UNIVERSIDAD DON BOSCO
FACULTAD DE INGENIERIA

TRABAJO DE GRADUACION PARA OPTAR AL GRADO DE:
INGENIERO EN CIENCIAS DE LA COMPUTACION

GUIA GENERAL PARA ELABORAR UNA AUDITORIA DE SISTEMAS. UNA APLICACION PRACTICA EN EL AREA DE INFORMATICA DE LA UNIVERSIDAD DON BOSCO

PRESENTADO POR:
Carlos Francisco Carballo Alvarado
José Carlos López Ruiz

ASESOR:
Lic. Roberto Rivas Bayona

SOYAPANGO, ABRIL 1995

AUTORIDADES ACADEMICAS
UNIVERSIDAD DON BOSCO
1995

Pbro. y Lic. Heriberto Herrera, sdb
PRESIDENTE

Pbro. y Lic. Salvador Cafarelli, sdb
DIRECTOR

Ing. Federico Miguel Huguet
RECTOR

Ing. José Miguel Hernández
DECANO FACULTAD DE INGENIERIA

Ing. José Roberto Guzmán
VICE-DECANO FACULTAD DE INGENIERIA

Pbro. y Lic. Pierre Muyshondt, sdb
SECRETARIO GENERAL DE LA UNIVERSIDAD DON BOSCO

AGRADECIMIENTOS

Queremos agradecer al Lic. Roberto Rivas Bayona, Asesor de nuestro trabajo de graduación quien supo darnos a lo largo de éste, una valiosa guía y apoyo aportando desinteresadamente sus conocimientos y experiencia para poder culminar el trabajo. Al Lic. Arnulfo Avelar quien nos brindó su colaboración y orientación en el campo de la Auditoría de Sistemas. Al Ing. Manuel Orellana, encargado del área de sistemas de la Ciudadela Don Bosco, por su ayuda en la recopilación de la información necesaria para poder desarrollar el trabajo. Al Sr. Javier Serrano, Contador de la Universidad Don Bosco por su colaboración en el área contable. A la Sra. Cecilia de Guerrero, Contador, quien nos brindó su ayuda y conocimientos. Al Lic. José Atilio Campos, de la Empresa Castellanos Campos y Cía. por orientarnos en el campo de la Auditoría. A nuestros Jurados, Ing. Manuel Orellana y Lic. Walter Turcios por su valiosa colaboración. Al Sr. Salvador Alexander Miranda y a la Arq. Ella Salinas por su colaboración desinteresada. A las familias Carballo Alvarado, Huezo Lemus y López Ruiz por su apoyo y ayuda.

CARLOS FRANCISCO CARBALLO ALVARADO
JOSE CARLOS LOPEZ RUIZ

AGRADECIMIENTOS

A DIOS TODOPODEROSO:
Por guiarme en el camino correcto y proporcionarme sabiduría para poder culminar con mi meta trazada.

A MI ESPOSA:
Silvia Carolina Huezo de Carballo, por darme su ayuda, comprensión, apoyo y sobre todo fuerza para alcanzar este logro.

A MIS PADRES:
Sr. Carlos Alberto Carballo Ulloa y Sra. Melba Alvarado de Carballo, por el esfuerzo realizado para brindarme una buena educación y que lograse ser una persona de provecho.

A MI HERMANO:
Douglas Mauricio Carballo Alvarado, por su apoyo y útiles consejos.

A LA FAMILIA HUEZO LEMUS:
Por impulsarme a lograr mi propósito y tener siempre fé en mi.

A MI COMPAÑERO Y AMIGO:
Sr. José Carlos López Ruiz, por el esfuerzo compartido durante esta dura y larga trayectoria.

A MIS PROFESORES:
Por engrandecer mis conocimientos y formarme para ser una persona útil a la sociedad.

A MIS COMPAÑEROS:
Con los que compartí gratos momentos durante mi carrera universitaria.

A MI FAMILIA Y AMIGOS:
Por incentivarme a concluir mis propósitos anhelados.

CARLOS FRANCISCO

AGRADECIMIENTOS

A DIOS:
Por haberme dado luz en mis momentos oscuros, fuerza en mis momentos de flaqueza y la determinación suficiente para poder culminar mi carrera.

A MI ESPOSA:
Cecilia Corral de López, que con su amor me dio empuje y aliento estando a mi lado desde siempre y para siempre.

A MI PADRE:
Arq. José Carlos López Candell, quien con paciencia supo darme su apoyo cuando más lo necesite tendiéndome siempre su mano fraternal, sincera, amiga.

A MIS HERMANOS:
Ana María y Rafael Guillermo por su apoyo en todo momento.

A CARLOS FRANÇISCO:
Por ser un buen compañero de trabajo y un excelente amigo.

A ALFREDO ESTRADA:
Quien supo demóstrarme su amistad sincera dentro y fuera del campo académico.

A MIS EDUCADORES:
Por haber sembrado su semilla del conocimiento que ahora da frutos.

A MIS COMPAÑEROS Y AMIGOS:
Por haber compartido conmigo alegrías y frustraciones.

Y EN ESPECIAL, A MI MADRE:
Ana María Ruiz de López Candell† que desde el cielo supo guiar mis pasos a lo largo de este arduo camino y a quien dedico este triunfo.

JOSE CARLOS

INDICE

PARTE I. GUIA GENERAL PARA ELABORAR UNA AUDITORIA DE SISTEMAS

PARTE III - UNA APICACION PRACTICA EN EL SISTEMA CONTABLE DE LA UDB

PARTE I

GUIA GENERAL PARA ELABORAR UNA AUDITORIA DE SISTEMAS

CAPITULO 1

GLOSARIO

1. GLOSARIO

Siempre que en el presente documento se utilicen los términos que posteriormente se enlistan, debe entenderse que significan lo que a continuación se expresa:

ADS	: Auditoría de Sistemas
PED	: Procesamiento Electrónico de Datos
Amenaza	: La causa de producir un riesgo. La materialización de una amenaza puede ocasionar uno o más riesgos.
Aplicación	: Uso específico de la computadora; programa específico del usuario.
Archivos	: Conjunto de registros relacionados.
Arquitectura	: Diseño de una computadora; el diseño determina la forma en que la computadora dará servicio a las actividades concurrentes, la cantidad necesaria de memoria y el tamaño de los canales internos para la transmisión de datos e instrucciones en uno y otro sentido.
Bases de Datos	: Es una organización electrónica de datos y de información, organizada y conservada por un sistema de manejo de bases de datos, además implica la integración de los datos de todo el medio ambiente al que da servicio. También implica un control central consistente y preciso de los datos, el cual permite que los usuarios los consulten.
Campo	: Unidad definida de datos o información en un registro; un campo define la localización

física de almacenamiento de una unidad de datos o información.

Controles : Es un procedimiento o un proceso que reduce la exposición al riesgo.

Datos : Unidades de información que pueden definirse con precisión; desde el punto de vista técnico, los datos son las materias primas que al ser procesadas dan lugar a la información.

Datos Fuente : Son aquellos datos originales que fueron utilizados para dar inicio a la información.

Documentos Fuente : Forma en la cual se inscribió la transacción original; son formas de documentos fuente los pedidos, pagarés, solicitudes, etc.

Encriptar : Cifrar la información con fines de seguridad; el cifrado transforma los códigos digitales estándar en códigos especiales que son transmitidos a través de un canal de comunicaciones.

Estándar : Tipo, modelo, patrón. Todos los sistemas tienen niveles aceptables de desempeño denominados estándares y contra los cuales se comparan los niveles de desempeño actuales.

Factibilidad : La posibilidad de que alguna cosa sea llevada a cabo. La posibilidad de que un sistema sea de utilidad para una organización.

Hardware : Cualquier dispositivo microelectrónico que contrasta con el software, constituido por las instrucciones que indican ala computadora que hacer. La maquinaria, el CPU y todos los periféricos.

Interfaz	: Interconexión entre elementos de hardware y software y seres humanos; las interfaces de hardware son trayectorias físicas que deben conectar e intercambiar señales electrónicas en un orden preestablecido. Las interfaces de software están constituidas por los mensajes específicos establecidos entre los programas.
Lenguajes	: Lenguaje de programación; lenguaje de desarrollo de programas de aplicación que puede referirse a cualquier lenguaje convencional de programación.
Mecanizar	: Sustitución de operadores manuales por sistemas de cómputo.
Medios de Almacenamiento	: Dispositivo en el que pueden introducirse datos, que puede retenerlos y del cual pueden recuperarse posteriormente. En sentido general, cualquier dispositivo capaz de aceptar datos, retenerlos durante un período indefinido de tiempo y facilitarlos previa petición.
Password	: Palabra clave, tiene como finalidad restringir el acceso a un programa, archivo, terminal, sistema, etc.
Recurso	: Acción y efecto de recurrir. Medio a que se recurre para algo. Un recurso se define como algo tangible, de valor que es usado durante los procesos y que puede estar expuesto a amenazas.
Registro	: Grupo de campos de datos relacionados; un registro es un conjunto de datos y de información sobre un sujeto o tema.
Riesgo	: Es un resultado desfavorable que trae como consecuencia pérdidas de tipo cualitativo o cuantitativo.

Sistemas Abiertos	: Son aquellos que interactúan con su medio ambiente. Reciben entradas y producen salidas.
Software	: Instrucciones de computadora; los conjuntos de instrucciones constituyen el software.
Usuario	: Cualquier persona que utilice la computadora; generalmente el término usuario se refiere a las personas que no pertenecen al personal técnico y que proporciona entradas y reciben salidas de la computadora.

CAPITULO 2

INTRODUCCION - PARTE I

2. INTRODUCCION - PARTE I

Basta con observar el medio en el que se desarrolla la sociedad moderna para darse cuenta de que la computadora se ha convertido en una herramienta indispensable en el desarrollo de cualquier actividad. La velocidad con la que se realizan las transacciones y el grado de complejidad que estas han alcanzado han impulsado al hombre a buscar la mejor forma de administrar sus recursos.

En tan solo dos generaciones, la computadora a alterado de manera palpable la estructura y funciones de la mayoría de las organizaciones. Esta tecnología ha vuelto obsoletos muchos de los métodos que se utilizaban para manejar, controlar y verificar la información y procedimientos de la organización.

Estos aspectos también han traído una serie de nuevos problemas que deben afrontarse con el fin de lograr maximizar el potencial que tienen las computadoras. En lo que se ha dado por llamar centros de cómputo, áreas de informática, departamentos de procesamiento electrónico de datos y otros tantos nombres, han surgido una serie de aspectos que deben observarse con cuidado. A manera de ejemplo puede mencionarse: es latente la falta de una adecuada organización que permita avanzar al ritmo de las exigencias de las

organizaciones; a esto puede agregarse la situación que presentan los nuevos equipos en cuanto a sistemas, software, hardware, etc. Todo esto combinado con la necesidad de una eficiente planeación estratégica y corporativa de las organizaciones y una descentralización de equipos y centralización de la información, a provocado que la complejidad de las decisiones y las dimensiones de los problemas en cuanto a la mejor forma de organizar el área de informática, requieran aplicar técnicas modernas de control y administración.

Como respuesta a esta situación surge la disciplina conocida como "Auditoría de Sistemas", la que trata de incorporar a personal con conocimientos tanto de computadoras como de principios de control. La necesidad crítica de auditores de sistemas junto con la complejidad e importancia de sus responsabilidades, presentan a los auditores un reto difícil. Deben tener profundos conocimientos en computación y mantenerse al paso con los desarrollos de tecnología en equipo, comunicaciones y software. Deben estar en capacidad de utilizar las ultimas metodologías en cuanto a auditoría. Y deben establecer y mantener relaciones efectivas de trabajo con la alta gerencia, el usuario y el personal de sistemas.

La auditoría de sistemas ha ido cobrando auge en los últimos años gracias a los esfuerzos de distintas organizaciones internacionales de Auditores que se dedican a esta rama de la disciplina. Es cada vez más frecuente encontrar

organizaciones norteamericanas y europeas que cuentan con su propio auditor de sistemas.

En El Salvador, aún no se ha propagado de la misma forma que en otros países. Más aún, no se cuenta con un programa formal para la capacitación de este tipo de profesionales, y las Universidades, Colegios Profesionales y firmas de Auditoría solo cuentan con aspectos de carácter introductorio a la disciplina.

Por todo lo anterior, el presente trabajo de graduación pretende incursionar en la rama de Auditoría de Sistemas como un intento de brindar un poco más de información a todo aquel interesado en investigar sobre el tema. Al mismo tiempo, presentar a la Universidad Don Bosco con una herramienta que le permita lograr una mejor utilización de sus recursos de informática.

CAPITULO 3

ASPECTOS GENERALES DE SISTEMAS

3. ASPECTOS GENERALES DE SISTEMAS

Antes de poder hablar de lo que es Auditoría de Sistemas (ADS), es necesario exponer una serie de términos que están de una forma u otra relacionados con esta disciplina.

Cuando se habla de ADS se hace referencia a sistemas, esta palabra en si podría ser tema de discusión por si sola. Este trabajo se limita a hacer algunas observaciones al respecto para dejar claro el ambiente en que se desenvuelve la ADS.

3.1 DEFINICION DE SISTEMAS

En la actualidad, se pueden encontrar una gran cantidad de definiciones para la palabra sistema. Se ha vuelto tan común que a cualquier proceso en que interactúan varias partes nos da por llamarle sistema lo cual dista mucho de ser la realidad, lo que se podrá comprender mejor cuando se estudien las diferentes definiciones.

En el diccionario Larousse se encuentra las siguiente definición: "Combinación de partes reunidas para obtener un resultado o formar un

conjunto". Esta no parece ser la mejor de las definiciones ya que según este concepto, un pastel de manzana podría ser un sistema.

El Sr. Alan Freedman lo define en su glosario de computación como: "Conjunto de componentes y eventos relacionados que interactúan unos con otros para ejecutar una tarea".

En su libro "Análisis y Diseño de Sistemas de Información", James Senn dice: "En el sentido más amplio, un sistema es simplemente un conjunto de componentes que interactúan para alcanzar algún objetivo".

Después de estudiar varias definiciones, una de las que más se acerca a abarcar todo lo que caracteriza a un sistema nos la dan Robert G. Murdick y John C. Munson: "El sistema es un conjunto de elementos organizados que se encuentran en interacción, que buscan una meta o metas comunes, operando para ello sobre datos o información sobre energía o materia u organismos en una referencia temporal para producir como salida información, energía, materia u organismos".

3.2 CARACTERISTICAS DE LOS SISTEMAS

Para que un sistema pueda tener un rendimiento que cumpla con todos los requisitos esperados, es necesario que cumpla con una serie de características cuya descripción se expone a continuación.

a) Todo sistema debe de estar compuesto de una entrada que puede ser todos aquellos materiales, personal y conocimientos necesarios para poder producir lo que se desea; un proceso donde se realice la transformación de los componentes y la comparación con el medio; y como último la salida donde se muestre el producto terminado.

b) Debe existir una retroalimentación que sirva como reajuste o readecuación al sistema.

c) Los sistemas deben ser abiertos para poder soportar cualquier cambio que pueda tener el medio ambiente.

d) Debe existir un modelo de control que indique que el sistema se desenvuelve en la forma esperada.

e) Sus partes deben de interactuar entre si sin perder su independencia.

3.2.1 ELEMENTOS DE UN SISTEMA

A continuación se presenta la descripción de los elementos de un sistema y seguidamente una representación gráfica (gráfica No. 1) del funcionamiento del mismo.

Entrada: es lo que se alimentará al sistema para que sea transformado; podrían ser insumos provenientes de otro sistema o simplemente entradas crudas o en bruto por ejemplo materia prima, dinero, energía o información.

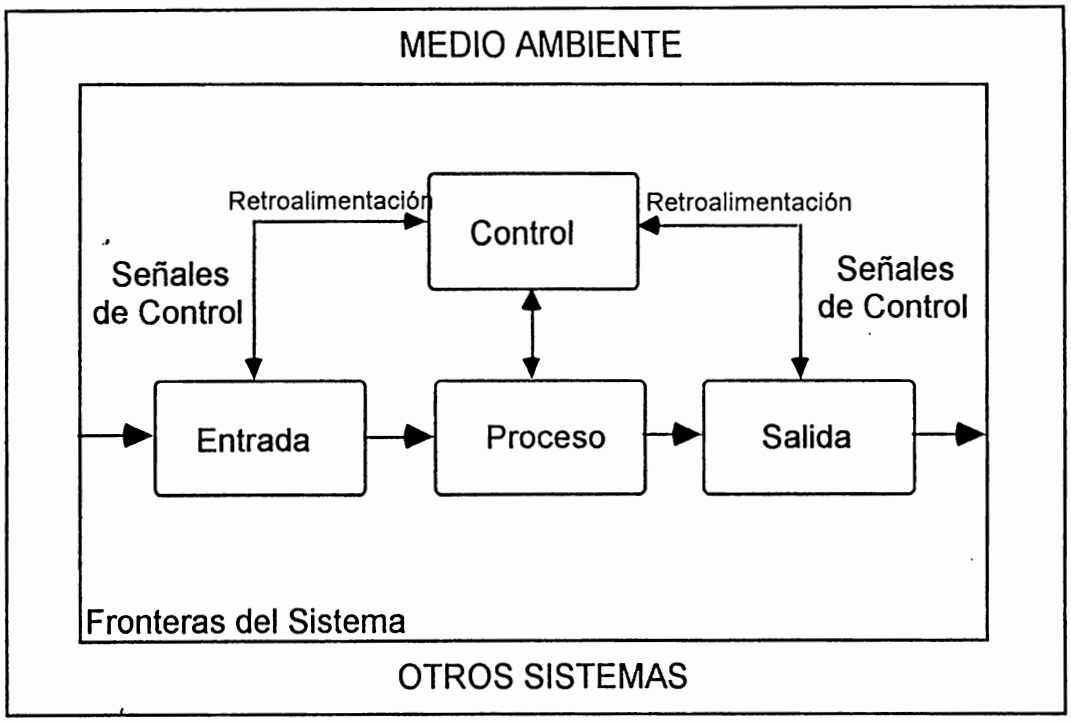
Proceso: es el mecanismo que se encargará de transformar las entradas para producir un producto final, maquinaria, el cerebro humano, una computadora.

Salida: Es el resultado del proceso, puede decirse que es el objetivo del sistema. Esta podría ser productos o servicios y dados casos ser un producto intermedio que sirva de entrada a otro sistema.

Control: Es el encargado de planificar, controlar y guiar el funcionamiento del sistema. Se encarga de vigilar por que el sistema cumpla con los objetivos esperados.

Retroalimentación: Es la que se encarga de comparar el sistema con los estándares establecidos y administrar la información necesaria para que el sistema pueda ser reajustado para mejorar su desempeño. Debe entenderse por estándares, el establecimiento de normas y políticas bajo las cuales se desempeña el sistema. Son aquellos aspectos que rigen y determinan la forma en que debe funcionar un determinado sistema o subsistema.

Medio Ambiente: Es el entorno en el cual se desenvuelve el sistema. Es todo aquello externo al sistema que de alguna u otra forma afectan el funcionamiento del mismo.



Gráfica Nº 1

3.3 CICLO DE VIDA DE LOS SISTEMAS

Este inicia siempre que se pone en marcha un nuevo sistema y se ve afectado cuando el sistema es modificado. Para su mejor entendimiento, puede definirse como un conjunto de actividades que se deben de llevar a cabo para desarrollar y poner en marcha un sistema y su duración dependerá de la naturaleza y de la utilización que este reciba.

Gráfica Nº 2

El ciclo de vida de los sistemas puede desglosarse en una serie de actividades específicas (gráfica No. 2). Dado que el enfoque de este trabajo no es el análisis de sistemas en sí, el ciclo de vida de los sistemas se ha agrupado en un conjunto de actividades concretas y resumidas que se describen a continuación.

3.3.1 INVESTIGACION DE SISTEMAS

La investigación es la primera actividad en el proceso de desarrollo de sistemas. Esta se inicia cuando existe un requerimiento de sistema para resolver una problemática específica.

1.	Planeación del Sistema y Selección	Estudio de la organización para detectar y seleccionar el desarrollo de sistemas potenciales, incluyendo aquellos generados por procesos formales de planificación de sistemas.
2.	Estudio de Factibilidad	Se debe hacer una determinación de las necesidades del usuario final. Se debe determinar la factibilidad de desarrollar nuevos sistemas o mejorar los existentes para satisfacer dichas necesidades. Se desarrolla una planificación del proyecto.
3.	Reporte de Factibilidad	Se documentan y comunican los resultados del estudio de factibilidad a los usuarios y la gerencia.

3.3.2 ANALISIS

Esta fase se puede considerar como una extensión del estudio hecho en la etapa anterior. Se utilizarán algunos de los métodos para recolectar información usados en la investigación pero en esta etapa el estudio será

mucho más profundo y detallado, procurando determinar los requerimientos del sistema.

1.	Análisis del medio ambiente organizacional	Se analizan las necesidades de información del usuario final incluyendo sus subsistemas y sistemas del medio ambiente.
2.	Análisis de los sistemas existentes	Se analizan los recursos, productos y actividades de cualquier sistema utilizado actualmente.
3.	Análisis de los requerimientos del sistema	Se determinan las capacidades del sistema de información que cumplirán con las necesidades del usuario final.
4.	Requerimientos del sistema.	Documenta la entrada lógica, proceso, salida, almacenamiento y los requerimientos de control de un sistema de información nuevo o existente.

3.3.3 DISEÑO

En la etapa de diseño se especifica como el sistema cumplirá con los objetivos esperados satisfaciendo las necesidades planteadas en la etapa de análisis. Esta consiste tanto del diseño lógico como del diseño físico los cuales producen las especificaciones del sistema, satisfaciendo los requerimientos del mismo especificados en la etapa de análisis.

1.	Diseño Lógico	Se desarrollan especificaciones generales de como la entrada, proceso, salida, almacenamiento y control de actividades cumplirán con los requerimiento desarrollados en la etapa de análisis.
2.	Diseño Físico	Se desarrollan especificaciones detalladas para las interfaces del usuario y los métodos, estructuras de base de datos, y procedimientos de proceso y control. También se especifica equipo y software y especificaciones de personal
3.	Especificaciones de Sistemas	Se documentan y comunican las especificaciones detalladas del sistema propuesto para el usuario final.

3.3.4 IMPLEMENTACION

Esta actividad envuelve el equipo, el software desarrollado, prueba de programas y procedimientos, desarrollo de documentación y una variedad de actividades de instalación según se detalla a continuación.

1.	Adquisición	Evaluación y adquisición del equipo necesario y el software requerido.
2.	Desarrollo de software	Se desarrollan los programas que no sean adquiridos externamente como paquetes.
3.	Entrenamiento	Educar y capacitar a todo aquel personal que hará uso del sistema.

4.	Prueba	Se probará y se harán las correcciones necesarias a los programas procedimientos y al equipo a utilizar.
5.	Documentación	Se registrarán y comunicarán las especificaciones detalladas del sistema, incluyendo los procedimientos para el usuario final y el personal de operación, y ejemplos de las entradas, salidas y reportes.
6.	Conversión	Se hará la conversión del sistema existente a un sistema nuevo o mejorado. Esto puede involucrar la operación paralela de los dos sistemas por un período de prueba.

3.3.5 MANTENIMIENTO

Esta etapa incluye el monitoreo, evaluación y modificación de un sistema para hacer las mejoras deseadas o necesarias. Podría incluir un proceso de revisión de una post-implementación para asegurar que el nuevo sistema cumple con las necesidades y objetivos establecidos para este. Los errores del desarrollo o uso de un sistema se corrigen en la etapa de mantenimiento. En esta etapa también se incluyen modificaciones debido a cambios en el medio ambiente.

3.4 SISTEMAS DE INFORMACION

Al analizar las varias definiciones que existen de sistema, todo parece indicar que al referirse a un sistema es necesario y casi indispensable asignarle un calificativo que indique a que tipo de sistema se esta haciendo referencia.

Así pues se puede hablar del sistema nervioso o del sistema bancario, los cuales a pesar de no tener mucho en común siguen siendo buenos ejemplos de lo que es un sistema.

Ahora, es muy común escuchar la palabra sistemas y automática pero erradamente se relaciona su significado con la informática.

Dado este mal habito, se ha considerado conveniente hablar un poco de lo que son sistemas de información que son en sí el medio ambiente en que se desarrolla este trabajo de graduación. Por ello, quizás antes convenga mencionar que se entiende por informática.

En una conferencia presentada en diciembre de 1983 en la Universidad Autónoma de México se presento el siguiente análisis: "No existe una sola

concepción acerca de lo que es informática; etimológicamente, la palabra informática, deriva del francés informatique. Este neologismo proviene de la conjunción de information (información), y automatique (automática). Su creación fue estimulada por la intención de dar una alternativa menos tecnocrática y menos mecanicista al concepto de proceso de datos".

Antes de esta conferencia se habían dado una serie de definiciones para lo que es la informática sin que alguna de ellas fuera aceptada como única o estándar, pero para efectos de dirigir la investigación se tomará como valedera la siguiente: Ciencia del tratamiento automático y racional de la información.

Sistemas de Información

Debido a la amplia gama de sistemas existentes en la vida cotidiana, como los ya ejemplificados, es conveniente aclarar que el enfoque de este estudio esta dirigido a lo que se conoce como sistemas de información.

Para ello se debe tener claro que es información. Este es un concepto tan común, que pocas veces se repara en su importancia. No se puede decir que la información son datos, porque estos por si solos no son más que símbolos sin sentido. La información es un conjunto de datos que

colocados en forma lógica, clasificados y ordenados tienen el fin de alcanzar un objetivo.

Conociendo los conceptos de sistema e información, se puede establecer una relación y lograr una definición para lo que es un sistema de información: Es una recolección de recursos, mecanismos y procedimientos relacionados entre si e interdependientes que absorben datos, los transforman y distribuyen información en una organización.

3.4.1 TIPOS DE SISTEMAS DE INFORMACION

Para poder satisfacer las diversas necesidades que se le presentan a una empresa, se ha hecho necesario el desarrollo de diferentes tipos de sistemas de información, entre los que se pueden mencionar:

- Sistemas de Procesamiento de Transacciones (SPT)

  Estos se encargan de realizar las labores diarias de la organización. La mayor parte de los procesos de operación que ayudan a un mejor manejo de las transacciones están contenidos en los programas desarrollados en el área de cómputo y servirán para controlar la entrada de datos, el procesamiento y almacenamiento y presentación de la información final. Dentro de sus características se pueden mencionar: la

de datos, el procesamiento y almacenamiento y presentación de la información final. Dentro de sus características se pueden mencionar: la sustitución de procedimientos manuales por los computarizados; se relacionan con procesos de rutina bien estructurados y toman en cuenta aplicaciones para el manejo de registros.

- Sistemas de Información Gerencial (SIG)

  Estos están dirigidos a la toma de decisiones, lo que implica al área gerencial, y toda la información que se necesita puede ser obtenida ya sea de los datos de las transacciones o información que se genere dentro o fuera de la empresa. Esta información se presenta en formatos prediseñados con anticipación.

  Al igual que los SPT poseen una serie de características de las cuales se pueden mencionar: facilitan la información necesaria que será utilizada en los procesos de decisión administrativa; se relacionan con el soporte de situaciones de decisión bien estructuradas y pueden lograr adelantar los requerimientos de información más frecuentes.

- Sistemas para el soporte de decisiones (SSD)

  Tiene como objetivo brindar ayuda cuando se presenta el problema de la toma de decisiones, es decir, contribuyen a determinar que información es la que debe ser elegida.

  Por lo general, las decisiones que deben tomarse no suelen repetirse debido a la diferencia de factores para una misma situación en dos momentos diferentes, por ello, estos sistemas de soporte ayudan a los directivos a tomar decisiones no muy estructuradas. Las decisiones son consideradas no estructuradas cuando para tomarlas no existen procedimientos claros y resulta difícil identificar los factores que deben ser considerados en la decisión.

  Las características principales de este tipo de sistemas son: proporcionan toda la información necesaria para poder tomar decisiones sobre situaciones particulares y brindan un soporte a la toma de decisiones en aquellas situaciones que no están bien estructuradas.

CAPITULO 4

ASPECTOS GENERALES DE AUDITORIA

4. ASPECTOS GENERALES DE AUDITORIA

Luego de haber expuesto lo que comprende todo lo relacionado con sistemas y especialmente los de información, se debe cubrir otro aspecto que es de mucha importancia para poder posteriormente incursionar en lo que es ADS, ello es el término de Auditoría.

Se tratará de ser lo más general posible, ya que en la actualidad la auditoría se aplica a varias áreas de la empresa, de esa forma se tienen auditorías operacionales, administrativa, financiera, de sistemas, etc.

4.1 HISTORIA DE LA AUDITORIA

Se ha podido investigar a través de estudios hechos por historiadores que el registro de operaciones se origino aproximadamente 4,000 años A.C., cuando civilizaciones antiguas en el cercano Oriente empezaron a establecer gobiernos organizados y consecuentemente negocios. Desde el principio, el gobierno estuvo interesado en la contabilización de desembolsos y recolección de impuestos. Una parte integral de este interés fue el establecimiento de controles incluyendo auditorías, para reducir errores y fraude por parte de los oficiales a cargo. Varias formas

modernas de control interno se describen en la Biblia, la cual encierra un período desde los años 1,800 A.C. hasta el 95 D.C., y la explicación de la lógica en el establecimiento de controles (si los empleados tienen una oportunidad de robar, seguramente le sacaran ventaja) refleja el mismo escepticismo profesional esperado de los auditores en esta época.

El sistema de contabilidad establecido por el gobierno de la dinastía Zhao (1,122-256 A.C.) en China incluía procesos complicados de presupuestos y auditoría para todos los departamentos del gobierno. En el siglo V A.C. en Atenas, la Asamblea Popular controlaba la recepción y distribución de fondos públicos. El sistema de finanzas públicos incluía Auditores de gobierno quienes examinaban los registros de todas las gobernaciones al vencimiento de sus períodos. En el sector privado los administradores de propiedades solían realizar auditorías de sus contabilidades. Las finanzas públicas en el Imperio Romano estaban bajo el control del Senado y la contabilidad pública era examinada por un equipo de auditores examinado por el tesorero. Los Romanos mantuvieron segregación de tareas entre los oficiales que autorizaban impuestos y gastos y aquellos que manejaban recibos y pagos, y al igual que los Griegos llevaban un sistema elaborado de cheques y contracheques.

Dentro de los registros más antiguos de contabilidad y auditoría (países Anglosajones) se encuentran los de "Exchequers of England and Scotland", que datan de 1,130. Hay referencias de auditores y auditorías tanto en Inglaterra como en Italia y un trabajo Francés en la administración de propiedades escrito en el mismo siglo que recomienda una auditoría anual para la contabilidad. La ciudad de Londres cuenta con registros de auditoría desde inicios de los 1,200's, y a inicio del siglo XIV los auditores formaban parte de los oficiales de gobierno. Desde esa época se cuenta con bastante evidencia de que el valor de la auditoría era ampliamente reconocido y que la contabilidad de las municipalidades, propiedades privadas y cofradías eran auditadas regularmente.

Las primeras auditorías en Gran Bretaña eran de dos tipos: Las auditorías de ciudades y pueblos eran realizadas en forma pública ante oficiales del gobierno y ciudadanos y consistían en la lectura de la contabilidad por el tesorero para ser analizadas por los auditores. Similarmente la auditoría de las cofradías era realizada ante una audiencia de sus miembros. A mediados del siglo XVI los auditores de las ciudades firmaban las contabilidades anteponiendo frases como "Escuchadas por los auditores firmantes". Los primeros reportes de auditoría se conocían como "Certificados de Auditoría". El segundo tipo de auditoría involucraba una examinación detallada de los "Cargos y Descargos" de las cuentas

mantenidas por los oficiales financieros, seguida de una "Declaración de Auditoría", que era un reporte oral ante el señor de los bienes y el Consejo. Típicamente, el auditor era miembro del Consejo de Propiedades y fue el precursor del Auditor Moderno.

Ambos tipos de auditorías realizadas en Gran Bretaña antes del siglo XVII estaban dirigidas primordialmente a asegurar la contabilidad de los fondos confiados a los oficiales públicos o privados. Esas auditorías no estaban diseñadas para evaluar la calidad de las cuentas, excepto cuando las inexactitudes apuntaran a la existencia de un fraude. Los cambios económicos entre 1,600 y 1,800 que vieron el crecimiento de ciudades, la transformación de cofradías en industrias y el inicio del comercio internacional, introdujeron nuevos enfoques de contabilidad. Estos estaban orientados al registro de propiedades y el cálculo de ganancias y pérdidas en el sentido de negocio. La auditoría también inició una transformación de un proceso de audiencia a una examinación minuciosa de registro escritos y la prueba de evidencias. A finales del siglo XVII se estableció la primera ley (en Escocia) que prohibía a algunos oficiales de servir como auditores públicos introduciéndose así al mundo Occidental la noción moderna de independencia del auditor.

A pesar de estos avances en la práctica de auditoría no fue sino hasta mediados del siglo XIX (con la construcción de ferrocarriles y el crecimiento de compañías de seguros, bancos y empresas de inversión) que el auditor profesional se convirtió en parte importante del mundo de los negocios. La industria ferrocarrilera de los Estados Unidos fue una de las primeras en contratar Auditores Internos. Para finales del siglo XIX los llamados auditores viajeros visitaban diferentes empresas para evaluar la administración de la contabilidad y el registro de ganancias bajo sistemas de reportes.

4.2 CONCEPTOS DE AUDITORIA

En primer lugar se dice que la palabra Auditoría viene del Latín Auditorius y de ésta proviene Auditor de la cual se dice que poseen la virtud de escuchar y revisar cuentas y cuyo objetivo específico es el de evaluar la eficiencia y eficacia con que se opera.

Hay muchos que entienden incorrectamente este término y lo consideran como aquel encargado de detectar errores y señalar fallas; Auditoría en si posee un concepto más amplio ya que además de señalar y detectar errores se encarga de llevar a cabo un examen detallado de lo que una

sección u organización realiza, para que posteriormente tengan un funcionamiento acorde a lo que se desea.

A lo largo de el tiempo se han venido dando muchas definiciones sobre lo que es Auditoría y con el transcurso del tiempo éstas se han venido mejorando debido a la gran utilidad que esta actividad brinda. De acuerdo a la investigación realizada se han elegido varias definiciones de Auditoría para sacar provecho de la esencia de cada una.

Según el Boletín "C" de Normas de Auditoría del Instituto Mexicano de contadores se define como aquella actividad que no es meramente mecánica en la cual se incluyen ciertos procedimientos cuyos resultados, una vez llevados a cabo, son de carácter indudable. La auditoría requiere el ejercicio de un juicio profesional, sólido y maduro, para juzgar los procedimientos que deben de seguir y estimar los resultados obtenidos.

Para Kell Ziegler y su libro Auditoría Moderna, la Auditoría es el proceso sistemático donde se obtiene y evalúa la evidencia de una manera objetiva respecto a las afirmaciones concernientes a actos económicos y eventos para determinar el grado de correspondencia entre estas afirmaciones y criterios establecidos y comunicar los resultados a los usuarios interesados.

4.3 TIPOS DE AUDITORIAS

Con el correr del tiempo la Auditoría a venido dando cambios en cuanto a como dar un control más adecuado a todas las operaciones que se realizan dentro de una organización o Empresa. Es por esto que se ha hecho necesario que la Auditoría sea clasificada en diferentes tipos, para que a partir de ésta, sus procesos de ejecución sean más ordenados y fáciles de controlar:

1- Auditoría Financiera

2- Auditoría Operacional

3- Auditoría Administrativa

4- Auditoría de Sistemas

1- AUDITORIA FINANCIERA

Como propósito y finalidad de esta Auditoría se puede mencionar el dar confianza a los interesados en la información financiera. Con esta finalidad el Auditor se prepara, a través del examen de los estados financieros, para expresar su opinión profesional sobre la razonabilidad con que éstos presentan los resultados de la gestión ejercida por los directores.

Este tipo de Auditoría tiene como objeto de examen los estados financieros, los registros contables y documentos que soportan la información contenida en los primeros y que reflejan el efecto de las operaciones y transacciones financieras realizadas por la empresa en un período determinado. Con el propósito de especificar la naturaleza, el alcance y la oportunidad de los procedimientos de auditoría aplicables en su examen, el Auditor evalúa el control interno financiero haciendo énfasis en dos de sus objetivos: que proporcione información constante, completa y oportuna y que sirva de protección a los activos de la empresa.

2- AUDITORIA OPERACIONAL

Esta Auditoría persigue favorecer a los directores en el ejercicio de una gestión administrativa más eficaz, con la consecuente obtención de resultados más beneficiosos; es decir, examina la causa de los resultados y no los resultados mismos. En este caso el Auditor se prepara a través del examen de la superaciones, para verificar el logro de objetivos y el cumplimiento de políticas y procedimientos, y para recomendar mejoras en las operaciones en términos de eficiencia y eficacia.

El objetivo de realizar una auditoría operacional es evaluar: procedimientos de operación, métodos de control y manejo de recursos, cuyo desarrollo constituye la causas de los resultados obtenidos por la empresa en un período determinado. El Auditor Operacional centra su atención en el examen del control interno, no solo del área financiera sino de todas las áreas y hace énfasis en la promoción de eficiencia de operación y en el cumplimiento de la política establecida.

3- AUDITORIA ADMINISTRATIVA

Esta Auditoría examina los métodos administrativos y la eficacia de todas las funciones y operaciones de la empresa, con la finalidad de evaluar la capacidad administrativa en todos los niveles jerárquicos de la organización.

La Auditoría Administrativa evalúa los métodos administrativos y de operación, y examina la administración de las operaciones, no solo con referencia a la función de control, como lo hace la auditoría operacional, sino también a las otra funciones de planeación, organización, dirección y ejecución; es decir, examina el proceso

administrativo en conjunto, abarcando las funciones y operaciones ya sea parcial o integralmente, y en todo caso incluyendo personas y/o departamentos en todo los niveles jerárquicos.

En la Auditoría Administrativa se adquiere el compromiso de solucionar los problemas detectados y de ejercer labor de seguimiento posterior a la implantación de las soluciones, con el objeto de asegurar una mejor gestión administrativa de los directores.

4- AUDITORIA DE SISTEMAS

No se da una explicación de esta disciplina ya que es el objeto de estudio del presente trabajo de graduación y se explica con mayor detalle a lo largo de éste.

4.4 TIPOS DE AUDITORES

De acuerdo a la necesidad que una empresa requiera en cuanto a auditar actos y eventos económicos, existen en el medio grupos de personas que se encargan de llevar a cabo la Auditoría, estos dependiendo a lo que realicen se pueden clasificar en:

- Auditores Independientes
- Auditores Internos
- Auditores del Gobierno
- Auditores de Interés Especial

AUDITORES INDEPENDIENTES

Estos son los que trabajan por su propia cuenta ó trabajan como miembros de un despacho de contadores públicos.

Los clientes a los que les prestan servicios, se incluyen aquellos cuyo objetivo son la obtención de utilidades, organizaciones sin fines de lucro, dependencias gubernamentales e individuos. Por el momento se dice que para ser independiente, el Auditor debe de evitar opiniones o juicios hechos antes de tener un verdadero conocimiento del cliente al que se le está auditando.

Para efectos de comparación y como un ejemplo de como diferenciar lo que es independencia con lo que es dependencia tomemos a un Auditor Independiente y a un Abogado. El Auditor siempre mantendrá lo que es su independencia al realizarle a su cliente la auditoria, mientras que el

Independiente y a un Abogado. El Auditor siempre mantendrá lo que es su independencia al realizarle a su cliente la auditoria, mientras que el abogado "favorecerá" al cliente a quien le presta sus servicios legales y por lo tanto tendrá que mantener la dependencia.

AUDITORES INTERNOS

Estos se involucran en la evaluación de actividades independientes dentro de una organización como un servicio para esta misma. El objetivo principal es de brindarles ayuda a los administradores con respecto a la delegación de responsabilidades dentro de la organización.

Se dice también que los auditores internos pueden completar el trabajo hecho por los auditores independientes cuando se refiera a auditorías de trabajos financieros.

Dentro de las características importantes que un Auditor Interno debe poseer están: de ser objetivo al realizar su trabajo y al obtener resultados informar sobre sus hallazgos.

AUDITORES ESPECIALES

Estos se dedican a trabajar normalmente para un organismo gubernamental o para una empresa cuyo objetivo es el de una revisión contable realizada junto con el grupo que ha hecho un negocio.

Dentro de este tipo de Auditores están los Auditores del Gobierno, como su nombre lo dice estos son empleados por las dependencias del gobierno ya sean locales, estatales y federales. Solamente existen 2 agencias que tienen este tipo de auditores: El U.S. General Accounting Office (GAO) y el Internal Revenue Service (IRS).

La GAO es una agencia federal de gobierno, no perteneciente a ningún partido político responsable de realizar la función de Auditoría para el gobierno. La IRS es una agencia del departamento del tesoro que es responsable de la Administración de las leyes fiscales federales.

Hasta este momento la AGA (Asociación de Contadores de Gobierno/ Association of Gobernment Accountants) no ha extendido certificado para este tipo de Auditores, aunque la mayoría poseen títulos de contadores públicos independientes o auditores internos.

CAPITULO 5

AUDITORIA DE SISTEMAS (ADS)

5. AUDITORIA DE SISTEMAS (ADS)

Luego de haber incursionado en el aspecto de sistemas y de auditoria y haber dado algunas definiciones relacionadas con estos términos, se puede proceder a profundizar en lo que será el tema principal de este estudio, la Auditoría de Sistemas, no sin antes definir lo que se entiende por esta disciplina.

5.1 DEFINICION DE AUDITORIA DE SISTEMAS

Antes de dar una definición de "Auditoría de Sistemas", es necesario aclarar que este término es normalmente mal utilizado pues en él se quieren encerrar una serie de actividades que no le corresponden ,así como también se le adjudican otras para las que el término se queda corto. Se hará uso de "Auditoría de Sistemas", debido a que es lo normalmente aceptado, pero se estará hablando de "Auditoría en Informática".

Investigando y analizando diferentes conceptos de auditoría de sistemas, se ha tomado como el más completo, el siguiente: "Es la revisión y evaluación de los controles, sistemas, procedimientos de informática, de

los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participa en el procesamiento de la información a fin de que por medio del señalamiento de distintas alternativas, se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

La auditoría de sistemas deberá comprender no solo la evaluación de los equipos de cómputo o de un sistema o procedimiento, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información. Ello debe incluir los equipos de cómputo como la herramienta que permite obtener la información adecuada y la organización específica que hará posible el uso de los equipos de cómputo.

Conforme la sociedad se va haciendo más compleja y su tecnología avanza a pasos agigantados, se ha visto la necesidad de crear esta nueva disciplina. Se pueden mencionar algunas de las razones por las que ha surgido este tipo de auditoría especializada: Las pistas utilizadas por la auditoría ya no son documentos visibles o físicos, sino más bien medios magnéticos. Se ve la aparición de nuevos procedimientos relacionados directamente con la "mecanización" de las transacciones en las empresas

por lo que se requieren nuevos tipos de auditoría. La seguridad física adquiere nuevos enfoques y se deben integrar nuevas normas de seguridad.

5.2 OBJETIVOS DE LA AUDITORIA DE SISTEMAS

Para poder entender bien los objetivos de una auditoría de sistemas no se debe perder de vista lo que se espera de un Auditor de Sistemas, que puede delinearse en lo siguiente:

- Que pueda prevenir los riesgos posibles en el área a examinar.
- Que sepa evaluar y determinar los controles necesarios, ya sean estos existentes o por implantar.
- Que lleve a cabo técnicas avanzadas de Auditoría.
- Que pueda interrelacionarse con las demás disciplinas de la empresa.
- Que brinde la comunicación necesaria a la Administración, cuando ésta lo solicite.

Se puede entonces definir los objetivos de la Auditoría de Sistemas como sigue:

◊ Cumplimiento de Políticas, Planes, Procedimientos, Normas y Reglamentos.

La Auditoría debe revisar la existencia de cada uno de estos aspectos para lograr la integración completa del área de sistemas a través de mecanismos preestablecidos así como también el cumplimiento de los mismos, y en caso necesario mejorarlos.

◊ Salvaguardar Activos.

Como puede deducirse, se debe proteger todos los activos a través de controles internos. Simultáneamente debe realizarse una evaluación de eficiencia de todos los controles que se llevan en ese momento. Se entiende por activos de los sistemas a los equipos, aplicaciones, archivos, documentos, programas y suministros. No debe olvidarse que el activo más importante y delicado es la información.

◊ Integridad de la Información.

Toda organización debe tener siempre presente que su éxito dependerá de la integridad de su información. Si la información que manipula una empresa no es representativa de la realidad, ésta no podrá autoevaluarse y mucho menos lograr el control de lo que ocurre dentro

de ella. La integridad de la información es indispensable para el proceso de toma de decisiones.

