2ej · 8

UNIVERSIDAD NACIONAL AUTONOMA
DE MEXICO

FACULTAD DE INGENIERIA

# CONTROL Y AUDITORIA EN CENTROS DE COMPUTO

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACION

P R E S E N T A N:

Cuevas Guzmán María Teresa de Jesús
Torres Becerril Martín César
Zorrilla Cangas María Cristina

Director de Tesis:
DR. ACT. SERGIO CASTRO R.

MEXICO, D. F. 1987


**UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso**

# CONTROL Y AUDITORIA EN CENTROS DE COMPUTO

# I N D I C E .

# CONTROL

# INTRODUCCION

En la actualidad, nuestro país está pasando por un auge muy fuerte en el campo de la computación, y la proliferación de los Centros de Cómputo ha llegado a todos los géneros del Sector Público y Privado, debido a que la aplicación de las computadoras es universal. La tecnología ha sido aprovechada para la satisfacción de las necesidades de procesamiento de información y así poder contar con datos reales y rápidos para una toma de decisiones acertada por parte de la Alta Dirección.

Sin embargo, se han presentado muchos problemas en la mayoría de los Centros de Cómputo, debido a la inexistencia de preparación, organización y control.

Podemos hablar de un porcentaje muy bajo de Centros de Cómputo en los que, al hacerles una auditoría, resultaran con pocas deficiencias o sin ellas. Esto se debe a que los métodos de organización, planeación y administración no son los adecuados o son muy pobres, a veces por falta de recursos económicos, otras por falta de un conocimiento general de lo que representa tener una computadora, pero principalmente se da por la falta absoluta de un sistema de Control; que no existen en los Centros de Cómputo pequeños y medianos y que son muy deficientes en los mayores.

No debemos olvidar nunca que todas las actividades y todas las cosas son factibles de controlar.

Así pues la primera parte de este documento, Control, se ha dividido para su estudio en 4 grandes ramas que son:

- Administración.
- Operación.
- Documentación.
- Seguridad.

En ellos se abarcan los puntos mas importantes a controlar y en las que se envuelven todas las actividades de los Centro de Cómputo desde su Preimplantación hasta su Postimplantación.

Ahora bien, teniendo ya instalado un Sistema de Control, lo siguiente será un sistema para verificar que este sistema de control funcionará adecuadamente y si no se hiciere así, ver las medidas necesarias y proponer alternativas para su funcionamiento y/o mejoría, es así, como aparece la Auditoría, que deberá ser el espejo o la misma imagen reflejada de lo que está haciendo el Control, la Auditoría corrobora las acciones tomadas por el Control, que todo lo del reporte se verá reflejado en la Auditoría. Esta Auditoría podrá realizarse por una persona o grupo de personas que serán "Auditores en Centros de Cómputo", que a partir de este momento se les llamará simplemente "Auditores", no habiendo esta especialidad en México, los Ingenieros en Computación podrán participar activamente en esta otra área de trabajo.

En esta segunda parte proporcionaremos las herramientas necesarias para poder auditar un Centro de Cómputo, los problemas a los que se puede enfrentar y como realizarla.

# CONTROL

## 1. INTRODUCCION.

Ambos, la computadora y la mente humana son instrumentos maravillosos para grandes realizaciones, pero ambos tienen la capacidad de cometer errores. Porque los errores pueden ocurrir en un Centro de Cómputo, es esencial entonces que un sistema de controles sea implementado y mantenido.

### 1.1 NECESIDADES DE CONTROLAR.

En los sistemas manuales y aún en algunos Centros de Cómputo anteriores los controles fueron ejecutados por una persona que checaba el trabajo de otra.

El Centro de Cómputo completo está ahora en las manos de un pequeño grupo de personas que se comunican directamente con la computadora.

Para eso, la administración y los dueños de las organizaciones deben tener una gran conciencia de la integración del Centro de Cómputo y el personal que labora aquí.

Un error no detectado puede tener un serio impacto, yendo através del sistema y provocando muchos otros errores que pueden ocurrir.

Hay que pensar siempre, en por lo menos cinco errores que pudieran suceder, e intentar divisar los controles que deben ayudar a reducir la probabilidad de su ocurrencia.

Día con día, la mayoría de nosotros intentamos incrementar la probabilidad de que cosas buenas sucedan y reducir la probabilidad que las malas cosas sucederán.

De cualquier manera, no se tiene la garantía que lo bueno siempre sucederá. Lo mismo sucede con el desarrollo de un sistema de control puesto que no existe un sistema infalible.

Los controles son necesarios para un propósito: reducir los riesgos. Antes de poder evaluar los controles dentro de cualquier contexto, debemos identificar los riesgos que los controles deben prevenir, detectar o corregir.

A continuación damos una lista de riesgos a los que puede enfrentarse una empresa:

- Contabilidad errónea.
- Pérdida o destrucción de activos.
- Costos excesivos/ingresos deficientes.
- Sanciones legales.
- Fraude y robo.
- Decisiones erróneas de la Gerencia.
- Interrupción del negocio.
- Contabilidad inaceptable.
- Desventaja ante la competencia.

Un riesgo es el efecto de una causa multiplicado por la frecuencia probable de su ocurrencia. Un control actúa para reducir una causa de riesgo, en vez de afectar al riesgo directamente. Por lo tanto, aún cuando los controles tienen por objeto reducir los riesgos, lo que en realidad hacen es actuar sobre una causa.

No existe una relación directa simple entre controles y causas. Por consiguiente varias técnicas de control pueden tener efectos sobre una causa particular, y una causa particular puede ser controlada mediante diversas técnicas.

