemplo.

Dicho trabajo comprende en el apartado de “introducción” los antecedentes de la Universidad, así como de la división académica de Telemática y posteriormente la creación de la división de TIC, área RyT y los problemas que dicha división tuvo durante la implementación del área de Multimedia y Comercio Electrónico (MCE), con respecto a la parte de infraestructura de los laboratorios de cómputo para poder soportar ambas carreras en una misma división académica, además de la falta de un plan de Control y Administración de dicha infraestructura.

Cabe señalar que en este apartado también se establece el marco teórico sobre la función de los manuales administrativos y su clasificación, además de la forma en que están estructurados y como se deben desarrollar de acuerdo a su función.

Por lo cual, en los siguientes capítulos se desarrolla un plan estratégico, el cual consta de la elaboración de tres manuales principalmente, el primero de ellos involucra el desarrollo de las funciones y actividades de cada uno de los responsables de los laboratorios de cómputo, además de la propuesta de un coordinador, el cual lleva a cabo las actividades del administrador de la red y coordina a los responsables de cada laboratorio para llevar a cabo las diversas actividades con respecto a su puesto, de acuerdo a la elaboración de un directorio de responsables de cada laboratorio.

En el segundo manual se establecen las políticas de cada laboratorio, por lo que se elaboró un reglamento interno junto con diversos formatos de control como horario de clases, préstamo de equipos y orden de servicio entre otros, así como las políticas de acceso y control de dichos laboratorios, como el mantenimiento del software y restricciones.

Por último el tercer manual contempla la administración de la red, a través de un manual de funciones específicas para la implementación de nodos de red, además de la elaboración de los diferentes cables de red necesarios para su funcionamiento, así como un manual de operación para la administración de un servidor DHCP, en el cual se establece un rango de asignación mediante la reservación de las direcciones IP de los equipos de acuerdo a su dirección MAC, por lo cual el coordinador puede fácilmente identificar que equipos se encuentran activos en la red y cuáles no, además de identificar direcciones IP duplicadas.

Índice

INTRODUCCIÓN	10
Antecedentes de la UTN.....	10
Objetivos	11
Misión.....	11
Visión	12
Organigrama General de la UTN	13
Antecedentes de la división académica de TIC, Área RyT	14
Problemática.....	15
Análisis FODA de las carreras TIC-RT y MCE	16
Justificación	18
Objetivo General	20
Objetivos Particulares	20
CAPÍTULO 1.- PLAN ESTRATÉGICO PARA EL LABORATORIO DE TIC, ÁREA RYT21	
CAPITULO 2. MANUAL ESPECÍFICO DE ORGANIZACIÓN DEL LABORATORIO DE TIC, ÁREA RYT	25
2.1 Organigrama Específico de TIC, Área RyT	26
2.2 Manual Especifico de Organización.....	26
2.2.1 Funciones y Actividades.....	27
2.2.2 Descripción de puestos.....	35
2.3.2 Directorio del Laboratorio de TIC, Área RyT	50
CAPITULO 3. MANUAL DE POLITICAS DEL LABORATORIO DE TIC, ÁREA RYT	51
3.1 Políticas de Seguridad y Control	52
3.1.1 Manual de Políticas de acceso.....	53
3.2 Políticas de uso y control para el laboratorio de RIC área RyT	56
3.2.1 Parches y actualizaciones.....	56
3.2.2 Protección contra virus y spyware	57
3.2.3 Directivas de Restricción de Software.....	60

3.2.3.1 Manual de Directivas de Restricción de Software.....	61
3.2.4 Restauración del sistema operativo.....	68
3.2.4.1 Manual de Restauración del Sistema Operativo	70
CAPITULO 4. MANUAL DE FUNCIÓN ESPECÍFICA PARA LA	
 ADMINISTRACIÓN DE LA RED	75
4.1 Manual de implementación de un Servidor DHCP	77
4.1.1 Instalación del Servidor DHCP	77
4.1.2 Configuración del Servidor DHCP.....	81
4.1.3 Configuración de un Cliente DHCP	88
4.1.4 Administración del Servidor DHCP	90
CONCLUSIONES	96
Glosario	98
Bibliografía	99
ANEXO A.- Formato de Horario de Clases del laboratorio	101
ANEXO B.- Formato de Control de Practicas del laboratorio	102
ANEXO C.- Formato de Control de Fallas del laboratorio	103
ANEXO D.- Formato de Uso Extra clase del laboratorio	104
ANEXO E.- Formato de Orden de Servicio	105
ANEXO F.- Tabla de direccionamiento IP	106
ANEXO G Inventario técnico para un laboratorio	107

INTRODUCCIÓN

En México, los jóvenes que concluyen los estudios de nivel medio superior tienen, después de por lo menos doce años de educación formal, la opción de continuar con los estudios de licenciatura constituye prácticamente la única alternativa de educación formal posbachillerato.

Por lo que con la finalidad de ampliar las opciones de educación superior a quienes concluyen su bachillerato, la Secretaría de Educación Pública (SEP) ha concebido el Sistema de *Universidades Tecnológicas* (UT's).

Las *UT's* creadas en 1991 a partir del análisis de sistemas educativos internacionales y nacionales, se presentan actualmente como una alternativa viable de educación a nivel superior para los estudiantes de Educación Media Superior que se encuentren interesados en incorporarse al mercado de trabajo en corto tiempo.

ANTECEDENTES DE LA UTN

La *Universidad Tecnológica de Nezahualcóyotl* (UTN) es un organismo público descentralizado, que se crea a partir de 1991 como un ciclo corto de educación superior, a cargo del Gobierno del Estado de México, con personalidad jurídica propia e integrada a la *Coordinación General de las Universidades Tecnológicas* (CGUT).

La UTN inicia actividades en septiembre de ese año, en los terrenos del que fue el Club Deportivo Neza, a un lado del Estadio de Fútbol Neza 86, su dirección fiscal es Circuito Universidad Tecnológica S/N Col. Benito Juárez C.P. 57000 en Ciudad Nezahualcóyotl.

Dicha Universidad se constituye como miembro fundador del *Subsistema Nacional de Universidades Tecnológicas* (SNUT) y tiene por principal objetivo impartir educación tecnológica de tipo superior para la formación de recursos humanos, aptos para la aplicación de conocimientos y la solución creativa de los problemas, con un sentido de innovación en la incorporación de los avances científicos y tecnológicos, de acuerdo con los requerimientos del desarrollo

económico y social de la región, del Estado y del País; ésta trabaja con el modelo pedagógico propio del subsistema, a partir de un currículo organizado en torno a tres ejes rectores: el general especializado, el teórico-práctico y la vinculación escuela-planta productiva, con el objetivo principal de crear Técnicos Superiores Universitarios en las siguientes divisiones académicas:

- Tecnologías de la Información y Comunicación (TIC)
 - Área sistemas Informáticos (SI)
 - Área Redes y Telecomunicaciones (RyT)
 - Área Multimedia y Comercio Electrónico (MCE)
- Administración de Empresas
- Procesos de Producción
- Tecnología Ambiental
- Comercialización

La formación en la UTN tiene una duración de dos años para una carrera técnica universitaria, desarrollada en estudios cuatrimestrales bajo un novedoso modelo educativo, basado en un 30% de teoría y un 70% de práctica para formar al Técnico Superior Universitario (TSU), en un periodo de 6 cuatrimestre, siendo el último de ellos una estadía profesional

Objetivos

- Impartir estudios de Calidad y de formación polivalente que permitan al egresado desempeñarse profesionalmente en una amplia gama de actividades productivas.
- Combinar los estudios en aula, taller y/o laboratorio, prácticas y estadías en la planta productiva de bienes y servicios.
- Impulsar las aptitudes, capacidades y habilidades del estudiante para que pueda desempeñarse profesionalmente en una empresa, o para prestar sus servicios libremente.

Misión

Ofrecer educación superior de calidad y excelencia, vinculada con la sociedad y el sector productivo, para formar profesionales que impulsen el desarrollo del

país, con profunda responsabilidad social y solidad preparación tecnológica, humanística y científica que los mantenga competitivos nacional e internacionalmente.

Visión

Ser una institución de educación superior de alta calidad y excelencia académica, vinculada con su entorno, vanguardista, con liderazgo en el sistema de educación universitaria tecnológica y reconocimiento nacional e internacional, que ofrezca las mejores perspectivas del ejercicio profesional tecnológico a través de un desarrollo integral y competitivo que coadyuve al fortalecimiento de la Nación.

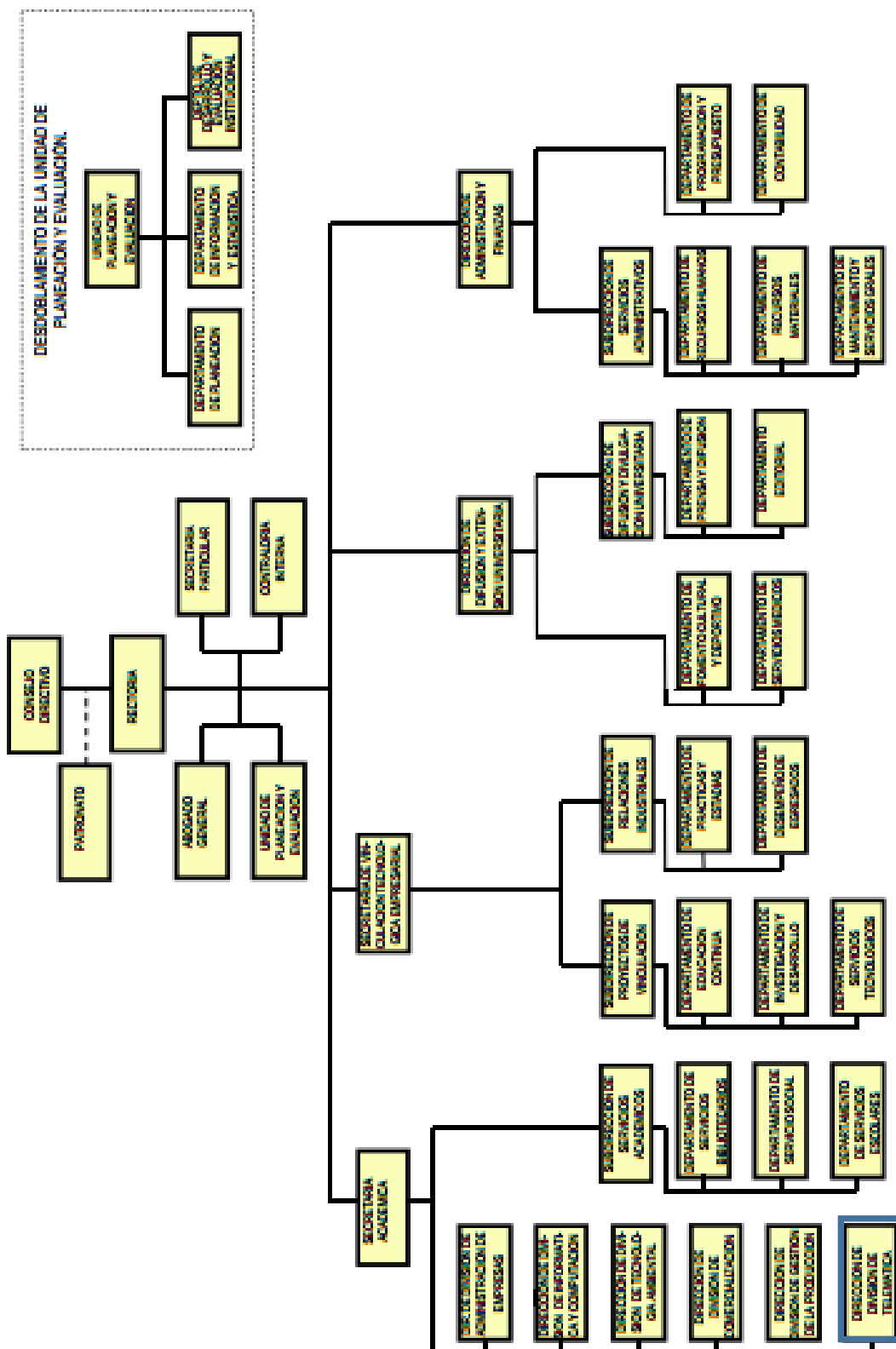
Cada una de sus carreras técnicas actualmente cuenta con un edificio de clases y su propio laboratorio de prácticas, por lo que cada una de estas carreras demanda una calidad de servicio en cuanto a infraestructura en equipo de cómputo, pero sobre todo en cuanto al adecuado y el eficiente traslado de la información y uso de los servicios de Internet.

A continuación se presenta el organigrama general de la UTN, donde se puede apreciar la división de Telemática, como parte de la Secretaria académica, de acuerdo a la información obtenida desde el siguiente enlace:

Disponible en: http://transparencia.utn.edu.mx/htm/organigrama_utn.pdf, 2012

Organigrama General de la UTN

VI. ORGANIGRAMA DE LA UNIVERSIDAD TECNOLÓGICA DE NEAHUACÓYOTL



ANTECEDENTES DE LA DIVISIÓN ACADÉMICA DE TIC, ÁREA RYT

La División de Telemática fue creada por las necesidades en el área de telecomunicaciones detectadas en las empresas del entorno del municipio de Nezahualcóyotl y por la necesidad de brindar oportunidades de desarrollo a los jóvenes de los municipios del oriente del Estado de México. Por lo cual en el año de 1996 surge dicha división como un área académica, la cual fue una respuesta a la creciente demanda en Educación Superior especializada en el área de las Telecomunicaciones con las aplicaciones de la Informática.

Es importante destacar que cada división académica cuenta con sus propios laboratorios para el desarrollo y fortalecimiento del proceso enseñanza-aprendizaje de acuerdo al modelo educativo mencionado anteriormente, por lo cual la importancia que tienen los laboratorios, acordes a las necesidades del perfil de egreso del TSU de acuerdo a la carrera cursada.

Por lo que respecta a la división de Telemática cuenta actualmente con un laboratorio general para la aplicación del modelo educativo, que a su vez se subdivide en cinco laboratorios de cómputo: *Sistemas, Redes, Informática, Linux y Windows 2K (W2K)*; y tres laboratorios de telecomunicaciones (*Telecomunicaciones, Electrónica y Física*), asimismo la actividad que directamente se relaciona con el uso de este tipo de laboratorios, es el cumplimiento de las **prácticas** realizadas por las asignaturas del área tecnológica y establecidas en el plan cuatrimestral de curso de cada una de dichas asignaturas pertenecientes a las diferentes academias que conforman la división académica.

A partir del año 2006 se fusionan las divisiones de Informática, Telemática y Ofimática, dando como resultado la División Académica de *Tecnologías de la Información y Comunicación (TIC)* con la especialidad en el *Área de Redes y Telecomunicaciones (RyT)*, así como la especialidad en el *Área de Aplicación de Sistemas Informáticos (SI)*, además de la especialidad en el *Área de Multimedia y Comercio Electrónico (MCE)*.

PROBLEMÁTICA

Como resultado de esta fusión, la división de Telemática (Área Redes y Telecomunicaciones) tuvo que compartir sus instalaciones con la nueva Área de Multimedia y Comercio Electrónico (MCE), lo cual originó que algunos profesores tuvieran que participar en ambas divisiones, además de que la infraestructura del Área de RyT también tuvo que ser asignada para ambas áreas, lo cual ocasionó una disminución en el porcentaje de aprovechamiento de los alumnos del 70% de practica asignado por el modelo académico.

Sin embargo el problema se fue agravando con el paso de los años ya que la construcción de un nuevo laboratorio para el área de MCE se fue retrasando y la utilización de la infraestructura de los laboratorios de cómputo fue sobre utilizada, además de no contar con un plan de mantenimiento y control adecuado, por lo cual se pudo observar un aumento en el índice de alumnos que desertaban en los periodos del 2007-1 al 2009-3 en la división de TIC, Área RyT principalmente.

Dichas estadísticas representan de manera cuatrimestral un promedio de 708 alumnos de nuevo ingreso, de los cuales aproximadamente 264 alumnos desertan por diferentes causas, lo cual representa que el 37% de la población abandona los estudios, de acuerdo a los siguientes datos obtenidos del informe anual de actividades de la Universidad durante el año 2009, realizado para cada división académica mencionada:

Área RyT	2007- Cuatrimestre 1	2007- 2	2007- 3	2008- 1	2008- 2	2008- 3	2009- 1	2009- 2	2009- 3
Ingreso	767	556	788	755	561	805	758	817	571
Deserción	280	274	237	279	169	229	287	339	280

Fuente: Informe anual de actividades 2009, Universidad Tecnológica de Nezahualcóyotl

Debido a dicha situación se propone realizar un análisis FODA sobre dichas áreas y determinar las posibles causas en el aumento de deserción.

Análisis FODA de las carreras TIC-RT y MCE

Se propone una **metodología** basada en el planteamiento del problema a través de un análisis detallado sobre las Fortalezas, Oportunidades, Debilidades y Amenazas, mejor conocido como FODA, sobre la división académica de TIC área MCE y particularmente sobre el área de RyT, además también se realizará el análisis estadístico de los datos de los problemas con mayor incidencia del área en estudio para posteriormente realizar una delimitación del problema y obtener una propuesta de solución.

A continuación se presenta el siguiente análisis FODA, realizado a las carreras de TIC, área RyT, así como Multimedia y Comercio Electrónico (MCE):

Fortalezas	Debilidades
<p>F1. La carrera de TIC, es de vanguardia con amplio espectro de crecimiento y desarrollo debido a que su mapa curricular es el mismo en todo el subsistema.</p> <p>F2. TIC, área RyT posee un sólido vínculo con el sector empresarial, principalmente con la empresa CISCO SYSTEMS, siendo una Academia Regional.</p> <p>F3. Participación de profesores en el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE).</p> <p>F4. TIC área RyT cuenta con el reconocimiento del Nivel Uno, por parte del Comité de Ingeniería de los CIEES.</p> <p>F5. Ambas áreas cuentan con una matrícula estable acorde a los recursos disponibles.</p> <p>F6. Su Programa Educativo (PE) se actualiza cada tres años, de acuerdo a las necesidades del sector productivo</p>	<p>D1. Reducción en la obtención de reconocimientos en la aplicación del <i>Examen General de Egreso del Técnico Superior Universitario</i> (EGETSU) tasado en un 60%.</p> <p>D2. Duplicidad de funciones debido a que se comparten los recursos humanos, materiales y tecnológicos del área de RyT con el área de MCE.</p> <p>D3. Aumento en el índice de rotación de docentes entre ambas carreras.</p> <p>D4. Incremento en el índice de deserción en un 37%, en los últimos 3 años en el área de RyT con respecto a la matrícula por cuatrimestre.</p> <p>D5. Ha aumentado el índice de reprobación en un 35%, debido a la falta de medidas preventivas.</p> <p>D6. No se cuenta con un gran número de PTC's con perfil deseable reconocido por el PROMEP.</p>

<p>F7. TIC área RyT tiene la acreditación del CONAIC para su PE.</p> <p>F8. Capacitación de docentes mediante posgrados y cursos de actualización.</p> <p>F9. Certificación ISO/9001:2000 como resultado del SGC en esta Institución.</p> <p>F10. Actualización del personal docente y administrativo con base a los programas anuales de capacitación y recursos financieros disponibles.</p>	<p>D7. Evaluación docente con fluctuaciones de 7.0 hasta 8.5 en los últimos cinco años.</p> <p>D8. Carencia de un programa de control y mantenimiento para el uso de laboratorios.</p> <p>D9. Reducción de horas de prácticas escolares en los laboratorios debido a que se comparten recursos humanos, materiales y tecnológicos del área RyT con el área de MCE.</p> <p>D10. Tener una infraestructura de red insuficiente para cubrir las necesidades de alumnos y docentes.</p>
Oportunidades	Amenazas
<p>O1. El crecimiento del corredor industrial y comercial de la zona de influencia con necesidades marcadas en el área de las TI, lo que permite un incremento de la demanda del servicio educativo relacionado con esta área, por lo que la opción del turno vespertino ofrece la posibilidad de una mayor atención a la creciente demanda de formación educativa en áreas relacionadas con el campo de aplicación de la carrera.</p> <p>O2. Al incrementarse la pirámide poblacional en los grupos de edad de 15 a 24 años, se presenta una ventana de oportunidad para atender a estos grupos de jóvenes que egresan del nivel medio superior. Considerando además que la parte oriental del estado de México se está poblando en un 11% con respecto a otras zonas del mismo.</p>	<p>A1. Existe una mayor competencia, particularmente representada por una unidad de la Universidad Autónoma del Estado de México (UAEM), en el municipio de ciudad Nezahualcóyotl, así mismo el Campus de la Universidad La Salle. Siendo estas opciones igual o más atractivas para la demanda de servicio educativo de nivel superior del municipio, aun cuando se renegociaron las carreras a ofertar en éstas.</p> <p>A2. Perder la certificación de CONAIC por no mantener los requisitos mínimos de infraestructura, matrícula y recursos humanos. Lo cual podría provocar una disminución del presupuesto asignado de acuerdo a una disminución de matrícula, debido principalmente a la pérdida de horas de práctica en los laboratorios.</p>

Fuente: Elaboración propia (2011)

JUSTIFICACIÓN

Para poder obtener un análisis más detallado sobre los problemas que impactan directamente en el índice de alumnos que abandonan sus estudios en las áreas mencionadas, se realizó también un análisis a partir de los resultados obtenidos de la aplicación del sistema de “Grado de Satisfacción al Cliente” (GRASC), el cual se aplica al término de cada cuatrimestre a todos los alumnos de cada división académica, dicho sistema evalúa el desempeño académico de los docentes, el cumplimiento de los programas y además de la evaluación de los servicios proporcionados por la universidad, como son: Servicios médicos, deportivos y de biblioteca, además de evaluar la infraestructura como salones y laboratorios, cabe mencionar que al término de cada evaluación los alumnos pueden expresar sus comentarios.

Cabe señalar que dicho análisis se realizó de acuerdo a los periodos mencionados anteriormente, para el área de RyT, así como para el área de MCE, donde su índice de alumnos reprobados y que desertan es del 25% durante los mismos periodos debido a que su promedio de alumnos es de 418.

Una vez analizados estos resultados se detectó que una de las causas que mayormente influye en la deserción de los alumnos es el problema de la **infraestructura**, con una calificación de 6, donde se tienen los siguientes puntos a destacar:

- Falta de equipamiento de los laboratorios de cómputo.
- Falta de personal de apoyo para la utilización de los laboratorios.
- Falta de mantenimiento al Software y de actualización del mismo.
- Falta de mantenimiento al Hardware y actualización del mismo.
- Problemas de administración y acceso a Red e Internet.
- Carencia de mecanismos para la gestión de clases en los laboratorios de cómputo.

Además de la falta de políticas para el uso apropiado de los laboratorios de cómputo, así como del personal calificado y responsable de los mismos, lo

cual provoca que no se tenga un control de dichos laboratorios, por lo que es difícil poder ofrecer un servicio eficiente y de calidad.

Como resultado del análisis de los datos obtenidos sobre el FODA y el GRASC aplicado en ambas áreas, se pueden establecer las siguientes relaciones con respecto a las debilidades principales de dichas áreas:

- Aumento en el índice de deserción en un 37%, en los últimos 3 años con respecto a la matrícula por cuatrimestre en el área de RyT y 25% en el área de MCE debido a la falta de equipamiento de los laboratorios de cómputo y ampliación de los mismos.
- Reducción de horas de prácticas escolares en los laboratorios debido a que se comparten recursos humanos, materiales y tecnológicos del área RyT con el área de MCE, además de la falta de mantenimiento al Hardware, software y actualización de los mismos.
- Falta de medidas preventivas y carencia de un programa de control y mantenimiento para el uso de los laboratorios de cómputo, así como del personal de apoyo para la utilización de los laboratorios.
- No poseer una infraestructura de red robusta y suficiente para cubrir las necesidades de alumnos y docentes, además de la falta de una administración adecuada para el acceso a Red e Internet.