◊ Efectividad de los Sistemas.

Se puede medir la efectividad de un sistema en la medida en que se puede medir el cumplimiento de sus objetivos y para ello es necesario estar empapado de las necesidades de los usuarios y de sistema en si.

A través de la Auditoría de Sistemas es posible identificar y cuantificar la efectividad de un sistema, ya sea durante la etapa de desarrollo de este o después de que fue implantado.

◊ Eficiencia de los Sistemas.

Cuando se habla de eficiencia se entiende logro de objetivos con el mínimo de recursos sin ir en detrimento de los demás sistemas ni del sistema en cuestión.

La medición de la eficiencia no es tan cuantificable, ni existen procedimientos específicos para determinar la eficiencia de un sistema, sin embargo, a través del uso de técnicas de auditoría se

puede analizar el consumo de recursos, los tiempos de respuesta y los demás aspectos desmembrados de un sistema y concluir o recomendar soluciones y procedimientos para mejorar su eficiencia.

NOTA: De las definiciones del Nuevo Diccionario Español Sopena se obtiene lo siguiente: "Eficacia es virtud, actividad, fuerza para poder obrar y Eficiencia es virtud y facultad para lograr un efecto determinado" por lo que eficacia es simplemente lograr los objetivos, mientras que eficiencia es poder lograr lo planeado con los menores recursos posibles.

◊ Economía de los Sistemas

Se logra la economía de los sistemas cuando estos están dando los resultados deseados y para ello se ha incurrido en el menor gasto posible.

5.3 BENEFICIOS DE LA AUDITORIA DE SISTEMAS

Si se hiciera una lista detallada de todos los beneficios que se obtienen de aplicar una auditoría, se podría elaborar un documento completo solo de este aspecto.

Se exponen a continuación algunos de los beneficios más tangibles de la elaboración de una Auditoría de Sistemas.

Una de las mayores debilidades de cualquier instalación de sistemas de información, es la cantidad de riesgos a que se ve expuesta. Dentro de estos riesgos se pueden mencionar:

- Pérdida de los activos de información
- Incorrecta toma de decisiones sobre recursos de la empresa basadas en sus sistemas de información.
- Posibilidad de fraude o desfalco en la organización.
- Costos derivados de los errores cometidos por el sistema.
- Fallas de seguridad en la información.

En alguna medida, estos riesgos significan pérdida de los recursos con que cuenta una organización. La mejor forma de reducir o eliminar estos riesgos en la mayor medida posible, es el establecimiento de controles. Esto puede sin embargo, significar un incremento en los costos, sobre todo si estos controles son innecesarios, no utilizados correctamente, redundantes o excesivos.

Puede entonces visualizarse que uno de los beneficios de la auditoría de sistemas, es que permite el establecimiento de estos controles, evaluar el funcionamiento de los mismos y más lejos aún, presentar mejoras al sistema de control.

Todo esto puede resumirse en una verdadera reducción de riesgos a los que se puede encontrar expuesta el área de informática.

5.4 APLICACIONES DE LA AUDITORIA DE SISTEMAS

Dentro de las diferentes aplicaciones que realiza la Auditoría de Sistemas, se han elegido 4 grandes áreas en las que se agrupan la mayoría de actividades relacionadas con esta disciplina.

A través de estas aplicaciones se puede realizar una mejor evaluación de todas la actividades de Informática que se realizan en una organización.

5.4.1 EVALUACION DEL AREA DE INFORMATICA

En ésta se procede a efectuar la inspección del lugar a través de los métodos de observación y entrevistas de fondo, del cual deberá acatar lo siguiente:

- Una buena Estructura Orgánica
- Verificar el desempeño de las funciones
- Revisar la situación de los recursos humanos
- Conocer la situación presupuestal de la Organización

5.4.1.1 INFORMACION SOBRE LA ORGANIZACION

Después de que se han analizado y estructurado los planes de auditoría en los cuales se plantean las distintos elementos que la componen como tiempos, costos y prioridades, es necesario iniciar la recopilación de información que servirá para realizar una buena auditoría.

Deberá recopilarse información de diferentes áreas y situaciones dentro de las cuales es importante mencionar:

A) Estructura Orgánica.

- Jerarquías
- Estructura Orgánica
- Funciones
- Objetivos

B) Es necesario censar y analizar la situación de los Recursos Humanos.

- Personal Disponible
- Determinación de Puestos
- Salarios
- Capacitación
- Conocimientos
- Experiencia Profesional
- Antigüedad
- Historial de Trabajo
- Movimientos Salariales
- Rotación del Personal

C) Se entrevistará personal de Procesamiento Electrónico de Datos

- Jefatura
- Análisis
- Programadores
- Operadores
- Digitadores
- Personal Administrativo

D) Deberá hacerse un análisis de los presupuestos.

- Presupuestos
- Recursos Financieros
- Recursos Materiales
- Mobiliario y Equipo

E) Se debe revisar el cumplimiento de los Documentos Administrativos.

- Normas y Políticas
- Planes de Trabajo
- Controles
- Estándares
- Procedimientos

La recopilación de información será útil para asentar una buena base para la realización de una auditoría. Dentro de sus usos más específicos se pueden mencionar: Determinar si las responsabilidades en la organización están definidas adecuadamente; si la estructura organizacional está adecuada a las necesidades; si se tienen los objetivos y políticas adecuadas, se encuentran vigentes y están bien definidas; si existe documentación de las actividades, funciones y responsabilidades, si los puestos se encuentran definidos y señaladas sus responsabilidades; si el nivel de salarios esta de acuerdo al mercado de trabajo; si los planes de trabajo concuerdan con los objetivos de la empresa; si se cuenta con los recursos humanos necesarios que garanticen la continuidad de la operación o se cuenta con "indispensables"; si se evalúan los planes y se determinan las desviaciones; etc.

5.4.1.2 ESTRUCTURA DE LA ORGANIZACION

Para desarrollar una buena evaluación de la estructura orgánica es necesario solicitar lo que se conoce como manual de organización y

realizar una revisión detallada del mismo, el cual deberá de estar compuesto como mínimo de lo siguiente:

- Organigrama con sus Jerarquías
- Funciones
- Objetivos y políticas
- Análisis, descripción y evaluación de puestos
- Manual de procedimientos
- Manual de normas
- Instructivos de trabajos

Una vez hecha la revisión del manual, se deberá de elaborar un cuestionario, que tendrá por objeto conocer la organización del departamento de informática y su dependencia dentro de la organización total, los cuales tendrán que ser llenados por el Jefe de Informática o por aquellas personas con un cargo de directivo.

Ya que se hizo mención de la dependencia que pueda tener el área de informática dentro de la organización, se ha considerado que ésta puede ser de cuatro tipos:

1) Los que dependen de una dirección, por lo general de finanzas. Esto se debe a que al principio el departamento de informática se encargaba solamente de procesar información de tipo contable, financiera o administrativa, por ejemplo: facturación, nóminas, etc.

Esta forma de depender de una dirección o gerencia se da normalmente en estructuras pequeñas o en aquellas que comienzan a utilizar el área de informática.

Dentro de la ventaja que pueda tener este tipo de dependencia esta la no creación de una estructura adicional para el área de informática dentro de la organización permitiéndole al que dirige el departamento, tener un mejor control de los sistemas.

Su principal desventaja es que al resto del personal que labora en el departamento se le considera como secundario y no se le da la importancia ni la prioridad que estos necesitan. Otra de las desventajas es que suele suceder que el Gerente de Finanzas

no tiene los conocimientos necesarios sobre informática. (Gráfica 3)

2) Los que dependen de la Gerencia General.

Esta dependencia puede darse de dos formas: en línea (gráfica 4) o como asesoría (gráfica 5). La ventaja que ofrece esta dependencia es proporcionar al jefe del área de informática un mejor nivel dentro de la organización, lo que le permitirá tener una mejor comunicación con los otros departamentos y brindarles un mejor servicio con la asignación de prioridades dada por la Gerencia General.

Su desventaja será el incremento de la estructura organizacional, lo que ocasionará que los costos en la utilización de los sistemas computarizados se eleven.

3) Otra de las posibilidades se presenta en estructuras de tamaño considerablemente grande, en donde se cuenta con bases de datos, redes y distribución de equipo en diferentes lugares.

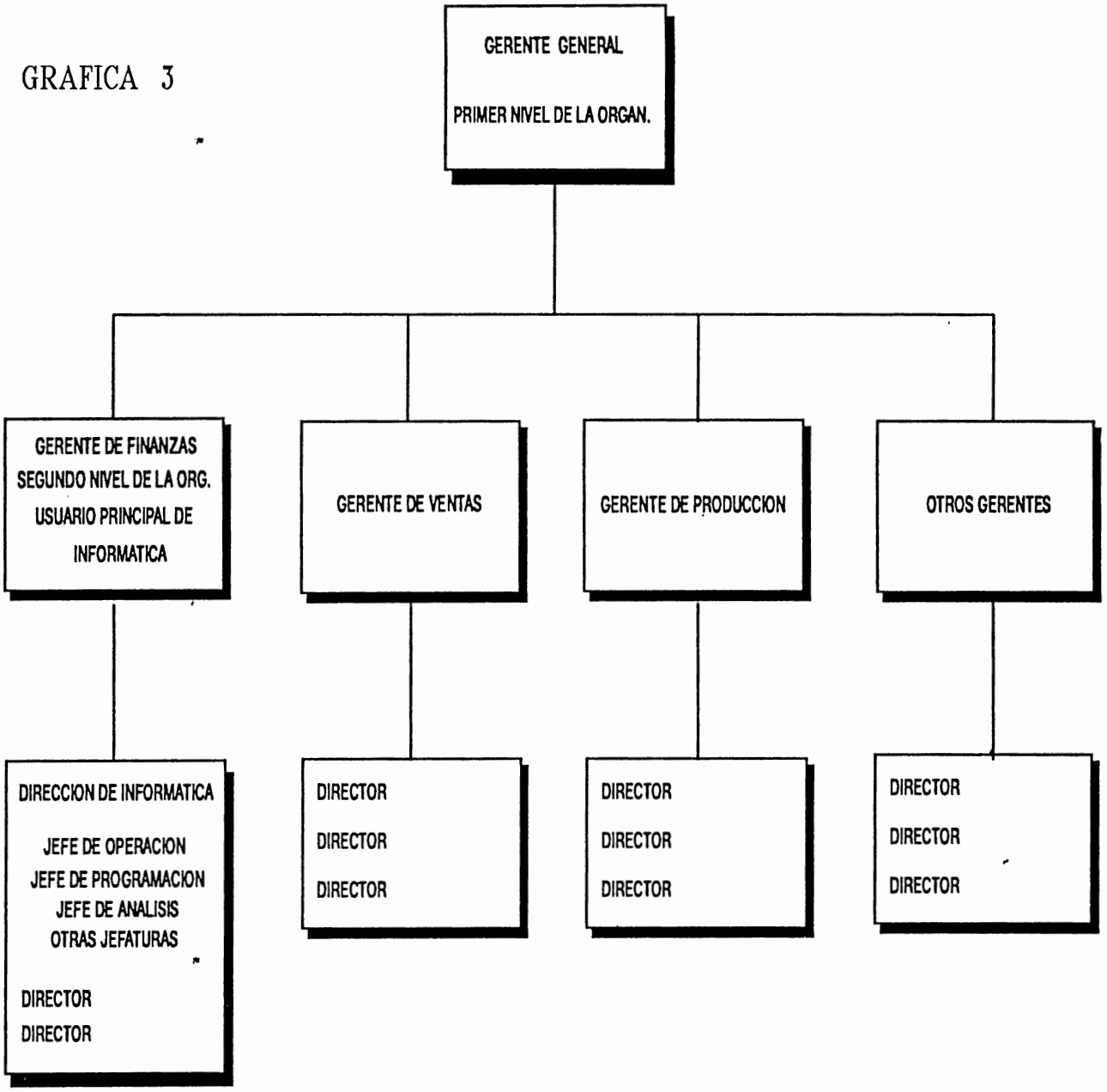
En este caso, el área de informática depende generalmente de la Gerencia General o de otros departamentos de informática de menor volumen o capacidad dentro de las distintas Gerencias en la misma organización. Todas las reglas, políticas, procedimientos y estándares están dados por el área de central de informática, aunque sus funcionamientos dependan de la Gerencia General.

Para estas dependencias, es necesario especificar las funciones de cada departamento para evitar que exista duplicidad de mando y duplicidad en el desarrollo de sistemas o programas.

Su principal ventaja es que se puede tener centralizada la información y descentralizados los equipos, y para el logro de esto, debe existir una buena coordinación del área de informática y los departamentos que poseen una sección de informática. (Gráfica 6)

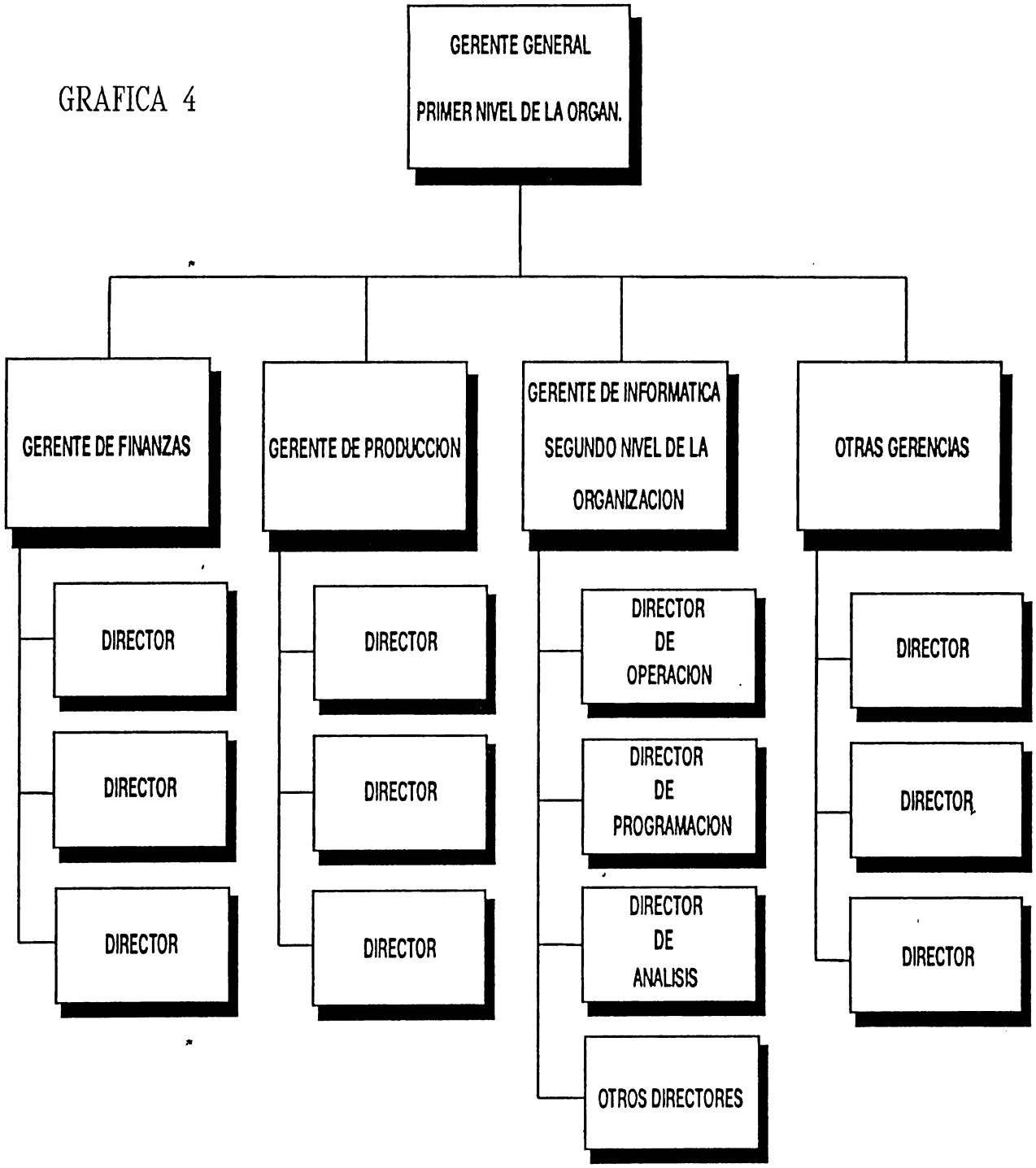
LA DIRECCION DE INFORMATICA ESTA DEPENDIENDO DE LA GERENCIA DE FINANZAS O DEL USUARIO PRINCIPAL

GRAFICA 3



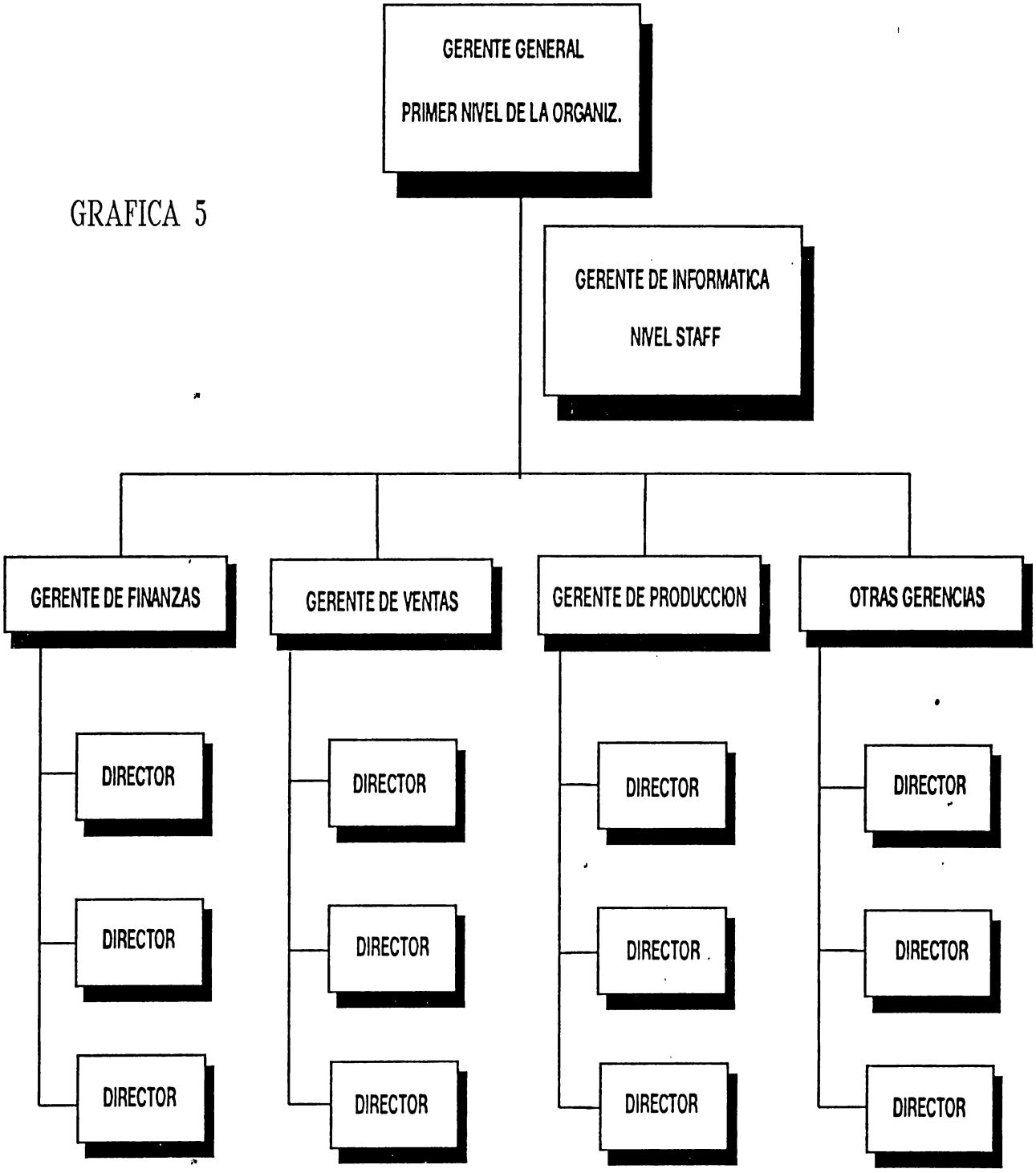
LA GERENCIA DE INFORMATICA SE ENCUENTRA DEPENDIENDO DE LA GERENCIA GENERAL

GRAFICA 4



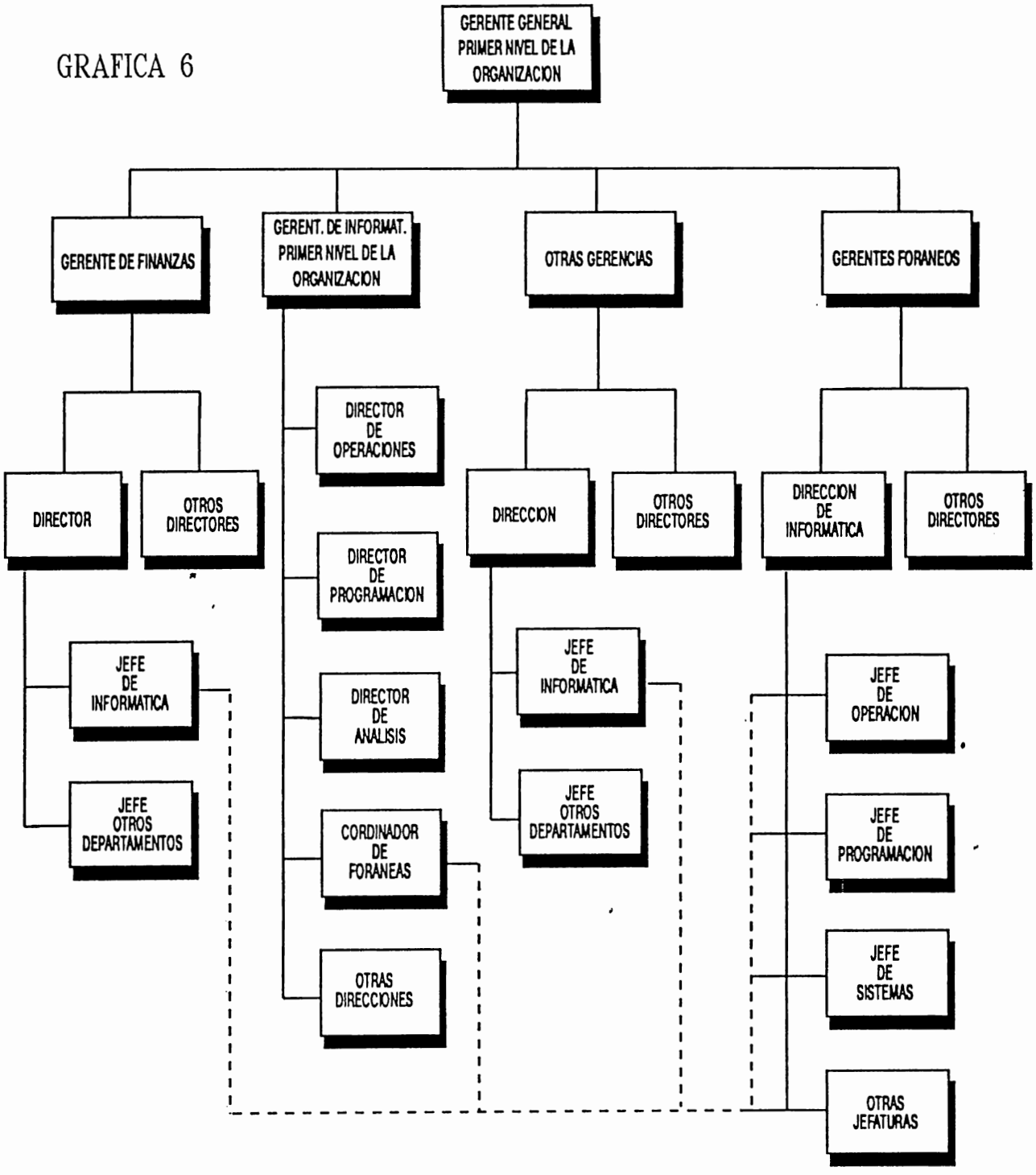
LA GERENCIA DE INFORMATICA ESTA DEPENDIENDO DE LA GERENCIA GENERAL COMO STAFF

GRAFICA 5



LA GERENCIA DE INFORMATICA SE ENCUENTRA DEPENDIENDO DE GERENCIA GENERAL Y SE TIENE UNA ORGANIZACION CORPORATIVA

GRAFICA 6



4) La última forma es la creación de una organización independiente que preste servicios de informática a varias empresas o a la misma empresa en diferentes lugares como podría ser el caso de una empresa multinacional.

Dentro de la Estructura de la Organización existen diferentes aspectos que deben tomarse en cuenta al momento de realizar una auditoría.

a) Estructura Orgánica

Aquí se analizan situaciones relacionadas directamente con la forma en que está estructurada la organización.

Se deben considerar los aspectos legales o jurídicos y verificar si la estructura de la organización se ajusta a las disposiciones jurídicas vigentes.

Se deben conocer los niveles jerárquicos para poder evaluar si son los necesarios y si están bien definidos.

Se debe considerar la departamentalización, y constatar si los departamentos, áreas y oficinas en que esta dividida la organización son los adecuados.

Se deben definir correctamente los puestos y las funciones de cada uno de ellos para evitar la confusión al momento de dar los nombres a los puestos en el área de informática.

Es necesario verificar que se están cumpliendo las expectativas establecidas. En esta sección se pueden detectar deficiencias y frustraciones del personal.

Un aspecto muy importante es definir las líneas de autoridad y verificar si esta está de acuerdo a las responsabilidades asignadas.

b) Funciones

Es frecuente encontrar que las funciones en el área de informática difieren de un organismo a otro a pesar de que se designen con nombres iguales.

Primeramente se debe establecer la existencia de funciones en el área, si están documentadas y autorizadas.

Las funciones deberán estar encaminadas a la consecución de objetivos y acordes al reglamente interno.

Se debe velar por que las funciones establecidas sean cumplidas a cabalidad y que se realicen las actividades determinadas para cada una de ellas.

Es necesario determinar si para el cumplimiento de las funciones se debe contar con el apoyo de otras áreas y tener el cuidado suficiente para evitar la duplicidad de funciones.

c) Objetivos

Un aspecto muy importante es el establecimiento de objetivos y la correcta comunicación de los mismos entre el personal involucrado. La falta de estos puede provocar un desajuste en la planeación.

Como primer paso se debe verificar la existencia de los objetivos para cada área los cuales deberán ser congruentes con los objetivos de las demás áreas de la organización.

El establecimiento de objetivos debe realizarse de manera formal, por escrito, de forma sencilla y clara y deben ser específicos evitando ambigüedades. Deben de hacerse del conocimiento del departamento y de aquellas personas encargadas de verificar su cumplimiento.

Los objetivos deben ser los adecuados, tratando de abarcar toda la operación del área, deben ser realistas y ante todo alcanzables, de acuerdo a las funciones del área y deben servir como guía y motivación para el personal.

No solo será necesario verificar su cumplimiento sino establecer mecanismos para poder conocer o medir en que forma se están cumpliendo y en donde están fallando.

Los objetivos de una organización deberán ser revisados y mantenerse actualizados. Al mismo tiempo que sean rígidos deberán tener cierto grado de flexibilidad para permitir la incorporación de modificaciones.

d) Análisis de Organizaciones

Existen en la informática diferentes formas de establecer las funciones de esta área. Por ejemplo, en una organización pueden considerarse algunas funciones propias de un programador mientras que en otra organización, las mismas funciones serán asignadas a un analista, o podría existir una división de niveles para las funciones: Programador I, Programador II, Programador III.

Al no existir una definición estándar de los niveles, funciones y conocimientos en el área de informática, se obtiene como resultado que en las organizaciones se den diferentes tipos de nombramientos que en muchos casos son erróneos. Por ejemplo se encuentran en las organizaciones Ingenieros en Sistemas sin haber obtenido el grado académico. O también

existen una serie de escuelas "técnicas" que confieren grados académicos que no son reconocidos oficialmente. Por ello es necesario que la auditoría tome en cuenta de que forma se analizarán las funciones y cual será el procedimiento de evaluar al personal que ingrese a los diferentes niveles de la organización.

Debe contarse con un organigrama de la organización, y en caso de que no exista, el auditor deberá recomendar la elaboración de uno y dar algunos lineamientos guía para una buena estructuración del mismo.

Cuando se realiza un estudio de la estructura orgánica, se deben tomar en cuenta una serie de aspectos para la asignación de tareas a cada puesto:

Existen líneas de autoridad justificadas?

Hay una extralimitación de funciones?

Hay demasiada supervisión de funcionarios?

Es excesiva la supervisión en general?

Hay uniformidad en las asignaciones?

5.4.1.3 RECURSOS HUMANOS

Dado que este es uno de los recursos más valiosos de cualquier organización, debe tenerse especial cuidado en la evaluación de esta área. Se debe recabar información sobre la situación del personal, y algunos de los aspectos que deben considerarse son los siguientes:

- Desempeño y comportamiento
- Condiciones de trabajo
- Ambiente
- Organización en el trabajo
- Desarrollo y motivación
- Capacitación
- Supervisión

Estos aspectos, por mencionar algunos, involucran una serie de actividades que deben ser controladas: Se cuenta con el personal suficiente para el desarrollo de funciones y es este personal el idóneo, capacitado, eficaz.

La capacitación es un aspecto muy importante dentro del área de informática debido al constante cambio; se debe incluir dentro de los programas de capacitación los siguiente: dirección, análisis, programación, operación, administración, digitación, etc.

Las condiciones de trabajo deben de tenerse siempre presentes para aumentar la productividad del personal.

Uno de los puntos más difíciles en una organización es la remuneración al personal. Normalmente, el personal esta inconforme con su remuneración o en todo caso desearía que esta fuese mejor. Debe analizarse si esta situación se debe a conflictos externos a la remuneración en si así como también se debe mantener una competitividad salarial en cuanto al medio externo. No siempre las remuneraciones son en el aspecto dinero, pueden darse otro tipo de beneficios.

Relacionado con las condiciones de trabajo esta el ambiente de trabajo el cual es particularmente importante en el área de informática para poder obtener un adecuado desarrollo de sistemas. Se debe considerar si las condiciones ambientales son

adecuadas con respecto a: espacio del área, iluminación, ventilación, equipo, mobiliario, ruido, limpieza, instalaciones sanitarias, instalaciones de comunicación, etc.

Por último pero no menos importante debe de tomarse en cuenta el desarrollo y motivación del personal. Se debe dar oportunidad a toda persona a tener un desarrollo creciente, se debe motivar adecuadamente al personal, lo que significa que debe existir un plan de estímulos y recompensas. Se debe dar oportunidad de ascensos y promociones.

5.4.1.4 PRESUPUESTOS

Es necesaria la obtención y análisis de la situación presupuestal del departamento de informática. Es necesario exponer desde un punto de vista económico el estado y disposición de las distintas características que conforman al departamento.

1. Costos del departamento, desglosado por áreas y controles.
2. Presupuesto del departamento, desglosado por áreas.
3. Características de los equipos, número de ellos y contratos.

Deben existir planes para calcular el gasto total para un determinado período, del área de informática. Esto significa desarrollar un programa de contabilidad de costos, el cual debe ser conocido por los usuarios. Se debe poder comparar lo gastado con lo presupuestado. Se deben involucrar aspectos como personal, aplicaciones, equipo, mobiliario, papelería, cintas, discos, etc.

También deben considerarse aspectos menos cuantificables pero que también involucran costos en el área de informática: utilización del equipo, mantenimientos, capacitaciones, asesorías, instalaciones, seguros, etc.

5.4.2 EVALUACION DE LOS SISTEMAS

Esta es una de las áreas que deben evaluarse con mayor detalle, para lo que debe existir un plan estratégico para la elaboración de sistemas y evaluar si se están elaborando con las prioridades y objetivos adecuados.

Para el plan estratégico se deben tener respuestas a lo siguiente:

¿ Cuáles servicios se implementarán?

¿ Cuándo deberán estar disponibles para los usuarios?

¿ Qué características tendrán?

¿ Cuantos recursos requerirá el sistema?

Para poder desarrollar los sistemas deberá seguirse una estrategia preestablecida la cual deberá indicar qué aplicaciones y recursos proporcionará el área de sistemas y bajo que arquitectura se fundamentarán.

¿ Qué aplicaciones serán desarrolladas y cuándo?

¿ Qué tipos de archivos se desarrollarán?

¿ Qué bases de datos serán desarrolladas?

¿ Qué lenguajes y software será utilizado?

¿ Qué tecnología será utilizada y cuándo será implementada?

¿ Cuántos recursos se requerirán aproximadamente?

¿ Cuanto será la inversión en cuanto al hardware y software?

Se debe realizar una investigación en cuanto a los usuarios del sistema, de quienes se debe obtener valiosa información como requerimientos,

objetivos, metodología, recursos con que se cuenta, personal necesario y usuarios finales, etc.

Para una adecuada planeación de sistemas es necesario asegurarse que se han identificado y evaluado todos los recursos requeridos en el plan de desarrollo de aplicaciones. Es primordial, que estos recursos sean compatibles con la estrategia, arquitectura, tecnología con que se cuenta para el desarrollo.

Para poder señalar los problemas de los sistemas, se debe detectar primeramente los síntomas, los cuales normalmente reflejan el área problemática para que después de analizar los síntomas se pueda definir y detectar las causas, parte medular de la Auditoría.

Es imprescindible aprender a diagnosticar, es decir, reunir todos los síntomas y distinguirlos antes de señalar las causas, evitando confundir uno con el otro y desechar todo aquello que sea trivial y sin fundamento.

Los sistemas deben ser evaluados de acuerdo al ciclo de vida que normalmente siguen: requerimientos del usuario, estudio de factibilidad,

diseño general, análisis, diseño lógico, desarrollo físico, pruebas, implementación, evaluación, modificaciones, instalación, mejoras.

Lo primero que debe evaluarse de un sistema es su estudio de factibilidad, determinar si es susceptible de realizarse, establecer la relación beneficio/costo, en conclusión, determinar si su elaboración es favorable.

Si el sistema ya existe, se deberá comprobar si se realizó el estudio de factibilidad con los puntos especificados y se comparará con la realidad, es decir, si el estudio de factibilidad señaló determinado costo y una serie de beneficios de acuerdo a las necesidades requeridas, se debe verificar cual fue su costo real y evaluar si en realidad se satisfacieron las necesidades indicadas.

Algunos de los beneficios que justifican el desarrollo de un sistema son: el ahorro en los costos de operación, la reducción de tiempo de proceso de un sistema, mayor exactitud, mejor servicio, mejoría en los procedimientos de control, mayor confiabilidad y seguridad, etc.

Algunos de los problemas más comunes en los sistemas son:

- Falta de estándares en el desarrollo, en el análisis y la programación.
- Falta de participación y de revisión por parte de la alta gerencia.
- Falta de participación de los usuarios.
- Inadecuada especificación del sistema al hacer el diseño detallado.
- Deficiente análisis costo/beneficio.
- Nueva tecnología no usada o usada incorrectamente.
- Inexperiencia por parte del personal de análisis y del de programación.
- Diseño deficiente.
- Proyección pobre de la forma en que se realizará el sistema.
- Control débil o falta de control sobre las fases de elaboración del sistema y sobre el sistema en sí.
- Inadecuados procedimientos de seguridad, de recuperación y de archivos.
- Falta de integración de los sistemas con sus subsistemas.
- Documentación inadecuada o inexistente.
- Dificultad para dar mantenimiento al sistema.
- Problemas en la conversión e implementación.
- Procedimientos incorrectos o no autorizados.

5.4.2.1 ANALISIS Y DISEÑO

Análisis

Se evaluarán en esta fase las políticas, procedimientos y normas establecidas para la realización del análisis.

También se evaluará la planeación de las aplicaciones. Estas pueden provenir de:

a. Planeación Estratégica: Se agruparán las aplicaciones en conjuntos relacionados entre sí y no como programas aislados. En estas aplicaciones estarán comprendidos todos los sistemas que pueden ser desarrollados sin importar los recursos que serán necesitados y sus justificaciones.

b. Requerimientos de los usuarios.

c. Inventario de los sistemas en procesos. Estas aplicaciones pueden agruparse de acuerdo a su situación:

- Planeada para ser desarrollada en el futuro.
- En desarrollo.
- En proceso, pero con modificaciones en desarrollo.
- En proceso con problemas detectados.
- En proceso sin problemas.
- En proceso esporádicamente.

Debe notarse que es necesario documentar detalladamente la fuente que generó la necesidad de la aplicación.

La auditoría de sistemas se encarga de evaluar los documentos y registros usados en la elaboración del sistema, así como todas las salidas y reportes, la descripción de las actividades de flujo de la información y de procedimientos, los archivos almacenados, su uso y su relación con otros archivos y sistemas, su frecuencia de acceso, su conservación, su seguridad y control, la documentación propuesta, las entradas y salidas y los documentos fuente a usarse.

Diseño

En esta etapa se deberán analizar las especificaciones del sistema. Qué debe hacer, cómo lo debe hacer, la secuencia y ocurrencia de los datos, el proceso y la salida del sistema.

Los aspectos a evaluar en esta etapa son:

- Entradas
- Salidas
- Procesos
- Especificaciones de datos
- Especificaciones de proceso
- Métodos de Acceso
- Operaciones
- Manipulación de datos
- Proceso lógico para producir informes
- Identificación de archivos, tamaño de los campos y registros
- Proceso en línea o lote y su justificación
- Frecuencia de volúmenes de operación
- Sistemas de seguridad

- Sistemas de control
- Responsables
- Número de usuarios

Para el estudio de los sistemas en uso se estudiará:

- Manual del usuario
- Descripción del flujo de información
- Descripción y distribución de la información
- Manual de formas
- Manual de reportes
- Lista de archivos y especificación

Se debe determinar para el sistema:

En el procedimiento:

¿ Quien hace, cuándo y como?

¿ Que formas se utilizan en el sistema?

¿ Son necesarias, se usan, están duplicadas?

¿ El número de copias es el adecuado?

¿ Existen puntos de control o faltan?

En el flujo de información:

¿ Es fácil de usar?

¿ Es lógico?

¿ Se encontraron lagunas?

¿ Hay faltas de control?

En las formas de diseño:

¿ Cómo está usada la forma en el sistema?

¿ Que tan bien se ajusta la forma al procedimiento?

¿ Cuál es el propósito, por qué se usa?

¿ Se usa y es necesaria?

¿ El número de copias es el adecuado?

¿ Quien lo usa?

En la auditoría de sistemas se debe estudiar en la fase de diseño dos circunstancias importantes para el no entorpecimiento de los sistemas.

El ruido: esto es todo aquello que interfiere en una adecuada comunicación, no solamente los sonidos sino todo aquello que impida una adecuada comunicación. Ejemplos de este podrían ser

errores en la digitación, pantallas sobresaturadas, reportes inadecuados, etc.

La redundancia: es toda aquella duplicidad que tiene el sistema con la finalidad de que en caso de que exista ruido, esta redundancia permita que la información llegue al receptor en forma adecuada. Como ejemplo de redundancia se conoce el bit de paridad, el que permite que en caso de pérdida de un bit, se pueda recuperar la información que contiene el byte.

4.4.2.2 DESARROLLO E IMPLEMENTACION

Después de dar una breve explicación introductoria a esta fase de la evaluación, se le dará un enfoque un tanto peculiar para poder apreciar mejor la relevancia de la auditoría en esta etapa, exponiendo los objetivos de los controles, objetivos de la auditoría y aspectos de las pruebas de auditoría para cada etapa en el desarrollo e implementación de sistemas.

Controles del Desarrollo de Sistemas

Para la implementación de sistemas de información o computarizados existen diferentes métodos, ya sea para programas desarrollados en el departamento o software especializado y especifico adquirido fuera de la organización, o incluso una combinación de ambos. Independientemente de cual sea el caso, las actividades de administración para los proyectos deberán ser consistentes para cada uno de ellos. La instalación deberá tener lineamientos guías debidamente documentados de tal manera que se logre estandarizar los eventos en cada fase del desarrollo. Estos lineamientos guía deberán proveer a cada encargado de proyecto los argumentos necesarios para cada fase del desarrollo. De esta manera, el administrador de varios proyectos podrá evaluar más fácilmente el desempeño de los encargados de proyectos permitiéndole concentrarse en el progreso de eventos de mayor relevancia.

Cada fase, desde la proposición hasta la implementación, requiere que se agrupen hechos específicos de tal manera que la construcción sea progresiva y que cada paso del desarrollo asiente

la base para el siguiente paso lógico en el programa de actividades. Los controles para el desarrollo de sistemas aseguran que estos hechos sean recabados y debidamente documentados.

Los lineamientos guías para el desarrollo de sistemas deben contener las tareas administrativas que deben ser realizadas, incluyendo:

- Definición del trabajo
- Organización y selección del personal
- Estimación de tiempos y costos
- Desglose y asignación de pasos a seguir
- Procedimientos para implementación de cambios necesarios
- Criterios de aceptación
- Establecimiento de estándares mínimos de comunicación

La revisión de los controles para el desarrollo de sistemas requiere de mucho criterio de parte del auditor para indagar como, cuándo y porqué se debe reaccionar a problemas aparentes.

El proceso de desarrollo deberá ser planificado y organizado de tal forma que progrese en fases con puntos de chequeo adecuados para revisión gerencial o administrativa y su respectiva aprobación.

A continuación se plantean una serie de controles para los que se plantearán sus objetivos y aspectos de auditoría para lo que es el desarrollo e implementación de sistemas.

Objetivo del Control: Asegurar que la proposición de justificación contiene suficiente información relevante, que esta soportada por investigación adecuada y consistente, que fue formulada con la participación adecuada del personal apropiado y que comprueba la efectividad-costo de continuar con el proyecto hacia la fase de factibilidad.

Objetivo de Auditoría: Determinar si la proposición de justificación es precisa y correcta y que además contiene datos relevantes.

Aspectos de Auditoría: La proposición de justificación debe ser evaluada.

Objetivo del Control: Asegurar que se lleve a cabo una investigación adecuada para comprobar la factibilidad del desarrollo del sistema propuesto.

Objetivo de Auditoría: Determinar que el contenido del estudio de factibilidad es preciso.

Aspectos de Auditoría: Esta prueba determina que el planteamiento del estudio se desarrollo en forma lógica y que el problema fue presentado con hechos a través de una revisión profunda de la documentación de la factibilidad.

Objetivo del Control: Aislar adecuadamente y documentar los requerimientos del usuario que serán las bases para el diseño o evaluación del paquete.

Objetivo de Auditoría: Determinar si los requerimientos del usuario contienen todo lo necesario para el proceso y control del sistema.

Aspectos de Auditoría: Los requerimientos del usuario deben ser evaluados para asegurar que fueron preparados con el suficiente detalle y con la participación del usuario.

Objetivo del Control: Proveer un diseño general del sistema propuesto.

Objetivo de Auditoría: Determinar si el diseño general fue preparado partiendo de los requerimientos del usuario, si satisface las necesidades establecidas en la propuesta y si cumple con los elementos del estudio de factibilidad.

Aspectos de Auditoría: El diseño general debe ser revisado para comprobar si es completo y se debe determinar si el diseño no incluirá en su mecanización las ineficiencias de un proceso o sistema existente.

Objetivo del Control: Determinar efectivamente si los paquetes de software que están bajo consideración cumplirán con las necesidades de la organización.

Objetivo de Auditoría: Determinar si el proceso de evaluación del software es profundo y completo y satisface los requerimientos del estudio de factibilidad y las especificaciones de los usuarios.

Aspectos de Auditoría: Se debe establecer si se utilizaron criterios de evaluación precisos.

Objetivo del Control: Asegurar que se realicen las suficientes pruebas para determinar que el paquete es aceptable.

Objetivo de Auditoría: Determinar si la prueba realizada fue adecuada.

Aspectos de Auditoría: La planificación para las pruebas de aceptación y los resultados de las pruebas deberán ser revisadas.

Objetivo del Control: Asegurar que existe un plan preliminar de implementación y que éste refleja adecuadamente el ciclo de vida del sistema aún por realizarse.

Objetivo de Auditoría: Determinar si los elementos restantes del proyecto han sido planificados en forma precisa.

Aspectos de Auditoría: Se debe determinar que el plan preliminar de implementación es el adecuado.

Objetivo del Control: Proveer a la alta gerencia con recomendaciones adecuadas, basadas en los resultados del proyecto a la fecha, lo que permitirá evaluar los beneficios del sistema propuesto.

Objetivo de Auditoría: Asegurar que las recomendaciones hechas a la gerencia son completas y precisas en todos los aspectos.