Las áreas generales de las operaciones de un negocio que normalmente son motivo de preocupación son: la información financiera, los activos del negocio y la eficiencia operacional. La introducción del procesamiento electrónico de datos no cambia estas preocupaciones, pero sí modifica las cosas que pueden ocurrir dentro de tales áreas.

Primero, el uso de una computadora normalmente implica el almacenamiento de grandes cantidades de información en un solo lugar.

Segundo, la introducción de una computadora tiene impacto sobre la organización básica de la mayoría de los negocios.

Los efectos que las computadoras tienen sobre los controles son los de cambiar tanto la efectividad de los diferentes tipos de controles como el medio en el que se implantan. Consecuentemente, aún cuando no ha habido ningún cambio fundamental en la naturaleza de los controles, sí existen cambios radicales en el aspecto externo de los controles que se implantan en los sistemas computarizados:

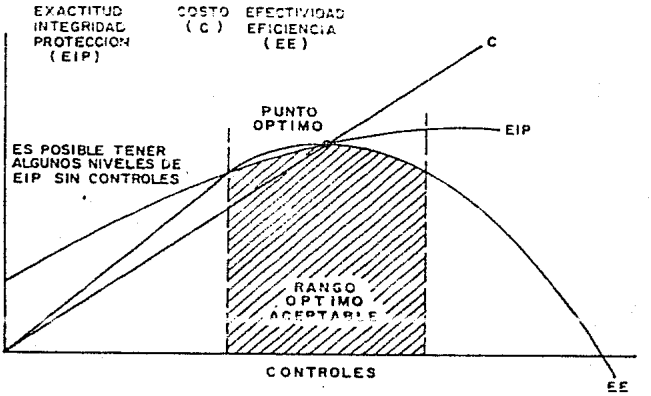
- Se reduce la utilización de controles manuales.
- Puede haber un cambio en los puntos en los que se implantan los controles: de los empleados y supervisores de la computadora y los analistas de sistemas.
- Los controles deben ser mas explícitos debido a que han reducido o eliminado muchos de los puntos de procesamiento que antes permitían el juicio humano.

Por todas estas razones, la estructura y la aplicación de los controles deben ser claras para todas las partes interesadas.

## 1.2 NIVELES DE CONTROL.

Un sistema de controles presenta al auditor un dilema. También demasiados controles y los controles que son muy estrechos, pueden impedir el procesamiento. De otra manera, los controles inadecuados pueden hacer el procesamiento de datos inservible. El incremento directo de controles aumenta la exactitud, integridad y protección (EIP) del Centro de Cómputo también como su costo (C).

La mayoría de los controles pueden también incrementar la efectividad y eficiencia (EE) del procesamiento en un punto óptimo, después del cuál la implementación de mas controles resultan inútiles. El objetivo de la administración en general es alcanzar el punto óptimo como se indica en la figura 1. La instalación de controles excesivos decrementa la eficiencia y efectividad en su curva (EE) a tal grado que con algún punto, este tiene una tendencia a jalar la curva (EIP) con éste.




F I G U R A 1

Ejemplo de un Sistema Optimo de Controles

## 2. CLASIFICACION GENERAL DE LOS CONTROLES.

Los controles pueden clasificarse en diversas formas, cada una de ellas nos dice algo distinto respecto a la forma en que los controles y el punto de vista del auditor, cambian en las situaciones del procesamiento de datos.

### 2.1 CONTROLES VERTICALES Y HORIZONTALES.

Otra forma de clasificar los controles es dividirlos entre aquellos que siguen las líneas verticales de autoridad de un organigrama y aquellos que siguen los flujos de procesamiento que cruzan dichas líneas.

La implantación de las computadoras implica en muchas situaciones un giro ascendente del nivel mínimo de supervisión común o del control de la gerencia en línea. Este giro ascendente afecta la naturaleza de los controles verticales debido a que quienes tienen autoridad general sobre los procesos se encuentran en posición más alta dentro de la organización y tienen menos tiempo para ejercer una supervisión detallada.

Por otra parte, en virtud de que ciertos departamentos adicionales participan en un proceso en el que antes existía un solo departamento, surge la necesidad de mas controles horizontales.

Como resultado, una estructura organizacional que proporcionaba controles adecuados para un sistema manual, normalmente no proporcionará el mismo grado de control para un sistema después de la introducción de una computadora y de aplicaciones integrales.

Esto no quiere decir que los controles verticales, tales como la supervisión y la segregación de funciones, ya no sean importantes para un sistema computarizado; sin embargo, se reduce su efectividad y el énfasis relativo. Tal énfasis debe dirigirse más bien hacia los controles de tipo horizontal, tales como los documentos de envío, las cifras de control y las ediciones.

## 2.2 CONTROLES PREVENTIVOS, DETECTIVOS Y CORRECTIVOS.

Esta técnica se refiere a si una determinada técnica de control evitará que ocurra una causa de riesgo, detectará el hecho de que ya ha ocurrido o corregirá sus defectos después de que ha sido detectada.

Los controles preventivos son aquellos que reducen la frecuencia con que ocurren las causas de riesgo.

Los controles detectivos no evitan que ocurran las causas de riesgo, sino que, más bien las detectan después de que han ocurrido. No es suficiente la simple detección de una causa de riesgo. Cuando se detectan tales situaciones, debe tomarse una decisión respecto a cual es la acción correctiva apropiada y posteriormente debe llevarse a cabo dicha acción.

Un control preventivo actúa como una guía para ayudar a que las cosas sucedan como deben ser. Con frecuencia son pasivos y no implican ninguna actividad física directa. Por otra parte, tales controles, a menudo permiten cierto porcentaje de violaciones.

Los controles preventivos se encuentran a menudo tan sutilmente intercalados dentro de un proceso, que las personas involucradas en la operación pueden no estar siquiera concientes de su existencia.