Debido a las debilidades expuestas anteriormente es necesario contar con un plan que permita reducir el efecto de estas, a través de un ***Plan estratégico para el Control y Administración del laboratorio de TIC, Área RyT***, el cual impactará en la optimización de los recursos de infraestructura, así como personal administrativo y docente de dichas áreas, hasta que se tenga un laboratorio propio para el área de MCE.

Dicho Plan está basado en la creación y puesta en marcha de *manuales específicos de Organización, Políticas y Procedimientos específicos* para la administración de los recursos en tiempo y forma (infraestructura), delimitación

de funciones y responsabilidades para todo el personal involucrado, así como mecanismos de control para el uso adecuado y eficiente de los laboratorios.

Objetivo General

Establecer un Plan Estratégico para lograr una administración y control eficiente del laboratorio de TIC, Área Redes y Telecomunicaciones (RyT) a través de la implementación de manuales específicos de organización, políticas y procedimientos que garanticen su uso adecuado y eficaz.

Objetivos Particulares

- Realizar un Manual específico para el control y mantenimiento de los laboratorios que se tienen actualmente asignados a la carrera de TIC, área RyT.
- Desarrollar un Manual de políticas para la gestión estratégica de los laboratorios del área RyT, así como su uso adecuado de acuerdo a las materias asignadas.
- Implementar y evaluar un Manual de operación para el control, la administración e instalación de la Red de los laboratorios de TIC, área RyT.

Una vez que se ha desarrollado un análisis detallado sobre los principales problemas ocasionados por una sobre utilización de la infraestructura de la división de TIC, área RyT para dar cabida a una nueva área como MCE y la falta de un plan estratégico para lograr una administración y control eficiente de dicha infraestructura, se expone a continuación la relevancia y función de un manual o manuales administrativos para una organización como herramientas de apoyo y control de sus actividades y procedimientos.

Capítulo 1.- Plan estratégico para el laboratorio de TIC, Área RyT

Un plan estratégico involucra elaborar un borrador sobre el propósito, los objetivos y los métodos que utilizará la organización para lograr dichos objetivos. Como tal, este plan es una parte integral del funcionamiento de la organización y es importante que la tarea de desarrollarlo se aborde con seriedad, consideración y atención a los detalles. A continuación se mencionan los siguientes pasos para redactar un plan estratégico para una organización:

1. Contemplar la visión de la organización. Identificar cuáles son las bases, lo que se espera lograr, qué responsabilidades se tienen, a qué segmento de la población desea dirigirse y qué imagen desea proyectar.
2. Redacta cuál es la misión de la organización. El propósito de la misión es resumir el objetivo subyacente o visión de la organización. Los planes estratégicos son una extensión de la misión, ya que es esta última la que guía los objetivos y sirve como un medio para medir el éxito de la organización.
3. Evaluar la posición actual de la organización. Con el fin de trazar un curso para alcanzar las metas y entender en qué punto del proceso de alcanzar dichas metas se encuentra. Se debe de considerar lo siguiente:
 - a) Determinar cuáles son las fortalezas y debilidades.
 - b) Identificar las oportunidades de crecimiento.
 - c) Localizar las amenazas contra el éxito de los planes estratégicos.
4. Enumerar los factores que son necesarios para el éxito. Los planes estratégicos deben incluir detalles específicos sobre los tipos de circunstancias que resultarán en el cumplimiento de las metas.
5. Desarrollar una estrategia para cumplir con cada factor de éxito. Esto debe hacerse en la forma de un plan con pasos detallados, el cual debe esbozar exactamente qué debe hacerse, en cuánto tiempo, con cuánto importe de inversión y quién será el responsable.
6. Dar prioridad a las estrategias según las metas de crecimiento y la viabilidad. Al tener en cuenta todos los pasos necesarios para alcanzar

cada una de las metas, así como su orden de importancia, clasifica tu plan estratégico cronológicamente.

Es importante involucrar a cada miembro de la organización, desde los altos directivos hasta los empleados de medio tiempo, en el desarrollo de la visión y la misión. Al involucrar a todos en este paso de planeamiento estratégico, se promueve una cultura de trabajo en equipo, autonomía y responsabilidad en la organización.

Una vez que se han desarrollado los objetivos particulares para dicho proyecto, en los siguientes capítulos se explica cómo se llevó a cabo la elaboración de cada uno de los manuales propuestos, de acuerdo con la definición y clasificación que realiza Franklin en su libro: Organización de Empresas (2009).

“Los manuales administrativos son indispensables debido a la complejidad de las estructuras de las organizaciones, el volumen de sus operaciones, los recursos de que disponen, la demanda de sus productos, servicios o ambos, y la adopción de tecnología de la información para atender adecuadamente todos estos aspectos, y más.

Estas circunstancias obligan a usar manuales administrativos que apoyen la atención del quehacer cotidiano, ya que en ellos se consignan, en forma ordenada, los elementos fundamentales para contar con una comunicación, coordinación, dirección y evaluación administrativas eficientes.

Para manejarlos con consistencia y claridad se incluye un procedimiento por medio del cual se analiza con precisión y profundidad el marco de referencia para su diseño, elaboración, presentación, aprobación, manejo, revisión y actualización permanentes.

Es un hecho que los manuales administrativos representan un elemento crucial para el proceso de toma de decisiones, la mejora

continua y el logro de un desempeño por encima del estándar regular.”

De acuerdo a la clasificación de los manuales administrativos que realiza B. Franklin (2009), se utilizará la clasificación básica que realiza en función de su contenido, donde se incluyen los siguientes manuales:

- **Manual de organización.-** Es un documento normativo que contiene, de forma ordenada y sistemática, información sobre el marco jurídico-administrativo, atribuciones, antecedentes históricos, misión, visión, objetivos, organización y funciones de una dependencia o entidad. De este modo se constituye en un instrumento de apoyo para describir las relaciones orgánicas que se presentan entre las diferentes unidades de la estructura organizacional.

Estos manuales contienen información detallada sobre los antecedentes, legislación, atribuciones, estructura orgánica, organigrama, misión y funciones organizacionales. Cuando corresponden a un área específica comprenden la descripción de puestos; de manera opcional pueden presentar el directorio de la organización. Los Manuales de Organización por el alcance de su información se pueden clasificar en:

- Manual General de Organización: refleja la estructura orgánica de la organización en su totalidad.
 - Manual Específico de Organización: comprende las funciones y responsabilidades de una unidad administrativa en especial, de acuerdo a la división administrativa que se posea en la Organización.
-
- **Manual de procedimientos.-** Constituyen un documento técnico que incluye información sobre la sucesión cronológica y secuencial de operaciones concatenadas entre sí, que se constituyen en una unidad para la realización de una función, actividad o tarea específica en una organización.

Todo procedimiento incluye la determinación de tiempos de ejecución, el uso de recursos materiales y tecnológicos, así como la aplicación de métodos de trabajo y control para desarrollar las operaciones de modo oportuno y eficiente.

La descripción de los procedimientos permite comprender mejor el desarrollo de las actividades de rutina en todos los niveles jerárquicos, lo que propicia la disminución de fallas u omisiones y el incremento de la productividad.

- **Manual de políticas.-** También conocidos como de normas, estos manuales incluyen guías básicas que sirven como marco de actuación para realizar acciones, diseñar sistemas e implementar estrategias en una organización.

El Manual de Políticas contiene escritas en él las políticas establecidas por una institución, en este documento se indican la forma de proceder y los límites dentro de los cuales deben enmarcarse las actividades tendientes a alcanzar los resultados Institucionales. Este Manual puede incluir las políticas generales de la institución, así como de las unidades administrativas de la misma. Un manual de políticas es fundamental para asegurar la uniformidad de acción de una institución.

Los Manuales de Políticas por el alcance de su información se clasifican en:

- Manuales Generales de Políticas: abarcan a toda la Institución, incluye como elemento primario todas aquellas disposiciones generales, las cuales las establece cada unidad administrativa a efectos de sus propias responsabilidades y autoridad funcional.
- Manuales específicos de Políticas: se ocupan de una función operacional o una unidad administrativa en particular.
- **De operación**

Estos manuales se utilizan para orientar el uso de equipos y apoyar funciones altamente especializadas o cuyo desarrollo demanda un conocimiento muy específico.

De acuerdo a dicha clasificación, a continuación se explica la función de cada uno de los manuales propuestos para dicho Plan estratégico.

CAPITULO 2. Manual Específico de Organización del Laboratorio de TIC, Área RyT

Los manuales administrativos son medios valiosos para la comunicación, y sirven para registrar y transmitir la información, respecto a la organización, y funcionamiento de la dependencia; es decir, entenderemos por manual de organización en general el documento que contiene, en forma ordenada y sistemática, la información y/o las instrucciones sobre historia, organización, política y/o procedimientos de una institución, que se consideren necesarios para la mejor ejecución del trabajo.

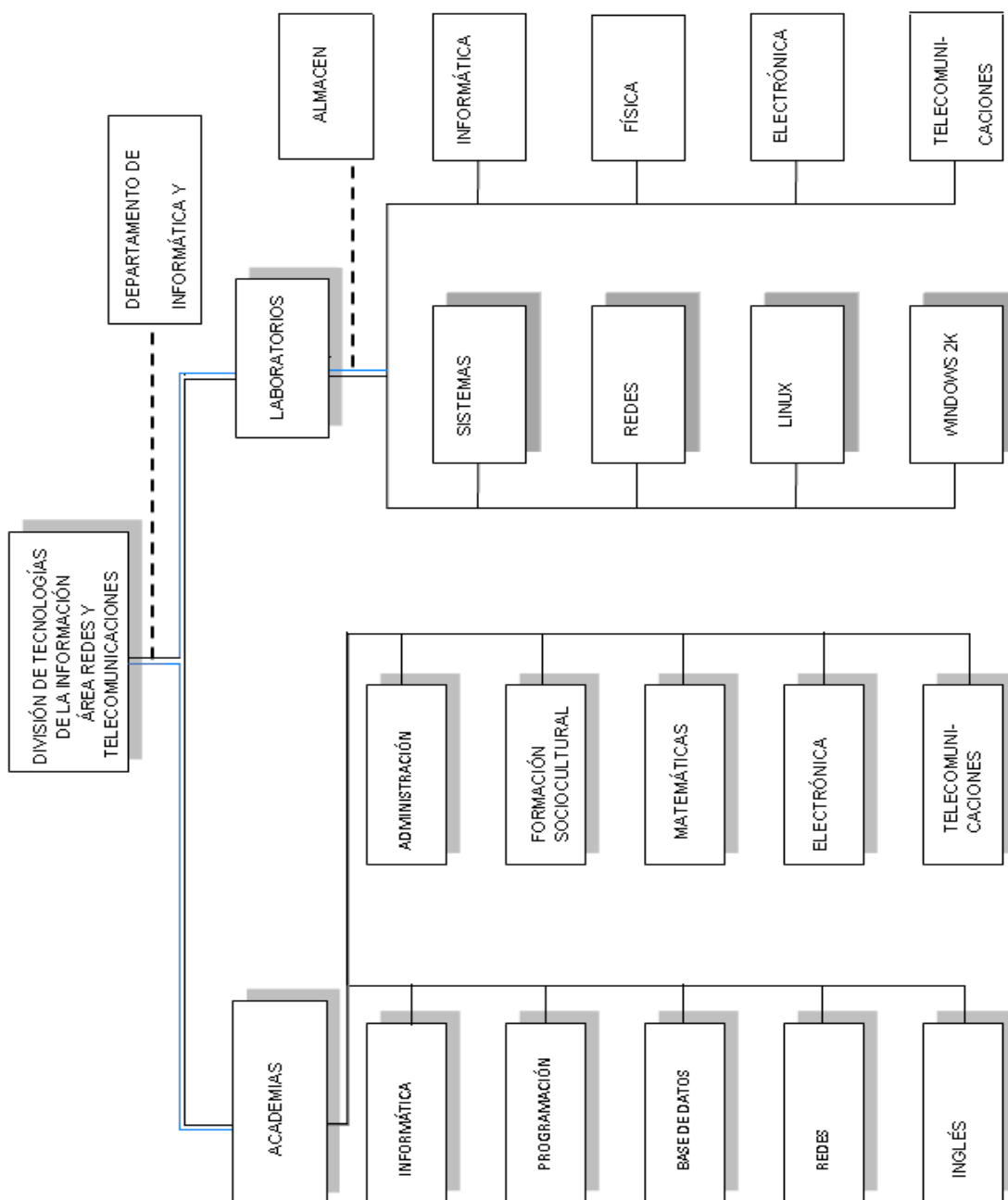
El manual de organización es un documento oficial que describe claramente la estructura orgánica, el organigrama que representa en forma esquemática la estructura de la organización, las funciones de los órganos que integran una unidad administrativa, los niveles jerárquicos, los grados de autoridad, responsabilidad, así como las líneas de comunicación y coordinación existentes, que esquematiza y resume la organización de una unidad responsable.

El manual de organización es, por tanto, un instrumento de apoyo administrativo, que describe las relaciones orgánicas que se dan entre las unidades administrativas de una dependencia, enunciando sus objetivos y funciones, siendo por ello, un elemento de apoyo al funcionamiento administrativo.

Por lo cual primeramente se realizó el **organigrama específico** de TIC, área RyT donde se contemplan las diferentes academias que integran dicha división académica, así como los laboratorios de cómputo que dependen de cada una de las academias, junto con el apoyo de un almacén para el préstamo de equipo de telecomunicaciones.

Dichos laboratorios dependen del departamento de Informática y Estadística, el cual se encarga de proporcionar el servicio de Internet, así como de la administración de todo el direccionamiento IP de la universidad, además del seguimiento y control de todos los bienes informáticos, por lo cual es importante contar con un administrador de red por división académica para realizar dichas funciones. A continuación se muestra dicho organigrama y la relación entre departamentos, academias y laboratorios:

2.1 Organigrama Específico de TIC, Área RyT



Elaboración propia (2012)

2.2 Manual Especifico de Organización

Posteriormente se realizó la elaboración del manual de Organización, en el cual se incluye la descripción de puestos que se requiere para cada uno de los responsables de laboratorio así como el coordinador de los mismos, además de un directorio de dichas personas responsables.

Este manual debe incluir, en primer término, los siguientes datos:

- a) Logotipo de la organización.
- b) Nombre de la organización.
- c) Denominación y extensión del manual (general o específico).
- d) Lugar y fecha de elaboración.
- e) Número de páginas.
- f) Sustitución de páginas (actualización de información).
- g) Unidades responsables de su elaboración, revisión y autorización.
- h) Clave de la forma; en primer término se deben escribir las siglas de la organización; en segundo, las de la unidad administrativa responsable de elaborar o utilizar el formulario; en tercero, el número consecutivo del formulario y, en cuarto, el año.

En la siguiente imagen se muestra un ejemplo de cómo quedo el formato propuesto para dicho manual, el cual se puede apreciar completo en el apartado correspondiente de “Funciones y Actividades”.

(a)	(b)	Fecha	(d)		
		Página	(e)	De	
		Sustituye a:			
	(c)	(f)			
		Página		De	
		De fecha			
Área o puesto	Función	Actividad			
		(g)			


Fuente: Elaboración propia (2011).

2.2.1 Funciones y Actividades

El presente manual establece las funciones y actividades de cada uno de los responsables de cada laboratorio de cómputo del área de RyT, así como del coordinador, además del organigrama específico de dicha carrera, además de


los formatos necesarios para el registro y control de las diferentes actividades llevadas a cabo en dichos laboratorios, los cuales se muestran a continuación:

Funciones y Actividades del Coordinador

	División de TIC, Área Redes y Telecomunicaciones	Fecha			
		Página		De	
	Manual de Organización específico Área de Laboratorios	Sustituye a:			
		Página		De	
		De fecha			
Área o puesto	Función	Actividad			
Coordinador de laboratorios	1. Organizar el servicio de cómputo y acceso a la red	1.1. Integrar los horarios de atención a grupos. 1.2. Planeación del uso de los equipos y software que cada materia requiera. 1.3. Verificar que los laboratorios se encuentren en Red.			
	2. Controlar el servicio de cómputo e internet.	2.1. Programar el mantenimiento preventivo de los laboratorios. 2.2. Controlar el uso de las licencias de software original. 2.3. Llenar y dar seguimiento a los formatos de mantenimiento. 2.4. Llevar un registro del uso de los laboratorios de acuerdo al horario establecido y acceso a internet. 2.5. Revisar el estado de los laboratorios al término del día.			
	3. Concentrar el inventario general de cada uno de los laboratorios.	3.1. Realizar el inventario físico de los bienes materiales de los laboratorios. 3.2. Entregar reporte del inventario general de los laboratorios.			


Fuente: elaboración propia, 2012

Funciones y Actividades del Laboratorio de Sistemas

	División de TIC, Área Redes y Telecomunicaciones	Fecha				
		Página		De		
	Manual de Organización específico Área de Laboratorios	Sustituye a:				
		Página		De		
		De fecha				
Área o puesto	Función	Actividad				
Responsable del Laboratorio de Sistemas	1. Brindar el servicio de cómputo.	1.1. Llevar registro del control de acceso a usuarios acorde al horario asignado. 1.2. Proporcionar apoyo técnico a los usuarios del laboratorio. 1.3. Asignar el tipo de claves de usuario según las necesidades. 1.4. Proporcionar el software necesario para la realización de prácticas.				
	2. Brindar el servicio de Red.	2.1. Realizar el mantenimiento preventivo de los equipos. 2.2. Realizar la vacunación de los equipos de cómputo. 2.3. Reportar equipos con y sin garantía para su reparación. 2.4. Revisar el buen estado de los equipos y acceso de Red al término del día.				
	3. Realizar el inventario general del laboratorio de Sistemas.	3.1. Realizar el inventario físico del equipo de cómputo y bienes materiales del laboratorio. 3.2. Entregar reporte de existencia de los equipos de cómputo y bienes materiales al coordinador de laboratorios. 1.4. Llevar un registro de posibles fallas de hardware y software por parte de los usuarios del laboratorio.				


Fuente: elaboración propia, 2012

Funciones y Actividades del Laboratorio de Redes

	División de TIC, Área Redes y Telecomunicaciones	Fecha	
		Página	De
		Sustituye a:	
	Manual de Organización específico Área de Laboratorios	Página	De
		De fecha	
Área o puesto	Función	Actividad	
Responsable del Laboratorio de Redes	<p>1. Brindar el servicio de cómputo y manejo de equipo Cisco.</p> <p>2. Brindar el servicio de acceso a Red.</p> <p>3. Realizar el inventario general del laboratorio de Redes.</p>	<p>1.1. Llevar registro del control de acceso a usuarios acorde al horario asignado.</p> <p>1.2. Proporcionar apoyo técnico a los usuarios del laboratorio en el manejo de equipo Cisco.</p> <p>1.3. Asignar el tipo de claves de usuario según las necesidades.</p> <p>1.4. Revisar el correcto funcionamiento de los equipos de la marca Cisco.</p> <p>2.1. Realizar el mantenimiento preventivo de los equipos.</p> <p>2.2. Reportar equipos con y sin garantía para su reparación.</p> <p>2.3. Realizar la vacunación de los equipos de cómputo.</p> <p>2.4. Revisar el buen estado de los equipos y nodos de Red al término del día.</p> <p>3.1. Realizar el inventario físico del equipo de cómputo y bienes materiales del laboratorio.</p> <p>3.2. Entregar reporte de existencia de los equipos de cómputo y bienes materiales al coordinador de laboratorios.</p>	


Fuente: elaboración propia, 2012

Funciones y Actividades del Laboratorio de Informática

	División de TIC, Área Redes y Telecomunicaciones	Fecha			
		Página		De	
	Manual de Organización específico Área de Laboratorios	Sustituye a:			
		Página		De	
		De fecha			
Área puesto	Función	Actividad			
Responsable del Laboratorio de Informática	1. Brindar el servicio de cómputo y programación.	1.1. Llevar registro del control de acceso a usuarios acorde al horario asignado. 1.2. Proporcionar apoyo técnico a los usuarios del laboratorio. 1.3. Asignar el tipo de claves de usuario según las necesidades. 1.4. Proporcionar el software necesario para la realización de prácticas.			
	2. Brindar el servicio de conectividad en redes.	2.1. Realizar el mantenimiento preventivo de los equipos. 2.2. Reportar equipos con y sin garantía para su reparación. 2.3. Realizar la vacunación de los equipos de cómputo. 2.4. Revisar el buen estado de los equipos y nodos de Red al término del día.			
	3. Realizar el inventario general del laboratorio de Informática.	3.1. Realizar el inventario físico del equipo de cómputo y bienes materiales del laboratorio. 3.2. Entregar reporte de existencia de los equipos de cómputo y bienes materiales al coordinador de laboratorios.			


Fuente: elaboración propia, 2012

Funciones y Actividades del Laboratorio de Linux

	División de TIC, Área Redes y Telecomunicaciones	Fecha				
		Página		De		
		Sustituye a:				
		Página		De		
	Manual de Organización específico Área de Laboratorios	De fecha				
Área puesto	Función	Actividad				
Responsable del Laboratorio de Linux	<p>1. Brindar el servicio de cómputo y manejo del sistema operativo Linux.</p> <p>2. Brindar el servicio de Red.</p> <p>3. Realizar el inventario general del laboratorio de Linux</p>	<p>1.1. Llevar registro del control de acceso a usuarios acorde al horario asignado.</p> <p>1.2. Realizar la instalación de los sistemas operativos necesarios para las prácticas del laboratorio.</p> <p>1.3. Asignar el tipo de claves de usuario según las necesidades.</p> <p>2.1. Realizar el mantenimiento preventivo de los equipos.</p> <p>2.2. Reportar equipos con y sin garantía para su reparación.</p> <p>2.3. Realizar la vacunación de los equipos de cómputo.</p> <p>2.4. Revisar el buen estado de los equipos y nodos de Red al término del día.</p> <p>3.1. Realizar el inventario físico del equipo de cómputo y bienes materiales del laboratorio.</p> <p>3.2. Entregar reporte de existencia de los equipos de cómputo y bienes materiales al coordinador de laboratorios.</p>				


Fuente: elaboración propia, 2012

Funciones y Actividades del Laboratorio de Windows 2k

	División de TIC, Área Redes y Telecomunicaciones	Fecha			
		Página		De	
	Manual de Organización específico Área de Laboratorios	Sustituye a:			
		Página		De	
		De fecha			
Área puesto	Función	Actividad			
Responsable del Laboratorio de Windows 2K	<p>1.- Brindar el servicio de cómputo y administración del sistema operativo Windows Server 2003 y Windows Server 2008</p> <p>2. Brindar el servicio de Red.</p> <p>3. Realizar el inventario general del laboratorio de Sistemas.</p>	<p>1.1. Llevar registro del control de acceso a usuarios acorde al horario asignado.</p> <p>1.2. Realizar la instalación de los sistemas operativos necesarios para las prácticas del laboratorio.</p> <p>1.3. Asignar claves de usuario restringido, según las necesidades.</p> <p>2.1. Realizar el mantenimiento preventivo de los equipos.</p> <p>2.2. Reportar equipos con y sin garantía para su reparación.</p> <p>2.4. Revisar el buen estado de los equipos y nodos de Red al término del día.</p> <p>3.1. Realizar el inventario físico del equipo de cómputo y bienes materiales del laboratorio.</p> <p>3.2. Entregar reporte de existencia de los equipos de cómputo y bienes materiales al coordinador de laboratorios.</p>			

Fuente: elaboración propia, 2012

Funciones y Actividades del Almacén

	División de TIC, Área Redes y Telecomunicaciones		Fecha			
			Página		De	
			Sustituye a:			
	Manual de Organización específico Área de Laboratorios		Página		De	
		De fecha				
Área o puesto	Función	Actividad				
Responsable del Laboratorio de Windows 2K	<p>1.- Brindar el servicio de cómputo y administración del sistema operativo Windows Server 2003 y Windows Server 2008</p> <p>2. Brindar el servicio de Red.</p> <p>3. Realizar el inventario general del laboratorio de Sistemas.</p>	<p>1.1. Llevar registro del control de acceso a usuarios acorde al horario asignado.</p> <p>1.2. Realizar la instalación de los sistemas operativos necesarios para las prácticas del laboratorio.</p> <p>1.3. Asignar claves de usuario restringido, según las necesidades.</p> <p>2.1. Realizar el mantenimiento preventivo de los equipos.</p> <p>2.2. Reportar equipos con y sin garantía para su reparación.</p> <p>2.4. Revisar el buen estado de los equipos y nodos de Red al término del día.</p> <p>3.1. Realizar el inventario físico del equipo de cómputo y bienes materiales del laboratorio.</p> <p>3.2. Entregar reporte de existencia de los equipos de cómputo y bienes materiales al coordinador de laboratorios.</p>				

Fuente: elaboración propia, 2012

Una vez realizado el Manual de Especifico de Organización, donde se detallan las funciones y actividades de cada responsable de los laboratorios, es importante definir las características que deben reunir dichas personas y los requisitos para cubrir el “puesto” asignado, lo cual se explica en el siguiente apartado:

2.2.2 Descripción de puestos

Es la reseña del contenido básico de los puestos que componen cada unidad administrativa, que incluye la información siguiente:

- Identificación del puesto (nombre, ubicación, ámbito de operación, etcétera).
- Relaciones de autoridad, donde se indican los puestos subordinados y las facultades de decisión, así como las relaciones de línea y asesoría.
- Funciones generales y específicas.
- Responsabilidades o deberes.
- Relaciones de comunicación con otras unidades y puestos dentro de la organización, así como las que deba establecer externamente.
- Especificaciones del puesto en cuanto a conocimientos, experiencia, iniciativa y personalidad.