Aspectos de Auditoría: Se debe determinar que las recomendaciones a la gerencia sean las adecuadas.

Objetivo del Control: Asegurar que el diseño detallado del sistema a desarrollarse internamente es completo en lo que respecta a requerimientos.

Objetivo de Auditoría: Determinar si el diseño detallado incluye todos los elementos materiales en cuanto al sistema y operaciones de la organización.

Aspectos de Auditoría: Se debe revisar la documentación de diseño para asegurar que se incluyen todos los elementos necesarios.

Objetivo del Control: Asegurar que el equipo para el proyecto sea seleccionado adecuadamente.

Objetivo de Auditoría: Determinar si los miembros de equipo seleccionado para el proyecto tienen la experiencia suficiente y la autoridad necesaria para llevar a cabo las tareas del proyecto.

Aspectos de Auditoría: Se debe determinar que la organización y selección del equipo de personas para el proyecto sea el adecuado.

Objetivo del Control: Asegurar que se prepare un plan detallado de la implementación, de tal forma que cada miembro del equipo tenga una guía de sus actividades.

Objetivo de Auditoría: Determinar si todas las tareas necesarias están incluidas en el plan y si los estimados de tiempo son realísticos.

Aspectos de Auditoría: Se debe determinar que el plan sea completo y que sus estimados sean precisos.

Objetivo del Control: Asegurar que las instrucciones para el analista de sistemas están documentadas adecuadamente y cubren todos los elementos necesarios del sistema.

Objetivo de Auditoría: Determinar que las especificaciones del programa están documentadas adecuadamente y cubren todos los elementos necesarios del sistema.

Aspectos de Auditoría: Se debe determinar si las especificaciones del programa son precisas y cumplen con los estándares internos.

Objetivo del Control: Asegurar que la programación se realiza en forma ordenada y que los programadores sean supervisados adecuadamente.

Objetivo de Auditoría: Asegurar que las actividades de los programadores sean bien administradas y supervisadas.

Aspectos de Auditoría: La fase de programación debe ser monitoreada para asegurar una buena administración; es importante tener presente que la función del auditor es solamente monitorear el progreso y señalar debilidades a través de los canales apropiados.

Objetivo del Control: Asegurar que todos los programas sean probados para demostrar que cumplen con las especificaciones. Esta primera fase de pruebas puede ser definida como pruebas unitarias, ya que se concentra en pruebas individuales de programas o módulos.

Objetivo de Auditoría: Determinar si los programas individuales han sido probados adecuadamente.

Aspectos de Auditoría: Revisar los resultados de las pruebas de los programas para asegurar que estos son adecuados.

Objetivo del Control: Asegurar que todos los programas y procesos de sistemas están lo suficientemente explicados en el sistema, centro de datos y manuales del usuario.

Objetivo de Auditoría: Determinar si la documentación del sistema comunica adecuadamente la función del sistema a los analistas, programadores y usuarios.

Aspectos de Auditoría: Se debe evaluar la documentación para que todo aspecto en ella sea adecuado y consistente.

Objetivo del Control: Asegurar que todas las funciones del sistema han sido probadas adecuadamente previas a la conversión a un ambiente real.

Objetivo de Auditoría: Determinar si todos los programas ha sido probados lógica y organizativamente de acuerdo a los requerimientos.

Aspectos de Auditoría: Se debe determinar si el plan de pruebas es el adecuado.

Objetivo del Control: Asegurar que el nuevo sistema sea implementado bajo controles estrictos (con la previsión de que si el nuevo sistema falla, pueda regresarse al sistema antiguo) y que todo el personal necesario pueda operar el sistema.

Objetivo de Auditoría: Determinar si la conversión al nuevo sistema será controlada adecuadamente para prevenir perdida de información.

Objetivo del Control: Asegurar que el sistema sea asignado a un programador(es) competente para su mantenimiento y modificaciones y que recibirá la atención necesaria para operar eficientemente.

Objetivo de Auditoría: Determinar si existen los planes adecuados para el mantenimiento y modificación del nuevo sistema.

Aspectos de Auditoría: Se deben revisar los planes para mantenimiento y modificación.

Controles en el Análisis de Sistemas

El objetivo de la auditoría es determinar que existen los controles externos y controles de programa adecuados para verificar la entrada, proceso y salida. Se puede establecer una lista de chequeo que establecerá las bases para determinar los controles mínimos. Los controles necesarios para actividades específicas de los sistemas, dependen del tipo de datos y del método de procesamiento. Es la responsabilidad del auditor señalar situaciones especiales de proceso y determinar si existen los controles necesarios.

Esta revisión establece la auditoría de aplicaciones, con una distinción importante: un sistema en desarrollo no provee la evidencia física de las actividades diarias de proceso, por ello, el auditor solamente podrá tener una idea de lo que sucederá.

El análisis debe iniciar en las primeras fases del ciclo de vida del sistema en desarrollo y deberá finalizar justamente antes de la preparación de modificaciones para el software comprado externamente. Los sistemas diseñados internamente, requieren del análisis durante la fase de diseño, y éste finalizará antes de la preparación de las especificaciones funcionales. Esta especificación de tiempos permite que las recomendaciones de auditoría sean incorporadas al diseño del sistema y no insertadas después de la implementación.

Evaluación del comportamiento de las pruebas

Todas las fases en el ciclo de vida del desarrollo de sistemas son importantes, pero la fase de pruebas demuestra el éxito de las fases precedentes e indica si el sistema esta listo para ser instalado. Esta fase produce la primera evidencia tangible de los resultados del proceso. El auditor debe prestar especial atención al desarrollo de controles en la fase de pruebas porque saltos u omisiones en esta fase para ahorrar tiempo pueden resultar en un sistema que no opera adecuadamente. Los controles del sistema que suponían estar presentes durante el desarrollo deben ser

examinados específicamente en esta fase para determinar su existencia. Es vital para el auditor determinar que todas las pruebas han sido completadas.

Evaluación del comportamiento de la conversión

Además de los controles administrativos, es vital la revisión de las actividades que se realizan en la realidad en esta última etapa, debido a su naturaleza crítica. El sistema antiguo, en el que ya existían registros, esta siendo reemplazado por un sistema que a pesar de haber sido probado, su efectividad no ha sido comprobada a ciencia cierta. Por ello, es crucial que la información sea protegida contra destrucción o alteración y que este completamente convertida al nuevo sistema.

NOTA: Los objetivos de los controles y sus objetivos de auditoría asociados y pruebas presentadas, no son las ideales para todo sistema en desarrollo; deben ser adaptadas a las necesidades de cada sistema. Adicionalmente, como cualquier revisión de auditoría, se requiere mucho criterio del auditor. Pero el uso de estos lineamientos puede

ayudar a asegurar los controles adecuados para el desarrollo e implementación de sistemas.

5.4.3 EVALUACION DEL PROCESO DE DATOS

5.4.3.1 CONTROLES

En cualquier organización, los datos son uno de los activos más valiosos y el hecho de ser intangibles no los exime de tener que ser controlados y auditados, incluso, con mayor cuidado que los demás activos de la organización. Por ello debe tomarse en cuenta lo siguiente:

- La responsabilidad de los datos deberá estar a cargo de la entidad que los proporciona y de la dirección del departamento de informática.

- Debe considerarse, principalmente en esquemas que utilizan redes y bases de datos, que muchos problemas se originan debido a la duplicidad de datos.

- Los datos deben manejarse en una forma estándar, (estructuración, clasificación, etc.) esto facilitará la detección de duplicidades y redundancias.

a. Datos Fuente

La forma más común de delitos por computadora se dan a través de la modificación de datos fuente, las que pueden ser:

- Suprimir u omitir datos
- Adicionar datos
- Alterar datos
- Duplicar procesos

Esta situación es crítica para los sistemas que trabajan en línea, en los que los usuarios son los responsables de la captura y modificación de datos; en dicha situación, debe señalarse uno y solamente un responsable de determinado dato. Además se establecerán claves de acceso que estarán de acuerdo a niveles.

Los niveles pueden estructurarse como el departamento de informática lo estime conveniente, pero algunos de los niveles más comunes son: primer nivel, solo para consultas; segundo nivel, captura, modificación y consulta; tercer nivel, todo lo anterior y eliminaciones.

b. Operación

Es necesario que todo proceso que deba realizarse a través de la computadora cuente con la documentación adecuada. De esto depende en gran parte la eficiencia y costo de la operación de un sistema.

Los instructivos de operación sirven al operador para saber que procedimientos se deben seguir, ya sea en situaciones normales o anormales. Si la documentación es inexistente, incompleta o inadecuada, se obliga al operador a tomar decisiones improvisadas, lo que puede dar como resultado errores, reprocesos, desperdicio de tiempo, lo que consecuentemente incrementa los costos.

c. Salida

Este tipo de controles esta íntimamente relacionado con la etapa de reportes del sistema, la cual puede estar incorporada como una fase final del proceso o puede ser un subsistema por separado. Estos controles están diseñados para asegurar que la salida sea completa, precisa, oportuna y que cuente con una distribución adecuada, ya sea en forma impresa o a través de medios magnéticos. Algunos de los tipos más comunes de controles en la salida pueden ser:

- Etiquetas: Esto asegura que se esta creando o actualizando el archivo correcto.
- Reconciliación: Este proceso asegura que la cantidad correcta de datos ha sido procesada y reportada. Los reportes de reconciliación pueden ser producidos para permitir ya sea a la función de control de datos o al departamento usuario, determinar que toda la información ha sido recibida, procesada y reportada.
- Reportes de cantidad: Estos detallan los tipos de reportes y la cantidad de páginas impresas para cada reporte, lo que permite

a la función de control de datos y al departamento usuario asegurarse de que toda la salida impresa ha sido recibida.

- Programas de distribución: Estos ayudan al centro de datos a asegurarse de que todos los reportes son despachados con suficiente tiempo para cumplir con los requerimientos del usuario.

Se puede resumir que los reportes de salida resultantes del procesamiento se deben de revisar en cuanto a coherencia y distribución oportuna a los destinatarios autorizados, para lo que se deben tener los siguientes controles: revisar los reportes de salida en cuanto a forma e integridad; se debe comparar la salida contra los totales de control, disponiendo de las pistas de auditoría para facilitar el rastreo y la conciliación; la distribución de las salidas debe estar de acuerdo con las instrucciones escritas; deben existir procedimientos para reportar y controlar los errores contenidos en las salidas; se deben establecer los procedimientos para el manejo y la retención de la salida; se deben documentar las medidas de seguridad de los reportes de salida que deben ser distribuidos.

d. Medios de Almacenamiento

En cualquier tipo de organización en que se utilice la computadora como herramienta, existirán medios de almacenamiento masivo, los que representan archivos de mucha importancia, los cuales si por cualquier motivo llegasen a perderse, dañarse ya sea parcial o totalmente, podría llevar a repercusiones altamente dañinas.

Toda auditoría de sistemas debe prever que se cuente con un mecanismo de protección de este tipo de dispositivos.

También se debe indicar una metodología de identificación de los medios de almacenamiento; de esta forma se reduce la posibilidad de una utilización errónea o destrucción de la información.

Se deben tener ubicaciones pre-asignadas para el almacenamiento de los archivos, debidamente resguardada contra desastres físicos y riesgos de robo o duplicación de información confidencial.

Se debe diseñar una metodología para la organización de la "biblioteca" de archivos, indicando cual será la información mínima que deberán contener los registros.

Mantenimiento (Hardware)

Es necesario que todo el equipo que esta bajo la responsabilidad de un departamento de informática tenga un mantenimiento adecuado. El mantenimiento se pude clasificar de tres maneras:

- Mantenimiento Total

  Este tipo de mantenimiento es el que incluye el mantenimiento preventivo y el correctivo y este a su vez puede dividirse en dos tipos, el que incluye las partes y el que no las incluye. Este tipo suele ser el más caro de todos los mantenimientos, pero la ventaja es que se deja todo bajo responsabilidad del proveedor, con excepción de daños por negligencia en la utilización del equipo.

- Mantenimiento "por llamada"

Este tipo de mantenimiento se maneja de tal forma que cuando surge el desperfecto o falla, entonces se llama al proveedor para que atienda al momento; en este caso el proveedor cobra de acuerdo a una tarifa determinada y no se incluyen las partes necesarias para reparar el equipo. Casi en todos los casos, el proveedor suministra el transporte hacia y desde el taller.

- Mantenimiento "en banco"

En este tipo, le corresponde al propietario del equipo llevarlo a las oficinas del proveedor, quien le prepara una cotización en base a la mano de obra y partes necesarias. Este tipo de mantenimiento se recomienda solo para computadoras personales.

Es necesario mantener siempre presente el hecho de que la capacidad del equipo en cuanto a su utilización se ve influenciada por las actividades de mantenimiento, por lo que es necesario, para evaluar dicha capacidad, preveer el

mantenimiento preventivo, fallas internas y externas no previstas.

5.4.3.2 ORDEN EN EL CENTRO DE COMPUTO

Un aspecto muy importante es poder mantener y observar reglas específicas en cuanto al orden y cuidado del centro de cómputo.

Es necesario establecer un conjunto de reglas que indiquen como deberá de organizarse el mantenimiento y orden del centro de cómputo, para evitar que el equipo y demás mobiliario se vean dañados o decrementen su capacidad. Esto a la larga evitará costos elevados y pérdida de valiosa información.

Algunos de los aspectos que se deben observar son los siguientes:

- Con que periodicidad se hace limpieza en el centro de cómputo y al equipo.
- Existe un lugar asignado para los medios de almacenamiento.
- Existe un lugar asignado para papelería y utensilios de trabajo.

- Es adecuado el mobiliario (muebles) asignado al equipo y los lugares de almacenamiento.
- Existen prohibiciones para fumar, tomar alimentos y especialmente líquidos en el área del centro de cómputo.
- Existen carteles que indiquen tal prohibición.
- Se tienen restricciones para el uso del equipo.

5.4.4 EVALUACION DE LA SEGURIDAD

La seguridad del área de informática, incluyendo en este término, los sistemas de información, se torna cada día más importante en cualquier organización. Una de las razones para esta situación es que cada vez más la información es tratada electrónicamente y las empresas dependen de la información en que basan sus decisiones para lograr el éxito.

La seguridad suele depender de la situación particular a que se aplique, por lo que se requiere mucha creatividad y diseño detallado.

Conforme se desarrolla la tecnología, los sistemas de información se ven más y más mecanizados, para poder seguir el ritmo de la evolución. Por ello y como ya se dijo en distintas oportunidades en este documento, la

información es uno de los elementos más importantes en una organización, pero por el mismo hecho de los avances tecnológicos, cada vez es más difícil protegerla. Esto significa que la seguridad en informática es una tarea delicada y complicada pero no imposible.

En una auditoría de sistemas, se debe considerar la seguridad en una serie de aspectos que varían en sus procedimientos y en sus conceptos mismos, los cuales se exponen a continuación.

5.4.4.1 SEGURIDAD LOGICA

A través de las computadoras se manejan grandes cantidades de información la que puede considerarse en ocasiones confidencial, ya sea para un usuario, departamento o para la organización, y el mal uso o divulgación de ésta puede causar estragos a la estabilidad de la empresa. Son conocidos aspectos como robo, fraude o sabotaje que provocan la destrucción total o parcial de la actividad computacional.

El área de informática puede resultar el activo más valioso de cualquier organización y al mismo tiempo el más vulnerable.

Además de los factores ya mencionados, en la actualidad existe una amenaza cada vez más latente y muy peligrosa: los "virus" de computadoras, los que pueden tener diferentes intenciones. Esta situación se da comúnmente en aquellas organizaciones que suelen "piratear" software.

El auditor debe tener el cuidado de no obtener software en forma pirata, como también de que al momento de ingresar a una red, no exista la posibilidad de adquirir un virus.

Al tener implementado un buen sistema de seguridad lógica en los sistemas de computación, se reduce considerablemente la posibilidad de fraude por computadora.

Los motivos de delito por computadora suelen ser de distintos tipos:

- Beneficio Personal
- Beneficios para la organización
- Síndrome de Robin Hood (beneficio para otras personas)

- Vandalismo
- Desfalco
- Deshonestidad
- Odio o venganza
- Necesidad económica
- Búsqueda de Poder, etc.

Estudios han demostrado que existen cuatro factores que permiten el incremento de los crímenes por computadora:

- Aumento de personas que estudian computación.
- Aumento de empleados con acceso al equipo.
- Facilidad del uso de los sistemas de cómputo.
- Incremento en la concentración del número de aplicaciones y por ende de la información.

Paralelamente al incremento en los fraudes por computadora se ha perfeccionado los sistemas de seguridad tanto física como lógica.

En general, un sistema integral de seguridad deberá contener:

- Elementos administrativos
- Definición de una política de seguridad
- Organización y división de responsabilidades
- Seguridad física y contra catástrofes
- Prácticas de seguridad del personal
- Pólizas de seguros
- Elementos técnicos y procedimientos
- Sistemas de seguridad de equipos y sistemas
- Aplicación de los sistemas de seguridad
- El papel del auditor
- Planeación de programas de desastre y su prueba

Uno de los aspectos más importantes en una auditoría y que debe ser realizado con mayor detalle es el de tener cifras de control y un medio adecuado que permita conocer el momento en que se produce un fraude o cambio en el sistema. Se deben diseñar una serie de indicadores que permitan auditar en forma rápida y eficiente el sistema, los que deben servir como un auto auditor para la computadora.

Es necesario evaluar el nivel de riesgo que pueda tener la información, lo que permitirá realizar un estudio preciso de beneficio/costo entre el valor de la perdida de información y el costo de un sistema de seguridad. Para ello debe evaluarse lo siguiente:

- Clasificar las instalaciones en términos de riesgo (alto, mediano o pequeño).
- Identificar las aplicaciones que tengan un alto riesgo.
- Cuantificar el impacto en caso de suspensión del servicio en aquellas aplicaciones con un alto riesgo.
- Formular medidas de seguridad necesarias dependiendo del nivel de seguridad que se requiera.
- La justificación del costo de implantar las medidas de seguridad.

Para clasificar las instalaciones en términos de riesgo se debe:

- Clasificar los datos, información y programas que contienen información confidencial que tenga un alto valor dentro del

mercado de competencia, e información que sea de difícil recuperación.

- Identificar aquella información que tenga un gran costo financiero en caso de pérdida o bien que pueda provocar un gran impacto en la toma de decisiones.

- Determinar la información que signifique una gran pérdida en la organización y consecuentemente provoque la posibilidad de no sobrevivir sin esa información.

5.4.4.2 SEGURIDAD EN EL PERSONAL

Un centro de cómputo funcionará bien en la medida en que el personal sea el idóneo. Esto no sólo significa que debe ser bien preparado sino que también debe cumplir con ciertas cualidades como confidencialidad, integridad y lealtad entre otras. Es una buena medida realizar varios tipos de pruebas para seleccionar al personal, exámenes psicológicos, médicos y realizar una investigación de sus antecedentes de trabajo.

Los trabajos en los centros de informática suelen ser bastante pesados y se está expuesto a mucho estrés, dando la pauta a que algunas personas se vuelvan indispensables para el centro de cómputo. Esto puede ser problemático ya que le da a la persona un tipo de poder dentro de la organización al creerse insustituibles. Es necesario tener un buen programa de vacaciones, lo que permite evaluar la dependencia que se tiene de algunas personas para poder evitarla a tiempo.

Se necesita, como otra medida de seguridad, contar con un plan de rotación del personal; esto puede reducir la posibilidad de fraude al evitar el conocimiento total de un solo aspecto a una sola persona. La rotación también evita que una persona se sienta indispensable le reduce el nivel de confianza que pueda adquirir al adueñarse de un puesto. Esto es esencial en puestos que requieran de altos niveles de confianza.

5.4.4.3 SEGURIDAD FISICA

Con esta se trata de evitar que el servicio que presta un centro de cómputo se vea interrumpido debido a contingencias como

desastres, sabotaje o disturbios. Debe contar con un medio de emergencia que le permita continuar funcionado hasta normalizar la situación.

Es necesario proteger el centro de cómputo contra personas inescrupulosas que deseen dañar a la organización. Por ello se ha cambiado la idea tradicional de exhibir el centro de computo de una empresa. No se debe olvidar que éste es el cerebro de cualquier organización donde radica toda su información. El trafico en el centro de cómputo debe estar limitado a personas autorizadas y altos ejecutivos de la organización, con estrictos controles de acceso a personas extrañas.

También deben tomarse precauciones en cuanto a las instalaciones físicas del centro de informática. Se deben reducir los materiales altamente inflamables. Las fundaciones de su construcción debe ser sólidas y evitar la filtración de materias dañinas para el equipo como agua, polvo o humo.

Se deben considerar los niveles de temperatura a que esta sometido el equipo, para el que se recomienda que la temperatura

se encuentre en un rango de 10 a 40 grados centígrados y su nivel de humedad debe oscilar entre el 40% y el 60%. Los cambios drásticos y repentinos en la temperatura o la humedad pueden dañar la información, los medios magnéticos y hasta ocasionar un corto circuito.

Se debe observar que los campos magnéticos de ciertos equipos pueden afectar el rendimiento del equipo, por lo que se recomienda colocar los equipos a una distancia de por lo menos 1.5 metros de distancia uno de otro en aquellos casos en que se produzca esta clase de ondas.

La instalación eléctrica es otro aspecto importante dentro de la seguridad de un centro de cómputo. Se deben proteger los cables por medio de ductos y evitar que éstos estén dispersos por el suelo o las paredes, para evitar choques eléctricos o que accidentalmente se desconecte un equipo. Toda la instalación eléctrica de un centro de cómputo debe estar debidamente polarizada.

Deben haber dispositivos que permitan evitar un incendio. Este tipo de dispositivos (extinguidores) deben ser de un material químico que no dañe al equipo en caso de sea necesario su utilización.

Se debe contar con un área adecuada para resguardar los medios de almacenamiento como discos o cintas y cualquier otro documento importante que deba tenerse a mano en el centro de cómputo. Este local debe ser a prueba de incendios y otras contingencias y debe estar debidamente resguardado del acceso de personas no autorizadas.

5.4.4.4 SEGURIDAD EN LA UTILIZACION DEL EQUIPO

Existen una serie de puntos que deben revisarse cuando se analiza la seguridad de la utilización del equipo:

1. Los programas y archivos deben tener acceso restringido.
2. Los operadores y digitadores no deben tener la posibilidad de modificar los programas.
3. Solamente personas autorizadas deberán tener entrada a la red y sus terminales.

4. La información confidencial deberá ser codificada o encriptada.
5. Se deben realizar revisiones continuas de la utilización de las terminales y generar los reportes adecuados.
6. Se deben guardar copias de los archivos y programas en lugares ajenos al centro de cómputo y en instalaciones de alta seguridad.
7. Debe haber un estricto control del transporte de dichos archivos de un lugar a otro.
8. Se debe verificar que los usuarios hayan recibido un entrenamiento adecuado en el manejo del equipo, sistema operativo y software.
9. Deben existir en el área del centro de cómputo, manuales actualizados del sistema operativo y demás software que se utilice así como también los manuales operativos del equipo.
10. Deben existir procedimientos adecuados para la rotulación de los medios magnéticos de almacenamiento.
11. Se deben respetar las leyes de protección a la propiedad intelectual y evitar la copia indiscriminada de programas y fotocopia de manuales.
12. Debe haber un buen programa de copias de respaldo de la información crítica del centro de cómputo.

En todas las actividades relacionadas con las ciencias de la computación, existe un riesgo aceptable; y es necesario analizar y entender estos factores para establecer los procedimientos que permitan eliminarlos al máximo y, en caso de que ocurran, poder reparar el daño y reanudar la operación lo más rápidamente posible. En una situación real se deberían elaborar planes para manejar cualquier contingencia que se presente.

5.4.4.5 SEGURIDAD DE RESPALDO

Es necesario que todo centro de cómputo cuente con un plan de emergencia que debe ser aprobado por la dirección de informática. El objetivo de éste es ayudar a la recuperación de interrupciones en la operación del sistema de cómputo.

El sistema que sea diseñado para este objetivo deberá ser probado bajo situaciones anormales para verificar que el plan dará los resultados para los que fue diseñado. Esto significa que deben crearse situaciones ficticias pero lo más acercadas a la realidad posible en que se considere el caso de emergencia.

Algunos de los desastres que pueden suceder pueden clasificarse de la siguiente manera:

- Completa destrucción del centro de cómputo.
- Destrucción parcial del centro de cómputo.
- Destrucción o mal funcionamiento de equipos auxiliares del centro de cómputo (electricidad, aire acondicionado, etc.).
- Pérdida total o parcial de información, manuales o documentación.
- Pérdida del personal clave.
- Problemas laborales.

El plan en caso de desastre debe incluir:

- La documentación de programación y operación.

Los equipos

- El equipo completo
- El ambiente de los equipos
- Datos y archivos
- Papelería y equipo accesorio
- Sistemas (sistemas operativos, bases de datos, programas de utilería, software en general).

Es necesario considerar que toda documentación de cualquier tipo debe estar lo más actualizada posible. De no ser así, si las últimas modificaciones no han sido incluidas en la documentación, el sistema de emergencia corre el peligro de no funcionar.

Cuando se necesite incorporar el plan en caso de emergencia, se deberá:

- Asegurar que todos los miembros sean notificados.
- Informar al director del área de informática.
- Cuantificar el daño o perdida del equipo, archivos y documentos para definir qué parte del plan será activada.
- Determinar el estado de todos los sistemas en proceso.
- Nofiticar a los proveedores del equipo cual fue el daño.
- Establecer la estrategia para implementar las operaciones de emergencia.

5.5 HERRAMIENTAS DE LA AUDITORIA DE SISTEMAS

Debido al aumento en lo que se refiere a procesamiento de datos, se ha visto la necesidad de incrementar la complejidad con la cual es manejada la información en los sistemas automatizados.

Para el auditor ya no es suficiente examinar los documentos fuentes y reportes de computadora en forma manual, ya que se enfrenta con una serie de dificultades tales como:

- Todos los procesos que son realizados por el computador carecen de evidencias visibles.
- Se procesan grandes cantidades de transacciones.
- Existen cálculos con mucha complejidad, etc.

Debido a este tipo de problemas, el auditor se ha visto en la necesidad de utilizar la misma computadora como herramienta para poder resolver esta dificultad, ya que viene a dar mayor eficiencia y eficacia al auditor y al mismo tiempo, es la única manera de poder examinar algunos procesos.

A esta forma de utilizar el computador como herramienta para dar solución a los diferentes problemas mencionados anteriormente se le denomina "Técnicas de Auditoría Apoyadas en el Computador", cuyas siglas en el idioma inglés son CAAT (Computer Aided Audit Techniques).

Estas herramientas CAAT son clasificadas en tres áreas, las cuales se mencionan a continuación:

- CAAT para la auditoría de controles generales:
  - Controles de implantación
  - Controles de seguridad de programas
  - Controles de seguridad de archivos de datos
  - Controles de la administración de operaciones
  - Controles de programas de soporte del sistema

- CAAT para la auditoría de aplicaciones:
  - Herramientas utilizadas para probar los procesos y control incluidos en los programas de aplicaciones:
    * Pruebas de datos
    * Facilidades de pruebas integradas
    * Simulación de paralelo

- Herramientas utilizadas para asegurar la completicidad, exactitud y validez de entradas y actualizaciones a la aplicación y el adecuado mantenimiento de la información.

- CAAT que facilitan las funciones de administración de la auditoría de sistemas.

  - Planificación de la auditoría.
  - Control sobre la ejecución de la auditoría.
  - Documentación de la auditoría.
  - Comunicación de resultados de la auditoría.

Para cada una de las clasificaciones señaladas anteriormente ya existen las herramientas adecuadas; desde aquellas en las cuales se necesita tener un alto conocimiento en computación hasta una simple hoja electrónica ó un procesador de palabras.

Como ejemplo se pueden mencionar algunos de estos productos: TICOM III, ICE, PRO TEST, EDP AUDITOR y otros utilitarios como ACF2, GUARDIAN, TOP SECRET, etc.

Debidó a la gran cobertura que ofrecen las herramientas de auditoría de sistemas, existen otras formas para clasificarlas, entre las cuales se pueden mencionar:

- Software Especializado:

  Son todos aquellos programas diseñados y desarrollados en forma específica, con el único fin de cubrir algún tipo de requerimiento especial de una ADS.

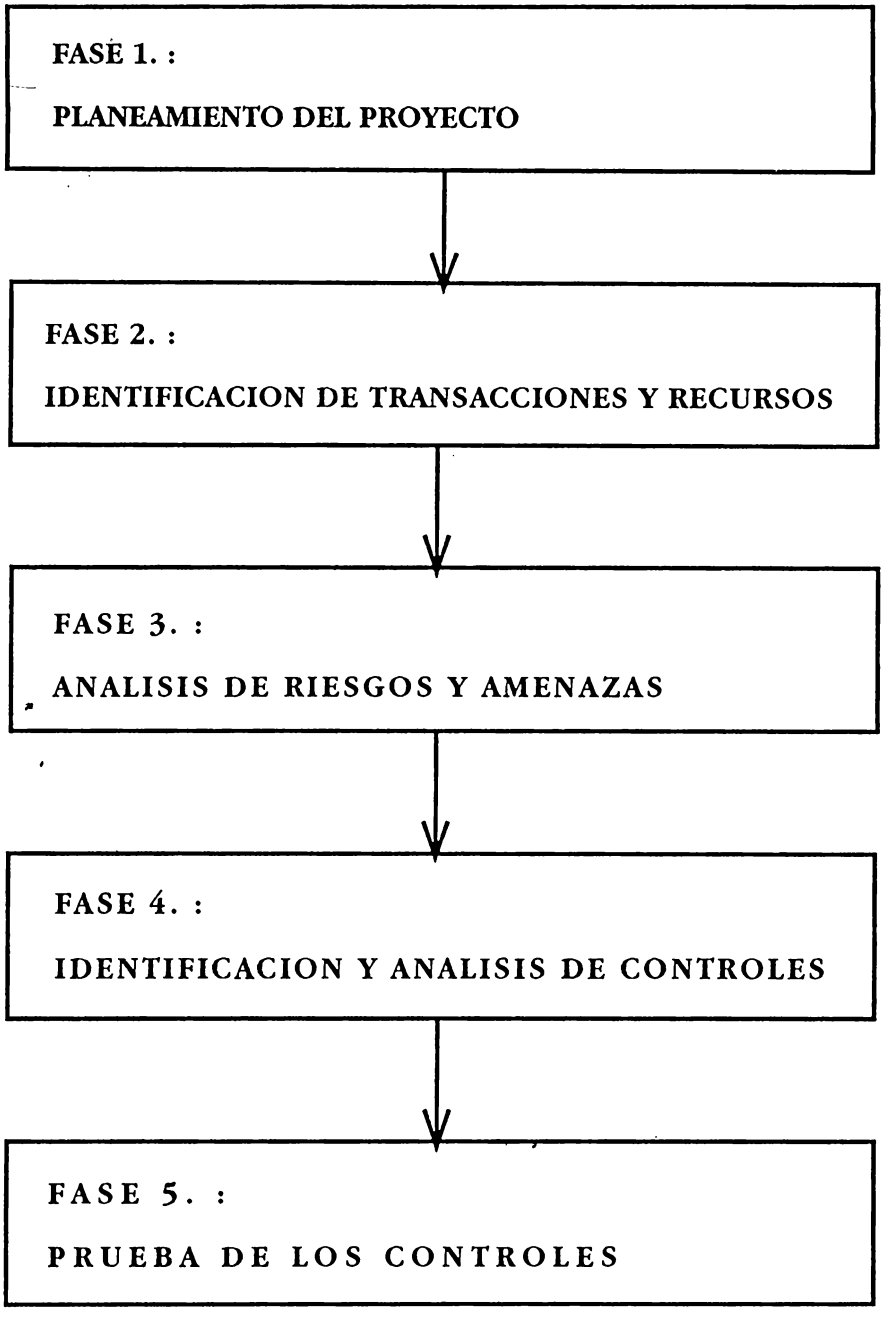
- Software Generalizado de Auditoría:

  Estos son realizados por compañías que se dedican a la elaboración de este tipo de software y que se adaptan a diferentes situaciones a las que puede enfrentarse un auditor.

5.6 METODOLOGIA

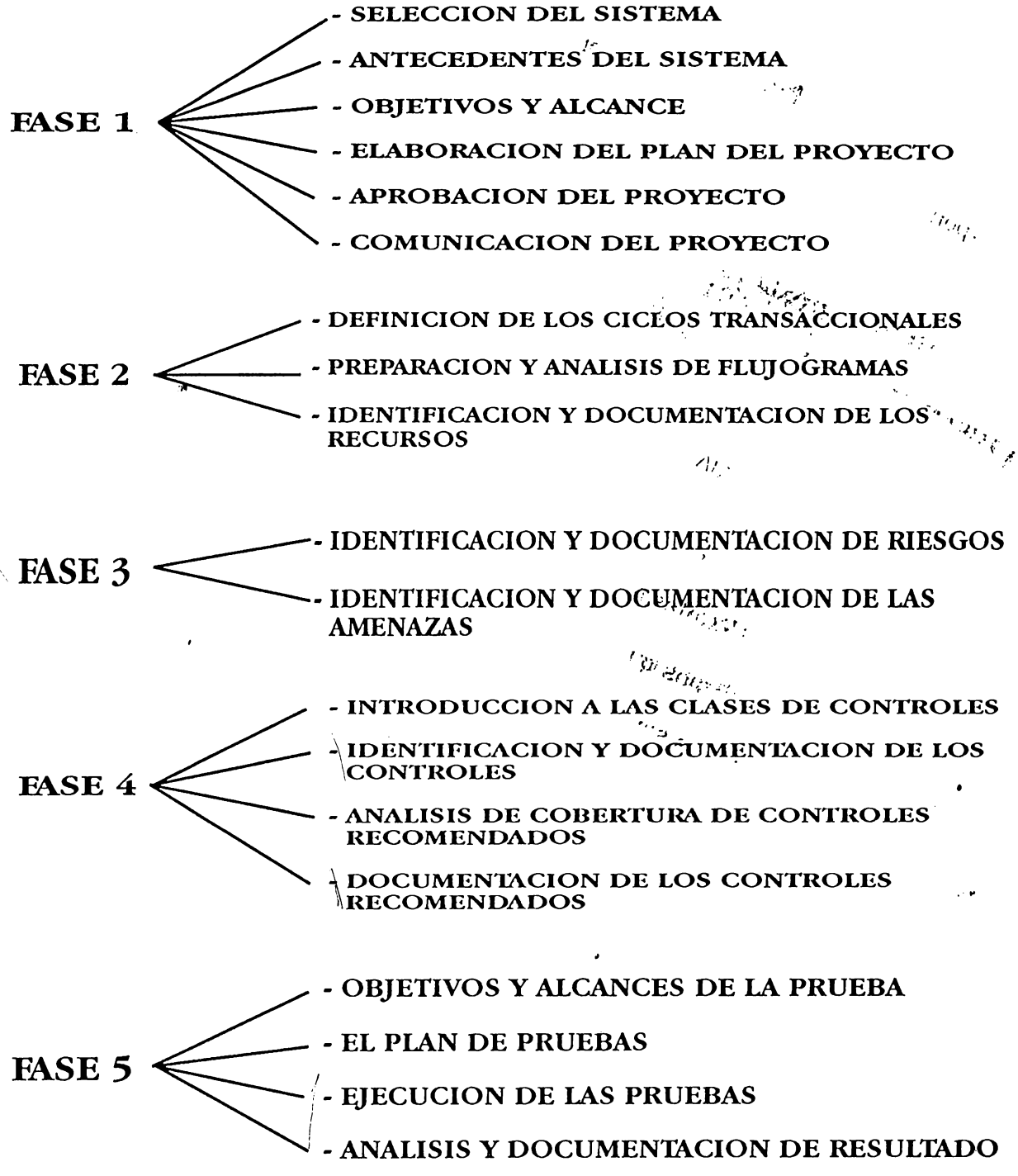
Para lograr un mejor entendimiento de todos los procesos que se llevan a cabo en la realización de la Auditoría de Sistemas, se hizo necesario dividir la metodología en 5 fases, lo que tiene como objetivo brindar una mejor estructuración de toda la información que se maneje durante el desarrollo de la Auditoría. A continuación se presentan las fases en forma gráfica para ser explicadas posteriormente. (Gráficas 7 y 8)

METODOLOGIA PARA LLEVAR A CABO LA AUDITORIA DE SISTEMAS



GRAFICA Nº 7

ACTIVIDADES DE CADA FASE



GRAFICA Nº 8

A continuación se pasa a exponer cada una de las fases en forma más detallada:

5.6.1 FASE 1. PLANEAMIENTO DEL PROYECTO

5.6.1.1 SELECCION DEL SISTEMA

Con el único objetivo de garantizar que la auditoría de sistemas se lleve a un término en base a ciertas prioridades, es necesario tomar en cuenta una serie de criterios que son utilizados al momento de seleccionar el sistema, éstos son:

- ACTIVOS CONTROLADOS POR EL SISTEMA

Toma como antecedente los valores que son controlados por el sistema y su utilización se lleva a cabo en base a 2 formas:

1. Llevando un control del valor de los activos o pasivos por medio del sistema en forma permanente (Valor del archivo maestro).

2. Llevando el control del valor de las nuevas transacciones de un período determinado (Valor de compras o pagos mensuales).

✧ INTEGRACION DEL SISTEMA

Hace referencia al nivel de integración física ó lógica que posee el sistema, tomándose como una de sus mayores importancias el traslado de información que un sistema puede proporcionar para poder actualizar en forma automática otros sistemas.

✧ FORMA DE OPERACION

Se consideran de mayor importancia aquellos sistemas que realizan sus operaciones en forma real (Proceso en Línea), es decir que todos los archivos son actualizados en el mismo momento en el cual se lleva a cabo la transacción. Los de menor importancia son los que realizan sus transacciones de actualización de archivos en diferentes períodos de tiempo y se les conoce con el nombre de procesos en lotes.

✧ IMPACTO POR FALLAS EN EL SISTEMA

Se le da mayor importancia a aquellos sistemas que debido a una serie de fallas provoca un impacto en cuanto a las operaciones externas que la empresa realiza con clientes o terceras personas.

Obtienen menor importancia los sistemas cuya fallas causan impacto solamente en las operaciones específicas del área del usuario dejando de afectar las operaciones totales internas o externas de la empresa.

✧ ARCHIVOS DEL SISTEMA

Este criterio se clasifica en 3 niveles:

1º Los Sistemas cuyos archivos son almacenados en terminales inteligentes conformando así una red de procesamiento.

2º Consiste en el manejo de archivos en bases de datos y cuyo acceso se realiza por diferentes aplicaciones ó sistemas.

3º Corresponde a los archivos convencionales dedicados es decir los que son accedidos por programas que pertenecen a una misma aplicación de computadora.

✧ NUMERO DE MODULOS/PROGRAMAS

Con este criterio se da a conocer que un sistema entre menor cantidad de programas contenga, tendrá menos posibilidades de que ocurran interrupciones durante el procesamiento de información debido a fallas.

Para poder prevenir cualquier tipo de interrupción, se necesita realizar una comparación de sistemas que poseen la misma naturaleza con el fin de evitar que una aplicación contenga mayor número de programas.

✧ PARTICIPACION DE AUDITORIA

Este criterio determina dar una mayor valorización aquellas aplicaciones que no tuvieron ninguna intervención de la auditoría durante su desarrollo.

5.6.1.2 ANTECEDENTES DEL SISTEMA

Es conveniente que antes de planificar el desarrollo de un proyecto de auditoría y dar a conocer los objetivos y alcances que se persiguen, es necesario realizar una investigación general del sistema que se ha seleccionado, con el fin de hacer llegar la información existente, el cual ayudara a tener con más claridad los procesos automatizados, administrativos y comerciales, así como también conocer a los usuarios y las operaciones que estos realizan y a su vez establecer que personas tienen una estrecha relación con el sistema.

Toda esta información no solamente servirá para que el auditor se familiarice con las características del sistema, sino también servirá como base para determinar los puntos de referencia del proyecto.

Para poder alcanzar lo antes mencionado, es necesario cumplir con los siguientes pasos:

1) Realizar la identificación de quienes laboran en el área de sistemas y cuya función es la de operar, actualizar y dar mantenimiento a este.

   Para poder lograr está identificación es necesario que exista un contacto con las siguientes áreas:

   - Personal Administrativo
   - Usuario Principal
   - Usuario Secundario
   - Organización y Método
   - Departamento de Sistemas:
   - Jefe del Departamento
   - Personal de Operaciones
   - Entrada de Datos
   - Control de Entrada/Salidas

2) Discutir el sistema automatizado con los auditores financieros y obtener copias de reportes de auditorias previamente realizadas.

La incorporación de los auditores financieros vendrá a ser de gran utilidad a la hora de establecer los diferentes controles que serán introducidos a los sistemas ya sea en forma manual o automatizada. Podrán proporcionar aspectos que hayan sido revisados y que se les hubiera hecho algún tipo de recomendación, adicionalmente conocen los tipos de reportes y conclusiones que presentan los auditores externos y consultores.

El objetivo de la revisión de toda esta información, es enterarse de la cantidad de deficiencias de control que fueron encontradas en trabajos desarrollados anteriormente y de aquellas que aún no se han corregido y como la administración logró solucionar algunas de éstas.

3) Obtener el organigrama del Usuario Principal y el Area de Sistemas.

Se debe conocer como se encuentra en la actualidad la estructura orgánica tanto del usuario principal como del área de sistemas, y a través de las definiciones funcionales saber cada una de sus responsabilidades, teniendo en cuenta la separación de funciones incompatibles.

4) Entrevistar el personal de usuarios y departamento de sistemas.

Las entrevistas deben ser dirigidas a los que se encargan de operar y mantener el sistema en buen estado. El propósito de estas entrevistas, es para conocer las responsabilidades de cada usuario y si se tienen los conocimientos de la aplicación con la que se está trabajando. También se puede verificar si no ha existido algún tipo de cambio en cuanto al organigrama y detectar si los usuarios tienen bien definidas todas sus responsabilidades.

Existen una serie de aspectos más específicos dentro de la realización de una entrevista a los que se les debe de estudiar con más profundidad, éstos son:

a) Analizar las funciones

- De acuerdo al sistema automatizado se deben de discutir las funciones y responsabilidades de cada persona.
- Establecer cual es la relación entre mantenimiento y operación de la aplicación
- Adquirir copias de la descripción de funciones.

b) Conocer sobre el Sistema

- Historia del desarrollo y modificaciones del sistema
- Problemas enfrentados durante el desarrollo del sistema (ejemplo: retiro de personal clave).
- Medio ambiente
- Personal
- Controles
- Interfaces del sistema
- Operaciones en el procesamiento

- Estándares de la instalación
- Integridad y control de datos:
  - Tablas de "password" o claves de acceso
  - Lista de autorizaciones de acceso
  - Log de Acceso
  - Transacciones críticas
  - Manejo y correcciones de errores

c) Conocer el grado de satisfacción que el usuario posee con la aplicación y con todos los servicios de procesamiento de datos.
   - Documentar alguna preocupación existente y cualquier mantenimiento pendiente de implantación.
   - Indicar si el usuario está satisfecho en cuanto a la exactitud y tiempo de respuesta, así como también a los formatos y al propósito al cual fue definido.
   - Anotar los posibles problemas e indicar los posibles errores.

d) Adquirir documentación de usuario y de sistemas.

La documentación obtenida será de mucha importancia a la hora de llevar a cabo el trabajo de campo.

Dentro de la documentación que se debe obtener esta la siguiente:

- Manual de Procedimientos Operativos
- Manual de Funciones

- Manual de Usuario

  Este poseerá la información sobre la realización de los procedimientos del sistema tanto manualmente como automatizados.

- Manual Técnico de la Aplicación

  Este debe de contener las especificaciones técnicas de los archivos, programas y procedimientos que servirán para conocer el diseño detallado de la aplicación.

5.6.1.3 OBJETIVOS Y ALCANCE

Luego de haber obtenido una serie de referencias que han servido para tener un conocimiento más amplio del sistema, es necesario establecer los objetivos y el alcance que el proyecto persigue, entre los cuales se pueden mencionar:

- Poder establecer si en el control interno de los procedimientos manuales y automatizados existe algún tipo de inseguridad o posible falla.

- Examinar los controles que existen para el mantenimiento de las aplicaciones.

- Verificar si por parte del usuario se cumplen los siguientes aspectos:
  * Conocimiento de sus responsabilidades y de la aplicación.
  * Satisfacción en cuanto a los servicios que presta el sistema.
  * Manejo de alguna documentación para la administración del sistema.

- Verificar riesgos y controles en la red de comunicación del sistema.

- Probar los procedimientos de control en la generación de datos.

- Revisar los controles en cuanto a la circulación de información entre el usuario y el departamento de sistemas.

