DISEÑO DE POLÍTICAS DE SEGURIDAD PARA LA RED DE LA CUTB.

JAIRITH CARRILLO MANCERA

JAIRO TOVIO BUELVAS

CORPORACION UNIVERSITARIA TECNOLOGICA DE BOLIVAR

FACULTAD DE INGENIERIA DE SISTEMAS

CARTAGENA DE INDIAS D. T. Y C.

2002

DISEÑO DE POLÍTICAS DE SEGURIDAD PARA LA RED DE LA CUTB.

JAIRITH CARRILLO MANCERA

JAIRO TOVIO BUELVAS

Trabajo de grado para optar el título de Ingeniero de Sistemas

Director:

JUAN CARLOS MANTILLA
ING. DE SISTEMAS

CARTAGENA DE INDIAS D.T Y C.

CORPORACION UNIVERSITARIA TECNOLOGICA DE BOLIVAR

FACULTAD DE INGENIERIA DE SISTEMAS

2002

Cartagena, Mayo 20 del 2002

Señores:

COMITÉ DE PROYECTOS DE GRADO

Corporación Universitaria Tecnológica de Bolívar

Escuela de Ingenierías

La Ciudad

Estimados Señores:

Por medio de la presente nos permitimos hacer entrega formal del proyecto de grado titulado: ***DISEÑO DE POLÍTICAS DE SEGURIDAD PARA LA RED DE LA CUTB***, el cual sometemos a su consideración y aprobación.

Esperando su apoyo y colaboración.

Cordialmente,

_____	_____
JAIRITH CARRILLO MANCERA	***JAIRO TOVIO BUELVAS***
COD. 0105353	***COD. 0105352***

Cartagena, Mayo 20 del 2002

Señores:

COMITÉ DE PROYECTOS DE GRADO

Corporación Universitaria Tecnológica de Bolívar

Escuela de Ingenierías

La Ciudad

Respetados señores:

La presente tiene como objeto presentar el proyecto de tesis de grado titulado: ***DISEÑO DE POLÍTICAS DE SEGURIDAD PARA LA RED DE LA CUTB*****,** el cual realizaron los estudiantes ***JAIRITH CARRILLO MANCERA*** *y* ***JAIRO TOVIO BUELVAS***, como requisito necesario para obtener el titulo de Ingeniero de Sistemas.

Cordialmente,

_____

JUAN CARLOS MANTILLA
Ingeniero de Sistemas
Director

Cartagena de Indias D. T. Y C., Octubre 16 de 2001

Ingeniero
GONZALO GARZÓN
Decano de la Facultad de Ingeniería de Sistemas.
Corporación Universitaria Tecnológica de Bolívar.

Respetado Ingeniero:

Por medio de la presente nos permitimos hacer entrega formal del trabajo de grado titulado "***DISEÑO DE POLÍTICAS DE SEGURIDAD PARA LA RED DE LA CUTB"*****,** como requisito parcial para optar al título de Ingeniero de Sistemas.

Atentamente,

_____	_____
JAIRITH CARRILLO MANCERA	***JAIRO TOVIO BUELVAS***
COD. 0105353	***COD. 0105352***

NOTA DE ACEPTACIÓN:

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

_____

Jurado

Cartagena, 20 de Mayo de 2002

DEDICATORIA

Dedico la culminación de este logro

A mi madre Florinda Mancera Camelo que esperó pacientemente la culminación de mi carrera y nunca perdió la fe en mi, mi padre Juan carrillo Beltrán por aconsejarme de seguir progresando cada día más.

A Angélica María Correa Yanes por su apoyo incondicional para la culminación de este objetivo.

A Juan Martínez. (Juancho), gracias a tu amistad y por haberme apoyado en esto, sin interés, solo con la consigna de verme realizado profesionalmente.

A Juan Carlos Mantilla por haberme brindado toda su colaboración y confiado en mi cuando más lo necesité.

Gracias,

Jairith Alberto Carrillo Mancera

Ante todo a Dios....

A mis padres, Reina Buelvas Rojas y Jairo Tovio Naizzir por brindarme todo su apoyo incondicional para culminar mis estudios y regalarme lo más hermoso que unos padres pueden brindarle a sus hijos, la educación.

A mi abuela Carolina Naizzir Villamizar, por el apoyo brindado durante la realización de mi carrera.

Y a todos mis amigos que me colaboraron en el desarrollo de este proyecto.

Gracias,

Jairo Tovio Buelvas

AGRADECIMIENTOS

Los autores expresan su agradecimiento a:

Mantilla, Juan Carlos, Ingeniero de Sistemas, por su valiosa colaboración en el desarrollo de nuestro trabajo, a él muchas gracias.

Martínez, Juan, Ingeniero de Sistemas, profesor de la C.U.T.B. por su amistad y colaboración en el desarrollo del trabajo.

Garzón, Gonzalo, Ingeniero de Sistemas, Decano de la facultad de Ingeniería de Sistema, por su amistad y apoyo.

Vásquez, Giovanni, Ingeniero de Sistemas, profesor de la C.U.T.B. y jefe del Departamento de JESIN, por asesoría en el desarrollo de nuestro trabajo.

C.U.T.B., por su apoyo para el desarrollo de nuestra entrevista, sin ellos no hubiéramos podido terminar nuestro trabajo y por la amabilidad que nos expresaron durante todo el año 2001 que estuvimos con ustedes.

ARTÍCULO 105

La Corporación Universitaria Tecnológica de Bolívar se reserva el derecho de propiedad intelectual de todos los trabajos de grado aprobados y no pueden ser explotados comercialmente sin su autorización.

CONTENIDO

LISTA DE FIGURAS

LISTA DE ANEXOS

MARCO TEÓRICO

BASE TEORICA

- **Políticas de Seguridad**.

Las políticas de seguridad son un conjunto de normas y reglas escritas y difundidas, definidas junto al comité de seguridad, que rigen el uso de los recursos presentes en la red por los usuarios internos y externos. Las políticas de seguridad son la base de un sistema de seguridad efectivo, por lo que es importante contar con un comité de seguridad que considere personal de diferentes áreas.

En general las políticas de seguridad deberán contemplar los recursos, usuarios, vulnerabilidad, pautas de uso aceptable, derechos y responsabilidades de usuarios y administradores, y por supuesto, procedimientos que permitan mantener y controlar el cumplimiento de las políticas.

- **Seguridad en Redes**

La seguridad en los sistemas de información y de cómputo se ha convertido en uno de los problemas más grandes desde la aparición, y más aun, desde la globalización de Internet. Dada la potencialidad de esta herramienta y de sus

innumerables aplicaciones, cada vez mas personas y más empresas sienten la necesidad de conectarse a este mundo.

A raíz de lo anterior, los administradores de red han tenido la necesidad de crear políticas de seguridad a través de las cuales se garantice el mayor nivel de seguridad en las conexiones, en el envío y recepción de información encriptada, el control de los accesos e información, la confiabilidad de la información y demás características de la seguridad de una red.

No obstante lo anterior, el interés y la demanda por Internet crece cada día y el uso de servicios como World Wide Web (WWW), Internet Mail, Telnet y el File Transfer Protocol (FTP) es cada vez más popular, trayendo consigo la necesidad de aplicar controles más rigurosos.

- **Servicios de Seguridad en la Red**

Para poder hacer frente a este tema de seguridad, se definen una serie de servicios para proteger los sistemas de proceso de datos y de transferencia de la información.

Confidencialidad. Requiere que la información sea accesible únicamente por las personas o entidades autorizadas. La confidencialidad de los datos se

aplica a todos los datos intercambiados por las entidades autorizadas o solo a una porción o segmentos seleccionados de los datos.

Autenticación. Requiere una identificación correcta del origen del mensaje, asegurando que la entidad no sea falsa. De esto se encarga las Firmas Digitales.

Integridad. La información solo puede ser modificada por las entidades autorizadas, esta modificación incluye escritura, borrado, creación y demás. Esta integridad puede ser de datos o secuencia, la integridad de los datos asegura que los datos recibidos no han sido modificados

No Rechazo. Protección a un usuario frente a otro usuario para que posteriormente este no niegue la realización de la comunicación. Existen dos tipos, el no rechazo de origen, por el cual se protege al receptor de que el emisor niegue haber enviado un mensaje y el no rechazo de recepción, que protege al emisor de que el receptor niegue haber recibido el mensaje. Las firmas digitales constituyen el mecanismo más empleado para este fin.

Control de Acceso

Requiere que el acceso a los recursos (información, capacidad de cálculo, nodos de comunicaciones, entidades físicas, etc.) sea controlado y limitado por

el sistema destino, mediante el uso de contraseñas o llaves hardware, protegiéndolos frente a usos no autorizados o manipulación.

Disponibilidad. Requiere que los recursos del sistema informático estén disponibles a las entidades autorizadas cuando los necesiten.

- **Firmas digitales**

Las firmas digitales son bloques de datos que han sido codificados con una llave secreta y que se pueden decodificar con una llave publica, son utilizados principalmente para verificar la autenticidad del mensaje o la de una llave publica.

- **Posibles Riesgos**

Es indispensable tener en cuenta que, independientemente de si la red está conectada o no al internet, es probable que alguien quiera eventualmente intentar violar sus privilegios de usuario o simplemente atacar la red en alguna forma, sin importar lo interesante de la información o el poco valor que pueda tener. Simplemente un usuario mal intencionado puede intentar atacarla.

En consecuencia, si es posible asegurar al máximo las protecciones contra los ataques, entonces el administrador solo tendrá que preocuparse de que el

tráfico entrante y saliente esté debidamente controlado y sea compatible con las políticas y criterios de utilización que tiene la organización, en este caso la Tecnológica de Bolívar. De nada servirá tener un Firewall perfectamente configurado si los usuarios hacen lo que quieren entre ellos.

- **Firewalls**

¿Qué es un firewall ? Un firewall es un sistema o un grupo de sistemas que decide que servicios pueden ser accesados desde el exterior (Internet, en este caso) de un red privada, por quienes pueden ser ejecutados estos servicios y también que servicios pueden accesar los usuarios de la intranet hacia el exterior (Internet). Para realizar esta tarea todo el trafico entre las dos redes tiene que pasar a través de él.

El firewall solo dejará pasar el trafico autorizado desde y hacia el exterior. En concreto, el firewall solamente filtra información.

Desde el punto de vista de política de seguridad, el firewall delimita el perímetro de defensa y seguridad de la organización. El diseño de un firewall, tiene que ser el producto de una organización consciente de los servicios que se necesitan, además hay que tener presentes los puntos vulnerables de toda red, los servicios que dispone como públicos al exterior de ella (WWW, FTP, telnet, entre otros) y conexiones por módem.

Finalmente, los firewalls también son usados para albergar los servicios WWW y FTP de la intranet, pues estos servicios se caracterizan por tener interfaces al exterior de la red privada y se ha demostrado que son puntos vulnerables en varios sentidos.

Limitaciones del firewall. La limitación mas grande que tiene un firewall sencillamente es el hueco que no se tapa y que coincidencialmente, es descubierto por un Hacker. Los firewalls no son sistemas inteligentes sino que actúan de acuerdo a parámetros introducidos por su diseñador, y de acuerdo con la configuración que su administrador establezca.

Otra limitación es que el firewall "no es contra humanos", es decir que si un Hacker logra entrar a la organización y descubrir passwords o se entera de los huecos del firewall y difunde la información, el firewall no podrá detectarlo, pues no posee ningún nivel de inteligencia.

Es claro que el firewall tampoco provee de herramientas contra la filtración de software o archivos infectados con virus, dado ellos pueden ingresar a la red como parte del trafico autorizado. En consecuencia, es indispensable definir y aplicar controles al contenido de la información, adicionales al filtrado establecido por el firewall.

GLOSARIO

AUDITORIA : Inspección y examen independiente de los registros del sistema y actividades para aprobar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y procedimientos operativos, y para recomendar cualquier cambio que se estime necesario.

ADMINISTRACIÓN DE LA RED: Es la entidad encargada de desarrollar el plan estratégico de colectividad del centro que favorezca la prestación de servicios eficientes y de utilidad en la transición de datos, voz y vídeo para apoyar efectivamente los requerimientos del usuario.

CORREO ELECTRÓNICO: Servicio de transporte de mensajes electrónicos, a través de una red o por el Internet, con arreglo a algún protocolo de comunicaciones bien conocido. El correo electrónico puede existir en una red de cualquier tamaño. Después del Web, posiblemente el correo electrónico sea el servicio de mayor uso en el Internet.

CUENTAS DE USUARIO: Es el ambiente en el cual un usuario obtiene acceso al sistema. Generalmente contiene un login (nombre de usuario) y password (contraseña).

CRACKER: Delincuente informático con amplio conocimiento sobre sistemas de computo.

***CONTROL DE ACCESO*:** Requiere que el acceso a los recursos (información, capacidad de cálculo, nodos de comunicaciones, entidades físicas, etc.) sea controlado y limitado por el sistema destino, mediante el uso de contraseñas o llaves hardware, protegiéndolos frente a usos no autorizados o manipulación.

DATABASE SCANNER: Los datos más críticos y sensitivos de una organización residen en bases de datos relacionales, que muchas veces están desprotegidas y son vulnerables a intrusos. Esta información con frecuencia está disponible para cualquiera, por lo que se corre el riesgo de que sea robada o saboteada, debido a claves débiles o inexistentes, malas configuraciones o "puertas traseras" (*backdoors*) de los sistemas. Este software provee una auditoria completa de la autorización, autenticación, integridad del sistema y compatibilidad con el Año 2000, desde una base de datos relacional.

DIRECCIÓN IP: Identificador único de 32 bits para una computadora principal TCP/IP en una red.

FILE TRANSFER PROTOCOL FTP): FTP es un servicio heredado del Internet, pero todavía es ampliamente utilizado para hacer algunos tipos de información

disponibles. Básicamente FTP es un protocolo de Internet usado para transferir información y/o documentos de una computadora a otra.

***FIRMA DIGITAL**:* Las firmas digitales son bloques de datos que han sido codificados con una llave secreta y que se pueden decodificar con una llave publica, son utilizados principalmente para verificar la autenticidad del mensaje o la de una llave publica.

FIREWALL: Un firewall es un sistema o un grupo de sistemas que decide que servicios pueden ser accesados desde el exterior (Internet, en este caso) de una red privada, por quienes pueden ser ejecutados estos servicios y también que servicios pueden accesar los usuarios de la intranet hacia el exterior (Internet).

HACKER: Personas con amplios conocimientos de informática, cuya pasión es exclusivamente aprender más.

INTRANET: :Una intranet, es una red que utiliza tecnología de Internet aplicada a una red interna con la diferencia que el contenido sólo está disponible internamente, en la red de área local.

IP: INTERNET PROTOCOL, parte de la familia de protocolos TCP/IP, que describe el software que supervisa las direcciones del nodo de Internet, encamina mensajes salientes y reconoce los mensajes entrantes.

USUARIO: Usuario es cualquier persona que tenga algún nivel de autorización para ingresar a un sistema o para utilizar alguno de los recursos o servicios ofrecidos por ese sistema, mediante cualquier medio.

SERVIDOR: es un equipo de una red de área local que ejecuta software para controlar el acceso a toda la red, o a parte de ella, y sus recursos. Un equipo con capacidades de servidor puede poner los recursos a disposición de otros equipos de una red.

PC : es una máquina cuyo funcionamiento interno se basa en el uso de un microprocesador, y que a través de el se consigue una serie de prestaciones, que en potencia, manejabilidad, portabilidad y precio cubren la gama mas baja de necesidades en el mundo de la informática.

***POLÍTICAS DE SEGURIDAD**:* Las políticas de seguridad son un conjunto de normas y reglas escritas y difundidas, definidas junto al comité de seguridad, que rigen el uso de los recursos presentes en la red por los usuarios internos y externos.

PORTÁTIL : se trata de una computadora de características físicas especiales que permiten fácilmente su transporte de un sitio para otro si perder ninguna de las cualidades de una computadora personal.

SAFESUITE: Provee herramientas de monitoreo, ejecución de políticas, detección de intrusos y respuestas en tiempo real en el tráfico de la red, sitios web, firewalls y sistemas operativos UNIX y NT.

INTERNET SCANNER: Realiza evaluaciones automatizadas de seguridad de redes TCP/IP.

SYSTEM SCANNER: Identifica y prioriza la vulnerabilidad y las malas configuraciones a nivel del sistema operativo, permisos y pertenencia de archivos, servicios de red, configuración de cuentas y aspectos comunes de seguridad, tales como claves débiles de usuarios.

SECURITY MANAGER: En un ambiente cliente-servidor, verifica interactivamente las vulnerabilidades y malas configuraciones. Se puede calendarizar para que se ejecute en forma automática, generando alertas cuando aparezca un nuevo problema. Las verificaciones están definidas en una base de conocimiento (*knowledge base*) que reside en cada cliente.

***SAFESUITE DECISIONS*:** Es un sistema completo de seguridad adaptable, que integra datos críticos de otros sistemas (como los antes enumerados) para evitar que los administradores de la red tengan que recolectar y analizar datos, maximiza la seguridad de redes y de comercio electrónico basado en Internet y genera reportes que permiten establecer el estado de las condiciones cambiantes en los riesgos de las empresas.

UNIDADES ZIP : Una unidad ZIP, es una unidad de almacenamiento masivo, la cual permite guardar archivos grandes que se guardarían normalmente en 15 disquetes o más, en un solo disco sin comprimir. Otra característica importante de este dispositivo es la seguridad que éste brinda, ya que rara vez da problemas, por lo que no es necesario contar con los típicos disquetes de “por si acaso”. Una de las ventajas de copiar archivos directamente en la unidad Zip es que es posible acceder a ellos fácilmente y en cualquier momento que sea necesario, sin necesidad de realizar un procedimiento de restauración.

WORLD WIDE WEB: También llamado WWW o simplemente "el web", este servicio de Internet es el más ampliamente difundido. De hecho muchas personas piensan en el web e Internet como un sinónimo, y no se dan cuenta que "el web" es una entidad que corre en el Internet. La característica más importante de los documentos WWW es que están enlazados con otros documentos por medio de hipertexto. El hipertexto permite enlazar documentos con sólo hacer un click con el ratón.

WEB BROWSER: Un browser es un programa que provee una interfase para accesar y ver archivos en Internet. Antes de que existieran los browsers, se necesitaba saber una serie de complicados comandos para ver los recursos en el Internet. Los browsers básicamente hicieron el Internet más amigable y fácil de usar.

INTRODUCCIÓN

Durante las últimas dos décadas, y como consecuencia del inmenso desarrollo de las comunicaciones computacionales a través de redes, y de la masificación de los servicios de internet, la seguridad informática ha tomado gran importancia, dadas las cambiantes condiciones que hacen aparecer nuevas posibilidades y nuevos riesgos casi a diario, y también a la aparición de nuevas plataformas y filosofías de computación disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes para explorar más allá de las fronteras tradicionales, situación que ha abierto el mundo para los usuarios y ha permitido nuevas formas de trabajo, pero que también como es conocido ampliamente, ha llevado a la aparición de nuevas amenazas y riesgos para los usuarios de los sistemas computarizados.

En consecuencia, son muchas las organizaciones gubernamentales y no gubernamentales internacionales que han desarrollado documentos y directrices para orientar a la comunidad en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas y evitar su uso indebido, lo cual puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

En este sentido, las políticas de seguridad informática (PSI) han surgido desde hace algún tiempo como una herramienta organizacional indispensable para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la compañía desarrollarse y mantenerse en su sector de negocios y para establecer mecanismos de control y desarrollo tendientes a disminuir los riesgos potenciales en los rec ursos computacionales de las organizaciones.

Obviamente, la promulgación y adopción de una política de seguridad computacional al interior de una organización requiere en principio, de un alto compromiso en la organización, de un alto nivel de agudeza técnica para establecer fallas y debilidades, y de una constancia permanente para renovar y actualizar dicha política en función del ambiente dinámico que rodea las organizaciones modernas, y particularmente a los servicios, y recursos de carácter computacional.

La tecnología computacional le ha dado al hombre tiene la capacidad para abrir las puertas de un vasto mundo de recursos de información, así como de personas, permitiéndole a cualquier persona, como son los estudiantes o miembro de la comunidad universitaria el acceso a todos los recursos y servicios ,con el simple hecho de tener disponible una conexión a Internet.

En general, las oportunidades que se tienen con esta conectividad son casi ilimitadas, mas no así, los recursos computacionales y de conectividad disponibles. Además, la aparición de riesgos sobre los recursos

computacionales, que se originan tanto en vulnerabilidades de los mismo como en comportamientos inadecuados por parte de los usuarios requiere de las organizaciones un diseño de políticas de seguridad para el uso de la red, y de los recursos computacionales a fin de asegurar su uso correcto.

En este sentido, la TECNOLÓGICA DE BOLÍVAR cree firmemente en que el desarrollo de reglas que sean bien entendidas, que circulen ampliamente y que sean efectivamente implementadas, conllevará a hacer de la red y de los servicios de Internet un ambiente seguro y productivo para estudiantes, profesores y miembros en general de la comunidad universitaria.

Este documento contiene una propuesta de Políticas de seguridad para los recursos computacionales y de conectividad presentes en la red Universitaria. En ellas se establecen entre otras cosas, el comportamiento esperado de los miembros de la comunidad universitaria hacia diferentes servicios de información (e-mail, www, ftp, etc.) y las reglas en cuanto al uso adecuado de recursos físicos y lógicos, las cuales se han diseñado con el fin de definir un marco de referencia que le permita a la dirección, tomar decisiones basadas en claros criterios.

1. ANTECEDENTES

Este proyecto surge en respuesta a la preocupación por mantener los sistemas y la información de la red de la TECNOLÓGICA DE BOLÍVAR seguros contra cualquier forma de ataque. Se pretende no solo establecer una filosofía de seguridad, sino forjar una educación y un hábito en usuarios y administradores que conlleve a un ambiente mas seguro tanto en la comunidad de usuarios de la TECNOLÓGICA DE BOLÍVAR como en las transacciones de información desde y hacia al mundo entero.

Las políticas de seguridad para la red de la TECNOLÓGICA DE BOLÍVAR se han definido considerando dos premisas esenciales:

1. Se requieren políticas de seguridad como medida preventiva de la aparición de vulnerabilidades, riesgos, y ataques que si bien no han ocurrido en forma importante, se deben evitar hasta el mayor grado posible, dada su incidencia en la vida institucional

2. Se requieren políticas de seguridad como marco de referencia para la definición de soluciones a los problemas de seguridad en cómputo que han ocurrido en la red de la TECNOLÓGICA DE BOLÍVAR y de los que actualmente son motivo potencial de incidentes de seguridad.

Para definir las dos premisas anteriores, es indispensable estudiar a fondo la problemática enfrentada por los usuarios de la red y los servicios que sobre ella se ofrecen, con el objeto de formar una imagen clara de la situación de seguridad de los mismos. Los incisos que a continuación se presentan, describen de forma general los problemas y consideraciones que afectan directa o indirectamente la seguridad, de la información y de la infraestructura de recursos y servicios informáticos de la Tecnológica, y con base en los cuales se formulan las políticas.

1.1 ACCESO DEMASIADO LIBRE A LAS SALAS DE *CÓMPUTO*

1.1.1 De los Usuarios. *Actualmente la institución confía solamente en el buen ojo y memoria del personal de vigilancia, lo que obviamente no es suficiente para garantizar que entran solo las personas que deben entrar y que nadie extraerá, alterará o hará un uso indebido de los sistemas de cómputo y de sus recursos y servicios.*

Este problema origina el riesgo de que cualquier persona de cualquier departamento o aún personas externas a la institución pueda sustraer, dañar, hacer mal uso de los recursos de cómputo o utilizar las cuentas y los huecos de seguridad que eventualmente existan en ellas para comprometer los sistemas o información de los usuarios.

Por este motivo se han tenido en el pasado, incidentes de seguridad que se materializan justamente en la pérdida parcial de recursos de cómputo que si bien no han traído consecuencias directas como la destrucción, revelación e integridad de la información, si suponen un compromiso serio de la seguridad de la infraestructura, además del perjuicio a las actividades académicas.

Algunos otros problemas tienen que ver con la oportunidad de acceso de un eventual atacante o hacker a las salas de cómputo y con mayor razón a los sistemas de cómputo de la institución, dado que pertenecen a la misma infraestructura de red.

1.1.2 De las Visitas. *Aunque aparentemente muchas personas no consideran las visitas un riesgo potencial, Generalmente las visitas pueden accesar a la institución de una manera libre y sin mayor control administrativo. Una vez que el visitante ha ingresado, prácticamente se encuentra en libertad de movimiento dentro del campus y fácilmente podría hacerse pasar por cualquier estudiante. Si a esta facilidad se le agrega que los recursos de cómputo, por ejemplo las aulas de informática, están abiertas y sujetas a un nivel de control muy flexible, nuevamente se está ante una grave amenaza en la seguridad computacional de la institución.*

1.2 REVELACIÓN DE PASSWORD Y COMPARTICIÓN DE CUENTAS

A pesar de que muchos usuarios tienden a justificar este problema suponiendo que la persona que revela su password acepta los riesgos que esto supone como deserciones, vengativas o disgustos por la otra parte que pueden materializarse en el daño o revelación de la información, el hecho de revelar a terceros o compartir el password o clave de acceso, es una importante fuente de riesgos para la seguridad de la plataforma computacional de la institución. Incluso sin que esta acción deba tener necesariamente carácter de malicia, una equivocación o error sobre la información del propietario de la cuenta, puede acarrear serios problemas de diversos órdenes.

Ahora bien, si el password es revelado a otra persona y esta tiene intereses secundarios, el hecho de tener el acceso a una puerta del sistema (cuenta), le abre una mayor posibilidad de acceder a otros privilegios que pueden llegar a comprometer la información de terceros, el sistema mismo, o servir de puente para un atacante.

La revelación de passwords y la compartición de cuentas constituye un problema de seguridad cotidiano en algunos departamentos de la institución. Independientemente de las razones por la cual estas actitudes son permitidas y vistas con naturalidad por los usuarios (por razones como desarrollo de un proyecto conjunto, o la total confianza en el otro) lo que sí es real es que con esta actitud permisiva y laxa, aparecen grandes huecos de seguridad en toda la institución. Es claro que existen muchos métodos y herramientas de hackers para explotar cualquier hueco en los sistemas, y por lo tanto el uso de

passwords y cuentas estrictamente personales puede contribuir a minimizar y evitar problemas potenciales.

1.3 ÉTICA EN SEGURIDAD EN CÓMPUTO

Por otra parte también es válido considerar que las faltas a la ética suelen ser el origen de muchos problemas de toda índole. Especialmente en ambientes como el computacional, en el que ciertamente todo se mueve y se hace en función de lo que la conciencia dicta que se debe hacer y lo que no. En materia de cómputo la ética tiene que ver con muchos aspectos que desgraciadamente involucran a la seguridad. La intimidad por ejemplo, es un derecho constitucional que con los medios de comunicación tradicionales como el correo postal, correo certificado, etc. está hasta cierto punto garantizado, en cambio con el uso generalizado de los sistemas de comunicación electrónicos, la intimidad y el anonimato de las personas resultan crecientemente amenazadas, debido a ciertas creencias de algunos usuarios en el sentido de que “dar un vistazo” no perjudica a nadie, y además resulta muy difícil de detectar.