Este apartado normalmente forma parte de un manual de organización de una unidad administrativa en particular.


En la siguiente imagen se muestra un ejemplo de cómo quedo el formato propuesto para dicho manual, el cual se puede apreciar completo en el apartado correspondiente.

(a)	(b)	Fecha	(d)		
		Página	(e)	De	
	Sustituye a: (f)				
	(c)	Página		De	
		De fecha			
Descripción de puestos					

Fuente: Elaboración propia (2011).

A continuación se describen los puestos para cada uno de los responsables de los laboratorios de cómputo propuestos, así como el puesto de coordinador:

Descripción del Puesto de Coordinador

	División de TIC, Área Redes y Telecomunicaciones	Fecha				
		Página		De		
	Manual de Organización específico Área de Laboratorios	Sustituye a:				
		Página		De		
		De fecha				
Descripción del puesto						
<p>Identificación y relaciones:</p> <p>A) Identificación <u>Nombre del puesto: Coordinador de laboratorios</u> Número de plazas: 1 Clave: 01-L-01 Ubicación (física y administrativa): Laboratorio de Telemática Tipo de contratación: Permanente Ámbito de operación: Operativo</p> <p>B) Relación de autoridad Jefe inmediato: Director Área Redes y Telecomunicaciones. Subordinados directos: Responsables de laboratorios Dependencia funcional: Secretaría Académica y Departamento de Informática y estadística.</p> <p>Propósito del puesto: Organizar y controlar el servicio de cómputo e internet.</p> <p>Funciones generales: Organizar el servicio de cómputo y acceso a la red. Controlar el servicio de cómputo e internet. Concentrar el inventario general de cada uno de los laboratorios.</p> <p>Funciones específicas: Administrar claves de usuario para el uso de laboratorios. Controlar el uso de las licencias de software original. Proporcionar un acceso permanente de Red. Llevar un registro del uso de los laboratorios.</p>						

Llevar un control de los reportes de mantenimiento.
Entregar reporte del inventario general de los laboratorios.

Responsabilidad:

Ofrecer de forma eficaz y eficiente el servicio de laboratorios.
Salvaguardar los equipos de cómputo y componentes de los laboratorios.
Dar seguimiento a las solicitudes de servicio.
Controlar la confidencialidad y el correcto uso de las claves de acceso.

Comunicación:

Ascendente: Director Área Redes y Telecomunicaciones.
Horizontal: Presidentes de las Academias
Descendente: Responsables de cada laboratorios
Externa: Departamento de Informática y Estadística y con el encargado de Almacén.

Especificaciones del puesto:

Conocimiento:

Ingeniero en computación, sistemas y áreas afines.

Experiencia:

Administración y Mantenimiento de Redes.
Implementación y manejo de Servidores y servicios de Red.
Mantenimiento preventivo y correctivo de equipo de cómputo.

Iniciativa:


Mejora continua y sistemas de control
Calidad en el Servicio a usuarios finales.

Personalidad:

Organizado y responsable.
Sentido de autoridad y disciplina.
Abierto al diálogo y propositivo.

Fuente: elaboración propia, 2012

Descripción del Responsable del Laboratorio de Sistemas

	División de TIC, Área Redes y Telecomunicaciones	Fecha			
		Página		De	
	Manual de Organización específico Área de Laboratorios	Sustituye a:			
		Página		De	
		De fecha			

Descripción del puesto

Identificación y relaciones:

A) Identificación

Nombre del puesto: Responsable del laboratorio de Sistemas.

Número de plazas: 1

Clave: 01-L-02

Ubicación (física y administrativa): Laboratorio de Sistemas.

Tipo de contratación: Permanente.

Ámbito de operación: Operativo.

B) Relación de autoridad

Jefe inmediato: Coordinador de Laboratorios.

Subordinados directos: Alumnos de Servicio Social.

Dependencia funcional: Secretaría Académica y Departamento de Informática y estadística.

Propósito del puesto:

Brindar el servicio de cómputo y acceso a red.

Funciones generales:

Brindar el servicio de cómputo y servicios de Red.

Realizar el inventario general del laboratorio de Sistemas.

Funciones específicas:

Llevar un registro del servicio de cómputo y acceso a la red.

Proporcionar apoyo técnico a los usuarios del laboratorio.

Asignar el tipo de claves de usuario según las necesidades.

Realizar el mantenimiento preventivo de los equipos.

Llevar un registro de reportes de equipos con y sin garantía para su reparación.

Realizar el inventario físico del equipo de cómputo y bienes materiales del laboratorio.

Responsabilidad:

Ofrecer de forma eficaz y eficiente el servicio del laboratorio.

Salvaguardar los equipos de cómputo y componentes del laboratorio.

Dar seguimiento a las solicitudes de servicio.

Controlar la confidencialidad y el correcto uso de las claves de acceso.

Comunicación:

Ascendente: Coordinador de Laboratorios.

Horizontal: Responsables de Laboratorios.

Descendente: Profesores y usuarios del servicio.

Externa: Empresa asignada al soporte técnico.

Especificaciones del puesto:

Conocimiento:

Ingeniero en computación, sistemas y áreas afines.

Técnico Superior Universitario en Informática o Telemática.

Experiencia:

Instalación y mantenimiento de Redes.

Mantenimiento preventivo y correctivo de equipo de cómputo.

Iniciativa:

Mejora continua y sistemas de control.

Calidad en el Servicio a usuarios finales.

Personalidad:


Organizado y responsable.

Abierto al diálogo y propositivo.

Acostumbrado a trabajar bajo presión.

Fuente: elaboración propia, 2012

Descripción del Responsable del Laboratorio de Redes

	División de TIC, Área Redes y Telecomunicaciones	Fecha			
		Página		De	
	Manual de Organización específico Área de Laboratorios	Sustituye a:			
		Página		De	
		De fecha			

Descripción del puesto

Identificación y relaciones:

Identificación

Nombre del puesto: Responsable del laboratorio de Redes.

Número de plazas: 1

Clave: 01-L-03

Ubicación (física y administrativa): Laboratorio de redes.

Tipo de contratación: Permanente.

Ámbito de operación: Operativo.

Relación de autoridad

Jefe inmediato: Coordinador de Laboratorios.

Subordinados directos: Alumnos de Servicio Social.

Dependencia funcional: Secretaría Académica y Departamento de Informática y estadística.

Propósito del puesto:

Brindar el servicio de cómputo y acceso a red.

Funciones generales:

Brindar el servicio de cómputo y manejo de equipo Cisco.

Realizar el inventario general del laboratorio de Sistemas.

Brindar el servicio de acceso a Red.

Funciones específicas:

Llevar un registro del servicio de cómputo y acceso a la red.

Proporcionar apoyo técnico a los usuarios del laboratorio.

Asignar el tipo de claves de usuario según las necesidades.

Realizar el mantenimiento preventivo de los equipos.

Realizar reportes de equipos con y sin garantía para su reparación.
Realizar el inventario físico de los bienes materiales del laboratorio.

Responsabilidad:

Ofrecer de forma eficaz y eficiente el servicio del laboratorio.
Salvaguardar los equipos de cómputo y componentes del laboratorio.
Dar seguimiento a las solicitudes de servicio.
Controlar la confidencialidad y el correcto uso de las claves de acceso.

Comunicación:

Ascendente: Coordinador de Laboratorios.
Horizontal: Responsables de Laboratorios.
Descendente: Profesores y usuarios del servicio.
Externa: Empresa asignada al soporte técnico.

Especificaciones del puesto:

Conocimiento:

Ingeniero en computación, sistemas y áreas afines.
Técnico Superior Universitario en Informática o Telemática.

Experiencia:

Instalación y mantenimiento de Redes.
Manejo de equipos de interconexión Cisco.
Mantenimiento preventivo y correctivo de equipo de cómputo.

Iniciativa:


Mejora continua y sistemas de control
Calidad en el Servicio a usuarios finales.

Personalidad:

Organizado y responsable.
Abierto al dialogo y propositivo.
Acostumbrado a trabajar bajo presión.

Fuente: elaboración propia, 2012

Descripción del Responsable del Laboratorio de Informática

	División de TIC, Área Redes y Telecomunicaciones	Fecha			
		Página		De	
	Manual de Organización específico Área de Laboratorios	Sustituye a:			
		Página		De	
		De fecha			

Descripción del puesto

Identificación y relaciones:

Identificación

Nombre del puesto: Responsable del laboratorio de Informática

Número de plazas: 1

Clave: 01-L-04

Ubicación (física y administrativa): Laboratorio de Informática

Tipo de contratación: Permanente

Ámbito de operación: Operativo

Relación de autoridad

Jefe inmediato: Coordinador de Laboratorios

Subordinados directos: Alumnos de Servicio Social.

Dependencia funcional: Secretaría Académica y Departamento de Informática y estadística.

Propósito del puesto:

Brindar el servicio de cómputo, programación y acceso a red.

Funciones generales:

Brindar el servicio de cómputo y programación.

Brindar el servicio de conectividad en redes.

Realizar el inventario general del laboratorio de Informática.

Funciones específicas:

Llevar un registro del servicio de cómputo y acceso a la red.

Proporcionar el software necesario para la realización de prácticas.

Proporcionar apoyo técnico a los usuarios del laboratorio.

Asignar el tipo de claves de usuario según las necesidades.

Realizar el mantenimiento preventivo de los equipos.
Llevar un registro de equipos con y sin garantía para su reparación.
Realizar el inventario físico del equipo de cómputo y bienes materiales del laboratorio.

Responsabilidad:

Ofrecer de forma eficaz y eficiente el servicio del laboratorio.
Salvaguardar los equipos de cómputo y componentes del laboratorio.
Dar seguimiento a las solicitudes de servicio.
Controlar la confidencialidad y el correcto uso de las claves de acceso.

Comunicación:

Ascendente: Coordinador de Laboratorios.
Horizontal: Responsables de Laboratorios.
Descendente: Profesores y usuarios del servicio.
Externa: Empresa asignada al soporte técnico.

Especificaciones del puesto:

Conocimiento:

Ingeniero en computación, sistemas y áreas afines.
Técnico Superior Universitario en Informática o Telemática.

Experiencia:

Instalación y mantenimiento de Redes.
Instalación y manejo de lenguajes de programación.
Mantenimiento preventivo y correctivo de equipo de cómputo.

Iniciativa:


Mejora continua y sistemas de control
Calidad en el Servicio a usuarios finales.

Personalidad:

Organizado y responsable.
Abierto al diálogo y propositivo.
Acostumbrado a trabajar bajo presión.

Fuente: elaboración propia, 2012

Descripción del Responsable del Laboratorio de Linux

	División de TIC, Área Redes y Telecomunicaciones	Fecha			
		Página		De	
	Manual de Organización específico Área de Laboratorios	Sustituye a:			
		Página		De	
		De fecha			

Descripción del puesto

Identificación y relaciones:

Identificación

Nombre del puesto: Responsable del laboratorio de Linux.

Número de plazas: 1

Clave: 01-L-05

Ubicación (física y administrativa): Laboratorio de Linux.

Tipo de contratación: Permanente.

Ámbito de operación: Operativo.

Relación de autoridad

Jefe inmediato: Coordinador de Laboratorios.

Subordinados directos: Alumnos de Servicio Social.

Dependencia funcional: Secretaría Académica y Departamento de Informática y estadística.

Propósito del puesto:

Brindar el servicio de cómputo, red y manejo del sistema operativo Linux.

Funciones generales:

Brindar el servicio de cómputo y servicios de Red.

Brindar el uso y manejo del Sistema operativo Linux.

Realizar el inventario general del laboratorio de Linux.

Funciones específicas:

Llevar un registro del servicio de cómputo y acceso a la red.

Proporcionar apoyo técnico a los usuarios del laboratorio.

Asignar el tipo de claves de usuario según las necesidades.

Realizar el mantenimiento preventivo de los equipos.

Llevar un registro de reportes de equipos con y sin garantía para su reparación.
Realizar el inventario físico del equipo de cómputo y bienes materiales del laboratorio.

Responsabilidad:

Ofrecer de forma eficaz y eficiente el servicio del laboratorio.
Salvaguardar los equipos de cómputo y componentes del laboratorio.
Dar seguimiento a las solicitudes de servicio.
Controlar la confidencialidad y el correcto uso de las claves de acceso.

Comunicación:

Ascendente: Coordinador de Laboratorios.
Horizontal: Responsables de Laboratorios.
Descendente: Profesores y usuarios del servicio.
Externa: Empresa asignada al soporte técnico.

Especificaciones del puesto:

Conocimiento:

Ingeniero en computación, sistemas y áreas afines.
Técnico Superior Universitario en Informática o Telemática.

Experiencia:

Instalación y mantenimiento de Redes.
Instalación y administración de Sistemas operativos de Red
Mantenimiento preventivo y correctivo de equipo de cómputo.

Iniciativa:


Mejora continua y sistemas de control
Calidad en el Servicio a usuarios finales.

Personalidad:

Organizado y responsable.
Abierto al diálogo y propositivo.
Acostumbrado a trabajar bajo presión.

Fuente: elaboración propia, 2012

Descripción del Responsable del Laboratorio de Windows2k

	División de TIC, Área Redes y Telecomunicaciones	Fecha				
		Página		De		
	Manual de Organización específico Área de Laboratorios	Sustituye a:				
		Página		De		
		De fecha				

Descripción del puesto

Identificación y relaciones:

Identificación

Nombre del puesto: Responsable del laboratorio de Windows 2K

Número de plazas: 1

Clave: 01-L-06

Ubicación (física y administrativa): Laboratorio de Windows 2K

Tipo de contratación: Permanente.

Ámbito de operación: Operativo.

Relación de autoridad

Jefe inmediato: Coordinador de Laboratorios.

Subordinados directos: Alumnos de Servicio Social.

Dependencia funcional: Secretaría Académica y Departamento de Informática y estadística.

Propósito del puesto:

Brindar el servicio de cómputo, acceso a red y manejo de Sistemas operativos de Red

Funciones generales:

Brindar el servicio de cómputo y servicios de Red.

Brindar el uso y administración del Sistema operativo Windows Server 2003 y 2008.

Realizar el inventario general del laboratorio de Windows.

Funciones específicas:

Llevar un registro del servicio de cómputo y acceso a la red.

Proporcionar el software necesario para la realización de prácticas.

Proporcionar apoyo técnico a los usuarios del laboratorio.

Asignar el tipo de claves de usuario según las necesidades.
Realizar el mantenimiento preventivo de los equipos.
Llevar un registro de equipos con y sin garantía para su reparación.
Realizar el inventario físico del equipo de cómputo y bienes materiales del laboratorio.

Responsabilidad:

Ofrecer de forma eficaz y eficiente el servicio del laboratorio.
Salvaguardar los equipos de cómputo y componentes del laboratorio.
Dar seguimiento a las solicitudes de servicio.
Controlar la confidencialidad y el correcto uso de las claves de acceso.

Comunicación:

Ascendente: Coordinador de Laboratorios.
Horizontal: Responsables de Laboratorios.
Descendente: Profesores y usuarios del servicio.
Externa: Empresa asignada al soporte técnico.

Especificaciones del puesto:

Conocimiento:

Ingeniero en computación, sistemas y áreas afines.
Técnico Superior Universitario en Informática o Telemática.

Experiencia:

Instalación y mantenimiento de Redes.
Instalación y manejo de Sistemas operativos de Red
Mantenimiento preventivo y correctivo de equipo de cómputo.

Iniciativa:


Mejora continua y sistemas de control
Calidad en el Servicio a usuarios finales.

Personalidad:

Organizado y responsable.
Abierto al diálogo y propositivo.
Acostumbrado a trabajar bajo presión.

Fuente: elaboración propia, 2012

Descripción del Responsable del Almacén

	División de TIC, Área Redes y Telecomunicaciones	Fecha				
		Página		De		
	Manual de Organización específico Área de Laboratorios	Sustituye a:				
		Página		De		
		De fecha				

Descripción del puesto**Identificación y relaciones:****Identificación****Nombre del puesto: Responsable del Almacén**

Número de plazas: 1

Clave: 01-A-01

Ubicación (física y administrativa): Almacén del Laboratorio de TIC.

Tipo de contratación: Permanente.

Ámbito de operación: Operativo.

Relación de autoridad

Jefe inmediato: Coordinador de Laboratorios.

Subordinados directos: Alumnos de Servicio Social.

Dependencia funcional: Secretaría Académica y Departamento de Informática y estadística.

Propósito del puesto:

Brindar el servicio de préstamo de equipo de telecomunicaciones y electrónica para el desarrollo de prácticas, así como el resguardo y mantenimiento de dichos equipos.

Funciones generales:

Brindar el servicio de préstamo de equipo para la realización de prácticas.

Brindar el resguardo de los equipos de telecomunicaciones y electrónica.

Proporcionar el mantenimiento adecuado a los equipos mencionados.

Realizar el inventario general de los equipos en resguardo.

Funciones específicas:

Llevar un registro del servicio de préstamo de equipo

Realizar el mantenimiento preventivo de los equipos.
Llevar un registro de equipos con y sin garantía para su reparación.
Realizar el inventario físico del equipo de telecomunicaciones y electrónica.

Responsabilidad:

Ofrecer de forma eficaz y eficiente el servicio del almacén.
Salvaguardar los equipos de telecomunicaciones y electrónica.
Dar seguimiento a las solicitudes de servicio y garantía.

Comunicación:

Ascendente: Coordinador de Laboratorios.
Horizontal: Responsables de Laboratorios.
Descendente: Profesores y usuarios del servicio.
Externa: Empresa asignada al soporte técnico y garantías.

Especificaciones del puesto:

Conocimiento:

Ingeniero en electrónica y áreas afines.
Técnico Superior Universitario en Telemática.

Experiencia:

Manejo y control de equipos de telecomunicaciones y electrónica.
Mantenimiento preventivo y correctivo de equipos de electrónica.
Mantenimiento preventivo y correctivo de equipos de telecomunicaciones

Iniciativa:


Mejora continua y sistemas de control
Calidad en el Servicio a usuarios finales.

Personalidad:

Organizado y responsable.
Abierto al diálogo y propositivo.
Acostumbrado a trabajar bajo presión.

Fuente: elaboración propia, 2012

2.3.2 Directorio del Laboratorio de TIC, Área RyT

 DIVISION DE TELEMÁTICA	División de TIC, Área Redes y Telecomunicaciones			Fecha	
				Página	De
	Manual de Organización específico			Sustituye a:	
	Área de Laboratorios			Página	De
				De fecha	
Directorio del Laboratorio					
No	Nombre	Ubicación	Cargo/Puesto	Correo electrónico	
1	Juan Esteban Yáñez Yáñez	Laboratorio de Redes	Coordinador de laboratorios	jestey@utn.edu.mx	
2	Raymundo Ríos Cárdenas	Laboratorio de Sistemas	Responsable del laboratorio	rayrios@utn.edu.mx	
3	Juan Estrada López	Laboratorio de Redes	Responsable del laboratorio	juanel@utn.edu.mx	
4	Claudia Hernández Medina	Laboratorio de Informática	Responsable del laboratorio	medinah@utn.edu.mx	
5	Rodolfo Melgarejo Salgado	Laboratorio de Linux	Responsable del laboratorio	melgarejo@utn.edu.mx	
6	Rodolfo Hernández Valdez	Laboratorio de Windows 2K	Responsable del laboratorio	rhvaldez@utn.edu.mx	
7	Ernesto Guerrero España	Almacén	Responsable del Almacén	ernesep@utn.edu.mx	

Fuente: elaboración propia, 2012

CAPITULO 3. MANUAL DE POLITICAS DEL LABORATORIO DE TIC, ÁREA RYT

Sin importar si están conectadas por cable o de manera inalámbrica, las redes de computadoras cada vez se tornan más esenciales para las actividades diarias. Tanto las personas como las organizaciones dependen de sus computadores y de las redes para funciones como correo electrónico, contabilidad, organización y administración de archivos. Las intrusiones de personas no autorizadas pueden causar interrupciones costosas en la red y pérdidas de trabajo. Los ataques a una red pueden ser devastadores y pueden causar pérdida de tiempo y de dinero debido a los daños o robos de información o de activos importantes.

Los intrusos pueden obtener acceso a la red a través de vulnerabilidades del software, ataques al hardware o incluso a través de métodos menos tecnológicos, como el de adivinar el nombre de usuario y la contraseña de una persona. Por lo general, a los intrusos que obtienen acceso mediante la modificación del software o la explotación de las vulnerabilidades del software se los denomina piratas informáticos.

Una vez que el pirata informático obtiene acceso a la red, pueden surgir cuatro tipos de amenazas:

- Robo de información
- Robo de identidad
- Pérdida y manipulación de datos
- Interrupción del servicio

Las **amenazas de seguridad** causadas por intrusos en la red pueden originarse tanto en forma interna como externa, las cuales se mencionan a continuación:

Amenazas externas

Las amenazas externas provienen de personas que trabajan fuera de una organización. Estas personas no tienen autorización para acceder al sistema o

a la red de las computadoras. Los atacantes externos logran ingresar a la red desde Internet, enlaces inalámbricos o servidores de acceso dial-up.

Amenazas internas

Las amenazas internas se originan cuando una persona cuenta con acceso autorizado a la red a través de una cuenta de usuario o tiene acceso físico al equipo de la red. Un atacante interno conoce la política interna y las personas. Por lo general, conocen información valiosa y vulnerable y saben cómo acceder a ésta.

Sin embargo, no todos los ataques internos son intencionales ya que en algunos casos la amenaza interna puede provenir de un empleado confiable que capta un virus o una amenaza de seguridad mientras se encuentra fuera de la compañía y, sin saberlo, lo lleva a la red interna.

La mayor parte de las compañías invierte recursos considerables para defenderse contra los ataques externos; sin embargo, la mayor parte de las amenazas son de origen interno. De acuerdo con el FBI, el acceso interno y la mala utilización de los sistemas de computación representan aproximadamente el 70% de los incidentes de violación de seguridad notificados.

No todos los ataques causan daños o evitan que los usuarios legítimos tengan acceso a los recursos. Muchas amenazas están diseñadas para recopilar información acerca de los usuarios que, a su vez, puede utilizarse con fines de publicidad, comercialización e investigación. Algunas de estas amenazas son el spyware, las cookies de seguimiento, el adware y los elementos emergentes. Si bien es posible que éstos no dañen la computadora, sí pueden invadir la privacidad y generar molestias.