Un control detectivo no evita que una causa de riesgo ocurra, sino que dispara una alarma después de que ya ha ocurrido. El control detectivo puede poner fin al procesamiento posterior o simplemente registrar la ocurrencia. Esta función de vigilancia con frecuencia es bastante confiable; sin embargo, la detección de que una causa ha ocurrido es simplemente eso y nada más. Los controles detectivos alertarán a las personas involucradas en el proceso, a fin de que estén concientes de la existencia de un problema. Tal conocimiento es imprescindible si ha de seguirse la acción correspondiente para corregir los defectos de la causa detectada.

El último tipo de control es el correctivo. Este ayuda en la investigación y corrección de las causas de riesgo detectadas. La acción correctiva siempre es necesaria para remediar las causas de riesgo que se detectan. En ciertas ocasiones puede decidirse que no vale la pena seguir una acción correctiva, pero tal decisión debe tomarse consciente y consistentemente, no por negligencia. La alarma que proporciona un control detectivo es inútil si nadie la escucha.

Debido a que los controles preventivos son a menudo pasivos (como las instrucciones para llenar una forma), es necesario un control detectivo, para determinar si el control preventivo está funcionando. Aún si así fuese, los controles detectivos seguirán siendo necesarios para detectar los riesgos que evaden el control preventivo.

Además, las partidas que originan errores son con frecuencia más diffciles de manejar, que las partidas normales; de lo contrario, el error no hubiera ocurrido. La corrección apropiada también puede ser diffcil; por lo tanto, todas las partidas que se corrigen deben procesarse subsecuentemente a través de los mismos controles detectivos, o de otros todavía más estrictos. No obstante que la corrección sea fácil, sigue existiendo la posibilidad de que se procese en la dirección equivocada, de tal forma que algo que debiera sumarse, en realidad se reste. Los controles detectivos sobre los controles correctivos son esenciales debido a que la corrección del error es en sí misma una actividad altamente propensa a errores.

## 3. PUNTOS DE CONTROL.

El Centro de Cómputo es un recurso valuable para la organización. Existen cuatro puntos que el auditor debe considerar :

- Los controles efectivos deben ser diseñados dentro del sistema, no anexados después.

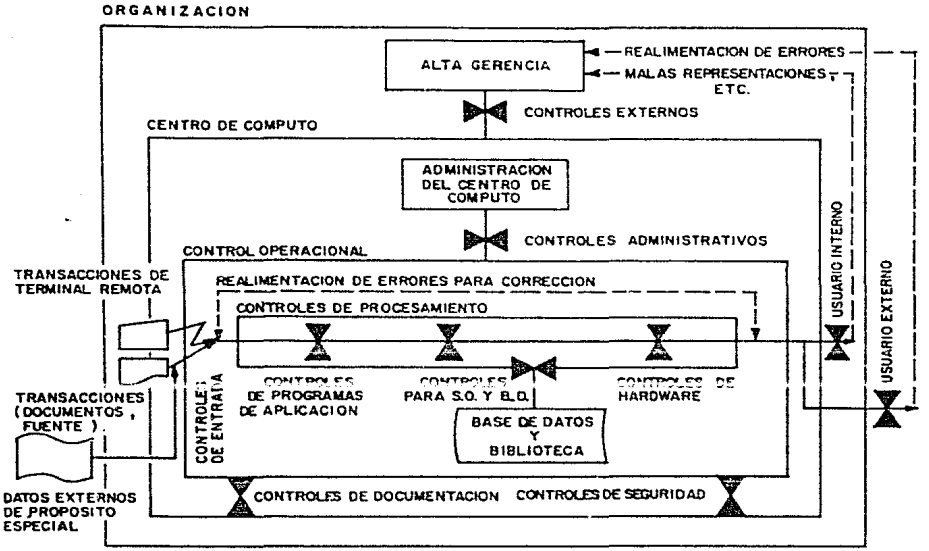
- En general, los analistas de sistemas y programadores no han dedicado suficiente tiempo para los controles. En efecto, mucha de esta gente es adversa al establecimiento de controles.

- Los auditores deben estar mas envueltos en el desarrollo de sistemas para ayudar a asegurar que los controles apropiados sean implementados.

- Los auditores deben informar a la administración que un sistema de controles no sirve solamente para el concepto de contabilidad tradicional de control interno sino que también es importante alcanzar una operación eficiente del Centro de Cómputo.

La figura 2 nos dá un esquema de los puntos importantes de control de un Centro de Cómputo.

Estos controles pueden ser agrupados en cinco categorías generales y definidos como sigue :




F I G U R A 2

Puntos de Control relacionados con los Sistemas de Información

1. Controles Administrativos.

Estos controles son la responsabilidad de la Gerencia del Centro de Cómputo. Incluyen funciones tradicionales de administración, tales como establecimiento de planes; reclutamiento, selección, asignación y capacitación de personal; desarrollo, implementación y realización de estándares; y un desarrollo organizacional adecuado.

2. Controles Operacionales.

Estos controles se relacionan directamente a las operaciones de procesamiento de datos y consecuentemente ayudan a asegurar que las transacciones sean manejadas apropiadamente y que los datos sean convertidos exacta y viablemente en información.
Estos controles incluyen lo siguiente :

- Controles de Entrada.
- Controles del Sistema Operativo.
- Controles de Procesamiento.
- Controles en Programas de Aplicación.
- Controles de Manejadores de Base de Datos.

- Controles de Hardware.
- Controles de Operaciones de la Computadora
- Controles de Biblioteca y de Base de Datos.
- Controles de Salida.