- Examinar el flujo de procesamiento en el departamento de sistemas.

- Probar los procedimientos de entrada y salida de datos.

- Revisar los procedimientos de distribución o entrega de reportes.

- Verificar si la documentación técnica esta actualizada y completa.

5.6.1.4 ELABORACION DEL PLAN DEL PROYECTO

Es uno de los aspectos importantes dentro de la Fase de Organización, teniendo como proceso de preparación el siguiente:

1. Definir las actividades que corresponden a cada una de las fases.
2. Determinar cuales son los recursos responsables para la ejecución de las actividades.
3. Estimar el tiempo y el costo del proyecto.
4. Creación del plan o cronograma del proyecto.

Debido a que este tipo de actividad realizada manualmente ocasiona mucha pérdida de tiempo y gasto, se recomienda que se utilicen los diferentes tipos de aplicaciones desarrollados en la computadora, entre los cuales podemos mencionar: Total Harvard Project Manager, SuperProject y Timeline.

El cronograma de actividades servirá de mucha importancia para la administración, ya que con éste se podrá medir que tanto a evolucionado el sistema y cuales podrán ser las fechas para la

realización de las entrevistas y reuniones con las áreas. También se conocerá claramente el tiempo, el costo y las personas que son responsables de su cumplimiento.

Este podrá ser manejado en forma dinámica, es decir, se podrán hacer evaluaciones periódicas con el objetivo de reasignar tareas, tiempos y responsabilidades para poder cumplir con los objetivos propuestos.

Al momento de terminar el proyecto de auditoría, es necesario hacer una revisión detallada del cronograma para determinar los ajustes que deberán llevarse a cabo en procesos de planeamiento posteriores.

5.6.1.5 PAPELES DE TRABAJO

Se hace necesario la existencia de documentación sobre la Auditoría de Sistemas que se está llevando en ejecución en ese momento, tomando como base los principios para la organización y compilación de los papeles de trabajo.

Existen variaciones en cuanto al contenido y organización que puedan tener diferentes empresas en sus papeles de trabajo. A continuación se muestra una forma de como presentar la documentación, dividiendo cada actividad en secciones, para lograr con esto un mejor ordenamiento:

Sección 0. Tabla de Contenido

Dentro de esta tabla se realiza la descripción detallada de cada sección con su correspondiente numeración de página inicial y final. Esta numeración estará hecha de una forma que ayude a realizar una mejor clasificación, adición y revisión de los papeles de trabajo.

Sección 1. Programa de Auditoría

Esta sección se considera como la creación del Plan de Trabajo de Auditoría que debe ponerse en marcha para poder cumplir con los objetivos trazados.

El programa deberá incluir la definición precisa de los objetivos y la descripción detallada de los pasos en donde se especificará el trabajo a ser realizado.

Se hace necesario que al momento de llevar a cabo la revisión de los papeles de trabajo, éstos posean alguna referencia con los pasos definidos en el programa de auditoría.

Sección 2. Informe de Auditoría

En esta sección se incluye una copia del informe final de auditoría.

Sección 3. Respuesta al Informe de Auditoría

Para la administración, las respuestas dadas por la auditoría pueden manejarce de diferentes formas. En algunas se toman como parte del reporte final, en cambio en otras se mantienen en forma separada para lograr que se facilite el seguimiento de su implantación.

Sección 4. Seguimiento de la Auditoría

En esta sección se documenta la correspondencia y los trabajos de auditoría realizados por la administración, a efecto de continuar con las acciones correctivas dados en los controles recomendados.

Sección 5. Papeles de Trabajo detallado

Esta sección incluye la documentación del trabajo realizado y todas las evidencias obtenidas por el auditor. Se recomienda que los papeles de trabajo sean preparados al mismo tiempo en que se desarrolla el trabajo. Estos deben de ser completos, deberán de poseer número de página, título y su referencia para poder facilitar el mantenimiento de los papeles en caso de que alguno sea removido.

Dentro de está sección se puede hacer mención a ciertos tipos de formularios especiales, que están diseñados para facilitar la recolección de los datos en el trabajo de auditoría. La forma como están diseñados los formularios permiten que sean utilizados como fuente de información para alimentar las bases de datos que fueron

diseñadas para soportar el trabajo de análisis de controles. A continuación se exponen cada uno de estos formularios:

- Formulario 1.0- Ciclo de Actividad
  Utilizado pará describir en forma detallada los ciclos de actividad en que está dividido el Sistema que se audita.

- Formulario 2.0- Descripción de Recursos
  Utilizados para la descripción de recursos empleados en el sistema.

- Formulario 3.0- Relación entre Ciclos y Recursos
  Se utiliza para hacer una relación entre los Ciclo de Actividad del Sistema y los recursos en cada uno de los proceso o subproceso del cual está compuesto cada uno de los diferentes Ciclos de Actividad.

- Formulario 4.0- Descripción de Riesgos
  Utilizado para describir los Riesgos que se asocian al sistema auditado.

- Formulario 5.0- Descripción de Amenazas
  Utilizado para describir las Amenazas a que se exponen los recursos del sistema y al mismo tiempo establecer la relación que existiera con los riesgos si se llegaran a materializar las amenazas.

- Formulario 6.0- Descripción y Prueba de Controles
  Utilizado para describir las características de los controles que han sido identificados y documentar los resultados que se obtienen de la prueba o verificación.

- Formulario 7.0-Relación entre Recursos, Amenazas y Controles
  Es utilizado para establecer la relación entre los recursos, las amenazas a que están expuestos y los controles para poder prevenir o eliminar la amenaza identificada.

Se presentan a continuación los formularios mencionados y explicados en los párrafos anteriores para poder entender gráficamente el funcionamiento de cada uno de ellos.

Se presentan siguiendo la misma numeración utilizada en su explicación.

FORMULARIO 1.0

LOPEZ-CARBALLO AUDITORES

Hoja ___ de ___

AUDITORIA Y SEGURIDAD DE SISTEMAS

Sistema _____

_____

CICLO DE ACTIVIDAD

AREA	CICLO	PROCESO	SUBPROCESO	DESCRIPCION	PESO

FIRMA DEL AUDITOR _____ FECHA _____

FORMULARIO 2.0

LOPEZ-CARBALLO AUDITORES

Hoja ___ de ___

Sistema _____

_____

AUDITORIA Y SEGURIDAD DE SISTEMAS

DESCRIPCION DE RECURSOS

NUMERO CONSEC.	NUMERO INTERNO	◄——DESCRIPCION——►	PESO

FIRMA DEL AUDITOR _____ FECHA _____

FORMULARIO 3.0

LOPEZ-CARBALLO AUDITORES

AUDITORIA Y SEGURIDAD DE SISTEMAS

TABLA DE RELACION DE CICLOS Y LOS RECURSOS UTILIZADOS EN LOS PROCESOS

Hoja ___ de ___

Sistema _____

AREA		
CICLO		
PROCESO		
SUB-PORCESO		

RECURSOS

EQUIPOS	E							
DOCUMENTOS FUENTES	F							
ARCHIVOS MAGNETICOS	M							
INFORMES	I							
PROGRAMAS	P							
ARCHIVOS DOCUMENTAR	A							
DOCUMENTACION Y MANUALES	D							
RECURSOS HUMANOS	R							
CUENTAS	C							
INSTALACIONES	N							
OTROS RECURSOS	O							

FIRMA DEL AUDITOR _____ FECHA _____

FORMULARIO 4.0

LOPEZ-CARBALLO AUDITORES

AUDITORIA Y SEGURIDAD DE SISTEMAS

DESCRIPCION DE RIESGOS

Hoja ___ de ___

Sistema _____

_____

NUMERO	DESCRIPCION	PESO

FIRMA DEL AUDITOR _____ FECHA _____

FORMULARIO 5.0

LOPEZ-CARBALLO AUDITORES

Hoja ___ de ___

AUDITORIA Y SEGURIDAD DE SISTEMAS

Sistema _____

_____

DESCRIPCION DE AMENAZAS

NUMERO	DESCRIPCION	PESO	RIESGOS POTENCIALES						

FIRMA DEL AUDITOR _____ FECHA _____

FORMULARIO 6.0

LOPEZ-CARBALLO AUDITORES

AUDITORIA Y SEGURIDAD DE SISTEMAS

DESCRIPCION Y PRUEBAS DE CONTROLES

Hoja ___ de ___
Sistema
Area Responsable
Numero
Tipo

DESCRIPCION DEL CONTROL

PROPOSITO DEL CONTROL

CLASE DE CONTROL	AMENAZAS CUBIERTAS	RECURSOS PROTEGIDOS
1. DISUASIVO 2. PREVENTIVO 3. DETECTIVO 4. RECUPERATIVO 5. CORRECTIVO		

PRUEBA DE CONTROL

PRUEBA A REALIZAR	TIPO DE PRUEBA	
	1. Prueba en Línea	PL
	2. Observación Documentos Fuente	OD
	3. Verificación Archivos	VA
	4. Otras	OT

RESULTADOS OBTENIDOS	EVALUACION DE RESULTADOS
	1. NO EXISTE 2. CONTROL DEBIL 3. CONTROL SATISFACTORIO 4. CONTROL BUENO 5. CONTROL MUY BUENO

ESTADO DEL CONTROL RECOMENDACION

1. IMPLANTADO
2. RECOMENDADO
3. DESCARTADO

FECHA ESTIMADA IMPLANTACION

FIRMA DEL AUDITOR _____ FECHA DE VERIFICACION _____

FORMULARIO 7.0

LOPEZ-CARBALLO AUDITORES

AUDITORIA Y SEGURIDAD DE SISTEMAS

TABLA DE RELACION-RECURSOS/AMENAZAS/CONTROLES

Hoja ___ de ___

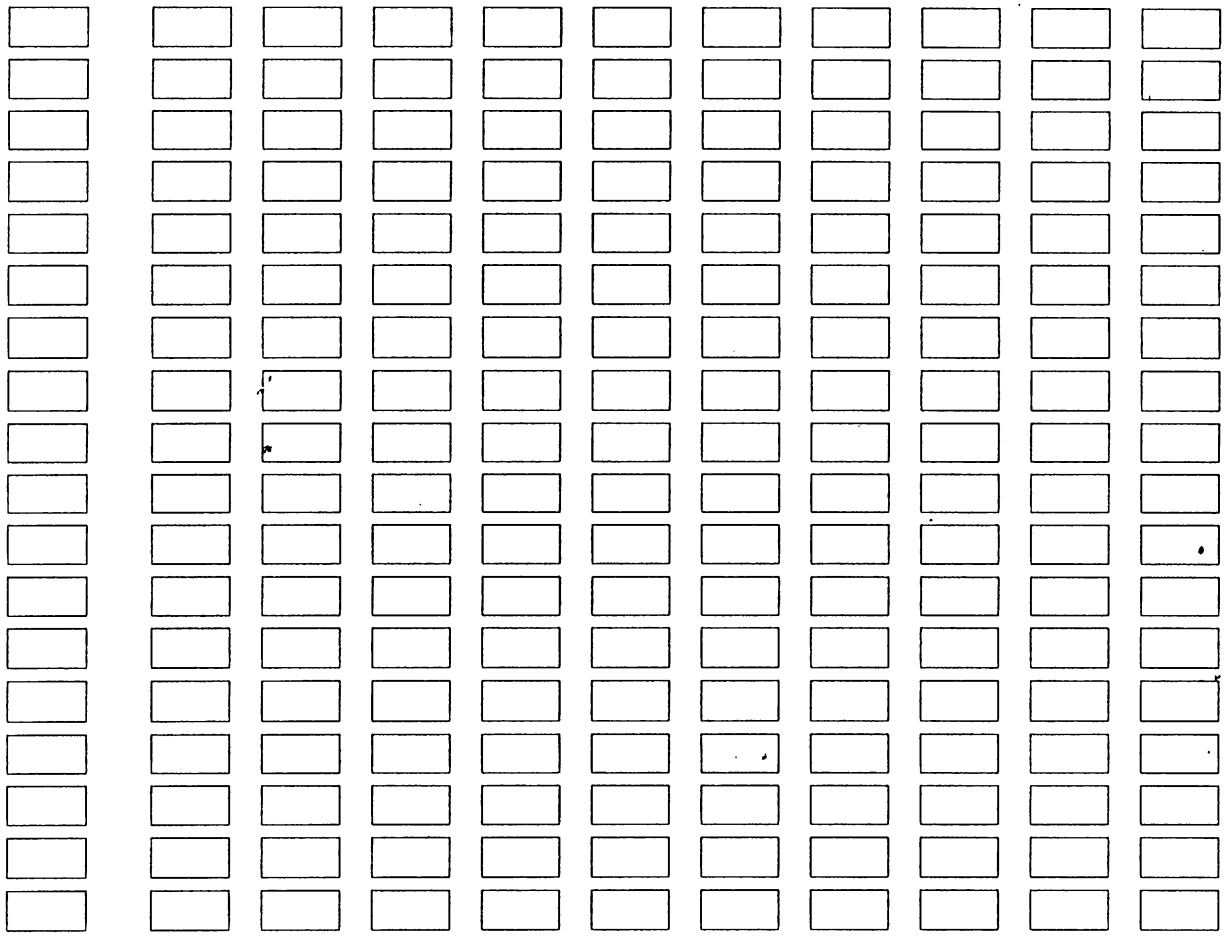
Sistema _____

_____

NUMERO CONSEC.	DESCRIPCION DEL RECURSO

TIPO DE RELACION: POR GRUPO DE RECURSOS ☐ POR SUBGRUPO ☐ POR RECURSO INDIVIDUAL ☐

AMENAZAS ◄——— CONTROLES ———►



AUDITOR _____ FECHA _____

Sección 6. Análisis de Control

En esta sección se guardan las Matrices Relaciónales y todos los reportes que fueron hechos para realizar la evaluación de los controles existentes.

Sección 7. Plan de Pruebas y sus Resultados

En esta sección se incluyen los formularios que han sido realizados para poder detallar la prueba que se debe de llevar a cabo a cada control, la forma como realizarla y los resultados obtenidos.

Sección 8. Consideraciones para Auditorías Futuras

Hay ocasiones en que alguna exposición considerada de mucha importancia no fue cubierta durante el desarrollo de la auditoría, esto pudo haber sido ocasionado porque no fueron identificados aspectos con anticipación.

Con el hallazgo de esta información se hace necesario la ampliación de la cobertura, dejándolo en algunas ocasiones como aspecto a ser considerado en una revisión posterior.

Sección 9. Archivo Permanente

Recibe este nombre debido a que todos los datos o informaciones que se manejan no están expuestas a modificaciones. Los archivos permanentes deben estar compuesto por los siguientes ítems: flujogramas de procesos, formatos, contratos, diagramas de las aplicaciones, etc.

Mantener este tipo de archivo permite que la ejecución de futuras auditorias sean realizadas con mucha facilidad, especialmente si éstas son realizadas por auditores diferentes a los que llevaron a cabo el trabajo.

4.6.1.6 APROBACION DEL PROYECTO

Es considerada la parte final de la Fase de Organización. Es por esto, que una vez escogido el sistema, definido los alcances y

objetivos y especificado el Plan, la documentación deberá ser presentada por el Director del Proyecto al Auditor Interno.

El aporte que el Auditor Interno realiza al revisar y aprobar el proyecto se puede considerar como significativo, ya que es quien conoce las metas generales de su área y la forma de constituir los diferentes recursos en los diversos proyectos para cumplir con los objetivos que se han trazado en un período determinado.

El informe realizado por el Auditor encargado del proyecto, debe estar desarrollado sin ninguna limitante en cuanto al manejo de elementos técnicos automatizados. Todas sus definiciones deben ser precisas, ya que con esto facilitará al Auditor Interno a realizar la aprobación del proyecto y al mismo tiempo se podrá contar con un soporte para garantizar el éxito de los resultados.

Cuando el proyecto ha sido aceptado, se debe de realizar una hoja de aprobación, el cual contendrá la información básica del proyecto, los objetivos y el alcance de lo que se desea realizar, el presupuesto en días/hombre y las fechas tanto de inicio, preparación y obtención de resultados dado por los encargados.

4.6.1.7 COMUNICACION DEL PROYECTO

Para un mejor entendimiento a la hora de llevar a cabo la actividad de campo, es necesario realizar reuniones con todas las áreas que estarán presente en el desarrollo del proyecto, para darles a conocer los objetivos que se pretenden, su alcance, duración, compromisos y los resultados que se esperan, indicándoles al mismo tiempo la forma como estos serán presentados a la administración general.

Como uno de los aspectos importantes dentro de esta etapa, es aclarar quien es el encargado de la implantación y cumplimiento de los controles. Esta responsabilidad está dada para que sea realizada por la administración, dándole al auditor el trabajo de evaluar la existencia y suficiencia de los controles para poder así preparar el informe con las recomendaciones que ayudarán a mejorar el sistema de control. Queda claramente establecido que el auditor servirá como un soporte tanto para el área operativa como administrativa.

5.6.2 FASE 2. IDENTIFICACION DE TRANSACCIONES Y RECURSOS

5.6.2.1 DEFINICION DE LOS CICLOS TRANSACCIONALES

El objetivo de definir los Ciclos de Actividad, es poder identificar los pasos lógicos que deben cumplirse durante la vida del sistema. Con esta identificación se logrará que la revisión de la auditoría se realice con la misma secuencia con la cual fue hecha la operación, logrando con esto una mayor claridad en el proceso y una recopilación ordenada de los aspectos que se consideran en la auditoría. Para obtener una información más detallada el auditor se basará de el Manual de Procedimientos Operativos y de el Manual de Usuario del Sistema.

Una vez definidos los Ciclos de Actividad, deberá de llevarse a cabo reuniones con los encargados de la operación, con el único fin de poder aclarar las diferencias y poder obtener una base común para la realización del trabajo.

Para poder definir los Ciclos de Actividad, debe tomarse en cuenta los objetivos y alcances que son establecidos para la auditoría,

incluyendo al mismo tiempo actividades de tipo operacional, administrativo y de revisión, así como las aplicaciones llevadas a cabo por el computador.

En cuanto a los proceso automatizados, su definición dependerá de las características de la aplicación y el uso dentro del sistema operativo. Dependiendo del diseño de la aplicación, se puede clasificar como:

- Aplicación por lotes
- Aplicación en línea

5.6.2.2 PREPARACION Y ANALISIS DE FLUJOGRAMAS

El concepto de Ciclo de Actividad, Procesos y Sub-Procesos tiene como propósito asegurar que el trabajo de análisis de amenazas y controles pueda tener la cobertura necesaria de acuerdo con los alcances de la auditoría y que la evaluación se realice de una forma ordenada.

Pero cabe decir que lo vertido en este concepto no es lo suficiente para poder llevar a cabo la evaluación, por lo tanto se hace necesario el análisis de los procesos y subprocesos con el único objetivo de:

a) Poder conocer los funcionarios responsables por los procesos. Aquí se podrá identificar si las funciones están debidamente separadas unas de otras y si cumplen con los especificado en los Manuales de Funciones y Procedimientos.

b) Identificar las relaciones entre los diferentes procesos y subprocesos que conforman los Ciclos analizados. A través de este análisis se podrá detectar que actividades o procedimientos hacen ineficiente el manejo de la operación.

c) Tener claramente establecidos los puntos donde son almacenados el flujo de documentos. Con este se pretende analizar si se está llevando a cabo correctamente las políticas en materia de retención, custodia de documentos y listados del computador.

d) Reconocer los recursos que tienen participación en cada uno de los procesos y subprocesos. Este es de los recursos más importantes para que el análisis cumpla con su propósito, pues es donde se reconoce las amenazas y controles.

Para una mejor realización del análisis referido, se hace necesario que sea explicado a través de un procedimiento que venga a constituir un medio de comunicación que pueda ser entendido con mucha facilidad por todas las personas que estén involucradas en la operación, este procedimiento muy conocido por la mayoría recibe el nombre de Diagramas de Flujo o Flujogramas de los proceso.

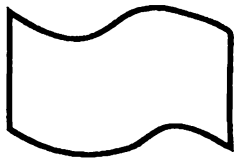
Los flujogramas facilitan a través de su simbología la identificación y análisis de los recursos utilizados en la operación, evitando al mismo tiempo la descripción literal de los procesos.

Muchas empresas con el único fin de erradicar los procedimientos realizados manualmente, han adquirido una serie de herramientas desarrollas por microcomputadoras, que vienen a agilizar la

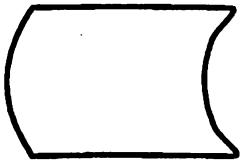
elaboración, actualización y almacenamiento de todos los procesos. Algunas de estas herramientas son: Flowchart o Freelance.

A continuación se muestra la simbología que se emplea para la elaboración de algunos Diagramas de Flujo.

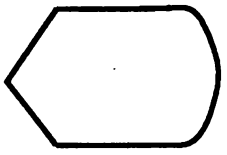
SIMBOLOGIA UTILIZADA PARA LA REALIZACION DE DIAGRAMAS DE FLUJOS



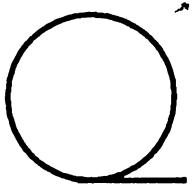
CINTA PERFORADA



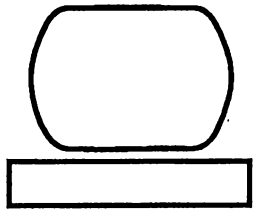
ALMACENAMIENTO EN LINEA



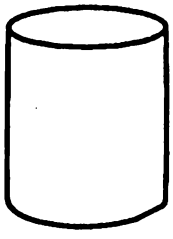
TERMINAL



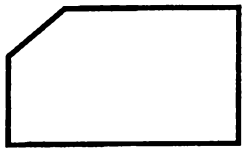
CINTA MAGNETICA



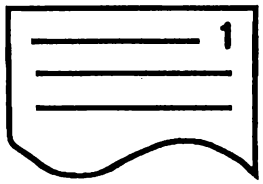
MICRO



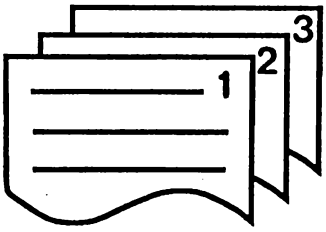
DISCO MAGNETICO



TARJETAS PERFORADAS

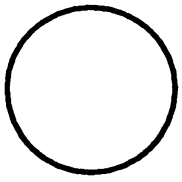


LISTADO DE COMPUTADOR

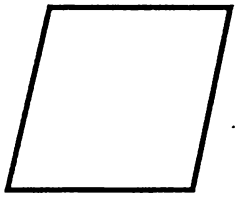


LISTADO DE COMPUTADOR CON ORIGINAL + 2 COPIAS

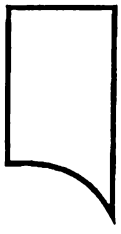
PROCESO



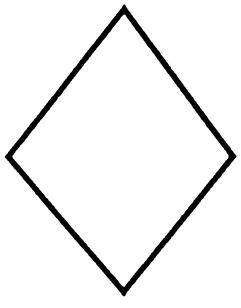
CONECTOR



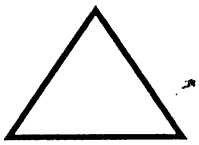
ENTRADA/ SALIDA



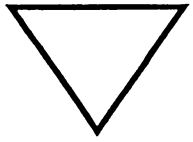
CINTA EN TRANSITO



DECISION

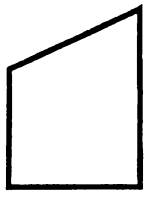


EXTRAER



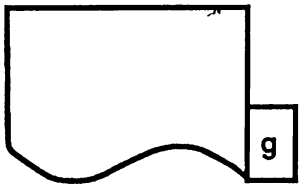
UNIR

LIBRO O REGISTRO CONTABLE

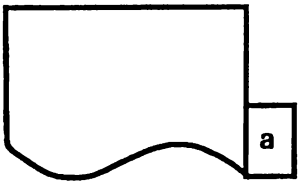


ENTRADA MANUAL

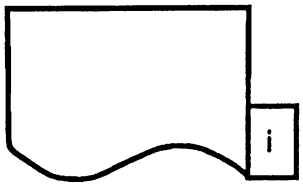
PREPARACION



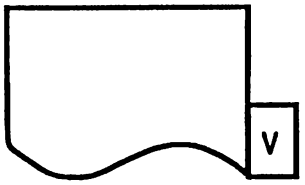
GENERAR DOCUMENTO



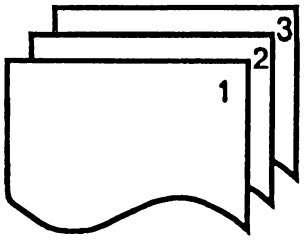
APROBAR DOCUMENTO



AGREGAR DATOS AL DOCUMENTO

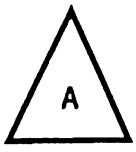


VERIFICAR DOCUMENTO

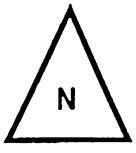


DOCUMENTO CON ORIGINAL Y 2 COPIAS

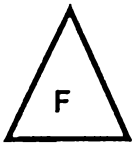
DOCUMENTO ARCHIVADO EN FORMA TEMPORAL



ALPHABETICO

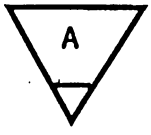


NUMERICO

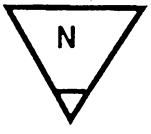


POR FECHA

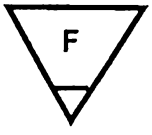
DOCUMENTO ARCHIVADO EN FORMA PERMANENTE



ALPHABETICO



NUMERICO



POR FECHA

5.6.2.3 IDENTIFICACION Y DOCUMENTACION DE LOS RECURSOS

Uno de los objetivos principales en la revisión de auditoría de un sistema automatizado, es la identificación de las amenazas a que están expuestos los recursos que se utilizan en dicho sistema, de tal forma que se puedan definir los controles pertinentes para eliminar o reducir tales amenazas.

El análisis de los recursos se inicia durante la preparación de los Diagramas de flujo, en los cuales deberán quedar claramente identificados los recursos y su relación con los procesos en que ellos son utilizados.

Un recurso se define como algo tangible, de valor, que es usado durante los procesos identificados y que puede estar expuesto a amenazas que de materializarse podrían originar los riesgos para el sistema.

Realizada la identificación en los flujogramas, debe procederse a su documentación, para lo cual es conveniente el uso de una codificación específica de todos los recursos que son utilizados.

5.6.3 FASE 3. ANALISIS DE RIESGOS Y AMENAZAS

5.6.3.1 IDENTIFICACION Y DOCUMENTACION DE RIESGOS

Debido a la imposibilidad que la auditoría presenta al momento de querer cubrir todas las áreas donde se ha desarrollado el sistema, se hace necesario la implantación de una estrategia basada en el análisis de riesgos, lo cual permitirá poner una mayor atención a aquellos riesgos que sean considerados críticos de acuerdo al sistema que se esté analizando.

En forma general se pueden decir que las áreas que poseen mayor riesgo son las siguientes:

- La dependencia de los negocios de sus sistemas automatizados
- La integridad de la información
- La posibilidad de fraude
- La privacidad y confidencialidad de la información manejada por el sistema

Es necesario que el auditor antes de querer diseñar una estrategia de auditoría con base en el entendimiento y evaluación de la fuerza y fragilidad del sistema, conozca los riesgos que están asociados al sistema.

El Instituto Americano de Contadores Públicos Certificados (AICPA), ha publicado el Estándar de Auditoría (SAS) número 47, que dice: "Riesgo de Auditoría y Materialidad en la Realización de una Auditoría: Modelo de Riesgos de Auditoría". Esto significa que las fallas de los negocios, la incertidumbre económica, las decisiones de las cortes y los cambios impuestos por la tecnología PED deben tenerse en cuenta para incrementar la atención de los profesionales de auditoría sobre los riesgos de auditoría.

A medida que el usuario tenga un conocimiento más amplio sobre la tecnología utilizada, puede aumentar el riesgo de fraude. Para poder evitar esta situación es necesario la implantación de controles de acceso sobre los reportes a través de rutinas programadas y la verificación de todos los programas que allí se utilicen.

Para la Auditoría de Sistemas, el análisis de riesgo está definido como un enfoque sistemático para evaluar las exposiciones potenciales asociadas con un sistema en funcionamiento. El análisis de riesgo permite identificar las causas más probables de riesgo, o sea, las amenazas, garantizando que el sistema de control elimine o reduzca los riesgos asociados con el sistema.

Un riesgo es un resultado desfavorable que trae como consecuencia pérdidas de tipo cualitativo o cuantitativo.

5.6.3.2 IDENTIFICACION Y DOCUMENTACION DE LAS AMENAZAS

Se puede definir una amenaza como la causa de producir un riesgo. Cuando una amenaza llega a concretarse dentro de un sistema, ésta puede provocar que existan uno o más riesgos.

Para poder dejar más claro en lo que se refiere al riesgo/amenaza, tomemos un ejemplo del riesgo de "Fraude-Desfalco". Supongamos que se trata del procedimiento de un retiro en una cuenta de ahorros de un banco. A través del proceso de evaluación de riesgo/amenaza se pueden identificar los recursos que se utilizan

para el procesamiento de la operación, estos recursos son: Solicitud de retiro, una terminal para la captura de datos, el archivo maestro de clientes, etc.

Utilizando el concepto de riesgo, el auditor puede identificar las amenazas a las cuales esta expuesto los recursos; estas son:

- Transacción no autorizada
- La no existencia de copias de recibo para el cliente
- Transacciones no registradas
- Acceso no controlado a documentos fuente
- Ausencia de control de acceso al software de la aplicación
- Ausencia de procedimiento para corrección de errores
- Falta de totales de control.

5.6.4 FASE 4. IDENTIFICACION Y ANALISIS DE CONTROLES

5.6.4.1 INTRODUCCION A LAS CLASES DE CONTROLES

Para que exista una mejor utilización de los controles a la hora de realizar una revisión, es necesario tener un buen conocimiento y entendimiento de las clases de controles que existen.

A continuación se mencionan y se describen en forma detallada los controles que son considerados con más importancia:

CONTROLES DISUASIVOS:

Estos se encargan de parar actividades que no desean antes de que estos puedan actuar.

Como ejemplo a este control se tiene: Colocar un aviso a la entrada del centro de computo que diga: "PROHIBIDA LA ENTRADA A PERSONAL NO AUTORIZADO". Este rotulo servirá para poder desanimar a las personas que no tienen autorización a ingresar a el área. Otro ejemplo sería la creación de un CODIGO DE ETICA para poder ingresar al sistema, con el fin de prohibir algún tipo de manejo no autorizado y que la persona desistiera de su intento.

CONTROLES PREVENTIVOS:

Estos son los considerados de mayor importancia y están realizados para poder prevenir la ocurrencia de una amenaza.

Un ejemplo sería el control de acceso que un usuario requiere para poder ingresar al sistema, pudiéndolo hacer a través de su identificación y una clave de acceso. Otro ejemplo de este control sería la creación de rutinas en los programas que servirán para poder validar los datos en el momento de ingresarlos y al mismo tiempo borrar los datos incorrectos.

CONTROLES DETECTIVOS:

Estos se encargan de capturar o identificar algún evento anormal luego de que éste ha ocurrido, y posteriormente combatirlo con acciones correctivas y recuperativas.

Como ejemplo para este control se tiene: la creación de un registro de actividades que se encarguen en guardar información acerca de que terminal, a que hora y fecha se realizaron intentos ilegales para poder ingresar al sistema, y a través de un reporte poder saber que persona estuvo realizando esta operación. Otro ejemplo sería la realización de Bitácoras de Transacción, las cuales servirán para registrar cada uno de los cambios que se le hacen a la Base de

Datos y poder verificar que solamente acepte los cambios que han sido autorizados.

CONTROLES RECUPERATIVOS:

Este control entra en funcionamiento una vez a ocurrido el evento, o sea las amenazas se han cumplido y han sido detectadas por los controles para poder llevar a cabo la acción de recuperar la situación normal.

Como ejemplo a este control se tiene la utilización de cintas magnéticas como respaldo para poder reprocesar el sistema de nóminas después de haber detectado que por daños en los archivos maestros el proceso salió incorrecto.

CONTROLES CORRECTIVOS

Este control se relaciona a menudo con el control recuperativo, ya que una vez que ha ocurrido el problema y ha sido detectado, se hace necesario recuperar la situación y llevar a cabo una serie de

ajustes al sistema de control para poder garantizar la prevención de futuros eventos.

Como ejemplo está el envío de un usuario o empleado al departamento de personal para que se le apliquen sanciones disciplinarias debido a que se le detecto querer ingresar indebidamente al sistema.

5.6.4.2 IDENTIFICACION Y DOCUMENTACION DE LOS CONTROLES

El propósito principal de la creación de los controles fue para disminuir la posibilidad de reducir la ocurrencia de amenazas y recuperar lo perdido debido a los riesgos.

A parte de identificar los recursos que intervienen en las transacciones y a las amenazas a que están expuestas, es necesario conocer los controles que se necesitan para su prevención.

No se hace necesario realizar un trabajo de creación de controles cada vez que se quiera llevar a cabo una auditoría, sino que se

debe de utilizar listas de referencias en las cuales se especifica cada uno de los controles con diferentes niveles y propósitos. Esto servirá al auditor para tener un mejor criterio al momento de seleccionar los controles más adecuados para el sistema que se ha escogido analizar.

Luego de haber identificado los controles necesarios para prevenir o detectar amenazas y lo que se refiere a la corrección y recuperación de pérdidas, se debe de realizar la documentación de estos controles.

Es más recomendable la documentación de los controles al mismo tiempo que son identificados y definidos. Por otra parte, el auditor debe tener muy en cuenta la inclusión de controles existentes y controles que el considere necesario recomendarlos.

5.6.4.3 ANALISIS DE COBERTURA DE CONTROLES EXISTENTES

Luego de haber determinado las amenazas, identificado y documentado los controles, es necesario iniciar la etapa de Análisis de Cobertura.

Este Análisis tiene como objetivo determinar los ciclos con menor protección, o aquellos que por la debilidad de los controles están más expuestos a los riesgos. También permite realizar la evaluación razonable de nuevos controles y reforzar los argumentos que son usados para hacer recomendaciones.

Para poder realizar este análisis se utilizan dos tipos de herramientas, las cuales se mencionan a continuación:

1. REPORTES DE RELACION

Para poder utilizar este reporte es necesario que antes se generen y revisen de manera individual los elementos amenazas, riesgos, recursos y controles. Esto servirá para ver si los datos que son almacenados en el sistema poseen calidad, y la relación que se haga entre ellos sea buena.

Dentro de los reportes de relación existen diferentes tipos, entre los más importantes se mencionan:

a) Reporte de Amenazas/Riesgos

Este logra hacer un análisis de la relación que existe entre los riesgos identificados y las amenazas que los originan.

b) Reporte de Recursos/Amenazas

Este permite determinar la relación entre los recursos y las amenazas a que ellos están expuestos.

c) Reporte de Transacciones / Amenazas

Este reporte permite realizar una composición entre los Ciclos de Transacciones y las amenazas existentes para ellos, las cuales se determinan por la relación directa entre los recursos comprometidos en los Ciclos y sus amenazas directas.

d) Reporte de Recursos / Controles

Este puntualiza los controles sobre cada uno de los recursos y permite ser analizado para poder identificar las posibles debilidades que se originan en el diseño de los controles.

e) Reporte de Transacciones / Controles

Este reporte muestra los controles totales existentes sobre los ciclos de actividad o transaccional. También permite llevar a cabo Matrices Relacionales.

2. MATRICES RELACIONALES

Conocidas también como Matrices de Control y utilizadas para el análisis de cobertura de control.

Con la utilización de filas y columnas, y las celdas de cruce entre ellas, permite la relación de manera integrada entre los diferentes elementos que se desean analizar, logrando a su vez facilitar la identificación de las transacciones que están o no protegidas ante las amenazas.

Las columnas se utilizan para poner los riesgos o amenazas, las filas para colocar los recursos o ciclos transaccionales y las celdas para poner los códigos de los controles existentes, que ayudarán a proteger las parejas de la relación, o sea, Transacciones / Riesgos, o Recursos / Amenazas.

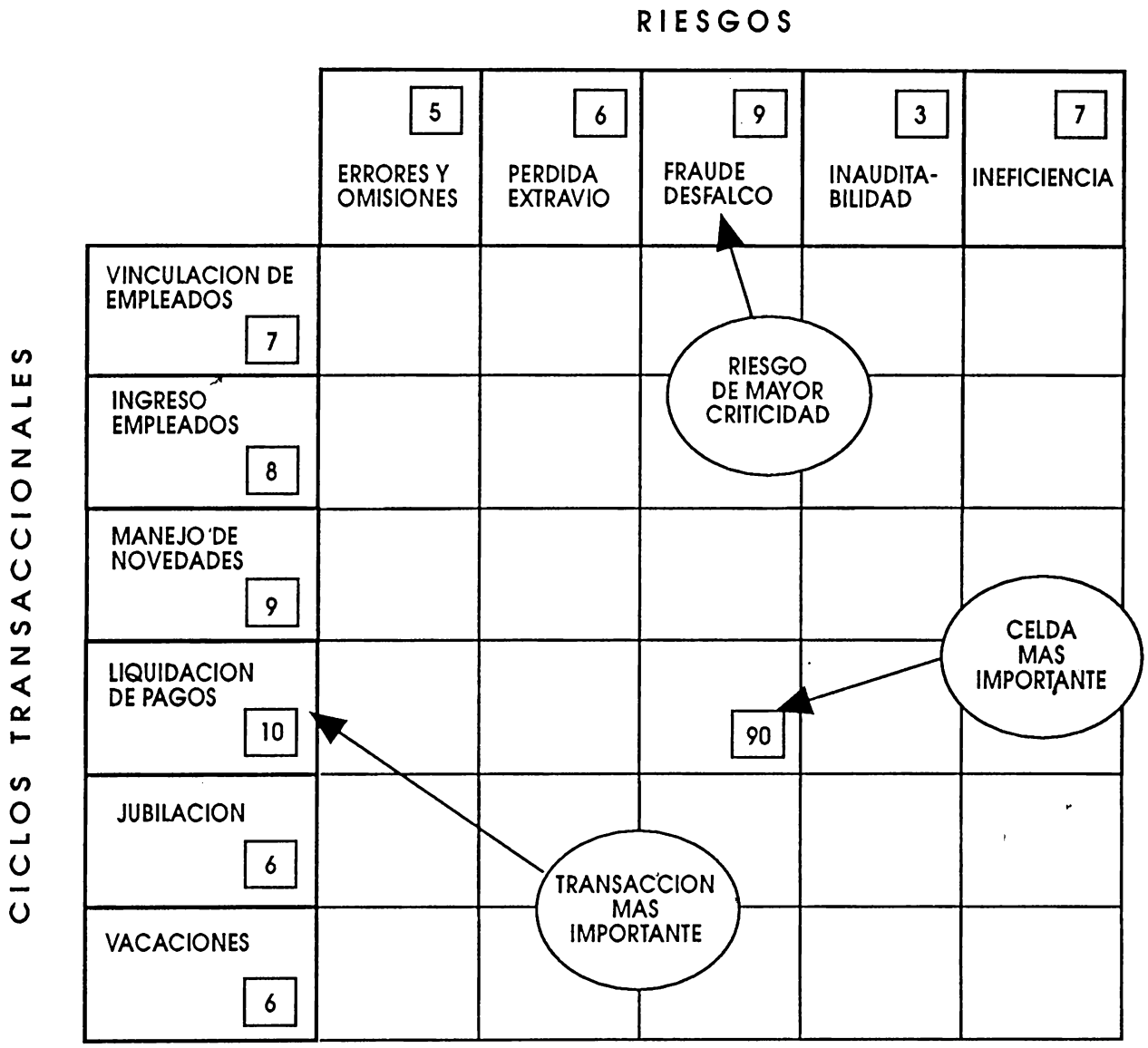
La Matriz más utilizada es la Matriz de Relación Riesgo/Transacciones. Esta da a conocer la relación que existe entre los riesgos identificados para el sistema y las transacciones que lo conforman.

La realización de la Matriz Relacional se lleva a cabo a partir de las relaciones existentes entre las amenazas que generan los riesgos, los recursos que están expuestos a las amenazas y los recursos utilizados en las transacciones.

Cabe aclarar que aunque la Matriz Riesgo/Transacciones sea la de mayor importancia, no impide al auditor crear otras matrices de relación, las cuales vendrán a darle una ayuda para poder realizar evaluaciones más detalladas.

En la siguiente página se presenta un ejemplo de una matriz de control.

MATRIZ DE CONTROL BI-DIMENSIONAL



5.6.4.4 DOCUMENTACION DE LOS CONTROLES RECOMENDADOS

Dentro del proceso de Auditoría no existe una etapa que identifique los nuevos controles que el auditor considere recomendar. Durante la práctica pueden aparecerse:

- Durante la identificación de las amenazas
- Durante la identificación de los controles existentes
- Como resultado del análisis de cobertura de los controles
- En la ejecución de las pruebas de los controles existentes.

Es recomendable que toda la documentación se realice a medida que se identifican los controles. Se debe considerar el buen manejo de los controles ya que puede suceder que durante la prueba de los controles se confirme la existencia de algún control que no había sido identificado antes o se elimine uno que se había considerado recomendar.

5.6.5 FASE 5. PRUEBA DE LOS CONTROLES

5.6.5.1 OBJETIVOS Y ALCANCES DE LA PRUEBA

El objetivo que se persigue con la prueba de los controles es observar si se están cumpliendo con las diferentes etapas del proceso donde estos se ubican, y al mismo tiempo evaluar su suficiencia para poder controlar las amenazas.

En lo que se refiere al alcance, la relación la tiene directamente con los objetivos definidos en la Fase de Planeación del proyecto.

Para la verificación de los controles se puede decir que resultaría muy poco práctico querer llevarlos a cabo todos. Es por está razón que el Auditor debe definir con mucha anticipación los controles que por su naturaleza y característica son determinadas para el sistema de control.

Dentro de la verificación de ejecución de pruebas el Auditor puede realizar diferentes pruebas que servirán para tener una mayor

cobertura, éstas pueden ser la revisión de los archivos de datos o transacciones.

Como un principio, el Auditor debe evitar realizar algún tipo de comentario parcial de los resultados de las pruebas, aunque en la mayoría de los casos los encargados del sistema están enterados del programa de actividades que deben seguir para la evaluación.

5.6.5.2 EL PLAN DE PRUEBAS

Este plan asegura que la ejecución se realice de una forma ordenada, dándole mayor importancia a los controles con mayor prioridad y destinando los recursos que se encargaran de la evaluación. Cuando se selecciona los controles debe tenerse muy en cuenta que los controles preventivos son los más importantes ya que ofrecen una barrera lógica y física que ayudan a impedir que ocurran eventos fuera de lo normal.

En cuanto a la preparación de el plan de pruebas, debe darse una definición del tipo de prueba que se debe realizar y una definición

de los criterios que deben usarse para determinar la razonabilidad y suficiencia de los controles.

Luego de haber realizado el plan de pruebas, se pasa a comunicar a las diferentes áreas la fecha en que se llevara a cabo, solicitando al mismo tiempo el escrito de los elementos que se necesitaran para su cumplimiento.

Para poder llevar a cabo la ejecución del Plan de Pruebas se hace necesario que existe la autorización por parte del Jefe de Auditoria.

5.6.5.3 EJECUCION DE LAS PRUEBAS

PRUEBAS DE LOS CONTROLES GENERALES DEL SISTEMA

La comprobación de los controles del sistema está dirigido a la revisión de la documentación y manuales del sistema. Esta documentación se incluye:

a) Manual de Políticas y Normas Generales

b) Manual de Procedimiento

c) Manual de Función

d) Manual Técnico de la Aplicación

e) Manual de Usuario de la Aplicación

Dentro de la revisión se debe abarcar los procedimientos definidos para la modificación y actualización de tales manuales.

El papel del Auditor deberá ser el de verificar que se cumpla con las normas que fueron definidas en cada documento. Como un caso específico del Manual del usuario, el auditor verificará si las responsabilidades dadas a cada encargado son las especificadas en el manual y al mismo tiempo poder determinar la razonabilidad de las modificaciones.

El Auditor deberá solicitar a los funcionarios la documentación donde se especificaron las modificaciones de la prueba.

Si existiese algún incumplimiento por insignificante que éste sea, deberá ser evidenciado en el resultado de la prueba.

No podrá ser tomado por el auditor como base para obtener conclusiones, aquellas situaciones en las cuales la documentación de un sistema no exista o no esté actualizada. Es por eso necesario la verificación directa de su cumplimiento.