3.1 Políticas de Seguridad y Control

No se pueden eliminar o evitar completamente los riesgos de seguridad, sin embargo, tanto la administración como la evaluación efectiva de riesgos puede minimizar significativamente los riesgos de seguridad existentes. Para minimizar los riesgos es importante comprender que no existe un único producto que pueda

asegurar una organización, ya que la verdadera seguridad de redes proviene de una combinación de productos y servicios junto con una política de seguridad exhaustiva y un control para asegurar que se respeten dichas políticas.

Una política de seguridad es una declaración formal de las normas que los usuarios deben respetar a fin de acceder a los bienes de tecnología e información. Puede ser tan simple como una política de uso aceptable o contener muchas páginas y detallar cada aspecto de conectividad de los usuarios, así como los procedimientos de uso de redes y equipos.

La política de seguridad debe ser el punto central acerca de la forma en la que se protege, se supervisa, se evalúa y se mejora una red. Mientras que la mayoría de los usuarios domésticos no tienen una política de seguridad formal por escrito, a medida que una red crece en tamaño y en alcance, la importancia de una política de seguridad definida para todos los usuarios aumenta drásticamente.

Los puntos principales que se incluyen en esta **política de seguridad y control** son:

- políticas de acceso
- políticas de uso y control

Cuando se desarrolla una política de seguridad es necesario que todos los usuarios de la red la cumplan y la sigan para que sea efectiva, ya que esta debe ser el punto central acerca de la forma en la que se protege, se supervisa, se evalúa y se mejora una red.

3.1.1 Manual de Políticas de acceso

De acuerdo con los estatutos y lineamientos que rigen esta institución como un organismo descentralizado y cuyo fin es la educación superior, se presenta el siguiente **reglamento de uso interno y de control** para el buen uso y correcto desempeño de los laboratorios de cómputo, el cual aplica a todos los usuarios que deseen hacer uso de dichos laboratorios.

Para poder llevar a cabo dicho reglamento se desarrollaron varios formatos de control los cuales se mencionan a continuación y se encuentran como anexos:

Anexo A.- Horario de Clases del Laboratorio

Anexo B.- Control de prácticas del laboratorio

Anexo C.- Registro de fallas del laboratorio

Anexo D.- Registro de uso extra clase del laboratorio

A continuación se presenta el Reglamento propuesto para los laboratorios de cómputo de la división de TIC, Área de RyT:

REGLAMENTO INTERNO

- 1 El uso del laboratorio será principalmente de carácter educativo, por lo que deberá ser utilizado de acuerdo a las asignaturas que así lo requieran, así como el horario establecido por la Dirección para dicho fin, por lo que el profesor que este ocupando el laboratorio en ese momento será el *responsable* del correcto uso de los equipos.
- 2 El *profesor responsable* deberá llenar el formato de “control de prácticas del laboratorio” (Anexo B) al inicio del uso del laboratorio, el cual se encuentra bajo el resguardo del responsable del almacén, así mismo deberá de notificar en caso de no haber otra clase posterior a la suya, para el cierre del laboratorio.
- 3 Los alumnos que utilicen el laboratorio durante clases y se percaten de cualquier falla o problemas con el equipo de cómputo deberán llenar el formato de “Registro de fallas del laboratorio” (Anexo C), que es controlado por el profesor titular de la asignatura y el cual deberá de entregar al termino del día al *responsable del laboratorio* correspondiente para su análisis y reparación de dichos problemas.
- 4 Toda aquella persona que desee hacer uso del laboratorio después del horario de Clases (Anexo A) deberá pedir autorización al *responsable del laboratorio* o *coordinador* del mismo, así como registrarse en el formato de

“registro de uso del laboratorio” (Anexo D) y entregar su credencial de alumno vigente.

- 5 Cualquier falla de hardware detectada por algún *responsable del laboratorio*, deberá reportar dicho evento al *coordinador de los laboratorio*, el cual debe llenar y dar seguimiento al formato de “orden de servicio” (Anexo E) para su correspondiente reparación.
- 6 El uso de Internet queda limitado solo para fines didácticos, por lo que los alumnos no podrán descargar videos, música o juegos. Por lo tanto cualquier alumno que sea sorprendido jugando en los equipos de cómputo será acreedor a una suspensión de 3 días hábiles sin poder utilizar cualquier laboratorio de cómputo de la división.
- 7 Queda prohibido guardar información en los equipos de cómputo, debido a que se encuentra congelado el sistema, por lo que el sistema se restaura una vez que se reinicia el sistema.
- 8 Queda prohibido mover de lugar los equipos de cómputo, así como el intercambio de accesorios como mouse o teclado.
- 9 Queda estrictamente prohibido el acceso a los laboratorios de cómputo con alimentos y bebidas de cualquier tipo, así como fumar dentro del laboratorio y pasillos.
- 10 Al término de la clase deberán apagar los equipos de cómputo y acomodar sus accesorios (teclado y mouse), así como acomodar las sillas en su lugar correspondiente.

Fuente: elaboración propia, 2012

Por lo cual es importante que dicho manual sea revisado y autorizado por las autoridades correspondientes para su implementación, el cual será complementado con el manual de procedimientos para una mayor calidad en la prestación del servicio.

A continuación se describen cada una de las Políticas de Seguridad y Control específicamente para el laboratorio de la división de TIC Área RyT:

3.2 Políticas de uso y control para el laboratorio de RIC área RyT

Los procedimientos de seguridad implementan políticas de seguridad, por lo que estos procedimientos definen la configuración, el inicio de sesión, la auditoría y los procesos de mantenimiento de los hosts y dispositivos de red. Incluyen la utilización tanto de medidas preventivas para reducir el riesgo como de medidas activas acerca de la forma de manejar las amenazas de seguridad conocidas.

Los procedimientos de seguridad abarcan desde tareas simples y poco costosas, como un reglamento de uso general, las actualizaciones de software y su protección (puntos de restauración), hasta implementaciones complejas de firewalls y sistemas de detección de intrusiones.

Algunas de las herramientas y aplicaciones de seguridad utilizadas en la protección de redes incluyen:

- Parches y actualizaciones de software
- Protección contra virus y spyware
- Directivas de Restricción de Software
- Restauración del Sistema operativo

A continuación se explica cómo se utilizaron dichas herramientas dentro de los laboratorios de TIC, área RyT para poder asegurar una política de uso y control de los equipos de cómputo.

3.2.1 Parches y actualizaciones

Uno de los métodos más comunes que utiliza un pirata informático para obtener acceso a los hosts o a las redes es atacar las vulnerabilidades del software. Es importante mantener las aplicaciones de software actualizadas con los últimos parches y actualizaciones de seguridad a fin de ayudar a evitar las amenazas. Un parche es un pequeño código que corrige un problema específico. Por otro lado, una actualización puede incluir funciones adicionales al paquete de software y también parches para problemas específicos.

Los proveedores de SO (Sistemas Operativos, como Linux, Windows, etc.) y aplicaciones proporcionan continuamente actualizaciones y parches de seguridad que pueden corregir vulnerabilidades conocidas del software. Además, los proveedores lanzan, por lo general, conjuntos de parches y actualizaciones, conocidos como paquetes de servicios.

Afortunadamente, muchos sistemas operativos ofrecen una función de actualización automática que permite que las actualizaciones de SO y las aplicaciones se descarguen e instalen automáticamente en un host.

3.2.2 Protección contra virus y spyware

Aun cuando los SO y las aplicaciones tengan todos los parches y actualizaciones actuales, pueden seguir siendo vulnerables a ataques. Todo dispositivo conectado a una red es vulnerable a virus, gusanos y caballos de Troya. Éstos pueden utilizarse para dañar el código del SO, afectar el rendimiento de una computadora, alterar las aplicaciones y destruir los datos.

Éstos son algunos indicadores de la presencia de un virus, gusano o caballo de Troya:

- Se utiliza demasiado el CPU y no hay procesos visibles.
- La computadora comienza a actuar de forma anormal.
- Los programas no responden al mouse ni a las combinaciones de teclas.
- Los programas se inician o se apagan por sí solos.
- El programa de correo electrónico comienza a enviar grandes cantidades de correos.
- Se ejecuta una gran cantidad de procesos, ya sean conocidos o no identificables.
- La computadora funciona mucho más lentamente o deja de funcionar.

El software antivirus puede utilizarse como herramienta preventiva o reactiva. Previene las infecciones y detecta y elimina virus, gusanos y caballos de Troya. El software antivirus debe estar instalado en todas las computadoras conectadas

a la red. Existen muchos programas antivirus disponibles, por lo cual en este caso no hablaremos de uno en particular ya que estos dependen de las funciones que incluyan y del soporte que tengan, además de que se cuentan en la mayoría con versiones corporativas, las cuales cuentan con una consola de administración para ejecutar varias tareas desde el servidor, como la actualización del propio antivirus.

Algunas de las funciones que pueden incluirse en los programas antivirus son:

- Verificación de correo electrónico: escanea los correos electrónicos entrantes y salientes e identifica archivos adjuntos sospechosos.
- Escaneo dinámico de residentes: verifica archivos y documentos ejecutables cuando se accede a éstos.
- Escaneos programados: detecciones de virus para que se ejecuten a intervalos regulares y verificar controladores específicos o toda la computadora.
- Actualizaciones automáticas: verifican y descargan características y patrones de virus conocidos. Se puede programar una verificación de actualizaciones.

El software antivirus depende del conocimiento del virus para poder eliminarlo. Por lo tanto, cuando se identifica, es importante notificar al administrador de red acerca del virus o de cualquier comportamiento que se asemeje a un virus. Generalmente, esto se lleva a cabo al enviar un informe de incidentes de acuerdo con la política de seguridad de redes de la empresa, (Huidobro, 2007).

Por lo que como se comentó anteriormente, se recomienda contar con una versión de antivirus corporativa y que todos los equipos se encuentren conectados al servidor, ya que el mejor antivirus siempre va a ser el que se esté “actualizado” constantemente.

Lo que nunca debemos hacer es tener más de un antivirus activo, ya que podríamos tener serios problemas de seguridad e incluso colgar el sistema.

Estas son algunas direcciones en español de programas antivirus donde podremos analizar nuestro equipo online, probarlos, y si quedamos satisfechos comprarlos:

- Trend micro en <http://la.trendmicro.com>
- Bit Defender en <http://www.bitdefender.com/latin>
- Kaspersky en <http://latam.kaspersky.com/mx>
- Norton en <http://mx.norton.com>
- McAfee en <http://www.mcafee.com/mx/>

El **Spyware** es un software espía creado con la finalidad de recoger información del usuario que lo tiene instalado y, en la mayoría de casos, sin que este usuario sea consciente de lo que está ocurriendo.

Existen varios tipos de spyware, por lo que los podemos llamar según la función que realice su código malicioso:

1. **Adware:** abren ventanas (pop-ups) en las que se muestra publicidad mientras ejecutamos aplicaciones.
2. **Spyware:** pequeño programa que se instala en nuestro equipo para robar nuestros datos y espiar nuestros movimientos por la red, recopilando datos sobre las webs que visitamos.
3. **Hijackers:** programa que redirige el navegador de Internet a páginas de su elección “secuestrando” la página de inicio o de búsqueda de nuestro navegador.
4. **Dialers:** programa capaz de modificar el número de teléfono con el que nos conectamos a nuestro ISP (Proveedor de Servicios de Internet) para que llamemos a un número de tarificación adicional con el coste que eso supone. (906;806;807;etc).

Algunos se instalan automáticamente sin nuestro consentimiento, no están calificados como virus pero invaden nuestra intimidad y hacen peligrar en la mayoría de los casos la estabilidad del sistema y especialmente el funcionamiento del navegador o el cliente de correo electrónico, e incluso pueden llegar a recopilar información sobre nosotros y nuestro PC. Otros se instalan

cuando descargamos “extras” para nuestro navegador como por ejemplo toolbars (barras de herramientas adicionales).

Hay ciertos programas que pueden recabar información de nuestros hábitos de navegación para elaborar complejas estadísticas de consumo, normalmente con fines comerciales. La solución para librarnos de esos programas que recogemos a veces de forma involuntaria cuando instalamos un programa freeware, es instalar en nuestro ordenador un antispysware.

3.2.3 Directivas de Restricción de Software

Según Microsoft las directivas de restricción de software mediante su configuración regulan el uso de software en el sistema, software benigno y maligno para el caso de virus informáticos. Entonces las directivas de restricción de software son directivas de confianza, es decir, son reglas definidas por un administrador para restringir aquel software o las secuencias de comandos en las que no se confía y así impedir que realicen acciones no autorizadas en el sistema operativo.

Los usuarios deben tomar decisiones constantemente sobre si ejecutar software desconocido. Con frecuencia, los virus y los caballos de Troya se camuflan intencionadamente para que los usuarios los ejecuten. Resulta difícil para los usuarios hacer elecciones seguras sobre el software que deben ejecutar.

Con las directivas de restricción de software, puede proteger su entorno informático de software en el que no se confía mediante la identificación y la especificación del software cuya ejecución está permitida. Puede definir el nivel de seguridad predeterminado en Irrestringido o No permitido para un objeto de directiva de grupo (GPO) de modo que el software, ya esté permitido o no, se ejecute de manera predeterminada. Puede crear excepciones a este nivel de seguridad predeterminado mediante reglas de directivas de restricción de software para determinado software. Por ejemplo, si el nivel de seguridad predeterminado está establecido en No permitido, puede crear reglas que permitan que determinado software se ejecute.

Nota: Las directivas de restricción de software no deben utilizarse como sustitutos del software antivirus.

A continuación se explica el desarrollo del manual de Directivas de Restricción de Software como parte del manual de Políticas de Seguridad para los laboratorios de TIC, área RyT:

3.2.3.1 Manual de Directivas de Restricción de Software

Como primer requisito, es necesario tener una instalación reciente y limpia de Windows XP. Si no se tiene, siempre antes de implementar esta técnica es recomendable formatear la computadora con Windows XP y hacer una instalación limpia desde cero.

Importante: Se recomienda ampliamente tener dos particiones en el disco duro, por ejemplo: C:\ y D:\ Esto servirá para tener una unidad para el sistema y una para guardar los archivos una vez que el sistema este congelado con DeepFreeze o Shadow User.

1. Configuración del bloqueo de ejecutables en Windows XP

Una vez que se tiene instalado y limpio el sistema operativo, en este caso se hará la configuración en Windows XP, se ejecuta desde la opción de ejecutar el comando **secpol.msc** y damos **Enter**, o **Aceptar** así como se ve en la siguiente imagen.

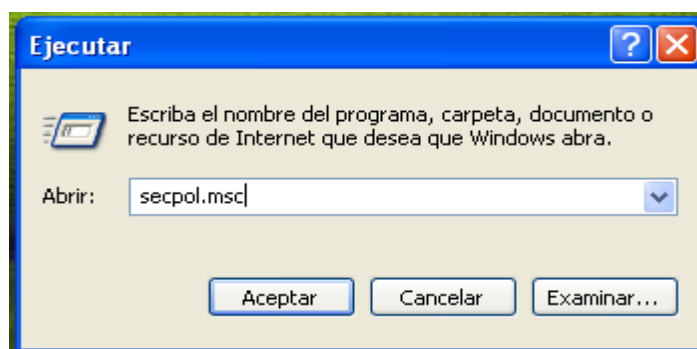


Figura 1.- Ejecutar aplicación

En seguida tendremos otra pantalla en la que buscaremos la siguiente cadena de directorio.

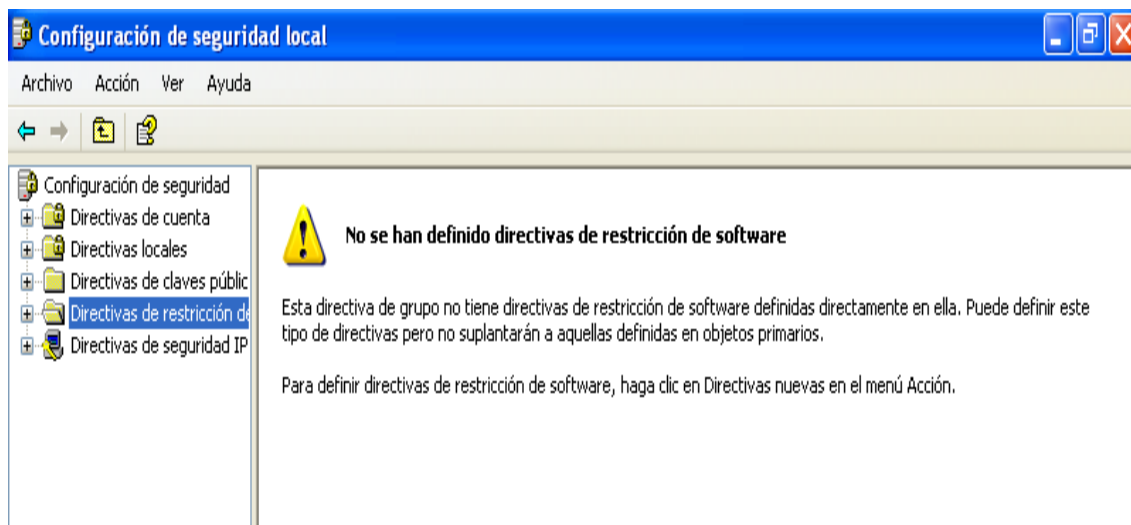


Figura 2.- Directivas de restricción de software

Luego en esa ventana crearemos permiso para crear las Directivas de Restricción de Software. Y para ello solo damos en **Acción/Crear nuevas directivas/**

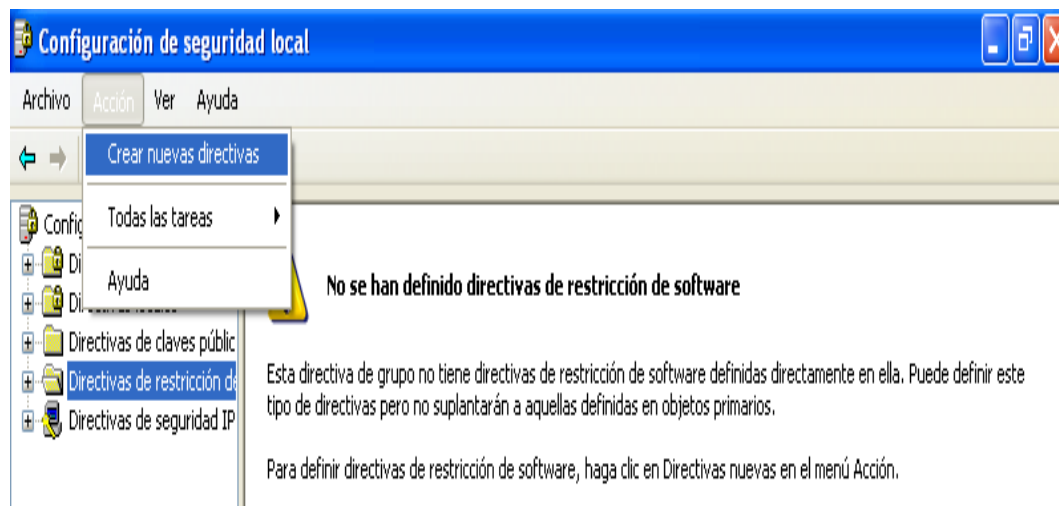


Figura3.- Creación de nuevas directivas

Una vez seleccionada la opción en el menú acción, tendremos la ventana de esta forma.

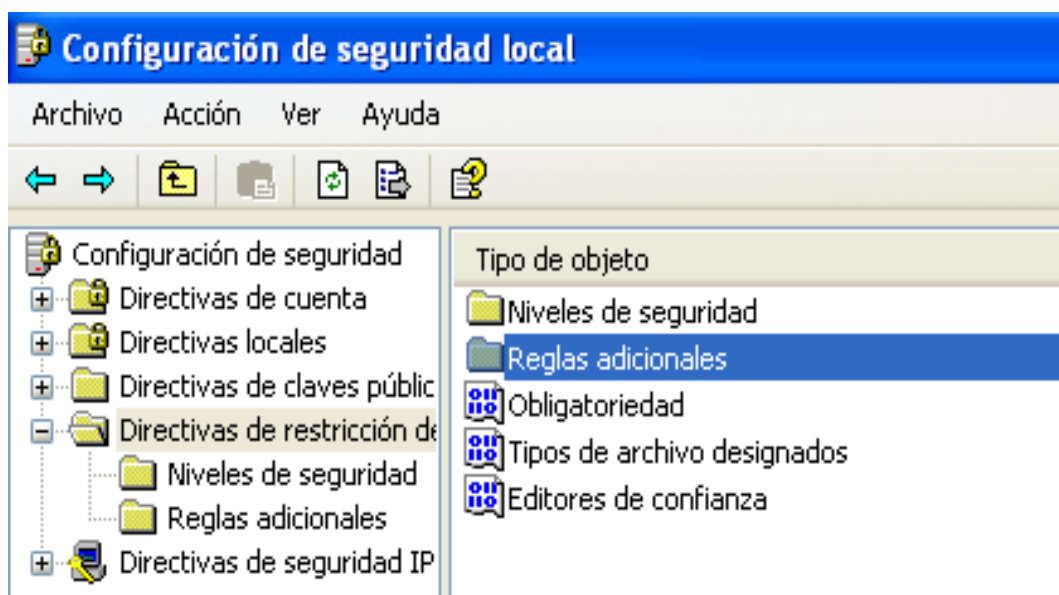


Figura 4.- Reglas adicionales

IMPORTANTE...

Si el nivel de seguridad predeterminado se establece en **No permitido**, automáticamente se crean las siguientes cuatro reglas de ruta de acceso del Registro.

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SystemRoot%

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SystemRoot%.exe*

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SystemRoot%\System32.exe*

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%

Estas reglas de ruta de acceso del Registro se crean como protección contra el bloqueo del sistema para uno mismo y todos los usuarios. Sólo los usuarios avanzados deben considerar la opción de modificar o eliminar estas reglas y se colocan en el Registro:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Para que se ejecuten, asegúrese de crear una regla de ruta de acceso del Registro para ellos.

2. Proceso de configuración

En la ventana anterior daremos doble clic en la opción **Reglas adicionales** y en la siguiente ventana daremos clic derecho y seleccionamos la opción **Regla de nueva ruta...**

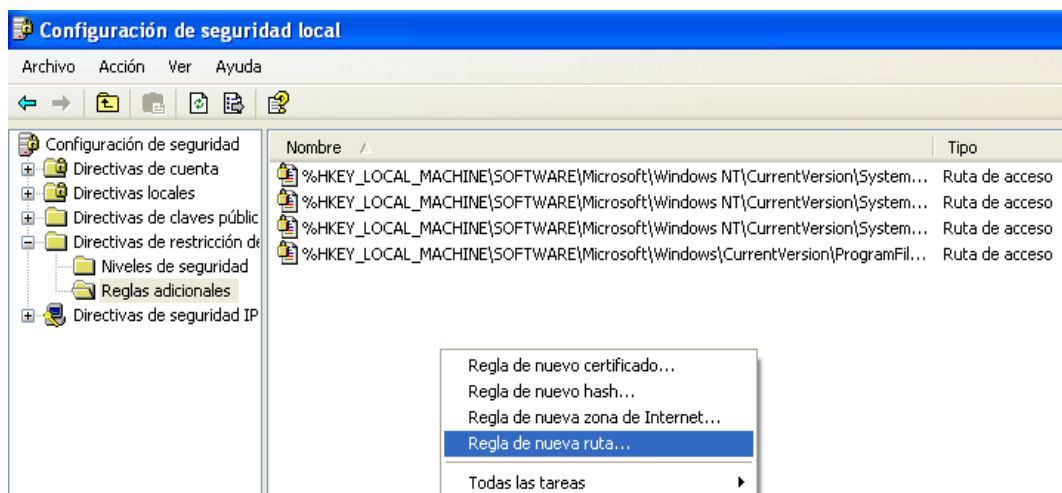


Figura 5.- Creación de regla de nueva ruta

Luego nos aparecerá otra ventanita en la cual tendrá **3 campos de escritura** y una opción de **Examinar...**

El que nos importa por ahora es el campo de escritura **Ruta de acceso:** en el cual escribiremos **A:** y revisa que en el campo de **Nivel de seguridad:** diga **No permitido** y luego da un clic en **Aceptar**.