1.4 USO IRRESPONSABLE DE LOS RECURSOS DE CÓMPUTO

Desde hace tiempo en la institución se han detectado en diversas ocasiones usos indebidos de los recursos de cómputo que la institución asigna a su personal para el desarrollo de sus actividades. No existe un ambiente de cultura computacional uniforme en los empleados a cargo de los recursos

computacionales, lo que genera riesgos por desconocimiento (falta de alfabetización informática), por uso incorrecto de los equipos (usar los equipos en forma equivocada o errada) y aún por usos indebidos (usar los recursos para actividades diferentes a las funciones laborales). Ello ha causado en varias ocasiones daños a los equipos, o aún pérdidas, y aunque esto puede no haber afectado ampliamente la seguridad de los sistemas y la información, si la hace indisponible.

Particularmente conviene analizar con detalle otro problema que se ha encontrado en los departamentos de la institución, es el uso indebido de los recursos de almacenamiento de datos (discos duros), para diversos fines, como por ejemplo, el almacenamiento de software no autorizado (chat, archivos MP3, MPEG,) que paulatinamente genera un cierto grado de indisponibilidad en operaciones de entrada y salida en los sistemas.

1.5 FALTA DE UN CONTROL EFECTIVO SOBRE LOS RECURSOS DE CÓMPUTO

El Departamento de Servicios Informáticos, responsable de la organización y administración de los recursos de cómputo de la institución debe, como parte de sus actividades básicas llevar un control del software y hardware de la institución y de los incidentes de seguridad ocurridos en la misma. Esta actividad merece una revisión profunda, pues con una revisión superficial a los recursos, se puede concluir con relativa facilidad que el control de software y hardware se ejerce con una cobertura muy baja.

Por otra parte para fines de control y seguridad de los sistemas de cómputo, todo administrador está obligado a reportar cualquier ataque o sospecha de ataque a la seguridad de los sistemas a su cargo. Esto con el fin de tomar medidas inmediatas a nivel institucional en caso de ser necesarias, ya que cuando un sistema es comprometido existe la posibilidad de que otros sistemas también lo estén o ya hayan sido comprometidos. En este aspecto, no existe información recopilada sobre los ataques, caídas de los servicios, y demás incidentes de seguridad, lo que dificulta la toma de decisiones. De igual manera, históricamente no se ha efectuado un monitoreo serio al uso de los servicios de internet, ni al uso de los canales de comunicaciones.

Es muy importante agregar que los usuarios también son responsables de la seguridad de sus cuentas, por lo que tienen la obligación de reportar cualquier anomalía o inconsistencia en las mismas, además están obligados a formar parte activa en la restauración o prevención de incidentes de seguridad que incluyan cuentas, tiempo, y demás recursos del usuario. Ello implica la necesidad de trabajar en el fortalecimiento de una cultura de seguridad al interior de la institución, sin la cual los usuarios tal vez no adquieran ese nivel de responsabilidad compartida que en últimas es indispensable para que se logren los niveles de seguridad deseables.

1.6 SEGURIDAD EN LOS SISTEMAS

Ningún Sistema de Cómputo puede estar completamente seguro sino hasta que éste se encuentre apagado y físicamente bien resguardado. Ciertamente tratar asuntos sobre la implementación de seguridad en los sistemas suele ser muy extenso, no solo por la diversidad de métodos y herramientas que actualmente existen para implementar seguridad, sino además por la cantidad cada vez más creciente de métodos y técnicas de ataque que día a día los intrusos innovan para comprometer sistemas. Es necesario tener en mente que la complejidad de la seguridad puede crecer exponencialmente con el número de servicios proporcionados, y que entre más comunicada se encuentre una máquina mayores serán los riesgos y los requerimientos de seguridad.

1.7 DESCRIPCION FÍSICA DE LA RED DE DATOS DE LA CUTB

1.7.1 Equipos con que se cuenta. La red de la CUTB cuenta con distintas clases de equipos, dependiendo de la función que cumplen. Son los siguientes:

- **Servidores.**

1. Sun Ultra 10
2. Sun Ultra 5
3. Compaq proliant ML350
4. PC clon.

- **Enrutadores**

2 enrutadores 3com 227

- **Concentradores**

Switches 3COM 3300 y 1100

1.7.2 Red Internet (Nodo). Se cuenta con 4 conexiones en fibra óptica utilizadas de la siguiente forma:

Ternera - RedNET a una velocidad de 512 kbps

Manga - RedNET a una velocidad de 128 kbps

Manga - Ternera a una velocidad de 64 kbps, para el tráfico exclusivo de las aplicaciones de bases de datos corporativas.

Un canal E1 para el acceso telefónico (30 canales disponibles)

Ver Figuras 2,3,4,5,6,7 y 8

Los servicios de Internet se encuentran distribuidos de la siguiente forma:

- **SunUltra 10**. Se utiliza para el servidor de correo, DNS, acceso telefónico y WEBMAIL. Su sistema operativo es Solaris 7

- **SunUltra 5.** en esta máquina se se encuentra instalado un firewall que administra las redes que se encuentran físicamente separadas a través de una tarjeta fastethernet de 4 puertos. Por esta maquina pasa todo el trafico de la red institucional. Su sistema operativo es Solaris 7

- **Compaq Proliant**: Servidor Proxy Squid, webserver, servidor base datos mysql, php, y próximamente se instalara el servicio de DHCP. S.O Caldera Open Linux
- **PC clon.** Proxy squid, firewall. S.O. RedHAT Este PC se encuentra instalado en la sede de Manga y los otros servidores en la sede principal del nodo (Ternera)

1.8 ESQUEMA DE LA RED

El esquema de la red consta de una sección identificada con direcciones validas, y otra con direcciones privadas.

La red de direcciones validas, está integrada por las máquinas que son visibles para todo el Internet, que en este caso son los servidores sun utra 5, utra 10, Compaq proliant y el router.

En la red privada, se colocan todos los demás elementos de la red de la Universidad.

El hecho de utilizar direcciones privadas permite completa libertad en el manejo del espacio de direcciones IP, admitiendo subsecuentes crecimientos tanto de estaciones como acceso a Internet, como elementos de la red interna que lo necesiten.

El tener varias redes permite además colocar un elemento Firewall, que controle el acceso desde unas redes hacia las otras, es decir, desde Internet a la red de la universidad, de la red de los estudiantes a la administrativa y viceversa.

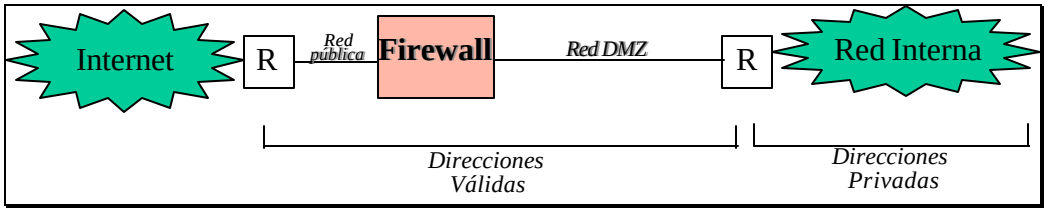

figura 1. Esquema actual de la Red. Sede Ternera

Con este esquema, se cuenta con una DMZ (Demilitarized Zone), en la que las maquinas tienen acceso completo desde y hacia Internet pero están protegidas por el firewall.

1.9 DIRECCIONES IP

Las direcciones validas están comprendidas por la subred 64.76.51.0 con mascara 255.255.255.240 para la sede de ternera y 64.76.51.16 con mascara 255.255.255.240 para la sede de manga.

Para las direcciones IP de la red interna, y de acuerdo con el RFC 1918, hemos escogido la clase B 172.16.0.0, la cual se dividirá en 255 subredes, cada una con 255 elementos, así:

Red Estudiantes Ternera	172.16.4.0
Red Administrativa Ternera	172.16.3.0

Red Profesores	172.16.8.0
Red Acceso Telefónico	172.16.7.0
Red sede manga	172.16.1.0

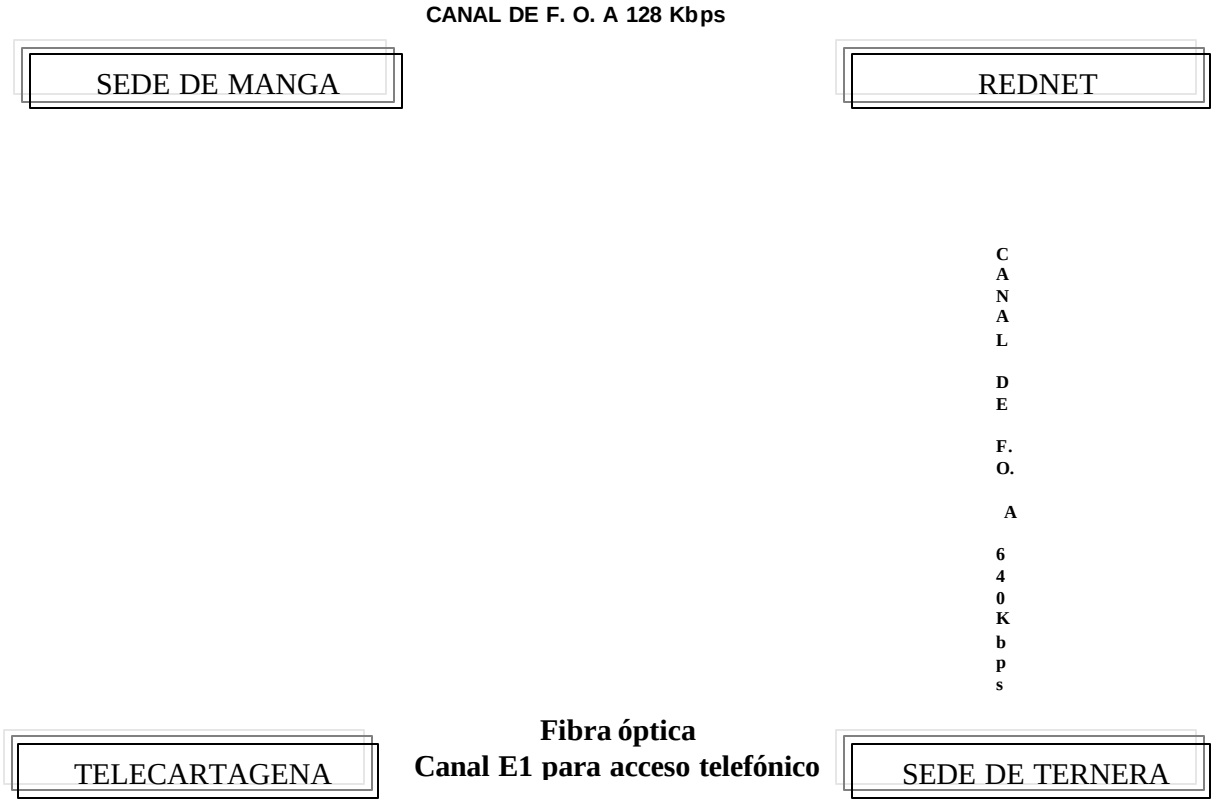

Figura 2. Red Interna de la CUTB. Esquema General

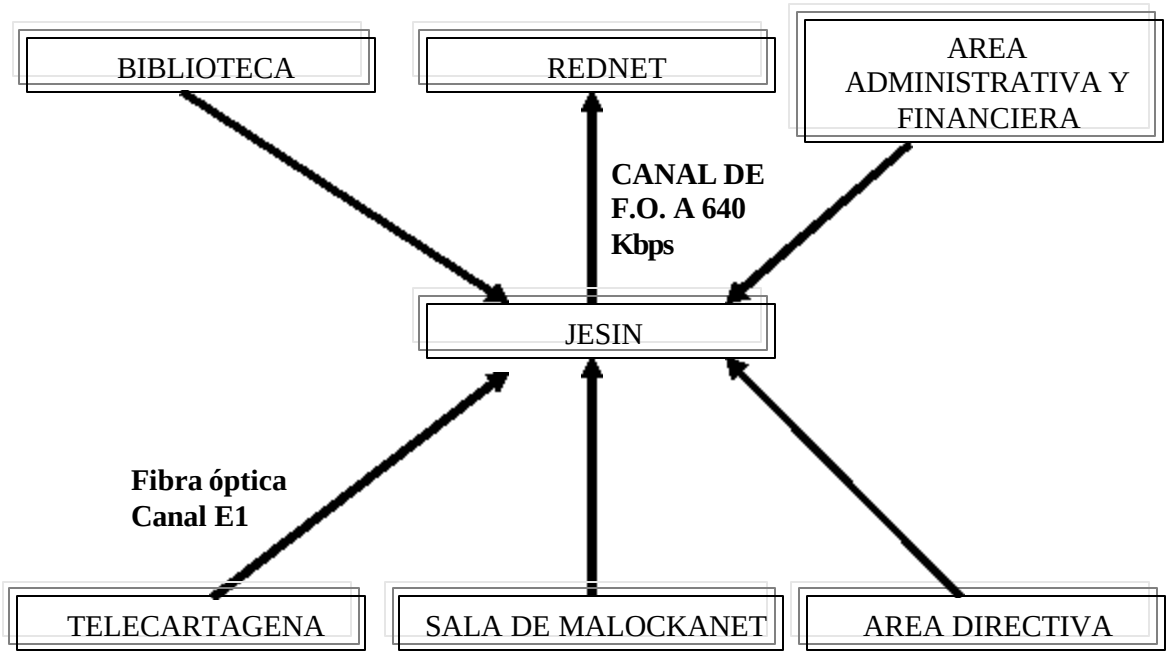

Figura 3. Red Institucional en la sede de Ternera

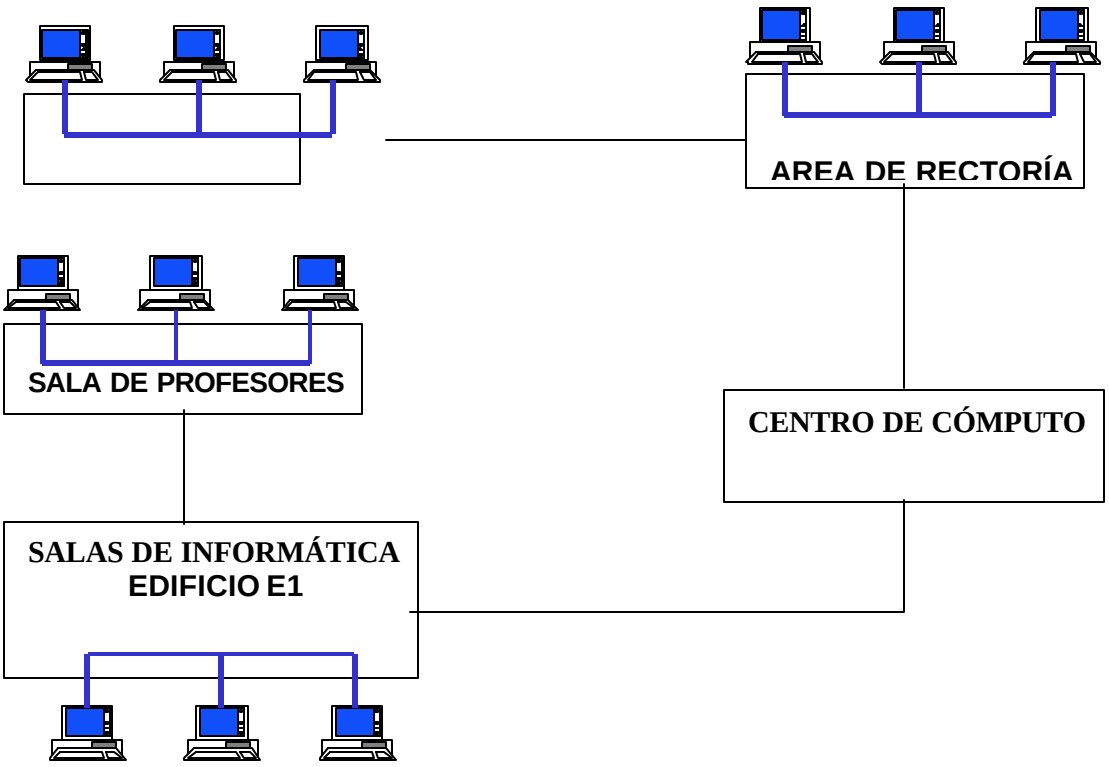

Figura 4. Área Directiva

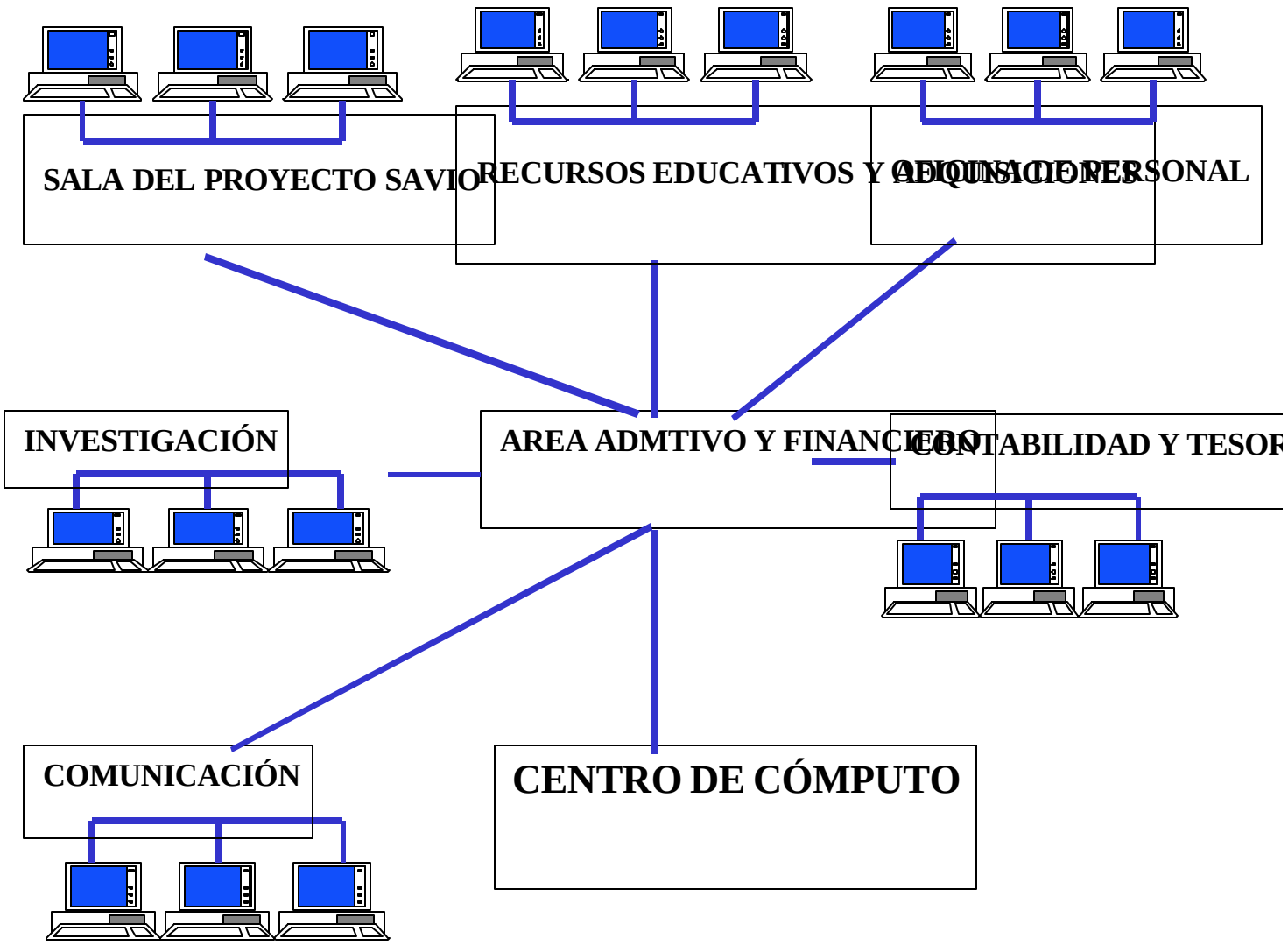

Figura 5. Área Administrativo y Financiero

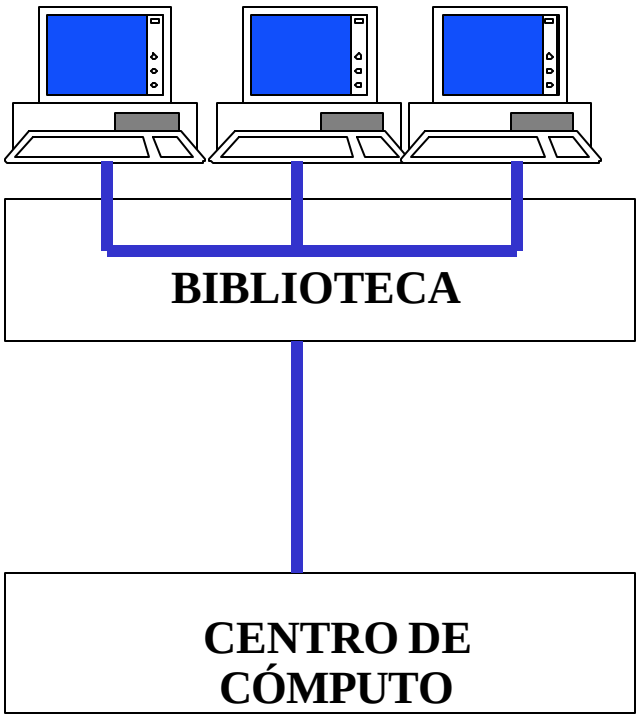

Figura 6. Biblioteca

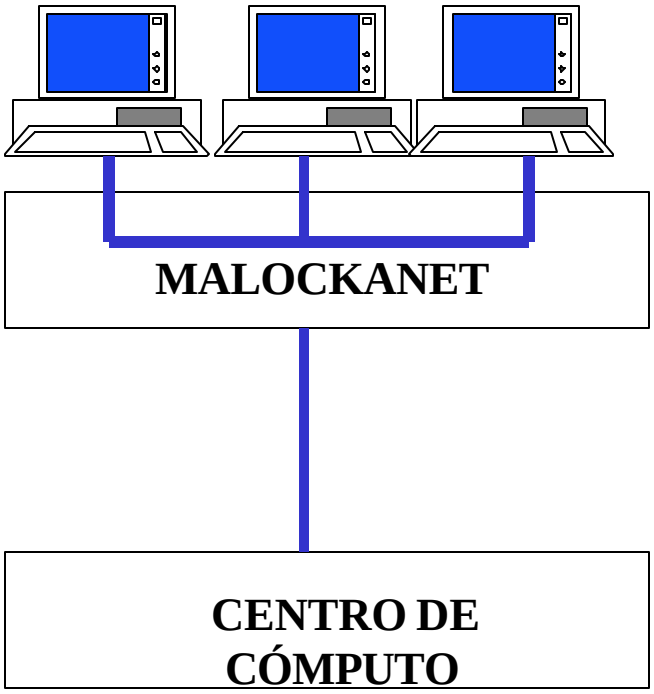

Figura 7. Malockanet

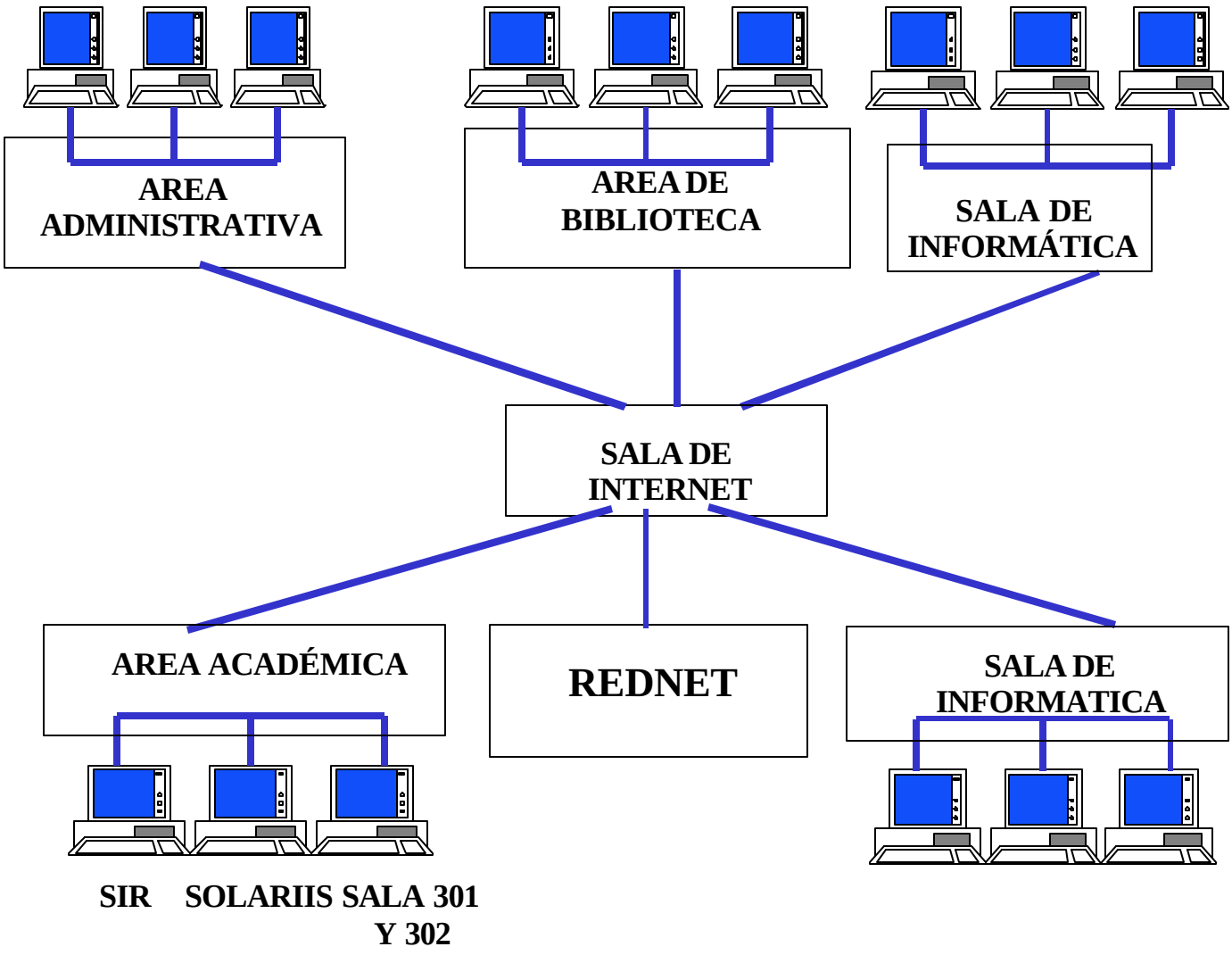

Figura 8. Sala de Informática y Computo

2. DESCRIPCIÓN DE LA METODOLOGÍA UTILIZADA

La TECNOLÓGICA DE BOLÍVAR, posee dos sedes: una en Ternera y la otra en Manga. Los servicios de red son suministrados por Rednet, las dos dependencias se comunican a través de fibra óptica, mediante servicio suministrado por la empresa DUCTEL.

La red corporativa de datos, se encuentra a cargo del Departamento de Servicios Informáticos, y se extiende a cinco grandes localizaciones las cuales son las siguientes:

- **Área directiva:** Incluye las instalaciones de las oficinas de la dirección general y extiende la red hacia el área de rectoría, gestión universitaria, vicerrectoría y decanaturas, sala de profesores y demás oficinas ubicadas en ese edificio.