PRUEBA DE LOS CONTROLES MANUALES

Estos tienen una relación directa con las siguientes actividades:

a) Preparación de los documentos fuente del sistema

b) Autorización de las Transacciones

c) Custodia de Documentos fuente en blanco

e) Manejo de archivos documentarios

Para una mejor realización de este tipo de prueba se recomienda llevar a cabo un seguimiento de la ejecución de los procesos juntamente con los encargados de la realización y dependiendo de las insuficiencias presentadas sea necesario que el auditor realice una verificación de los documentos fuente con información histórica.

Es necesario que el Auditor obtenga copias de aquellos documentos fuentes que posean errores, lo cual le servirán como parte de su archivo personal y como una fuente para sus conclusiones.

PRUEBA DE LOS CONTROLES DE LA APLICACION

Esta actividad va orientada principalmente a la evaluación de los controles que son incorporados en los programas y cuya utilización es la de capturar, validar y actualizar los archivos maestros. Junto a esto tendrán que ser revisados en forma detallada los controles que existen en ese momento para la administración de datos de entrada y para la distribución de los reportes.

Para llevar a cabo en forma correcta la verificación de los controles de los programas existe una técnica que recibe el nombre de SIMULACION, la cual consiste en la realización de un sistema paralelo independiente al utilizado para el procesamiento normal de la aplicación. Pero se deberá utilizar las mismas versiones de los programas que operan en condiciones normales.

Una vez llevado a cabo el sistema, deberá ser preparado por parte del Auditor un paquete completo de los documentos fuentes que fueron utilizados durante el registro de las transacciones, lo cual servirá como base para alimentar al sistema que se desea probar.

Luego de haber alimentado los datos, el Auditor llevará a cabo los reportes más importantes del sistema o en su defecto obtendrá vaciados de los archivos actualizados en los cuales se puede verificar la calidad de los datos actualizados por los programas.

Si la ejecución de la prueba se llevase a cabo dentro del centro de cómputo, se deberá tomar muy en cuenta las siguientes consideraciones:

a) No hacer ningún tipo de comentario con los programadores o analistas si existiese algún tipo de deficiencia detectada. Al igual que los controles manuales esto puede generar que los programadores puedan proceder lo más pronto posible a modificar los programas.

b) En casos de existir abortos o fallas del sistema, se recomienda no realizar acciones de tipo correctivas al sistema ni solicitar ningún tipo de ayuda aún cuando se conozca la solución. La información de cualquier problema deberá ser solicitada en forma escrita al Jefe de Sistema.

c) No tomar sin autorización elementos necesarios para la prueba (cintas, diskettes, etc.)

d) Llevar a cabo los procedimientos tal como aparecen en los Manuales de Usuario, aunque éstos parezcan obvios.

e) Cuando se trate de aplicaciones en proceso por lotes, el Auditor deberá crear los datos directamente utilizando los programas de la aplicación o los dispositivos de grabación.

En cuanto a la administración de los reportes, el Auditor deberá verificar a través de normas escritas la periodicidad con que son realizados los reportes, el número de reportes a producir y al personal que se le enviará. Con estas normas el Auditor podrá saber que tipo de utilización se le está dando a cada informe y al

mismo tiempo conocer los procedimientos aplicados para su almacenamiento.

También el Auditor tendrá la responsabilidad de revisar los procedimientos establecidos para la generación y custodia de los archivos de respaldo, incluyendo además una inspección física de las instalaciones de almacenamiento de tales archivos.

5.6.5.4 ANALISIS Y DOCUMENTACION DE RESULTADOS

Se deberá hacer un análisis sobre los resultados que se obtuvieron de las pruebas de los controles, lo cual servirá para determinar si los resultados permiten una conclusión sobre la capacidad del control o si se hace necesario la implantación de algún tipo de prueba complementaria.

Para poder realizar la documentación de los controles se hace necesario basarse en los siguientes aspectos:

a) Prueba a Realizar:

Se debe dar una descripción de la prueba y documentarla al mismo tiempo que se está llevando a cabo la planeación de las pruebas.

b) Tipo de Prueba:

Las más importantes son: Prueba en Línea, Verificación de Documentos Fuentes, Verificación de Archivos Magnéticos.

c) Resultado de la Prueba:

Describir el resultado obtenido de la Prueba.

d) Evaluación del Resultado:

Calificación del control según el resultado.

e) Recomendación:

El Auditor proporciona una descripción sobre recomendaciones para poder lograr un mejor control de las amenazas analizadas.

5.7 RESULTADOS Y PRESENTACION

5.7.1 PREPARACION DEL INFORME PRELIMINAR

Después de finalizar todas las pruebas y controles, analizar los resultados y definir todos aquellos controles que sea necesario añadir, el auditor deberá proseguir a la elaboración de un primer informe preliminar de auditoría. Este reporte debe dividirse en dos partes, una que estará orientada a la administración en forma de resumen y otra en el que se detallen específicamente los controles.

En el resumen mencionado se deben incluir los siguientes aspectos:

- Contenido: En esta sección deberá darse una visión de lo que será el contenido del informe.
- Introducción: Aquí se debe aclarar a que tipo de auditoría se estará haciendo referencia, ya sea esta de carácter especial o regular.
- Propósito de la Auditoría: Se especifican los objetivos que se alcanzarán con la auditoría.
- Alcance: Se debe especificar hasta donde se llegará con las pruebas planteadas en el desarrollo del proyecto.

- Opinión: En esta sección el auditor expresa cual es su opinión profesional en cuanto al sistema que se esta evaluando, basado en los controles establecidos para el mismo. Esta parte del reporte es de mucha relevancia, pues implanta una prioridad con que deben ser tratados los problemas, de acuerdo a los resultados obtenidos durante el desarrollo del trabajo.
- Hallazgos: En esta parte se presentan todos los descubrimientos importantes de la auditoría, ya sean estos favorables o desfavorables para el área que está siendo auditada en ese momento. Como parte importante del reporte se deben considerar los descubrimientos favorables pues esto ayudará a demostrar la objetividad del trabajo y también servirán como un apoyo para las recomendaciones.
- Recomendaciones: Es aquí donde el auditor expresa sus recomendaciones orientadas a mejorar los procesos de control interno.

En su resumen para la administración, el auditor expone su análisis en el que indica cuales han sido sus hallazgos más relevantes en cuanto a las áreas críticas que presentan deficiencias relacionadas con el control interno, para lo que manifiesta sus recomendaciones con las que se logrará un nivel adecuado en la operación. Todas las recomendaciones y/o conclusiones estarán basadas en los aspectos críticos de los riesgos que

se corren. Es necesario que se especifique claramente cuales son los propósitos y objetivos de las recomendaciones, los cuales deberán aportar una solución práctica para el mejoramiento de los controles y la eficiencia operacional. También deben resaltarse en el informe, todos aquellos aspectos que dan fortaleza al sistema, es decir, aquellos que satisfacen los propósitos para lo que fueron implantados.

A forma de ejemplo: en el resumen se podrán expresar cuales rutinas de validación poseen debilidades y en el informe detallado se expondrán cada una de estas debilidades para las que se indicará cual es el control adecuado para su mejoramiento.

En el informe detallado deberán incluirse todos los controles ya sean estos implantados o recomendados y que han servido como base para la elaboración del resumen. Las recomendaciones se deberán elaborar en una forma clara y sencilla pero práctica de manera que puedan ser entendidas y puestas en práctica, por todo aquel que se relacione con el sistema.

Dentro del informe que se elabore deberán incluirse los siguientes aspectos:

* Número de control

* Estado de Control

* Area (s) responsables del control

* Descripción del control

* Propósito del control

* Prueba realizada

* Resultados de la Prueba

5.7.2 DISCUCION DEL INFORME PRELIMINAR

Antes de que el informe de auditoría (resumen y detallado) sea entregado a la administración de la organización, es necesario que se presente a discusión a todos aquellos encargados del área auditada y también a las personas encargadas de la elaboración e implementación de controles.

El auditor debe lograr que las personas a que se presenta el informe preliminar logren entender la lógica que se ha seguido en el establecimiento de los controles y además obtener un compromiso de estas personas involucradas en cuanto a que dichos controles sean implantados. Estas presentaciones también sirven para que cuando la

administración llame a las personas indicadas para exponer los nuevos controles, éstas ya tengan entendida la situación que se les planteará.

El auditor debe tener la habilidad de vender las recomendaciones para evitar así el hecho de que se le tome como resaltador de problemas o delatador de responsables. Lo importante entonces, no es señalar los errores, sino establecer los controles que permitirán la solución de las deficiencias.

El auditor debe poder escuchar las argumentaciones del personal involucrado al momento de establecer un control, con ello se podrá considerar la no inclusión de alguno de los controles recomendados si el auditor así lo considerase, pero si no se llegase a ningún acuerdo, el auditor deberá tratar de exponer la conveniencia y el porque del control establecido. Debe considerarse a este respecto, que la responsabilidad del cumplimiento o no de un determinado control, recae sobre los administradores generales y operativos, por lo que ellos deberá asumir completa responsabilidad de las consecuencias que se originen de la no implementación de algún control.

No es recomendable que los controles que se descarten por mutuo acuerdo y como resultado de estas reuniones sean eliminados del informe, sino más bien seguirán apareciendo en el mismo bajo una cláusula especial que puede denominarse "Controles Descartados". Esto podrá ser de mucha utilidad para futuras auditorías, cuando se realicen nuevas revisiones del sistema considerado.

5.7.3 PREPARACION Y ENTREGA DEL INFORME FINAL

Cuando se hayan finalizado las reuniones para la discusión del informe preliminar, el auditor deberá elaborar todas las recomendaciones y correcciones necesarias que correspondan a:

- Controles descartados
- Precisión en la descripción y propósito del control
- Reclasificación del control
- Inclusión o exclusión de áreas con responsabilidad en el control

Cuando ya se hayan realizado las correcciones y modificaciones respectivas, se procederá a la elaboración del informe final que será presentado a la administración de la empresa.

El reporte de auditoría deberá repartirse a todos aquellos ejecutivos o técnicos que tengan algún interés en la auditoría realizada, dentro de los que se pueden mencionar: Presidente, Gerente General, Ejecutivo al cual reporta el área de auditoría, ejecutivo responsable por el área auditada, funcionarios de otras áreas con responsabilidad en la implantación de los controles.

5.7.4 COMPROMISOS

Es necesario que el auditor obtenga por escrito y de manera formal una respuesta al informe de auditoría. Dicha respuesta deberá ser analizada para determinar si cumple con los requisitos especificados. La respuesta deberá incluir:

- La forma en que se realizarán los controles y la corrección de las deficiencias.
- Una fecha estimada en la que se implementará el control.
- La respuesta deberá estar orientada a la solución global del problema y no limitarse a los aspectos específicos mencionados por el auditor.

5.7.5 RECOMENDACIONES

5.7.5.1 Generación de Informes de Seguimiento

Por lo general, de forma mensual, el departamento de auditoría deberá generar un reporte de seguimiento, el cual será enviado a las áreas encargadas de la implantación de los controles. En dicho informe se establecerán aquellos controles que a la fecha del informe deberían haber sido implantados pero aún no se ha recibido información alguna.

Para la respuesta al informe, el área involucrada podrá utilizar un formato preestablecido en el cual indique cual será la nueva fecha de implantación o la fecha real de implantación.

En base a las respuestas obtenidas, el auditor deberá planear la pruebas de auditoría que estime conveniente para los controles implantados e informará a la administración sobre aquellos casos relevantes o sobre los que aún no se han desarrollado acciones correctivas concretas.

5.7.5.2 Auditoría de los Controles Implantados

El auditor deberá planear las pruebas de acuerdo a las respuestas que se obtuvieron con los informes de seguimiento, para poder evidenciar la implantación de los controles y la funcionabilidad de los mismos.

Por razones de economía y practicidad es recomendable elaborar las pruebas cuando ya todos los controles han sido implantados, no obstante, dada la importancia de algunos controles, podría ser necesario el establecimiento de pruebas individuales.

El proyecto de auditoría no concluye con la presentación del informe de auditoría a la administración. Del seguimiento permanente que se haga sobre la implantación de las recomendaciones depende en alto grado el logro de los objetivos propuestos al inicio del proyecto.

5.7.6 PRESENTACION DE INFORMES DE AUDITORIA

Los reportes de auditoría presentan al auditor tres problemas. Primero, el reporte discute dos aspectos, la aplicación del usuario y el sistema de

procesamiento de datos, es decir, que los reportes de auditoría están dirigidos a dos tipos de audiencia. Segundo, el lenguaje de procesamiento de datos suele ser desconocido por el personal ajeno a ese departamento. Tercero, pocos auditores tienen los suficientes conocimientos de procesamiento de datos para desarrollar recomendaciones completas, entonces el auditor debe con frecuencia, defender una recomendación sin tener los suficientes conocimientos para ello.

Las quejas más comunes que se reciben de los reportes de auditoria son:

- Uso excesivo de lenguaje técnico: Debido al uso de este tipo de tecnisismos los reportes de auditoria se vuelven prácticamente incomprensibles para el personal ajeno al procesamiento de datos. Los reportes de auditoria son utilizados por ejecutivos responsables por la toma de decisiones y su tarea se vuelve más difícil si no alcanzan a entender la intensión de las recomendaciones plasmadas en el reporte.

- Recomendaciones y hallazgos demasiado generales: Por ejemplo, el reporte puede hacer alusión a debilidades en los controles de entrada, pero no detallar las áreas específicas en las que se encontraron las

debilidades. Este tipo de hallazgos son entonces difíciles de comprender y corregir. El reporte de auditoría debe ser específico cuando identifique áreas vulnerables en sistemas complejos.

- Omisión de efectos secundarios a las recomendaciones: Los cambios en cualquier parte de un sistema pueden ocasionar una serie de cambios en cascada a otros programas del sistema. El costo y esfuerzo de hacer un cambio de este tipo puede exceder los costos aparentes en un reporte de auditoría. Frecuentemente los costos exceden a los beneficios.

- Omisión de alternativas de menor costo: Muchas recomendaciones de auditoría suelen ser del tipo "Todo o Nada". Cuando se dan distintas alternativas para resolver algún problema, el departamento de procesamiento de datos puede buscar la solución más factible, sin embargo también puede rechazar una recomendación que no presente opciones.

Este tipo de reclamos acerca de los reportes de auditoría claramente señalan que los auditores de sistemas deben reevaluar los métodos para realizar un reporte así como su contenido.

TIPOS DE REPORTES DE AUDITORIA

Es tarea de un auditor identificar los tipos de reportes y las características de cada uno de ellos. La generalización de que todos los reportes de auditoría son idénticos conlleva a una serie de problemas para la aceptación de las recomendaciones.

Se han agrupado los tipos de auditoría en 5 sectores en lo que respecta a los reportes de auditoría:

- Auditoría de aplicaciones automatizadas
- Auditoría de desarrollo de sistemas
- Auditoría de post-instalación
- Auditoría de Centros de Computo
- Auditoría de procedimientos

El tipo de revisión que se realice afecta el estilo y propósito del reporte de auditoría. La revisión de una aplicación operacional está por ejemplo basada en hechos y este reporte de auditoría esta diseñado para identificar, cuantificar y corregir las debilidades en la aplicación. El reporte deberá ser entonces basado en hechos y puede ser directo al presentar

las severidad de un problema y la necesidad de una corrección. Por otro lado, en una auditoría de desarrollo de sistemas el auditor participa con el equipo en el desarrollo de soluciones de control. Este reporte de auditoría debe realizarse con el cuidado de incluir la participación de todos los miembros del equipo, para evitar romper las líneas de comunicación entre el analista de sistemas y el auditor.

Conferencia Preliminar

La conferencia preliminar es el área de pruebas para los reportes de auditoría. El auditor se enfrentan a dos grandes riesgos al realizar un reporte de auditoría, los cuales pueden ser minimizados a través de estas conferencias. El primer riesgo es información incorrecta, y el segundo es la negativa de el auditado a aceptar las recomendaciones.

El la conferencia preliminar antes de impresión del reporte, el auditor puede reducir significantemente la probabilidad de que estos eventos ocurran. Primero, el auditor debe preguntar específicamente al auditado si está de acuerdo con que la información presentada en el reporte es correcta. Segundo, el auditor puede identificar cuales recomendaciones no serán aceptadas por el auditado, si existiese alguna. Esto le da al auditor

dos oportunidades, auditor y auditado pueden comprometerse a una solución aceptable, o si el auditor cree extremadamente necesaria una recomendación, puede presentar alternativas para la implementación de la misma previas a la presentación del reporte a la Gerencia. Es raro que la Gerencia no acepte una recomendación de auditoría cuando ésta ha sido previamente aceptada por el auditado.

Elementos para un buen reporte de Auditoría

Existen cuatro lineamientos guías para la elaboración efectiva de reportes de auditoría, las cuales pueden ser aplicadas a cualquier tipo de reporte.

- Presentar hallazgos y recomendaciones explícitas. El auditor deberá realizar una investigación suficiente para asegurar que sus hallazgos y recomendaciones estén planteadas claramente para garantizar un entendimiento común entre auditor y auditado. El auditor podrá verse en la necesidad de consultar con los analistas de sistemas y programadores para describir con exactitud la solución planteada.

- Usar recomendaciones y hallazgos con bases firmes. El auditor debe sustanciar sus recomendaciones con suficiente evidencia; hallazgos no

sustanciales restan credibilidad. Una investigación cuidadosa es esencial para proveer seguridad en los hechos y recomendaciones de cualquier sistema; sin embargo este paso es usualmente innecesario.

- Desarrollar soluciones factibles. Los auditores deben recomendar soluciones de control solamente después de que la factibilidad de dichas soluciones ha sido verificadas. Las recomendaciones que no son factibles pueden ser replanteadas antes de ser presentadas. Muchas soluciones pueden ser inaceptables debido a que no se conocen su factibilidad. Estas podrían haber sido aceptadas si el costo de la corrección de esos problemas se hubiese conocido.

- Presentar recomendaciones aceptables. A pesar de que no todas las recomendaciones serán aceptables para el usuario, el grupo de auditoría que continuamente enfrenta rechazos podrá lograr su aceptación. Los auditores que realizan un buen trabajo podrán prevender sus recomendaciones al auditado y gozar de mayor credibilidad y aceptación. A pesar de que los auditores no deben de dejar de presentar recomendaciones valederas, no deberán insistir en la solución óptima si una solución aceptable será implementada por el auditado de forma inmediata.

A continuación se explican los tipos de reporte que pueden desarrollarse para los cinco tipos de auditoría mencionados anteriormente en este apartado.

Reportes de Auditoría para Aplicaciones Automatizadas

Auditar aplicaciones automatizadas es una de las principales tareas del auditor de PED, quien verifica la exactitud, integridad y autorización de las transacciones procesadas por la aplicación, así como los controles que gobiernan dicho proceso.

Esta auditoría puede involucrar tanto los segmentos manuales como los mecanizados de la aplicación. Algunas organizaciones limitan la auditoría del PED a los segmentos automatizados. Sin embargo, es una buena práctica auditar y reportar acerca de la integridad e ambos aspectos.

Aspectos del Reporte.

Este reporte abarca las actividades del usuario y la adecuación de los controles en una aplicación automatizada. Por lo mismo, el reporte es

dirigido al usuario y al equipo de mantenimiento de la aplicación y debe identificar claramente al personal responsable de los problemas encontrados.

Debido a que los cambios realizados en una aplicación operacional pueden costar significativamente más que realizar los mismos cambios a una aplicación en desarrollo, el método que se utilizará para realizar el cambio deberá ser explicado en el reporte de auditoría. Los reportes de auditoría pueden ser inefectivos si no se dedica el esfuerzo necesario para desarrollar soluciones económicamente prácticas.

Reporte de Auditoría para Desarrollo de Sistemas

La participación de la auditoría en el desarrollo de sistemas es una de las mejores utilizaciones del tiempo de auditoría debido a que los controles no implementados durante el desarrollo de sistemas podrían resultar poco económicos si se instalan después. El propósito de los reportes de auditoría para sistemas en desarrollo, resulta entonces predecible. El auditor estima la adecuación de los controles en un futuro, basado en la adecuación de los controles propuestos o parcialmente desarrollados al momento de la auditoría.

Aspectos del Reporte.

El reporte de auditoría para sistemas en desarrollo esta orientado primordialmente para el equipo de desarrollo de sistemas, para proveerles una asesoría de los controles que se están desarrollando para la aplicación. El reporte usualmente no recomienda controles adicionales sino más bien identifica áreas de debilidad, dejando el desarrollo de soluciones al equipo del proyecto.

Estos reportes deben ser generados inmediatamente después de la revisión. Mientras más temprano en el desarrollo de la aplicación se den las recomendaciones, más económicas y fáciles las soluciones.

Reportes de Auditoría Pos-Instalación

La auditoría post-instalación esta diseñada para verificar que se cumple con las especificaciones de la aplicación y del usuario. En esta oportunidad, la auditoría se realiza después que se implementa el sistema.

Aspectos del Reporte.

Este reporte esta diseñado para dar a los usuarios y administración una idea de como el sistema operacional cumple con las especificaciones y para identificar aquellas áreas que no cumplen. A pesar de que se puede reportar sobre otro tipo de problemas, el reporte debe concentrarse en el no cumplimiento de las especificaciones del sistema.

Reportes de Auditoría sobre el Centro de Cómputo

El centro de cómputo es responsable de la operación de la aplicación. Cabe aclarar que se debe entender por centro de cómputo no un solo cuarto con equipo sino más bien una red de instalaciones que se interconectan a través de un sistema de comunicaciones. Adicionalmente, el centro de cómputo suele ser el responsable de la seguridad de los datos.

Para cumplir con las responsabilidades del centro de cómputo, se deben establecer diferentes funciones. Estas pueden incluir, librería de datos,

programación y control de producción y contabilización del trabajo. La auditoría puede incluir cualquiera o todas estas actividades.

Aspectos del Reporte.

El reporte de auditoría sobre centros de cómputo revisa que se cumpla de forma efectiva los controles generales que gobiernan las operaciones de las computadoras. Los tópicos del reporte pueden variar desde aspectos no técnicos como el bienestar del usuario hasta aspectos técnicos como controles sobre la librería de programas.

Reportes de Auditoría sobre Procedimientos

El personal de sistemas y programación suele implementar procedimientos para las actividades de desarrollo y mantenimiento. Estos procedimientos usualmente son un combinación de estándares y lineamientos guía que aseguran la uniformidad del desarrollo de sistemas y facilitan el mantenimiento de los mismos.

Aspectos del Reporte.

El objetivo de este reporte es asesorar en cuanto a los estándares y lineamientos para el desarrollo de sistemas. Si existen debilidades en estos procedimientos, se obtiene como resultado sistemas inefectivos, poco económicos y con controles pobres. Este reporte esta dirigido a la administración del departamento de PED e identifica debilidades generales en los controles para que la administración pueda tomar las medidas correctivas que estime conveniente.

Las auditorías de procedimientos, evalúan incluso la administración del departamento de PED, por lo mismo, esta auditoría debe ser realizada por un auditor con suficiente experiencia y con el conocimiento necesario en ambos aspectos, desarrollo de sistemas y políticas y procedimientos de la organización.

CAPITULO 6

CONCLUSIONES - PARTE I

6. CONCLUSIONES PARTE I

i. La Auditoría de Sistemas es una disciplina relativamente nueva en el área de informática y definitivamente aún no se explota en su totalidad en El Salvador. Son escasas las empresas que realizan una verdadera Auditoría de Sistemas para optimizar sus recursos y obtener mejores resultados de sus Sistemas y Centros de Cómputo.

ii. Es necesario que se abran nuevas brechas en cuanto a la capacitación de profesionales en este campo de la Informática. Uno de los problemas más palpables es que la Auditoría de Sistemas está siendo realizada por personal no capacitado o con estudios insuficientes, lo que puede ocasionar más problemas que beneficios. Se debe aclarar que a pesar que la implantación de una Auditoría de Sistemas no es una solución barata, los resultados que se obtienen de ella justifican la inversión realizada. Por lo mismo, es necesario hacer un análisis a fondo de las necesidades de la organización antes de proceder a realizar una Auditoría de este tipo.

iii. A lo largo de la investigación, se ha podido observar que la forma más conveniente para realizar una Auditoría de Sistemas, es contar con un auditor interno a tiempo completo, quien se encargará de velar por que se cumplan

todos los requisitos establecidos para una Auditoría de este tipo. Como se explicó en el transcurso del documento, no existe una sola empresa que sea idéntica a otra, por lo que, los objetivos y metodologías variarán de una organización a otra, pero en concreto, la Auditoría será la herramienta de control más poderosa con que cuente una institución. Puede entonces visualizarse que los controles establecidos desde un principio resultan más efectivos y menos costosos que los implantados a un sistema en desarrollo, por ello resulta más provechoso contar con un Auditor Interno de planta.

iv. Es necesario concientizar a las organizaciones que realizan su trabajo diario ayudados por computadoras y sistemas, que la Auditoría de Sistemas se vuelve una práctica necesaria para poder lograr los objetivos que se planteen y obtener un máximo beneficio de la herramienta computarizada.

v. Como en cualquier otra disciplina, en la Auditoría de Sistemas es necesario contar con documentación suficiente que sirva de base o apoyo a los conocimientos técnicos que deben poseerse en el área. Por lo mismo se ha deseado que este documento llene algunos de los vacíos encontrados por todas aquellas personas que en un momento determinado se interesen en la materia. Se puede mencionar especialmente, a los alumnos de la Universidad Don Bosco, que carecen de la información necesaria para cursar esta materia.

PARTE II

UNA APLICACION PRACTICA EN EL AREA DE INFORMATICA

CAPITULO 7

INTRODUCCION - PARTE II

7. INTRODUCCION - PARTE II

Esta parte del documento se presenta como una continuación y una aplicación práctica al trabajo elaborado anteriormente y titulado "Guía General para la Elaboración de una Auditoría de Sistemas".

En éste se incluyen un pequeño instructivo, una serie de cuestionarios y un Informe final de Auditoría en los que está recopilado la investigación de campo realizada en el área de Informática de la Universidad Don Bosco.

Solamente como aspecto interesante, se incluye en esta introducción una breve reseña histórica del desarrollo del Centro de Cómputo de la Universidad Don Bosco.

La Universidad fue creada jurídicamente en el año de 1984, pero no dio inicio a sus labores académicas sino hasta el año de 1986. Sus primeras instalaciones fueron en lo que es actualmente la Escuela Domingo Savio con 7 carreras profesionales en su pensum y un aproximado de 400 alumnos.

Hasta el siguiente año, 1987, la UDB incluye en su Facultad de Ingeniería la carrera de computación sin contar todavía con ningún equipo para organizar su

centro de cómputo. Conforme se fue incrementado la población estudiantil y las necesidades fueron siendo mayores, se adquirió un sistema Mainframe de IBM, modelo 9370, el cual fue donado parcialmente por una Congregación Salesiana de los Estados Unidos. Este equipo fue puesto en funcionamiento en el año de 1988 habiéndose trasladado de la Domingo Savio a Don Rua.

Para el año siguiente, las instalaciones fueron insuficientes y la Universidad Don Bosco se vio obligada a trasladarse al Instituto Técnico Ricaldone (ITR), donde impartían todas las carreras de la facultad de Ingeniería. A pesar de ello, el IBM 9370 permanecía en Don Rua y era utilizado únicamente para uso administrativo. Para ese año, la Universidad hacía uso del centro de cómputo del ITR para impartir sus clases y realizar los laboratorios.

En 1990, el IBM 9370 fue trasladado de Don Rua al Centro de Cómputo del ITR. Finalmente, en 1992, la Universidad se traslado al campus en la Ciudadela Don Bosco y el IBM 9370 (único equipo propiedad de la Universidad) fue llevado a una ubicación temporal en las oficinas administrativas de la Ciudadela Don Bosco donde se mantuvo hasta que fue construido el edificio de talleres en el que esta ubicado actualmente.

Por un período de aproximadamente 6 meses, la Universidad hizo uso del centro de cómputo del Colegio Don Bosco ubicado dentro de la Ciudadela, pero

a mediados de 1993, cuando el edificio de talleres fue concluido, el CITT instaló y organizó el centro de cómputo en el que se trabaja actualmente.

De esa manera ha quedado configurado el Centro de Cómputo de la Universidad Don Bosco y bajo esa estructura se ha realizado la presente investigación, previendo que aún pueden existir cambios en un futuro no muy lejano que afecten circunstancialmente la estructura y organización de lo que es el Area de Informática de la UDB.

CAPITULO 8

OBJETIVOS - PARTE II

8. OBJETIVOS - PARTE II

8.1 OBJETIVO GENERAL

Presentar a la Administración de la Institución con una herramienta útil para la correcta y oportuna toma de decisiones a través de un análisis a fondo de la situación actual de su área de informática, con el único propósito de hacer de ésta una dependencia más eficiente.

8.2 OBJETIVOS ESPECIFICOS

1. Establecer si el área de informática de la institución o empresa esta funcionado de acuerdo a las políticas establecidas y conforme a las normas fijadas por la alta gerencia.
2. Determinar si existe una estructura orgánica funcional que permita a la institución o empresa desempeñarse con el mínimo de obstrucciones.
3. Verificar si la situación del personal del área o departamento es idónea conforme a las tareas que se realizan en el mismo.
4. Evaluar la sección de presupuestos del área de informática.
5. Conocer el ambiente de trabajo bajo el cual se desarrollan las actividades del área de Informática.

6. Examinar el grado de seguridad con que se trabaja en el área.

7. Evaluar la eficacia y eficiencia con que trabaja el centro de cómputo.

CAPITULO 9

INSTRUCTIVO Y MANUALES

9. INSTRUCTIVO Y MANUALES

El siguiente manual está diseñado con el único propósito de poder obtener la mayor cantidad de información posible concerniente al área de informática. Es necesario que al momento de realizar la auditoría, se escuchen las reacciones de los auditados, pues de ellas podrá obtenerse información que no se refleja en los cuestionarios.

Es necesario realizar todas y cada una de las preguntas con la mayor objetividad posible dejando el menor número de dudas sin aclarar y teniendo en cuenta que el Auditor no debe perder nunca su independencia.

Para poder entender mejor el manejo de este manual, se explica a continuación cada uno de los pasos que deben seguirse para poder llevar a cabo la auditoria:

1- Realizar cada una de las preguntas y al mismo tiempo colocar en la casilla S/N (Si o No) si se cumple ó no con lo que se está expresando, en caso de que la pregunta no aplique, podrá colocarse NA.

2- Comentarios: En este campo, se dará una ampliación sobre lo observado en cada pregunta realizada, lográndose con esto una mejor comprensión

del área que se esta evaluando, lo que ayudara a dar las recomendaciones del caso.

3- Riesgo: En esta casilla deberá clasificarse el riesgo al que se ve expuesto el área de informática con el problema detectado, de la siguiente manera:

A Alto
M Medio
B Bajo

Se considerará un riesgo Alto cuando la consecuencia de su ocurrencia afecte directamente el funcionamiento normal del Centro de Cómputo y se necesite resolver en el menor tiempo posible, o si la ocurrencia del mismo ocasione una gran pérdida para la institución.

Un riesgo medio será aquel que su ocurrencia entorpezca el funcionamiento del Centro de Cómputo, pero permita seguir trabajando y exista la necesidad de proporcionar una solución a corto o mediano plazo.

Se tomará como un riesgo bajo todo el que no interrumpa ni altere el funcionamiento del centro de cómputo pero que para un mejor desempeño del mismo sería recomendable darle solución.

De esta manera, la administración y el área auditada podrá priorizar los problemas, atendiendo de manera más inmediata, aquellos que representen riesgo alto.

A continuación se presenta una lista de los tipos de riesgos que pueden encontrarse en una Auditoría de Sistemas.

1. Fraude - Desfalco
2. Pérdida - Extravío
3. Robo - Hurto
4. Interrupciones
5. Daños - Destrucción
6. Multas - Sanciones
7. Ineficiencia
8. Mala o inexistente Estructura Organizativa y Procedimientos
9. Perdida de Continuidad de Operaciones

Se recomienda que al momento de realizar los cuestionarios, se haga de manera individual y con el Auditor realizando las preguntas, pues es de suma importancia analizar la reacción del auditado al momento de responder a las mismas. Es una buena práctica, grabar en un tocacintas el cuestionario

realizado para evitar la omisión de comentarios importantes al momento de hacer el análisis.

En el siguiente capítulo se presentan los cuestionarios diseñados para realizar la auditoría. Se ha tratado de cubrir la mayor parte de aspectos que pueden ser auditados al momento de examinar un departamento de informática. Sin embargo, existe la posibilidad que para situaciones específicas sea necesario incluir otros puntos que no se han incluido en estos cuestionarios, para lo que el Auditor deberá utilizar su criterio al momento de realizar el estudio.

Los cuestionarios se presentan con la información recopilada al realizar la Auditoría en el Area de Informática de la Universidad Don Bosco, información que fue utilizada para realizar el análisis respectivo y presentar el informe que se incluye en un capítulo más adelante.

MANUALES

MANUAL DE AUDITORIA DE SISTEMAS

DEPARTAMENTO : INFORMATICA
AREA : ORGANIZACION
SECCION : ESTRUCTURA ORGANIZATIVA

EMPRESA AUDITORA :
AUDITOR :
FECHA :

Nº	Pregunta	S/N	Comentario	Riesgos
	ORGANIZACION			
0-1	Existe un Manual de Organización con su respectivo organigrama?	N	Se tienen planes para la elaboración de uno.	M
0-2	Contiene el Manual la descripción de todos los puestos existentes en el área?	NA		M
0-3	Es clara y objetiva la descripción de los puestos de tal manera que se eliminen posibles dudas, dualidades o duplicidad de funciones?	NA	Se tiene una idea informal de la obligaciones de cada puesto de trabajo a pesar de que solo son 2.	M
0-4	Comparar las descripciones de puestos con las responsabilidades actuales y determinar su exactitud.	NA	Pocas personas realizan multiples tareas.	B
0-5	Evaluar si la estructura actual esta encaminada a la consecución de los objetivos del área.	NA	No se tiene una estructura definida.	M
0-6	Se considera adecuados los departamentos en que está dividida el área?	N	No hay diferentes departamentos.	B
0-7	Esta delimitada la responsabilidad de cada departamento o subdepartamento?	NA		M
0-8	Estan bien definidos los niveles jerárquicos?	N	Si se siguen algunas líneas de jerarquía.	M
0-9	Permiten estos niveles una adecuada comunicación ascendete y descendente?	S	A pesar de no existir división formal, se respeta una línea vertical de comunicación	
0-10	Es suficiente la cantidad de personal asignado al área?	N	Solamente hay 2 personas encargadas	A
0-11	Existen conflictos debido a la carga de trabajo?	S	No se logra realizar en el tiempo óptimo las tareas asignadas al personal.	A
0-12	Se detiene alguna actividad por falta de personal?	S		A
0-13	Se han establecido funciones del área y estan debidamente documentadas y autorizadas?	N	No existe documentación organizativa de ningún tipo.	M

MANUAL DE AUDITORIA DE SISTEMAS

DEPARTAMENTO : INFORMATICA
AREA : ORGANIZACION
SECCION : ESTRUCTURA ORGANIZATIVA

EMPRESA AUDITORA :
AUDITOR :
FECHA :

0-14	Evaluar si las funciones estan adecuadas a la realidad.	NA	Debido a la falta de documentos, se realizan algunas actividades fuera de las funciones del personal	M
0-15	Se cumplen a cabalidad las funciones establecidas?	NA		M
0-16	Se requiere de la participación de otras áreas para el cumplimiento de las funciones?	NA		M
0-17	Existe algún encargado de velar por el cumplimiento de las funciones?	S	Si existe un encargado, pero éste no verifica continuamente ese cumplimiento	
0-18	En caso de estar ausente el supervisor existe otro encargado de velar por el cumplimiento de funciones?	N	Hasta el momento no ha existido la necesidad	A
0-19	Se han establecido objetivos del área y estan debidamente documentados y autorizados?	N	Existe un vago conocimiento de los objetivos que se miden a traves del cumplimiento de resultados	M
0-20	Existe un método adecuado para dar a conocer los objetivos?	N		M
0-21	Estan los objetivos establecidos deacuerdo con las funciones del área?	NA		M
0-22	Se verifican los objetivos y son estos actualizados.	NA		M
0-23	Participa cada departamento en el establecimiento de sus objetivos y en la actualización de los mismos?	NA		B
0-24	Se verifica el cumplimiento de los objetivos y se cuenta con un mecanismo adecuado para medir en que forma se estan cumpliendo?	S	Nuevamente, existen evaluaciones periódicas en base a resultados obtenidos en un período, sin existir objetivos específicos establecidos.	

MANUAL DE AUDITORIA DE SISTEMAS

DEPARTAMENTO : INFORMATICA
AREA : ORGANIZACION
SECCION : ESTRUCTURA ORGANIZATIVA

EMPRESA AUDITORA :
AUDITOR :
FECHA :

0-25	Existe el establecimiento de plazos para el cumplimiento de los objetivos (corto, mediano y largo plazo)?	N	No de manera formal.	M
0-26	Existe un analisis organizacional del área de informática?	N	Se confunden los aspectos organizacionales de los 2 centros de computo que son en realidad uno solo.	B
0-27	Se ha establecido para cada puesto que características debe llenar el aplicante?	N	Conforme existe una necesidad, se establecen las características.	A
0-28	Se verifica la competitividad del personal asignado a cada puesto?	N		A
0-29	Es adecuado el "nombre" asignado a cada puesto (programador, analista, etc.)	NA	No existen este tipo de divisiones en el personal existente.	B
0-30	Existen otro tipo de manuales especificos que afecten el funcionamiento de la organización (procedimientos, normas, políticas, instructivos)	N	No existe ningún tipo de manual organizativo.	M
	RECURSOS HUMANOS			
0-31	Se cuenta con una metodología definida para la selección del personal en cuanto a cantidad, experiencia, etc.?	N	La selección del personal es hecha por los directores de la institución, no por el departamento interesado.	A
0-32	Verificar la existencia de mecanismos para la medición de la eficiencia del personal.	N	La miden a través de la consecución de resultados.	M
0-33	Existe rotación dentro del personal interno en el área de sistemas?	N	De ningún tipo.	B
0-34	Se evalua la puntualidad, faltas y ausentismos?	S	Existe un marcador de tarjeta	
0-35	Existen políticas dentro del área que permitan las promociones y ascensos?	N		B

MANUAL DE AUDITORIA DE SISTEMAS

DEPARTAMENTO : INFORMATICA
AREA : ORGANIZACION
SECCION : ESTRUCTURA ORGANIZATIVA

EMPRESA AUDITORA :
AUDITOR :
FECHA :

0-36	Tiene la institución programas de capacitación para todo el personal (desde los operadores hasta los puestos directivos)?	N	Si se mencionó planes de capacitación, pero no se llevan a cabo. La capacitación es unicamente para programas desarrollados internamente.	M
0-37	Asegurar que los empleados de nuevo ingreso esten concientes de los objetivos de la organización.	N		M
0-38	Se verifica que la capacitación del personal surta el efecto deseado en el desarrollo de sus funciones?	N	Nuevamente, la verificación de resultados.	M
0-39	Existe alguien encargado de supervisar o controlar el desempeño del personal?	S	Usualmente los directores. No hay supervisores de nivel intermedio.	
0-40	Evaluar las relaciones laborales entre el personal y la dirección.	S		
0-41	Existen medios para comunicar las insatisfacciones del personal?	S	No se da mucho este caso por temor a las consecuencias.	M
0-42	Cuenta la dirección con algún plan para resolver situaciones laborales?	N	Despido	M
0-43	Como se enfrentan los despidos o reemplazo del personal?		Varía según el caso.	M
0-44	Evaluar las remuneraciones del personal.		Hasta hace poco, se ha empezado a evaluar un sistema de escalafones. Pero aún no se ha puesto en marcha.	M
0-45	Son las remuneraciones adecuadas en cuanto a capacidad, experiencia, carga de trabajo?	N		M
0-46	Se cuenta con remuneraciones competitivas en comparación a otros puestos similares en el medio?	N		M
0-47	Evaluar el ambiente de trabajo.		Se desenvuelve sin ninguna anormalidad.	

MANUAL DE AUDITORIA DE SISTEMAS

DEPARTAMENTO : INFORMATICA
AREA : ORGANIZACION
SECCION : ESTRUCTURA ORGANIZATIVA

EMPRESA AUDITORA :
AUDITOR :
FECHA :

0-48	Se cuenta con instalaciones comodas y adecuadas para el desarrollo de las tareas?	N		M
0-49	Se tiene un mobiliario adecuado para el equipo utilizado?	N		M
0-50	Existen buenas instalaciones de comunicación?	S		
0-51	El espacio utilizado para el área de informática es el suficiente y esta separado de las demás áreas de la institución o empresa?	N	El área no se adapta para el tamaño del centro de cómputo. El área se comparte con otros talleres.	A
0-52	Revisar las condiciones adicionales de trabajo como beneficios, prestaciones, motivación, etc.	N	No existe ningun tipo de beneficios adicionales.	M
0-53	Existen políticas de motivación para los empleados?	N		M
0-54	Existen prestaciones de tipo motivacional (seguros, vacaciones, bonificaciones en efectivo)?	N		M
0-55	Determinar en base a que se otorgan las bonificaciones y motivaciones.	NA		M
0-56	Revisar si se cuenta con contratos estandares para la adquisición de nuevo personal.	S		M
0-57	Se cuenta con formas de organizar el trabajo?	N		B
0-58	Se preveen las necesidades del personal con anterioridad?	N		B
0-59	Se cuenta con planes de sustitución del personal clave?	NA	De hecho, si falta el encargado, sería una verdadera catastrofe.	A
0-60	Se realizan reuniones de trabajo entre el personal y los supervisores?	S	Con alguna frecuencia.	
0-61	Esta el personal concientizado a trabajar como un equipo y no de forma individual?	S		B
0-62	Existen empleados sobreutilizados o subutilizados?	S		M

MANUAL DE AUDITORIA DE SISTEMAS

DEPARTAMENTO : INFORMATICA
AREA : ORGANIZACION
SECCION : ESTRUCTURA ORGANIZATIVA

EMPRESA AUDITORA :
AUDITOR :
FECHA :

0-63	Se han elaborado planes de trabajo con tiempos definidos?	N		M
	PRESUPUESTOS			
0-64	Se realizán presupuestos relacionados con el área de informática?	S	No siempre los realiza la persona adecuada.	B
0-65	Existe un control de los gastos aproximados que se invierten en el área de informática para algún determinado período?	S	No es realizado por personal de informática.	
0-66	Se cuenta con el equipo y mobiliario adecuados y en cantidad suficiente para desarrollar el trabajo?	N		M
0-67	Se dejan de realizar actividades por falta de material y equipo?	N		M
0-68	Se cuenta con un inventario del equipo existente y tiene este su valor actualizado en cuanto a su depreciación?	S	Esto es realizado por el departamento administrativo.	
0-69	Se cuenta con contratos de mantenimiento para el equipo y mobiliario?	S	Con IBM. Mantenimiento Correctivo.	
0-70	Como se maneja la aparición de una necesidad de equipo o material?		Conforme aparece la necesidad se improvisa la satisfacción de la misma.	M
0-71	Que se hace con el equipo en desuso u obsoleto?		Hasta ahora, todo el equipo es utilizado al máximo.	B
0-72	Con que frecuencia se renueva el equipo y mobiliario?	N	No con la frecuencia debida.	M
0-73	A la hora de realizar los presupuestos se toma en cuenta aspectos como software, accesorios, papelería y salarios del personal, capacitaciones?	S	Nuevamente, la persona encargada de esto, es alguien ajeno a informática.	M
0-74	Quien es el encargado de verificar la calidad de los equipos y mobiliarios utilizados?		La persona responsable de cada centro de computo.	