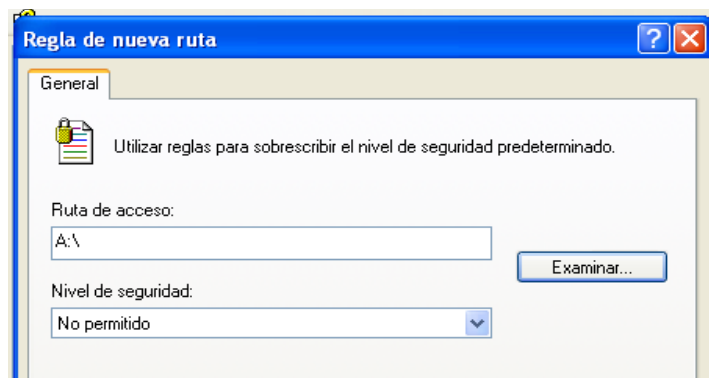


Figura 6.- Nivel de seguridad

Lo anterior es para evitar que archivos ejecutables con extensión tales como: **.exe**, **.bat**, **.com**, **.cmd**, **.vbs**, **.inf**, entre otros considerados como ejecutables, no se ejecuten en la unidad **A:**

Nota: Después de esto hay que repetir 26 veces más, los pasos del proceso y escribiendo la letra que sigue del abecedario por cada paso que se repita y en el campo **Nivel de seguridad:** que diga siempre **No permitido**. Hasta que quede la pantalla de la siguiente manera:

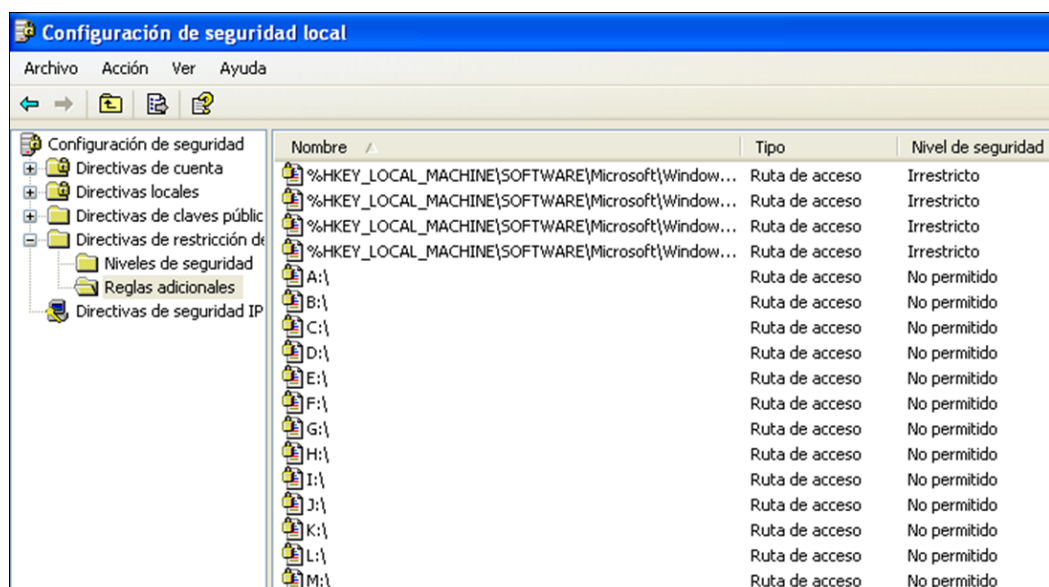


Figura 7.- Niveles de seguridad

Ahora ya todo está restringido, ante ficheros ejecutables y en ninguna parte del sistema se pueden abrir ficheros ejecutables excepto en **algún directorio en particular**. Como se aprecia en la siguiente imagen al tratar de ejecutar el archivo RED.EXE, el cual se encuentra dentro de *Mis documentos* aparecerá un mensaje de error.

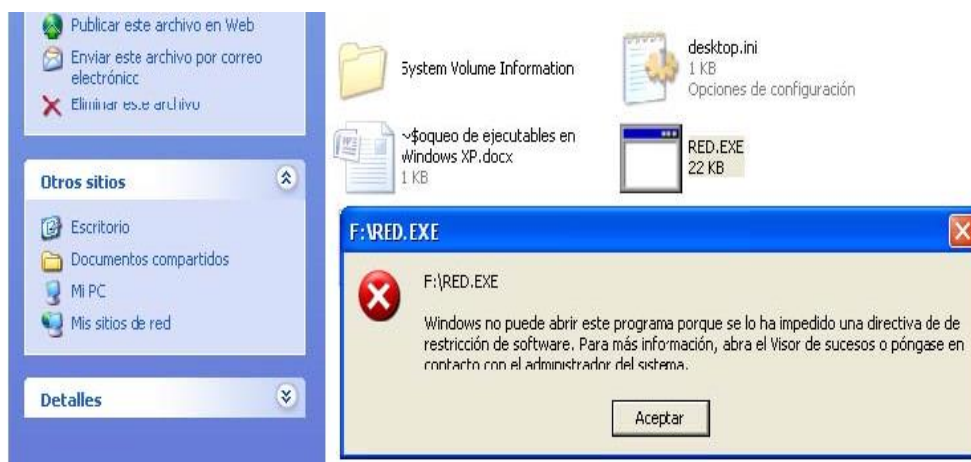


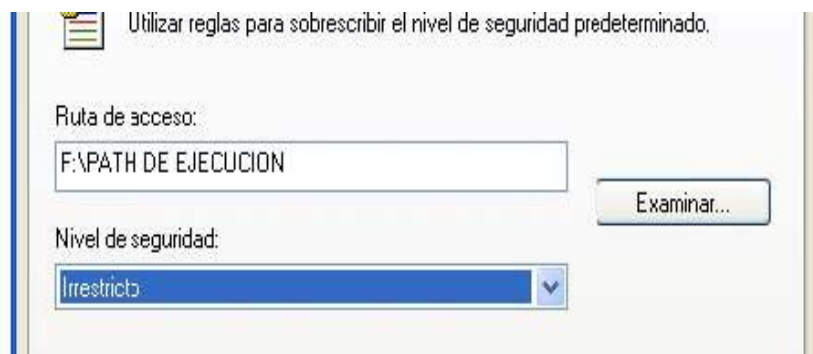
Figura 8.- Bloqueo de ejecutables

Posteriormente, el siguiente paso será crear un directorio en el cual podamos ejecutar los ficheros, en este ejemplo el directorio se llamara *PATH de EJECUCION*, el cual se creara dentro de *Mis documentos*, como se puede apreciar en la siguiente imagen:



Figura 9.- Ruta de ejecución

Ahora vamos de nuevo a nuestra directiva de restricción de software para darle permiso de ejecución a ese directorio **repetiendo los pasos del proceso 1** solo que esta vez daremos clic en el botón **Examinar...** y buscamos el directorio que dice *PATH de EJECUCION* y damos **Aceptar**, y en **Nivel de seguridad:** ponemos **Irrestringido** y damos en **Aceptar**, como se puede apreciar en las siguientes imágenes



F:\	Ruta de acceso	No permitido
F:\PATH DE EJECUCION	Ruta de acceso	Irrestringido
G:\	Ruta de acceso	No permitido

Figura 10 y 11.- Niveles de seguridad irrestringido

Por último, tomamos el programa que deseamos instalar y primero lo copiamos al directorio de instalación y lo ejecutamos, como se muestra en la imagen siguiente:

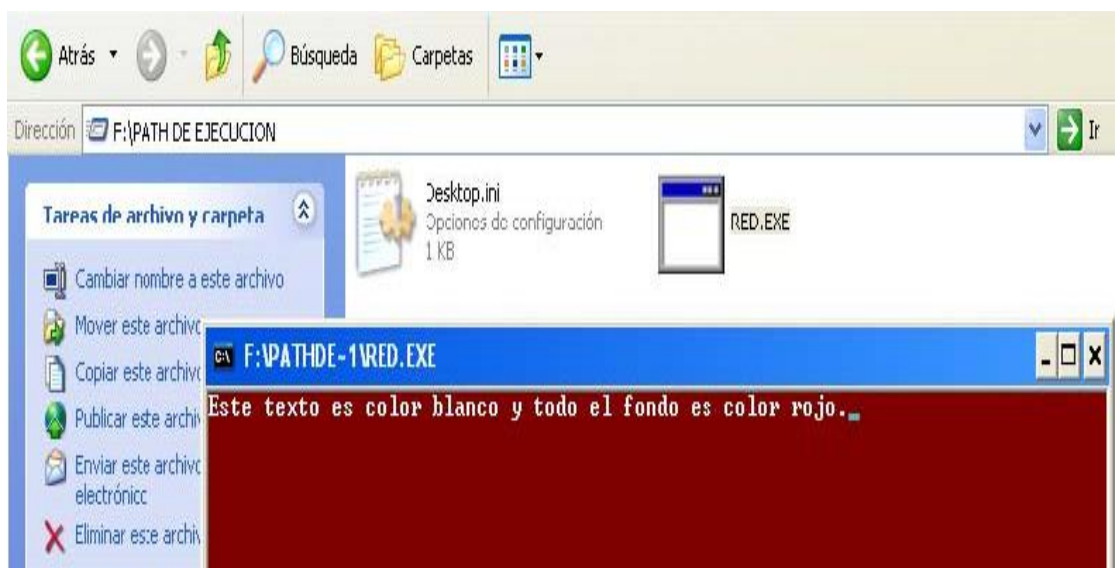


Figura 12.- Única ruta de ejecución

NOTA: Esta es una técnica bastante tediosa pero también bastante efectiva, (López E. 2011)

3.2.4 Restauración del sistema operativo

La restauración del sistema permite restaurar los archivos de sistema del equipo a un momento anterior. Es una manera de deshacer cambios del sistema realizados en el equipo, sin que esto afecte a los archivos personales, como el correo electrónico, documentos o fotografías.

A veces, la instalación de un programa o un controlador puede hacer que se produzca un cambio inesperado en el equipo o que el sistema operativo de Windows funcione de manera imprevisible. Por lo general, al desinstalar el programa o el controlador se corrige el problema. Si la desinstalación no soluciona el problema, se puede intentar restaurar el sistema del equipo al estado en que se encontraba en una fecha anterior, cuando todo funcionaba bien.

La restauración del sistema usa una característica denominada Protección del sistema para crear y guardar puntos de restauración en el equipo. Estos puntos de restauración contienen información acerca de la configuración del Registro y otra información del sistema que usa Windows, además se pueden crear puntos de restauración manualmente.

Por lo tanto, la aplicación “Restaurar Sistema” es una herramienta implementada en Windows que permite devolver al equipo a un estado anterior y no está diseñada para hacer copias de seguridad de archivos personales, de manera que no puede usarse para recuperar un archivo personal que se ha eliminado o dañado. Se deben de hacer copias de seguridad periódicas de archivos personales y datos importantes con un programa de copia de seguridad.

En esta aplicación el usuario puede crear un punto de restauración manualmente, elegir un punto existente para restaurar el sistema o cambiar la configuración. Sin embargo esta aplicación generalmente esta deshabilitada debido al espacio que puede llegar a ocupar en el disco duro y por el tiempo que tarda en generarse

Por lo que existen aplicaciones más eficientes que permiten mantener siempre un punto de restauración único, es decir que mantiene el sistema operativo en un punto congelado.

StorageCraft proporciona una nueva forma de resolver los actuales problemas de seguridad, la protección de datos y problemas de recuperación de desastres. Su enfoque único proporciona la prevención de desastres, la protección de datos y problemas de recuperación de desastres antes de que ocurran. ¿Por qué recuperar desde una PC desastres cuando se pueden prevenir?

Esta aplicación utiliza un método único llamado Shadow Mode para asegurar que los datos de la PC están protegidos, sin importar lo que suceda. Shadow Mode da seguimiento de cada cambio en el sistema y los redirige a un lugar no utilizado en el disco. Estos cambios en el sistema pueden ser permanentemente guardados en el disco, o descartarse por completo.

Shadow User ofrece protección para los sistemas operativos Windows y es una de las mejores maneras para evitar cambios no deseados o maliciosos que se realicen a una PC y es de fácil uso y de seguridad de escritorio, ya que puede restaurar el estado previo del sistema, sin importar lo que haya pasado en la PC.

Esta solución de Storage Craft tiene cero impacto en la configuración actual de la PC, ya que no hay modificaciones en el Master Boot Record (MBR), particiones o la estructura del disco. Dicha solución captura una instantánea de su sistema y se ejecuta un duplicado exacto de su PC en un estado virtual.

Este estado virtual, llamado Shadow Mode, permite al usuario utilizar la PC sin tener que escribir en el disco. Los cambios del sistema o archivos que se producen durante una sesión de Shadow Mode, pueden ser de forma automática o manual guardados en el disco o descartados. Esto les da completo control al usuario de la PC y profesionales de TI.

Shadow Mode no permite que los virus o gusanos que se escriben en el equipo guarden sus modificaciones, ya que el virus puede llegar al volumen virtual, pero puede ser descartada antes de los cambios se confirman en el disco.

Este enfoque es la primera línea de defensa a la seguridad, protección de datos y de recuperación de desastres y evita los problemas de siempre existente. Este método proporciona una capa de la prevención de desastres a su sistema en lugar de tratar de recuperar un sistema mediante la aplicación de actualizaciones de virus o un gusano después de ocurrido el desastre.

A continuación se explica de forma detallada el desarrollo del manual de Restauración del S.O. con la aplicación mencionada y su funcionamiento:

3.2.4.1 Manual de Restauración del Sistema Operativo

Para realizar este manual, utilizaremos el software de **Shadow User Pro**, el cual como ya se explicó nos permite “congelar” el sistema de nuestro equipo de cómputo, por lo que la restauración del sistema es automática cada vez que se reinicia el sistema, a continuación se explica dicho procedimiento:

1. Como podemos ver en la siguiente imagen, el programa nos indica que el Volumen C está desprotegido y que Shadow User Pro está deshabilitado. Vámonos al apartado de configuración como se aprecia a continuación:

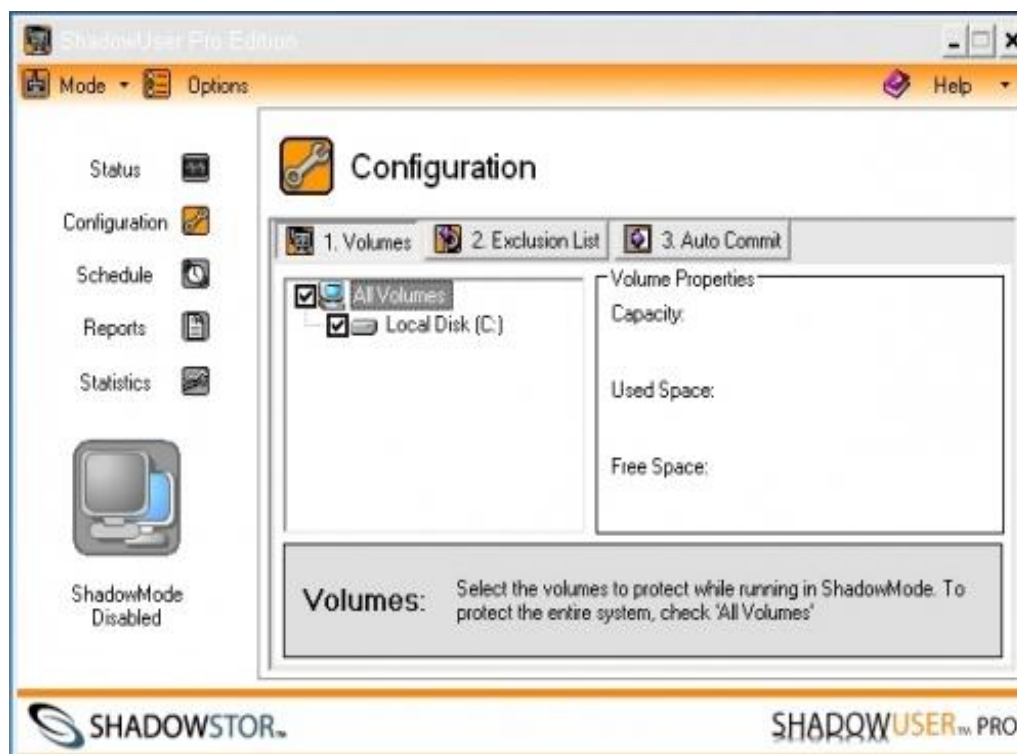


Figura 13.- Configuración de unidades

Aquí nos saldrían los discos duros que podemos congelar. En este caso sólo disponemos de Unidad C:\ pero sería válido también para otros discos duros o particiones.

También podemos indicar que directorio del disco duro queremos excluir de que quede congelado. Es decir, que si congelamos el disco duro pero queremos que la persona que lo utiliza pueda guardar lo que necesite en la carpeta *PATH de EJECUCION* por ejemplo o la carpeta *DATOS* podemos habilitar esta opción, como se muestra enseguida.

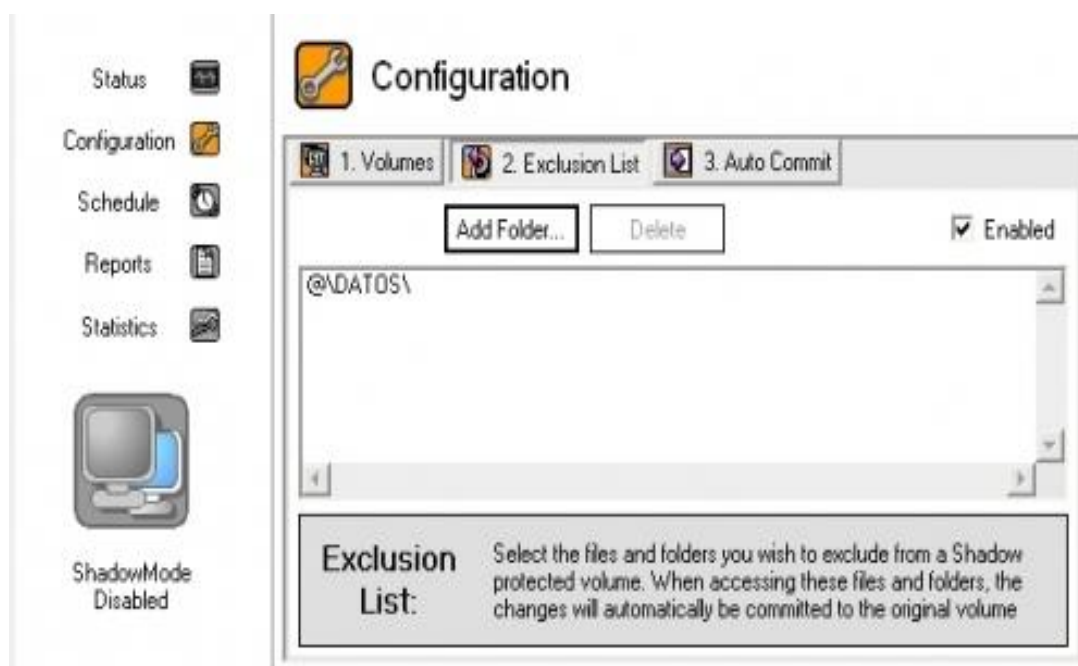


Figura 15.- Carpeta excluida para guardar datos

Posteriormente le damos a activar Shadow User Mode y nos dirá que va a reiniciarse la computadora, como se muestra en la siguiente imagen:

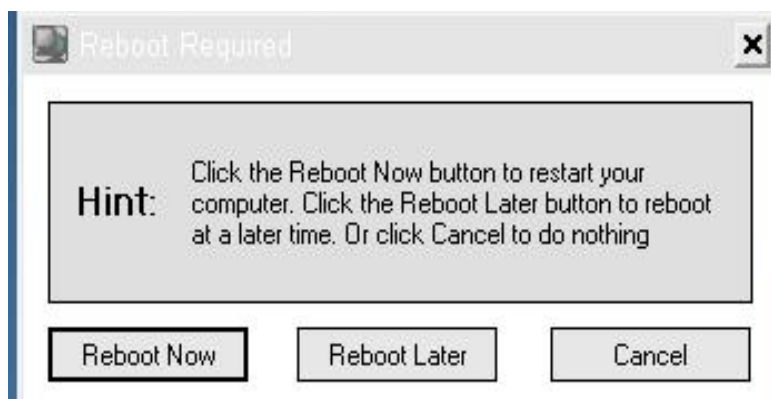


Figura 16.- Reiniciar la aplicación al aplicar cambios

Una vez aplicados los cambios y después que el equipo se reinicie, nos aparecerá la siguiente imagen, donde se aprecia como papel tapiz la imagen del programa SHADOW.



Figura 17.- Papel tapiz de la aplicación

Este fondo nos indica que Shadow User Pro está activo. Y por lo tanto ahora cualquier cambio que hagamos **no quedará guardado**, excepto lo que sea

almacenado en el directorio *PATH de EJECUCION*, o *DATOS* el cual fue excluido.

Desventajas:

1. La primera y la más grande es que los usuarios comunes o a quienes se les de soporte aplicando esta práctica de restricción, no podrán usar al 100% su sistema, puesto que no tendrán la facilidad de instalar y quitar programas. *Para hacerlo tienen que recurrir al administrador del sistema.*
2. Para ejecutar un programa, no podrás hacerlo desde un USB, o una unidad de CD o DVD, para ello tienes que copiarlo al directorio *PATH DE EJECUCION* y ejecutarlo desde allí.

Ventajas:

1. Una de las ventajas es que los ficheros que son considerados ejecutables y que resultan ser una amenaza de seguridad para tu sistema, no se ejecutarían desde tu unidad USB/CD/DVD u otro, ni los ficheros autorun.inf y eso ya es un gran avance de seguridad.
2. Cualquier persona que no sea el propietario podrá usar el equipo y no tiene que preocuparse por infección de virus, además de que tampoco infectara a otros usuarios.
3. La otra ventaja que se refleja en esta práctica, es que no volverás a saber más de infección de virus en el sistema, siempre y cuando se sigan los consejos expuestos aquí.
4. La última y la más importante: Si un usuario intencionalmente mete un **virus** en algún directorio donde esté permitido su ejecución, por ejemplo el directorio *PATH DE EJECUCION*, el virus infectara temporalmente tu equipo y posteriormente al reiniciar, el sistema estará tan impecable como si nunca se hubiese infectado. Puesto que cada cambio que se haga en el sistema mientras SHADOW este activado será devuelto a su estado anterior.

Es importante mencionar que existen varios programas de este tipo, conocidos como: "reinicie y restaure" (*Reboot and Restore*). Uno de los más importantes

aparte del SHADOW expuesto anteriormente, es el **DeepFreeze** desarrollado por la compañía Canadiense Faronics en 1996, el cual es un controlador del núcleo que protege la integridad del disco duro redirigiendo la información que se va a escribir en el disco duro o partición protegida, dejando la información original intacta.

Esto permite a los usuarios realizar cambios *originales* en el equipo, por ejemplo para probar cambios potencialmente estables o benignos, sabiendo que al reiniciar el sistema volverán a desaparecer.

Durante el desarrollo de este proyecto, se realizó la implementación de la aplicación de StorageCraft (SHADOW), de acuerdo al procedimiento mencionado anteriormente, sin embargo se pretenden realizar pruebas de rendimiento con respecto a la herramienta de Faronics (DeepFreeze) y poder realizar la propuesta para su adquisición, ya que las versiones que se tienen son sólo de evaluación.

Por último, se explica a continuación el desarrollo y propósito del manual de procedimientos sobre la función específica para la administración de la red, mediante el direccionamiento dinámico de los equipos a través de un servidor DHCP, así como su control e implementación.

CAPITULO 4. MANUAL DE FUNCIÓN ESPECÍFICA PARA LA ADMINISTRACIÓN DE LA RED

Diariamente las personas utilizan los servicios disponibles en las redes y en Internet para comunicarse con otros y realizar tareas de rutina. Pocas veces pensamos en los servidores, clientes y dispositivos de redes necesarios para poder recibir un correo electrónico, introducir información en un blog o comprar los mejores artículos a buen precio en una tienda en línea. La mayoría de las aplicaciones de Internet más comunes se basa en interacciones complejas entre diversos servidores y clientes.