3. Controles de Documentación.

Estos controles se refieren a todas las comunicaciones y documentos que nos dicen como opera el sistema. La documentación típica contiene : reportes de desarrollo de sistemas, diagramas de flujo del sistema, lay-outs de archivos, registros y reportes, diagrama de flujo de los programas y tablas de decisión, procedimientos de prueba, listados de programas fuente y objeto, y procedimientos manuales generales.

4. Controles de Seguridad.

Estos controles incluyen todas las operaciones físicas y de procedimiento utilizadas para asegurar que el Centro de Cómputo no sea erróneo o resquebrajado intencional o desintencionalmente por fuerzas internas o externas.
Los conceptos asociados con controles internos apropiados es de suma importancia para el auditor.

5. Controles Externos.

Estas funciones de control emanan y son realizadas, tanto por grupos de la función de auditoría como de la función consultora, de la alta gerencia, staff especial en grupos de control, y varias personas de la organización.
Todos ellos ayudan a establecer un chequeo independiente en las actividades generales del Centro de Cómputo através del uso del sistema de observación y retroalimentación.

Cada uno de estos controles (hasta el 4) se verá mas claramente en los siguientes capítulos de esta tesis.
Los controles pueden clasificarse en diversas formas. Cada una de las clasificaciones nos dice algo distinto respecto a la forma en que los controles y el punto de vista del auditor cambian en las situaciones de procesamiento electrónico de datos.

6. Relación entre Costo/Beneficio de los Controles.

En los sistemas de información, como en cualquier otra parte, cada control tiene un factor de costo. Ningún control debe costar más que los errores potenciales para cuya detección, prevención o corrección se establece. El costo de comprender y corregir los errores no debe pasarse por alto en esta consideración de costo-riesgo. En la medida en que los controles se diseñan inapropiadamente o son excesivos, llegan a ser agobiantes y existe el peligro de que sean ignorados. Debe hacerse una revisión para ver si los errores pueden ser descubiertos con mayor anticipación en el ciclo de procesamiento, minimizando:

- Los puntos de control requeridos.
- El daño que puede hacerse al archivo.
- El trabajo de corrección necesario.

Las necesidades de la gerencia y la importancia de cualquier error dado, así como la evaluación de los costos y riesgos, son consideraciones efectivas para determinar en donde y en que medida deben aplicarse los controles.

Los controles preventivos son generalmente los de más bajo costo. Los controles detectivos normalmente requieren de ciertos gastos operativos moderados. Por otra parte, los controles correctivos son casi siempre muy costosos, puesto que implica de tres a diez veces más trabajo corregir algo que ocurrre en forma inadecuada que hacerlo bien desde el principio.

El diseño de controles óptimos, por lo tanto, requiere que se hagan una serie de consideraciones. Los controles preventivos son los más baratos de operar pero rara vez son suficientes por sí solos. Por consiguiente casi siempre resulta necesaria cierta actividad correctiva. El equilibrio entre los costos y los beneficios debe encontrarse entre el costo de implantar controles preventivos adicionales y el de llevar a cabo las actividades de corrección. La eliminación de los controles de detección es rara vez un medio apropiado para reducir costos. Sin ellos no puede medirse ni la efectividad de los controles preventivos ni el riesgo resultante.

## 3.1 CONTROLES ADMINISTRATIVOS.

Los controles administrativos para nuestro estudio se clasificarán en tres puntos importantes :

1. Control de la Organización.
2. Control del Personal.
3. Control del Presupuesto.

Ahora cada uno de ellos se verá detalladamente para su estudio y comprensión.

### 3.1.1 CONTROL DE LA ORGANIZACION.

**El Centro de Cómputo en la Institución.**

Lo primero que tenemos que hacer es definir claramente que es un Centro de Cómputo, su ubicación en las empresas hasta haber encontrado su lugar de forma adecuada para proporcionar el mejor servicio y funcionalidad, así como sus características.

**Definición de un Centro de Cómputo.**

Podemos definir al Centro de Cómputo como el conjunto de Hardware (Equipo) y Software (Programas) através de los cuales se procesa una aplicación. Así como una unidad de servicio y asesoría dentro de la empresa para ayudar a realizar los procedimientos al área solicitante o usuaria.

Se crea en base al incremento de la demanda de recursos tecnológicos que ha hecho posible a la computadora, recurso que sirve para lograr, superar, y satisfacer las metas y objetivos de las organizaciones públicas y privadas modernas, pues crea así, la necesidad de diseñar e implementar formas organizadas de trabajo, con el fin de poder utilizar la herramienta, que es la computadora, de una manera racional y con el máximo de aprovechamiento.

Características.

- Combinar un alto nivel de actividad técnica combinada con creatividad.
- Requiere una amplia perspectiva de dirección en sus etapas de diseño y una perspectiva detallada en sus etapas de implementación.
- Estar conciente del impacto de su trabajo en las políticas, procedimientos y estructura de organización de la institución y aún así mantener un interes en los campos de datos individuales y en la calidad de adaptación de los mismos.
- Mantener la objetividad para encontrar las necesidades de otros o para saber las funciones que se cruzan o abarcan muchas líneas de la organización, aunque organizacionalmente pueda estar situada en un área o ejercer una función específica.

Papel de un Centro de Cómputo.

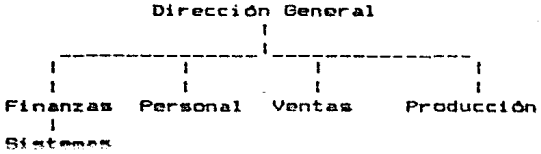
El Centro de Cómputo requiere de una organización adecuada, que le permita satisfacer las necesidades de sus usuarios de una manera eficiente; dicha organización, en virtud de la magnitud que alcanza un Centro de Cómputo y de la diversidad de servicios que le corresponde prestar, se forma cada vez mas compleja y difícil de controlar pues el servicio que presta dependerá del nivel, tipo, y manera en que lo desarrolla ya que diferirá de una institución a otra en los siguientes puntos :

- Tipo de Procesamiento.
- Liderazgo.
- Autoridad.
- Clientes.
- Integración.
- Exactitud.
- Prioridad.
- Nivel de Servicio.
- Costos.
- Educación.
- Diseño.