- **Área administrativa y financiera:** Este tramo de la red comunica el centro de computo con las siguientes dependencias: Oficina de comunicaciones, oficina de investigaciones, Oficinas del proyecto SAVIO, oficina de recursos educativos, Adquisiciones, Departamento de recursos Humanos, dirección financiera, oficina de admisiones, portal del estudiante, coordinación del programa de comunicación social.

- **Edificio de laboratorios y Biblioteca:** este segmento de la red comunica a la biblioteca y todos los laboratorios que se encuentran ubicados en el mismo edificio.

- **Malockanet:** Este espacio que cuenta con un máximo de sesenta puntos de red, tiene comunicación permanente con el centro de computo.

- **Aulas de Informática**: constituyen un tramo de la red, que también tiene servicios permanentes de acceso a internet y se utilizan como espacio académico para las labores asociadas a la docencia.

2.1 DESCRIPCIÓN DEL PROCESO DE LEVANTAMIENTO DE LA INFORMACIÓN

La técnica utilizada para recopilar la información necesaria para el desarrollo de las Políticas consignadas en este documento, fue principalmente la entrevista directa. Se entrevistaron todos los diferentes jefes de dependencia, a los administradores de la red, una amplia muestra de los usuarios, los funcionarios de las distintas dependencia, profesores y decanos de facultad. Asimismo, de la red de la CUTB tanto en pregrado como Posgrado.

A continuación se mencionaran las distintas dependencias visitadas:

- ***Área Directiva*** En esta dependencia se cubrieron las siguientes dependencias:

Rector, Secretario General, Dirección de Gestión Universitaria, Asesor de gestión académica, Asesor de planeación, Auditoría de gestión, Pool de secretarias de rectoría, Vicerrectoría, decanos, pool de secretarias de decanaturas, registro académico.

- ***Área administrativa y financiera:*** Consta de los siguientes departamentos:

Departamento de Adquisiciones, departamento de recursos humanos, Informática y cómputo, departamento de recursos educativos, Dirección de servicios administrativos, asistente administrativo de control, dirección financiera, dirección de investigaciones, departamento de mercadeo, oficina de admisiones, departamento de idiomas, oficina de comunicaciones. Además, en esta sección se hizo la cobertura relacionada con las áreas que dependen

jerárquicamente del departamento de recursos educativos: Biblioteca, aulas de informática (de ambos campus).

- ***Área de Posgrados y Educación Permanente.*** La conforman cuatro dependencias que son:

Jefe de Especializaciones, jefe de educación permanente, jefe de mercadeo, secretaria.

Para llevar a cabo este procedimiento se elaboraron instrumentos para recolectar la información relativa a los siguientes aspectos:

2.1.1 Primera Parte (Entrevista)

- ***Usuarios***

a) clases.
b) privilegios.
c) servicios que pueden usar.
d) controles.

- ***Servicios que existen***

a) tipos
b) a quienes van dirigidos.
c) donde recide el servicio.
d) quien lo administra.

- ***Controles que existen***

a) controles de software.
b) controles de hardware.
c) mantenimiento.
d) licenciamiento.
e) soporte.

- ***Instrumentos de control***

Toda la información recolectada en este proceso de levantamiento mediante entrevistas y visitas a todas las dependencias, está consignada en documento anexo (Ver: Anexo C), en el que se consignan las dependencias visitadas, las funciones que cumple cada una como usuaria de la plataforma tecnológica y los procedimientos relacionados.

2.1.2 Segunda Parte

Con base en esta recopilación de datos se evidenció el estado de la infraestructura computacional y de comunicaciones, a partir del cual se pueden formular políticas de seguridad y administración, de acuerdo con el siguiente esquema:

2.1.2.1 Definir políticas de seguridad

a) Clase de usuarios(estudiantes, profesores) de pregrado y posgrado.
b) Privilegios de cada clase.

2.1.2.2 Definir políticas para el manejo de cuentas

a) Servidor de Internet
b) Servidores administradores.

2.1.2.3 Definir Políticas de Administración de la Información

a) Uso de disco en los puesto de trabajo.
b) Formas de respaldo.
c) Normas para identificar medios de almacenamiento.

2.1.2.4 Políticas para el manejo de software

a) Almacenamiento.
b) Copias.
c) Licencias.
d) Políticas para el diseño, mantenimiento o revisión de aplicaciones y para la aceptación de aplicaciones por parte de los usuarios.

3. DESARROLLO DE LAS POLÍTICAS DE SEGURIDAD PARA LA RED DE LA CUTB

3.1 DEFINICIONES

Para efectos de las políticas contenidas en este documento se entenderán los siguientes conceptos como se definen a continuación.

3.1.1 Usuario. Son usuarios de los recursos de computo e informática de la CUTB los siguientes:

3.1.2 Estudiantes de pregrado. Son aquellas personas que ingresaron a estudiar en cualquiera de los programas de pregrado en la institución y que aun permanecen en ella en calidad de estudiantes activos.

3.1.3 Estudiantes de pos-grado. Son todas aquellas personas que se encuentran registradas como estudiantes activos en programas de maestría y/o especializaciones.

3.1.4 Profesores de tiempo completo. Son los docentes que tienen una vinculación de tiempo completo, que cumplen una jornada laboral de 40 horas a la semana y que además deben cumplir con una carga académica exigida conforme a las normas de la institución.

3.1.5 Profesores de cátedra. Son los docentes contratados por horas, conforme a la demanda de clases que tenga la institución en cada período académico.

3.1.6 Empleados. Son todas las personas vinculadas laboralmente a la institución, que de una u otra manera tienen acceso a los recursos de computo e informática y hacen parte del cuerpo administrativo.

3.1.7 Equipos. La plataforma de hardware que soporta los servicios de red de la institución está conformada por equipos de diferentes propósitos que se definen como aparece a continuación:

3.1.7.1 Servidor. Es un equipo conectado a una red de área local que ejecuta software para controlar el acceso a toda la red, o a parte de ella, y sus recursos y que además puede poner sus recursos de hardware y/o software a disposición de otros equipos de una red ofreciendo servicios de distintas clases.

3.1.7.2 PC. Es una máquina cuyo funcionamiento interno se basa en el uso de un microprocesador, y que a través de él se consigue una serie de prestaciones, que en potencia, manejabilidad, portabilidad y precio cubren la gama mas baja de necesidades en el mundo de la informática.

3.1.7.3 Portátil. se trata de una computadora de características físicas especiales que permiten fácilmente su transporte de un sitio para otro si perder ninguna de las cualidades de una computadora personal.

3.1.8 Cuenta. una cuenta es el privilegio que tiene un usuario para registrarse y trabajar en un sistema adscrito a una red o que ofrece algún servicio sobre ella.

3.1.8.1 Cuentas de usuario: es el ambiente en el cual un usuario obtiene acceso al sistema. Generalmente se identifica con un login (nombre de usuario) y password (contr aseña), sin los cuales no puede tener acceso al mismo y que son de uso privativo y exclusivo del propietario.

4. CRITERIOS GENERALES PARA LA DELIMITACION DE LAS CONDUCTAS ACEPTABLES DE LOS USUARIOS DE INTERNET

Establecer unos límites corporativos para Internet es algo que puede provocar tensiones, al estar relacionado con la intimidad personal y la responsabilidad individual. Pero simultáneamente es una necesidad institucional dado el crecimiento de los riesgos de seguridad computacional causados principalmente por el desarrollo de los niveles de interconectividad, que suponen la posibilidad de acceso desde distintos orígenes. Por ello, es necesario evitar que sea visto como una imposición "desde arriba".

El acceso a Internet no tiene que ser una cuestión de "todo o nada". No debe serlo. Por el contrario, se pueden restringir ciertos servicios, tipos de accesos, ciertos usuarios, franjas horarias, duración de las conexiones, etc, dependiendo de las intenciones y las políticas corporativas. La capacidad de adaptación a las necesidades de la institución es total. Ello ayuda a concebir la conexión a Internet como un privilegio y no un derecho inalienable.

Las políticas tienen que comenzar especificando los principios generales que rigen el uso de Internet por parte de los empleados, y de los profesores y de los estudiantes, tanto durante su actividad laboral como durante otras actividades. Seguidamente, deben detallarse claramente las condiciones de uso de cada servicio individual. Finalmente, deben explicarse las consecuencias de no cumplir las normas.

Todos los miembros de la Comunidad Universitaria también deben saber si la Institución controla regularmente el uso del e-mail o Internet, así como también debe ser evidente y claro para toda la comunidad de usuarios, qué consecuencias conlleva el incumplimiento del código de conducta. Es decir, la existencia de políticas que no tienen consecuencias para quienes las incumplen es inocua.

Por otra parte, un tema en el que deben ser claras y explícitas las normas de uso de Internet es hasta qué nivel se acepta en la institución la navegación en internet para fines personales. Algunas organizaciones, especialmente aquellas que se basan o necesitan de la creatividad o la información, quizás deban incluso incitar a que sus miembros circulen libremente por la red. Otras pueden elegir limitar toda navegación a fines exclusivamente de trabajo y otras se decantarán hacia el justo medio. En el caso especifico de la Universidad: hay que establecer criterios claros para empleados, docentes y estudiantes,

dado que cada categoría de usuarios tiene actividades, finalidades y propósitos diferentes.

En lo que tiene que ver con el horario, dependiendo del tipo y coste de la conexión a la red de cada empresa, es posible decidir -incluso fomentar- un uso adecuado de la red fuera de la jornada de trabajo. Además, con frecuencia se restringe el acceso a ciertos contenidos, tipos de páginas visitadas o actividades específicas, tanto para optimizar el uso del ancho de banda, como para encausar las actividades dentro de los lineamientos filosóficos de la institución.

Pero es necesario recordar que, incluso una vez acabada la jornada laboral, la empresa sigue siendo responsable cualquier actividad que se realice desde el puesto de trabajo, sea ella de acoso sexual, difamación o cualquier otra acción errónea. Además, es evidente que la navegación de los empleados, y todo lo que realicen mientras tanto, sigue repercutiendo en la imagen de la Institución.

Además de los puntos anteriores ahora que es posible enviar e-mails a centenares de personas con un solo clic del ratón, los empleados deben ser conscientes de la necesidad de proteger la información confidencial o de valor de la institución. Planes de negocios, estrategias de mercadeos, análisis de

ventas, proyecciones económicas, y cualquier otra información institucional no deben compartirse con cualquiera.

Este es un tema que afecta directamente al grado de profesionalidad de cada individuo, independientemente de la posición que ocupe en la empresa. Pero es necesario recordar que incluso en Internet siguen existiendo unas normas a cumplir, y proteger la información es cada vez más importante. Sin encriptación, es necesario mentalizar a los empleados de que nada que circule por la red pública es privado.

En general, las acciones de los trabajadores durante su actividad laboral son responsabilidad de la empresa. Debido a que el correo electrónico es un documento escrito, sigue existiendo incluso después de haber sido borrado. Por ello, cualquier empleado tiene que tener claras las implicaciones legales de sus acciones en la red, ya que pueden llegar a incluir acusaciones de acoso sexual o racial, publicación de material obsceno, difamación, infracción de los derechos de autor, transmisión de virus o violación de la seguridad, etc.

En todos los casos, es esencial en tener definidas unas políticas claras y comunicarlas a todo el personal. Por supuesto, ello no garantiza que nunca se tendrán problemas legales, pero es responsabilidad de la empresa que ha tomado medidas razonables para prevenir este tipo de incidentes.

Por ejemplo, incluso el firewall más seguro puede verse comprometido porque un empleado ha revelado un password o una dirección IP. La realidad es que se presentan muchos más problemas causados por negligencia y despreocupación que por ataques hackers.

Una buena solución para evitar las infecciones víricas es la institución de algún tipo de programa antivirus que realice exploración de los e-mails. Pero ello implica que se debe advertir a los usuarios que sus mensajes sufrirán escaneos de rutina como parte de la seguridad de la red. Ello no debe comportar ningún problema, ya que estos escáneres antivirus no suponen ningún tipo de filtrado de contenidos.

Todos los anteriormente dichos tiene sentido siempre y cuando se especifique a quien afectan las Políticas para el Uso de Internet. Si se pretende crear un código de conducta que afecte a todos los alumnos u profesores, debe indicarse que así es y debe ser públicamente conocido por la comunidad de la institución.

Tanto si los responsables del cumplimiento de las Políticas para el Uso de Internet están en Recursos Humanos como en el departamento de Informática, se debe asegurar que existe una persona que sea la responsable y cabeza

visible de estas políticas. Tiene que conocer, además, las responsabilidades que implican:

a. Extenderlas más allá de sus preceptos iniciales

b. Desarrollar el proceso para tratar los incumplimientos de la normativa, como por ejemplo qué hacer en caso de ser la primera falta, en la segunda, en la tercera, etc.

c. Detallar las consecuencias de no cumplir o aplicar las políticas para el uso de Internet

No sobra decir que un requisito imprescindible es el apoyo completo de la alta Dirección así como de todo el cuerpo directivo, de cara a lograr una implantación correcta de las políticas. Como en otros temas, es obvio e indispensable, que los miembros de Dirección sean los primeros en acogerse a la aplicación de las políticas.

Además las Políticas para el Uso de Internet deben ser parte las normas internas de la institución. De esta forma se consigue que el respaldo por parte de la institución y la obligatoriedad de cumplirlas por parte de los trabajadores, ya que en la mayoría de contratos se puede obligar a firmar una cláusula que obliga al cumplimiento de las normas internas.

Además de trabajar en los principios de las Políticas, es importante solucionar también los detalles técnicos para que la nueva normativa esté en línea con la seguridad informática actual que existe en la empresa para redes y usuarios.

Crear unas Políticas es muy semejante a montar unas aduanas: hay que decidir qué tipos de información se quieren dejar entrar y quién va a tener acceso a cada uno. Se deben tener en cuenta los diferentes tipos de ficheros que van a entrar, su tamaño máximo permitido, procedencia y otros detalles, llegando incluso a filtrar el contenido si se juzga conveniente.

La mejor forma de reflejarlo es a través de una tabla, para aplicar las normas y sus excepciones -también explicitadas- a los diferentes usuarios.

Este tema se debería trabajar conjuntamente con los directores y los representantes de los usuarios. No es necesario publicar todos los detalles siempre y cuando se consiga su cooperación y se acuerde revisar las políticas regularmente para adaptarse al cambio de los requisitos, tareas, funcionalidades, técnicas y procedimientos.

Desde otro ángulo, cada vez es más frecuente en todo el mundo, utilizar los correos electrónicos como pruebas en acciones jurídicas. Para evitar la

responsabilidad de la empresa en estos procesos legales, es conveniente incluir un mensaje de negación de responsabilidades al final del texto, Ver Figura 9.

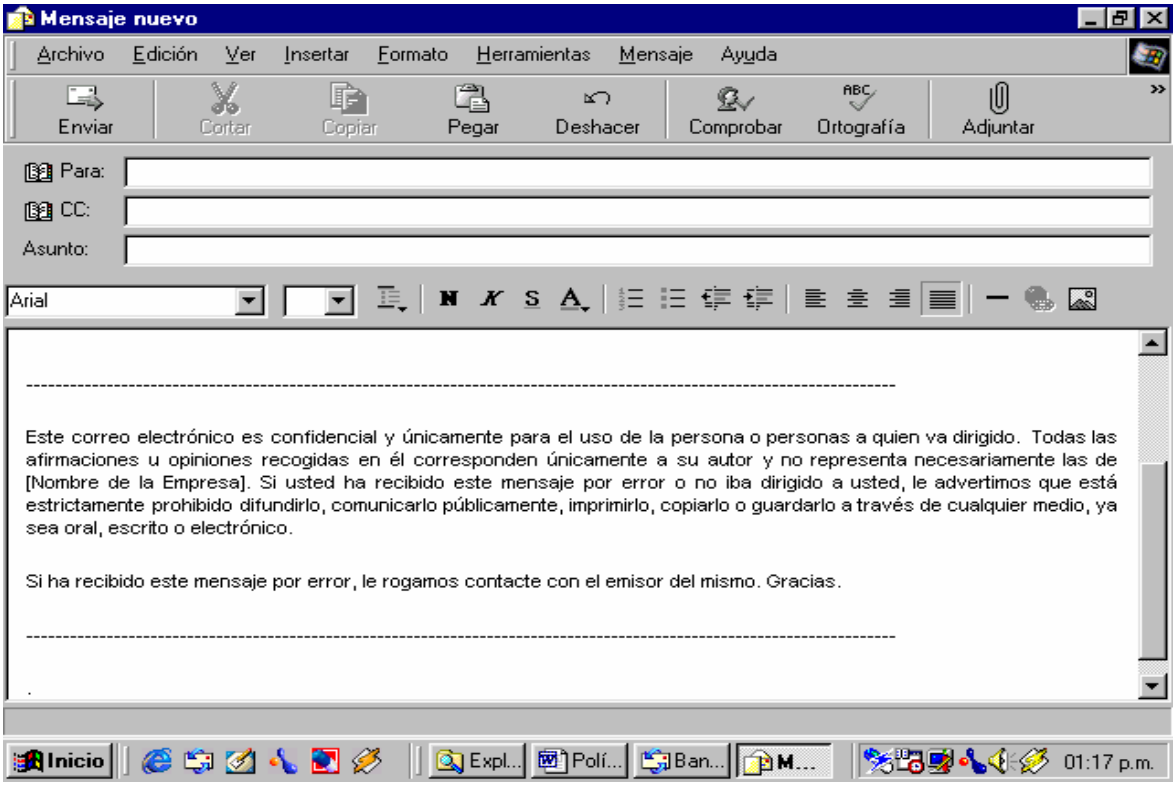

Figura 9. Mensaje de negación de responsabilidad

5. POLÍTICAS PARA MANEJO DE CUENTAS Y CORREO ELECTRONICO

5.1 ESTUDIANTES DE PREGRADO Y POSTGRADO

Las cuentas de correo electrónico para los usuarios de la institución, se utilizan para mantenerlos en contacto con la Institución educativa y brindar servicios tecnológicos de punta para una mejor formación académica. El correo electrónico se concibe en la institución como un medio de comunicación de primer orden, tanto para la comunicación interna a nivel administrativo, como para las comunicaciones entre docentes y estudiantes.

El uso correcto de ellas se define conforme a los siguientes principios:

1. Todo alumno matriculado en los campus de Ternera y Manga tiene derecho a una cuenta y correo electrónico en el servidor del campus por el tiempo que su matricula este vigente. Esto significa que en el momento en que

el estudiante pierde su condición de estudiante activo, pierde también el privilegio de acceder a una cuenta de correo electrónico institucional.

2. Es de completa responsabilidad del us uario hacer buen uso de su cuenta, entendiendo por buen uso los siguientes comportamientos:

a. El no enviar ni contestar cadenas de correo, hoaxes y cualquier otra forma de mensajes considerados como SPAM.

b. La cuenta de correo electrónico institucional se otorga a cada usuario con fines académicos y/o de investigación únicamente. En consecuencia, el uso comercial o de otra naturaleza diferente, es causal de suspensión del privilegio.

c. Es una obligación del usuario depurar periódicamente su buzón en el servidor de correo (INBOX)

d. Se considera mal uso del recurso, el acceso de un usuario a la cuenta de correo electrónico de otro usuario.

e. Es una obligación del usuario hacer uso ¿de un lenguaje apropiado en todas las comunicaciones que sostenga mediante este recurso.

f. Es obligación del usuario el respetar las reglas de conducta universalmente aceptadas para las comunicaciones en internet.

g. Es obligatorio para el usuario respetar todo los términos que se establezcan en el contrato firmado por el estudiante para el uso de Internet.

3. Se asignará solamente una cuenta por usuario con su correo electrónico bajo la denominación estándar establecida por la institución y es obligación del usuario mantener los parámetros de identificación en la mas absoluta reserva.

4. Toda cuenta de correo electrónico es de naturaleza personal e intransferible por lo cual es una falta grave el permitir su utilización por otro usuario o por personas ajenas la institución. La violación a esta política específica constituye causal de sanción para el usuario conforme a los reglamentos.

5. Toda cuenta de correo electrónico tendrá vigencia mientras el usuario mantenga su vinculación activa con la institución. Esto significa que para el caso de usuarios estudiantes y profesores la institución podrá suspender la vigencia de las cuentas en los períodos de inactividad docente.

6. El usuario será responsable de la información que sea enviada con su cuenta, por lo cual se asegurará de no enviar mensajes SPAM, ni anexos que pudieran contener información nociva para otro usuario tal como virus, pornografía, software o documentos ilegales, y en general cualquier información contraria a las normas y principios institucionales.

7. El usuario es responsable de respaldar sus archivos de correo manteniendo en el buzón de correo (INBOX) solamente documentos en tránsito, sus demás comunicados deberá mantenerlos en su equipo personal o en su defecto en carpetas dentro de su cuenta en el servidor.

8. Al responder comunicados generales o para un grupo específico de usuarios, el usuario deberá cuidar de no responder a TODOS los usuarios salvo cuando ésta sea la finalidad de la respuesta.

9. La C.U.T.B se reserva el derecho de enviar al usuario la información que considere necesaria como un medio de comunicación institucional.

10. La vigencia y espacio de las cuentas será definido por el Departamento de Informática y Computo de acuerdo a los recursos disponibles, con base en las necesidades del usuario.

11. El Departamento de Informática y Computo de la C.U.T.B se reservará el derecho de monitorear las cuentas que presenten un comportamiento sospechoso para la seguridad de la red de la C.U.T.B.

12. El Departamento de Informática y Computo de la C.U.T.B realizará chequeos sobre los passwords de correo del campus de manga y ternera de

manera que cancelará aquellos que no se consideren seguros notificando al usuario para su posterior reactivación.

13. El usuario es responsable de respetar la ley de derechos de autor, no abusando de este medio para distribuir de forma ilegal licencias de software o reproducir información sin conocimiento del autor.

14. El incumplimiento por parte del usuario del buen uso de su cuenta puede ocasionar la suspensión y posterior baja del sistema de su cuenta.

15. El usuario podrá generar sus listas de distribución de correo con un máximo de 20 cuentas, y siempre y cuando éstas no interfieran con el buen funcionamiento y la distribución del correo del servidor.

16. El Departamento de Informática y Computo de la C.U.T.B no se compromete a entregar mensajes de correo a cuentas de uso gratuito en servidores externos a la red institucional, tales como hotmail, usa.net, correoweb, excite, starmedia, etc.

5.2 PERSONAL DOCENTE Y ADMINISTRATIVO

Para los usuarios no estudiantes, el uso correcto de este recurso se entiende definido en los siguientes párrafos:

1. Todos el personal vinculado a la C.U.T.B, para propósitos docentes y administrativos, puede tener acceso a una cuenta de correo electrónico en el servidor de correo institucional, previa solicitud a su superior inmediato para su autorización. En todos los casos la institución se reserva el derecho de autorizar el acceso a este servicio, conforme a sus necesidades e intereses. En consecuencia, todos los usuarios deben entender el acceso al recurso del correo electrónico como un privilegio y no como un derecho.

2. Es responsabilidad del usuario hacer buen uso de su cuenta, entendiendo por buen uso:

a) El no enviar ni contestar cadenas de correo, hoaxes o spam.
b) El uso de su cuenta con fines exclusivamente académicos, administrativos y/o de investigación, que estén relacionados directa o indirectamente con las actividades propias de su vinculación con la institución..
c) La depuración de su INBOX del servidor (no dejar correos por largos periodos en su buzón de correo).
d) El no hacer uso de la cuenta para fines comerciales o personales.
e) El respetar las cuentas de otros usuarios Internos y externos.
f) El uso de un lenguaje apropiado en sus comunicaciones.
g) El respetar las reglas de conducta generalmente aceptadas en internet para las comunicaciones entre usuarios.

3. Se asignará solamente una cuenta por usuario. Las cuentas por proyectos o para dependencias específicas se asignarán previa autorización de la Vicerrectoría, de la C.U.T.B, a partir de solicitud escrita de la dirección respectiva.

4. Las cuentas conmutadas para el personal administrativo serán asignas por la rectoría.

5. La cuenta de correo está definida como de uso exclusivamente personal e intransferible. Por lo tanto, el que un usuario permita que segundas personas hagan uso de ella, (secretarias, becados, amigos, hijos, etc.) se considera una falta a las normas y puede conducir a la suspensión de la cuenta y eventualmente a una sanción.

6. La cuenta se dará de baja en el momento que el usuario deje de pertenecer al campus.

7. Es responsabilidad del usuario el actualizar su password con regularidad, como una medida de seguridad, cumpliendo con las normas que se definen en administración de correo acerca del manejo de passwords

seguros. El tiempo de vida de los passwords deberá ser de, a lo más, un semestre.

8. El usuario será responsable de la información que sea enviada con su cuenta, por lo cual se asegurará de no enviar, responder o reenviar, SPAM, ni anexos que pudieran contener información nociva para otro usuario como virus, pornografía, mensajes ofensivos, software ilegal o cualquier otra forma de información contraria a los principios y normas institucionales.

9. El usuario es responsable de respaldar sus archivos de correo manteniendo en el INBOX (Buzón de correo) solamente documentos en tránsito, sus demás comunicados deberá mantenerlos en su equipo personal.

10. Al responder comunicados generales o para un grupo específico de usuarios, el usuario deberá cuidar de no responder a todos los usuarios salvo cuando ésta sea la finalidad de la respuesta.

11. La C.U.T.B se reserva el derecho de enviar al usuario la información que considere necesaria como un medio de comunicación institucional, dado que la cuenta de correo electrónico institucional se considera como un medio de comunicación institucional.

12. La vigencia y espacio de las cuentas será definida por la Dirección de la C.U.T.B. de acuerdo a los recursos disponibles, con base en las necesidades del usuario.

13. La dirección de la C.U.T.B. se reserva el derecho de dar de baja las cuentas que no tengan actividad por periodo de un mes, quedando su "nombre de usuario" reservado para el mismo usuario por el resto del respectivo período académico, siempre y cuando la persona permanezca vinculada a la institución.

14. La dirección de la C.U.T.B reservará el uso de monitorear las cuentas que presenten un comportamiento sospechoso para la seguridad del campus.

15. La dirección de la C.U.T.B realizará chequeos sobre los passwords de correo del campus de manera que cancelará aquellos que no se consideren seguros notificando al usuario para su posterior reactivación.

16. El usuario es responsable de respetar la ley de derechos de autor, no abusando de este medio para distribuir de forma ilegal licencias de software o reproducir información sin conocimiento del autor.

17. El incumplimiento por parte del usuario del buen uso de su cuenta puede ocasionar la suspensión y posterior baja del sistema de su cuenta.

18. El usuario podrá generar sus listas de distribución de correo con un máximo de 20 cuentas, y siempre y cuando éstas no interfieran con el buen funcionamiento y la distribución del correo del servidor**.**

6. POLÍTICAS PARA ADMINISTRACION DE LA PLATAFORMA TECNOLOGICA

Actualmente la seguridad informática ha tomado gran auge, dadas las cambiantes condiciones y nuevas plataformas de computo disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes para explorar mas allá de las fronteras institucionales, situación que ha llevado la aparición de nuevas amenazas en los sistemas computarizados.

Como una consecuencia de lo anterior, es de primordial importancia la determinación de políticas y normas claras sobre la utilización de la plataforma computacional que soporta los servicios de red y comunicaciones.