MANUAL DE AUDITORIA DE SISTEMAS

DEPARTAMENTO : INFORMATICA
AREA : ORGANIZACION
SECCION : ESTRUCTURA ORGANIZATIVA

EMPRESA AUDITORA :
AUDITOR :
FECHA :

0-75	Cuenta la institución o empresa con normas establecidas para el control de calidad?	NA		M
0-76	Han surgido problemas por la falta de este tipo de controles?	S	Trabajo doble o duplicidad de tareas.	M
0-77	Existe un programa sobre los servicios generales que requiere el área?	N		B
0-78	Se incluyen dentro de estos servicios los servicios externos a la institución?	NA		B
0-79	Cuenta el área con suficientes recursos financieros para lograr su funcionamiento de forma eficiente?	S	Hasta la fecha no ha habido ninguna necesidad que no sea satisfecha.	
0-80	Quien es el encargado de asignar estos recursos?		Personal de Administración	M
0-81	Es este encargado constantemente informado de los recursos necesitados por el área?	N	Se actualiza conforme surgen las necesidades.	M
0-82	Se hacen analisis de tipo costo/beneficio en cuanto a la adquisición de equipo?	S	Todo equipo debe ser auto financiable para ser adquirido.	
0-83	En relación al costo, se analiza si el software necesitado debe ser comprado o puede ser desarrollado en la institución o empresa?	N	Las decisiones se toman, en algunas oportunidades, fuera del área de informática.	M
0-84	Cuando se adquiere software, se compra a sus distribuidores?	N		A
0-85	Se toma en cuenta dentro de los presupuestos del área la adquisición de seguros?	N		A
0-86	Se lleva un control de los activos del área de informática?	S		
0-87	Existe una persona encargada de controlar la entrada a los accesorios, papelería, etc.?	S	En librería.	
0-88	Se establecen controles para los puntos de pedido?	N		M

MANUAL DE AUDITORIA DE SISTEMAS

DEPARTAMENTO : INFORMATICA
AREA : SEGURIDAD
SECCION : SEGURIDAD LOGICA

EMPRESA AUDITORA :
AUDITOR :
FECHA :

Nº	Pregunta	S/N	Comentario	Riesgos
L-1	Existen medidas de seguridad para proteger la información de la institución o empresa contra cualquier tipo de pérdidas?	S	Aunque no son claras ni las más adecuadas.	M
L-2	Esta clasificada la información de la institución conforme a su importancia? (Desde información poco relevante hasta información confidencial)	S	Pero no lo conoce todo el personal.	A
L-3	Se han asignado responsabilidades en cuanto al manejo de la información?	N	No se cuenta con medidas que sirvan para proteger el manejo de información.	A
L-4	Existe un encargado de velar por la seguridad de la información?	N		A
L-5	Se tienen niveles de acceso a la información?	S	Pero no son bien establecidos	M
L-6	Se controla la generación de reportes de acuerdo a las necesidades de los mismos y al destinatario de la información?	N		A
L-7	Existen métodos adecuados de distribución de la información?	N		M
L-8	Se han diseñado procedimientos para la asignación de claves de acceso (password)?	S	Todo lo que se refiere a claves de acceso (password), va dirigido solamente al Centro de Cómputo de la UDB.	
L-9	Se hacen cambios periódicos en los passwords asignados?	N		M
L-10	Se cuenta con un sistema que informe los intentos fraudulentos de adivinar un password?	N		B
L-11	Cuando se asigna un password, se controla la correcta utilización de este y se elimina cuando ya no es necesario?	S		

MANUAL DE AUDITORIA DE SISTEMAS

DEPARTAMENTO : INFORMATICA
AREA : SEGURIDAD
SECCION : SEGURIDAD LOGICA

EMPRESA AUDITORA :
AUDITOR :
FECHA :

L-12	Se restringe el acceso dentro del sistema a programas y archivos solamente a personal autorizado?	S		
L-13	Están protegidos estos programas y archivos contra copias no autorizadas?	S		
L-14	Cuando se reciben archivos nuevos, se prueban para detectar defectos en el almacenamiento?	N	Si no se utilizan en el momento, se almacenan hasta que se necesiten.	M
L-15	Se tiene una lista actualizada de todos los sistemas operativos, paquetes, programas, etc., indicando el número del programa y su nombre?	N		M
L-16	Existen políticas establecidas para controlar la utilización de programas piratas?	N	Después de la primer semana de estar en funcionamiento, todas las máquinas tenían virus. Esto ocurrió en el Centro de Cómputo del CITT.	A
L-17	Se controla el contenido de las computadoras para verificar la no existencia de tales programas?	N		A
L-18	Existe un encargado de verificar que las computadoras no estén saturadas de programas innecesarios como juegos u otros paquetes de esta índole?	N		A
L-19	Se cuenta con programas antivirus?	S	Pero no están actualizados.	A
L-20	Existen métodos para evitar la contaminación de equipo con estos "programas"?	N		A
L-21	En caso de infección, existen métodos establecidos para contrarrestar tal situación?	N		A

MANUAL DE AUDITORIA DE SISTEMAS

DEPARTAMENTO : INFORMATICA
AREA : SEGURIDAD
SECCION : SEGURIDAD DE PERSONAL

EMPRESA AUDITORA :
AUDITOR :
FECHA :

Nº	Pregunta	S/N	Comentario	Riesgos
P-1	Existen métodos para comprobar la confiabilidad del personal?	N	Nunca se han realizado pruebas para determinar la confiabilidad del personal.	A
P-2	Cuando se detecta una fuga de información, se siguen procedimientos para detectar la fuente.	S		
P-3	Existe una metodología para garantizar el trabajo realizado por el personal?	N	No se tiene un supervisor encargado de velar por que el personal cumpla con sus obligaciones. Solamente utilizan como medida el cumplimiento de objetivos.	B
P-4	Se realizan exámenes constantes para verificar la capacidad del personal, especialmente cuando existe capacitación?	N	No se realiza ningún tipo de pruebas.	B
P-5	Se compromete de alguna manera al personal antes de brindarle capacitación.	N/A	No se da ningún tipo de capacitación.	
P-6	Se garantiza que la capacitación al personal sea aprovechada por la institución.	N/A		
P-7	El personal de informática que haya sido despedido por la institución, se retira de inmediato?	S		
P-8	A los empleados despedidos por la institución se les elimina su clave de seguridad antes de ser informados de su retiro.	N/A	No existen operadores para ningún centro de cómputo con clave asignada.	
P-9	En caso de faltar alguna de las personas claves del centro de cómputo, existe alguien más que este capacitado para sustituirle?	N	Todo el trabajo del centro de cómputo de la UDB está centralizado en una sola persona, no existen substitutos. Para el CITT existen dos encargados, en caso de faltar ambos, la persona sustituta no está capacitada para esa labor.	A

MANUAL DE AUDITORIA DE SISTEMAS

DEPARTAMENTO : INFORMATICA
AREA : SEGURIDAD
SECCION : SEGURIDAD FISICA

EMPRESA AUDITORA :
AUDITOR :
FECHA : Noviembre, 1994.

No.	Contenido de la Pregunta	S/N	Comentarios	Riesgo
	EDIFICIOS Y CONSTRUCCION			
F-1	Está ubicado el centro de cómputo en un edificio sólido y a prueba de incendios?	N	El edificio tiene bases sólidas pero tiene una serie de riesgos que pueden evitarse.	M
F-2	Están fabricadas con materiales no combustibles los accesorios del centro de cómputo (cortinas, tapetes u otros elementos decorativos)?	N	Existen divisiones de plywood que son extremadamente flamables al igual que el poliestireno que ha utilizado para cubrir las ventanas y el cielo falso.	A
F-3	Están las ventanas del centro de computo fabricadas con vidrio de seguridad y cierran éstas herméticamente?	N	Es vidrio normal y no sellan herméticamente	M
F-4	Son las paredes adyacentes inmediatas a los archivos o al equipo de ladrillo u otro material sólido que impida la penetración a la sala de computadoras fácilmente?	N	Existen algunas paredes de plywood que pueden ser fácilmente alteradas.	M
F-5	Verificar que los techos son a prueba de agua de manera que esta no fluya a los pisos.	N	No se ha dado el caso pero en caso de existir un rompimiento en el techo superior, el agua se filtraría sin ningún problema.	A
	UBICACION DEL AREA DE COMPUTO			
F-6	Está el centro de cómputo separado físicamente de las demás áreas de la organización?	N	Tiene otros talleres adyacentes. Uno de ellos incluso dentro del mismo centro de cómputo.	A
F-7	Verificar que el centro de cómputo esté en un área interna, sin tener acceso directo a la calle o a edificios vecinos.	N	El edificio tiene un pasillo exterior que colinda con la calle y otros edificios.	A

MANUAL DE AUDITORIA DE SISTEMAS

DEPARTAMENTO : INFORMATICA
AREA : SEGURIDAD
SECCION : SEGURIDAD FISICA

EMPRESA AUDITORA :
AUDITOR :
FECHA : Noviembre, 1994.

F-8	Se encuentra fuera de la visibilidad del público el centro de cómputo y el área de almacenamiento de copias de respaldo y otros accesorios?	S		
F-9	Verificar que la distribución física de áreas evita que el centro de computo sea área de tránsito para otras oficinas?	N	Como ya se mencionó, existe un taller ajeno al centro de cómputo dentro de este mismo, lo que obliga a tener circulación innecesaria y de personal ajeno al centro.	M
F-10	Está la biblioteca de cintas y discos separada de la sala de computadores?	S		
F-11	Existe un área de almacenamiento de papelería y accesorios separada del centro de cómputo?	S	A pesar de que los accesorios se mantienen en otro departamento, no se cuenta con el mobiliario necesario para la ubicación de papelería, útiles y otros implementos que se necesitan.	M
F-12	Verificar que el cuarto ó sala de máquinas para los equipos de potencia es externo al salón de computadoras.	N/A	No existen equipos de potencia, no existe cuarto de máquinas.	
	ACCESOS			
F-13	Se mantienen libres de obstáculos los corredores, pasillos y áreas alrededor del centro de cómputo?	N	Debido a las limitaciones de espacio, se pueden observar mesas u otro tipo de mobiliario que entorpece la circulación.	B
F-14	Verificar que solo exista una puerta de entrada y salida que sea usada por el personal de operación y visitantes al centro de cómputo.	S	Si se cuenta con una sola puerta de entrada/salida, pero también existe otra puerta que da al pasillo del exterior del edificio y que es utilizada por el taller de electrónica, por donde es posible ingresar al centro de cómputo.	A

MANUAL DE AUDITORIA DE SISTEMAS

DEPARTAMENTO : INFORMATICA
AREA : SEGURIDAD
SECCION : SEGURIDAD FISICA

EMPRESA AUDITORA :
AUDITOR :
FECHA : Noviembre, 1994.

F-15	Se cuenta con controles de acceso al área de informática?	N	No se tiene ningún tipo de control	A
F-16	Existe más de una persona encargada de abrir el centro de computo (con llave de acceso)?	S		M
F-17	Están las puertas de entrada al centro de cómputo cerradas todo el tiempo y controladas por un mecanismo de cierre?	N	Por el contrario, la puerta de cómputo siempre permanece abierta.	M
F-18	Verificar si se utiliza un sistema de control e identificación con carnés tanto para personal como para visitantes.	N		M
F-19	Existen en el departamento puertas para salida de emergencia?	N		A
F-20	Están estas puertas debidamente identificadas y visibles?	N		A
F-21	Es eficiente el patrón de tráfico en el área circundante del centro de cómputo en términos de entradas y salidas en caso de una emergencia?	N	Si fuese necesario un desalojo, se corre el peligro de accidentes innecesarios debido a que solamente se utiliza una puerta y unas escaleras, lo que definitivamente causaría una aglomeración de personas.	M
F-22	Cuenta el personal de la organización con algún tipo de identificación para poder circular libremente en el departamento de cómputo?	N		M
F-23	Existen personas encargadas de acompañar a los visitantes dentro del centro de cómputo?	N	Cuando los visitantes son oficiales, si llevan a una persona de la Universidad con ellos, pero en caso contrario, cualquiera puede "visitar" el centro de cómputo.	M

MANUAL DE AUDITORIA DE SISTEMAS

DEPARTAMENTO : INFORMATICA
AREA : SEGURIDAD
SECCION : SEGURIDAD FISICA

EMPRESA AUDITORA :
AUDITOR :
FECHA : Noviembre, 1994.

F-24	Está prohibido el ingreso de paquetes, portafolios y bolsas de mano dentro de las áreas más sensitivas del centro de computo?	N	Cualquier usuario del centro de cómputo puede ingresar llevando consigo cualquier tipo de paquete, maletín, etc.	A
	INSTALACIONES ELECTRICAS			
F-25	Verificar que toda la instalación eléctrica donde se conecte equipo de informática u otro equipo sensible, esté debidamente polarizada.	S		
F-26	Está ubicado el interruptor principal de tal forma que pueda desconectarse el equipo y el aire acondicionado en caso de una emergencia?	S		
F-27	Está la instalación eléctrica del centro de cómputo separada por un tablero propio de las demás áreas de la organización?	S		
F-28	Están protegidos todos los circuitos del centro de computo del vandalismo? (Esto implica proveer de cerraduras para los tableros de control)	N	Los tableros están al alcance de cualquier persona.	A
F-29	Verificar que se encuentran marcados apropiadamente los circuitos del tablero de manera que si se le da servicio al equipo permita una referencia rápida.	S		
F-30	Están protegidas contra agua las instalaciones eléctricas?	N	Existen instalaciones "regadas" dentro del centro que corren el riesgo de humedecerse en caso de filtración de agua.	A
F-31	Cuenta el centro de computo, en caso de falta de energía, con su propia fuente de poder (planta eléctrica)?	N		A

MANUAL DE AUDITORIA DE SISTEMAS

DEPARTAMENTO : INFORMATICA
AREA : SEGURIDAD
SECCION : SEGURIDAD FISICA

EMPRESA AUDITORA :
AUDITOR :
FECHA : Noviembre, 1994.

F-32	Verificar que la distribución de cables de energía eléctrica este fuera de la circulación del personal?	N	Existen cables que están ubicados dentro del paso de los usuarios y demás personas.	A
F-33	Asegurar que los cables estén debidamente identificados.	N	Están tan mal distribuidos que es imposible identificar a que equipo pertenecen los cables.	M
F-34	Cuenta el centro de computo de luces de emergencia accionadas por baterías?	N	Cuando existe un corte de energía quedan completamente a oscuras.	B
	PROTECCION CONTRA INUNDACION			
F-35	Existe en el área de informática el riesgo de inundación ya sea por tuberías u otros desastres naturales?	S	Existen filtraciones de agua por las rendijas de las puertas que dan al pasillo exterior del edificio. A pesar de haberse suscitado dicho incidente, aún no se hace nada por resolver la situación.	A
F-36	Verificar si existen facilidades de drenaje de agua bajo el piso para proteger el equipo?	N	Cuando existe filtración de agua, ésta queda empozada dentro del centro.	M
F-37	Existen tanques de agua elevados ubicados por encima del cielo del centro de cómputo?	N		
	PROTECCION CONTRA INCENDIOS			
F-38	Existen mecanismos para controlar incendios como extingidores o irrigadores aéreos?	N	No se cuenta con ningún dispositivo para combatir el fuego en caso de un accidente.	A
F-39	Se remueven inmediatamente las acumulaciones de material inflamable ubicadas en el centro de cómputo o en las área circundantes?	N	Se pudo observar acumulación de papeles y otros materiales.	A
F-40	Se tienen detectores de calor o detectores de humo?	N		M
F-41	Están los extiguidores de fuego accesibles a los usuarios y provistos de marcos indicadores?	N/A		

MANUAL DE AUDITORIA DE SISTEMAS

DEPARTAMENTO : INFORMATICA
AREA : SEGURIDAD
SECCION : SEGURIDAD FISICA

EMPRESA AUDITORA :
AUDITOR :
FECHA : Noviembre, 1994.

F-42	Están todos los extinguidores en condiciones operativas y se inspeccionan periódicamente?	N/A		
F-43	Hay equipo en la sala de cómputo que represente riesgos de incendio innecesarios? (cafeteras, microondas, etc.)	S	El taller de electrónica cuenta con equipo que puede ser propenso a incendio y debido a que está ubicado dentro del centro de cómputo, éste también corre el riesgo.	A
F-44	Está la biblioteca debidamente protegida contra incendio, inundaciones u otro tipo de contingencias?	N/A		
	AIRE ACONDICIONADO			
F-45	Tiene la sala de computadores su propio sistema de aire acondicionado separado?	S		
F-46	Es el sistema de aire acondicionado el adecuado?	S	Si se cuenta con el equipo suficiente de aire acondicionado, pero las instalaciones no son las más indicadas.	
F-47	Se revisan los requerimientos de aire acondicionado cuando se instalan nuevos equipos?	N		B
F-48	Se cuenta con extractores de aire que evacuen el aire caliente o viciado que se acumula en el cielo del centro de cómputo?	N	No existe ningún sistema de escape que expulse el aire que se acumula en la parte superior del centro de cómputo.	B
F-49	Existe el área de computo un medio ambiente de temperatura y humedad controlada?	S		
F-50	Se tiene un plan de mantenimiento y chequeo periódico del equipo de aire acondicionado?	S		
	SEGUROS			
F-51	Cuenta la Organización con un plan de seguros que cubra cualquier tipo de daños ya sea este hardware o software?	N	La institución no cuenta con ningún plan de seguro de ninguna índole, lo que la expone a un riesgo crítico.	A

MANUAL DE AUDITORIA DE SISTEMAS

DEPARTAMENTO : INFORMATICA
AREA : SEGURIDAD
SECCION : SEGURIDAD FISICA

EMPRESA AUDITORA :
AUDITOR :
FECHA : Noviembre, 1994.

F-52	El seguro cubre valor de reposición o valor según libros?	N/A		
F-53	La póliza cubre todo el equipo incluyendo líneas de comunicación de datos, aire acondicionado, medios magnéticos, etc.?	N/A		
F-54	La póliza refleja la configuración actual y se mantiene actualizada con las nuevas modificaciones?	N/A		
F-55	La póliza cubre daños maliciosos así como también daños por accidentes?	N/A		
	ASPECTOS VARIOS			
F-56	Está dotada el área de informática de alarmas contra incendio u otro tipo de contingencias como robo?	N	El área de informática no cuenta con ningún dispositivo que alerte al personal de cualquier circunstancia anormal.	M
F-57	Se cuenta con carteles sobre los procedimientos de emergencia y evacuación?	N	Existe un pequeño cartel en la entrada del centro de cómputo, pero no es suficiente-mente explicativo no resalta. Además no existe ningún anuncio para las medidas prohibitivas de cualquier centro de cómputo.	M
F-58	Se dispone de botiquines de primeros auxilios y equipos médicos de emergencia en las instalaciones?	N	No existe nada en toda el área del edificio que sirva para dar auxilio básico a cualquier usuario. El más cercano está a cerca de 500 mts.	A
F-59	En caso de un temblor, está sujetado el equipo para prevenir caídas accidentales del mismo?	N	Ninguna máquina cuenta con dispositivos que la protejan de movimientos bruscos o repentinos.	M

MANUAL DE AUDITORIA DE SISTEMAS

DEPARTAMENTO : INFORMATICA
AREA : SEGURIDAD
SECCION : SEGURIDAD FISICA

EMPRESA AUDITORA :
AUDITOR :
FECHA : Noviembre, 1994.

F-60	Tiene la persona encargada de administrar el centro de computo un puesto fijo desde donde pueda controlar todo el movimiento?	S	Si existe dicho puesto pero no es utilizado para ese fin.	M
F-61	Se controla el manejo de medios magnéticos ajenos al centro de computo? ✓	N	Cualquier usuario puede hacer uso de diskettes ajenos al centro de cómputo sin que estos sean siquiera verificados.	A
F-62	Existen personas encargadas de vigilar el área de informática cuando ésta se encuentra vacía o en horas nocturnas? ✓	N	Existe un vigilante de la Universidad pero no es suficiente como para vigilar el área del centro de cómputo.	A

MANUAL DE AUDITORIA DE SISTEMAS

DEPARTAMENTO : INFORMATICA
AREA : SEGURIDAD
SECCION : SEGURIDAD EN EL EQUIPO
EMPRESA AUDITORA :
AUDITOR :
FECHA : Noviembre, 1994

No.	Contenido de la Pregunta	S/N	Comentario	Riesgo
E-1	Existen medidas adecuadas para el cuidado, mantenimiento y respaldo del equipo de computación?	N	No se han tomando las medidas necesarias para el buen cuidado del equipo. Este tipo de servicio se da solo cuando existe algún problema.	A
E-2	Se cuenta con protectores de voltaje para todo el equipo delicado del área de informática?	S		
E-3	Existen fundas o cobertores adecuados para proteger el equipo de las condiciones del medio ambiente como polvo y humedad?	S	Si se cuenta con este tipo de protector para el equipo, pero no es utilizado por ningún usuario.	B
E-4	Se realizan limpiezas periódicas al equipo de computación (desde el teclado hasta las partes internas del equipo)	S	Solamente se hace limpieza cuando esta es solicitada. No hay un programa periódico para este mantenimiento.	B
E-5	Existen medidas prohibitivas para el consumo de bebidas y alimentos cerca de los equipos así como también el consumo de cigarrillos?	N	No existe en todo el centro de computo ningún cartel o aviso visible que prohiba estas situaciones.	M
E-6	Verificar que el ambiente donde está ubicado el equipo este libre de polvo, humo y motas u otras partículas dañinas para los sistemas.	N	Debido al tipo de construcción y a sus accesorios (ventanas y puertas) existe una gran filtración de partículas dañinas, además de que se está construyendo alrededor del edificio lo que colabora a la acumulación de suciedad.	M
E-7	Se cuenta con medidas para controlar que el equipo se desconecte cuando éste no se encuentre en uso?	N	No existen medidas que controlen estas anormalidades.	B
E-8	Existe algún encargado de verificar que los usuarios del equipo no coloquen sobre las rendijas de ventilación de las computadoras papeles, libros o cualquier otro elemento que obstruya la ventilación de los mismos?	S	Si existe un encargado que no cumple con este tipo de labores.	B

MANUAL DE AUDITORIA DE SISTEMAS

DEPARTAMENTO : INFORMATICA
AREA : SEGURIDAD
SECCION : SEGURIDAD EN EL EQUIPO
EMPRESA AUDITORA :
AUDITOR :
FECHA : Noviembre, 1994

E-9	Se cuenta con un listado o inventario de equipo con que se cuenta en el área de informática?	S	Si existe pero no es manejado por el área o departamento de informática.	
E-10	Se actualiza este inventario cada vez que existe una modificación, ya se adquisición o venta de equipo?	S		
E-11	Se tiene un registro de los números seriales de todos los equipos, periféricos y sus partes más relevantes?	S		
E-12	Existen programas de mantenimiento periódico para todo el equipo de informática?	N	El programa de mantenimiento no es periódico.	M
E-13	Que tipo de mantenimiento se utiliza en la organización, total, por llamada o en banco?		Mantenimiento por llamada. Solo se hace cuando es solicitado directamente al proveedor.	M
E-14	Existe un encargado de verificar las fechas en que se realizan los mantenimientos así como también las fechas de vencimiento de los contratos para éste servicio?	N		B
E-15	Se lleva un control escrito de las fallas encontradas en los mantenimientos y de las acciones realizadas para corregir estas fallas?	N	No existe ningún tipo de bitácora que controle a que máquina se le dio servicio y cual fue la reparación.	B
E-16	Se cuenta con equipo de respaldo en caso de que falle alguna instalación?	N		A
E-17	Determinar si el equipo de respaldo es compatible con el equipo que se maneja en forma normal	N/A		
E-18	Se tienen existencias de partes de repuesto esenciales en caso de que éstas sean necesarias?	N	No existen herramientas ni repuestos mínimos que deberían haber en un centro de cómputo para cualquier eventualidad.	B

MANUAL DE AUDITORIA DE SISTEMAS

DEPARTAMENTO : INFORMATICA
AREA : SEGURIDAD
SECCION : SEGURIDAD EN EL EQUIPO

EMPRESA AUDITORA :
AUDITOR :
FECHA : Noviembre, 1994

E-19	Existe una persona capacitada para realizar reparaciones sencillas cuando se necesite hacer alguna instalación?	S	Si existen alumnos o técnicos de la universidad que están en capacidad de realizar reparaciones sencillas.	
E-20	Existen planes de control del rendimiento del equipo y en que estado se encuentra?	N	No se verifica constantemente si alguna máquina ha reducido su capacidad de trabajo (aspectos como velocidad y manejo e memoria).	M

MANUAL DE AUDITORIA DE SISTEMAS

DEPARTAMENTO : INFORMATICA
AREA : SEGURIDAD
SECCION : SEGURIDAD DE RESPALDO

EMPRESA AUDITORA :
AUDITOR :
FECHA :

Nº	Pregunta	S/N	Comentario	Riesgos
R-1	Se cuenta con un programa de copias de respaldo?	S	Unicamente se cuenta con dicho plan en el centro de cómputo de la UDB	A
R-2	Se encuentra debidamente documentado este programa de respaldo?	N	Como ya se mencionó anteriormente, no existe ningún tipo de manual.	M
R-3	Existen ejemplares del programa de respaldo fuera del centro de computo?	N		A
R-4	Está el personal consciente del programa de respaldo en caso de que ocurra un siniestro?	N/A	No existe personal adicional en caso de algún accidente	A
R-5	Se han determinado períodos establecidos para realizar estas copias de respaldo (actualización de las copias)?	S	Se realizan a diario	
R-6	Cuando se realizan las copias de respaldo, se hace más de un duplicado?	N	Solamente se realizan una copia de respaldo en cada oportunidad	A
R-7	Se hace algún tipo de verificación durante el procedimiento de respaldo para garantizar la integridad de los archivos de respaldo?	N	Debido a que una sola persona realiza todo el trabajo de respaldo no cuenta de suficiente tiempo para esta actividad.	A
R-8	Garantizan los medios de respaldo una reconstrucción rápida de datos y programas en caso de que se produzca su pérdida total o parcial?	N	No hay forma de garantizar que las copias de respaldo cumplirán con su objetivo cuando sean utilizadas	A
R-9	Se tiene un lugar seguro para almacenar las copias de respaldo?	N	Actualmente se guardan en un archivo de administración. Se ha previsto la compra de una Caja Fuerte para este efecto.	M
R-10	En caso de existir más de una sola copia, se almacena por lo menos una copia adicional en un lugar ajeno al departamento en estudio?	N		M
R-11	Se mantienen los archivos de respaldo en diskettes separados de los archivos de trabajo?	S		

MANUAL DE AUDITORIA DE SISTEMAS

DEPARTAMENTO : INFORMATICA
AREA : SEGURIDAD
SECCION : SEGURIDAD DE RESPALDO

EMPRESA AUDITORA :
AUDITOR :
FECHA :

R-12	Existen programas o archivos a los cuales no se les hace respaldo?	N		
R-13	Poseen los operadores conocimiento sobre cuales son los archivos que se deben respaldar?	N/A		
R-14	Se controla el acceso a los archivos de respaldo?	N	Cualquier persona en contacto con dichos archivos puede accesarlos.	A
R-15	Se tiene respaldo para cada producto de software utilizado (adquirido o desarrollado)?	S	En el centro de cómputo del CITT no se tiene ninguna copia de los programas fuentes utilizados para laboratorios.	A
R-16	Se utilizan programas de utilidad probados para recuperar datos en medios destruidos?	S	Se utiliza el utilitario conocido como "Norton".	M
R-17	Se cuenta con procedimientos adecuados para la identificación de las copias de respaldo así como de los archivos de trabajo?	S		
R-18	Tienen los diskettes con archivos de respaldo los protectores contra escritura?	S		
R-19	Es el equipo de respaldo compatible con el equipo que maneja en forma normal?	N/A		
R-20	Se han hecho convenios para disponer de equipo de respaldo en otras instalaciones en el caso de que el equipo se vuelva inoperante durante un período extenso?	N	Si sucediera algún accidente o catástrofe, se suspenderían las labores en su totalidad.	A
R-21	Se solicitan a los programadores de aplicaciones que proporciones versiones de los programas para efectos de respaldo?	N/A		M
R-22	Se evalúa si los procedimientos de recuperación fueron efectivos?	N/A		A

CAPITULO 10

INFORME DE AUDITORIA

10. INFORME DE AUDITORIA

De las diferentes evaluaciones mencionadas en la Guía General para elaborar una Auditoría de Sistemas, del presente trabajo de graduación, se han seleccionado para desarrollar en esta etapa de la investigación, dos de las cuatro áreas mencionadas.

Así, el presente informe se ha estructurado de la siguiente manera:

- Evaluación del Area de Informática
  - Estructura de la Organización
  - Recursos Humanos
  - Presupuestos

- Evaluación de la Seguridad
  - Seguridad Lógica
  - Seguridad en el Personal
  - Seguridad Física
  - Seguridad de la Utilización del Equipo
  - Seguridad de Respaldo

Se ha realizado la investigación de campo correspondiente, la que ha arrojado diferentes resultados para cada área mencionada anteriormente. Dichos resultados serán comentados y detallados en el desarrollo del presente informe, resaltando cuales son los defectos más dañinos para la organización así como también las consecuencias de los mismos.

Para la obtención de información de la presente investigación, se utilizaron métodos como cuestionarios, entrevistas, observación en el sitio, etc. a través de los cuales fue posible establecer los aspectos más relevantes del sistema manteniendo siempre la objetividad necesaria para la realización de una Auditoría.

Al momento de realizar la investigación, se observo que el "Centro de Cómputo" de la Universidad es en realidad dos centros de cómputo en uno. Uno de ellos pertenece a la UDB (Universidad Don Bosco) y el otro al CITT (Centro de Investigación y Transferencia Tecnológica), cada uno dependiendo de diferentes administraciones. Para efectos de este informe, cuando sea necesario se hará diferencia entre cada uno de ellos, el resto de las veces, se tomará como un solo centro de cómputo.

Cabe aclarar, que no es objetivo de esta investigación, señalar culpables ni responsables, sino establecer puntos frágiles del sistema que deben ser mejorados para lograr el buen funcionamiento del área de informática.

Adicionalmente al análisis de la situación actual del Centro de Cómputo se presentan las recomendaciones que se estiman convenientes para mejorar el funcionamiento del Area de Informática de la Universidad Don Bosco.

Es recomendable que en toda Auditoría se ataquen los problemas, estableciendo prioridades de acuerdo al tipo de riesgo que representan. Así, un problema de riesgo alto debe ser resuelto antes de pasar a estudiar los problemas con riesgo medio y bajo. Usualmente, los riesgos altos, son los más difíciles y económicamente más costosos de resolver, pero también, la ocurrencia de uno de ellos representa una mayor perdida para la institución que esta siendo auditada.

A continuación se presentan los problemas encontrados en todas las áreas investigadas con una descripción de la situaciones encontradas. Seguidamente y simbolizadas por una **"R."** se presentan las recomendaciones para cada aspecto señalado. Debe tenerse en cuenta, que es importante que se resuelvan en primera instancia, las situaciones de alto riesgo, las que se señalan en los cuestionarios anexos a este informe.

ANALISIS Y RECOMENDACIONES

Evaluación del Area de Informática

Estructura de la Organización.

1. Se constató la inexistencia de ningún tipo de manual escrito en lo que respecta a: organización, procedimientos, normas y políticas, instructivos, etc. lo que conlleva a un funcionamiento inadecuado del área de informática. Al momento de una discrepancia, duda o problema, no existe ningún tipo de referencia al que se pueda acudir para resolver dicha situación.

   La primordial causa de la inexistencia de los manuales es la insuficiencia de personal auxiliar, problema que se discutirá más adelante.

   Debido a la carencia de instructivos, se presentan una serie de problemas que se mencionan a continuación:

   - Las responsabilidades del personal se dan por entendidas, lo que deja una flexibilidad demasiado amplia y dañina para la consecución de objetivos.

- Existe duplicidad de funciones por no existir delimitación de responsabilidades.

- Se carece de sub-departamentos, lo que obliga al supervisor a realizar todas las tareas, sobrecargándolo de trabajo.

- El personal de Informática realiza funciones que no le corresponden.

- No existe una forma de medir el cumplimiento de funciones, objetivos, metas, etc. ya que no han sido establecidas.

- Debido a que no existen manuales, no se han establecido normas de seguridad de ningún tipo, lo que representa el mayor riesgo para el área de informática.

R. Es necesario que en toda estructura organizativa de cualquier institución, se establezca desde un inicio los manuales organizativos, de puestos, procedimientos, etc. Con ello se logrará aclarar: los objetivos que se persiguen, las metas esperadas, las funciones que corresponden a cada departamento, las obligaciones de cada empleado, las características que deben llenarse para cada puesto, etc. En concreto, esto permite dibujar el esquema general de la organización y ayuda a que se trabaje de una manera organizada y eficiente.

Se recomienda que se asignen recursos para la elaboración de todos los manuales necesarios. Algunos de los más importantes son:

- Manual de Organización incluyendo diagrama.
- Manual de Procedimientos.
- Manual de Descripción de Puestos.
- Manual de Normas y Políticas.

2. El problema de organización se vuelve más serio debido a que existen dentro de la misma instalación 2 centros de cómputo que se manejan como uno solo. Por lo mismo, existen dos encargados, uno para cada centro, que son completamente ajenos y excluyentes el uno del otro. Esto se torna crítico en el momento de que falta uno de los dos, ya que no se cuenta con ninguna persona capacitada para sustituir, ni momentáneamente, a alguno de ellos.

   Cada uno de los supervisores depende de una diferente administración (CITT y UDB), por ello, es aún más difícil aunar esfuerzos en el manejo del centro de computo, pues cada administración persigue objetivos diferentes y maneja usuarios de distinta índole.

R. Se considera conveniente, que al momento de analizar la situación organizativa del centro de cómputo, se tome éste como una sola entidad y no como dos

distintas. Se deberá nombrar un Administrador que tendrá a su cargo todo el centro de cómputo y éste a su vez deberá contar con personal subalterno en el que delegará responsabilidades para el eficiente funcionamiento del área de informática.

3. Solamente se cuenta con 2 personas encargadas de controlar y manejar el área de informática, con una tercer persona a medio tiempo. Es fácil entender la sobrecarga de trabajo.

   Para el caso del Centro de Cómputo del CITT, se cuenta con dos personas, una a tiempo completo y otra a medio tiempo, encargadas solamente de controlar y manejar dicho centro a manera de instructores.

   Para el caso del Centro de Cómputo de la UDB, se cuenta con una sola persona, encargada de manejar, controlar, programar, hacer análisis de sistemas, supervisar, dar mantenimiento, es decir, realizar todas las labores relacionadas con ese centro de cómputo. La sobrecarga de trabajo en este caso sobrepasa los límites de lo aceptable, lo que reduce la productividad, efectividad y eficiencia del personal; obliga al retraso de trabajos por falta de tiempo; se recarga con tareas que no le corresponden, etc.

Por si ello no fuera un problema suficiente, no existe nadie más en toda la "Ciudadela Don Bosco" capaz de reemplazar a esta persona en caso de una emergencia, lo que traería consecuencias extremadamente serias para el funcionamiento de toda la Institución.

R. Es una necesidad imperante, la contratación de más personal capacitado para el área de informática. Partiendo desde el punto de vista de que debería ser una sola entidad, es necesario que para el equipo IBM 9370 (UDB) se contrate personal para el área de análisis, programación y operación. Solamente con esta variante, se estaría liberando de la mitad de la carga de trabajo al encargado actual, con lo que se le permitiría dedicarse a la administración del centro de cómputo con más libertad, incluso, podría ser él quien estableciera la estructura organizativa del área.

Para el caso de la red de PC's (CITT) solamente se necesita coordinar el trabajo de los instructores que permanecen en el centro, de tal manera que puedan realizar su trabajo de manera eficiente; su labor primordial es administrar que el equipo se mantenga funcionando correctamente y servir de apoyo a los profesores e instructores de los centros educativos (UDB y Tecnológico).

Como una nota relevante, cabe mencionar, que si dentro de la obligación de los instructores de la red de PC's esta servir de apoyo a los profesores de todas

las cátedras que se imparten en el centro de cómputo, no es suficiente con dos personas. Cada profesor y laboratorio, deberá tener su propio instructor y dejar a los administradores de la red como personal de apoyo permanente en el centro de cómputo.

4. En el Centro de Cómputo del CITT, que es ocupado por la Universidad, el Tecnológico y en algunas ocasiones el Colegio Don Bosco, las personas encargadas de administrarlo no tienen la suficiente autoridad como para tomar decisiones relevantes o que afecten directamente al Centro de Cómputo. Por el contrario, éste es administrado por personas ajenas al área de informática, lo que causa un conflicto de conocimientos en cuanto a las necesidades y problemas de un centro de cómputo. (Lo que para un Ing. en Sistemas puede ser crítico, para un Administrador de Empresas puede resultar subjetivo). En algunos casos sucede igual con el centro de cómputo de la UDB.

R. Como ya se mencionó, lo más recomendable es que una sola persona sea administrador de toda el área de informática, auxiliándose de personal en el que se delegará responsabilidades. Debe aclararse, que el administrador del centro de cómputo debe ser una persona capacitada tanto en el aspecto administrativo como en el aspecto técnico, siendo este segundo de suma importancia, pues solo conociendo el área y sus necesidades, podrá lograrse una buena administración. Lo ideal es que el administrador del centro de

cómputo sea un Ingeniero o Licenciado en Ciencias de la Computación con conocimientos en el área de administración pudiendo ser en algunos casos, otro Profesional con especialidad en la rama de Informática.

Recursos Humanos

5. No se cuenta con procedimientos adecuados para la selección de personal en el área de informática. Esto implica que no se realizan exámenes de conocimiento, psicológicos o de algún otro tipo que sirva para sentar los requerimientos mínimos para la contratación de empleados. Esto es aún más crítico debido a que no existe ningún tipo de capacitación de personal para ningún área de informática.

   Cabe aclarar que esto se ha constatado con el personal existente. Sin embargo, la cantidad de personal, como ya se mencionó, dista mucho de ser el suficiente por lo que el problema debe verse como un todo global.

R. Para lograr conformar un buen equipo de trabajo, es necesario que todo departamento cuente con un mecanismo lógico de selección de personal. Este mecanismo debe ser diseñado de tal manera que permita formarse una idea bastante amplia de su experiencia, conocimientos, criterio, etc. de tal manera que llene los requisitos mínimos necesarios para la asignación del puesto.

Es recomendable que este tipo de evaluaciones sea realizado por una persona con conocimientos en el tema que esta siendo evaluado ya que esto permitirá que la selección se realice de manera objetiva y con fundamentos reales.

6. No cuenta la institución con ningún programa de capacitación de personal en ningún área del departamento de informática. Esto conlleva a una serie de situaciones que solo dañan a la organización:

- Carencia de conocimientos del personal en cuanto al manejo del equipo.
- Atraso en tecnología.
- Espera innecesaria por la búsqueda de personal con el conocimiento deseado.
- Resultados no deseados por falta de conocimientos.
- Falta de motivación en el personal.

R. Bajo todo punto de vista, un programa de capacitación es sumamente beneficioso para la institución. Un aspecto importante de estos programas y que suele no tomarse como punto de evaluación, es que sirve de motivación para el personal quienes lo ven como una oportunidad de mejorar su preparación técnica o profesional. Aunado a esto, se pueden ver los beneficios a corto o mediano plazo mejorando la eficiencia y el desempeño del personal.

También, si el deseo es mantenerse a un nivel tecnológicamente competitivo, es necesario, que el personal se mantenga al paso con el desarrollo de la ciencia.

7. Se considera necesario la examinación de las tarifas de remuneración o pago de sueldos. Debe existir una competencia con los otros puestos de características similares en el medio.

   Tampoco existe ningún otro tipo de prestaciones que permitan que el personal este motivado, beneficios, promoción, ascensos, etc. Esta situación no ayuda a mejorar el desempeño de los empleados por carecer de incentivos que los empujen a ser buenos trabajadores.

R. Para poder mantener un nivel adecuado de personal capacitado, es necesario que se mantenga, dentro de las políticas de la empresa, una metodología que permita estudiar constantemente las remuneraciones del personal, las cuales deben estar siempre a la par de las demás instituciones. Por remuneración no debe entenderse solamente pagos en efectivo sino también beneficios en forma de especies tales como planes de vacaciones, seguro médico hospitalario, bonificaciones por buen desempeño, pago de horas extras, etc.

Nunca debe perderse de vista el aspecto de que la remuneración siempre será de acuerdo a la capacidad del personal así como a su carga de trabajo y no en

base a favoritismos, preferencias o como se conoce en el medio "por conectes" con directores o personal ejecutivo. Esto implica que la selección del personal deberá ser cuidadosamente estudiada, como ya se mencionó anteriormente.

8. El ambiente en que se desempeña el personal, a pesar de no ser de mala calidad, no es el más indicado. No se cuenta con un mobiliario adecuado, las instalaciones no son idóneas para un centro de cómputo, no se cuenta con servicios sanitarios en el departamento, etc. El espacio en que se desarrollan las actividades cotidianas es escasamente suficiente.

R. Iniciando por la imagen que presente un centro de cómputo, sus instalaciones deben dar la idea de seguridad, confiabilidad y calidad. Por lo mismo, éstas deberán ser estudiadas de acuerdo a las necesidades que tendrá el centro, proporcionado al personal un ambiente de trabajo saludable, cómodo y bien distribuido. En la medida en que el personal se sienta cómodo, así será su nivel de producción. Además de ello, el mobiliario debe ser el idóneo para el tipo de actividad a que sea destinado.

9. El departamento de informática no cuenta con planes de trabajo debidamente organizados y planificados con el suficiente tiempo de anticipación como para tener una idea de en que manera se cumplirá con los objetivos. No se

especifica en cuanto tiempo y que personal será el asignado a determinada actividad sino más bien en el momento que surge la necesidad o el problema, se busca la manera de resolverlo.

R. Es importante que todo departamento organice su trabajo desde el momento en que este es asignado, estableciendo tiempos y recursos necesarios. Con ello es posible llevar un mejor control de las actividades, así como también prever que recursos se necesitarán a lo largo del trabajo y no encontrarse con interrupciones imprevistas por falta de planificación.

Presupuestos

10. Se maneja, dentro de la administración general, un presupuesto destinado al área de informática, pero dicho presupuesto no es realizado por el personal de cómputo sino más bien por el administrador y por el encargado de librería, que es donde están los accesorios de trabajo para el centro de cómputo. Cuando existe una nueva necesidad, esta debe ser canalizada a través de la administración, quien determinará si es factible o no. Esto tiende a indicar que el presupuesto no está programado de tal forma que cubra en su totalidad o en un porcentaje mayoritario, las necesidades en que incurrirá el área de informática.

Este mismo problema tiene sus consecuencias dentro de las propias instalaciones, debido a que no se cuenta con mobiliario adecuado, espacio suficiente, distribución de equipo en forma eficiente, etc. Al no existir un presupuesto realizado con suficiente anticipación y con las previsiones necesarias, se cae en los problemas planteados en algunos de los numerales anteriores.

Otro aspecto que no es incluido dentro de los presupuestos, es la adquisición de software de ningún tipo. Todo el software utilizado en el centro de cómputo, con excepción del 9370, es aportado por el alumno o por el profesor, lo que representa un riesgo que se discutirá más adelante. Incluso, se ha llegado al punto de adquirir software, sin consultar en absoluto a ninguna persona del área de informática.

En el centro de cómputo del CITT, debido a la carencia de recursos, se dejan de realizar actividades necesarias para el desarrollo normal del centro. Debido a que no existe software de ninguna clase, propiedad del centro de cómputo, los instructores deben ingeniárselas para adquirir "paquetes" para llevar a cabo sus actividades cotidianas. Incluso, han existido períodos en que no se han impartido laboratorios debido a la carencia del software necesario para ello.

R. Para llevar a cabo cualquier tarea, es necesario que desde un inicio se cuente con un presupuesto detallado al máximo posible y así conocer cuales serán las necesidades que deberán satisfacerse en el camino. Usualmente, el más indicado para realizar el presupuesto es aquel que estará íntimamente relacionado con la actividad en si. Con esto se quiere recomendar que no solo para el área de informática sino para todos los departamentos, los presupuestos sean presentados por el encargado de cada departamento y después sea discutido con el personal de administración, de tal manera que se establezca el porque de lo planteado en el mismo.

También es necesario que año con año o por períodos pre-establecidos, se estudie y se realice un nuevo presupuesto, debido a que las necesidades son cambiantes. Sobre todo en un centro educativo, donde en cada período se necesitarán recursos diferentes.

Debido a la actividad que realiza el área de informática de la Universidad Don Bosco (Centro de computo del CITT y UDB), es recomendable que a la hora de llevar a cabo su presupuesto se tomen en cuenta los siguientes aspectos, que normalmente son dejados fuera del estudio:

- Mobiliario Adecuado (mejoramiento)
- Archiveros

- Software
- Bodega de materiales y equipo
- Seguros
- Servicios ajenos al área (mantenimiento, etc.)

Esto no es limitante de un presupuesto, siempre deberá considerarse los demás requisitos como papelería y útiles, accesorios, mantenimiento, etc.

11. Otro problema relacionado con los recursos, es que no existe un método o procedimiento de actualización o retroalimentación de informática a administración en cuanto a los recursos que necesitan o van a necesitar. Esto trae como consecuencia la no asignación de recursos debido a falta de información.

R. Con suficiente tiempo antes del vencimiento del período establecido para la elaboración de presupuestos, es necesario que el personal de Informática se reúna con el personal de administración para establecer cuales serán las necesidades que tendrá para el siguiente período, necesidades antiguas pero vigentes y nuevas necesidades. De está manera, la administración puede hacerse una idea de lo que se necesitará y determinar al personal de informática con cuantos recursos contará para su funcionamiento. Con esto, el

encargado de cómputo puede priorizar sus necesidades y basado en ello realizar su presupuesto.