La ubicación de los Centros de Cómputo depende de forma diferente en una empresa o institución y según sea determinado por la Alta Dirección o por la Dirección General. Las mas importantes y comunmente utilizadas se describen a continuación :

Dependencia del Area Financiera.

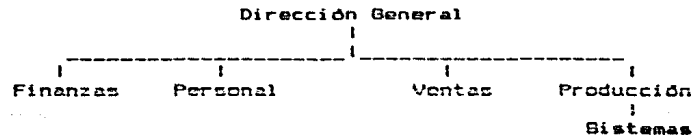
Esta ubicación es válida, cuando el porcentaje de los trabajos que se desarrollan en el área de Sistemas son de tipo Administrativo. Pero es importante hechar un vistazo de su funcionamiento pues por atender las peticiones de tipo administrativo, descuidaría otras áreas, resultando problemas por no tener ellos las facilidades.




Dependencia del Area de Producción.

Este tipo de ubicación será válida cuando el trabajo desarrollado por el área de Sistemas esté encaminado a las necesidades de producción de la empresa.

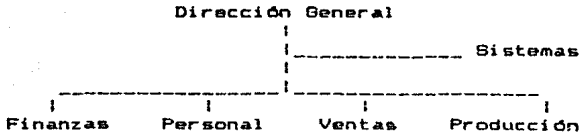
Esta ubicación no es muy común y solo en pocas ocasiones llega a justificarse.




Sistemas como Staff de la Dirección General.

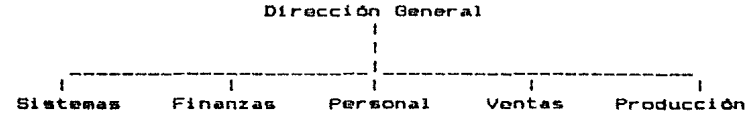
Siendo Sistemas una área de apoyo y asesoría a la Dirección General por generarse en ella información útil para la toma de decisiones, y siendo además una área de servicio a toda la organización, la comunicación que debe existir hacia la Dirección General es de gran importancia para el desarrollo de proyectos acordes a los objetivos de la empresa.

Esta ubicación permite que " Sistemas " tenga la fuerza necesaria para mantener una comunicación a cualquier nivel dentro de la organización lográndose con esto aprovechar positivamente los canales adecuados para proporcionar un servicio adecuado.




Sistemas como una Dirección dentro de la empresa.

Para facilitar la comunicación y tenerla en un buen nivel se puede colocar al área de Sistemas, como una Dirección dentro de la empresa para así se independizará, y podrá tomar decisiones propias que ayudarán a un mejor trabajo, agregando que cada día toma mas adeptos este tipo de organización por ser de las mas adecuadas.




La unidad de Sistemas empieza a aparecer como elemento significativo de la organización, pues se han utilizado ya varios modelos.

El modelo que se utilice tiene algún impacto en la efectividad de la función, sin embargo, el aspecto clave en el éxito de una Area de Sistemas e Informática es la calidad de su gente y no en la estructura de la organización.

Lo anterior no significa que una organización realista y razonable no pueda aminorar y facilitar las dificultades y objetivos de una forma clara y correcta.

## Estudio de Factibilidad.

### Introducción al Estudio de Factibilidad.

Se entiende por Estudio de Factibilidad al conjunto de investigaciones orientadas al establecimiento de una base que permita decidir sobre la posibilidad y conveniencia de utilizar sistemas de cómputo en una empresa ó institución.

Caracterfsticas.

El "alcance" de este estudio, son los resultados, que permitirán tomar decisiones sobre la posibilidad y conveniencia de modificar en forma total o parcial los procedimientos actuales de captación, tratamiento, diseminación y uso de la información, de tal manera, que los cambios resultantes lleven a las soluciones de los problemas detectados, aprovechando racionalmente la tecnologfa informática.

Por lo anterior, dichos resultados deberán comprender los beneficios e implicaciones en términos cualitativos y cuantitativos, en corto, mediano y largo plazo con respecto a : su eficacia, seguridad, fucionalidad, capacidad de desarrollo, flexibilidad y costo.

En conclusión podemos decir que este Estudio es en esencia un instrumento de planeación y control en el desarrollo y aplicación de la computación en cada institución pública ó privada.

a. Grupos de Realización.

Para la realización del Estudio se requiere de la integración, formación o constitución de dos grupos, uno de los cuales deberá fungir como coordinador del Estudio y el otro como ejecutor del mismo, los que tendrán caracterfsticas y funciones especfficas.

Comité de Sistemas e Informática o de Decisiones.

Este Comité es el mecanismo mediante el cuál se logra la participación de los funcionarios de la dependencia en las decisiones que habrán de tomarse a lo largo del Estudio.

Es conveniente que dicho Comité esté integrado por funcionarios de alto nivel, entre los cuales estén los responsables de las unidades de: Programación, Organización y Métodos e Informática. Es necesario que este grupo sea presidido por un funcionario de alto nivel jerárquico, nombrado preferentemente por el titular de la institución, de manera que pueda garantizar el acceso necesario a las distintas áreas involucradas ya que de ello depende en gran medida el éxito del Estudio.

Funciones.