El término servidor hace referencia a un host que ejecuta una aplicación de software que proporciona información o servicios a otros hosts conectados a la red. Un ejemplo conocido de dicha aplicación es un servidor Web. Existen millones de servidores conectados a Internet que proporcionan servicios como sitios Web, correo electrónico, transacciones financieras, descargas de música, etc. Un factor fundamental para permitir el funcionamiento de estas interacciones complejas es que todos emplean estándares o protocolos acordados.

Por ejemplo para solicitar y ver una página Web, el usuario utiliza un dispositivo que ejecuta software cliente de Web. Cliente es el nombre que se le da a una aplicación informática que se utiliza para acceder a información almacenada en un servidor. Un buen ejemplo de cliente es un explorador Web.

Cada servicio disponible en la red tiene sus propios protocolos de aplicación que se implementan en el software de cliente y servidor. Además de los protocolos de aplicación, todos los servicios de Internet tradicionales utilizan el protocolo de Internet (IP) para asignar direcciones a los mensajes y enrutarlos a los hosts de origen y de destino.

En las redes locales, es habitual que la población de usuarios cambie frecuentemente, ya que se agregan nuevos usuarios con equipos de cómputo y esos usuarios requieren una conexión de red, por lo cual el administrador de red debe asignar direcciones IP para cada estación de trabajo y mantener una administración adecuada de dichas direcciones, esto puede resultar muy tedioso y poco eficiente, por lo cual un método más simple de administración es que las

direcciones IP se asignen automáticamente desde un servidor. Esto se logra a través de un protocolo denominado Protocolo de Configuración Dinámica De Host (**DHCP**).

El protocolo DHCP proporciona un mecanismo para la asignación automática de información de direccionamiento, como una dirección IP, una máscara de subred, un gateway predeterminado y otra información de configuración.

“DHCP es generalmente el método preferido para asignar direcciones IP a los hosts de grandes redes, dado que reduce la carga para al personal de soporte de la red y prácticamente elimina los errores de entrada, (Atelin, 2007).”

Con lo que respecta a la estructura de la red, es importante mencionar que esta es la columna vertebral de toda red, por lo cual el cableado estructurado es el principal componente para un correcto desempeño de la red, además de su ampliación y administración debido a que este se encuentra dividido en módulos o subsistemas los cuales llevan a cabo funciones específicas, como las que se mencionan a continuación:

- Implementación del backbone entre sites (cableado vertical)
- Implementación de nodos de red (cableado horizontal)
- Identificación de puertos de acceso a red (cuarto de telecomunicaciones)
- Identificación de fallas en nodos de red (área de trabajo)

Por lo cual para una correcta administración de la Red, esta debe de contar con una infraestructura adecuada, es decir un cableado estructurado 100% funcional, ya que sin ello la administración de los equipos y servicios, así como la implementación de herramientas de gestión de recursos para un mayor aprovechamiento de estos sería muy difícil y poco eficiente.

A continuación se explica de forma detallada la elaboración de un manual para la implementación de un Servidor DHCP:

4.1 Manual de implementación de un Servidor DHCP

A continuación se describe el procedimiento para la **implementación de un Servidor DHCP** para la administración y control de las direcciones IP en los laboratorios de cómputo de la división de TIC, Área RyT.

4.1.1 Instalación del Servidor DHCP

El Protocolo de Configuración de Host Dinámico (DHCP) se puede instalar **manualmente** o mediante el **Asistente para administrar su servidor de Windows Server 2003**. En este caso vamos a utilizar el asistente para realizar la instalación.

1.- Para poder acceder al asistente es necesario ir al **menú, inicio / administrative tools / configure your Server wizard**, como se muestra en la imagen.

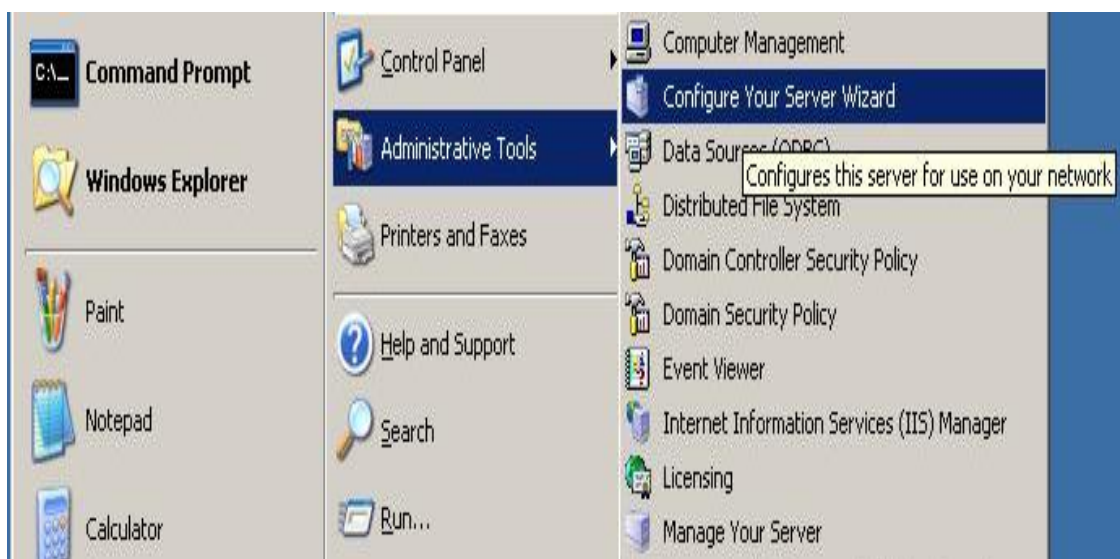


Figura 18.- Asistente para configurar el servidor

2.- En seguida nos muestra esta ventana la cual nos da la bienvenida al asistente, le damos un clic en **Next (siguiente)**.



Figura 19.- Bienvenida al asistente de instalación

3.- Posteriormente nos envía a la siguiente ventana en ella nos muestra los requerimientos que se necesitan para instalar algún servicio, y posteriormente le damos en la opción **Next (siguiente)**.

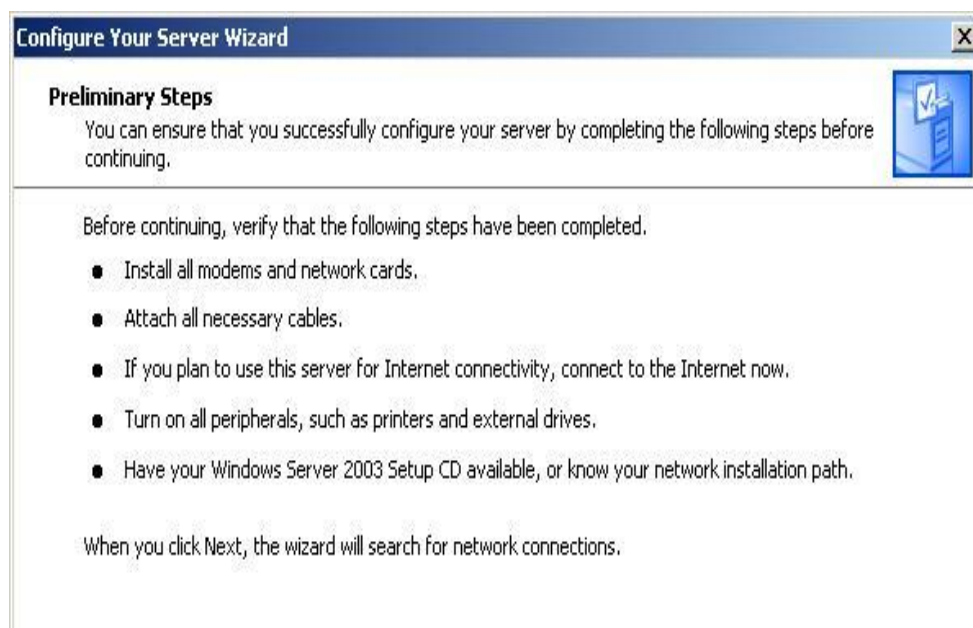


Figura 20.- Pasos preliminares para la instalación

4.- Después nos muestra esta ventana la cual nos hace referencia a que está buscando la red o redes que están directamente conectadas

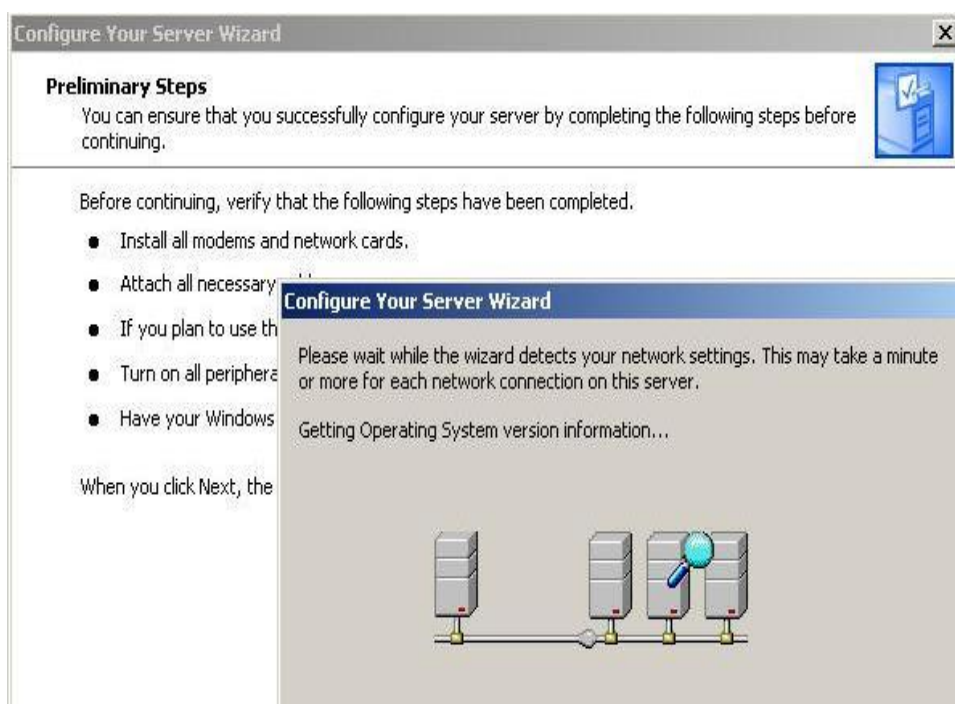


Figura 21.- Detección de la red para la instalación

5.- En esta ventana nos muestra todos los servicios que pueden ser habilitados con el asistente, en esta caso seleccionaremos la opción que dice **DHCP Server**

Nota: Esta opción solo nos permite dar de alta un Servicio y no varios al mismo tiempo como en el Panel de Control.

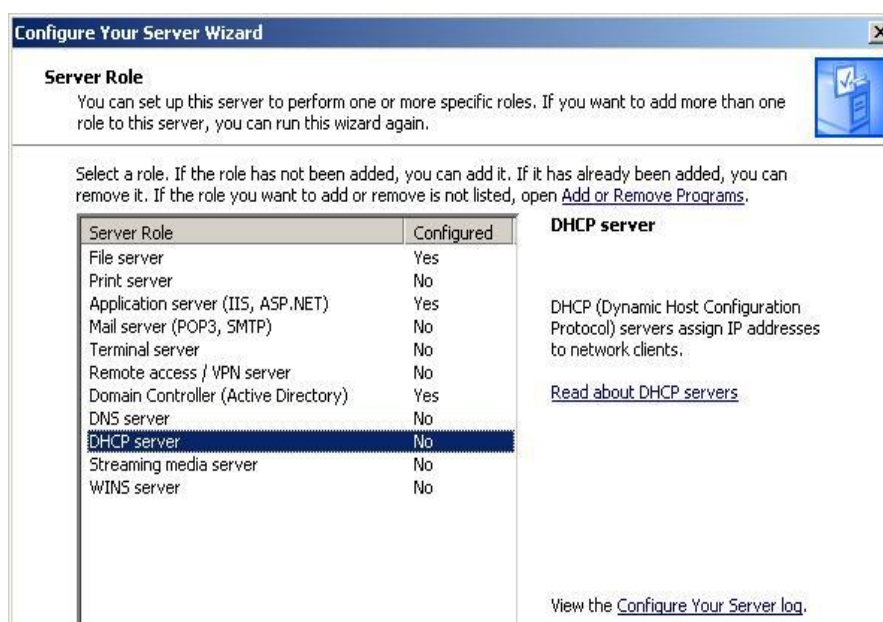


Figura 22.- Selección del servicio DHCP

6.- En esta ventana nos da un Resumen final del Asistente, por lo que debemos confirmar con la opción de **Next (siguiente)** que hemos seleccionado en este caso para el DHCP Server.

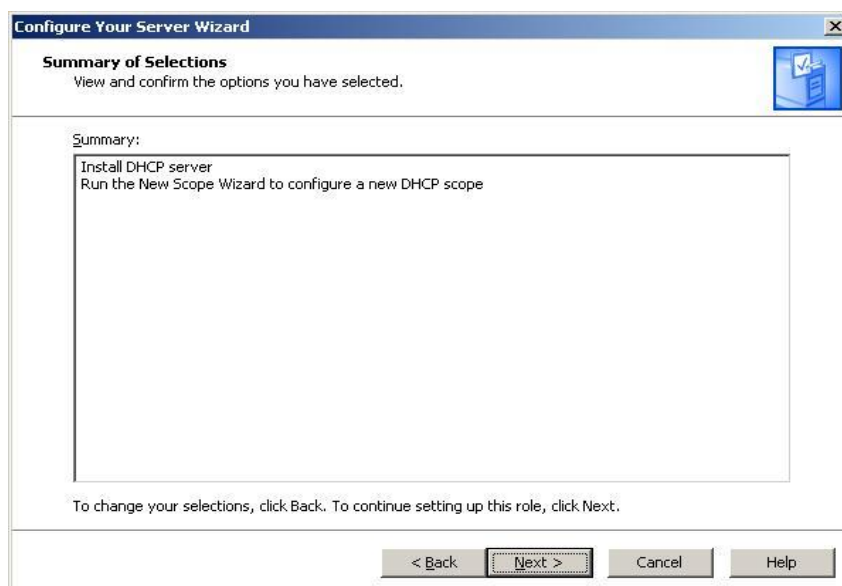


Figura 23.- Resumen de instalación del servicio DHCP

7.- A continuación nos muestra el proceso de instalación del servicio, después de que termine de llenarse la barra, le damos un click en **Next (siguiente)**.

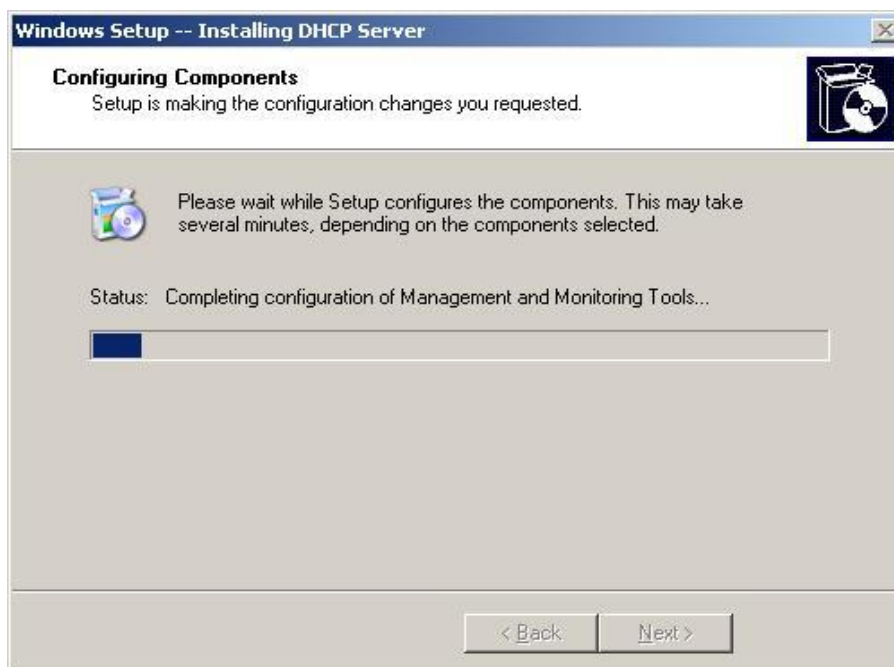


Figura 24.- Inicio de instalación del servicio DHCP

8.- Por último nos muestra el fin del proceso de instalación del asistente, y le damos **finalizar (finish)**.



Figura 25.- Finalización de instalación del servicio DHCP

Una vez instalado el servicio DHCP está listo para configurarlo, de acuerdo al siguiente procedimiento:

4.1.2 Configuración del Servidor DHCP

1.- Para poder configurar el DHCP es necesario ingresar a él para hacer estos se sigue la siguiente ruta **Start / administrative tools / DHCP**

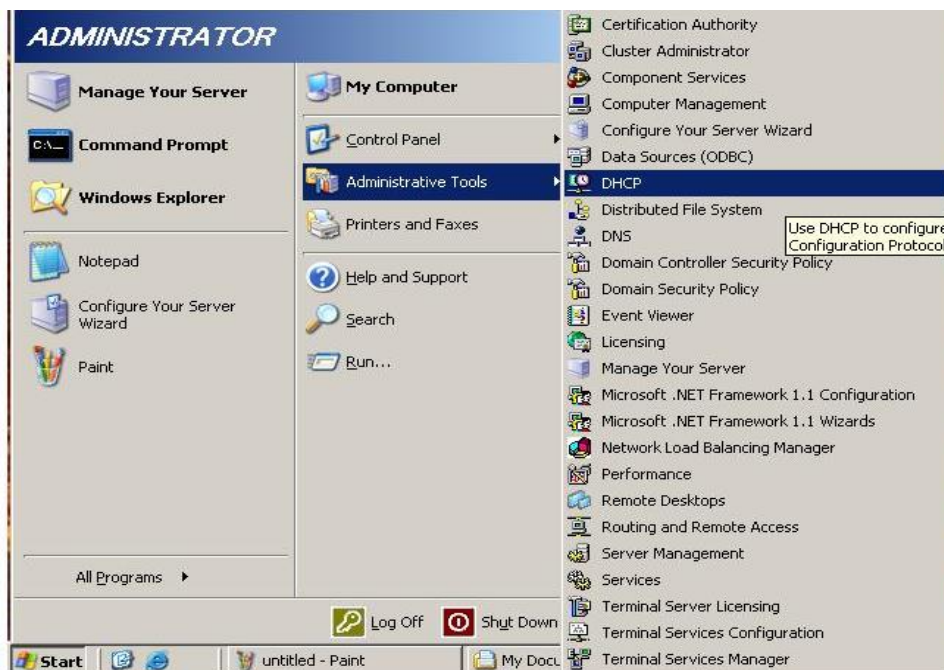


Figura 26.- Seleccionar el servicio DHCP instalado

2.- Esta es la ventana principal de DHCP pero nos muestra que el dispositivo está en rojo lo que significa que esta debe ser autorizado por el servidor principal,

desde la opción **Action / Authorize**. Posteriormente la fecha roja pasa a verde (oprima **F5** para actualizar).

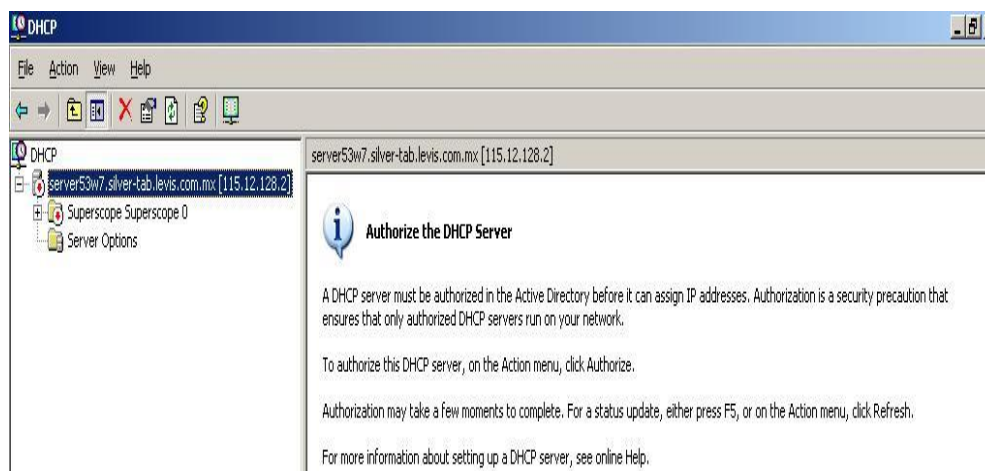


Figura 27.- Autorización del servicio DHCP

3.- Una vez autorizado el servicio DHCP es necesario agregar un nuevo rango para las direcciones IP. Para esto le damos click en el **menu / Action / new Scope**. Enseguida aparece el asistente de configuración y le damos en **Next (siguiente)** como lo muestra la imagen siguiente.



Figura 28.- Asistente para crear el rango de direcciones IP

4.- Esta ventana nos solicita el nombre del rango (Scope) y una descripción del mismo, esto es para que sea más fácil de reconocer en nuestra red el segmento que será utilizado por el servidor DHCP. En este caso le llamamos al Scope **LAB TIC Área RyT** le damos en **Next (siguiente)**.

New Scope Wizard

Scope Name
You have to provide an identifying scope name. You also have the option of providing a description.

Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name: LAB TIC AREA RYT

Description: HOSTS DEL LABORATORIO DE TIC RYT

< Back Next > Cancel

Figura 29.- Nombre y descripción del rango

5.- En esta ventana nos pide que ingresemos un rango de direcciones IP que va a utilizar nuestro Scope, así mismo también pide la máscara de red.

En nuestro escenario utilizamos el rango de direcciones IP de la **192.168.10.11** a la **192.168.10.250**, con una máscara de subred **255.255.255.0** y le damos en **Next (siguiente)**

New Scope Wizard

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 10 . 11

End IP address: 192 . 168 . 10 . 250

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length: 24

Subnet mask: 255 . 255 . 255 . 0

< Back Next > Cancel

Figura 30.- Rango de direcciones IP validas del DHCP

6.- En esta ventana nos da la opción de excluir un rango de IP's o direcciones individuales, ya sea para servidores, impresoras, routers o simplemente para tenerlas de respaldo. Se da de alta el rango desde donde inicia hasta donde termina y se agrega en la opción de **Add** y posteriormente la opción de **Next (siguiente)** para continuar. En este caso se excluyeron 6 rangos diferentes, uno para cada laboratorio y sala de profesores.

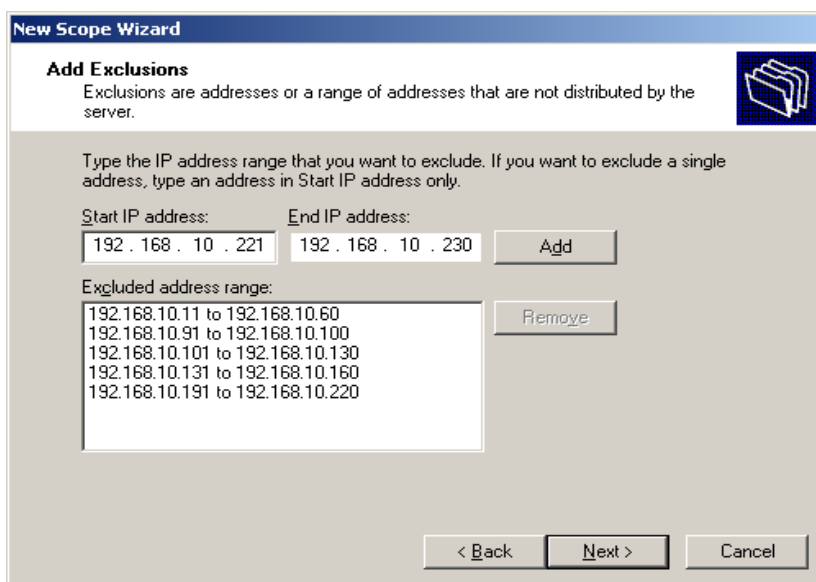


Figura 31.- Rango de direcciones IP excluidas

7.- Posteriormente en esta ventana nos pide que ingresemos el tiempo en días, horas y minutos que el Scope le brindara a las direcciones IP a los usuarios, en este caso se prestara la IP por 10 horas y luego le damos en **Next** para continuar.