12. El control de activos como mobiliario y equipo así como también el manejo de los accesorios tales como papelería, medios magnéticos, etc. (inventario) tampoco es manejado por el área de informática. Nuevamente es la administración, la encargada de controlar estos aspectos directamente relacionados con el centro de computo.

R. La única forma de establecer cuales serán las necesidades que se tendrán para los siguientes períodos y de contabilizar de que manera se están manejando y distribuyendo los recursos asignados para el período vigente, es llevar un control estricto de los recursos solicitados y asignados. Para ello, es necesario que el departamento de cómputo maneje su propio inventario; además, de esta forma puede justificarse más fácilmente la solicitud de nuevos recursos.

También, solo así puede establecerse cuando o cada cuanto se harán los nuevos pedidos de materiales y accesorios (establecimiento del punto de pedido).

Evaluación de la Seguridad

Seguridad Lógica

13. La institución y específicamente el área de informática, no ha establecido en forma clara medidas de seguridad para proteger la información de cualquier tipo de accidente o incidente.

    Por ejemplo, cuando se realizan reportes o informes de cualquier índole, no existe un encargado de velar por la confidencialidad del manejo de dichos reportes. Se utiliza al ordenanza para la distribución de los reportes sin velar por que no se adultere, se robe, se duplique, es decir, se altere la seguridad de la información

R. El activo más importante de cualquier institución o empresa es la información, por lo que deben tomarse medidas extremas para protegerla contra cualquier tipo de riesgo. La información está expuesta a todo tipo de situaciones contra las que debe tomarse medidas: Deformación o Adulteración de la Información, Robo de Información, Uso ilícito de información, etc. Por estas razones y muchas otras, se debe tener un gran cuidado cuando se maneja información.

No se puede dejar en manos de cualquier persona; debe controlarse el acceso a la misma; debe canalizarse a través de los medios adecuados; debe guardarse en lugares protegidos contra robo y desastres naturales o accidentes; debe codificarse de acuerdo a su nivel de confidencialidad.

Se recomienda que se realice un manual de información donde se codifique de acuerdo a su nivel de confidencialidad y se elabore un diagrama de flujo de información en el que se establezcan canales de distribución especificando niveles de seguridad, personas responsables, remitentes y destinatarios, períodos de distribución con fechas si es posible. Todo aquello que permita proteger al máximo la información.

14. No se lleva un control de los programas que son almacenados en las computadoras del centro de cómputo del CITT, lo que implica que en ellas, el usuario puede guardar a su libre albedrío cualquier tipo de información y de igual manera obtener información que se encuentre dentro de la máquina. Esto en determinado momento satura la máquina de información innecesaria.

Este mismo hecho trae varias consecuencias dañinas para el centro de cómputo: No se controla la utilización de programas pirata, lo que desde inicios del presente año es una medida ilegal. Tampoco existen medidas para evitar la

contaminación del equipo con virus, lo que hace extremadamente inestable al centro de cómputo desde cualquier punto de vista.

A pesar de que el centro de computo cuenta con copias de programas antivirus, no tienen ningún tipo de plan de descontaminación periódico para evitar que una máquina infectada contamine a otra y así sucesivamente. En este punto específico, tampoco se controla la utilización de medios magnéticos, los cuales son el medio de transporte del virus.

R. En todo centro de cómputo debe existir un encargado de velar por la integridad de las máquinas que están a su cargo. Con esto se quiere decir, que no basta con que este presente todo el tiempo, sino que examine periódicamente el equipo para verificar su contenido, tanto en cantidad como en calidad.

También es importante que este encargado verifique constantemente que el equipo no se encuentre contaminado con ningún tipo de virus. Para ello no basta con la buena intención del supervisor sino que es necesario contar con un buen sistema de descontaminación o programa antivirus el cual debe ser original y el método adecuado en el que se establezca un programa de examinación y limpieza.

También es recomendable que el encargado cuente con una bitácora en la que se controle las situaciones anormales que suceden en cada equipo (el cual debe estar codificado con un número diseñado por el supervisor) así como también un listado de los programas que deben estar grabados en cada máquina.

Seguridad de Respaldo

15. Dentro de esta sección se presenta la situación en una forma diferente para los dos centros de computo:

    Para el centro de computo del CITT, debido a que solamente es utilizado para laboratorios o prácticas, no cuenta con ningún tipo de información que sea de importancia para realizar copias de respaldo, pero si cabe hacer notar que dada la actividad que realiza no cuenta con ninguna copia de respaldo de los diferentes programas que utiliza para realizar las prácticas. Todos los programas con excepción del sistema operativo y Windows han sido instalados de copias que no son las originales (piratas).

R. Es una buena práctica en cualquier centro de cómputo hacer uso solamente de copias originales de los distintos programas que se utilizan normalmente para sus labores cotidianas. Por ello se recomienda que poco a poco se haga un

banco de programas originales de tal manera que se garantice la integridad de la información. Adicionalmente a esto, a inicios del presente año, se aprobó la ley de protección a la propiedad intelectual, lo que significa que cualquier copia de cualquier programa que sea adquirido de forma pirata es ilegal, y como centro de formación de profesionales, se debe dar el ejemplo e inculcar en los estudiantes el respeto a la propiedad intelectual.

Esta es una buena forma de garantizar que la información se mantenga integra y no dañe el equipo por distintas razones, la principal son los virus.

16. En cuanto al Centro de Computo de la Universidad, si se constato que se poseen copias de seguridad, aunque se pudo detectar que existen muchos vacíos en cuanto ha este tipo seguridad:
    - Inicialmente, no se cuenta con ningún tipo de documentación que respalde el método utilizado.
    - No se tiene un lugar que garantice que estas copias no sufran daños o variaciones de información por personas ajenas.
    - Solamente se tiene un duplicado de la copia de respaldo, pudiendo provocar con esto que al momento de querer recuperar alguna información esta no se encuentre completa.
    - No se cuenta con una seguridad que garantice que nadie tenga acceso a las copias de respaldo.

- En el caso de que el equipo sufra algún desperfecto en su funcionamiento no se ha tomado en cuenta disponer de algún lugar donde se pueda seguir procesando la información, lo que representa un riesgo sumamente grave para los intereses no solamente de la Universidad sino de toda la Ciudadela.

R. Para lograr el objetivo final de tener un programa de copias de respaldo, debe diseñarse un método que sea eficiente, eficaz y ante todo confiable. Es necesario que se elabore un sistema con períodos, archivos, cantidad, etc. para realizar dichas copias. Con ello no solo se reduce el riesgo de cualquier perdida de información sino se eleva el nivel de confiabilidad de las copias de respaldo. Una vez que se haya diseñado el sistema, debe dejarse debidamente documentado preferiblemente con un manual que sirva de referencia a todo el personal relacionado con estas copias.

En el proceso de investigación se dio a conocer la existencia de una caja fuerte destinada entre otras cosas a guardar las copias de respaldo pero aún no es utilizada para ese fin. Es necesario recalcar que la información es el activo más importante de cualquier empresa o institución, por lo mismo, no debe tomarse de menos la necesidad de contar con un lugar seguro para almacenar las copias de respaldo, que en un momento determinado podrían significar días de trabajo. También es importante que cuando se realicen estas copias, se hagan en más de un duplicado de los cuales uno por lo menos deberá ser guardado

fuera de las instalaciones de la Universidad (un banco, otro centro de cómputo, etc.).

Como una medida adicional y generalmente fuera del alcance de las posibilidades de cualquier empresa o institución, es recomendable contar sino con un centro similar, con una instalación que permita seguir las operaciones esenciales del área de informática en caso de accidente o desastre, en el cual se pueda instalar rápidamente los programas fuentes y las copias de respaldo más recientes. De esta forma se reducen las perdidas causadas por la interrupción de operaciones.

Seguridad Física

Edificios y Construcción

17. Se pudo constatar, que la construcción del edificio, a pesar de ser sólida y bien cimentada, presenta una serie de deficiencias. Una de ellas es el hecho de que algunas de las paredes que dividen al centro de cómputo de las demás áreas del edificio están hechas de madera (plywood), lo que significa un riesgo a la integridad del centro de cómputo.

R. Como una medida indispensable de seguridad en todo centro de cómputo, este debe estar protegido contra cualquier intento de ingreso no autorizado. Esto implica que todo su contorno debe estar construido con una superficie sólida que impida el acceso. Además como ya se mencionó es importante que el centro de cómputo este completamente separado de cualquier otro departamento o área de trabajo. Se recomienda que en cuanto se tenga más espacio en los edificios aledaños, se deje el centro de cómputo completamente aislado y con una distribución de espacios más adecuada.

18. También se verificó, que las ventanas del centro de cómputo no tienen la seguridad mínima necesaria para evitar cualquier tipo de contingencia. Dichas ventanas que dan al exterior (pasillo exterior circundante) están protegidas con una defensa que no cumple con los requerimientos de seguridad para evitar el acceso al centro. Además, las ventanas no son las adecuadas para un centro de cómputo que tiene acceso al exterior.

R. Es necesario que se incremente la seguridad a las defensas instaladas al exterior del centro de cómputo. Deben tener una estructura más rígida y sólida haciéndolas prácticamente imposibles de ser dañadas. También se recomienda que se instalen ventanas adecuadas para un lugar que requiere de un mínimo de seguridad. El tipo de ventana "solaire" sencillo son relativamente fáciles de retirar por lo que son más recomendables las de tipo "ONIN".

19. Las ventanas están cubiertas con pliegos de poliestireno (durapax) para evitar el paso de la luz. De igual manera, el cielo falso esta hecho del mismo material. Esto podría en determinado momento significar un alto riesgo de incendio debido a que dicho material es altamente combustible.

R. Nuevamente se puede iniciar por el aspecto estético del centro de cómputo. Para evitar el exceso de luz se recomienda la instalación de cortinas, que deben ser de un material no combustible. En lo que respecta al cielo falso, existe un material de bajo costo y resistente al fuego con el que se puede sustituir los pliegos utilizados actualmente. Además debe buscarse que el material utilizado sea impermeable, de tal forma que si por cualquier circunstancia, el agua se filtra del techo al cielo, este segundo no permita que se filtre y se precipite hacia el equipo.

20. Las gradas que conducen al centro de cómputo (ubicado en un segundo piso) presentan un alto grado de inseguridad para los usuarios que las utilizan pues carecen de la solidez necesaria y no cuentan con pasamanos a ambos lados de las escaleras. Esta situación también se vuelve crítica cuando existe la necesidad de mover equipo pesado del centro de cómputo a otra área de la Ciudadela.

R. Como primer punto, se recomienda la instalación de otro juego de gradas para agilizar la circulación del edificio, aspecto que se vuelve crítico en caso de emergencia.

Debe de buscarse la manera de reforzar la seguridad de las gradas actuales a las que se recomienda que también se incluya otro pasamanos ubicado al lado interno de las gradas.

Ubicación del Area de Cómputo

21. La ubicación que el centro computo tiene dentro del edificio es en el segundo piso, teniendo a su alrededor otros talleres, como son: Electrónica y Mecánica, los cuales representan un peligro debido a que algunos de estos talleres utilizan materiales y equipo que representan de una forma u otra un riesgo para el centro. Esta situación también genera mucho consumo de energía eléctrica, lo que provoca que existan caídas de voltaje que pueden dañar el equipo de cómputo.

R. Como ya se ha repetido en varias ocasiones, lo más indicado es que el centro de cómputo este completamente aislado de cualquier otro centro de trabajo por distintas razones: confidencialidad, seguridad de accesos, independencia, seguridad física, etc. Además, como se pudo verificar, el consumo de energía

eléctrica dentro del edificio es extremadamente alto, lo que ocasiona que existan caídas de voltaje e incluso perdida total del fluido eléctrico, por lo que se recomienda que el centro este completamente aislado de tal manera que el fluido sea constante a todo el centro de cómputo.

22. Como ya se mencionó, las paredes externas del centro de cómputo dan a un pasillo circundante que rodea todo el edificio. Dicho pasillo, a pesar de estar en un segundo piso, tiene acceso directo a un área de circulación pública y sin vigilancia constante, lo que representa un riesgo más para el centro de cómputo.

R. Debido a que no se puede recomendar la eliminación del pasillo exterior, se recomienda que se aumente la seguridad de puertas y ventanas que dan a dicho pasillo así como también que se incremente la vigilancia, más que todo nocturna, en esa sección de la universidad. Una buena medida sería instalar un sistema de iluminación que no deje rincones oscuros por donde pueda esconderse personal no autorizado. También sería una medida de precaución, instalar un sistema de alarma que permita saber si ha habido ingreso al edificio.

23. Otro aspecto que se debe mencionar es que en el mismo centro de computo, y solamente separados por una división de madera, se tiene un taller de

electrónica en donde se hacen reparaciones de toda clase, lo cual representa un peligro, ya que se utilizan materiales y equipos que pueden provocar una sobrecarga o cortocircuito, lo que conllevaría a un incendio. Este mismo aspecto tiene el problema de que uno de los accesos a dicho taller es a través del centro de cómputo, situación que debería evitarse.

También existe dentro del centro de cómputo una pequeña bodega de materiales y repuestos que es utilizada por los talleres de eléctrica, mecánica y electrónica, lo que genera los mismos problemas de acceso y circulación mencionados anteriormente.

R. Como ya se había recomendado, es importante que el centro de cómputo este totalmente aislado de cualquier otro departamento u área de trabajo. Esto significa que no debe circular por el centro ningún personal que no tenga relación con el mismo, de esta manera se puede llevar un mejor control del ingreso de extraños.

También deben eliminarse riesgos innecesarios como son accidentes por incendio o descargas eléctricas. Para ello es preciso que no exista ningún tipo de actividad que genere dichos riesgos en la misma área de informática. Cualquier tipo de taller que exista aledaño al centro de cómputo, debería ser trasladado a otra área.

24. Se carece de archivadores u otro tipo de mueble para poder guardar medios magnéticos, documentos propios de cada centro de computo, papelería, accesorios, etc. lo que obliga a los usuarios a colocar todo lo antes mencionado sobre el mobiliario destinado para el equipo. Esto no solo resta estética y orden al centro de cómputo sino también representa un riesgo de daño al equipo.

R. Se necesita ubicar dentro del centro de cómputo un área que sirva como almacenamiento de diferentes tipos. Para guardar papelería y accesorios; para almacenar medios magnéticos, manuales e información; una bodega de repuestos y una área para guardar artículos personales de los usuarios y de aquellos que laboran dentro del recinto.

Accesos

25. Debe aclararse a este respecto que ambos centros de cómputo, tanto el del CITT como el de la UDB, utilizan el mismo acceso para ingresar a sus instalaciones, situación que en determinado momento pueda no ser la más idónea.

Para el centro de cómputo de la Universidad no existe ningún tipo de control para poder ingresar al área ya que no es muy utilizado por diferentes usuarios, sino que solamente para procesar información de la Ciudadela, tarea que esta a cargo de una sola persona. Se pudo observar que en ciertas ocasiones este centro permanece solo, ya que el encargado realiza muchas funciones tanto dentro como fuera del recinto, y no existe otra persona que pueda cubrirle su puesto, lo que genera el riesgo de que cualquier persona ajena a dicho centro ingrese sin ninguna autorización.

En cuanto al centro de cómputo del CITT existe un serio problema de acceso, ya que no se tiene ningún tipo de control que verifique si la persona está o no autorizada para estar en el área, pudiendo estos ingresar sin que los encargados se den cuenta.

R. Como primer aspecto importante debe destacarse que si bien es cierto que ambos centros de cómputo deben organizarse como uno solo, la información que se maneja en cada uno de ellos es completamente distinta. Por ello, no es una buena práctica que ambos centros utilicen un mismo acceso, debido a que la información que se procesa en el centro de la UDB es mucho más delicada y confidencial. Si se separan los accesos, puede lograrse controlar casi en su totalidad el ingreso no autorizado al centro de la UDB que en nivel de seguridad es más crítico. Por efectos de conveniencia si sería recomendable que exista

una puerta que comunique a ambos centros, pero ésta no deberá ser utilizada como acceso.

Como se mencionó, no existe ningún tipo de control sobre el personal que ingresa a los centros de cómputo, lo que conlleva a elevar el riesgo de cualquier tipo de percance a cualquiera de los dos centros. Es importante el establecimiento de un control de acceso, para lo que debe haber una persona responsable a tiempo completo o varias personas (menos recomendable) que trabajen por turnos y que constantemente exijan una identificación o para el caso autorización de ingreso. Esto es valedero para ambos centros. Una buena medida es que el personal encargado cuente con listados proporcionados por los docentes de cada materia. Debe existir también para el personal que labora en los centros de cómputo un tipo de identificación, la cual deberá ser diferente a la de los alumnos y la deberán llevar consigo en un lugar visible mientras permanezcan dentro del área de informática.

En la actualidad y debido a que el único acceso esta en el área destinada para el centro de cómputo del CITT, que es donde fluye mayor cantidad de personas durante todo el período laboral (debido a su actividad primordial de laboratorios) es necesario que el personal destinado a ese centro se responsabilice de controlar el acceso al área de informática. Posteriormente y si son separados

los accesos a ambos centros, deberán haber dos personas encargado, una para cada centro de cómputo.

También puede recomendarse que cuando lleguen visitantes de otras instituciones o entidades, se notifique al personal del centro tanto la hora como la cantidad de personas que se presentarán las que deberán llegar acompañadas por alguna autoridad de la Ciudadela o por personal de informática.

26. El centro de cómputo cuenta con 5 puertas: una de ellas es utilizada como entrada y salida al centro de cómputo (metálica); dos dan al pasillo en el exterior de edificio y permanecen cerradas con llave todo el tiempo (metálicas); otra es una puerta de madera que lleva a una bodega de materiales y repuestos y la última es utilizada por el taller de electrónica, también de madera, que está contiguo al centro. A pesar de tener dichas puertas, no existe ninguna que este destinada a servir como puerta de emergencia en caso de un siniestro o catástrofe.

R. La puerta principal o de acceso, debe mantenerse, con la única modificación de una chapa eléctrica que sea controlada por el encargado del centro y además añadir un regresador automático para que la puerta permanezca cerrada todo el

tiempo. Si en determinado momento se separan los accesos a ambos centros, la puerta del otro también debe cumplir con las mismas características.

Las otras dos puertas deben permanecer cerradas todo el tiempo tomando la precaución de que se cuente, en el centro de cómputo, con un juego de llaves para dichas puertas. Más aún, se recomienda que una de ellas sea convertida en puerta de emergencia la cual debe estar debidamente identificada con rótulos visibles desde cualquier punto del centro de cómputo. Para ello, es necesario cambiar el mecanismo de cerradura, siendo este del tipo que solo puede abrirse por dentro y no necesita llave de ninguna clase. Dentro de esta misma recomendación, es necesario prever un mecanismo que permita al personal del centro desalojar el edificio si la puerta de emergencia es utilizada; para ello puede proveerse un tipo de escalera de emergencia que sea accionada desde la parte superior y que sirva para que el personal tenga una forma de bajar hacia la parte inferior del edificio.

En lo que respecta a la puerta de la bodega, debe recomendarse inicialmente que dicha bodega sea utilizada exclusivamente para el centro de cómputo y no para otro tipo de talleres o laboratorios. También es recomendable que permanezca con llave todo el tiempo y que el encargado de turno tenga un juego de llaves.

Por último, la puerta que da al pequeño taller de electrónica aledaño al centro de cómputo debe ser sellada permanentemente para evitar la circulación de personal ajeno al centro dentro de sus instalaciones. Cabe aclarar que dicho taller tiene otra puerta de acceso por el pasillo exterior del edificio así como también que puede habilitarse otra puerta que colinde con el laboratorio de electrónica.

27. No se tiene un control de ingreso de maletines, bolsas u otro tipo de objetos debido a que no existe un lugar adecuado para almacenarlos. Esto implica que los usuarios del equipo se ven forzados a colocar libros, bolsones u otro tipo de implementos encima del equipo o en todo caso en una orilla de la mesa. Esto representa un riesgo no solo para el hardware sino también para el personal.

R. El permitir que los usuarios ingresen con maletines, bolsas, etc., hace más difícil para el supervisor o encargado el estar controlando a cada usuario que en determinado momento podría llevar consigo objetos no autorizados dentro del centro como alimentos, líquidos o artículos peligrosos como armas, etc. También se corre el riesgo de daño físico al equipo por acumulación de objetos contiguo e incluso sobre el equipo.

Esta situación representa una serie de riesgos que pueden ser evitados de una forma relativamente sencilla. Se recomienda la instalación de un mueble tipo

casillero en el que el usuario pueda dejar sus objetos personales mientras se encuentra dentro del centro los cuales entregará a los instructores al ingresar al área.

Instalaciones Eléctricas

28. Se pudo observar que los interruptores del tablero de control del centro de cómputo están al alcance de cualquier persona que circule por el salón, lo que obviamente representa un riesgo innecesario.

R. Se recomienda que se busque una manera de proteger el tablero de control de tal forma que solamente el personal autorizado pueda tener acceso a él. Una buena forma es instalar una cerradura que no permita que se habrá dicho tablero, nuevamente, solo el personal encargado tendrá llave de dicha cerradura. Con esto se evita que por cualquier motivo alguien ajeno al centro interfiera con los controles eléctricos.

29. No se cuenta con un sistema de emergencia que pueda alimentar energía en caso de que hubiera un corte por lo que el trabajo debe ser detenido indefinidamente hasta que se cuenta con energía eléctrica de CAESS.

R. A pesar de que se cuenta con UPS (uno para cada dos máquinas), en el caso de una interrupción larga del fluido eléctrico, no hay forma de normalizar el trabajo. Se recomienda que se adquiera un sistema generador de energía lo suficientemente capaz de alimentar por lo menos al equipo indispensable, para el caso el IBM 9370 y las terminales que se estime conveniente además de algunas de las terminales del centro del CITT.

30. Un problema bastante serio que existe en el centro de cómputo es la distribución de cables del equipo. Estos se encuentran regados por todo el centro de cómputo, sin haber un orden que permita identificar a que equipo pertenecen. Por lo mismo, los cables se ven expuestos a una serie de riesgos altamente peligrosos. Existe la posibilidad de corto circuito al momento de que un usuario choque o arrastre cualquier cable por su mala distribución. También, debido a filtraciones de agua (se detallará más adelante) existe la posibilidad de corto circuito por humedad. Otro riesgo es la posibilidad de que un cable sea halado y se precipite algún equipo pudiendo dañarse permanentemente.

    Existe un completo desorden y es imposible la identificación de los cables debido a la mala ubicación en que se encuentran.

R. Primeramente, debe buscarse la manera de distribuir los cables de tal forma que estén completamente o casi en su totalidad fuera del alcance de los

usuarios. Para ello debe instalarse tuberías o canales dentro de los cuales se distribuyan los cables del centro. Dichos canales deberá ser accesibles y permitir la posibilidad de trabajar en los cables por secciones, además de permitir la movilización del equipo sin mucha dificultad. Estas tuberías o canaletas deberán estar debidamente rotuladas e identificadas para su fácil manejo y comprensión. Esta identificación deberá estar documentada y explicada en un pequeño manual o guía. Lo más utilizado en el medio es la coloración de las tuberías en las que cada color tiene un distinto significado.

Con esto se logra: organizar el cableado del centro de cómputo; proteger contra filtraciones de agua; proteger contra choques inadvertidos o accidentales; etc.

Debido a la forma en que esta distribuido el centro de cómputo, se recomienda que el cableado que sale de cada una de las computadoras sea sujetado por medio de un dispositivo de amarre, de tal forma que no se confundan ni enreden los cables de una máquina con otra.

También es necesario que se instalen luces de emergencia que automáticamente funcionen en caso de falta de energía eléctrica

Protección contra inundación

31. Cuando se dan lluvias fuertes, existe una filtración de agua por las rendijas de las puertas que dan al exterior del edificio. Esto no solo ocasiona un riesgo eléctrico sino también un riesgo contra el personal que labora en las instalaciones.

    Unido al problema anterior, el centro de cómputo no cuenta con un tipo de sistema de drenaje que le permita evacuar el agua en caso de que se de esta situación.

R. Es necesario que se resuelva a corto tiempo el problema de filtración de agua que se tiene durante la época de invierno. Hasta ahora han intentado una serie de alternativas de solución para dicho problema, pero ninguno ha cumplido con su objetivo. Una solución factible sería el levantamiento de una pequeña grada que no permita que el agua escurra hacia las puertas que dan al pasillo exterior del edificio.

La causa primordial de la filtración de agua hacia el centro de cómputo, es un mal diseño de drenaje o evacuación de aguas tanto en el pasillo exterior como en el interior del centro de cómputo. Por lo mismo se recomienda que se diseñe un sistema que permita evacuar las aguas lluvias del pasillo exterior de una

manera más eficiente así como incluir dentro del centro, un sistema de drenaje a través del cual se pueda sacar el agua que se acumule en él.

Protección contra incendios.

32. El edificio no esta dotado de ningún tipo de sistema contra incendios. No hay irrigadores ni extinguidores de ninguna clase.

R. Lo ideal es que se incluya en el centro de cómputo un sistema de irrigadores activados por medio de detectores de humo que eviten la propagación de un incendio y al mismo tiempo activen una alarma sonora para alertar al personal. Además todo departamento debe estar dotado de extinguidores, para los que se debe tener algunas precauciones: deben estar cargados con un material químico que no dañe el equipo en caso de que sean utilizados; deben estar pintados de rojo y ubicados en una posición visible desde cualquier punto del centro; debido a que no son utilizados constantemente, debe verificarse que dichos artefactos no estén descargados y que están trabajando normalmente.

También es importante mencionar que debe capacitarse al personal encargado de cada departamento en cuanto a la utilización del equipo de extinguidores.

33. Un problema de negligencia que pudo verificarse es que existe una acumulación

de material inflamable dentro del centro de cómputo. No solo están las ventanas y puertas cubiertas de poliestireno sino que entre el cielo falso y el techo, existe una acumulación de cajas de cartón utilizadas para empacar el equipo. También existen divisiones de madera dentro del centro de cómputo, mesas y utensilios, acumulación de papeles, etc. lo que se vuelve un riesgo potencial para incendios.

Como se menciono anteriormente, el centro de cómputo esta contiguo a dos talleres, eléctrica y mecánica y además, dentro del mismo centro existe un pequeño taller de electrónica, todo esto representa una posibilidad latente de incendio.

R. Los incendios representan una amenaza seria para cualquier centro de cómputo. Por lo mismo no debe de tomarse como una situación sin importancia al momento de analizar la seguridad de informática.

Como primera instancia, se recomienda que los pliegos de poliestireno utilizados como protección contra el sol, sean sustituidos por cortinas que sean de material no inflamable o poco inflamable, lo cual es aplicable al cielo falso que esta hecho del mismo material.

También es importante que se deje de utilizar el espacio entre el cielo falso y el techo como bodega o basurero para acumular cajas de cartón que no serán utilizadas. Si existe la necesidad de guardar las cajas en que el equipo venía almacenado, se recomienda que se utilice una bodega en la que se puedan guardar todas las cajas que en determinada instancia podrán ser útiles y que éstas sean desarmadas y dobladas para que utilicen menos espacio.

Otro aspecto que debe ser tomado en cuenta es que el mobiliario como escritorios, mesas, sillas, divisiones y demás deben ser de un material poco flamable, por lo que no es recomendable que estos sean de madera u otro material similar.

Como ya se mencionó anteriormente, el centro de cómputo esta rodeado por otro tipo de talleres como lo son el de eléctrica, mecánica y electrónica, en los que se trabaja con equipo y material que en determinadas circunstancia podrían ocasionar un incendio. Por ello, una buena práctica es aislar al centro de cómputo de este tipo de instalaciones para reducir el riesgo de cualquier accidente.

Aire Acondicionado

34. Se comprobó, que las instalaciones del aire acondicionado no son las adecuadas. La tubería de desagüe de los equipos, pasa por encima de computadoras, lo que significa que si una de ellas llegase a romperse, se corre el peligro de un corto circuito.

    La forma en que ha sido distribuida dicha tubería así como también el cableado eléctrico del equipo de aire acondicionado, va en detrimento de la imagen del centro de cómputo.

R. Bajo ningún punto de vista es recomendable que cualquier tipo de tubería se coloque en un área de tráfico de personal. Se corre el riesgo de que se rompan las tuberías, se dañe el equipo, exista algún accidente al personal, etc. Además, el aspecto estético del centro de cómputo deja mucho que desear. Para este caso, se recomienda, que las tuberías bajen junto a la pared hasta el piso y luego se distribuyan los cables por el suelo siendo protegidos por accesorios de aluminio o similares que puedan ser retirados para cualquier tipo de reparación. Previo a cualquier tipo de modificación, debe hacerse un análisis de cual sería la mejor distribución posible para evitar la saturación de tuberías y accesorios en el piso.

También debe mencionarse, que es recomendable que las tuberías de desagüe de los equipos de aire acondicionado, sean trasladadas al exterior del edificio y evitar así cualquier tipo de incidente ocasionado por fugas de agua en las tuberías.

35. El centro de cómputo no esta dotado de extractores de aire que expulsen el aire caliente y viciado que se acumula en la parte superior del salón. Esto hace que el aire acondicionado sea menos eficiente y por ende exista una gasto mayor de energía eléctrica.

R. En todo lugar donde existe acumulación de personas y equipos, existe la necesidad de evacuar el aire viciado que se genera de la combinación antes mencionada. Para ello se debe hacer uso de extractores de aire que se encarguen de expulsar el aire caliente para mejorar la eficiencia del aire acondicionado.

Seguros

36. Hasta donde pudo constatarse, la institución no cuenta con ningún plan de seguros de ninguna clase (robo, incendio, terremoto, etc.). Esto significa, que al momento de una catástrofe o accidente, la institución deberá correr con todos

los gastos de recuperación tanto del equipo e instalaciones como de software y programas.

R. Sería una buena política de parte de la institución, contar con un plan de seguros que le proteja contra cualquier tipo de situación. Con esto se puede garantizar que cuando ocurra un desastre se pueda recuperar cuando menos algo de lo perdido. Para ello debe hacerse un análisis previo de que es lo que cubrirá la póliza así como también un inventario del equipo e información que estará incluido. Estos inventarios deben ser actualizados constantemente cuando exista adquisición de equipo o software nuevos.

Aspectos Varios

37. En ninguna parte dentro del centro de cómputo se cuenta con ningún tipo de alarma, ya sea ésta contra robo o incendio o ingreso no autorizado. El área de informática está completamente desprotegida contra cualquier tipo de agresión u accidente fuera de las horas de trabajo.

R. Como ya se mencionó anteriormente en los puntos 22 y 30, se recomienda que se instalen alarmas contra ingresos no autorizados y contra incendio.

38. No existe dentro del centro de cómputo rótulos, carteles u otros avisos que indique las prohibiciones mínimas como lo son no fumar, no bebidas ni alimentos, etc. Existe un pequeño instructivo en la puerta de entrada que no es lo suficientemente visible como para llamar la atención del usuario, por lo que pasa completamente desapercibido.

R. Es necesario contar dentro y fuera del centro de cómputo con carteles que indiquen recomendaciones o prohibiciones de todo tipo, los cuales ayudarán a dar una mejor orientación a las personas que visiten el área de informática. Estos deberán esta colocados en lugares visibles y hechos de tal forma que llamen la atención de las personas, preferiblemente con colores vivos que atraigan la vista.

39. El centro de cómputo no esta dotado de ningún tipo de botiquín o implementos de primeros auxilios, lo que significa, que en caso de emergencia, el lugar más cercano con posibilidad de ayuda está a aproximadamente 500 metros.

R. Como en cualquier centro de trabajo, es necesario que siempre exista un botiquín de primeros auxilios conteniendo por lo menos un mínimo de medicamentos necesarios en cualquier emergencia. Se considera como mínimo, sin limitarse a ello, lo siguiente:

- Alcohol
- Algodón
- Gasas
- Mertiolate
- Analgésico en pastillas, etc.

40. El equipo no esta debidamente protegido contra la posibilidad de un temblor fuerte o terremoto. No existe ningún tipo de accesorio que lo sujete al mobiliario o que evite que el equipo se precipite en caso de un sismo.

R. Es necesario mejorar el mobiliario en donde esta ubicado parte del equipo, ya sea reforzando los resistentes o sustituyendo los actuales por unos nuevos, ya que estos no ofrecen ninguna seguridad en caso de que ocurra algún movimiento telúrico o que por el peso de las mismas máquinas puedan ceder, precipitándose el equipo al suelo.

Seguridad en el Equipo

41. No se realizan, periódicamente, limpiezas del equipo para prolongar su vida útil; y el único mantenimiento que se le da es cuando un equipo sufre alguna falla.

R. Se recomienda que debido a la utilización que se le da a ambos centros de cómputo, y por el ambiente que se tiene en sus alrededores (construcción,

calles de polvo, etc.),se le de mantenimiento periódico al equipo y no esperar hasta que el equipo sufra algún tipo de daño. Dentro de los servicios que se recomiendan (sin limitarse a ellos) están:

- Limpieza del equipo y de cada una de sus partes
- Revisión interna y externa
- Revisión de sus componentes electrónicos

Con este tipo de mantenimiento se garantiza que todas las máquinas estén en buenas condiciones y su durabilidad pueda ser mucho mayor.

42. Para el centro de cómputo de la UDB, se cuenta con cobertores para las máquinas pero no son utilizados, lo que ayuda a la acumulación de suciedad dentro del equipo.

El centro de cómputo del CITT no cuenta con los cobertores necesarios para proteger las máquinas del medio ambiente cuando no están siendo utilizadas.

R. Debe responsabilizarse a una persona para que ésta, al finalizar la jornada de trabajo, ponga a cada máquina su cobertor correspondiente y ayudar así a prolongar la vida del equipo. Actualmente no se hace por negligencia y descuido del personal que esta a cargo, pero es importante que se concientice al

personal de la utilidad de estos cobertores. De igual manera, debe existir un encargado que a la hora de iniciar labores, recoja todos los cobertores y los almacene de una forma ordenada en un lugar preestablecido para ello.

Se recomienda que para el equipo del centro de cómputo de la Universidad Don Bosco, se compren o se fabriquen dichos cobertores, ya que como se indicó anteriormente, en los alrededores del edificio existe acumulación de polvo, construcciones, calles de tierra, etc. que provocan partículas en exceso, que son nocivas para las computadoras y resto del equipo.

43. Se pudo verificar por medio de la examinación de algunas computadoras, que no se realiza limpieza de ningún tipo al equipo. Adicionalmente a esto y debido a la mala ubicación del mismo, no es posible realizar limpieza del mobiliario en que está colocado el equipo lo que colabora a la acumulación de suciedad dañina para el equipo.

R. Es recomendable que se establezca un programa periódico de limpieza del equipo, la cual deberá ser realizada por los encargados del centro de cómputo. Esta deberá ser una limpieza rápida y sencilla, del exterior, teclado, mouse, etc. ya que la limpieza general de la máquina debe estar dentro del contrato de mantenimiento.

También debe de buscarse la forma de organizar mejor el mobiliario, incluyendo cables y equipo, para que cada cierto tiempo pueda hacerse una limpieza del lugar y evitar la acumulación de basura, suciedad y polvo. Esto vendría a mejorar la imagen del área de informática así como también proveería un ambiente de trabajo más agradable.

44. No existen mecanismos que permitan que el equipo se apague cuando éste no se encuentra en uso.

R. Es necesario que las personas que laboran en el centro de cómputo, en especial el del CITT, realicen revisiones constantes para verificar que ninguna máquina quede encendida o funcionado cuando no será utilizada. Con esto se le estará dando un mejor cuidado al equipo y evitará consumo innecesario de energía eléctrica.

45. En el centro de cómputo del CITT, no se verifica que los usuarios no coloquen sobre el equipo, elementos que obstruyan la ventilación dentro del equipo. Esta es una situación que se origina con el hecho de que no existe ningún lugar en el que los usuarios puedan depositar sus pertenencias cuando están utilizando el equipo.

R. Como ya se recomendó anteriormente, es importante que se instale en el centro de cómputo un mueble que permita a los usuarios colocar sus pertenencias cuando están trabajando en las computadoras. De no ser esto posible, por lo menos debe disponerse de una mesa en la que se puedan colocar maletines, bolsas, libros y cuadernos, etc.

Es responsabilidad de los encargados del centro de cómputo velar por la seguridad del equipo, ello incluye revisar que los usuarios no coloquen objetos encima o al lado del equipo donde se obstruya la ventilación o se dañe al equipo de cualquier otra forma.

46. No se tiene un control escrito o bitácora que registre un historial de las fallas ocurridas en el equipo a lo largo de su utilización.

R. Una buena práctica en cualquier centro de cómputo, es llevar un registro de todo mantenimiento, mejora o modificación que sufra el equipo. Para ello se recomienda que se habrá un archivo en el que se lleve una bitácora de trabajos realizados al equipo en el que se debe incluir: fecha del trabajo, equipo al que se realizó el trabajo (número o código), descripción del trabajo realizado, nombre de la persona o empresa que realizo el trabajo, nombre del encargado que recibió el trabajo, recomendaciones.

Para poder llevar una buena bitácora de mantenimiento, es necesario que con anterioridad se codifique el equipo con un número diseñado por los encargados, de tal manera que pueda identificarse fácilmente cada una de las máquinas del centro de cómputo. Podría ser el número de inventario.

47. No se controla bajo ninguna circunstancia el rendimiento del equipo durante su utilización ni se verifica su estado y resultados durante períodos constantes y repetitivos de tiempo.

R. Después de la utilización por períodos largos de un equipo determinado, este tiende a reducir su eficiencia por diferentes motivos. Es conveniente que los encargados estén verificando constantemente si el equipo no ha reducido su efectividad. Para ello deben diseñarse rutinas estándar de trabajo que pongan a prueba el equipo y en base a resultados promedio esperados, comprobar que el equipo sigue funcionado con normalidad. Algunos de los aspectos que se utilizan para medir esta situación son: tiempos de lectura-escritura, de respuesta, resolución del video, etc.

Seguridad del Personal

48. No se realiza ningún tipo de capacitación del personal, con excepción de breves explicaciones del funcionamiento del equipo y algunos programas.

R. La capacitación del personal trae una serie de beneficios que amerítan que se incurra en los gastos que ello representa:

- Mantiene al personal motivado.
- Garantiza que exista un mejor manejo del equipo.
- Hace que el trabajo se realice con mas eficiencia y conocimiento.
- Evita la búsqueda (algunas veces por largo tiempo) de personal con especialización, lo que lo vuelve más caro.
- Puede existir transferencia de conocimientos dentro del mismo personal de la institución. Esto significa que no es necesario capacitar a todo el personal, sino al más calificado quien puede después capacitar al resto de los empleados.

49. No se realizan constantemente, pruebas o exámenes para comprobar la capacidad del personal, especialmente cuando se impartió algún tipo de capacitación.

R. Es necesario que periódicamente se este realizando algún tipo de prueba o examen para poder evaluar el grado de productividad del personal, en esto se debe incluir: manejo del equipo, conocimiento, relaciones laborales, asistencia y puntualidad, etc. Este aspecto se vuelve aún más importante cuando ha

recibido capacitación de parte de la institución, pues entonces se espera que ésta incremente la eficiencia.

Se recomienda que se mantenga en el centro de cómputo una biblioteca completa y actualizada que sirva de referencia al personal que labora en él.

50. No se registra a través de una supervisión el trabajo realizado por el personal durante la jornada de trabajo.

R. Para poder verificar que el personal de informática está realizando su trabajo a cabalidad, se recomienda establecer un método a través del cual se informe al supervisor del trabajo realizado. De esta forma se evitan atrasos innecesarios y cuellos de botella que resultan de no revisar el trabajo hasta que está demasiado retrasado.

Para no provocar inconformidad en el personal por esta medida, el supervisor puede buscar un método informal pero eficaz de medir el trabajo del personal.

51. No existe en toda la institución una persona que pueda reemplazar, aunque fuese temporalmente, al encargado del centro de cómputo de la UDB, lo que puede provocar situaciones extremadamente críticas

Para el centro de cómputo del CITT, en ocasiones se presenta como sustituto, un personero de la Administración del Universidad lo que dista mucho de ser lo más adecuado pues suele ser alguien sin el conocimiento necesario.

R. Bajo ninguna circunstancia es recomendable que se cuente con personal indispensable. Esto quiere decir que siempre debe haber una persona que pueda sustituir, ya sea momentánea o definitivamente, a un empleado que desempeñe un puesto crítico.

Para el centro del CITT lo más indicado es crear turnos de trabajo en los cuales debe existir por lo menos dos personas encargadas del centro de cómputo, de tal manera que si falta uno la otra persona pueda con un poco más de esfuerzo cumplir con la mayoría de las tareas. Esta de más decir que el personal seleccionado deberá estar debidamente capacitado para desempeñar su trabajo.

Como herramienta visual, en la página 41 se presenta una gráfica en la que se representa el porcentaje de riesgos encontrados en la investigación, tomando como un 100% el total de preguntas realizadas en los cuestionarios (222). Dichos porcentajes podrán variar en la medida en que se incrementen o disminuyan las preguntas de los cuestionarios, pero puede obtenerse una buena idea del estado en que se encuentra el o los Centros de Computo.

Para el presente caso de investigación se puede verificar a través de la gráfica No. 9, que los porcentajes de riesgos varían de la siguiente manera:

Riesgo Alto	25%
Riesgo Medio	36%
Riesgo Bajo	13%

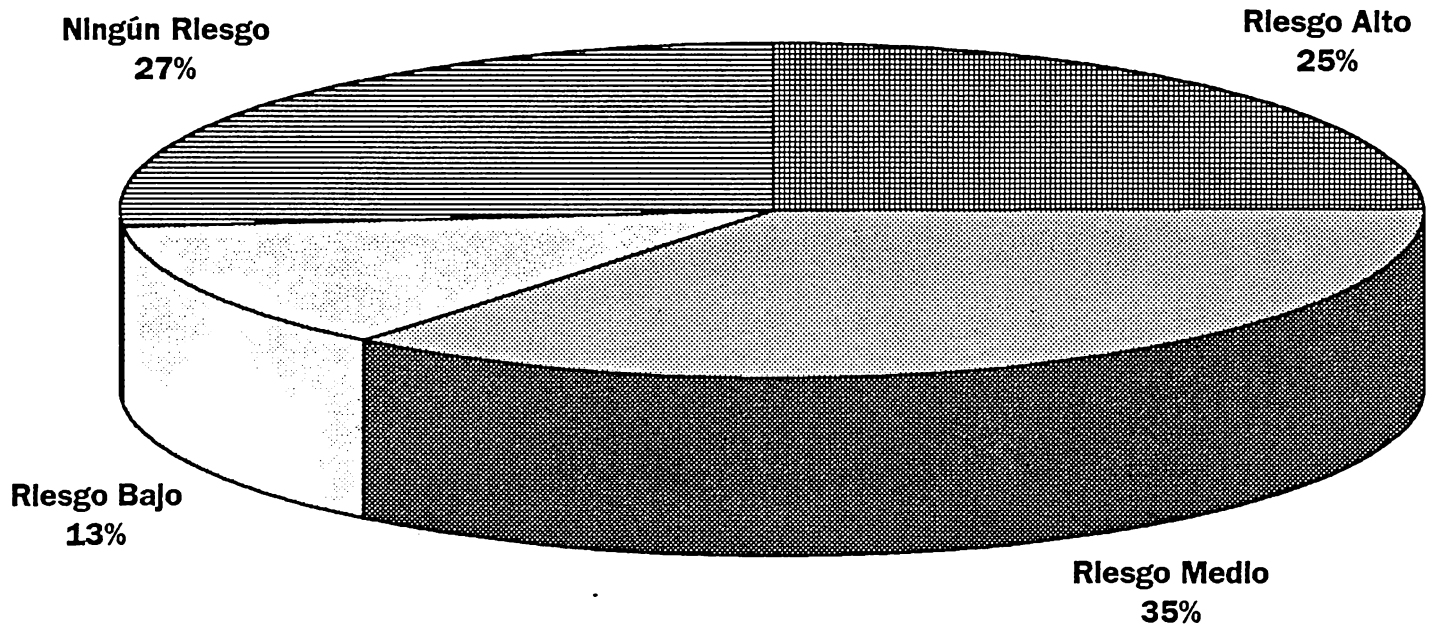
Esto es un buen indicador de que la situación en el Area de Informática de la Universidad Don Bosco dista mucho de ser la ideal.

Como ya se indicó al inicio de este informe, es prioritario que se atiendan primero aquellas situaciones con riesgo alto para proceder después a solucionar las de riesgos medio y bajo.

Gráfico de Riesgos

Auditoría realizada al Area de Informática de la UDB

Porcentaje de Riesgo encontrado de acuerdo
al número de preguntas realizadas



PARTE III

UNA APLICACION PRACTICA EN EL SISTEMA CONTABLE DE LA UNIVERSIDAD DON BOSCO

CAPITULO 11

INTRODUCCION - PARTE III

11. INTRODUCCION - PARTE III

Esta es la última fase del presente trabajo de graduación. En este documento se desarrolla una Auditoría aplicada a un Sistema de Contabilidad utilizado en la Universidad Don Bosco.