6.1 SERVIDOR DE INTERNET.

1. El departamento de informática y cómputo es el responsable de instalar y administrar el servidor de Internet (WWW, ftp), es decir, sólo se permiten servidores de páginas y sitios previamente autorizados y controlados por la institución. La descentralización de sitios web, podrá hacerse previo acuerdo técnico con el departamento de informática y cómputo, y siempre que la responsabilidad por su control quede a cargo de un directivo.

2. El departamento de informática y cómputo deberá emitir las normas y los requerimientos para la instalación de servidores de páginas locales, de bases de datos, del uso de la intranet institucional, así como las especificaciones para que el acceso a estos sea seguro.

3. Los accesos a las páginas de web a través de los navegadores deben sujetarse a las normas que previamente se manifiestan en el Reglamento de acceso a la red de la C.U.T.B.

4. A los responsables de los servidores de Web corresponde la verificación de respaldo y protección adecuada.

5. Toda la programación involucrada en la tecnología Web deberá estar de acuerdo con las normas y procedimientos del departamento de informática y cómputo.

6. El material que aparezca en la página de Internet de la C.U.T.B. deberá ser aprobado por el Departamento de comunicaciones, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).

7. En concordancia con la libertad de investigación, se acepta que en la red de la C.U.T.B. conectada a Internet pueda ponerse información individual sin autorización (siempre y cuando no contravenga las disposiciones que se aplican a las instituciones gubernamentales). Con referencia a la seguridad y

protección de las páginas, así como al diseño de las mismas deberá referirse a las consideraciones de diseño de páginas electrónicas establecidas por departamento de informática y cómputo.

8. El departamento de informática y cómputo tiene la facultad de llevar a cabo la revisión periódica de los accesos a los servicios de información, y conservar la información del tráfico.

6.2 SERVIDORES ADMINISTRATIVOS

El principio básico de seguridad en la red y en los servidores de la C.U.T.B será:

"Lo que no se permite expresamente, está prohibido".

Los siguientes puntos describen la forma en que los administradores de red deben conducirse al manejar sus servidores y al traficar información por la red de la C.U.T.B esto es, las estrategias y políticas de seguridad que se respetarán dentro de la red y dentro de los sistemas de cómputo (esto involucra todos los servidores que de alguna u otra forma estén conectados a la red de la C.U.T.B). Los administradores de sistemas seguirán estas políticas y podrán adecuarlas a su entorno.

6.2.1 Confidencialidad. Esto significa que la información debe estar protegida de ser copiada por cualquiera que no esté explícitamente autorizado por el propietario de dicha información. En este punto se deben considerar:

a. Los directorios en los servidores deberán tener los permisos necesarios para evitar ser accedidos por personas que no sean los propietarios de dichos directorios. Todos los servidores dentro de la Universidad, a menos que se justifique lo contrario, deberán de dar de alta a los usuarios, esto es, para un mejor desempeño; contar con cuentas para las personas que soliciten los servicios del servidor.

b. La C.U.T.B se reserva el derecho de determinar que programas tendrán permisos de ejecución para los usuarios en sus servidores.

6.2.2 Mantener la integridad de los datos. Esto es, proteger la información (incluyendo programas) de ser borrada o alterada en cualquier forma sin permiso del propietario o dueño de la información. Esto implica:

a. Hacer respaldos periódicos de la información en cintas magnéticas u otro medio del que se disponga.

b. Auditar las cuentas para verificar que no haya alguna copia de programas y archivos no autorizados por el administrador en el sistema.

6.2.3 Consistencia. Esto es, estar seguro que el sistema es manejado por personal autorizado.

El administrador de cada sistema debe cuidar de cambiar periódicamente los passwords de administración y estar seguro de que solo las personas necesarias saben de estas claves.

6.2.4 Auditoria.

a) Ejecutar periódicamente programas de auditoria o programas de diagnóstico para verificar la integridad de los sistemas.

b) Revisar periódicamente las bitácoras de acceso a los servidores para encontrar posibles ataques o accesos no autorizados.

c) Producir los informes de auditoria que se aparezcan.

La evaluación de la seguridad se hace utilizando herramientas de software que, con un completo conjunto de pruebas de penetración, buscan la debilidad que los intrusos explotan más comúnmente para obtener acceso no autorizado a la red. Así mismo, detectan riesgos, proporcionan reportes y recomiendan acciones corr ectivas.

En una auditoria y evaluación de seguridad se busca penetrar o evadir los mecanismos de seguridad existentes (si los hay), de manera similar a como lo hacen los *hackers*. De hecho, existen algunos tipos de software de seguridad:

a) SAFEsuite.- Provee herramientas de monitoreo, ejecución de políticas, detección de intrusos y respuestas en tiempo real en el tráfico de la red, sitios web, firewalls y sistemas operativos UNIX y NT.

b) Internet Scanner.- Realiza evaluaciones automatizadas de seguridad de redes TCP/IP.

c) System Scanner.- Identifica y prioriza la vulnerabilidad y las malas configuraciones a nivel del sistema operativo, permisos y pertenencia de archivos, servicios de red, configuración de cuentas y aspectos comunes de seguridad, tales como claves débiles de usuarios.

d) Security Manager.- En un ambiente cliente-servidor, verifica interactivamente las vulnerabilidades y malas configuraciones. Se puede calendarizar para que se ejecute en forma automática, generando alertas cuando aparezca un nuevo problema. Las verificaciones están definidas en una base de conocimiento (*knowledge base*) que reside en cada cliente.

e) Database Scanner.- Los datos más críticos y sensitivos de una organización residen en bases de datos relacionales, que muchas veces están desprotegidas y son vulnerables a intrusos. Esta información con frecuencia está disponible para cualquiera, por lo que se corre el riesgo de que sea robada o saboteada, debido a claves débiles o inexistentes, malas configuraciones o "puertas traseras" (*backdoors*) de los sistemas. Este software provee una auditoria completa de la autorización, autenticación, integridad del sistema y compatibilidad con el Año 2000, desde una base de datos relacional.

f) SAFEsuite Decisions.- Es un sistema completo de seguridad adaptable, que integra datos críticos de otros sistemas (como los antes enumerados) para evitar que los administradores de la red tengan que recolectar y analizar datos, maximiza la seguridad de redes y de comercio electrónico basado en Internet y genera reportes que permiten establecer el estado de las condiciones cambiantes en los riesgos de las empresas.

Desde luego se deben diseñar e implantar políticas de seguridad, como las que define el CAMM (*Computer Assurance Maturity Model*), que es una metodología para medir la "madurez" o nivel de avance del proceso de protección de la información de una empresa. Éste puede ser conceptualizado como un programa para asegurar la calidad de la información, permitiendo que una organización pueda iniciar su proceso hacia la postura deseada de seguridad, agregando políticas, procesos, tecnologías y mediciones para alcanzar, cada vez más, niveles superiores de seguridad.

6.2.5 Obligaciones y responsabilidades de los administradores. Los administradores de los sistemas son los encargados de mantener en buen estado los servidores dentro de la red de la Universidad. Los administradores deben:

a) Hacer respaldos periódicos de la información así como la depuración de los discos duros.

b) Realizar auditorias periódicas en el sistema con el fin de localizar intrusos o usuarios que estén haciendo mal uso de los recursos de un servidor.

c) Decidir sobre el uso de los recursos del sistema restricci de

directorios y programas ejecutables para los usuarios.

d) Revisar el tráfico de paquetes que se estén generando dentro de su segmento de red, a fin de determinar si se está haciendo mal uso de la red o se

esta generando algún problema que pueda llevar a que se colapsen los sistemas.

e) Dar de alta a usuarios y revisar las cuentas peri icamente para estar seguros de que no hay usuarios ficticios. Dar de baja a los usuarios.

f) Realizar monitoreos, lo más frecuentemente posible de la red y servidores para estar seguros que no hay usuarios indebidos y que no se está haciendo mal uso de los recursos de la r ed.

g) Recomendar sobre el uso e implementación de nuevas tecnologías para administración de los sistemas y la red.

h) Reportar a la C.U.T.B las fallas en el desempe de la red. Solucionar los problemas que se generen en su red local.

6.2.6 Control de accesos. En muchas ocasiones ha sido posible obtener acceso no autorizado a los sistema de computo, permitiéndole a los intrusos en cuestión, utilizar recursos a los que no debería tener acceso, o incluso realizar actos dañinos como robar o destruir información. Por esta razón, es muy importante tener en cuenta que el conectarse a una red, y sobre todo a una red de alcance global como Internet, trae también muchos problemas de seguridad.

6.2.7 Acceso a áreas críticas.

1. El acceso de personal se llevará acabo de acuerdo a las normas y procedimientos que dicta el departamento de informática y computo.

2. En concordancia con la política de la institución y debido a la naturaleza de estas áreas se llevará un registro permanente del tráfico de personal, sin excepción.

3. El departamento de informática y computo deberá proveer de la infraestructura de seguridad requerida con base en los requerimientos específicos de cada área.

4. Bajo condiciones de emergencia o de situaciones de urgencia manifiesta, el acceso a las áreas de servicio crítico estará sujeto a las que especifiquen las autoridades superiores de la institución.

6.2.8 Control de acceso al equipo de cómputo.

1. Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.

2. Las áreas donde se tiene equipo de propósito general cuya misión es crítica estarán sujetas a los requerimientos que el departamento de informática y computo emita.

3. Las áreas de cómputo de los departamentos donde se encuentre equipo cuyo propósito reúna características de imprescindible y de misión crítica, deberán sujetarse también a las normas que establezca el departamento de informática y computo.

4. Los accesos a las áreas de críticas deberán de ser clasificados de acuerdo a las normas que dicte el departamento de informática y computo de común acuerdo con su comité de seguridad informática.

5. Dada la naturaleza insegura de los sistemas operativos y su conectividad en la red, el departamento de informática y computo tiene la facultad de acceder a cualqui er equipo de cómputo que no esté bajo su supervisión.

6.2.9 Acceso a los sistemas administrativos.

1. Tendrá acceso a los sistemas administrativos solo el personal de la C.U.T.B. que es titular de una cuenta de gastos o bien tenga la autorización del responsable si se trata de personal de apoyo administrativo o técnico.

2. El manejo de información administrativa que se considere de uso restringido deberá ser cifrada con el objeto de garantizar su integridad.

3. Tendrá acceso al sistema de información de la Dirección de Estudios de Postgrado sólo aquellos usuarios de **C.U.T.B.** o externos autorizados por dicha dirección.

4. La instalación y uso de los sistemas de información se rigen por el reglamento de uso de la **C.U.T.B.** y por las normas y procedimientos establecidos por el departamento de Informática.

5. Los servidores de bases de datos administrativos son dedicados, por lo que se prohíben los accesos de cualquiera, excepto para el personal del departamento de Informática.

6. El control de acceso a cada sistema de información del departamento de informática y computo será determinado por la unidad responsable de generar y procesar los datos involucrados.

6.3 DE SALAS DE INFORMÁTICA (MALOCKA NET, LABORATORIOS, SALAS DE POST GRADOS, MAESTRÍAS, VIRTUALES Y SUS RECURSOS), SERVIDORES Y SERVICIOS.

Los recursos estarán disponibles a los usuarios para utilizarse conforme a las normas que se establezcan para los usos de los laboratorios del Centro. Con estos fines, la persona a cargo de dirigir el Centro tendrán la responsabilidad de publicar las normas que rigen su unidad, así como establecer el horario de servicios que se le brindara al usuario.

El centro, es un lugar para el estudio, investigación, y el trabajo, por lo cual debe de prevalecer un ambiente de orden, silencio y decoro.

El personal del Centro tiene la autoridad para requerirle a cualquier persona el carné de estudiante actualizado.

1. Para hacer uso del laboratorio el estudiante deberá presentar su carné de estudiante actualizado de la C.U.T.B al momento de ingresar al mismo.

2. Desde el equipo asignado será posible hacer uso de la red Internet, únicamente para fines académicos, definiéndose como académico a todas aquellas búsquedas de información que apoyen al aprendizaje de alguna de las materias que se estén cursando.

3. Únicamente se deberá acudir a los administradores de software si hay dudas o problemas con el funcionamiento del software para asesoría.

4. El uso de equipo de digitalización de documentos (scanners), impresoras a color, proyector de acetatos, proyector de opacos, video beam, retroproyectores exclusivamente para actividades académicas y se deberá de solicitar al auxiliar del laboratorio.

5. El uso de medios magnéticos estará sujeto a las normas de seguridad que se establezcan en cada caso.

6. Se prohíbe el ingresar a cualquier sala de informática con alimentos y bebidas, así como el fumar en ellas.

7. El contenido de los discos duros de las estaciones de trabajo y el del servidor es continuamente depurado para evitar la saturación de espacio. Por lo anterior es responsabilidad de los usuarios el respaldar su información en discos flexibles (disquetes). En caso de dejar algún archivo en algún disco duro o el servidor, es bajo la responsabilidad total del usuario.

8. El auxiliar asignará una máquina de la que será responsable durante el tiempo a permanecer en su poder.

9. La C.U.T.B se reserva el derecho de revisión del contenido de lo almacenado dentro de la cuenta del estudiante para velar por el correcto uso del equipo de laboratorio.

10. Cualquier uso que cause efectos opuestos a la operación de la C.U.T.B o ponga en riesgo el uso o rendimiento de la red, será analizado por esta administración para tomar medidas.

11. El lugar de trabajo debe quedar ordenado y limpio al término de cada sesión de trabajo.

12. La entrada y salida de docentes, estudiantes y auxiliares debe realizarse en forma ordenada y puntual.

13. El equipo, instalaciones y material de apoyo se entregarán en buenas condiciones. En caso de extravío o daño de equipo por parte del usuario, éste tendrá que reponerlo o pagarlo al valor de reposición.

14. Las únicas personas que pueden desconectar, mover o abrir el equipo y sus componentes, son las autorizadas por el laboratorio o sala correspondiente

15. Para eventos especiales que requieran el uso de algún laboratorio o sala en específico: El Departamento interesado deberá solicitarlo por escrito o por correo electrónico, a la cuenta de la sala o laboratorio correspondiente, con una semana de anticipación. Con mayor anticipación más probabilidades habrá de tener el servicio requerido.

16. Todo usuario debe asegurarse de cerrar la sesión de trabajo cuando desocupe el equipo.

17. Al terminar la sesión de trabajo, cada usuario tendrá un tiempo máximo de cinco minutos para desalojar y entregar el material prestado, antes de terminar el turno de trabajo.

18. Restricciones en las salas de informática: El presente reglamento normará el uso de las salas de informática e Internet en la C.U.T.B.

a) Permanecer como espectadores en el laboratorio y/o estar más de una persona por máquina, salvo que el profesor de la asignatura así lo autorice.

b) Consumir alimentos, bebidas o fumar dentro del laboratorio.

c) Utilizar servicio de voz, sonido o imagen no autorizados.

d) Usar lenguaje soez en la comunicación de Internet.

e) Demorar la entrega de máquina cuando sea solicitado por el profesor o supervisor del laboratorio.

f) Conectar periféricos o instalar software al equipo sin previa autorización por escrito a la dirección del departamento de informática y computo.

g) Hablar en voz alta, hacer tertulias, o ninguna otra actividad que perturbe el ambiente de estudio y trabajo.

h) Efectuar transacciones de compra – venta.

i) Vestimenta no apropiada o insegura.

j) Sentarse en las mesas, el piso y otros lugares no apropiados.

k) Instalar juegos y/o cualquier software no autorizado, y jugar en las computadoras.

Las faltas leves se sancionarán de la siguiente manera:

a) Amonestación por escrito con copia al expediente la primera vez.

b) Amonestación por escrita y suspensión del uso del laboratorio por un período de 3 meses en el caso de los incisos b, d y f.

c) Además de lo anterior de acuerdo con la gravedad se aplicara el régimen disciplinario previsto en los reglamentos.

19. Se consideran faltas graves, las siguientes infracciones:

a) Consultar y/o desplegar cualquier tipo de material erótico o de pornografía.

b) Mover máquinas, equipos, cables u otros elementos propios del laboratorio, sin supervisión y autorización de miembros de la dirección del departamento de informática y computo de la C.U.T.B.

c) Utilizar el equipo de la C.U.T.B para piratería o acceso no autorizado (hacking) a servidores propios o ajenos.

d) Haber acumulado 4 faltas leves durante un período.

e) Borrar Software instalado de la C.U.T.B.

f) Irrespetar de palabra o acción a los auxiliares o encargados del laboratorio.

g) Sustraer equipos del laboratorio.

h) Realizar acción voluntaria que cause daño a los equipos del laboratorio.

i) Causar daños o perjuicios a terceras personas.

j) Otras, que afecten en forma grave el funcionamiento del laboratorio.

20. Las faltas graves se sancionarán de la siguiente manera:

a) Las indicadas en los incisos b, d, e y j del numeral 19 se sancionarán por primera vez con amonestación escrita y suspensión temporal del uso del laboratorio; las reincidencias darán lugar a expulsión definitiva del laboratorio.

21. Toda amonestación será comunicada por la Decanatura respetiva o por otra autoridad de la C.U.T.B.

22. Las sanciones por faltas graves serán comunicadas por la Decanatura respectiva.

23. El estudiante tiene derecho a apelar ante el Consejo Académico a mas tardar en la semana siguiente de habérsele comunicado la sanción**.**

7. POLÍTICAS DE ADMINISTRACIÓN DE LA INFORMACIÓN

7.1 USO DE LOS DISCOS DUROS EN LOS PUESTOS DE TRABAJO

La primera medida de prevención es contar con un sistema antivirus y utilizarlo correctamente. La única forma de que se constituya un bloqueo eficaz para un virus es que se utilice con determinadas normas y procedimientos, las cuales deberían verificar los siguientes aspectos:

a) Un disco de sistema, protegido contra escritura y libre de virus.

b) Por lo menos un programa de Antivirus actualizado.

c) Una fuente de información sobre virus específicos.

d) Un programa de respaldo de áreas críticas

e) Lista de lugares donde acudir.

f) Un sistema de protección residente.

g) Tener respaldos.

h) Revisar todos los discos nuevos antes de utilizarlos.

i) Revisar todos los discos que se hayan prestado.

j) Revisar todos los programas que se obtengan vía red.

k) Procedimiento para revisar o desinfectar la computadora

l) Procedimiento para desinfectar el sector de arranque

m) Procedimiento para restaurar los respaldos.

n) Procedimientos para formatear discos duros en caso de que estén infectados.

o) Reportar a alguna autoridad la infección.

7.2 FORMAS DE RESPALDO (MÉTODOS)

Actualmente, los usuarios experimentan el continuo increm ento de la cantidad de datos que necesita archivar, consultar y transmitir. Los datos de computación son de misión crítica y nadie debería poner en riesgo sus negocios por no haberse preocupado de resguardar sus datos. La mayoría de las empresas depende netamente de los datos que guarda en su archivo, como son los bancos, financieras, periódicos, etc. Es por ello que todas las empresas deberían utilizar técnicas de back-up para respaldar sus datos, con la frecuencia necesaria para satisfacer sus exigencias.

Una estrategia de back-up adecuada es el seguro más efectivo contra incendios, inundaciones, crash de discos, errores humanos, robos, boicots o virus. Todas esas cosas pueden provocar la pérdida de datos importantes o en el mejor de los casos la necesidad de invertir un tiempo prolongado en operaciones para recuperarlos.

7.2.1 Dispositivos de Respaldo

7.2.1.1 Grabador de CD. Si actualmente la gran mayoría de los computadores poseen discos para almacenar información, la utilización de estos dispositivos tiene tres grandes ventajas con respecto al uso de la memoria principal como almacenamiento

- La capacidad de espacio de almacenamiento disponible es mucho más grande.
- El precio por bit es más bajo.
- La información no se pierde al apagar el computador.

Además, estos dispositivos tienen una serie de características físicas y técnicas que los hacen atractivos para los usuario de uso moderado principalmente, como son:

a) Es de fácil manejo y archivo (estuches de padrón internacional)
b) Soporta extremas temperaturas de calor
c) Alta resistencia a la manipulación, impresiones digitales, etc.
d) Consta con un método de distribución de Datos de bajo costo
e) Tiene larga vida útil para los datos recuperables
f) Guarda cualquier tipo de archivo de información
g) Guarda y corre programas de aplicación
h) Almacenamiento permanente de datos
i) Infinito número de Ciclos de lectura

j) Seguridad en la integridad de datos

7.2.1.2 Sistemas Disk array: Un Sistema Disk Array es un arreglo de discos y es un método por el cual se organizan dos o más discos duros con el objetivo de mejorar su capacidad, su performance y en algunos casos de otorgar la posibilidad de tolerar la falla de por lo menos uno de los discos. Un arreglo de discos permite cambiar uno de los discos duros del sistema en el caso que falle uno de ellos, sin tener que apagar el computador, como se debe hacer en los PC de discos duros que no pertenecen a un arreglo.

Los discos duros se pueden organizar de distintas maneras, cada una con distintas ventajas: la forma de organizarlos se denomina niveles RAID (Redundant Array of Inexpensive Disks). El entorno ideal para instalar un RAID son las redes Local Area Network, donde es inaceptable detener el Sistema por la falla de un disco. Además de la capacidad para tolerar fallas de discos, un Sistema Disk Array puede estar equipado para tolerar también fallas de otros componentes como fuentes de alimentación y ventiladores

7.2.1.3 El Disk array y el Back-up: Un Disk Array nos brinda seguridad para trabajar con nuestros datos, ya que en caso que falle algún componente o se dañe alguno de los discos rígidos, el sistema seguirá funcionando

ininterrumpidamente y no se perderán los datos dependiendo de los niveles de seguridad que previamente se haya elegido.

Sin embargo, tener los datos en un Sistema Disk Array no significa que los datos estén resguardados. El resguardo de datos se hace para que ante cualquier inconveniente que ocurra con nuestros discos rígidos, ya sean fallas del hardware, errores o siniestros como robo, incendio, inundaciones, error humano, etc. que provoquen la pérdida parcial o total de nuestros datos; tengamos una copia de los datos del día anterior o por lo menos de una semana atrás. Esa copia es el Back-up, que debe realizarse sobre una cinta o un medio óptico, y debe guardarse en un lugar físico distinto y alejado de donde se encuentran los discos. Entonces un Sistema Disk Array requiere indefectiblemente el Back-up.

7.2.1.4 Cintas Magnéticas: Estos dispositivos son los más utilizados en las empresas o instituciones que tienen gran movimiento de información, esto es debido a las características que ellas presentan: son reutilizables, lo que aminora su costo a largo plazo, también tienen la ventaja de ser físicamente pequeñas, pero de gran capacidad de almacenamiento.

Además de sus funciones de back-up, un sistema de almacenamiento en cinta tiene utilidad en otras aplicaciones como el almacenamiento jerárquico, el archivo, o la distribución de datos.

El almacenamiento en cinta implica copiar en ellas archivos que originalmente se almacenan en los discos duros de un computador. Las cintas permiten almacenar información por largos períodos de tiempo. La seguridad de los datos es total si se archiva sobre cintas confiables, redundantes, que se guarden fuera del lugar donde está el departamento encargado de realizar los respaldos.

Por tener la característica de ser reutilizables, las cinta pueden organizarse en un sistema de rotación, lo que se define como política de respaldo. Más cintas en el esquema de rotación no significa un mayor gasto de cintas, las cintas se gastan en función a sus horas de uso.

Al respaldar se suele utilizar la técnica de rotación de Cintas, la cual consiste en, por ejemplo, al llenarse la cinta A, se graba la B, luego la C, y al llenarse ésta, se regraba la cinta A, y así sucesivamente.

La organización de la reutilización de cintas dependerá de la periodicidad del respaldo que haya adoptado la empresa. Por ejemplo si la entidad tiene una política de respaldo diaria y semanal se tendrá que disponer de 5 cintas para

almacenar la información diaria (son 5 si se consideran sólo días hábiles). Al término de la semana se va a utilizar la cinta disponible para almacenar la información semanal. Una vez que esta información es respaldada, se pueden reutilizar las cintas diarias, almacenando nueva información en ellas.

Hay algunos casos en los que existe una cinta primaria que contiene toda la información más importante que se desea respaldar y una segunda cinta que sólo guarda las modificaciones, por lo tanto solamente se regraba esta segunda cinta, ya que la primera se trata de una cinta Maestra que no será regrabada.

Nota: No use la misma cinta dos días seguidos, si su sistema falla dentro del proceso de back up, usted perderá datos almacenados en disco y cinta

7.2.1.5 Unidades Zip. La unidad ZIP es una unidad de disco extraíble, portable, barata, de bajo rendimiento; está disponible en 3 versiones: SCSI, IDE, una versión para puerto paralelo y otra para el USB. La unidad ZIP utiliza discos con una capacidad de 96 MB que tienen el tamaño de un disco de 3,5" pulgadas y sus buenas prestaciones se deben a su alta velocidad de rotación de 3000 rpm, su buffer de 256 KB y, en el caso de las unidades IDE y SCSI, su tiempo medio de búsqueda de 29 ms (milisegundos), alcanzando así una transferencia de 1,4 MB/s (megas por segundo). Una unidad ZIP, es una

unidad de almacenamiento masivo, la cual permite guardar archivos grandes que se guardarían normalmente en 15 disquetes o más, en un solo disco sin comprimir.

Otra característica importante de este dispositivo es la seguridad que éste brinda, ya que rara vez da problemas, por lo que no es necesario contar con los típicos disquetes de “por si acaso”. Una de las ventajas de copiar archivos directamente en la unidad Zip es que es posible acceder a ellos fácilmente y en cualquier momento que sea necesario, sin necesidad de realizar un procedimiento de restauración.

Esta unidad existe en formato externo e interno, con conexiones SCSI (tanto interno como externo), IDE (sólo interno), puerto paralelo. Además, la versión ZIP PLUS, permite elegir entre conexión SCSI (externa o puerto paralelo), soporta puerto USB además de los anteriores, ampliando su capacidad hasta 250 MB, siendo compatible con discos de 100 MB.

La única desventaja de este dispositivo, es que no es compatible con los discos de 3,5", por lo que esta unidad se presenta como complemento a la disquetera, no como sustituto.

El uso de unidades de ZIP como dispositivos de respaldo se considera válido en la C.U.T.B, para datos catalogados como de “baja sensibilidad” y para

efectos de archivo temporal. En caso de que un usuario decida utilizarlo como medio de respaldo permanente, será su completa responsabilidad el mantenimiento de los discos en perfecto estado, así como su revisión periódica para garantizar su funcionalidad.

7.2.2 Características del Software de Respaldo: El software de respaldo debe tener la posibilidad de correr en modo "desatendido", lo cual significa que se le pueda programar para que comience la tarea de respaldo a una determinada hora y día.

Es conveniente que el software corra en el servidor, asegurando de esta manera no solo la disponibilidad del software, sino además el menor aprovechamiento de los recursos, además de que se mejora la seguridad.

El software debe ser capaz de respaldar los derechos de los usuarios en cada directorio.

Para poder respaldar estaciones de trabajo debe tener la posibilidad de colocar "agentes" en cada una de ellas.

Debe tener capacidad de poder respaldar múltiples sistemas operativos.

Es deseable que se le pueda incluir una contraseña a cada cinta respaldada, de forma que solamente pueda restaurar los datos la gente autorizada para esta tarea.

Nuevamente esto tiene que ver con la importancia de la información que se esta manejando.