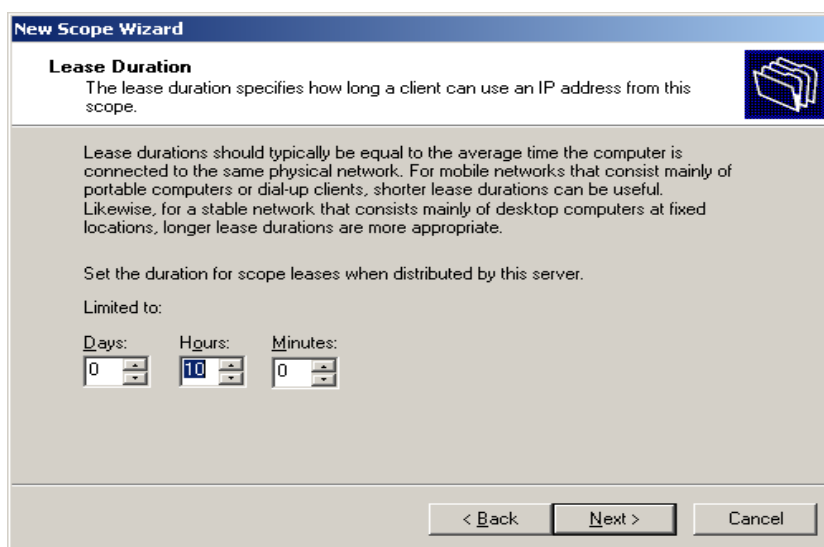


Figura 32.- Tiempo de asignación de las direcciones IP

8.- Una vez configurado el rango de direcciones IP, la siguiente ventana nos pregunta si queremos configurar la opciones del Scope, en este caso se pondrá la segunda opción la cual dice que queremos configurar las opciones después y le damos en **Next (siguiente)**

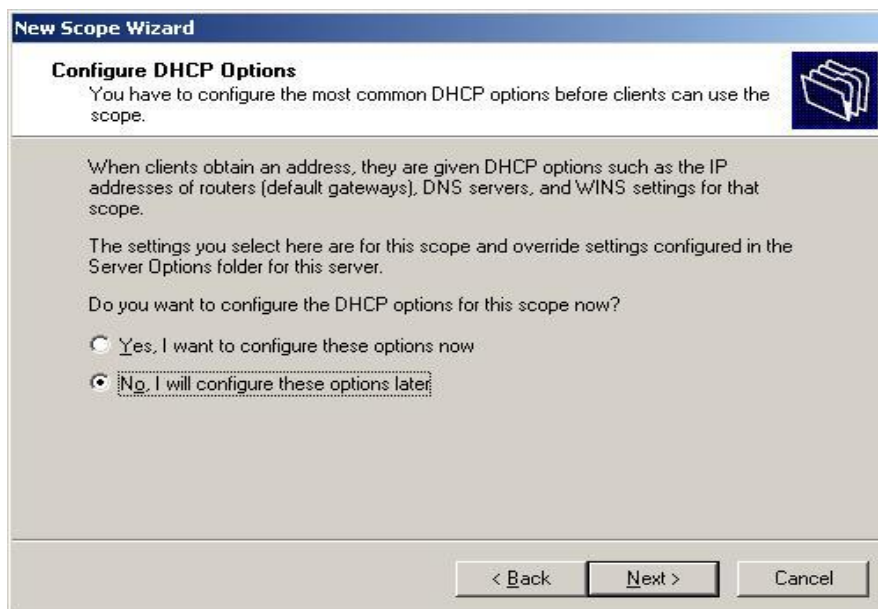


Figura 33.- Configuración de opciones del DHCP posteriormente

Finalmente, una vez completado la configuración del Scope, solo nos queda terminarla dándole a la opción **finalizar (finish)**.

9.- En la siguiente imagen se puede apreciar la consola del servidor DHCP, donde se muestra el rango de direcciones asignadas, así como los 6 rangos de exclusión.

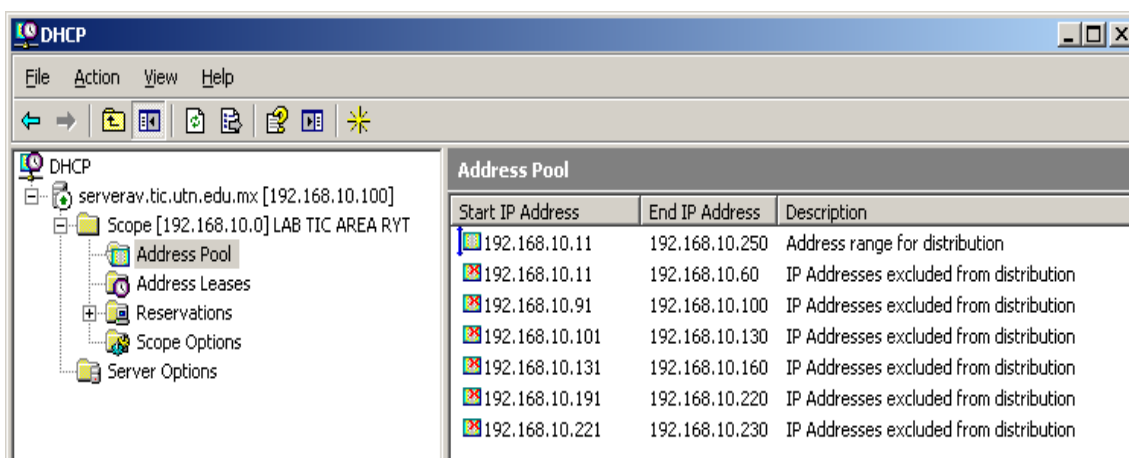


Figura 34.- Configuración final del DHCP

10.- Una vez configurado el rango (scope) del servidor DHCP y el tiempo de asignación de las direcciones IP de forma dinámica, es importante configurar los parámetros adicionales necesarios en la configuración de un host para poder tener acceso a Internet por ejemplo.

Esto se realiza desde la opción de Scope Options como se aprecia en la siguiente imagen:

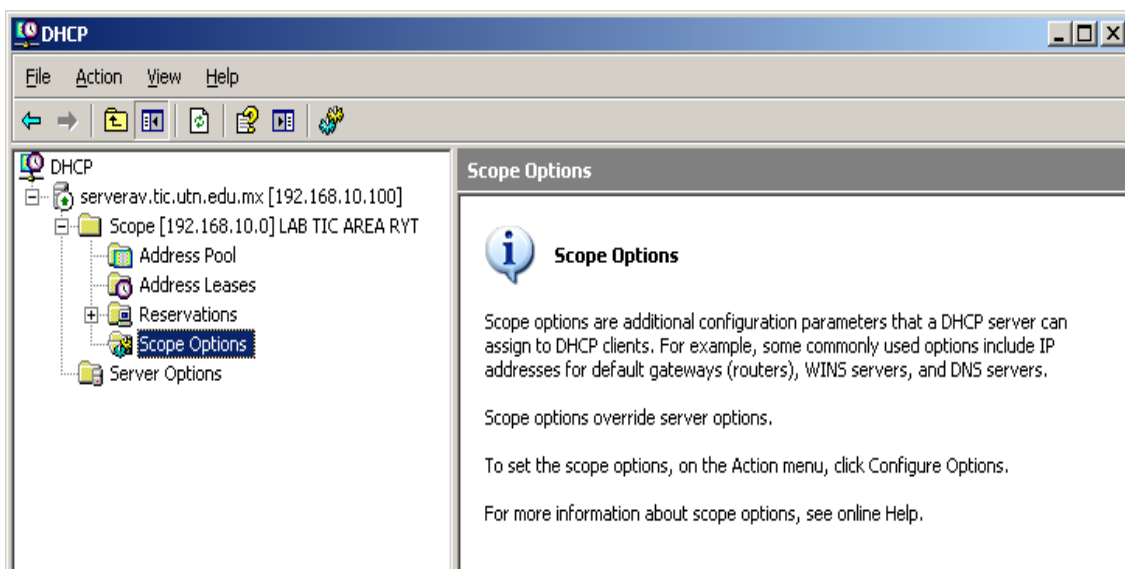


Figura 35.- Configuración de opciones del DHCP

11.- Uno de los parámetros principales que se configuran desde esta opción es el Default Gateway o Puerta de Enlace, la cual es necesaria para que los host puedan tener acceso a otras redes, ya sea dentro de la Intranet o hacia el Internet, como se muestra a continuación:

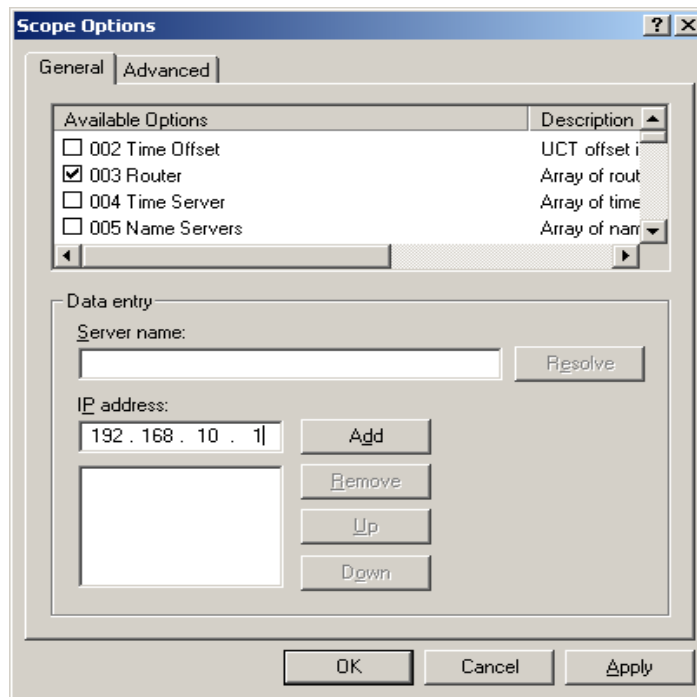


Figura 36.- Configuración del default Gateway del DHCP

12- Es importante recordar que para poder navegar por internet ya sea a través de una dirección IP privada o pública, es necesario contar con los servicios de uno o más Servidores DNS, los cuales son los responsables de resolver las peticiones de los host de acuerdo a una dirección IP de internet según el dominio al que corresponda. En este caso se muestra cuáles son las direcciones de los servidores DNS de la UTN.

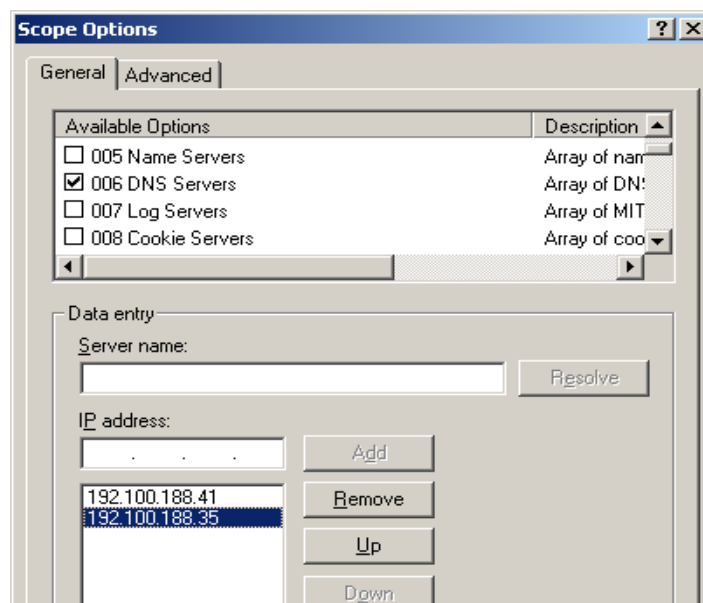


Figura 37.- Configuración de los servidores DNS del DHCP

Estos son los parámetros principales que se agregan al Servidor para que los clientes puedan obtenerlos de forma automática y tengan acceso a la red local y también a Internet.

Además si los equipos están dentro de un dominio, también se puede agregar este valor en la opción 015 “nombre del dominio”. En este caso el dominio público de la Universidad es “utn.edu.mx”.

4.1.3 Configuración de un Cliente DHCP

Una vez configurado el Servidor DHCP, deberán ser configurados los Clientes de acuerdo al siguiente procedimiento y posteriormente la comprobación de los mismos, así como su monitoreo desde el Servidor a través de la consola de direcciones asignadas y direcciones reservadas desde el Servidor DHCP como se muestra a continuación:

1.- Para obtener la IP de manera dinámica desde el Servidor sólo basta ir a **opciones de red / protocolo TCP/IP** y elegir la primera opción la cual nos dice que si queremos obtener la IP de manera automática. También podemos obtener de forma dinámica la dirección IP de los servidores DNS, como se muestra en la imagen.

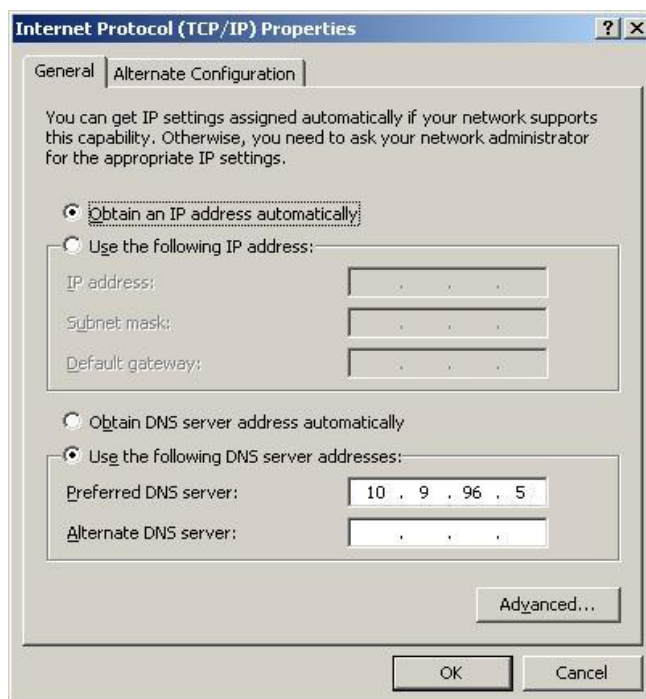


Figura 38.- Configuración TCP/IP del cliente DHCP

2.- Una forma de verificar la configuración asignada por el servidor DHCP desde el cliente es a través del comando **ipconfig /all** desde la consola de MS-DOS

```
C:\WINDOWS\system32\CMD.exe
C:\Documents and Settings\ADMIN>IPCONFIG /ALL
Configuración IP de Windows

Nombre del host . . . . . : JESTEY
Sufijo DNS principal . . . . . :
Tipo de nodo . . . . . : híbrido
Enrutamiento habilitado. . . . . : No
Proxy WINS habilitado. . . . . : No
Lista de búsqueda de sufijo DNS:  tic.utn.edu.mx

Adaptador Ethernet Conexión de área local 2      :
Sufijo de conexión específica DNS : tic.utn.edu.mx
Descripción. . . . . : Realtek RTL8169/8110 Family Gigabit Ethernet NIC
Dirección física. . . . . : 00-16-17-9A-F3-CA
DHCP habilitado. . . . . : No
Autoconfiguración habilitada. . . . . : Si
Dirección IP. . . . . : 192.168.10.132
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 192.168.10.1
Servidor DHCP . . . . . : 192.168.10.100
Servidores DNS . . . . . : 192.100.100.41
                             192.100.100.35
Concesión obtenida . . . . . : Lunes, 22 de Octubre de 2012 03:54:56 p.m.
Concesión expira . . . . . : Martes, 23 de Octubre de 2012 01:54:56 a.m.
```

Figura 39.- Asignación de valores del cliente DHCP

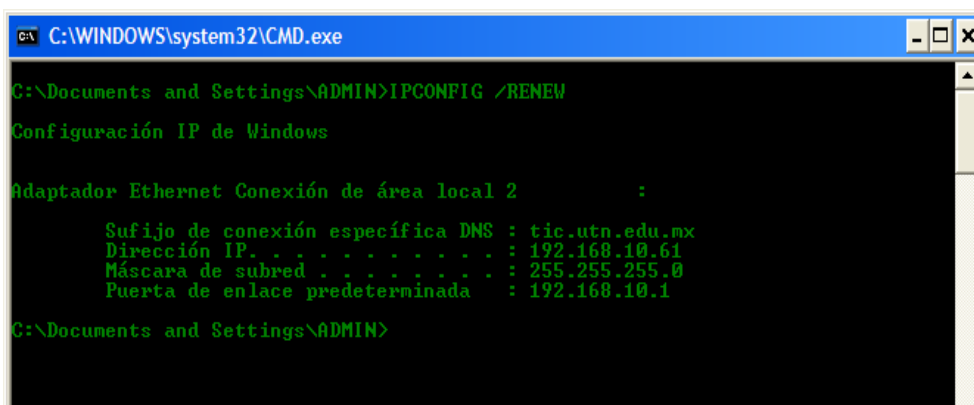
3.- Después en el símbolo del sistema se ingresa el comando: **ipconfig/release** para que libere la dirección IP que tenga asignada y nos de la dirección IP 0.0.0.0 como de muestra:

```
C:\WINDOWS\system32\CMD.exe
C:\Documents and Settings\ADMIN>IPCONFIG /RELEASE
Configuración IP de Windows

Adaptador Ethernet Conexión de área local 2      :
Sufijo de conexión específica DNS :
Dirección IP. . . . . : 0.0.0.0
Máscara de subred . . . . . : 0.0.0.0
Puerta de enlace predeterminada :
C:\Documents and Settings\ADMIN>
```

Figura 40.- Liberación de la IP del cliente DHCP

4.- Para solicitar una nueva dirección IP se hace a través del comando: **ipconfig/renew**, lo cual solicita al servidor DHCP una dirección IP disponible que le proporcionara el servidor DHCP de manera automática en este caso le dio la primer dirección IP disponible (192.168.10.61).



```
C:\WINDOWS\system32\CMD.exe
C:\Documents and Settings\ADMIN>IPCONFIG /RENEW

Configuración IP de Windows

Adaptador Ethernet Conexión de área local 2      :
    Sufijo de conexión específica DNS : tic.utn.edu.mx
    Dirección IP. . . . . : 192.168.10.61
    Máscara de subred : . . . . . : 255.255.255.0
    Puerta de enlace predeterminada : 192.168.10.1

C:\Documents and Settings\ADMIN>
```

Figura 41.- Renovación de la IP del cliente DHCP

NOTA: Dicho procedimiento sólo se puede realizar de forma local y con una cuenta de administrador, ya que un usuario restringido no tiene derechos de poder cambiar la dirección IP que fue asignada desde el Servidor.

Por lo cual los comandos mencionados anteriormente son usados para el soporte técnico que se le proporciona a un usuario en caso de no tener conexión de Red, o tener una conexión nula, en la cual le fue asignada una dirección APIPA (Automatic Private Internet Protocol Addressing - Direccionamiento Privado Automático del Protocolo de Internet), el cual es un protocolo que utilizan los sistemas que corren bajo Windows 98 o versiones posteriores para obtener la configuración de red cuando no encuentran un servidor DHCP.

Al no detectar la presencia de un servidor DHCP, el sistema por medio de APIPA se asigna una dirección IP privada, de clase B en el rango 169.254.0.1 a 169.254.255.254 con máscara 255.255.0.0. No obstante, cada cinco minutos el cliente buscará nuevamente un servidor DHCP. El procedimiento utilizado por APIPA sólo funciona con sistemas de IP v4, IP v6 utiliza otro procedimiento. Finalmente en el servidor es necesario actualizar el Scope para que nos muestre el nombre del host y dirección IP que le asigno de manera automática.

4.1.4 Administración del Servidor DHCP

Es importante mencionar que en este caso, se utilizó una dirección Clase C privada para el segmento 10, asignado al laboratorio de TIC, Área RyT, por lo cual la administración de dicho segmento se describe a continuación:

1.- Una vez actualizado el Scope podemos verificar que los hosts están conectados y tienen asignada una **dirección IP**, de forma **dinámica o reservada** de acuerdo al rango establecido.

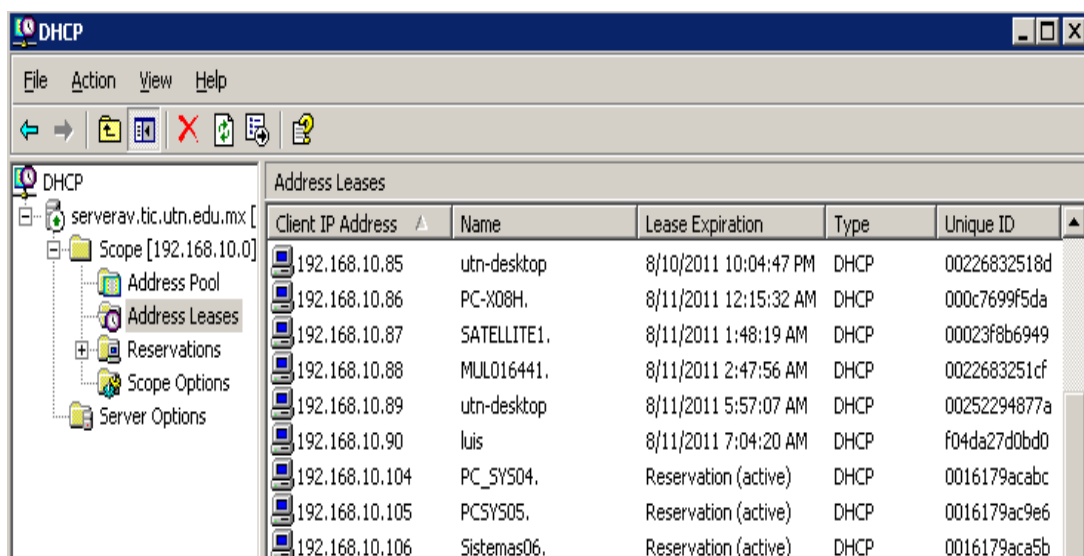


Figura 42.- Asignación de direcciones IP de los clientes DHCP

2.- En esta imagen se pueden apreciar los **rangos de exclusión** que se agregaron para cada laboratorio y sala de profesores, de acuerdo con la configuración inicial.

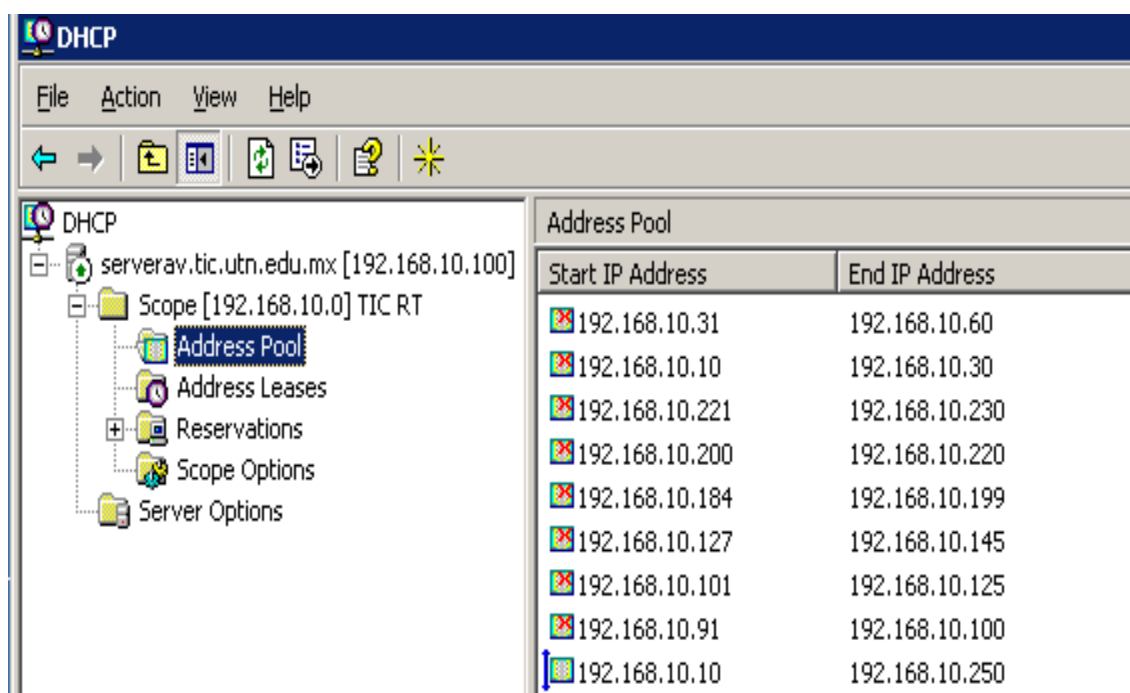


Figura 43.- Rangos de exclusión del servidor DHCP

NOTA: En el Anexo F se muestra una tabla de “*Distribución de direcciones IP*” del segmento de Red asignado a la división académica de TIC, Área RyT.