Para llevar a cabo dicha Auditoría, se han utilizado algunas de las herramientas explicadas a lo largo del Trabajo de Graduación, el cual ha sido tomado como base para el trabajo de investigación de esta etapa.

Para familiarizarse con el sistema, se da a continuación una descripción histórica del sistema en cuestión, además de otros aspectos relevantes para una mejor comprensión del mismo.

El sistema de contabilidad utilizado por la Universidad Don Bosco es un sistema que ha sido creado de acuerdo a los lineamientos dados por la Congregación Salesiana, incluyendo su sede en Roma. Con esto se desea aclarar, que su desarrollo ha sido normado por la Institución Salesiana y no creado para las necesidades específicas de la Universidad.

El programa contable, objeto de este estudio, ha sido desarrollado para aliviar las necesidades de la Congregación Salesiana en toda Centro América y es utilizado por dicha Institución en toda el área centroamericana con muy pocas diferencias entre uno y otro.

Este programa fue creado en el año de 1990 a iniciativa del Padre Juan Palamini, quien sugirió unificar los sistemas contables en todas las casas Salesianas a nivel de Centro América. Dicho sistema fue desarrollado por el Ing. Manuel Orellana y con la colaboración del Sr. Noel Anaya Gutiérrez, contador del Economato Salesiano e Inspectoría de Centro América quien aporto su experiencia contable dando valiosas recomendaciones durante el desarrollo del proyecto.

Desde su creación, el programa ha sido modificado en varias ocasiones mejorando de esta manera su funcionamiento y adaptándose mejor a los constantes cambios en el medio. También se han realizado pequeñas modificaciones para llenar las necesidades específicas de los usuarios locales.

CAPITULO 12

OBJETIVOS - PARTE III

12. OBJETIVOS - PARTE III

12.1 OBJETIVO GENERAL

Practicar un examen crítico, objetivo e independiente del sistema, a fin de garantizar que los datos generados por los usuarios están siendo procesados correctamente, de que se efectúan las validaciones adecuadas, que la información procesada esta siendo debidamente almacenada y que la información resultante del procesamiento es correcta y satisface los requerimientos del usuario final.

12.2 OBJETIVOS ESPECIFICOS

- Establecer aquellos puntos en donde el programa presenta debilidades y dar las recomendaciones correspondientes para el fortalecimiento del sistema.
- Recomendar la inclusión de nuevos procedimientos que hagan del programa uno más productivo y actualizado.
- Verificar la correcta operación de los programas.
- Comprobar la integridad, disponibilidad y confidencialidad de los datos.

CAPITULO 13

ALCANCE

13. ALCANCE

La presente fase del trabajo se limita a realizar una auditoría a la parte operativa del programa de Contabilidad utilizado por la Universidad Don Bosco.

No debe confundirse con esto que la auditoría se realizará también a la parte lógica y programática del sistema, sino más bien a la forma en que este realiza sus procesos y los resultados que se obtienen de los mismos.

Por razones de tiempo, la parte de la revisión de los programas con sus rutinas, variables, campos, etc. se deja para futuras auditorías en las que se debe analizar a profundidad y como un todo, el sistema en mención.

CAPITULO 14

FUNCIONAMIENTO DEL SISTEMA

14. FUNCIONAMIENTO DEL SISTEMA

Cabe mencionar que el Sistema Contable desarrollado para la Congregación Salesiana llena los requisitos necesarios para ser un Sistema funcional y efectivo, cumpliendo con los objetivos para los que fue diseñado. Pudo verificarse que: el sistema produce resultados razonables, que satisface la mayoría de necesidades del usuario, que desarrolla los procesos de manera exitosa y que a pesar de haber sido probado bajo situaciones adversas cumple con los requerimientos de funcionamiento esperados. También es importante mencionar, que el programa ha sido diseñado de tal manera que pueda ser modificado cuando así se necesite y que su flexibilidad le permite adaptarse a las demandas del medio.

A pesar de lo anteriormente expuesto, se pudieron detectar una serie de situaciones que pueden ser mejoradas y con el único objetivo de optimizar el sistema, se presentarán más adelante dichas situaciones con su respectivo análisis.

Se desea aclarar que únicamente se plantean los puntos en los que se encontró debilidad o deficiencia. Para todos aquellos aspectos que se aprecian en los menúes y que no son mencionados en el presente informe,

deberá entenderse que no se encontró ningún aspecto negativo respecto a ellos y que están funcionando de la manera esperada.

Antes de dicho análisis, se presenta a continuación y en forma general, el funcionamiento del sistema. No se harán explicaciones detalladas salvo en aquellas situaciones que lo ameriten.

Al iniciar la ejecución del sistema, este solicita al usuario una clave o password, con el que se da acceso al menú principal del mismo.

El programa esta diseñado utilizando el método de menúes o paneles, en los cuales se escoge una opción que conduce a la parte operativa de la opción seleccionada o en su caso, a otro menú de opciones.

El menú principal (Gráfica No.10) está compuesto por las siguientes opciones:

1. LIBRO MAYOR
2. MENU DE PARTIDAS
3. SALIRSE DEL SISTEMA
4. ACTUALIZACION
5. REPORTES FINANCIEROS
6. UTILITARIOS

Aconme1 Conme01
UNIVERSIDAD DON BOSCO '95

S I S T E M A D E C O N T A B I L I D A D

1. L I B R O M A Y O R
2. M E N U D E P A R T I D A S
3. S A L I R S E D E L S I S T E M A
4. A C T U A L I Z A C I O N
5. R E P O R T E S F I N A N C I E R O S
6. U T I L I T A R I O

Oprima el número correspondiente a su selección ...

GRAFICA Nº 10

Con el fin de no alargar más de lo debido la explicación de cada opción, se presenta en la sección de anexos, las pantallas respectivas utilizadas en cada una de las opciones mencionadas anteriormente. Solamente se hará una breve mención del funcionamiento de cada una de las opciones.

1. LIBRO MAYOR

Este menú es utilizado para manejar todo lo relacionado con el catalogo de cuentas y los saldos de las mismas. Es en esta opción donde pueden añadirse, modificarse, eliminarse y consultar las cuentas siempre y cuando se respeten los principios de contabilidad generalmente aceptados. Esto significa por ejemplo: a. Solo pueden modificarse el nombre, el tipo de saldo y el tipo de cuenta, b. Solo pueden eliminarse aquellas cuentas que su saldo sea cero y que no hayan registrado movimientos durante el período contable. etc.

El menú de esta opción puede verse en la Gráfica No. 11

Aconme2 Conme02
UNIVERSIDAD DON BOSCO '95

M E N U L I B R O M A Y O R

1. Mantenimiento Libro Mayor
2. Impresión de Saldos del Mayor y Aux.
3. Regresar al Menú Anterior
4. Impresión Catálogo de Cuentas
5. Inicializar Mes
6. Inicializar Año
7. Consulta Estados de Cuentas
8. Acumulaciones Mensuales por Cuenta
9. Consulta de Saldos del Mayor

Oprima el número correspondiente a su selección ...

GRAFICA Nº 11

2. MENU DE PARTIDAS

Esta parte se refiere al manejo de partidas y todo lo relacionado con ellas, consulta, ingreso, modificación y eliminación.

De acuerdo a la filosofía utilizada por el programa, el proceso de partidas se hace a través de lotes, lo que dicta el funcionamiento del programa a este respecto. Por esto mismo, solamente puede modificarse y eliminarse aquellas partidas que no han sido actualizadas; y solo puede consultarse las que ya lo fueron.

Esta opción además presenta otros dos sub-menúes que son utilizados para la generación de cheques y conciliaciones.

El menú de esta opción puede verse en las gráficas 12, 13 y 14

3. SALIRSE DEL SISTEMA

Esta opción sirve para abandonar el programa. De igual forma, en los demás menúes encontrados en el sistema, se utiliza el mismo número para salirse de la opción en que se encuentra. (opción 3)

Aconme3 Conme03
UNIVERSIDAD DON BOSCO '95

M E N U D E P A R T I D A S

1. Consulta de Partidas
2. Ingreso de Partidas
3. Regresar al Menú Anterior
4. Modificación de Partidas
5. Eliminación de Partidas
6. Impresión Part. no Actualiz.
7. Consulta de partidas ya Act.
8. Menú de Cheques
9. Menú de Conciliaciones

Oprima el número correspondiente a su selección ...

GRAFICA Nº 12

Aconme1 Conme11
UNIVERSIDAD DON BOSCO '95

M E N U D E C H E Q U E S

1. Emisión de Cheques
2. Emisión de Cheques con formato
3. Regresar al Menú Anterior
4. Hacer copias de Partidas
5. Estados Ctas. por actualizar

Oprima el número correspondiente a su selección ...

GRAFICA Nº 13

Aconm12 Conme12
UNIVERSIDAD DON BOSCO '95

MENU DE CONCILIACIONES

1. Consulta de Partidas
2. Impresión de Partidas
3. Regresar al Menú Anterior
4. Modificación de Partidas
5. Consulta Estados de Cuentas
6. Impresión Estados de Cuentas
7. Transferir partidas del mes
8. Cargar Cheques de Planilla
9. Cargar Partidas de Colecturía

Oprima el número correspondiente a su selección ...

GRAFICA Nº 14

4. ACTUALIZACION

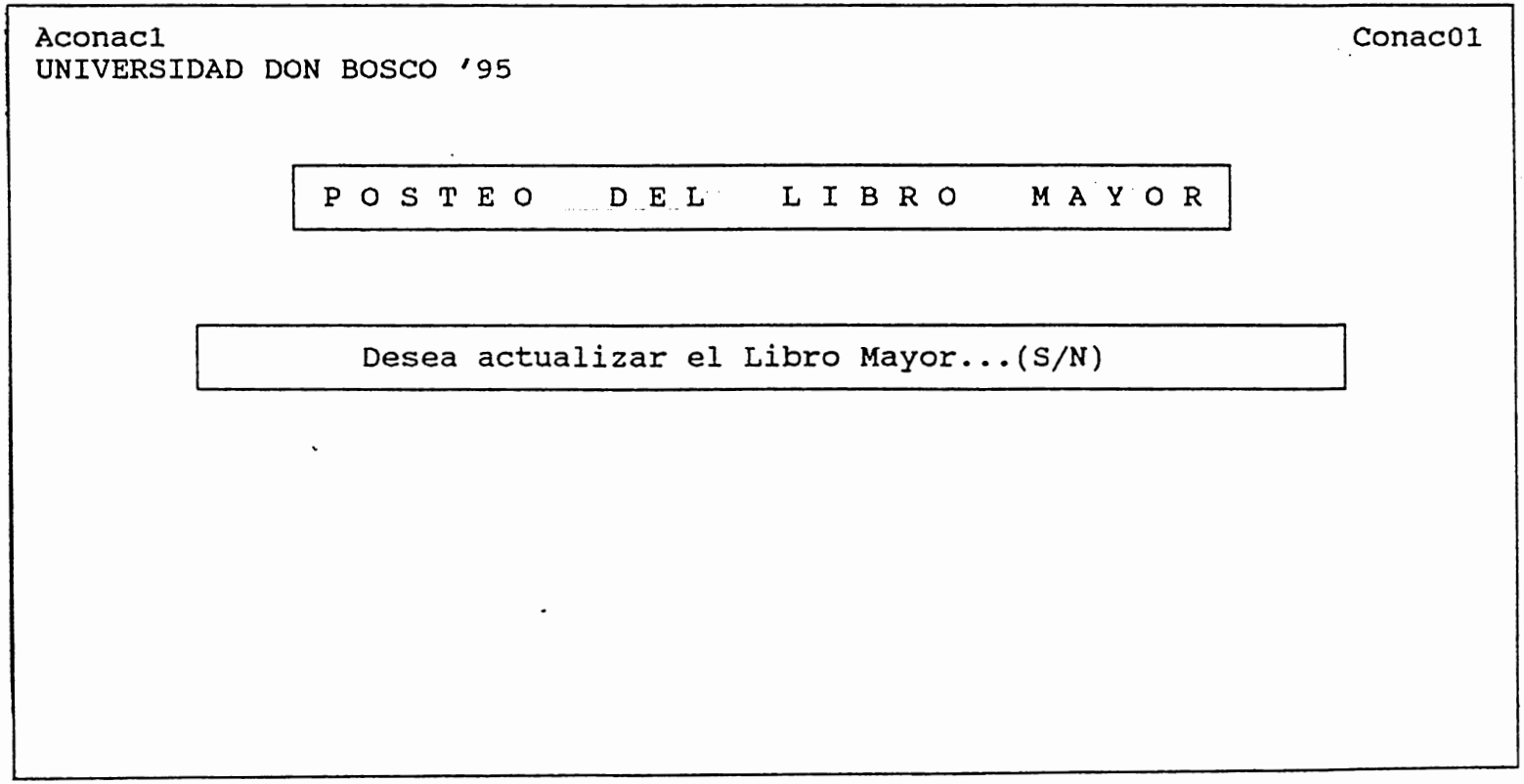
La función de esta opción es actualizar (postear) todos los movimientos registrados en el lote de partidas, en el libro mayor. Este proceso además traslada los movimientos a otro archivo en el que se lleva un registro histórico para poder ser consultados en períodos diferentes al actual.

El menú de esta opción puede verse en la Gráfica No. 15

5. REPORTES FINANCIEROS

Esta opción describe todos los reportes que pueden ser obtenidos del sistema. Al ingresar a ella se presenta un listado de los informes financieros que pueden ser impresos con la información contable ingresada al sistema.

El menú de esta opción puede verse en la Gráfica No. 16



GRAFICA Nº 15

Aconme4 Conme04

UNIVERSIDAD DON BOSCO '95

R E P O R T E S F I N A N C I E R O S

1. Balance de Comprobación
2. Balance General
3. Regresar al Menú Anterior
4. Estados de Cuentas
5. Cuadro Comparativo de Gastos
6. Estado de Pérdidas y Ganancias
7. Impresión Partidas Actualiz.
8. Presupuesto de cuentas
9. Saldos del Presupuesto

Oprima el número correspondiente a su selección ...

GRAFICA Nº 16

6. UTILITARIOS

Esta es la última opción del menú principal en la cual aparecen una serie de procedimientos complementarios para el sistema contable. Algunos de los puntos relevantes en este menú son el mantenimiento de fechas que se utiliza para indicar los períodos mensuales que tendrá el año contable. También aparece una opción que sirve para inicializar el año contable, en la que se trasladan todos los saldos al nuevo año y se dejan a cero todas las cuentas de gastos.

El menú de esta opción puede verse en la Gráfica No. 17

Aconme7 Conme07

UNIVERSIDAD DON BOSCO '95

M T T O. D E A R C H I V O S

1. Mantenimiento Fechas
2. Mtto. Nombres Casas Salesianas
3. Regresar al Menú Anterior
4. Fecha inicio periodo contable
5. Mtto. clave de Ingreso al Sistema
6. Backup de Archivos de Datos
7. Recuperar Archivos de Datos
8. Reindexar las bases de datos
9. Actualizar correlativo de partida

Oprima el número correspondiente a su selección ...

GRAFICA Nº 17

CAPITULO 15

ANALISIS DEL FUNCIONAMIENTO DEL SISTEMA E INFORME DE AUDITORIA

15. ANALISIS DEL FUNCIONAMIENTO DEL SISTEMA E INFORME DE AUDITORIA

Para poder conocer de la mejor manera posible el funcionamiento del sistema, se dividió el análisis en dos etapas:

1. Se instaló el programa en una computadora para poder partir de cero. Se le dieron saldos iniciales y se siguió un proceso contable para un período de 4 meses ingresando una serie de partidas y procesándolas por lotes teniendo siempre el cuidado de utilizar el Catálogo de Cuentas diseñado para la Universidad.

   Con el fin de analizar detalladamente el funcionamiento del programa, en esta etapa se solicitó la ayuda de un Contador ajeno a la universidad a quien se le explicó las bases del sistema y se le dio el catálogo de cuentas para que pudiese ingresar la información que él considerara pertinente.

2. Se llevó a cabo una investigación de campo, realizando varias visitas al departamento de Contabilidad de la UDB y viendo el programa en su funcionamiento diario. De esta forma también se logró aclarar las dudas

que habían surgido en la primera etapa del análisis. Para ello se contó con la colaboración del contador de la Universidad.

Después de haber estudiado lo más detenidamente posible el funcionamiento del programa, se procedió a determinar aquellos puntos en que se consideró necesaria una mejora o modificación debido a fallas o faltas en algunos procesos. También se tomo en cuenta las opiniones vertidas por ambos contadores.

Antes de proceder a enumerar los puntos en que se cree necesario un cambio, se desea aclarar que el programa cumple con los objetivos planteados por la Institución y que las modificaciones aquí mencionadas son únicamente con el objetivo de mejorar y hacer más eficiente el sistema.

Para poder mantener una secuencia en el desarrollo de esta Auditoría, se enumerarán los puntos de acuerdo al orden seguido por los menúes del programa (ver anexos) iniciando de esta manera con 1. LIBRO MAYOR y sus sub-menúes, para finalizar con 6. UTILITARIOS.

Para un mejor entendimiento del Análisis realizado, se ha estructurado la exposición de la siguiente manera:

1. MAYUSCULAS Menú al que corresponde el Análisis

1. Minúsculas Opción del menú a la que se hace referencia

"•" Punto en que se encontró un problema o debilidad.

"**R**" Recomendación que se hace al punto expuesto.

1. LIBRO MAYOR

1. Mantenimiento del Libro Mayor

- Cuando se desea hacer algún tipo de modificación que no es permitida en alguno de los campos desplegados en pantalla, no existe ningún tipo de mensaje que indique que no es posible corregir o modificar dicho campo. De igual manera, cuando se ingresa en el campo de opción cualquier otro número o carácter que no esta dentro del rango de opciones, no se despliega ninguna información. (Ver Gráfica No. 18)

R. Debería incluirse dentro del programa, rutinas que desplieguen pequeños mensajes de aclaración al usuario cuando este ingresa una opción no permitida.

```
Aconmt1                                                          Conmt01
UNIVERSIDAD DON BOSCO '95

      Adición      Consulta     Eliminación  Modificación Salirse

        1. Código de Cuenta ....:   - - -    -
        2. Nombre de la Cuenta .:
        3. Tipo de Saldo .......:            D. Débito  C. Crédito
        4. Tipo de Cuenta ......:            A. Activo  P. Pasivo
        5. Saldo inicio año ....:
        6. Saldo Mes Pasado ....:
        7. Cargos ..............:
        8. Abonos ..............:
        9. Cambio Neto .........:
       10. Nuevo Saldo .........:
       11. Ultima fecha Actuali.:            (dd/mm/aa)
       12. Saldo presupuestado..:

                  Datos Correctos (S/N ó #):
```

GRAFICA Nº 18

2. Impresión de Saldos del Mayor y Auxiliar

- En esta opción y en todas las relacionadas con impresión, si el impresor es apagado o interrumpido por algún motivo, el programa se aborta.

R. Se debería de incluir una validación que verifique el estado del impresor en cualquier momento de la rutina de impresión de tal manera que pueda regresarse al programa si no puede seguirse imprimiendo.

7. Consulta de Estado de Cuentas

- En esta opción, al inicio el programa pide al usuario que ingrese el período para el cual desea consultar los Estados de Cuentas; la fecha es ingresada en el formato "dd/mm/aa". Cuando el Estado es desplegado, la fecha esta cambiada de formato de la forma "mm/dd/aa", lo que puede confundir al usuario (Ver Gráficas No 19 y 20).

R. Corregir la forma en que es desplegada la fecha o período.

Aconco3 Conco03
UNIVERSIDAD DON BOSCO '95

E S T A D O S D E C U E N T A S

CUENTA A CONSULTAR : 10-01-02- -
CAJA CHICA

PERIODO FECHA A CONSULTAR:

DESDE : 01/03/95 (dd/mm/aa)

HASTA : 31/03/95 (dd/mm/aa)

Datos correctos (S/N) o Regresar (R) :

GRAFICA Nº 19

UNIVERSIDAD DON BOSCO '95 PAG. N.: 1
CUENTA : 10-01-02 CAJA CHICA
DESDE .: 03/01/95 HASTA .: 03/31/95

FECHA	PARTIDA	CONTRACTA	C A R G O	A B O N O
01/03/95	3	10-02-01-001-	1,000.00	
Valor fondo fijo				
11/03/95	16	30-01-05- -	10.00	
pago de papeleria eventual				

SALDO INICIAL	TOTAL CARGOS	TOTAL ABONOS	CAMBIO NETO	NUEVO SALDO
	1,010.00		1,010.00	1,010.00

Oprima... C : Otra Cta. A : Adelanta B : Atras I : Inicio F : Final

GRAFICA Nº 20

- Otra situación que se da en esta opción es que después de haber ingresado el Número de Cuenta para el que se desea obtener el Estado, no es posible regresar al inicio o abandonar el proceso en caso de haber cometido un error al digitar la cuenta.

R. Debería incluirse para todo proceso, una rutina que permita abandonar la opción en que se encuentra en ese momento, sin afectar el funcionamiento normal del programa.

- Existe otro problema cuando se quiere hacer consultas de saldos. El saldo solamente se puede observar cuando las partidas son actualizadas. Un problema que podría repercutir dentro de esta situación, es que no existe forma de conocer las disponibilidades de la institución. Ej.: Saldo de una cuenta bancaria después de "x" número de transacciones. Actualmente, el control de las disponibilidades se lleva a través de una hoja electrónica en la que se registran los cheques y retiros y se ingresan los depósitos o remesas.

R. Debería existir una opción que permita consultar saldos de forma inmediata sin importar si las partidas han sido o no actualizadas.

- Cuando se consulta el estado de cuentas, si el campo de la descripción de la transacción es demasiado extenso, ésta se extiende hasta llegar a la misma altura en que se despliegan los saldos (campos de cargos y abonos), lo cual tiende a confundir un poco al usuario.

R. Debe controlarse en el campo de despliegue de descripciones, hasta que columna deberá de llegar el texto desplegado para que este no se monte sobre los demás campos.

2. MENU DE PARTIDAS

1. Consulta de Partidas.

R. Debería aclararse para esta opción que se trata únicamente de consulta para partidas no actualizadas (Ver Gráfica No. 12).

2. Ingreso de Partidas

- Cuando se esta ingresando los movimientos de las partidas, una vez ha sido digitado el número de cuenta para un movimiento, no es posible eliminar por completo esa transacción. Esto hace el programa demasiado

rígido y no deja al usuario la posibilidad de cometer errores que puedan ser corregidos sin tener que elaborar una contrapartida.

A este mismo respecto, tampoco es posible abandonar la partida en proceso sin importar hasta donde se ha llegado, es necesario terminarla y cuadrarla (Ver Gráfica No. 21).

R. Si bien es cierto que la partida puede ser eliminada después de haber sido creada, debería existir la posibilidad de anular o eliminar una transacción en caso de que no sea deseada sin tener que salirse de esa opción del menú para entrar a otra. También debería poder eliminarse un movimiento sin tener que eliminar la partida; esto siempre y cuando la partida se deje cuadrada.

También debería poderse abandonar el proceso de ingreso de partidas en determinado momento, sin tener que finalizar esta.

La contabilidad está actualizada hasta el 16/03/95

I N G R E S O D E P A R T I D A S

1 9 9 5

Numero de Partida : 25	Fecha de Partida : 22/03/95 (dd/mm/aa)	M A R Z O
# CODIGO CTA. C O N C E P T O	D E B E	H A B E R
1 10-01-02- - CAJA CHICA		
	CONCTA: - - - -	

GRAFICA Nº 21

- El programa permite que se ingresen partidas con fecha futura a la fecha actual (entiéndase por actual del día en que se esta trabajando).

R. Después de consultar con ambos Contadores, se llegó a la conclusión de que no debería permitirse ingresar partidas con fechas futuras debido a que se origina un desorden tanto a nivel de número correlativo de partidas como a nivel de fechas. Por ello, si es necesario efectuar un movimiento previo a su fecha de realización, se recomienda que el Contador tenga el cuidado de ingresarlo en la fecha en que se llevará a cabo la transacción.

R. Otra recomendación para el Ingreso de Partidas es que pueda consultarse, por medio de la pantalla, el Catálogo de Cuentas al momento que se están ingresando transacciones. De esta manera se evita la pérdida de tiempo del usuario de tener que buscar en un catálogo impreso alguna cuenta.

6. Impresión de Partidas No Actualizadas

- El proceso de impresión de las partidas que aún no han sido actualizadas, no permite al usuario la posibilidad de imprimir una o un rango determinado de partidas, es decir, que al entrar a este proceso deberán imprimirse todas las partidas que aún no han sido actualizadas. Esto en determinado caso significan gasto de papel, recurso de máquina y tiempo.

R. Al igual que para el proceso de impresión de partidas ya actualizadas, debería incluirse una opción que de al usuario la libertad de imprimir solamente las partidas que se necesiten.

- En esta opción de impresión no existe una alternativa que permita cancelar el proceso de impresión.

R. Incluir dicho proceso.

8. Menú de Cheques

4. Hacer Copias de Partidas

- Esta opción estaba diseñada para poder copiar en un disco flexible las partidas relacionadas con la elaboración de cheques, pero dicha opción no funciona.

R. Corregir la rutina o en caso de que no sea necesaria, eliminarla.

5. Estado de Cuentas por Actualizar

- Si no existe ninguna partida sin actualizar, el proceso manda a impresión solamente el encabezado del Estado de Cuentas.

R. En el caso de que no existan partidas sin actualizar, debería desplegarse un mensaje que informe al usuario la inexistencia de partidas para después sacarlo del proceso sin que deba de imprimirse nada.

5. REPORTES FINANCIEROS

- De forma general, en esta sección del programa, no existe la posibilidad de consultar ningún reporte por medio de la pantalla. Si se necesita saber alguna información de los reportes, debe de mandarse a impresión para después consultarse. Nuevamente el programa se vuelve rígido sin la posibilidad de enmendar errores antes de imprimir.

R. Debería poder consultarse cualquier Reporte Financiero a través del monitor antes de mandar su impresión.

- Cuando se manda la impresión de algún reporte financiero y por algún motivo existe una interrupción (Ej.: corte de energía, atascamiento de papel, etc.), no puede imprimirse solamente la parte faltante del Estado Financiero, es necesario volver a imprimir todo el informe. O si solamente se necesita una parte específica del Informe, tampoco es posible obtenerla sin imprimirlo por completo.

R. Debería poderse controlar el número de páginas de un informe al momento de impresión.

1. Balance de Comprobación

- Al momento de imprimir dicho balance, lo hace comenzando con las sub cuentas para posteriormente imprimir la cuenta de mayor (Ver Gráfica 22).

R. De acuerdo a los principios de contabilidad, los Informes Financieros deben imprimirse iniciando con las cuentas principales, luego las de mayor, luego las subcuentas y así sucesivamente. Debe corregirse esta situación.

B
UNIVERSIDAD DON BOSCO ¶

DEPTO. DE SISTEMAS

B A L A N C E D E C O M P R O B A C I O N¶

22/03/95 AL : 16/03/95

C U E N T A	NOMBRE DE LA CUENTA	NIVEL 5	NIVEL 4	NIV
10-01-02	CAJA CHICA			1
10-01	CAJA			
10-02-01-001	CUENTA CORRIENTE		4,905.25	
10-02-01-002	CUENTA DE AHORRO		500.00	
10-02-01	BANCO CUSCATLAN			5
10-02-02-001	CUENTA CORRIENTE		800.00	
10-02-02	BANCASA			
10-02-03-001	CUENTA CORRIENTE		1,500.00	
10-02-03	AHORROMET			1
10-02-04-001	CUENTA CORRIENTE		1,200.00	
10-02-04	BANCO DE DESARROLLO E INVERSIONES			1
10-02	BANCOS			
10	DISPONIBLE			
12-01-05	LIBRERIAS			1
12-01	CLIENTES			
12	CUENTAS POR COBRAR			
14-02	DEUDORES PERSONALES			

GRAFICA Nº 22

4. Estados de Cuenta

- No aparece al momento de mandar a imprimir el mensaje "oprima x para cancelar la impresión"

R. Validar para esta opción, de la misma forma que en las otras, la rutina para cancelar la impresión.

6. UTILITARIOS

1. Mantenimiento de Fechas.

- Esta opción es utilizada para indicar al sistema los períodos mensuales que comprenderá el año contable (Ver Gráfica No. 23). El problema que se detectó es que el programa permite que dos períodos distintos estén traslapados, así:

Enero	01/01/95	**15/02/95**
Febrero	**01/02/95**	28/02/95

Esto indica que para dos períodos distintos, existirán los mismos días, lo cual no es permitido por los principios de contabilidad.

```
Aconmt2                                                          Conmt02
UNIVERSIDAD DON BOSCO '95

                Consulta      Modificación Salir

          #  M E S              D E S D E    H A S T A
          1. Enero .........:    01/01/95     15/02/95
          2. Febrero .......:    01/02/95     28/02/95
          3. Marzo .........:    01/03/95     31/03/95
          4. Abril .........:    01/04/95     30/04/95
          5. Mayo ..........:    01/05/95     31/05/95
          6. Junio .........:    01/06/95     30/06/95   Formato (dd/mm/aa)
          7. Julio .........:    01/07/95     31/07/95
          8. Agosto ........:    01/08/95     31/08/95
          9. Septiembre ....:    01/09/95     30/09/95
         10. Octubre .......:    01/10/95     31/10/95
         11. Noviembre .....:    01/11/95     30/11/95
         12. Diciembre .....:    01/12/95     31/12/95

              Datos Correctos (S/N ó #):
```

GRAFICA Nº 23

R. Debe hacerse una rutina de validación en la que se verifique que no pueden haber períodos traslapados.

5. Mantenimiento de Clave de Acceso

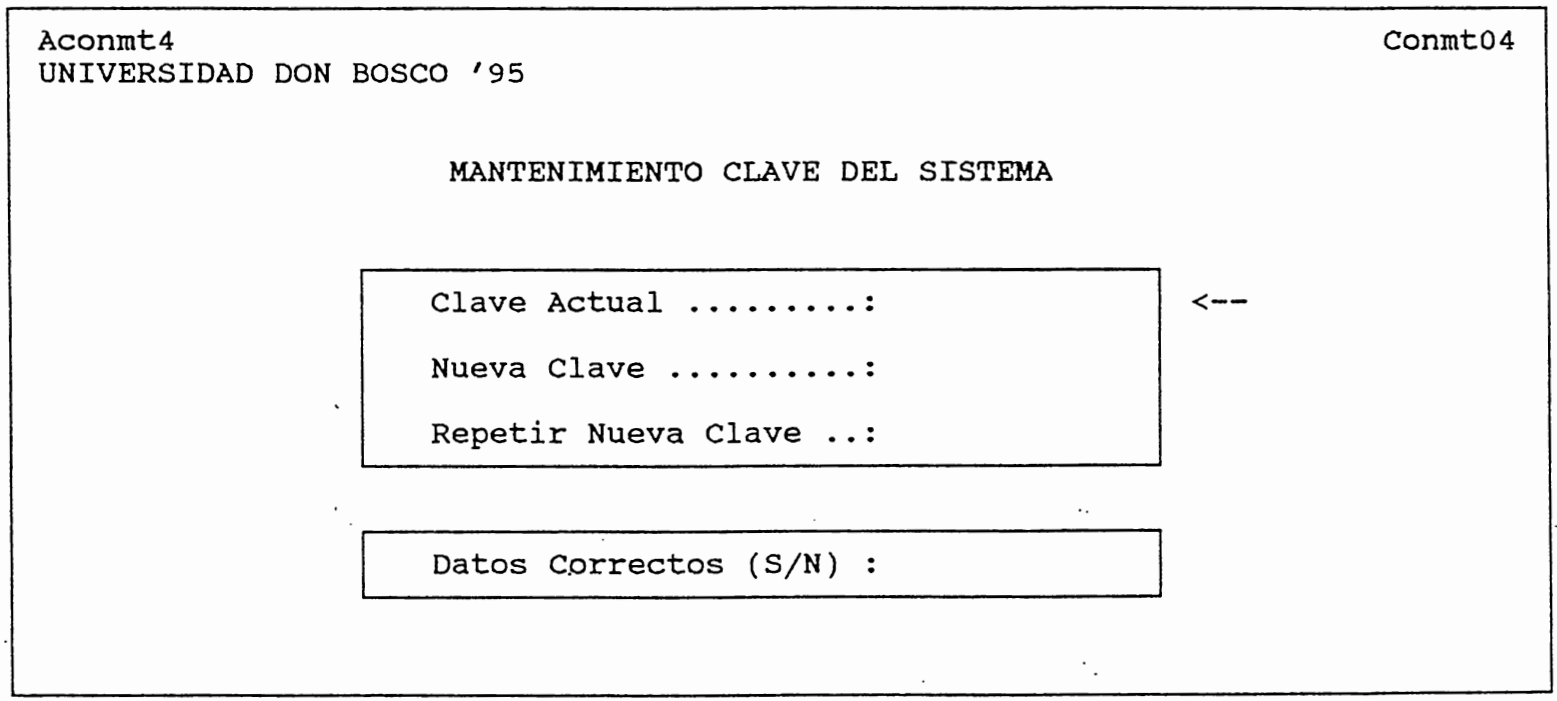
- El sistema permite al usuario cambiar su clave de acceso en cualquier momento, lo que presenta un riesgo de seguridad (Ver Gráfica No. 24).

R. Solamente el administrador de la red o del sistema debería tener acceso para cambiar la clave de cada usuario.

6. Backup de Archivos

- Esta función esta diseñada para hacer copias de respaldo los archivos importantes del sistema, pero la opción no funciona, es decir, no hace las copias de respaldo. Además, al finalizar el proceso manda el mensaje "COPIA DE RESPALDO HECHA SATISFACTORIAMENTE", incluso, aunque no exista diskette en el drive (Ver Gráfica No. 25).

R. La recomendación inmediata es que se corrija dicha opción y que se deje funcionando. En caso de que no fuese necesaria dentro de este proceso, debería eliminarse la opción del menú.



GRAFICA Nº 24

Desea hacer el Backup a disco flexible en el Drive A : (digite S o N)

Copia de respaldo hecha satisfactoriamente

Oprimar cualquier tecla para continuar ...

GRAFICA Nº 25

7. Recuperación de Archivos.

- Si se inserta en el drive un diskette que no contenga los archivos de respaldo, a pesar de que no hace la transferencia, aparece el mensaje "COPIA DE RECUPERACION SATISFACTORIA" (Ver Gráfica No. 26).

R. Dicho mensaje debería aparecer únicamente en el caso de que dicha recuperación sea valedera y satisfactoria verdaderamente. Debe verificarse que la rutina cumpla con su objetivo y no despliegue el mensaje sin importar cual fuese el resultado.

Desea Recuperar Archivos desde el Drive 'A'...: S (digite S o N)

Insert backup diskette 01 in drive A:
Press any key to continue . . .

Copias recuperadas satisfactoriamente

Oprima cualquier tecla para regresar ...

GRAFICA Nº 26

GENERALIDADES

A. En la mayoría de procesos del sistema, no existe la posibilidad de abandonar dicho proceso cuando el usuario así lo decida. Ya sea partidas, consulta de cuentas, ingreso de cheques, etc.

R. Debería incluirse una rutina dentro de todos los procesos interactivos que permita al usuario salirse de la opción en que se encuentre trabajando sin afectar el funcionamiento normal del sistema. Una buena práctica es utilizar la misma alternativa para todas las situaciones en que se amerite esta modificación.

B. Para el funcionamiento del sistema, es necesario que exista una copia de Fox instalada en la máquina en que se esta trabajando. Además deben estar los programas fuentes que hacen funcionar al sistema. Esto presenta un alto riesgo de seguridad bajo cualquier punto de vista. El programa puede ser copiado y robado para ser utilizado por terceras personas; también permite que cualquier persona con conocimientos de programación, específicamente del lenguaje Fox, modifique los programas fuentes con cualquier fin.

R. La nuevas versiones de Fox, permiten al programador que elabore programas ejecutables que no pueden ser modificados o que al menos reducen en un

gran porcentaje la posibilidad de que esto suceda. Además no es necesario de que una copia de Fox este instalada permanentemente dentro del disco para hacer que el programa funcione.

C. El sistema esta diseñado de tal manera que cualquier usuario con conocimiento de la clave de acceso pueda manejar el programa. No existen dentro del mismo sistema, niveles de acceso para las diferentes opciones que presentan los menúes. Esto indica que cualquier usuario que sepa utilizar el sistema puede obtener una copia de los balances o una persona no autorizada pueda entrar al menú de partidas y eliminar cualquiera de ellas (siempre que no hayan sido actualizadas), etc.

R. Es recomendable que el sistema cuente con algunos niveles de validación para aquellas operaciones más delicadas, como pueden ser los Reportes Financieros, las Partidas, y si así se desea, niveles para consultas. Es decir, en determinado momento podría darse que solo el Administrador General esté autorizado para eliminar una partida o agregar una nueva cuenta al Catálogo de Cuentas, para lo que es necesario validar diferentes niveles de acceso al sistema.

D. Como ya se mencionó, el sistema ha sido modificado en distintas oportunidades desde su creación, pero en el manual que existe de dicho sistema, no se ha dejado constancia de ninguna de ellas.

R. Para no perder el control de lo que se ha efectuado, sería conveniente que cada vez que se hace alguna modificación, adición o actualización al sistema, se deje por escrito e incluido en el manual, una descripción detallada de lo que se ha realizado, indicando: a. Como estaba antes, b. Cual es la modificación y c. Como funcionará a partir de dicho cambio.

E. Después de revisar el manual del sistema, existe un capítulo en el que se detallan los requerimientos del equipo, pero en ellos no se menciona nada acerca del impresor necesario o de los requisitos mínimos que debe cumplir el impresor que se ha de utilizar. Para el caso, se hicieron las pruebas de impresión en 4 impresores diferentes, en los cuales se pudo observar que no todos ellos funcionan para obtener los reportes del sistema.

R. Debería incluirse en el manual y en el mismo capítulo de "Requerimientos del Equipo" una cláusula que explique que tipos de impresores pueden utilizarse con el sistema o cuales son los requisitos que éste debe cumplir para obtener reportes de buena calidad.

RECOMENDACIONES EXTRAS

Las recomendaciones que se exponen a continuación son el resultado de opiniones expresadas por el personal que maneja el sistema dentro de la Universidad. Después de analizar todas las requisiciones del departamento de contabilidad se llegó a la conclusión que algunas de ellas podrían ser implementadas para hacer el sistema más eficiente y optimizar el recurso humano con que cuenta el departamento, ahorrando tiempos engorrosos de operaciones que aun se realizan manualmente.

1. Al sistema contable podría incluírsele un sub sistema que controle la facturación de la Universidad, que automáticamente actualice el sistema contable. La Universidad Don Bosco realiza facturación para los cursos técnicos individuales y para una línea de producción de piezas mecánicas.

2. No se encontró implementado dentro del sistema un sub sistema que lleve el libro de IVA, que ya podría estar incluido dentro del mismo programa para hacerlo más eficiente.

3. Debido a la cantidad de personal que maneja la Universidad y que es procesada a través del sistema de contabilidad, se recomienda que se incluya dentro del cierre de todo período, un proceso que calcule las retenciones que

se han realizado al personal y que imprima un reporte al final del año para que estas puedan ser entregadas a todo aquel que las solicite. Debe tomarse en cuenta que este es un requisito legal que tiene la Institución para con todo aquel que recibe remuneraciones en concepto de salarios, honorarios, etc., y que hacerlo manualmente requiere de una gran cantidad de tiempo, que podría utilizarse mas eficientemente si existe un sistema automatizado para ello.

4. Se pudo verificar la existencia de un programa de Planillas. Como recomendación, podría mencionarse la conveniencia de incluir una rutina que llame a dicho programa desde el sistema contable. Si bien es cierto que puede transferirse información de un programa a otro, es necesario abandonar el sistema contable para trabajar en la planilla. Una buena práctica sería que estuviera incluido dentro de una de las opciones del menú principal.

CAPITULO 16

CONCLUSIONES - PARTE III

16. CONCLUSIONES - PARTE III

1. Como se describió a lo largo del presente trabajo de graduación, es indispensable que la Auditoría forme parte del proceso de desarrollo de sistemas desde su inicio, nunca perdiendo de vista el principio de independencia que debe respetar todo Auditor. Con esto se puede garantizar que el proceso cuente con los controles necesarios para funcionar de una manera más eficiente. Esto es particularmente importante cuando el sistema en cuestión procesa información crítica para la institución interesada.

2. Se pudo verificar que la Auditoría de Sistemas juega un papel importante en todas las fases de un Sistema de Información, ya sea en sus inicios, en su desarrollo o en su funcionamiento. Los controles que se establecen a través de una Auditoría sirven para optimizar los recursos del área auditada, pero no solo se trata de establecer los controles, sino más bien de velar por el cumplimiento de los mismos, aportando todas las herramientas necesarias para hacer que estos controles sean tanto objetivos como eficientes.

3. A través de un correcto acercamiento entre el Auditor y la parte auditada, puede lograrse que la comunicación entre ambos sirva de herramienta al auditor y de apoyo al auditado. Después de todo, las personas que están en constante interrelación con el sistema son la mejor fuente de información para detectar los puntos que pueden estar dando problemas con un sistema determinado. Además de ello, el usuario suele ser un buen aportador de ideas (en forma general) que sirvan para hacer un sistema más eficiente.

4. Al momento de efectuar una Auditoría a un Sistema Específico, la documentación del mismo se vuelve una parte vital del proceso de Auditoría, pues en ella se ven plasmados los efectos del tiempo en el desenvolvimiento del sistema. Cuando no se cuenta con dicha documentación, se carece de la evidencia necesaria para elaborar un dictamen certero y apegado a la realidad. En este caso se observa la necesidad de contar como un Anexo al manual del sistema con una Bitácora de Modificaciones en la que se detallen las modificaciones realizadas, el motivo de las mismas y la fecha en la que fueron realizadas.

BIBLIOGRAFIA

BIBLIOGRAFIA

- Análisis y Diseño de Sistemas de Información.
  James A. Senn
  Segunda Edición
  Editorial Mc Graw Hill - 1992

- Auditing Computer Programs
  EDP Auditors Foundation
  Audit Guide Series
  William E. Perry
  1983

- Auditing Hardware and Software Contracts
  EDP Auditors Foundation
  Audit Guide Series
  William E. Perry
  1983.

- Auditing the Small Business Computer
  EDP Auditors Foundation
  Audit Guide Series
  William E. Perry
  1983.

- Auditoría Administrativa.
  Robert J. Thierauf
  Editorial Limusa - 1986

- Auditoría en Centros de Cómputo. Objetivos, Lineamientos y Procedimientos.
  David H. Li
  Editorial Trillas
  1990

- Auditoria en Informática.
  José Antonio Echenique
  Mc Graw Hill - 1990

- Auditoría Moderna.
  Kell Ziegler
  Editorial CECSA - 1987

- EDP Audit Work Papers
  EDP Auditors Foundation
  Audit Guide Series
  William E. Perry
  1983.

- EDP Auditing.
  James Hannan
  Editorial Van Nostrand Reinhold, Auberbach Publishers Inc. - 1982

- Manual para Auditoría y Seguridad de Sistemas
  Weights y Asociados de Colombia Ltda.

- Montgomery's Auditing.
  Vincent M. O'Reilly, Murray B. Hirsch, Philip L. Defliese, Henry R. Jaenicke
  Eleventh Edition - 1990

- Planing EDP Audits
  EDP Auditors Foundation
  Audit Guide Series
  William E. Perry
  1981.

- Selecting EDP Audit Areas
  EDP Auditors Foundation
  Audit Guide Series
  William E. Perry
  1980.

- Seminario de Auditoría y Control en Procesamiento de Datos.
  GBM de El Salvador, S.A. - 1993

- Seminario sobre Auditoría de Sistemas
  Camara de Comercio e Industria de El Salvador
  Septiembre de 1992

- Seminario sobre Auditoría de Sistemas
  Secretaria Técnica del Financiamiento Externo (SETEFE)
  Enero, 1994

- Sistemas de Información Administrativa.
  Robert G. Murdick
  Segunda Edición
  Prentice Hall - 1988

- Tesis: Aplicación de la Auditoría Operacional en la Empresa Industrial Salvadoreña
  Universidad Centroamericana "José Simeón Cañas", UCA.
  Ricardo Antonio Morales Cardoza
  Noviembre, 1979

- Tesis: Auditoría de Sistemas
  Universidad Centroamericana "José Simeón Cañas", UCA.
  José Luis Castellanos V.
  1992.