El software debe contar con facilidades de rastreo de archivos, llevando automáticamente una base de datos de cintas, con los contenidos de cada una de ellas

7.2.3 Periodicidad del respaldo. Las políticas de respaldo que se refieren a la periodicidad del respaldo consisten en cada cuanto tiempo se realiza el almacenamiento de la información deseada.

Dependiendo del grado de sensibilidad de la información administrada por una dependencia, el Departamento de informática y cómputo definirá el

procedimiento y la periodicidad para hacer copias de respaldo, la cual podrá ser:

- Diaria
- Semanal
- Mensual
- Anual

Igualmente, la frecuencia podrá ser variada dependiendo de la época, por razones de la variación en el tráfico y/o procesamiento de la información.

La institución debe realizar una combinación entre estas políticas. Pero como mínimo y lo más conveniente es contar con la ejecución de copias de respaldo semanal, debido al valor de la información que se maneja. En aquellas dependencias donde se manejan grandes cantidades de información el departamento de informática y cómputo se adoptará una combinación de estas políticas, definida por el departamento de informática y cómputo..

7.2.4 Estrategias de respaldo. Estas consisten en la forma en que se realiza la restauración de los datos. Esto puede ser completo, diferencial o incremental.

Los back-up completos, diferenciales o increméntales pueden ser combinados de varias formas.

- Un back-up total debería siempre guardarse en un lugar seguro. En un back-up total, se almacenan en la cinta todos los datos.
- Con un back-up diferencial, se almacenan los datos modificados después del último back-up total realizado. (Se almacena el documento en su versión original y el documento modificado)
- Con el back-up incremental, se almacenan todos los datos modificados desde el último back-up total, diferencial o incremental (se almacenan sólo los datos modificados desde el último back-up). El back-up incremental es más veloz pero la recuperación de datos desde una serie de back-up increméntales será más lenta.

La decisión acerca de hacer uno u otro, (diferencial o total) no es cuestión de elegir uno de ellos, sino que deben hacerse ambos, asegurándonos de esta forma que al restaurar los datos no perderemos otros.

Hacer un back-up total todos los días puede resultar muy lento, tampoco es necesario. Si todos los días se almacenan en un back-up incremental o diferencial los datos modificados, haciendo sólo un back-up total una vez a la semana se tendrá la seguridad y conveniencia necesaria en los sistemas pequeños.

Antes que nada se debe verificar que los datos del back-up puedan ser recuperados, luego se debe crear una versión histórica de los datos.

Se debe tener en cuenta las siguientes Políticas de Seguridad para el manejo de backup:

1. **Sistema financiero y contable.** Realizar una copia de seguridad diaria, guardadas en cintas diferentes. Elaborar, al final de cada semana, una copia de seguridad por semana y realizar, finalizado el mes, una copia mensual. Este procedimiento se repite cada mes. Al finalizar el año, haremos, una copia de seguridad anual, y tendremos doce copias mensuales. Para aplicar este procedimiento se requerirá un mínimo de 36 cintas.

2. **Sistema académico.** Realizar tres copias de seguridad por semana, cada una guardada en su propia cinta. Una los lunes, otra los miércoles y la última los viernes. Al final de cada mes, se realiza otra copia (copia mensual). Este procedimiento se repite mensualmente. Al finalizar el año, se tendrán doce copias mensuales, que se guardarán en el lugar adecuado que la administración disponga. Para aplicar este procedimiento se requieren 24 cintas.

3. **Servidor Ultra 10.** Realizar una copia de seguridad semanal, cada una en su propia cinta. Para aplicar este procedimiento, se requieren 4 cintas.

4. **Servidor web.** Realizar una copia de seguridad cada semana, cada una en su propia cinta. Para aplicar este procedimiento, se requiere de 4 cintas.

En total se requiere de 78 cintas para aplicar el procedimiento de copias de seguridad del sistema de información de la institución.

7.3 NORMAS PARA IDENTIFICAR MEDIOS DE ALMACENAMIENTO

1. Los archivos de datos almacenados en medios magnéticos u ópticos deben contar con un documento donde se registre:

a) Identificación del archivo, especificándose si se trata de un Archivo Maestro, Base de Datos, Archivo Primario o Archivo Temporal.

b) Identificación del Sistema o Aplicación que lo usa.

c) Frecuencia de proceso.

d) La longitud de registro del archivo (número total de caracteres por registro).

e) Factor de Bloqueo, si lo hubiera.

f) Utilitarios de compresión / descompresión si lo hubiera.

2. En el caso de medios de almacenamiento de software, se registrará la versión, número de la licencia, número de medios de almacenamiento que ocupa, si es un software que tiene un determinado número de instalaciones se registrará este número y cuantas instalaciones se han realizado hasta el momento.

3. Los medios magnéticos u ópticos (disquetes, cintas, discos), que contienen a los archivos de datos, estarán etiquetados, de manera que en la etiqueta respectiva se encuentre: el nombre de la aplicación o programa, nombre del archivo y si está empaquetado o no, así como cualquier otra

información relevante para su uso. Para el caso de las cintas magnéticas, las etiquetas también deberán contener la longitud de registro, factor de bloque, número de registros, versión y fecha de proceso.

4. Los archivos que son documentos se registrarán en un documento donde se indique:

a) Número de Dispositivo.

b) Nombre del Archivo.

c) Identificación del archivo, especificándose si se trata de un Archivo Oficio, Memo, Metodología, Informe, Convenio, Manual, Contrato, etc.

d) Asunto del documento.

e) Software en que se ha elaborado.

7.3.1 RESPALDO DE LOS ARCHIVOS

1. El personal encargado de la elaboración de los sistemas de procesamiento de datos, estimará anticipadamente la cantidad necesaria de medios magnéticos requeridos para realizar las copias de los archivos de datos y de programas.

2. Semanalmente se efectuará un respaldo de toda la información útil que se encuentra almacenada en el disco duro. Dicha actividad será realizada por el responsable designado para este fin. Los archivos que no van a ser utilizados en forma inmediata se eliminarán. Una copia de los datos importantes se harán entrega al departamento de informática y computo.

3. En los ambientes de trabajo en Red o en modo multiusuario, el administrador de la Red hará un respaldo semanal de la información útil del disco duro. Esta frecuencia podrá incrementarse a discreción del administrador, dependiendo del grado de sensibilidad de la información que en determinada época se esté procesando sobre la red.

4. Para un control de la realización de los backups se llenará un formato en el cual se tienen los siguientes campos:

a) Archivo: es la información a la cual se le va a hacer el respaldo.

b) Versión del archivo: si corresponde a la I, II o III versión. La información se almacenará como abuelo, padre, hijo. En las siguientes actualizaciones se graba primero en la versión del abuelo, reciclando la secuencia (el abuelo anterior se convierte en hijo; el hijo anterior en padre, el padre anterior en abuelo, con lo que podemos iniciar otro ciclo).

c) Medio de almacenamiento: donde va a estar almacenada la información, (disco, disquete, cinta, etc.).

d) Aplicación o Sistema: a la que pertenece la información.

e) Backup ordenado por: de acuerdo a un procedimiento que rige en la Institución o por un usuario determinado.

f) Fecha para realizar backup: de acuerdo al período que hay que realizar el backup.

g) Persona que realizó el backup: persona responsable de realizar el backup.

h) Fecha en que realizó el backup.

5. La información consistenciada y/o validada (cuando corresponda), se almacenará por versiones:

a) Versión 1: Información original de Entrada de Datos consistenciada.

b) Versión 2: Información consistenciada y validada.

c) Versión 3: Información definitiva.

6. La información almacenada en medios magnéticos u ópticos tendrán al menos una copia de respaldo (en disquetes o en otro medio de que disponga la Institución), debido a que si una de las Unidades falla, entonces se pueda recurrir al otro medio.

7. Se verificará la información que se almacene, íntegramente, tanto el original como las copias (en caso de encontrarse empaquetada, desempaquetarla como comprobación). Asimismo, debe verificarse que la información no esté contaminada con virus informático.

8. A los archivos importantes que están 100% operativos, se les sacará 2 copias, de las cuales una se almacenará en la caja fuerte y otra en uno de sus locales, como respaldo preventivo.

9. Los archivos que son textos, hojas de cálculo, gráficos, etc., mientras no se concluyan, serán almacenados en una sola copia para facilitar su almacenamiento. Una vez concluidos se debe guardar una copia adicional de respaldo en forma empaquetada o no, dependiendo del tamaño del archivo.

10. Cuando se quiera almacenar un archivo de respaldo, éste deberá guardarse físicamente en otra unidad magnética (disquete, cinta o disco) diferente a la que contiene el archivo original.

11. En el modo de trabajo monousuario, los usuarios son los responsables de hacer el respaldo de la información.

12. En el modo de trabajo multiusuario el responsable de hacer el respaldo de la información es el administrador de la red, previa orden de trabajo por parte del usuario.

7.3.2 Información Periódica

1. La información que se procesa por períodos, se almacenará por su respectivo período. Entendiéndose por período, al tiempo (mensual, bimensual, trimestral, semestral o anual) que transcurre para que se ejecute el procesamiento de la información.

2. Para el caso de la información que es determinante para el funcionamiento institucional y/o aquella que requiere almacenarse para hacer estudios o porque así lo manda la ley, se contará con el original y copia de los archivos así:

a) La información sin imputar (datos fuente, como calificaciones, asientos contables y en general transacciones individuales)

b) La información imputada (clasificada o consolidada).

c) Los archivos de procesos conducentes a generar cuadros.

7.3.3 MEDIDAS DE SEGURIDAD

1. Si se está trabajando con disquete, antes de reemplazar el medio en la unidad, siempre se debe cerrar el archivo en uso para evitar perder la información.

2. En todos los casos, de archivos almacenados en disquete, se debe en todos los casos copiarlo al disco duro y trabajar en él, una vez concluido el trabajo guarde su información a disquete y borrarlo del disco duro. Es decir, el disquete se considera exclusivamente un medio de almacenamiento.

3. Se evitará el uso de disquetes muy antiguos o guardados durante mucho tiempo (más de un año), así como los que empiezan a fallar. Todo disquete que presente fallas en su utilización debe ser diagnosticado y en caso de que se detecten sectores defectuosos u otra falla cualquiera, deberá ser descartado inmediatamente.

4. Los medios magnéticos deben estar alejados de los campos magnéticos y no se les debe almacenar o mantener cerca de cualquier cuerpo o equipo con propiedades magnéticas (como los imanes, teléfonos), ya que podrían provocar la pérdida irrecuperable de los datos ya almacenados.

5. Ningún usuario debe accionar el mecanismo de apertura de una unidad de disco, CD o DVD, o en general de cualquier medio de almacenamiento

mientras se encuentre encendida la luz indicadora de que el dispositivo está en funcionamiento activo, para evitar pérdidas de información.

6. El usuario no debe mover la CPU que contiene al disco duro cuando esté encendido, porque los cabezales de lectura-escritura pueden dañar al disco.

7. Los ambientes donde se depositan los medios magnéticos deben cumplir con las condiciones adecuadas de temperatura y no presentar humedad.

8. Los medios magnéticos en los cuales se almacenará los respaldos de la información serán completamente nuevos (primer uso), verificándose su buen estado operacional.

9. Los medios magnéticos donde está grabada la información recibirán mantenimiento de limpieza y diagnóstico de su superficie semanal.

10. Todo disco duro debe ser defragmentado con una frecuencia mínima mensual.

11. Sólo el personal responsable de la seguridad de los archivos tendrá acceso al ambiente donde se encuentren estos medios magnéticos.

12. Sólo el personal encargado de la elaboración y procesamiento del sistema y el usuario responsable del mismo podrán accesar y usar la información que está almacenada en los medios magnéticos u ópticos.

13. Antes de apagar el servidor, el supervisor debe enviar con 5 minutos de anticipación un mensaje a los usuarios para que salven su información.

8 POLÍTICAS DE SEGURIDAD DE MANEJO DE SOFTWARE

8.1 DE LA INSTALACIÓN DE SOFTWARE.

La Institución emplea tres tipos de Software:

- *SOFTWARE INSTITUCIONAL,* son los de propiedad intelectual de la Institución, que han sido desarrollados por sus estudiantes o sus empleados.
- *SOFTWARE OPERACIONAL,* son los sistemas operativos, lenguajes o Software en general que se compran a proveedores especializados y requieren licencia para su uso.
- *SOFTWARE DE DOMINIO PUBLICO,* a este grupo pertenecen las memorias de congresos, seminarios que son donados a la Institución; programas de uso público que pueden ser bajados de la Red Internet, entre otros.

8.3 IDENTIFICACIÓN DEL SOFTWARE.

Teniendo en cuenta el tipo de Software, la Institución identifica tres grupos para su utilización:

- ACADEMICA
- ADMINISTRATIVA

- APOYO DE OFICINAS.

Se deben tener las siguientes políticas de seguridad para administrar, actualizar y conservar el Software de las Institución:

a. El Departamento de Informática y Cómputo es el responsable directo de la seguridad, manejo y buen estado de operación de todo el Software, propiedad de la Institución, para lo cual debe:

- Responder porque todo el Software de la Institución tenga la debida autorización para utilizarlo.
- Mantener actualizado el inventario del Software disponible de la Institución.
- Mantener bajo su control directo todos los originales, estableciendo la protección necesaria para su correcto uso.
- Controlar la reproducción de duplicados y verificar el correcto uso de las copias que se hayan entregado a cualquier dependencia de la Institución.
- Efectuar el control las verificaciones y el mantenimiento periódico, para asegurar su correcta utilización.

b. Cada Jefe de Dependencia que tenga Software propiedad de la CUTB, deberá responder por su seguridad mantenimiento, adecuada utilización y buen uso.

c. La instalación y duplicación de toda clase de Software en la Institución debe ser hecha por el departamento de Informática y Cómputo, quien automáticamente garantiza al usuario como “licenciado”.

d. Las copias de respaldo del Software, en los casos que se establezcan estarán bajo la responsabilidad y seguridad así:

- Primera copia por el USUARIO
- Segunda copia por el Departamento de Informática y Cómputo
- Tercera copia por el Secretario General.

La actualización de las copias de respaldo del Software será hecha únicamente por el Departamento de Informática y Cómputo.

8.4 USO DE LAS LICENCIAS DE SOFTWARE

1. El departamento de informática y software no copiara software a los usuarios para los fines particulares y ajenos a la institución.

2. No se prestara el software original a los usuarios directamente, el proceso de instalación se seguirá conforme al convenio establecido por biblioteca y el área de software de servicios computacionales.

3. El usuario no deberá quedarse en posesión del software o manuales originales

4. Todo software o manual original deberá remitirse a la biblioteca para su adecuada administración

5. El software original solo podrá ser manipulado bajo la supervisión directa del área de software de servicios computacionales.

6. Los manuales originales se consideraran libros sujetos a los procedimientos de uso y cuidado propios de la biblioteca.

7. No se instalará ningún software excepto el permitido por la licencia correspondiente.

8.5 POLÍTICAS DE ACEPTACIÓN DE DESARROLLO Y ENTREGA DE APLICACIONES

8.5.1 Desarrollo y mantenimiento. Se establecen las siguientes políticas de seguridad para el proceso de desarrollo y/o mantenimiento de aplicaciones de software.

1. Detectada la necesidad de la nueva aplicación, el Directivo a cargo de la dependencia afectada elevará la solicitud correspondiente al Jefe de Servicios Informáticos para iniciar la etapa de análisis.

2. En cada caso, se conformará un equipo de trabajo para la fase de análisis, integrado como mínimo por las siguientes personas:

a) El Jefe de Servicios Informáticos

b) El programador encargado de la aplicación

c) El usuario de la aplicación.

3. Este equipo establecerá las especificaciones de la aplicación, en documento escrito, donde se deben consignar como mínimo los siguientes puntos:

a) Objetivo de la aplicación

b) Organización lógica de la aplicación donde se indiquen los módulos o subsistemas que la conforman, así como la forma en que se interrelacionan.

c) Descripción de cada uno de los procesos que la aplicación debe ejecutar. Debe incluirse por cada proceso:

- Diagrama lógico del proceso.
- Descripción de los datos involucrados en el proceso
- Documentos fuente que intervienen
- Descripción de los informes que la aplicación debe producir, tanto los informes impresos como las pantallas de salida.

d) Enlaces que deba tener la aplicación con las otras existentes. En estos casos, debe describirse el formato exacto de los datos (o tablas) que la nueva aplicación debe producir o actualizar.

e) Otros aspectos técnicos que se consideren relevantes

4. Una vez definidas las especificaciones de la aplicación, el departamento de Servicios Informáticos se encargará de elaborar el diseño de la aplicación, así como el respectivo cronograma de desarrollo.

5. Cuando existan circunstancias especiales de volumen de trabajo, urgencia de la aplicación o tamaño de la misma, el jefe de Servicios Informáticos deberá

conceptuar sobre la conveniencia de contratar mano de obra externa para el desarrollo de la misma, justificando debidamente su concepto. En tales casos el Jefe de Servicios Informáticos entregará su concepto al Director de Servicios Administrativos, quien hará la recolección de ofertas de proveedores de software, para su presentación ante el Consejo Administrativo.

6. En todos los casos el cronograma de desarrollo de la nueva aplicación deberá ser remitido por el Jefe de Servicios Informáticos a la oficina de Auditoría de Gestión, que se encargará del seguimiento respectivo. En los casos de aplicaciones contratadas con proveedores externos, el jefe de Servicios Informáticos actuará como interventor directo del proceso, sin perjuicio de la supervisión efectuada por la Auditoría de Gestión.

7. El seguimiento al desarrollo, implantación y prueba de la nueva aplicación se efectuará mediante puntos de control periódicos, establecidos al inicio del desarrollo de la misma e incluidos en el cronograma mencionado arriba. De cada reunión de control se producirá un informe de avance, suscrito por el desarrollador y el interventor, cuando se trate de puntos de control sobre la etapa de desarrollo, y por el desarrollador, el usuario y el interventor cuando se trate de puntos de control sobre la etapa de implantación y prueba de la aplicación.

8. La recepción de aplicaciones desarrolladas por proveedores externos, se hará por parte del usuario y el interventor, y causará la elaboración de un acta de entrega final, en la que conste que se han cumplido a satisfacción todos los

pasos previstos en el Procedimiento para la Entrega de Aplicaciones de Software y se ha recibido la documentación del diseño, los programas fuente en medio seguro y el manual del usuario de la aplicación. La verificación del cumplimiento de este punto corresponde al Jefe de Servicios Informáticos, en razón de que su dependencia es responsable por todo el software institucional.

8.5.2 Entrega y recepción. Se establecen las siguientes Políticas de Seguridad para la entrega y recepción de nuevas aplicaciones de software desarrolladas por el Departamento de Servicios Informáticos.

Una vez que el Departamento de Servicios Informáticos termina el desarrollo de una aplicación nueva, incluyendo las pruebas preliminares, se deberá proceder para su entrega al usuario y su puesta en funcionamiento, conforme a los siguientes pasos:

1. El Jefe del Departamento de Servicios Informáticos informa al usuario que la aplicación ha quedado terminada y lista para la etapa de pruebas.

2. En cada caso se conformará un comité de entrega de la aplicación integrado por el usuario, el Jefe de Servicios Informáticos o su delegado, y el superior inmediato del usuario que recibe la aplicación, quien actúa como interventor de la entrega. Este comité establecerá de común acuerdo el calendario para las pruebas de la aplicación en el cual se deben contemplar como mínimo las siguientes etapas:

8.5.2.1 Capacitación al usuario sobre el manejo de la aplicación. Es el proceso mediante el cual el usuario de la aplicación es informado acerca de la forma correcta de operar la aplicación, así como de los distintos aspectos relativos a su funcionamiento. Este proceso puede darse gradualmente a medida que la aplicación se va probando, y requiere la participación de Servicios Informáticos (quien capacita) y el usuario (quien recibe la capacitación).

8.5.2.2 Ejecución de la aplicación con datos reales, en paralelo con el sistema anterior para validación de los resultados. Esta etapa consiste en la ejecución de la aplicación nueva con fines de prueba, y la comparación de los resultados obtenidos con los producidos con el sistema anterior. Aunque esta etapa no es absolutamente indispensable para todas las aplicaciones, es recomendable en aquellas cuya información es particularmente crítica para el funcionamiento institucional.

8.5.2.3 Ajustes a la lógica de la aplicación que se detecten como consecuencia de las pruebas. Consiste en hacer las modificaciones que se requieran en el código de la aplicación cuando en la etapa anterior se detecten fallas a corregir o nuevas funciones a incluir.

8.5.2.4 Elaboración de la documentación de diseño de la aplicación. Toda aplicación de software deberá estar acompañada de la respectiva documentación de diseño, que contiene todas las especificaciones técnicas de los programas, estructuras de datos y demás recursos computacionales que

intervienen. Esta documentación se debe desarrollar paralelamente con la implementación de la aplicación y su versión final se almacenará en papel y en disco compacto, para respaldo y consulta. Toda nueva versión de la aplicación causará la respectiva actualización de la documentación técnica.

8.5.2.5 Entrega definitiva de la aplicación. Corresponde al acto mediante el cual el Departamento de Servicios Informáticos entrega la aplicación e incluye los siguientes productos en los diferentes casos:

a) **Cuando se trate de aplicaciones locales para el usuario.** Son aplicaciones pequeñas, generalmente en ambiente de Windows o similar, que no requieren la interacción con alguno de los servidores institucionales.

En este caso, la entrega formal incluye los siguientes productos:

- Aplicación debidamente instalada y funcionando, en el computador del usuario
- Manual del usuario de la aplicación, que puede ser en medio impreso o en formato electrónico (ayuda en línea)
- Instaladores de la aplicación en disco compacto.
- Copia de la aplicación en medio seguro (CD o DVD) con destino al archivo de software, para su aseguramiento. Una segunda copia de la aplicación deberá ser almacenada con fines de respaldo.

b) **Cuando se trate de aplicaciones Cliente-Servidor.** Son aplicaciones que residen en alguno de los servidores institucionales y que el

usuario puede consultar mediante una conexión de red, generalmente vía TELNET.

En este caso la entrega formal incluye los siguientes productos:

- Aplicación debidamente operativa instalada en el servidor.
- Nombre de Usuario (LOGIN) y clave de acceso (PASSWORD) mediante los cuales el usuario tendrá acceso a la aplicación. Estos datos son de carácter PRIVADO y deben entregarse en sobre cerrado, al DIRECTIVO A CARGO de la dependencia usuaria de la aplicación. En todos los casos, el DIRECTIVO A CARGO y el usuario, serán los responsables directos por cualquier utilización que se haga de estos datos.
- Manual del usuario de la aplicación, que puede ser impreso en papel o en formato electrónico (ayuda en línea).
- Copia de la aplicación en medio seguro (CD o DVD) que el departamento de Servicios Informáticos utilizará con fines de respaldo.

IMPORTANTE: Al terminar cada una de estas etapas, se levantará una acta suscrita por el usuario y por el Jefe de Informática y Cómputo, en donde conste la entrega a satisfacción.

3. Es responsabilidad del Departamento de Servicios Informáticos, mantener actualizada una hoja de vida de todas las aplicaciones producidas, en la cual se archivarán las actas de entrega de las mismas así como cualquier otra solicitud o documento relacionado con el mantenimiento de las mismas. De igual manera, se registrará en estas hojas de vida el personal que está a cargo

del mantenimiento de las aplicaciones, las fechas en que se han hecho las copias de seguridad y todos los demás aspectos que se juzguen relevantes.

4. Una vez que la aplicación entra completamente en la fase de producción, ésta quedará totalmente a cargo del usuario y toda actividad que requiera algún mantenimiento o reforma a la misma, deberá ser dirigida al Departamento de Servicios Informáticos, mediante solicitud escrita en la que se describa el problema a corregir, o la característica a modificar en la aplicación. El Departamento de Informática atenderá estas solicitudes en orden de llegada, excepto cuando se trate de situaciones de emergencia o con prioridad diferente que establecerá su superior inmediato.

8.6 DOCUMENTACION DE DISEÑO PARA APLICACIONES DE SOFTWARE

8.6.1 Definición. La documentación del diseño de aplicaciones de software es el conjunto de documentos que contienen las especificaciones técnicas y de organización interna de la aplicación, que sirven de referencia al programador para actividades posteriores de rediseño, modificación o ampliación de las funciones de la misma.

8.6.2 Estructura de la documentación.

1. Descripción General de la Aplicación. Consiste en una descripción general del propósito de la aplicación, los módulos en que se subdivide y el propósito de cada uno de ellos.

2. Diagramas de flujo de datos. Consiste en una descripción esquemática de la organización de la aplicación, donde se aprecien todos los procesos que la conforman, con los respectivos flujos de información, preferiblemente utilizando la conocida metodología Jordán DiMarco.

3. Diseño de la base de datos. Es una descripción esquemática detallada de la porción de la base de datos que utiliza la aplicación. En esta descripción debe incluirse:

- Modelo Entidad-Relación de la aplicación (cuando se trate de aplicaciones de base de datos)
- Descripción de las tablas que conforman la base de datos

De cada tabla debe describirse:

- Estructura del registro: nombres de campo, tipos y tamaño de los datos, descripción del contenido de cada campo
- Campos utilizados como llave.
- Archivos de índice asociados a la tabla.
- Lista completa de programas, rutinas o procedimientos que utilizan la tabla (consulta, modificación)

4. Requerimientos técnicos de la aplicación. Detalles relativos a las especificaciones mínimas que debe poseer el computador donde se corre la aplicación. Entre ellos: Memoria necesaria, tamaño de la aplicación (programas y datos), sistema operativo, bibliotecas requeridas, protocolos u otros elementos no descritos antes.

CONCLUSIONES

Este proyecto titulado ” Diseño de políticas de Seguridad para la Red de la C.U.T.B”, contiene unas normas que contemplan lo que está permitido a los usuarios dentro y fuera de la institución en materia de seguridad en computo.

De hecho en materia de seguridad lo que no se permite expresamente, esta prohibido. Pero aun así nos hemos tomado el trabajo de elaborar dichas normas con el objetivo de mantener y preservar los recursos informáticos de la institución.

Se logró establecer políticas de seguridad acorde con el estado actual y el desarrollo futuro de la red de la CUTB en cuanto a nivel usuario(profesores, estudiantes) de pregrado como de postgrado, en los diferentes puestos de trabajo, servidores, servicios, salas de informáticas y de software.

Estas políticas de seguridad establecidas en este proyecto de grado abarcan todas y cada una de las dependencias de la CUTB, con el objeto de crear lineamientos a partir de los cuales se expidan normas y reglamentos tendientes a proteger la integridad física y lógica de la red, asegurando de una manera rápida y efectiva la disponibilidad de los datos trasmitidos en ella.

Se pudo detectar que de todas formas, aun cuando no están expresamente escritas en ningún documento anterior a este, la institución ha adoptado y aplica políticas de seguridad para preservar la confidencialidad de la información que maneja cada servidor y que es transmitida por la red.

Luego del proceso de revisión detallada en las dependencias de la institución, resulta evidente que en la CUTB, muchos usuarios prefieren comportarse de acuerdo con un conjunto de reglas "sociales", mas que por las reglas específicas que se refieren al uso de la tecnología computacional.

Estas reglas motivan al respeto por la privacidad de los demás usuarios y de los ambientes de trabajo en un alto porcentaje. Pero así mismo, existe un cierto nivel de riesgo, que se hace palpable en el hecho de que no existe uniformidad de criterio entre los usuarios para el uso de los recursos de su computador.