- Definir los objetivos especfficos y cobertura del Estudio.
- Integrar al grupo técnico que se encargará del desarrollo y ejecución del Estudio de Factibilidad.
- Proveer al Comité Técnico de los elementos de apoyo necesarios para su correcta operación.
- Servir como medio de enlace entre las áreas involucradas y el Comité Técnico.

- Someter a la consideración de los niveles superiores de la institución los objetivos.
- Dirigir y controlar permanentemente el desarrollo del Estudio, determinando las prioridades de actuación sobre el mismo y decidir de acuerdo a los resultados parciales sobre la continuación o reorientación de los subprogramas.
- Finalizar y evaluar los resultados finales y propuestas del Comité Técnico, decidiendo sobre las acciones y requerimientos que mejor satisfagan las necesidades de la empresa o institución.
- Establecer la coordinación con el área de presupuesto de la institución para poder integrar la necesidad informática en las necesidades institucionales al elaborar el presupuesto global.

Comité Técnico.

El Comité Técnico deberá estar constituído por diferentes especialistas en disciplinas tales como: el análisis de sistemas, procesamiento de datos, investigación de requerimientos de información, métodos e instrumentos de capacitación, técnicas en diseminación y flujo de información, conjuntamente con los elementos interiorizados en las políticas y características actuales de operación en la entidad o institución.

Es recomendable que el responsable de la unidad de sistemas e informática o en su defecto el de organización y métodos, dirija al Comité Técnico y que ambos participen en el Comité de Sistemas e Informática.

Funciones.

- Definir la instrumentación para el desarrollo del estudio.
- Elaborar el Plan de Trabajo y sus fases de actividades para el desarrollo del programa y los estudios de factibilidad.
- Someter a la consideración del Comité de Sistemas e Informática los puntos anteriores para su aprobación.
- Desarrollar y documentar las diferentes etapas.
- Realizar la integración y síntesis del trabajo incluyendo las alternativas de solución y sus características.
- Llevar a cabo la selección y presentación de alternativas al Comité de Sistemas e Informática para su análisis y decisión.

b. Diagnóstico de la Situación Actual.

Para el desarrollo de este punto, es conveniente saber acerca de la institución en todos sus aspectos, a fin de lograr una visión completa de sus procedimientos actuales y requerimientos, pasando de lo general a lo particular.

Investigación General :

La visión general de la dependencia puede lograrse mediante el análisis de :

- Funciones y Objetivos.
- Estructura Orgánica.
- Atribuciones Legales.
- Estructura Programática.
- Reglamentos Internos y Lineamientos Generales.
- Instrumentos de Administración.
- Recursos Humanos, Materiales y Financieros.
- Sistemas de Trabajo.
- Sistemas de Organización.
- Areas Funcionales.

Para conocer lo anterior, el Comité Técnico puede apoyarse en material documental como : Manual de Organización, reglamentos, estatutos internos, organigramas y publicaciones oficiales, etc., así como en entrevistas con funcionarios y empleados de la entidad o instituciones y asesoría del Comité de Decisiones.

c. Determinación de Requerimientos de Información.

En esta fase del estudio deberán ser determinadas las necesidades específicas de información en la institución, identificando las diferentes áreas de la misma, los diversos tipos de información que maneja cada una y la relación que en esta materia existe entre ellas.

Para lograr lo anterior, una forma conveniente sería la de dividir la institución en :

- Areas de Planeación.
- Areas de Coordinación.
- Areas de Operación:
  - Técnicas.
  - Administrativas.
- Areas de Apoyo o de Staff.

Los diferentes tipos de información que maneja cada área, podrían ser fijados por la aplicación actual de la misma, la que puede estar orientada a la administración, producción, investigación científica, etc.. En cuanto a la interrelación existente en dichas áreas en materia de información, es importante identificar cuales son:

- Unidades Generadoras.
- Unidades Usuarias.
- Unidades Tratadoras.
- Unidades Diseminadoras.

Ahora bien, para cada una de estas unidades se deberán investigar:

De las Unidades Generadoras.

- Información que generan.
- Origen de la información.
- Forma de generación de la información.
- Frecuencia con la que generan la información.
- Volumen de la información.
- Procesos a que someten la información.
- Vida Util.
- Niveles de Agregación.
- Canales de Transmisión.
- Sistemas de actualización y periodicidad de los mismos.
- Métodos de Clasificación.
- Formas de representación.
- Tratamientos que requiere.
- Sistemas que se emplean (manuales, mecánicos, electrónicos, etc.).

De las Unidades Usuarias.

- Información que utilizan.
- Frecuencia con que la utilizan.
- Necesidades adicionales no cubiertas.
- Problemas en su obtención.
- Deficiencias en oportunidad, calidad, cantidad y presentación.
- Sistemas de archivo, uso que le den, etc..

De las Unidades Tratadoras.

- Información que manejan o procesan.
- Formas de Captura.
- Procesos a que los someten.
- Formas de organización.
- Instrumentos que utilizan.
- Métodos que siguen, etc..

De las Unidades Diseminadoras.

- Información que distribuyen.
- Unidades internas y externas a quienes la diseminan.
- Flujos que siguen.
- Formas de difusión.
- Tipos de presentación.
- Problemas de diseminación, etc..

d. Documentación del Estudio de Factibilidad.

Para documentar lo anterior, es necesario reunir y organizar la información recabada de las unidades investigadas elaborando matrices de clasificación, diagramas de flujo, esquemas de relación y manuales de explicación de la información que maneja la institución, señalando su origen y destino, tanto interno como externo, para que finalmente sea analizado y confrontado, determinando así, los requerimientos de información de las diferentes áreas en lo relativo a: problemas, carencias, deficiencias e insuficiencias de información; así como métodos manuales o mecanizados para su tratamiento y depuración que en forma preliminar se consideren aplicables.

e. Diagnóstico de la Unidad Informática.