Por último, para la administración de las direcciones IP de cada laboratorio y debido a que es necesario que los alumnos puedan modificar dicha dirección IP para realizar algunas prácticas donde utilizan direcciones estáticas, se decidió realizar la **reservación** de las direcciones IP de cada equipo de acuerdo a su dirección física (*MAC Address*), de acuerdo al siguiente procedimiento:

3.- En la imagen siguiente se muestra la opción de “Reservations” donde se dan de alta dichas reservaciones, las cuales siempre tendrán asignada la misma dirección IP.

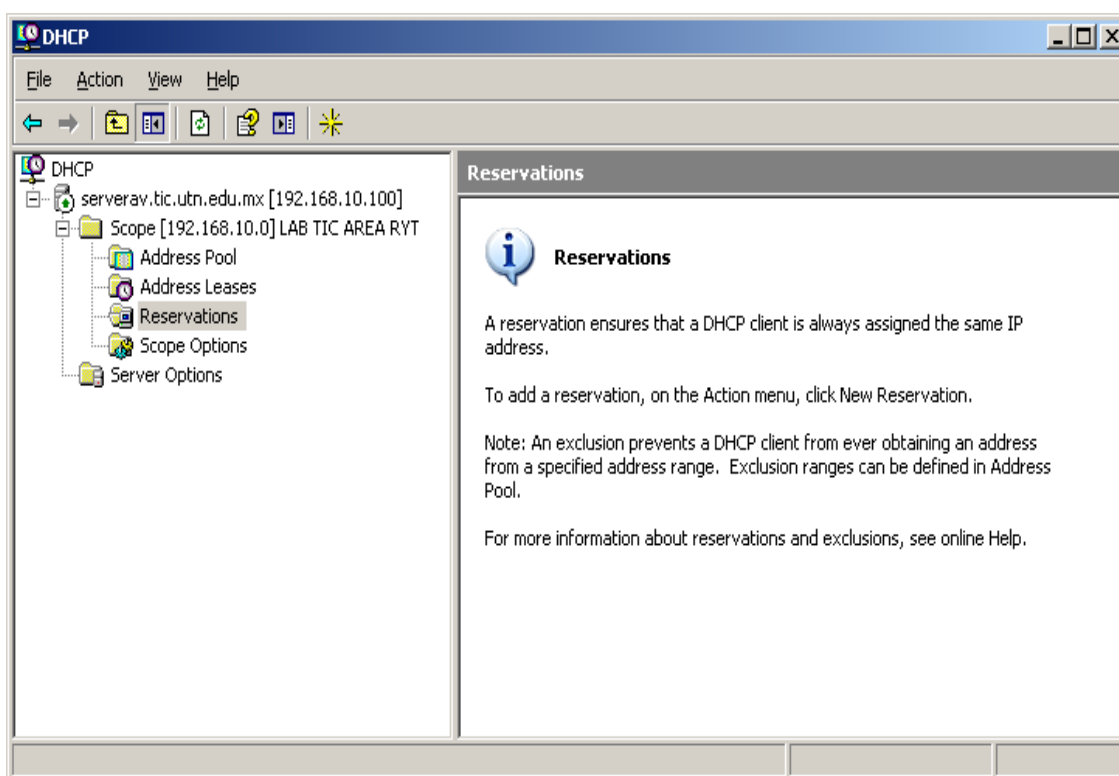


Figura 44.- Reservación de direcciones IP del servidor DHCP

4.- En la imagen siguiente se muestra el procedimiento para realizar una “New Reservations” donde se asigna la dirección que siempre tendrá asignado el equipo de acuerdo a su dirección MAC address y de acuerdo al tipo de protocolo (DHCP o BOOTP).

New Reservation

Provide information for a reserved client.

Reservation name: PCX01A

IP address: 192 . 168 . 10 . 131

MAC address: 00-16-E6-38-2E-41

Description: LAB REDES EQ01

Supported types

Both

DHCP only

BOOTP only

Add Close

Figura 45.- Creación de una reservación de IP

NOTA: Cabe mencionar que dicho procedimiento se realizó para cada uno de los equipos de cada uno de los laboratorios de cómputo.

5.- En la siguiente imagen se puede apreciar la consola del servidor DHCP, y como aparecen las reservaciones, para lo cual se necesitó un inventario de los laboratorios, donde se tiene el registro de las características técnicas de cada uno de los equipos de cómputo.

En el Anexo G, se muestra el *“inventario del laboratorio de Redes”*. Del cual se tomaron los valores de las direcciones MAC Address de cada equipo de cómputo.

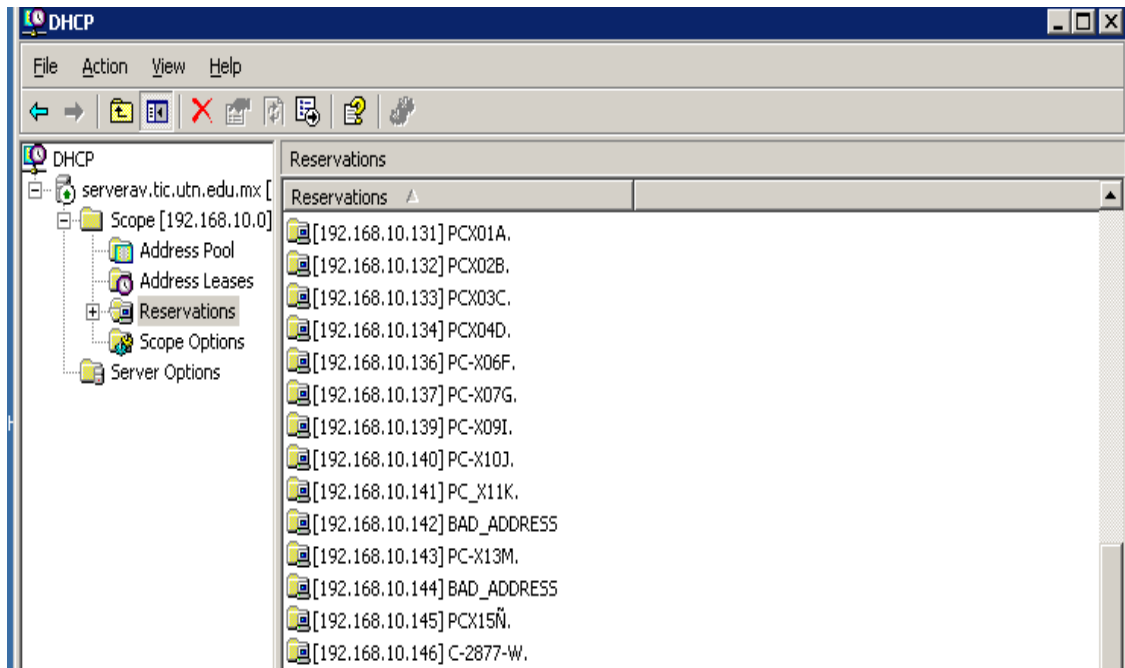


Figura 46.- Reservaciones IP de cliente DHCP

4.- Por último, en la siguiente imagen se muestran las direcciones IP que fueron reservadas para cada uno de los equipos y su estado (si están activas o inactivas), además de las direcciones que están asignadas de forma automática, el nombre del equipo en red y sobre todo, también se puede apreciar su dirección **MAC Address** en la columna de *Unique ID*.

A través de dicha consola también se puede apreciar si alguien quiere ocupar de forma estática una dirección IP que sea prestada por el servidor DHCP, la cual aparecerá en la columna *Name* como **BAD_ADDRESS**, lo cual indica que dicha dirección ya había sido asignada.

Address Leases					
Client IP Address ▾	Name	Lease Expiration	Type	Unique ID	Description
192.168.10.164	Elias-PC.tic.utn.edu.mx	10/22/2012 10:10:37 PM	DHCP	1c4bd6d2df10	
192.168.10.163		10/22/2012 11:22:57 PM	DHCP	fcc73481f0b7	
192.168.10.162	DJ-ROKE.tic.utn.edu.mx	10/22/2012 11:05:00 PM	DHCP	8c7b9d1c7316	
192.168.10.161	android_d29318665dac71c.tic.utn.edu.mx	10/22/2012 9:15:19 PM	DHCP	9471ac3d784b	
192.168.10.132	JESTEY,	Reservation (active)	DHCP	0016179af3ca	LAB REDES
192.168.10.131	PCX01A	Reservation (inactive)	None	0016e6382e41	LAB REDES EQ01
192.168.10.90	BAD_ADDRESS	10/22/2012 12:15:09 PM	DHCP	5a0aa8c0	This address is already in use
192.168.10.89	marla-desktop.tic.utn.edu.mx	10/22/2012 9:14:28 PM	DHCP	e06995d09a30	
192.168.10.88	android_9774d56d682e549c.tic.utn.edu.mx	10/22/2012 9:39:51 PM	DHCP	404d8e65b6f9	
192.168.10.87	luengas-desktop.tic.utn.edu.mx	10/22/2012 9:13:36 PM	DHCP	e06995e39f0d	
192.168.10.86	ania-desktop.tic.utn.edu.mx	10/22/2012 9:12:22 PM	DHCP	e06995d0c94f	
192.168.10.85	karliiux-desktop.tic.utn.edu.mx	10/22/2012 9:12:17 PM	DHCP	e06995e3a2b4	

Figura 47.- Liberación de la IP del cliente DHCP

Cabe señalar que dicho Servidor DHCP se implementó con una versión de **Windows 2003 Server Standar Edition**. Esto debido principalmente a los requerimientos de hardware, ya que la implementación del sistema operativo **Windows 2008 Server Standar Edition** son muy superiores con respecto a la versión anterior con respecto a procesamiento y memoria RAM principalmente.

Por otra parte el servidor se encuentra trabajando como un servidor independiente (stand alone), es decir que no se cuenta con un Dominio interno (local), por lo cual no fue necesario implementar el servicio de directorio “Active Directory” para la administración centralizada de los usuarios.

Sin embargo se propone en una etapa posterior la administración centralizada de todos los equipos de cómputo de los laboratorios, a través de herramientas de control como **NetOp School** el cual es un paquete de software muy eficaz que conecta nuestro equipo con los equipos de la audiencia para crear un aula interactiva en la red. Además ofrece una serie de eficaces herramientas de enseñanza como por ejemplo mostrar la pantalla a toda la clase, supervisar las pantallas del aula, bloquear el teclado y mouse de forma remota y otras herramientas que ayudarían a supervisar la clase y mantenerse en contacto con los alumnos de una forma más interactiva.

CONCLUSIONES

El control y la administración de una red nos permiten proveer información disponible del desempeño de esta en todos sus elementos (hardware y software), para asegurar que la capacidad y prestaciones de la red correspondan con las necesidades de los usuarios.

Se deben definir claramente los parámetros de funcionamiento o desempeño alrededor de los cuáles, se van a organizar las tareas de Administración de prestaciones como las siguientes:

- Obtención de la información de funcionamiento de la red a través del monitoreo sobre los recursos disponibles.
- Análisis de la información recolectada para determinar los niveles normales de utilización de la red.
- Comparación entre los valores obtenidos y los normales, para generar acciones de inicio de alarmas que pueden generar la toma de medidas preventivas o correctivas.

Por lo tanto, la administración de las fallas tiene como objetivos la detección, el aislamiento, la corrección, el registro y la notificación de los problemas existentes en la red, a través de un monitoreo periódico en busca de mensajes de error y establecimiento de alarmas.

La diferencia entre falla y error está en que un error es un evento aislado como la pérdida de un paquete o que éste no llegue correctamente, pero una falla es un funcionamiento anormal que requiere una intervención para ser corregido. La falla se manifiesta por un funcionamiento incorrecto o por exceso de errores.

Las acciones o procedimientos para esta corrección son:

- Determinar exactamente dónde está la falla.
- Aislar el resto de la red, para que pueda seguir operando sin interferencia.
- Reconfigurar la red para minimizar el impacto de operar sin el componente averiado.

Control y Administración del laboratorio de TIC, Área RyT

- Reparar o reemplazar el componente averiado para devolver la red al estado inicial.
- Si es posible, ejecutar un proceso de corrección automática y lograr el funcionamiento óptimo de la red.
- Registrar la detección y la resolución de fallas.
- Hacer seguimiento de la reparación de fallas.

Una buena política de Administración, es la prevención, es decir, debe adelantarse a los posibles problemas y resolverlos antes de que se produzcan.

Glosario

EIA (Electronics Industry Association.- Asociación de Industrias Electrónicas). Es una organización comercial compuesta como una alianza de asociaciones de comercio para los fabricantes de electrónica en los Estados Unidos. Estas asociaciones, a su vez rigen los sectores de la actividad de las normas de la EIA.

ETHERNET. Norma o estándar (IEEE 802.3) que determina la forma en que los puestos de la red envían y reciben datos sobre el medio físico. Ethernet utiliza un medio de difusión de bus y se basa en el método de acceso conocido como CSMA/CD para regular el tráfico en la línea de comunicación principal.

IEEE (Institute of Electrical and Electronics Engineers). Asociación de profesionales norteamericanos que aporta criterios de estandarización de dispositivos eléctricos y electrónicos.

JACK. Tipo de conexión que utilizan muchos cables, por ejemplo los de algunos dispositivos de sonido.

LAN (Local Area Network). Red de área local. El término LAN define la conexión física y lógica de ordenadores en un entorno generalmente de oficina. Su objetivo es compartir recursos.

NIC O TARJETA DE RED. Permite el acceso de una computadora a una red. Cada adaptador posee una dirección MAC que la identifica en la red y es única.

PROTOCOLO. Conjunto de normas y/o procedimientos para la transmisión de datos que ha de ser observado por los dos extremos de un proceso comunicación al (emisor y receptor).

TCP/IP (Transmisión Control Protocol/Internet Protocol). Se trata de un estándar de comunicaciones muy extendido y de uso muy frecuente para software de red basado en Unix con protocolos Token-Ring y Ethernet.

Bibliografía

1. Franklin, F. E. B. (2009). *Organización de Empresas*. 3era Edición México: McGraw Hill
2. Atelin, J. D. P. (2007). *TCP/IP y protocolos de Internet*. Barcelona: Ediciones Eni.
3. Huidobro M., José Manuel; Millan T., Ramón Jesús, (2007), *Redes de Datos y Convergencia IP*. México: Alfaomega grupo Editor.
4. Lorenz J., Reid A., Cisco Press (2008). *Guía portátil Cisco CCNA Discovery: Networking para el hogar y pequeñas empresas, Versión 4.1*, México: Cisco Press.
5. Olifer N., (2009) *Redes de computadoras 1ª Edición* México: McGraw Hill.
6. Tanenbaum, A. S., (2006), *Redes de computadoras*. México: Pearson Educación.

Cibergrafía

1. *Acerca de la UTN, La UTN: Misión y Visión*. Disponible desde Internet en: <http://www.utn.edu.mx/universidades/htm/acerca/mision-vision.htm>. con acceso el 10 de diciembre de 2012.
2. López, E. Mayo 2011, *Bloqueo de ejecutables en Windows XP*. Disponible desde Internet en: www.whitesec.com.mx. Con acceso el día 15 de diciembre de 2012.
3. Quiroga, E. 30 de septiembre de 2005, *Como proteger nuestro pc*. Disponible desde Internet en:

<http://recursostic.educacion.es/observatorio/web/ca/equipamiento-tecnologico/seguridad-y-mantenimiento/281> Con acceso el día 5 de noviembre de 2012
4. Febrero de 2013, *Guía equipos limpios de virus y espías*. Disponible desde Internet en: <http://www.brindys.com/sinvirus/> Con acceso el día 15 de noviembre de 2012.

ANEXO A.- Formato de Horario de Clases del laboratorio



Universidad Tecnológica De Nezahualcóyotl
 Organismo Público y Descentralizado del Estado de México
 División de TIC, Área Redes y Telecomunicaciones



HORARIO DE CLASES DEL LABORATORIO DE _____ PERIODO: _____ TURNO: _____

	LUNES	MARTES	MIÉRCOLES	JUEVES	VIERNES
7:00-8:00					
8:00-9:00					
9:00-10:00					
10:00-11:00					
11:00-12:00					
12:00-13:00					
13:00-14:00					

ANEXO B.- Formato de Control de Practicas del laboratorio



Universidad Tecnológica De Nezahualcóyotl
Organismo Público y Descentralizado del Estado de México
División de TIC, Área Redes y Telecomunicaciones





CONTROL DE PRÁCTICAS DEL LABORATORIO DE _____

FECHA	No. DE ALUMNOS	NOMBRE DE LA ASIGNATURA	NÚMERO Y NOMBRE DE LA PRACTICA	FIRMA DEL PROFESOR	GRUPO	HORA DE ENTRADA	HORA DE SALIDA

OBSERVACIONES _____

ANEXO E.- Formato de Orden de Servicio

	<p>UNIVERSIDAD TECNÓLOGICA DE NEZAHUALCOYTL</p> <p>LABORATORIOS DE TIC ÁREA RYT</p> <p>ORDEN DE SERVICIO No. _____</p>	 <p>DIVISION DE TELEMATICA</p>	
NO. INVENTARIO	MARCA	MODELO	NO. SERIE
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
FECHA DE INICIO	TRAMITE	PERSONA QUE SOLICITA EL SERVICIO	
<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	
FECHA DE TERMINO	GARANTIA	PROBLEMAS DE SOFTWARE	SI <input type="checkbox"/>
<input type="text"/>	<input type="checkbox"/>	REPARACIÓN	NO <input type="checkbox"/>
DIAGNÓSTICO	<input type="text"/>		
COMPONENTES DAÑADOS	<input type="text"/>		
SOLUCIÓN	<input type="text"/>		
DIAGNÓSTICO FINAL	<input type="text"/>		
_____ ENCARGADO DEL SERVICIO FIRMA	_____ CONFORMIDAD DEL SERVICIO FIRMA		

ANEXO F.- Tabla de direccionamiento IP

Asignación de las direcciones IP del segmento de **Red 192.168.10.0/24** en la División de TIC, Área RyT así como en los laboratorios de Telemática.

Laboratorio/Área	Rango de Direcciones IP	Observaciones
Área de Docentes	192.168.10.11 - .12	Impresoras de Red HP Laser Jet 2420
Área de Administrativos	192.168.10.13 - .30	Asignadas de acuerdo a su Roseta
Área de Docentes	192.168.10.31 - .60	Asignadas de acuerdo a su Roseta
Rango Libre	192.168.10.61 - .90	Asignadas por el Servidor DHCP
Laboratorio de Telemática	192.168.10.91 - .100	Docentes del Laboratorio y Sala de maestros
Laboratorio de Sistemas	192.168.10.101 - .130	Solo hay 24 Equipos en Red Total de equipos: 30
Laboratorio de Redes	192.168.10.131 - .160	Solo hay 26 Equipos en Red Total de equipos: 30
Laboratorio de Informática	192.168.10.161 - .190	Solo hay 20 Equipos en Red Total de equipos: 30
Laboratorio de Linux	192.168.10.191 - .205	Solo hay 10 Equipos en Red Total de equipos: 15
Laboratorio de Windows2k	192.168.10.206 - .220	Solo hay 10 Equipos en Red Total de equipos: 15
Laboratorio del PIFI	192.168.10.221 - .230	Todos los Equipos están en Red. Total de equipos: 10
Rango Libre	192.168.10.231 - .250	Asignadas por el Servidor DHCP
Rango Reservado	192.168.10.1 - .10 192.168.10.251 - .254	Reservadas por el Departamento de Informática y Estadística

ANEXO G Inventario técnico para un laboratorio



Universidad Tecnológica De Nezahualcóyotl
Organismo Público y Descentralizado del Estado de México
División de TIC, Área Redes y Telecomunicaciones

INVENTARIO TÉCNICO DEL LABORATORIO DE REDES

No.	MARCA	MODELO	PROCESADOR	VELOCIDAD	MEMORIA RAM	DISCO DURO	DIRECCION MAC	DIRECCION IP	NOMBRE DEL HOST	INVENTARIO MONITOR/ CPU
1	LANIX	BRAIN	CELERON	2.6 GHz	256 MB	40 GB	000C7699F54C	192.168.10.131	PCX01A	C-2864-W
2	LANIX	BRAIN	CELERON	2.6 GHz	256 MB	40 GB	000C7699F525	192.168.10.132	PCX02B	C-2886-W
3	LANIX	BRAIN	CELERON	2.6 GHz	256 MB	40 GB	000C7699F5EC	192.168.10.133	PCX03C	C-2874-W
4	LANIX	BRAIN	CELERON	2.6 GHz	256 MB	40 GB	000C765113C5	192.168.10.134	PCX04D	C-2882-W
5	LANIX	BRAIN	CELERON	2.6 GHz	256 MB	40 GB	000C7699F5D3	192.168.10.135	PCX05E	C-2872-W
6	LANIX	BRAIN	CELERON	2.6 GHz	256 MB	40 GB	000C7699F534	192.168.10.136	PCX06F	C-2879-W
7	LANIX	BRAIN	CELERON	2.6 GHz	256 MB	40 GB	0010DC6078D4	192.168.10.137	PCX07G	C-2868-W
8	LANIX	BRAIN	CELERON	2.6 GHz	256 MB	40 GB	000C7699F5DA	192.168.10.138	PCX08H	C-2881-W
9	LANIX	BRAIN	CELERON	2.6 GHz	256 MB	40 GB	000C7699F6BA	192.168.10.139	PCX09I	C-2870-W
10	LANIX	BRAIN	CELERON	2.6 GHz	256 MB	40 GB	000C7699F535	192.168.10.140	PCX10J	C-2885-W
11	LANIX	BRAIN	CELERON	2.6 GHz	256 MB	40 GB	000C7699F793	192.168.10.141	PCX11K	C-2884-W
12	LANIX	BRAIN	CELERON	2.6 GHz	256 MB	40 GB	000C7699F4D9	192.168.10.142	PCX12L	C-2865-W
13	LANIX	BRAIN	CELERON	2.6 GHz	256 MB	40 GB	000C7699F6CF	192.168.10.143	PCX13M	C-2867-W
14	LANIX	BRAIN	CELERON	2.6 GHz	256 MB	40 GB	000C766B9770	192.168.10.144	PCX14N	C-2887-W
15	LANIX	BRAIN	CELERON	2.6 GHz	256 MB	40 GB	0013D3BB92A	192.168.10.145	PCX15O	C-2890-W
16	LANIX	BRAIN	CELERON	2.6 GHz	256 MB	40 GB	000C76510EA4	192.168.10.146	PCX16P	C-2877-W
17	LANIX	BRAIN	CELERON	2.6 GHz	256 MB	40 GB	000C7699F43D	192.168.10.147	PCX17Q	C-2878-W
18	LANIX	BRAIN	CELERON	2.6 GHz	256 MB	40 GB	000C7699F48E	192.168.10.148	PCX18R	C-2863-W