Aunque en general los usuarios operan bajo una especie de alianza basada en la confianza, esa confianza es fácil de subvertir. Por lo tanto, la comunidad de usuarios puede ser fácilmente invadida por un atacante malicioso que intentará utilizar mal cualquier sistema en su camino. De hecho, la existencia frecuente de carpetas de disco compartidas, el tráfico de mensajes ajenos a las labores, la permanente circulación de archivos MP3 y el relativo descuido con que los usuarios administran su disco duro, es la principal fuente de contaminación por virus en los computadores de la red CUTB.

Como ya se dijo antes, todo sistema computacional debe contar al menos con un conjunto de reglas bien conocidas, documentadas y que se hagan cumplir de alguna manera, a través de las cuales se pueda garantizar la privacidad y la integridad de la información de todos los usuarios. **Las reglas deben poderse imponer pues no tiene sentido crear reglas que no puedan hacerse cumplir**. En muchos casos los usuarios están de acuerdo con que "**La justicia debe aplicarse y todos deben ver cuando se aplica**".

En el caso específico de la CUTB, la definición de las políticas de uso de los recursos contenidos en este documento es apenas el primer paso para implementar los controles que se requieren. Estas políticas deben ir acompañadas de una serie de acciones administrativas y de capacitación a los usuarios, de manera que todos interioricen la filosofía de la seguridad computacional, la importancia que tiene para cada uno y para la organización en general tener el más alto nivel de seguridad en su información, que constituye quizás uno de sus activos más valiosos.

RECOMENDACIONES

Implementar una técnica de encriptación, llámese PGP para el envío de correspondencias de las tareas, notas de parciales u otras actividades en las asignaturas de postgrado, especializaciones y maestrías.

Se debe mantener un alto nivel de concientización acerca de las políticas de seguridad establecidas en cada uno de los departamentos de la red de la cutb.

Mejorar la comunicación entre los empleados de la cutb(manga, ternera) tanto de pregrado como de postgrado, para lograr la reducción de posibles violaciones.

Implantar un proceso que proporcione un mensaje consistente y continuo sobre el programa de protección de la información de la cutb

Hacer llegar mensajes específicos a diferentes audiencias dentro de la cutb.

Asegurar que cada administrador de la información de la cutb tenga una copia de las políticas de seguridad.

Asegurar que cada usuario de la red de la cutb entienda su rol y responsabilidades en la protección de la información.

Desarrollar campeones de seguridad dentro de las áreas operativas y de soporte.

Una recomendación que se le hace al departamento de informática y computo y todas las dependencias relacionadas son que deben contar con una UPS para respaldar la energía lo que otorga un plazo suficiente para dar termina al respaldo.

Para llevar el control de software, hardware y de los incidentes de seguridad del sistema de computo de la institución, los administradores de cada área deben mantener un control de los recursos ya mencionados y reportarlos mensualmente a través de un formato estándar (ver anexos A y B).

Para efectos de agilizar y automatizar este proceso es recomendable que la recopilación de esta información sea a través de una pagina electrónica. De esta manera cada administrador captura la información en las bases de datos disponibles en web, sin tener que manejar papeles, y trasladarse para su entrega.

Estas políticas de seguridad formuladas en este documento deben ser revisadas periódicamente para su posterior actualización.

Es importante además, tomar acciones administrativas sobre los recursos computacionales, porque sus configuraciones no son uniformes y son débiles en exceso, especialmente las de aquellos equipos que soportan la actividad académica. Como mínimo, deben instalarse servidores de red, a través de los cuales se administren las configuraciones y los servicios, y se elimine el problema de la heterogeneidad en las configuraciones que es cotidiano en las aulas de informática.

Así mismo, en las oficinas, deben implementarse con urgencia reglas básicas con respecto a los mensajes de correo no relativos a las labores (humor, sexo, cadenas, SPAM, hoaxes , archivos MP3 y similares), así como el respectivo régimen de amonestaciones y sanciones para quienes las incumplan.

Por otra parte, el uso de software de mensajería en línea, estilo ICQ, MSN y similares, debe delimitarse específicamente, restringiéndolo a los usos estrictamente laborales, para evitar el desperdicio de tiempo, que supone una innegable disminución de la productividad del empleado y del estudiante. Siendo obvio que este servicio es análogo al de las conversaciones telefónicas, debe estar sujeto a consideraciones similares.

En lo referente a la navegación en internet, se recomienda regular su utilización desde los puestos de trabajo, en función de la necesidad del cargo, a juicio de la institución. Es urgente la instalación de una intranet que permita el tráfico interno de información, pero a la vez se recomienda establecer categorías de

usuarios para determinar a cada una de ellas el nivel de servicios (http, ftp, icq, kazaa, mp3, mpeg) a que tiene derecho y aplicar las restricciones de cada caso.

Finalmente se recomienda crear específicamente el cargo de responsabilidad por la seguridad computacional de la plataforma institucional, de manera que exista al menos un responsable directo de las especificaciones de seguridad, pues las labores de administración de la red no le permiten al administrador hacer una completa administración de las prácticas de seguridad en todos los puntos de la red, así como de la necesaria labor de concientización y capacitación de todos los usuarios de la red.

BIBLIOGRAFIA

COMER E. DOUGLAS, Redes de Computadoras. México: Prentice Hall Hispanoamérica S. A. 1997.

GONZALES S, Nestor. Comunicación y Redes de Procesamiento de Datos. México: Mc Graw Hill. 1995.

PC MAGAZINE EN ESPAÑOL, Edición Septiembre 2000

STALLINGS, William. Comunicación y Redes de Computación. 5 Ed. México: Prentice HALL Hispanoamérica, S. A. 1997.

STOLTZ, Kevin. Redes de Computadores. México: Prentice. 1995.

TANENBAUM, Andrew s. Redes de Computadoras. 3 Ed. México: Prentice. 1997.

INTERNET

POLÍTICAS DE SEGURIDAD EN COMPUTO INAOE.

http://

SEGURIDAD EN REDES.

- (Barcelona, España)
- (España)
- (Suiza)
- (Méjico)
-
-
- (EEUU)
- (Mundial)
- (Europeo)
- (Argentina)
- (Australia)
- (Croacia)
- (Dinamarca)
- (Estonia)
- (Finlandia)
- (Francia)
- (Alemania)
- (Islandia)
- (Italia)
-
- (Corea)
- (Polonia)
- (Japón)
- (Eslovenia)
- (Singapur)
- (KPN Telecom)
-

ANEXOS

Anexo A. Formato de Control del Hardware

FORMATO DE REGISTRO Y CONTROL DE EQUIPOS DE COMPUTO DE LA CUTB

Computadoras Personales, Estaciones de Trabajo
Y Dispostivos en Red

N°IP	Nombre	Servidores Marca/Modelo	Switches/Routers Marca/Modelo	Computadores Marca/Modelo	Procesador /Velocidad	Memoria Ram/Cache	Capacidad en Disco(s) Duros(s)	Floppy/Cinta/CD/Scanners Plotter,Impresoras	Monitor Modelo/ tamaño/tipo	S. O. /Versión	Aplicación /Servicios	Asignado	Of.
192.100.172.54	Biblioteca			Hacer	Pentium II 400 Mhz	64 Mb.	1.5 Gb.	Floppy 3.5”	AcerView SVGA 14”	Windows 98		Dr. Roberto Lora	101
192.100.172.56	Gw1		Cisco 2500							c1.2	Ruteo Exterior	Sala Principal	501
192.100.172.60	Sala principal	Ultra 10			Sun 1200 Mhz	512 Mb.	100 Gb.	Floppy 3.5”, CDROM vel 56x	Sun 19”	Solaris 2.5.1	D.N.S Sec.	Ing. Yovanny vasquez	502

Anexo B. Formato de Control de Incidentes de Seguridad

Reporte Nº _____

Fecha _____

Departamento _____

Antecedentes

1) Descripción del incidente

    a) Cómo se detectó

    b) Como se analizó el incidente

2) Describir lo que se encontró (Nombre del Software y versión, archivos, herramientas, etc.)

3) Consecuencias o daños del incidente

4) Primeras medidas en respuesta al incidente

Respuesta al Incidente

5) Recursos comprometidos (S. O, Servicios de Red, hw, etc.)

6) ¿Se detectó al intruso, interno y/o externo ?, (describir como se detectó)

7) ¿Se implementó algún recurso que bloqueara definitivamente la posibilidad de ocurrencia de dicho incidente ?. Describa lo que se hizo

8) Observaciones

Anexo C. Levantamiento de la Información

DEPARTAMENTO DE SERVICIOS ADMINISTRATIVOS

Consta de los siguientes departamentos:

1. Dpto. de Adquisición.
2. Dpto. de Recursos Humanos.
3. Dpto. de Informática y Computo.
4. Dpto. de Recursos Educativos.
5. Dpto. de Servicios Generales.
6. Dpto. de Asistente Administrativo de Control.

Información obtenida en cada uno delos departamentos.

1. DEPARTAMENTO DE ADQUISICIÓN.

Tipos de usuarios:

- Jefe
- Inventario.
- Almacenista.

Privilegios: El jefe como tal tiene mayor prioridad que los demás, el resto están al mismo nivel.

Servicios que pueden usar:

- El jefe puede usar los siguientes: Contabilidad, compra y caja menor.
- Inventario: Activo fijo, compra y almacén.
- Almacén: Almacén.

Controles: Los usuarios tienen su propia clave, la información queda guardada en el mismo sistema.

Tipos de servicios: Las funciones de cada usuario son las siguientes:

- A quienes va dirigido: Van dirigidos a Servicios Generales.
- Donde reside el servicio: En Informática y Computo.
- Quien lo administra: Márbel Márquez.

2. DEPARTAMENTO DE RECURSOS HUMANOS.

Tipos de usuarios:

- Jefe
- Auxiliar de Capacitación y de desarrollo.
- Auxiliar de Nomina.

Privilegios: El jefe como tal tiene mayor prioridad que los demás, el resto están al mismo nivel.

Servicios que pueden usar:

- El jefe puede usar los siguientes: Realiza consultas.
- Auxiliar de capacitación y desarrollo: En el sistema nuevo puede usar Cartera de los empleados, Nomina (datos básicos y estudios). En el sistema antiguo puede usar cátedra y Evaluación de Desempeño.

- Auxiliar de Nomina: En el sistema nuevo puede usar el menú de pagos. En el sistema antiguo puede usar el menú de Evaluación de profesores por estudiantes.

Controles: Los usuarios tienen su propia clave, la información queda guardada en el mismo sistema e informática y Computo.

Tipos de servicios: En el modo de Cartera, crear Deudores y Codeudores, elaborar tablas de financiación de empleados, con becas créditos o prestamos personales, elaborar tabla de condonación para los empleados con becas crédito, cambiar el DTF semestralmente a la tabla de financiación, reliquidar la tabla de financiación por abonos extraordinarios. En el modo de Nomina, alimentar la información personal de los empleados, en el programa de cátedra (software antiguo) crear el código de los profesores nuevos, elaborar la carga académica, pago a los profesores.

Funciones de cada usuario:

- Funciones de la auxiliar de capacitación y desarrollo.

1. Elaboración y trámite de los Contratos Beca-Crédito, Crédito y varios, que la Tecnológica otorga a sus empleados, el cual consta del siguiente proceso:

- Solicitud del empleado aprobada por Rectoría.
- Elaboración del Contrato, el cual consta de los siguientes anexos:
- Tablas de Financiación y Condonación (sí es Beca-Crédito)
- Carta Acta de matrícula (sí es estudio).
- Carta de compromiso
- Carta Oficina del Trabajo
- Pagaré en blanco, firmado por el empleado y un fiador

- Carta de instrucciones para llenar el pagaré
- Recoger las firmas correspondientes.
- Cambiar semestralmente (enero y julio) las tablas de financiación de acuerdo al DTF, del mercado.
- Entregar copia del Contrato y tablas de financiación y condonación al empleado, Contabilidad, Auxiliar de Nómina y DIPOS (sí es un estudio interno). Los demás documentos y el contrato original se guarda en la hoja de vida del empleado.

Nota: A los empleados que realizan curso de Educación Permanente inferior a 100 horas (Inglés, Redacción y Ortografía, Informática, etc.) y que solicitan Beca-Crédito, se le pasa una relación mensual a la Auxiliar de nómina y Contabilidad por cada curso dictado; donde se les informa la forma de financiación y la parte a condonar.

Departamentos involucrados para llevar a cavo esta función y requerimientos:

- Dirección General: envía la carta de aprobación.
- Dirección de Postgrado: suministra la información en cuanto a valor, iniciación del curso, etc. (sí es estudio interno).
- Dirección Financiera: se le envía copia del contrato y las tablas de financiación y condonación (si la hay), para que sea contabilizado.

2. Todo lo relacionado con los profesores de Cátedra:

- Elaboración de la carga Académica.
- Elaboración los Contratos semestralmente.
- Profesores nuevos:
- Asignar código
- Ingreso al sistema

- Matricularla de la cuenta en CONAVI
- Afiliarlos a la A.R.P, E.P.S, Fondos de Pensión y Comfenalco.
- Elaboración de la nómina (se les hace 4 pagos y la liquidación):
- Ingreso de novedades (Ausentismo, libranzas, embargos, etc.)
- Generación de reportes
- Elaboración de certificados.

Departamentos involucrados para llevar a cavo esta función y requerimientos:

- Decanaturas:
  - Suministra las hojas de vida de los profesores nuevos
  - Elabora los horarios de los profesores y les asigna las materias y el número de horas a dictar.
  - Firma los contratos
  - Envía el informe de ausentismo de los profesores para elaborar la nómina.
- Dirección Financiera: Se le envía la nómina y un medio magnético para el pago a través de la Gerencia Electrónica.

3. Clasificación de categorías a los profesores Cátedra y Tiempo Completo:
   - Estudio de hoja de vida.
   - Estudio de solicitud de los profesores para ascenso de categoría.
   - Elaboración de cartas a los profesores donde se les informa la categoría y los requisitos faltantes para mantenerla o ascender a una categoría superior.

   Departamentos involucrados para llevar a cavo esta función y requerimientos:

   - Aprobación del Comité de recursos Humanos.
   - Certificados del Dpto. de Idiomas, Decanatura de sistemas, etc.

4. Mantener actualizado los siguientes informes:
   - Informe mensual de la cédula de personal.
   - Informe mensual de la carga de personal
   - Informe mensual de los horarios y las funciones realizadas por los empleados de servicio, laboratorios y biblioteca.
   - Informe mensual de capacitación de los empleados en general.
   - Informe semestral de Producción Académica de los Profesionales y Docentes.
   - Informe de las personas que tienen Beca-Crédito y crédito.

   Departamentos involucrados para llevar a cavo esta función y requerimientos:

   - Informe del Jefe del Dpto. Servicios Generales y del Jefe del Dpto. de Servicios Educativos acerca de las funciones, horario y ubicación de sus subalternos.

5. Calificar, digitar y presentar informe de las evaluaciones de desempeño semestrales de los empleados no docentes de tiempo completo.

   Departamentos involucrados para llevar a cavo esta función y requerimientos:

   Cada jefe evalúa a sus empleados de acuerdo al formato suministrado por el Dpto. de Recursos Humanos.
6. Presentar el informe de los empleados (Auxiliares, Secretarias y Servicios Calificados) que tienen derecho a al incremento de sueldo en junio (Bonsal y Bonanti), de acuerdo a los resultados de las evaluaciones de desempeño.

7. Elaborar la Bonificación de Directivos (Bonadi) semestralmente.

8. Archivar todos los documentos que llegan a la Oficina de Recursos Humanos.

9. Revisar las hojas de vidas activas en el Dpto. de Recursos Humanos, cuando se soliciten candidatos para ocupar cargos solicitados por la Tecnológica, seleccionarlos y entregarlos al jefe de Recursos Humanos.

10. Todas aquellas funciones que de su naturaleza le sean asignadas por el Jefe del Dpto. de Recursos Humanos.

OBSERVACIONES: Todas las funciones desempeñadas están bajo la supervisión del Jefe del Dpto. de Recursos Humanos.

Auxiliar de Capacitación y Desarrollo: Yolenis Leguia Beleño
Jefe del Dpto. de Recursos Humanos: Armando A. Mendoza Diaz

Funciones de la auxiliar de nomina de recursos humanos.

1. Contestar teléfono.
2. Atender público.
3. Revisar y enviar correspondencia.
4. Entregar a los empleados nuevos folder que contenga:

- Copia del contrato de trabajo.
- Carta de nombramiento.
- Normas de rectoría y Reglamento de Personal

5. Elaborar contratos de trabajo a:
   - Profesores que se les paga por cuenta.
   - Empleados de Tiempo Completo o parcial.

6. Elaborar cartas de:

- Retiro de empleados o aceptación de renuncia
- Carta a fondos de cesantías para retirar empleados

- Cartas al médico para examen médico de admisión
- Cartas a la oficina del trabajo para retiro de cesantías
- Cartas a fondos para retiro de cesantías
- Cartas de traslado de empleados
- Carta de nombramiento
- Carta empleados que salen de vacaciones
- Carta al Banco Caja Social cuando el empleado solicita préstamo.

7. Elaborar afiliaciones a :
- Comfenalco
- A.R.P.
- Fondo de Salud
- Fondo de Pensión
- Fondo de Cesantías

8. Elaborar certificaciones de :
- Empleados de Tiempo Completo
- Certificación de carga académica
- Certificación de empleados retirados

9. Enviar todos los fines de mes a Rectoría y Bienestar Universitario listados de empleados que cumpleaños en el mes siguiente.

10. Nomina correspondiente a la primera quincena.
- Generar nómina
- Elaborar listado actualizado de empleados de Tiempo Completo.

11. Nomina de empleados de tiempo completo:
- Asignar código y crear en el sistema si hay empleados nuevos.
- Hacer carta Conavi solicitando apertura de cuenta
- Hacer fax a Conavi matriculando cuentas nuevas

- Revisar mensualmente los empleados que terminan libranzas.
- Crear libranzas nuevas
- Revisar y cuadrar la cuenta de Colsanitas
- Revisar y cuadrar la cuenta del Seguro de Vida
- Revisar y cuadrar la cuenta de Funeraria los Olivos
- Empleados que tengan días no remunerados descontarlos.
- Tener pendiente los empleados que cambian fondo de pensión y Salud.
- Incluir horas extras de empleados de manga, ternera y auxiliares.
- Elaborar listados de teléfono y cargos a la nómina.
- Liquidar el empleado que sale a vacaciones.
- Liquidar el empleado que regresa de vacaciones.
- Retirar de los fondos de Pensiones y Salud a los empleados que se retiren
- Atender y aclarar cualquier duda a los empleado tenga con respecto a su pago
- Revisar y entregar cuadrada al Jefe del Departamento de Recursos Humanos
- Entregarla al Director de Servicios Administrativos.

12. Cuando el empleado se retira de la tecnológica.
    - Hacer carta de retiro o aceptación de la renuncia.
    - Elaborar Paz y Salvo y hacerle seguimiento.
    - Elaborar liquidación.
    - Hacer Carta al fondo para retirar cesantías.

13. Elaborar informe de ausentismo :
    - Semana
    - Mensual
    - Semestral
    - Anual y Acumulados del año por empleado.

14. Elaborar planillas de los diferentes fondos de pensión, de las nóminas de Tiempo Completo y Cátedra, a máquina y computador, de :
    - Protección

- Porvenir
- Santander
- Colpatria
- Colfondos

15. Elaborar planillas de los fondos de salud, de las n inas de Tiempo Completo y C疸edra, a m疾uina y computador de :

- I.S.S.
- Unimec
- Sanitas
- Colmena
- Cafesalud
- SaludCoop
- Coomeva
- -Salud Total
- Cajanal
- Unicartagena

16. Procesar semestralmente las evaluaciones que realizan los estudiantes a los Docentes, procesar informe de acumulados por facultad, individual para cada docente y por asignatura.

17. Elaborar cruce de cuentas de acuerdo a las incapacidades que se presenten durante el mes, con el I.S.S. y los fondos de salud.

18. Solicitar y entregar pasajes, al empleado que van en comisión, reservar hotel y pasar al Departamento Financiero la carta de autorización de viaje para que elaboren cheque de gastos de viaje.

19. Entregar a los empleados todos los meses el volante de pago.

- cheque de Comfenaldo.
- carnet, ya sea de salud o extracto de pensión.
- Revista de Colsanitas.

20. Cancelar anualmente los intereses de cesantías y entregar a cada empleado la liquidación.

- Enviar al Departamento Financiero los listados de las cesantías con sus respectivas planillas.
- Entregar la liquidación de cesantías con intereses a los empleados que pertenecen al antiguo regimen.

Para realizar la Nómina de Tiempo Completo. necesito que las dependencias de Servicios Generales, Recursos Educativos, Auxiliares de Manga y el Jefe del Departamento que a veces tiene información de Rectoría, la entreguen el día 23 de cada mes.

Para realizar las planillas de los Fondos de Salud y Pensión, necesito que la Auxiliar de Capacitación y Desarrollo elabore la nómina de Cátedra.

Para la elaboración de las evaluaciones de los Docentes, necesito que las diferentes Decanaturas entreguen a tiempo toda las encuestas.

La Dirección Financiera depende que le entreguemos todo a tiempo.

- A quienes va dirigido: Van dirigidos a Financiera.

- Donde reside el servicio: En Informática y Computo.
- Quien lo administra: Armando Mendoza

3. DEPARTAMENTO DE INFORMÁTICA Y COMPUTO DE TERNERA.

Tipos de usuarios:

- Jefe
- Programadores (2),
- Asistente,
- Administrador de red (abrir cuenta de los estudiantes),
- Soporte en cuanto a la red (incorporación, configuración)
- Web Master (actualiza las paginas de Internet).
- Auxiliar de Nomina.

Privilegios: El jefe como tal tiene mayor prioridad que los demás, el resto están al mismo nivel.

Servicios que pueden usar: En Internet (WEB, FTP, Mail, Conexión Remota y Proxis) y la Intranet.

Controles: En cuanto a internet tenemos los controles de acceso de conexión(quienes se conectan y duración de la conexión), copias de seguridad diarias y semanales de la WEB, copias de cuenta de los usuario(cada 15 días). En cuanto a la Intranet los reportes de Financiera diariamente y registros académicos semanales.

Las funciones de cada usuario son las siguientes:

Nombre del funcionario: Willy Laza Barrios.

Cargo: Auxiliar de sistemas.

Labores: Es el encargado de administrar el nodo de internet. Sus labores incluyen las siguientes actividades:

- Crear nuevos usuarios. Consiste, básicamente, en registrar los usuarios del sistema, asignándole una cuota en disco, crear un buzón de correo electrónico para el usuario y, en general, crear las estructuras de su área de trabajo.
- Verificación de usuarios. Consiste en generar un listado de los usuarios y compararlo con un listado de estudiantes activos. Aquellos que no se encuentren en el listado de estudiantes activos, se borran del sistema.
- Soporte a usuarios. Se realiza diariamente. Con esta actividad se le brinda ayuda a los usuarios del nodo de Internet. La misma Consiste, esencialmente, en ayudarles a configurar su navegador y su conexión telefónica, para que los usuarios puedan conectarse, y disfrutar del servicio, desde sus casas.
- Mantenimiento de los servicios. Se realiza diariamente. Se verifican que los servicios de mail, web, proxy, ftp, y acceso telefónico, funcionen correctamente.
- Programación de la página web institucional. Esta actividad es prioritaria, por cuanto es la imagen de la institución en la web. Consisten en tomar el diseño elaborado por el web master, y programarlo en ASP según las características del mismo.

Nombre del funcionario: Alfredo Figueroa

Cargo: Auxiliar de sistemas

Labores: Se encarga de administrar la red institucional; administrar los equipos activos y pasivos de comunicación y los servidores de internet. Estas labores incluyen las siguientes actividades:

- Administración de los sistemas operativos. Se realiza diariamente, y su duración depende de la existencia, o ausencia, de problemas. Consiste en

verificar que los servicios estén activos y en examinar los archivos más importantes del sistema.

- Administración de los equipos de comunicación. Se realiza diariamente. La actividad consiste en verificar que los puertos de los routers estén activos, que no haya sufrido alteración la tabla de enrutamiento, y en realizar pruebas para verificar la comunicación entre éstos y los servidores. Se verifica, además, la comunicación de los switch's y el router.
- Administración de la red. Esta actividad le garantiza a los usuarios la comunicación con los servidores. Consiste en verificar las conexiones físicas, cuando hay problemas, y lógicas de los puntos de la red. Verificar que las rutas de red en los servidores sea la correcta; monitoreo diario del tráfico de la red y análisis de las bitácoras del sistema.
- Administración de la seguridad. Se realiza diariamente. Consiste en verificar las políticas de seguridad incluidas en el mecanismo de seguridad; reconfigurar las políticas de seguridad de acuerdo a las necesidades; revisar el informe de tráfico y restringir, o ampliar, los accesos a ciertos puntos.
- Administración de accesos. Se realiza mensualmente. Se elabora un informe del uso del acceso telefónico de nuestros usuarios. El informe incluye la cuenta, fecha de ingreso, hora del ingreso, duración de la conexión y dirección IP de la conexión.
- Configuración de servicios. Se realiza según las necesidades. Consiste en reconfigurar los servicios que presentan problemas.
- Instalación y configuración de software de sistema. Se realiza según la necesidad y puede durar hasta semanas. Consiste en el montaje y configuración de sistemas operativos y procesos servidores.
- Pruebas de comunicación y rutas alternas. Se deben realizar pruebas de enrutamientos para verificar la velocidad de transmisión; elaborar configuraciones alternas para probar y verificar si mejora la prestación de los servicios. Actualmente no se realiza por falta de un PC.

Nombre del funcionario: Ricardo Zapata.

Cargo: Web master.

Labores: Coordina y administra el website institucional. Incluye las siguientes actividades.

- Diseño y mantenimiento del website institucional. Se diseña y mantiene información actualizada en cualquiera de los módulos que constituyen el sitio web de la universidad.
- Desarrollo de la imagen corporativa en Internet. Desarrollar propuestas que mejoren y proyecten la imagen institucional en la web.
- Diseño e implementación de campañas de publicidad y marketing On line. Diseño de estrategias publicitarias de eventos, productos institucionales u otros, desarrollados en la web a través de banners e instrumentos de medición electrónica.
- Elaboración de los manuales de los sistemas de información Institucional. Diseña y elabora los manuales de usuarios para el software institucional.

Nombre del funcionario: Fredy Nieto Huertas.

Cargo: Analista de sistemas.

Labores: Se encarga de desarrollar el software institucional, de acuerdo con un diseño y un cronograma previamente elaborado y asignado por la jefatura de l dependencia. Este funcionario estaba desarrollando, hasta el día de Martes 27 de Marzo del 2001, el sistema financiero y administrativo de la institución. Su actividad actual incluye el desarrollo del sistema académico institucional. Proyecto que ya inició su etapa de revisión del sistema actual.

Nombre del funcionario: Hermes Trujillo.

Cargo: Asistente de Sistema.

Labores: Se encarga del diseño y desarrollo del software institucional. Actualmente es el administrador del sistema financiero y administrativo institucional, y se encuentra desarrollando el software académico de la escuela de

postgrados. Realiza actividad docente, impartiendo la cátedra de programación en Informix 4GL.