El diagnóstico de esta unidad, si existe, deberá realizarse, de manera muy completa, de tal manera que proporcione una imagen exacta que permita identificar sus problemas y con ello determinar las medidas de superación mas adecuadas, ya que por las funciones que desarrolla, los instrumentos que utiliza y la relación que tiene con el resto de la institución, requiere de una atención especial en la ejecución de este tipo de estudios.

Para lograr lo anterior , es necesario conocer aspectos de índole organizativo, administrativo, técnico y funcional de la unidad. A continuación se mencionan algunos conceptos de utilidad para el diagnóstico :

Organización.

- Descripción de la unidad.

  Considerando para ello la relación directa de dependencia superior, sus relaciones colaterales y las descendentes dentro de la estructura total de la dependencia.

- Objetivos, funciones y atribuciones.

  Son los establecidos en el reglamento interior y en el manual de organización correspondientes.

- Estructura orgánica interna.

  Describiendo claramente los niveles jerárquicos, la especie y funciones de cada parte integrante, tanto de la unidad central como de sus delegaciones regionales o estatales si las tuviese.

- Reglamentos de trabajo internos.
- Estructura programática de la unidad.
- Instrumentación administrativa.

La instrumentación administrativa se refiere a los mecanismos de los cuales se vale de la unidad para su administración, como son: métodos de planeación, organización, dirección, programación y control de actividades, recursos humanos, materiales y financieros a su cargo.

f. Medio Ambiente del Trabajo.

Es frecuente que el medio ambiente en el centro de trabajo tenga fuerte influencia sobre el estado de ánimo del personal, lo cual repercute positiva o negativamente en la productividad del mismo, es recomendable investigar las condiciones generales del local, su ubicación, distribución, mobiliario, equipo de oficina, iluminación y servicios en general con que opera.

g. Infraestructura Física y Lógica de Informática (HW y SW).

En este punto se determinará si pueden esperarse beneficios significativos de su futura aplicación al conocer sus limitaciones y grados de suficiencia.
Para ello, el grupo técnico debe de estudiar y documentarse ampliamente en lo siguiente :

- Configuración del equipo actual.
- Sistemas de programación.
- Soporte (por parte del proveedor).
- Equipos fuera de línea.
- Equipos de apoyo.
- Mantenimiento por parte de la institución.
- Bienes de consumo.

Contratación de servicios externos.

- Asesoría o consultorías externas de servicios y costos promedio.
- Renta o utilización de equipos externos (razones y costos).
- Servicios de mantenimiento, instalación o reparación de equipo.

Compromisos y erogaciones.

- Salarios, renta de equipo, mantenimiento, materiales de consumo, etc.

h. Cobertura y eficacia de los servicios de informática.

Estadísticas de funcionamiento del equipo.

- Indice de las fallas de equipo.
- Tipos y causas de fallas.
- Indice de destrucción total ó parcial de archivos y causas.
- Frecuencia de elaboración y proceso de trabajos no previstos.
- Indice de fallas de corriente.
- Indice de cargas de trabajo excesivas.
- Tiempos muertos por anomalías en el equipo.

Operación del sistema.

i. Preparación y documentación de la investigación para el diagnóstico.

Una vez investigados los puntos anteriores, es necesario integrar y organizar la información obtenida, documentándola mediante organigramas, diagramas de flujo, tablas de decisión, etc., para facilitar su análisis y con él, la identificación de problemas y el diagnóstico general de la situación actual.

j. Análisis de la información recabada y diagnóstico de la situación actual.

Esta fase es la última del diagnóstico de la situación actual; dónde se realiza un detallado análisis de los puntos investigados, identificando durante su desarrollo las necesidades y problemas que no son cubiertos por los sistemas actuales, las razones para ello y la posibilidad de solución mediante la utilización parcial o total de los procedimientos vigentes, o bien la modificación de los mismos y por consiguiente, la generación de diversas alternativas de solución y sus requerimientos.

Los resultados de esta etapa, serán publicados en un documento en el que se presentan los problemas y sus posibles soluciones, así como los requerimientos e implicaciones que ellos reclamen, el resumen del diagnóstico general del área de Sistemas e Informática, el cuál deberá incluir el reporte de eficiencia y disponibilidad de los recursos, sus necesidades adicionales, alternativas de solución y justificación de los mismos; dicho documento deberá ser presentado al Comité de Decisiones para su conocimiento y análisis.

Recomendaciones para el análisis.

Es recomendable elaborar formas que describan los problemas que vayan siendo identificados, así como sus características y posibles causas, procurando clasificarlos por áreas y grados de importancia, de acuerdo a los objetivos específicos de la institución.

Racionalización de los Centros de Cómputo.

Frecuentemente, varias unidades pueden procesar información similar, con criterios ligeramente diferentes en cada caso, por lo que un esfuerzo relativamente pequeño para contar con un sistema integrado de información puede reducir en forma sustancial la presión sobre la capacidad instalada existente en materia de cómputo. Esto es, especialmente importante en el caso de las dependencias que planean incrementar sus equipos ó cambiarlos por otros de mayor capacidad.

Controles en la etapa del Estudio de Factibilidad.

El principal control en las actividades del Estudio de Factibilidad tiene que ver con el uso efectivo del Comité de Sistemas e Informática.