Nombre del funcionario: José Luis Guzman.
Cargo: Auxiliar de sistemas.
Labores. Este funcionario se encarga de desarrollar aplicativos institucionales. Actualmente se encuentra desarrollando el sistema de circulación y préstamo de libros de la biblioteca de la universidad.

Nombre del funcionario: Giovanny Vásquez M.
Cargo: Jefe de Servicios Informáticos.
Labores: Encargado de coordinar y administrar los procesos y recursos que se utilizan en la dependencia para la realización de las labores encomendadas. Esta labor incluye el análisis y diseño, la elaboración del plan de desarrollo y la dirección de todos los proyecto de desarrollo de los aplicativos institucionales.

Nombre del funcionario: Edwin Gonzalez Alandete.
Cargo: Auxiliar de Sistemas.
Labores: Administra y hace mantenimiento a los servicios de comunicación que se manejan en la sede de Manga. Estos servicios incluyen el SIR y One Touch.

En la sede de Manga quienes administran el DPTO de Informatica y Compúto es Edwin Gonzales y Mauricio Martinez.Los cuales tiene el deber de velar por el funcionamiento de la red.

Realizan controles de back up cuando hay rotación de equipos.

Actualmente a las salas de informática se les aplico una política de Windows 95 en donde se lleva acabo un control de los paquetes permitidos con el objeto de evitar en cada momento configurar los PC

Actualmente la CUTB es una sede virtual, tiene convenio con la UNAB, ITESM, que le permiten recibir clases satelitales.

A continuación se dan una lista de software que utilizan : Microsoft Windows 95, Microsoft Office, Winzip, Viruscan, Acrobat reader, English Discovery, Toefl, WinQSB, Matlab, Derive, Spss, Stargraph.

- A quienes va dirigido: Van dirigidos a estudiantes y profesores de pregado y postgrado.
- Donde reside el servicio: En Informática y Computo de Ternera y Manga.
- Quien lo administra: Giovanny Vásquez.

4. DEPARTAMENTO DE ASISTENTE ADMINISTRATIVO DE CONTROL.

Tipos de usuarios: Existe un solo usuario

Privilegios: Ninguno.

Servicios que pueden usar: Internet, consultar los archivos de Registro académicos, a través de permisos puede ingresar al Dpto. de Financiera, Tesorería y Personal).

Controles: la información queda registrada en el sistema.

Tipos de servicios: Las funciones del usuario: Alimentar el sistema.

- Quienes va dirigido: Van dirigidos a Financiera(la parte de cartera) y Registro.
- Donde reside el servicio: En Informática y Computo.
- QUIEN LO ADMINISTRA: Cecilia Baquero.

El departamento de Servicios Educativos no está conectado a la red y el de Servicios Generales no está sistematizado.

5. BIBLIOTECA

Tipos de usuario: Usuarios de Pregrados internos(profesores, estudiantes de la CUTB), externos(U de Cartagena, U. Jorge Tadeo Lozano Escuela Naval, Biblioteca Bartolomé Calvo) y los Auxiliares(Circulación y Préstamo). Los usuarios de Postgrado que son: Internos (profesores y estudiantes de la CUTB) y Auxiliares(Circulación).
Privilegios: Monitores(todas las areas), Club de la Excelencia, Coro, Danza, Docentes y Directivos, en cuanto a los usuarios internos de Pregrado se refieren. De acuerdo a los Auxiliares no esta definidos aun los permisos respectivos.

Servicios que pueden usar: Inventarios(Contiene toda la existencia total del numero de volúmenes de ejemplares de la biblioteca), Circulación y Préstamo (contiene los prestamos de las materias mencionadas anteriormente, controla las devoluciones de los mismo) y Procesos Técnicos(encargado de catalogar y clasificar los materiales bibliográficos anotados anteriormente, alimentar el sistema y elaborar bibliografías).

Controles: El sistema tiene el reglamento interno de la biblioteca. También arroja los respectivos permisos que debe tener cada auxiliar.

Tipos de servicios: para usuarios externos de pregrado en cualquier terminal que vea la frase Login, teclee la palabra CAES (centro de atención a los estudiantes) y aparecerá el siguiente menú

1. CENTRO DE ATENCIÓN A ESTUDIANTES.
2. CONSULTA BIBLIOGRAFICA.
3. TERMINAR.

Si escoge la opción 1, la pantalla le pedirá el código de estudiantes, obtendrá otro menú que le permite consultar lo siguiente:

a) Datos Personales.
b) Historia del estudiante.
c) Localizar Estudiante/profesores.
d) Notas parciales en el Periodo.
e) Pesum académico.
f) Sombreado Académico.
g) Evaluación Docente.
h) Finalizar.

Si escoge la opción 2 aparece en pantalla la clasificación, por Titulo,Autor,Materia; Después de haber seleccionado su opción, anote la signatura topográfica que se encuentra en la parte superior izquierda con esta información acérquese a la sección de circulación y préstamo y solicite el servicio.

Las funciones de cada usuario son las siguientes:

- A quienes va dirigido: Van dirigidos a estudiantes y profesores
- Donde reside el servicio: Biblioteca
- Quien lo administra: Roberto Lora.

IMPLEMENTACIÓN DE TECNOLOGÍAS DE INFORMACIÓN

Las nuevas tecnologías de información y las telecomunicaciones hacen que sea necesario romper el aislamiento y el esquema de autosuficiencia, pues hoy en día las bibliotecas se ubican un mundo complejo de información, en donde la mayoría de sus participantes se encuentra geográficamente distante. Es por ellos que debe combinar su papel tradicional con nuevas tareas tales como el acceso y la transferencia de la información existentes en fuentes electrónicas y virtuales. Por tal razón la biblioteca debe contar con :

- Sala con cubicúlos con Computadores conectados a Internet, para facilitar a los usuarios la investigación y la exploración de otros conceptos, además de comunicarse con otras bibliotecas nacionales e internacionales.
- Tener un catálogo en línea que incluya toda la información real que posee la biblioteca
- Debe tener computadores destinados para los usuarios con multimedia y acceso a la red institucional.
- Diseñar una Biblioteca Electrónica compuesta de texto, imágenes, sonido, etc, en soporte tales como CD-ROM, Videos, Disketts
- Diseñar una Biblioteca Virtual, la cual debe estar dotada de: Servidores de bases de datos, mecanismos de derecho de autor sobre el material incluido en la misma, Escáner, cámaras fotográficas digitales, entro otros.
- Contar con un recurso humano capacitado en estas herramientas, que sirvan de soporte técnico y soporte logístico.
- Diseñar servicios especializados, tales como: Acceso a documentos electrónicos, Alerta electrónica, Bibliografías desde la Web, Correo electrónico, Acceso a servidores de información, Reserva y Renovación de materiales en línea.

6. DIRECCIÓN FINANCIERA

Tipos de usuario: Una jefe, una tesorera de pregrado y una de postgrado, una auxiliar contable de pregrado y una de postgrado, una contadora, un control financiero, una auxiliar administrativa y financiera, una asistente administrativa y financiera de postgrado.

Privilegios: Todas están al mismo nivel de responsabilidad.

Servicios que pueden usar: El Dpto. de Financiera consta con un software llamado SIFAD, que posee las siguientes opciones: Contabilidad, Pagaduría, Compras, Cartera, Activo Fijo, Tesorería, Caja Menor, Almacén; Nomina, Generales. También poseen Window 95, Internet.

Controles: Cada usuario tiene su clave de acceso, la información queda registrada en el sistema, en el Dpto. de Informática Y Computo existe un servidor que se encarga de guardar la información diariamente.

Tipos de servicios:

Las funciones de cada usuario son las siguientes:

Funciones generales analista contable de postgrado

1. Recibir las cuentas de cobro y facturas que envía Asapo.
2. Grabar las facturas y cuentas de cobro, elaborando el respectivo comprobante de egreso.
3. Crear códigos contables de estudiantes nuevos de los programas de postgrados, según su fecha de inicio.
4. Copiar disquete con información de la caja de postgrados, generar el respectivo reporte y compararlo con el enviado por la tesorera para hacer los correctivos pertinentes.

5. Hacer las devoluciones de los cursos de inglés que no se llegan a abrir o por cualquier otro concepto.
6. Hacer la legalización de la fuente 5 correspondiente a anticipos a empleados.
7. Hacer la legalización de la fuente 17 correspondiente a las Tarjetas de Crédito institucionales (Dipos, Jemer, Jedup).
8. Hacer la legalización de la fuente 18 correspondiente a las Facturas de Postgrados.
9. Revisar los cheques de la Escuela de Ingeniería para su respectivo pago.
10. Contabilizar todas las fuentes manuales que elabora la Contadora.
11. Verificar la fuente 02 y 06 para la elaboración del Balance.
12. Revisar el informe diario de caja que genera la tesorera en la Escuela de Postgrados y Administración.
13. Realizar los anticipos o reembolsos de Caja Menor de la sede de Manga.
14. Generar el Balance General y sus anexos, el Estado de Resultados, el Balance de Prueba, el listado de retenciones practicadas y el listado del impuesto de industria y comercio mensualmente de la escuela de administración y postgrados.
15. Generar mensualmente las fuentes manuales y archivarlas en forma correcta.
16. Generar listados para las liquidaciones de los diferentes programas de postgrados, ya sean propios o en convenio.
17. Realizar mensualmente el pago del Leasing de Occidente.
18. Revisar el listado de salidas de almacén.
19. Grabar y revisar el archivo enviado por Jecof de los pagos de cursos de ingles fuente 75 y 76.
20. Elaborar informe en excel semanal para Difin de los pagos a realizar.
21. Colaborar con otras dependencias en la búsqueda de información actual y de años anteriores.
22. Archivar en forma general todos los documentos generados por contabilidad y financiera para ser clasificados y enviar a empastar.
23. Apoyar el proceso de liquidación de estudiantes de pregrado.

24. Apoyar a la Contadora en la elaboración o corrección de movimientos contables (conciliación bancaria, nómina, etc.).
25. Las demás que sean asignadas por el Jefe inmediato.

Funciones generales analista contable de pregrado

1. Recibir las cuentas de cobro y facturas que envía Asapo.
2. Grabar las facturas y cuentas de cobro, elaborando el respectivo comprobante de egreso.
3. Crear códigos contables de estudiantes nuevos de los programas de pregrados, según su fecha de inicio.
4. Copiar disquete con información de la caja de pregrados, generar el respectivo reporte y compararlo con el enviado por la tesorera para hacer los correctivos pertinentes.
5. Hacer las devoluciones de los cursos de inglés que no se llegan a abrir o por cualquier otro concepto.
6. Hacer la legalización de la fuente 5 correspondiente a anticipos a empleados.
7. Hacer la legalización de la fuente 17 correspondiente a las Tarjetas de Crédito institucionales (Dipos, Jemer, Jedup).
8. Hacer la legalización de la fuente 18 correspondiente a las Facturas de Pregrados.
9. Revisar los cheques de la Escuela de Ingeniería para su respectivo pago.
10. Contabilizar todas las fuentes manuales que elabora la Contadora.
11. Verificar la fuente 02 y 06 para la elaboración del Balance.
12. Revisar el informe diario de caja que genera la tesorera en la Escuela de Pregrados y Administración.
13. Realizar los anticipos o reembolsos de Caja Menor de la sede de Manga.
14. Generar el Balance General y sus anexos, el Estado de Resultados, el Balance de Prueba, el listado de retenciones practicadas y el listado del impuesto de industria y comercio mensualmente de la escuela de administración y pregrados.

15. Generar mensualmente las fuentes manuales y archivarlas en forma correcta.
16. Generar listados para las liquidaciones de los diferentes programas de pregrados, ya sean propios o en convenio.
17. Realizar mensualmente el pago del Leasing de Occidente.
18. Revisar el listado de salidas de almacén.
19. Grabar y revisar el archivo enviado por Jecof de los pagos de cursos de ingles fuente 75 y 76.
20. Elaborar informe en excel semanal para Difin de los pagos a realizar.
21. Colaborar con otras dependencias en la búsqueda de información actual y de años anteriores.
22. Archivar en forma general todos los documentos generados por contabilidad y financiera para ser clasificados y enviar a empastar.
23. Apoyar el proceso de liquidación de estudiantes de pregrado.
24. Apoyar a la Contadora en la elaboración o corrección de movimientos contables (conciliación bancaria, nómina, etc.).
25. Las demás que sean asignadas por el Jefe inmediato.

Funciones tesorera de ternera

1. Recibir diariamente todos los ingresos de dinero a la institución.
2. Efectuar diariamente las consignaciones de esos ingresos.
3. Despachar el mensajero con todas las diligencias de banco.
4. Elaborar cartas a los bancos sobre créditos, CDT, traslados.
5. Efectuar las consignaciones de los cheques posfechados.
6. Hacer llamadas telefónicas a deudores de cheques posfechados.
7. Fichar, sellar y registrar en libros todos los cheques que gira la CUTB.
8. Efectuar los pagos por servicios, Leasings, etc.
9. Efectuar informes de movimientos de caja diario.
10. Enviar pagos de fondos de cesantías, ISS, Comfenalco, etc.
11. Enviar consignaciones de embargos a bancos Agrario.
12. Recibir las llamadas de deudores y proveedores.

13. Efectuar consignaciones a proveedores, profesores.

Funciones de la asistente del dpto administrativo y financiero de postgrado.

1. Crear la deuda a cada uno de los estudiantes en el SIFAD modulo de cartera por cada uno de los ciclos de los diferentes programas.
2. Conciliar de los Informes Contables con la cartera de postgrado y reporte de cambios o correcciones a contabilidad.
3. Revisión y control de pago honorarios de los profesores de Maestrías, especializaciones, diplomados, seminarios y cursos de ingles.
4. Revisión y control de las horas extras del personal de biblioteca y computo para su envío a Recursos Humanos.
5. Revisión y control de los gastos de Caja Menor.
6. Revisión y control de las facturas de cobro de la corporación elaboradas por TESORERA de MANGA.
7. Revisión y control del movimiento de la fotocopiadora de biblioteca Postgrados.
8. Control de la fecha de inicio de los diferentes programa para enviar JERAC la información necesaria para la elaboración de los recibos de pago de los estudiantes para los ciclos de los diferentes programas.
9. Entrega de recibos de matriculas a estudiantes para su pago.
10. Control y seguimientos de pago a cada uno de los estudiantes.
11. Informe de cartera mensual para DIFIN.
12. Envío de información a JERAC de las personas que realmente cancelaron su ciclo para actualización de los listados de clases.
13. Conciliación y listados de inscripciones de los diferentes programas que se manejan en postgrados para envío a contabilidad.
14. Manejo del procedimiento de Covinoc para los pagos de las matriculas de postgrado.
15. Elaboración de certificados a los estudiantes.

Funciones de la contadora:

1. Revisar la fuentes 1 y 12 que pasa tesorería ingresos y consignaciones hacer las correcciones respectivas, que tiene incidencia en las 3 escuelas.
2. Contabilizar en fuentes mensuales 7,11,25,18,45 según corresponda a la información y cartas adjuntas en los movimientos de caja.
3. Colocar los códigos contables a las facturas expedidas por la CUTB y pasar a la auxiliar para la digitación.
4. Contabilizar los ND y NC según los extractos bancarios.
5. Contabilizar los pagos a los créditos de conavi y Davivienda, asi como los valores cargados en el mes por UVR e intereses.
6. Contabilizar la diferencia en cambio en monedas extranjeras al final del mes.
7. Contabilizar los descuentos de nomina mensual sobre los créditos por estudios y anticipos y otros.
8. Contabilizar las condonaciones sobre los estudios a los empleados.
9. Contabilizar la información dada por la niña de inventarios sobre los muebles elaborados en carpintería en el mes.
10. Revisar las fuentes 7,8 y 23. Nomina y ajustar los valores de los descuentos de salud y pensión a los valores slg. relación de pagos.
11. Contabilizar los pagos de cartera que aparecen en la gerencia electrónica y no entran a contabilidad.
12. Revisar el balance de prueba por escuela y el consolidado y hacer las respectivas correcciones.
13. Contabilizar las liquidaciones de los convenios.
14. Crear centro de costos programas de postgrado generalmente.
15. Elaborar el flujo de efectivo.
16. Contabilización de los cargos diferidos.
17. Contabilización amortización matriculas.

Funciones de la tesorería – manga:

1. Recibir pagos en efectivo (mínimos hasta $ 40.000), cheques al día y posfechados , tarjetas de crédito y débitos y pagos en general.
2. Recibir los cheques posfechados de covinoc enviados por asapo .
3. Consignar los cheques posfechados de covinoc a la fecha establecida
4. Enviar los cheques devueltos del banco a covinoc para su cobro jurídico
5. Elaboración de las facturas de postgrados y enviarlas.
6. Seguimiento y cobro de las facturas de postgrados.
7. Enviar movimiento de caja diario a ternera
8. Cuadre de caja y consignar diario lo recibido.
9. Elaborar los recibos de pago de conavi por valores mayores de $ 40.000
10. Manejo de la gerencia electrónica de los pagos recibidos diariamente.
11. Elaborar y enviar reporte de caja y gerencia electrónica a cartera.
12. Elaborar y enviar reporte del seguimiento de cheques posfechado y cobro de facturas a difin, jecof y asapo.
13. Elaboración cuentas de cobro de los profesores de postgrados (especializaciones, maestrías diplomados y cursos de ingles por fin de semana).
14. Elaboración de contratos de profesores de postgrados (especializaciones, maestrías diplomados y cursos de ingles por fin de semana).
15. Reserva de tiquetes aéreos y hotelero (hacer reserva, elaborar y enviar carta)
16. Recibir correspondencia externa y enviar a secretaria de postgrado.
17. Recibir llamadas para información general y de tesorería.
18. Elaborar conciliación mensual de los cursos de ingles , llevar control de la misma y enviar a difin.
19. Legalizar la caja menor de postgrados
20. Legalizar formularios de inscripciones de postgrados y enviar al dpto. De mercadeo.
21. Atención al publico
22. Entregar los cheques de pago a proveedores y pago electrónico a los profesores de postgrados cada fin de semana para legalizar contrato y cuentas
23. Entregar listas a los profesores de posgrados

24. Enviar a contabilidad todo lo relacionado con la tesorería para control y balance (notas débitos, consignación de baucher tarjetas de créditos, consignaciones de los cheques posfechados de covinoc, consignaciones de pagos de facturas etc.)
25. Archivo

Funciones del dpto. de control financiero:

1. El Dpto. de Control depende jerárquicamente del director Financiero y es el responsable de planear, dirigir y controlar los procesos relacionados con:
2. Control contable financiero.
3. El presupuesto.
4. Los Costos.
5. La facturación y Cartera.
6. Son funciones del Dpto. de Control Financiero:
7. Responder por el proceso y sistema de control de todos recursos financieros de La Tecnológica.
8. Verificar que las Ordenes de compra, factura, salidas de almacén, cheques y demás documentos soportes de la contabilidad cumplan con las normas legales y con las reglamentaciones establecidas por la Tecnológica.
9. Dar soporte y asistencia al sistema de control de existencias y consumo de almacén y realizar inventarios físicos de verificación con la frecuencia que se establezca.
10. Ejecutar el proceso de recaudo por matriculas y otros servicios prestados, verificar y evaluar sus resultados.
11. Analizar y verificar los reportes de la conciliación bancaria de ingresos por matriculas y suministrar oportunamente la información correspondiente de Costo Y presupuesto.
12. Elaborar, analizar y evaluar el estudio de costo para cada periodo académico.

13. Desarrollar y mantener actualizadas las normas, sistemas y procedimientos administrativos, los manuales de presupuesto, contabilidad, costo, procurando su difusión y conocimiento, asegurándose de que su aplicación se haga de acuerdo con las normas legales vigentes.
14. Desarrollar, proponer mantener actualizadas las formas y documentos que operen en el departamento y crear las no existente.
15. Cumplir los procedimientos, normas y reglamentos vigentes.

- A quienes va dirigido: vicerectoria.
- Donde reside el servicio: En el dpto. de Informática y Computo.
- Quien lo administra: Alba Zulay Cárdenas

SALA DE INFORMÁTICA DE TERNERA

Tipos de usuarios:

- Profesores(oficina)
- Estudiantes
- Auxiliar
- Celador.

Privilegios: Profesores, estudiantes, auxiliar y celador.

Servicios que pueden usar: Internet, Windows 95,tienen acceso a toda la red de la C.U.T.B.

Controles: carné, vigilar a los estudiantes. En la oficina principal solo se admiten con permiso previo del decano.

Tipos de servicios:

- Quienes va dirigido: Estudiantes y profesores de la institución.
- Donde reside el servicio: En la misma sala.

- Quien lo administra: Humberto Marbello y Wilman Escorcia.

SALA DE INFORMÁTICA DE MALOKANET

Tipos de usuarios:

- Profesores
- Estudiantes
- Auxiliares (3)

Privilegios: profesores, estudiantes, auxiliar .

Servicios que pueden usar: Internet, Windows 95.

Controles: carné, vigilar a los estudiantes, una planilla donde se registra la hora, el PC y la hora de duración. También van ha implementar las políticas de Windows 95 que se aplicaron en Manga.

Tipos de servicios

- Quienes va dirigido: Estudiantes y profesores de la institución.
- Donde reside el servicio: En el Dpto. de informática y computo.
- Quien lo administra: Aminta Quiñónez

DEPARTAMENTO DEL MEDIO UNIVERSITARIO

Tipos de usuarios:

- Director
- Secretaria.
- Asistente de integración (2).

- Dpto. de relaciones universidad sociedad.
- Dpto. de Deporte.
- Dpto. de servicio a la comunidad.

Privilegios: Todos al mismo nivel, excepto el director, el dpto. de relaciones es el único que cuenta con servicio de internet.

Servicios que pueden usar: Windows 95.

Controles: los equipos no tienen claves de acceso, no esta red, la infraestructura de los equipos es obsoleta, no existen antivirus en cada PC. La información la guardan en el disco duro.
Nota: existe un software de egresados que no funciona.

Tipos de servicios

- A quienes va dirigido: Comunidad universitaria, estudiantes y profesores de la institución.
- Donde reside el servicio: En la Dirección del Medio Universitario.
- Quien lo administra: Nelson Gutiérrez.

DEPARTAMENTO DE IDIOMAS (TERNERA)

Tipos de usuarios:

- Un solo usuario.

Privilegios: Ninguno.

Servicios que pueden usar: Internet, Windows 95, tienen acceso a financiera a través del Internet y el software de idiomas.

Controles: Todo queda guardado en el sistema y en Informática y Computo, también para acceder al sistema se tiene que digitar una clave.

Tipos de servicios:

- Todo lo relacionado con la inscripción y matriculas de los diferentes cursos.

DEPARTAMENTO DE IDIOMAS (MANGA).

Tipos de usuarios:

- Jefe del Dpto. de idiomas y una secretaria.

Privilegios: Ninguno.

Servicios que pueden usar: Internet, Windows 95,tienen acceso a financiera a través del Internet y el software de idiomas que esta conectado don el de centro de idiomas de Ternera, también se puede comunicar con registro académico.

Controles: Todo queda guardado en el sistema y en Informática y Computo, también para acceder al sistema se tiene que digitar una clave.

Tipos de servicios:

- Todo lo relacionado con la inscripción y matriculas de los diferentes cursos.

Los servicios van dirigidos en la línea de coordinación Gustavo Ramírez, y en la línea de mando vicerectoria. Margarita Saravia es la Administradora.

POSGRADOS

Lo conforman cuatro dependencia que son:

1. DIRECTOR DE LA SEDE DE MANGA
2. OFICINA DE ESPECIALIZACIONES(YANET CEDEÑO)
3. OFICINA DE EDUCACION PERMANENTE.
4. MAESTRIA.
5. SECRETARIA.

Tipos de usuarios:

- Jefe del Dpto.

Privilegios:

Servicios que pueden usar: tiene acceso a toda la red como son: el Internet, Windows 95, Dpto de Maestria, direccion de Manga, Dpto de idiomas, Dpto de Educación Permanente, Dpto de Especializaciones, Mercadeo, Secretaria de Posgrado, Tesorera de Posgrado Conexión con Pregrado.,Salas de informáticas.

Controles: Su PC no tiene clave de acceso y la información queda registrada en el disco duro. Realiza copias de seguridad en disket.

Tipos de servicios:

- Quienes va dirigido: Vicerectoria.
- Donde reside el servicio: En el Dpto. de informática y computo de Manga.
- Quien lo administra: Víctor Espinosa.

DPTO DE EDUCACION PERMANENTE

Tipos de usuarios:

- Jefe del Dpto.

Privilegios:

Servicios que pueden usar: tiene acceso a toda la red como son:el Internet, Windows 95, Dpto de Maestria, direccion de Manga, Dpto de idiomas, Dpto de Educación Permanente, Dpto de Especializaciones, Mercadeo, Secretaria de Posgrado, Tesorera de Posgrado Conexión con Pregrado.,Salas de informáticas.

Controles: Su PC si tiene clave de acceso y la información queda registrada en el disco duro.Tambien informática y computo le realiza copias de seguridad .

Tipos de servicios:

- Quienes va dirigido: Vicerectoria.
- Donde reside el servicio: En el Dpto. de informática y computo de Manga.
- Quien lo administra: Viviana Londoño.

DPTO DE ESPECIALIZACIONES

Tipos de usuarios:

- Jefe del Dpto.

Privilegios:

Servicios que pueden usar: tiene acceso a toda la red como son: el Internet, Windows 95,Dpto de Maestria, direccion de Manga, Dpto de idiomas, Dpto de

Educación Permanente,Dpto de Especializaciones, Mercadeo, Secretaria de Posgrado, Tesorera de Postrado Conexión con Pregrado.,Salas de informáticas.
Esta conectada a la red las 24 horas, se comunica con los conferencistas, estudiantes de especialización, directivos de cada facultad, estudiantes externos de postrado.

Controles: Su PC si tiene clave de acceso y la información queda registrada en el disco duro. Tambien informática y computo le realiza copias de seguridad .La información la guarda en medios magnéticos.

Tipos de servicios:

- Quienes va dirigido: Vicerectoria.
- Donde reside el servicio: En el Dpto. de informática y computo de Manga.
- Quien lo administra: Yaneth Cedeño.

CORPORACION UNIVERSITARIA TECNOLOGICA DE BOLIVAR

ESCUELA DE POSGRADOS

MANUAL DE PROCEDIMIENTOS DEL DEPARTAMENTO DE ESPECIALIZACIONES

OBJETIVO:

Establecer los procedimientos del departamento de Especializaciones para proporcionar el apoyo administrativo a las facultades en la ejecución y el control de las actividades académicas de: las Especializaciones en convenio (presenciales y virtuales)

- E. En convenio: Presenciales y virtuales
- E. Propias

.

RESPONSABLES:

La Jefe del departamento de Especializaciones, las Facultades y los Coordinadores Académicos de las Especializaciones.

I. PROGRAMACION ACADEMICA Y A ASIGNACION DE DOCENTES PARA LAS ESPECIALIZACIONES

OBJETIVO: Elegir y someter a aprobación el programa de Especializaciones que cumpla con las expectativas de los profesionales.

DESCRIPCION

En la primera semana del mes de Octubre se efectúa una reunión con:

- Decanos de cada una de las facultades
- La jefe del Departamento de Mercadeo
- La jefe del Departamento de Especializaciones.

1.JEFE DEL DEPARTAMENTO DE ESPECIALIZACIONES:

Presenta informe sobre las Especializaciones realizadas y los comentarios recibidos de egresados y estudiantes de las Especializaciones ofrecidas en el año en curso para someterlas a un análisis académico de actualización mejoramiento continuo de los contenidos que respondan y estén acordes con las necesidades de cambio que necesitan las organizaciones.

2.DECANOS Y COORDINADORES ACADÉMICOS

Analizan la respuesta y el comportamiento en el mercado laboral para considerar la posibilidad de ser ofrecida nuevamente o dejar un tiempo prudencial para volverla a ofrecer en otro año.

Se analizan propuestas de los decanos, de nuevos programas de Especialización de acuerdo con las necesidades de sus facultades y se estudia la posibilidad de ser ofrecida en convenio o crearla directamente para ser aprobada por el ICFES.

3. JEFE DEL DEPARTAMENTO DE MERCADEO

ELABORACION DE LA INVESTIGACION DE MERCADEO

Previo estudio del medio, realiza una investigación de mercado, donde registra todos los programas (actuales y propuestos) que van a manejar en el semestre (máximo 12). Identifica las necesidades.

4. SECRETARÍA GENERAL

REVISION DE LA INVESTIGACON

Recibe la investigación de mercadeo, lo revisa y emite su aprobación o no, para enviarlo nuevamente al Jefe de Mercadeo.

5.DEPARTAMENTO DE ESPECIALIZACIONES

REVISION DE LA INVESTIGACION

Recibe la investigación de secretaria general ya autorizada, la revisa y emite su aprobación. Y se la comunica a los Decanos.

6.DECANOS

ELABORACION DE ESTRUCTURA ORGANICA

Recibe la notificación del jefe del departamento de Especializaciones y elabora la estructura académica del programa, para presentarla al Consejo Superior, quien emite su concepto de aprobación o no.

7. CONSEJO ACADÉMICO

EMISION DE CONCEPTO

Revisan la estructura y emiten su juicio sobre ella. Si se aprueba, el rector firma el documento y lo entrega al Director Académico.

8. DIRECTOR ACADÉMICO

ENVIO DE ESTRUCTURA

Normaliza la estructura, de acuerdo con los requisitos exigidos por el ICFES, para luego enviarla a ellos.

9. ICFES

ESTUDIO DE ESTRUCTURA

Recibe la estructura académica del Programa, y emite su aprobación o no. Envían respuesta al rector.

10. RECTOR

RECEPCION DE INFORME

Recibe la respuesta del ICFES e informa al jefe del departamento de Especializaciones.

11. JEFE DEL DEPARTAMENTO DE ESPECIALIZACIONES

Recibe la respuesta y si es aceptada lo envía al departamento de mercadeo.

II. PROCESO DE PUBLICIDAD

1.JEFE DE MERCADEO

ESTRUCTURA DE PUBLICIDAD

Recibe, del jefe del departamento de Especializaciones, Si la especialización es nueva recibe la notificación sobre el estudio del programa. Si es aprobado por el ICFES, recibe la estructura académica y se le envía al jefe del departamento de Especializaciones junto con el nombre del nuevo programa, los costos (de acuerdo con lo presupuestado), el calendario académico, la técnica de publicidad, entre otros.

Si la Especialización ha sido ofrecida y no tiene cambios académicos, obtiene la información de los folletos anteriores.

2. JEFE DEL DEPARTAMENTO DE ESPECIALIZACIONES

Recibe de mercadeo todo la estructura, revisa y lo devuelve a mercadeo.

3. JEFE DE MERCADEO

Recibe la estructura del jefe del departamento de Especializaciones y lo envía al Jefe de Comunicaciones para el diseño de la folletería y le solicita a la Jefe de Adquisiciones presentar ante el Comité de Compras la autorización para la impresión de los folletos.

4. JEFE DE COMUNICACIONES

ELABORACION DE TECNICA

Elabora las diferentes técnicas de publicidad, de acuerdo a lo solicitado por el Jefe de Mercadeo, para su posterior envío.

5. JEFE DE ADQUISICIONES

Informa al Jefe de Especializaciones los resultados de la solicitud.

6. JEFE DE COMUNICACIONES

Envía un diseño del folleto al Jefe de Especializaciones para su estudio y aprobación del contenido del folleto.

7. JEFE DE ESPECIALIZACI0NES

Emite comentarios y se lo envía al Jefe de Mercadeo para que emita sus comentarios en cuando al diseño del folleto y al Coordinador académico interno del programa.

8. JEFE DE MERCADEO

Emite comentarios y se lo envía al Jefe de Especializaciones quien remite este al Coordinador Académico para su visto bueno.

9. COORDINADOR ACADÉMICO INTERNO

Emite comentarios y se lo envía al Jefe de Comunicaciones.

10. JEFE DE COMUNICACIONES

Recibe los comentarios, realiza los últimos ajustes del diseño y contenido del programa. Posteriormente este ya listos, se lo envía a la Jefe de Adquisiciones, para que esta cotice con los proveedores y los hagan.

11. JEFE DE ADQUISICIONES

Envía los folletos al Jefe de Especializaciones.

Envía los folletos al Departamento de Mercadeo para ser utilizados en la promoción y venta del programa.

III. PROCESO DE MERCADEO

1. JEFE DE MERCADEO

MANIFESTACION DEL PROGRAMA

Da a conocer el programa propuesto utilizando la base de datos de mercadeo (egresados, profesores externos, empresas, entre otros). Envía información a cada empresa de la ciudad.

Si el programa no brinda los resultados esperados, termina el procedimiento con las matrículas e inscripciones de los aspirantes.

2. JEFE DE ESPECIALIZACIONES

Apoya al departamento de Mercadeo, realizando visitas a las empresas y profesionales interesados en la Especialización.

3. MERCADEO

Emite al Jefe de Especializaciones el balance del programa.

Los siguientes son los aspectos que se presentan:

- Población en estudio(base de datos, fuente)
- Numero de personas interesadas en el programa
- Número de personas desinteresadas
- Número de personas que no respondieron
- Número de personas descartadas
- Número de personas inscritas
- Número de personas matriculadas
- Número de personas por trabajar

4. JEFE DE ESPECIALIZACIONES

Estudia los resultados del balance y refuerza el mercadeo del mismo.
Solicita a la Tesorería un reporte del número de personas inscritas en el programa, para proceder a reconfirmar profesores.

5. TESORERÍA

Emite reporte a la Jefe de Especializaciones

6. JEFE DE ESPECIALIZACIONES

Solicita a la Jefe Administrativa y Financiera un reporte en cuanto al estado del programa:

- Número de personas Matriculadas en el programa

7. JEFE ADMINISTRATIVA Y FINANCIERA

Emite su reporte a la Jefe de Especializaciones y da sus comentarios sobre la apertura del programa.

8. JEFE DE ESPECIALIZACIONES

Estudia el balance y los reportes financieros y teniendo en cuenta los resultados de estos decide dar inicio, aplazamiento o la eliminación del programa.
Se presentan tres casos específicos:

- Inicio del programa
- Aplazamiento
- Eliminación

➢ Inicio del Programa

9. JEFE DE ESPECIALIZACIONES

Le reconfirma las fechas a los conferencistas de las materias por escrito y les envía un formato por fax para que lo diligencie con fin de efectuar los pagos por gerencia electrónica .

IV. INSCRIPCION Y MATRICULA de ESPECIALIZACIONES

OBJETIVO: MANEJAR DE UNA FORMA ORGANIZADA Y CLARA LAS INSCRIPCIONES DE LOS ESTUDIANTES PARA ASÍ LLEVAR UN CONTROL.

DESCRIPCION: Informar el valor de matricula de cada programa, la forma de pago y las fechas limite de cancelación de matriculas.
Teniendo en cuenta que las Especializaciones en convenio tienen un valor diferente a las propias.

INTERESADO

Solicita información en el Departamento de Mercadeo sobre el programa de su interés.

ASISTENTE DE MERCADEO

Suministra información general del programa.
Entrega Formulario de Inscripción para que el interesado lo diligencie y posteriormente lo entregue a Tesorería.
Remite al interesado a Tesorería para que efectúe el proceso de pago.

INTERESADO

Se remite a la Tesorería e informa la forma como pagará la Inscripción: Efectivo o Tarjeta de crédito

TESORERA

Si el interesado va a realizar el pago en efectivo, genera comprobante de pago de inscripción, indicando la entidad bancaria recaudadora donde se debe efectuar el pago.

Si el interesado va a realizar el pago con tarjeta de crédito, genera el recibo de caja correspondiente y recibe el pago.

Informa al interesado, que después de efectuado el pago, ya sea en la Entidad Bancaria o en la Tesorería de la institución, debe legalizar el pago presentando una copia del comprobante de pago cancelado y el Formulario de Inscripción diligenciado.

INTERESADO

Cancela el valor de la inscripción en la Tesorería si es con tarjeta de crédito o en la Entidad Bancaria asignada.

Legaliza el pago en la Tesorería de la institución, presentando la copia del comprobante de pago cancelado y el Formulario de Inscripción diligenciado.

TESORERA

Legaliza la inscripción del interesado y le informa que posteriormente se le citará para el proceso de admisiones.

Sella el Formulario de Inscripción colocando el código asignado al inscrito, la fecha de pago y su firma.

Envía Formulario de Inscripción sellado y copia del comprobante de pago cancelado a Mercadeo.

ASISTENTE DE MERCADEO

Recibe Formulario de Inscripción sellado y copia del comprobante de pago para actualizar el reporte de control de inscritos y archiva temporalmente.

Cerradas las inscripciones al programa en cuestión, remite por escrito todos los Formularios de Inscripción legalizados a la fecha a Registro Académico para grabación de información de los inscritos.

REGISTRO ACADEMICO

Recibe del departamento de Mercadeo los Formularios de Inscripción legalizados y graba la información de cada uno de los inscritos.

Solicita a la Asistente de Control Financiero las fechas y valores de matricula ordinaria y extraordinaria y la entidad bancaria seleccionada para realizar el recaudo y el número de la cuenta, a fin de generar las liquidaciones de matricula.

CONTROL FINANCIERO

Informa por escrito al Asistente de Registro Académico las fechas y valores de matricula ordinaria y extraordinaria y el nombre de la entidad bancaria seleccionada y el número de la cuenta.

ELABORACION DE COMPROBANTE DE PAGO

Elabora los “comprobantes de pago – Liquidación de Matricula” de cada inscrito en original y tres copias.

(Original: corporación bancaria, 1º copia para el estudiante, 2ª copia para Tesorería y 3ª para contabilidad).

Envía los comprobantes junto con un mosaico (nombre, dirección, teléfono) de cada estudiante al asistente administrativo de posgrado.

REGISTRO ACADEMICO

Graba en el sistema las fechas y valores de matricula ordinaria y extraordinaria y el nombre de la entidad bancaria y el número de la cuenta.
Espera los resultados del proceso de admisiones y por consiguiente el listado de admitidos, a fin de proceder a generar las liquidaciones de matricula en bloque.
Entrega las liquidaciones de matricula a la Asistente de Control Financiero remite a la Asistente de Control Financiero. Para que esta reciba información detallada de las diferentes modalidades de pago (pago por ciclos, Sistema Covicheque, Tarjeta de crédito, entre otros.)

CONTROL FINANCIERO

Recibe liquidaciones para entregar a cada interesado.
Suministra información a los interesados sobre las diferentes modalidades de pago(por ciclos, sistema Covicheque, tarjeta de crédito, entre otros.)

INSCRITO

Cancela según la modalidad de pago seleccionada.

TESORERA

Verifica diariamente por el Sistema de Gerencia Electrónica los recaudos de matriculas del programa, genera reporte e identifica por el código asignado a los inscrito, quienes realizaron pago.

Envía esta información a la Asistente de Control Financiero para que actualice la conciliación mensual de matriculas. Así mismo, envía copia de este reporte a la Jefe del Departamento de Especializaciones y de Mercadeo para actualización del reporte de matriculados.

CONTROL FINANCIERO

Finalizado el proceso de matricula, envía a Registro Académico listado de personas que pagaron matricula, con el fin de que se genere el listado definitivo de matriculados.

REGISTRO ACADEMICO

Recibe información de Control Financiero y genera el listado definitivo de matriculados para el control de asistencia y reporte de notas.

V. COORDINACION ACADEMICA

La coordinación académica puede ser de la siguiente manera:

A. Con un Coordinador Académico externo y otro interno nombrado por la facultad.
B. Con la coordinación de la facultad académica y un Coordinador Académico Interno.

A. COORDINADOR ACADÉMICO EXTERNO

Envía la estructura del programa a la Jefe de Especializaciones

1.JEFE DE ESPECIALIZACIONES

Analiza la estructura del programa bajo los lineamientos que se le plantearon al Coordinador Académico, expone sus comentarios y se la envía al Decano de la Facultad en el área específica tema.

2. DECANO

Asigna de su Facultad un Coordinador Académico Interno para que realice durante el desarrollo de este, el control, seguimiento y evaluación.

B. COORDINADOR ACADÉMICO INTERNO

(Ver anexo) Funciones

1.COORDINADOR ACADÉMICO INTERNO

Emite comentarios del programa al Jefe de Especializaciones

2. JEFE DEPARTAMENTO DE ESPECIALIZACIONES

Recibe los comentarios expuestos por el Coordinador Académico Interno y emite un comunicado al Coordinador Académico Externo, donde le informa si esta estructura fue aceptada o los cambios sugeridos para hacerle.

3. COORDINADOR ACADÉMICO EXTERNO

Recibe los comentarios expuestos por la Jefe de Especializaciones, sean de aprobación o de sugerencias para mejorar.

Si es de aprobación se programa la fecha de iniciación, si no es aprobada la estructura se repite nuevamente el mismo proceso hasta que esta sea aprobada por el Jefe de Especializaciones y el Coordinador Académico Interno de la Institución.

4. JEFE DEPARTAMENTO DE ESPECIALIZACIONES

Envía la estructura académica del programa al coordinador académico interno.

Recibe la información e inicia las gestiones de planeación del programa, realiza propuesta de presupuesto del programa bajo unos parámetros establecidos por la dirección de la Institución y envía propuesta de presupuesto del programa al Vicerrector para su información y Visto Bueno.

5. VICERRECTOR

Emite comentarios al Jefe de Especializaciones

6. JEFE DE ESPECIALIZACIONES

Envía un memorando al Departamento Financieros donde solicita la apertura del centro de costo para el programa.

7. JEFE DE ESPECIALIZACIONES

Envía una copia del presupuesto aprobado a la Asistente Administrativa y Financiera, para su archivo e información.

Anexa la programación académica la Especialización.

8. JEFE DE ESPECIALIZACIONES

Convoca semanalmente a Mercadeo para hacer evaluar el balance del programa, diagnóstico o situación de este.

9. JEFE DE ESPECIALIZACIONES

ELABORACION DE PROGRAMA ACADEMICO

Elabora de acuerdo con la decanatura respectiva y el coordinador académico interno y externo; el calendario académico de las especializaciones con la asignación de los docentes de cada materia y los envía a registro académico y a la dirección financiera.

Le envía a Financiera (ternera y manga) y Tesorería, un formato con la programación académica y los datos de los profesares de cada materia diligenciados y firmados por ellos.

10. JEFE DE ESPECIALIZACIONES

Le envía al Departamento Mercadeo la programación de la Especialización.

11. DEPARTAMENTO DE MERCADEO

Le informa a los participantes de la apertura del programa

12. JEFE DE ESPECIALIZACIONES

Le envía la programación académica a Registro Académico, Recursos Humanos y Servicios Administrativos(manga).

13. JEFE DE ESPECIALIZACIONES

Notifica al Jefe de Servicios Administrativos(manga), la necesidad de disponer un aula para el desarrollo del programa.

14. JEFE DE SERVICIOS ADMINISTRATIVOS

Le informa al Jefe de Especializaciones el aula asignada para la Especialización.

VI. PROFESORES

1. JEFE DE ESPECIALIZACIONES

Envía una carta al docente donde se le comunica formalmente su vinculación al programa y los lineamientos que debe seguir para el buen desarrollo de éste.
Además, se le solicita Tramitar formato para el pago por gerencia electrónica y que envíe la información o material académico a utilizar para ser impreso, fotocopiado y entregado a los estudiantes. Así mismo informe sobre las necesidades en cuanto a los recursos educativos y ayudas audiovisuales a utilizar.

2. DOCENTE

Envía el material al Jefe de Especializaciones y los requerimientos logísticos.
Remite formato diligenciado a la Jefe de Especializaciones

3.JEFE DE ESPECIALIZACIONES

DISTRIBUCION DEL MATERIAL

Imprime el material recibido por e-mail y solicita la reproducción del material. Distribuye el material fotocopiado (listado de asistencia y reporte de notas) a cada profesor y brinda explicación pertinente.

4. FOTOCOPIADORA

Emite las fotocopias al Jefe de Especializaciones

5. JEFE DE ESPECIALIZACIONES

Solicita al Jefe de Servicios Educativos el apoyo en los recursos educativos.

6,JEFE DE SERVICIOS GENERALES

Coordina el apoyo logístico.

7. JEFE DE ESPECIALIZACIONES

Realiza la carpeta de Bienvenida que será entregada a cada estudiante el día de la apertura del programa, esta incluye:

- Módulo respectivo
- Carpeta CUTB con:
- Carta de Bienvenida
- Formato de Programación académica de la especialización
- Reglamento de Posgrados
- Lapicero CUTB

8. COORDINACION ACADEMICA Y JEFE DE ESPECIALIZACIONES

Reciben a los participantes, les dan la bienvenida a la Tecnológica, a la especialización, les informa acerca de los compromisos que deben asumir y de la exigencia académica, seleccionan el estudiante representante del curso y le informa sus funciones

9. JEFE DE ESPECIALIZACIONES

Le informa al conferencista que debe firmar el contrato en tesorería.

10. CONFERENCISTA

Firma el contrato en tesorería recibe las listas de clase y el mosaico del grupo.

11. JEFE DE ESPECIALIZACIONES

Emite una nueva fecha de inicio del programa, Teniendo en cuenta los resultados de los balances de Mercadeo y Financiera y le informa a Mercadeo, financiera y Servicios Educativos, al Coordinador Académico y al docente respectivo.

VII. APLAZAMIENTO DE UNA ESPECIALIZACION

1. MERCADEO

Informa a los participantes inscritos y matriculados de la nueva fecha de inicio al programa.

Posteriormente, se inicia el mismo proceso.

- Eliminación del Programa

2. JEFE DE ESPECIALIZACIONES

Decide eliminar el programa, después de dos(2) aplazamientos y de estudiar los balances de Mercadeo y Financiera y al encontrar resultados negativos, se decide eliminar el programa.

3. JEFE DE ESPECIALIZACIONES

Informa a Mercadeo, Financiera y Servicios Educativos la eliminación del programa.

4. JEFE DE ESPECIALIZACIONES

Le solicita al Jefe Administrativo y Financiero, un reporte de gastos del programa.

5. JEFE ADMINISTRATIVA Y FINANCIERA

Emite reporte a la Jefe de Especializaciones

6.JEFE DE ESPECIALIZACIONES

Emite al Vicerrector un reporte del programa.

VIII. APOYO LOGISTICO

1.JEFE DE ESPECIALIZACIONES

Solicita con un mes de anticipación los diversos docentes el material a entregar una semana antes de la clase y la información sobre qué recursos educativos va a utilizar.

2.CONFERENCISTA

Envía semanalmente ala Jefe de Especializaciones la información del módulo y las requisiciones en recursos educativos.

3. JEFE DE ESPECIALIZACIONES

Informa semanalmente al Jefe de Servicios Educativos los recursos a utilizar.
Solicita a la fotocopiadora la reproducción del material.

4.FOTOCOPIADORA

Envía a la Jefe de Especializaciones los módulos listos para entregar a los estudiantes.

5. JEFE DE ESPECIALIZACIONES

Revisa que el aula tenga los recursos educativos solicitados y esté lista.

6.JEFE DE ESPECIALIZACIONES

Presenta semanalmente a los conferencistas.

Entrega al Estudiante representante del grupo, el formato de evaluación al docente para que lo diligencien los estudiantes.

7. ESTUDIANTE REPRESENTANTE DE LA CLASE

Entrega al final del módulo y de la clase a la Jefe de Especializaciones los resultados de las evaluaciones.

Este proceso se repite semanalmente durante el desarrollo del programa hasta su culminación.

IX. CONTROL DEL PROGRAMA

1. JEFE DE ESPECIALIZACIONES

Evalúa quincenalmente con la Jefe Administrativa y Financiera la cartera de los programas.

2. JEFE ADMINISTRATIVA Y FINANCIERA

Le informa a la Jefe de Especializaciones, la situación particular de los estudiantes de las diferentes especializaciones y los correctivos que se deben seguir.

3.JEFE DE ESPECIALIZACIONES

Inicia acciones correctivas.

X. EVALUACIÓN DEL PROGRAMA

1. REPRESENTANTE DE CLASE

Aplica la evaluación institucional al finalizar cada materia

2. JEFE DE ESPECIALIZACIONES

Recibe la evaluación y la entrega al coordinador académico interno para su tabulación

3. COORINADOR ACADEMICO INTERNO

Tabula y envía la información a la jefe de Especializaciones y a al coordinador académico externo para que este la reporte al profesor.

De la evaluación obtenida por el docente depende su permanencia en la institución como docente.

4. JEFE DE ESPECIALIZACIONES Y COORDINACION ACADEMICA

El último día de clase hacen una reunión para efectuar la evaluación de la especialización con todos los estudiantes y se comparte un refrigerio.

Es muy importante para hacer el mejoramiento continuo tanto académico como logístico. y para hacer una retroalimentación, compartir la experiencia y evaluar los aspectos que los estudiantes desean comunicar en cuanto a:

- Calidad Académica
- Nivel de los Docentes
- Recursos Educativos Utilizados
- Servicio

5. JEFE DE ESPECIALIZACIONES

Presenta al Vicerrector un informe académico y financiero de la Especialización al finalizar la misma.

XI. FINALIZACIÓN DE LA ESPECIALIZACIÓN

1. JEFE DE ESPECIALIZACIÓN

Solicita al vicerector convocar a consejo académico para fijar la fecha de la ceremonia de graduación.

2. VICERRECTOR

Convoca el consejo académico, e informa la fecha a la jefe de Especializaciones.

3. JEFE DE ESPECIALIZACIONES

Asiste al consejo académico y presenta a los estudiantes que se encuentran a paz y salvo por todo concepto con la institución.

4. EL CONCEJO ACADEMICO

Aprueba el grado de los estudiantes y fija la fecha de la ceremonia.

5. JEFE DE ESPECIALIZACIONES

Envía carta a los estudiantes de la especialización informándoles la fecha de grado y citándolos a una reunión previa para explicarles el protocolo de la ceremonia de graduación

MAESTRIAS

Tipos de usuarios:

- Jefe del Dpto.

Privilegios:

Servicios que pueden usar: tiene acceso a toda la red como son: el Internet, Windows 95, Dpto de Maestria, direccion de Manga, Dpto de idiomas, Dpto de Educación Permanente, Dpto de Especializaciones, Mercadeo, Secretaria de Posgrado, Tesorera de Postrado Conexión con Pregrado.,Salas de informáticas.

Esta conectada a la red las 24 horas, se comunica con los conferencistas, estudiantes de especialización, directivos de cada facultad, estudiantes externos de posgrado, conoce las cuentas de resguardo de cada uno de los estudiantes.

Controles: Su PC si tiene clave de acceso y la información queda registrada en el disco duro. Tambien informática y computo le realiza copias de seguridad .La información la guarda en medios magnéticos.

Tipos de servicios:

- Quienes va dirigido: Vicerectoria.
- Donde reside el servicio: En el Dpto. de informática y computo de Manga.
- Quien lo administra: Víctor Espinosa.

RECTORIA

Tipos de usuarios:
Esta conformada por :
RECTOR
SECRETARIO GENERAL
GESTION:
Director(Sofia Trillos).
ASESOR ACADEMICO(Misael Cruz).
ASESOR ACADEMICO(Juan Carlos Mantilla).
ASESOR DE PLANEACION(Jaime Acevedo).
AUDITORA General(Marta Anaya).
DOS SECRETARIA: Una de gestión y la otra de secretario general.

Privilegios: En cuanto a las secretarias la de gestión tiene menos prioridad que la de general, por ejemplo Si la secretaria General tiene que accesar al menú de

Decano ella le pide permiso a la jefe del DPTO de Registro Académico, en cambio la secretaria de gestión tiene que tener autorización de sus jefes.

Servicios que pueden usar: tiene acceso a toda la red como son: el Internet, Windows 98.

Controles: Su PC si tiene clave de acceso y la información queda registrada en el disco duro. También informática y computo le realiza copias de seguridad .La información la guarda en medios magnéticos.

Tipos de servicios:

- Quienes va dirigido: Vicerectoria.
- Donde reside el servicio: En el Dpto. de informática y computo de Manga.
- Quien lo administra: Victor Espinosa.

DPTO DE INVESTIGACIONES

Tipos de usuarios:

- Director de investigaciones, dos auxiliares y una secretaria.

Privilegios: la secretaria tiene acceso a registro académico solo ella conoce la clave.

Servicios que pueden usar: Internet, Windows 95, manejan el software de investigaciones, también se puede comunicar con registro académico.

Controles: Todo queda guardado en el disco duro del computador y en Informática y Computo,

Tipos de servicios :

Se maneja toda la información relacionada con: trabajo de grado, anteproyectos y propuestas , también se suministra información a las respectivas decanaturas.

REGISTRO ACADEMICO

Tipos de usuarios:

- Jefe del DPTO, y como también el Rector, Secretario General, Director de Gestión, Vicerector, utilizando nada mas la sección de Decano.

Privilegios: Solamente la jefe del DPTO.

Servicios que pueden usar: Internet, Windows 95, todo el sistema académico como son: generar listado para clase, listado para parcial, listado de Horarios, listado de estudiantes en prueba, listado de estudiantes sobresalientes, listado de estudiantes activos e inactivos, listado de estudiantes por nivel, listado de estudiantes por nivel, listado de estudiantes excluidos, todo lo especificado en el calendario de actividades.

Controles: Todo queda guardado en el disco duro del computador (equipo principal), se realizan back up semanales por Informática y Computo.

Tipos de servicios :

Se maneja una base de datos bajo UNIX, donde están registrados todos los estudiantes con una serie de información referente al mismo (datos personales, historia académica y otros).

- Quienes va dirigido: Vicerectoria.
- Donde reside el servicio: En el Dpto. de informática y computo de Manga.
- Quien lo administra: Patricia Llamas.

DPTO DE MERCADEO (PREGRADO).

Tipos de usuarios:
Jefe del Dpto, una Auxiliar, una Asistente del DPTO, y uno o dos estudiantes en practica.

Privilegios: Jefe, auxiliar, Asistente del DPTO y Estudiante.

Servicios que pueden usar: Internet, Windows 95, software de admisiones.

Controles: Todo queda guardado en el disco duro del computador (equipo principal), cada PC del Dpto. tiene clave de acceso, y utilizan disket cuando tienen relación con otros Dpto.

Tipos de servicios:

Se maneja un software donde se registran los estudiantes que desean ingresar a la universidad; clasificados en tres grupos: reingreso, transferencia y alumnos nuevos.

- Quienes va dirigido: Secretario General.
- Donde reside el servicio: En el DPTO de Mercadeo.
- Quien lo administra: Miguel López Fuentes.