Es tarea de este Comité, asegurarse de que se sigan procedimientos básicos y razonables, tal como se hace en cualquier otra área. El Comité debe encargarse directamente, de los siguientes aspectos :

- Asegurarse de que la alta gerencia confirme periódicamente las políticas existentes, o comunique las nuevas, o aquellas que han sufrido modificaciones a quienes conciernen.
- Hacer revisiones periódicas y cuidadosas de todos los presupuestos de tiempo y de costos que se hubieran desarrollado y/o usado en las actividades del Estudio de Factibilidad.
- Hacer análisis críticos de cualquier informe que muestre que el nuevo sistema llevará a una reducción inmediata de los costos de procesamiento, ya que ello raramente sucede.
- Si no va a haber ningún cambio en los pasos del sistema o en los resultados producidos, es decir, si los pasos actuales se van a continuar realizando, solo que ahora se llevarán a cabo en una máquina diferente, cuestionar el porqué de esto. Si las cosas se hacen en forma correcta, probablemente todo el sistema sufra cambios sustanciales, tanto en su lógica como en sus resultados.
- Insistir en que la compañía procese sus propios datos (para alguna aplicación significativa) en una computadora del vendedor. Esto ayudará a identificar a tiempo algunos problemas.

- Solicitar comentarios pertinentes a varios de los usuarios potenciales internos sobre que tan práctico consideran a la computadora. Si se instala un nuevo sistema sin conocer las sugerencias de los usuarios o ignorando sus protestas, este nunca trabajará bien.
- Exigir que cada propuesta remitida por el vendedor o por los analistas internos esté acompañada de una lista exhaustiva de desventajas. Es poco realista aceptar que una propuesta solo ofrezca ventajas.

  Una buena práctica para que el Comité sepa que está haciendo lo que debe hacer es usar listas de verificación. A menudo se las puede conseguir con los vendedores, las firmas de auditores o con consultores. También se debe recurrir a los amigos en otras compañías para obtener de ellos ideas valiosas.

  Por supuesto que el grupo o la persona a quien el Comité reporta debe revisar periódicamente su trabajo y determinar si este está funcionando como debe. Esta revisión debe hacerla la junta directiva, el Director general, o un ejecutivo de alto nivel.

**Requerimientos Organizacionales.**

El propósito de este paso es predecir los requerimientos organizacionales que existirán a la vez de que el nuevo sistema opere propiamente y sean tan largos como sea posible de aquí en adelante.

En muchas empresas la decisión de iniciar un esfuerzo de sistemas es parte de un plan a largo plazo, el cuál puede incluir algunas veces una redefinición parcial de las políticas de la empresa y las metas en los negocios, las cuales pueden resultar en algún grado de reorganización de la empresa. La intención útil de este tipo de reorganización es hacer a la empresa mas adaptable al cambio de medio ambiente en el cual opera.

Cualquier cambio mayor contemplado debe de estar permitido en el diseño del nuevo sistema.

En algunos casos será necesario, o al menos deseable, cambiar la organización de la compañía en orden para que los objetivos del sistema puedan ser realizados.

Los resultados de este paso serán una lista de los cambios organizacionales que van a ser llevados a cabo, junto con las fechas propuestas a las que van a ser implementadas. Algunos de estos cambios deben contemplar las modificaciones a los objetivos del sistema definidos en el paso anterior y generar requerimientos adicionales.

**Análisis Costo/Beneficio.**

En este inciso se verá básicamente la cuantificación del(los) sistema(s) en base a lo siguiente :

Costos y beneficios de un Centro de Cómputo.

Este reporte del costo y beneficio es una herramienta gerencial, para usarlo en el direccionamiento del esfuerzo de sistemas. Este provee una medida para :

- La evaluación del aprovechamiento del nuevo sistema y la investigación necesaria para esta.
- Clasificando las prioridades de los objetivos, en la base de aprovechamiento de esfuerzos parciales.

El reporte de costo y beneficio provee información básica :

- Para la decisión de continuar o no el esfuerzo de sistemas y llegar a la conclusión del Estudio de Factibilidad.
- Para el ajuste o confirmación de las prioridades al término del análisis del sistema y fase de diseño.
- Para soportar decisiones cruciales durante el curso del proyecto.
- Para la evaluación del nuevo Centro de Cómputo después de la implementación y entrega al usuario, la evaluación de postimplantación.

Aunque el reporte de costo y beneficio es tratado para el caso de un nuevo Centro de Cómputo, el mismo método puede ser usado y aplicado si se remplaza el equipo que se tiene.

Preparación del Reporte de Costo/Beneficio.

Se debe de tener la siguiente información disponible :

- Objetivos para el nuevo Centro de Cómputo definido en radios de interpretación.
- Esquema general de diseño, desarrollo e implementación.
- Proyecto presupuestal.
- Cambios en la organización.
- Valuación del sistema existente.
- Requerimientos de software y hardware así como la idea del nuevo diseño del sistema.

El documento de costo y beneficio se divide en las siguientes secciones :

- Costos Iniciales.
- Costos adicionales en la operación del nuevo sistema, bajo esta división son incluídos todos los costos que son aplicables al viejo sistema los cuales no intervendrán en el nuevo sistema.
- Impacto en la realización.
- Ahorros/Año en costos recurrentes; esta es la influencia en la economía de la organización efectuada por la operación del nuevo sistema.
- Ahorros Totales/Año; esto demuestra la influencia de los costos iniciales y de la operación del nuevo sistema, en los resultados de la empresa.
- Ahorros Totales Acumulativos; la suma de los ahorros totales sobre un número de años.

El cálculo del proyecto debe ser preparado sobre y en base a un número de años, o a corto, mediano y largo plazo; los beneficios deben ser provistos después de un período de 3 a 6 años, dependiendo del tiempo de vida planeado para el sistema.

Evaluación de los Costos y Beneficios.

Después de recolectar todos los costos y beneficios y acomodarlos de acuerdo a la detención de la documentación necesaria, una evaluación del proyecto puede hacerse. Una consideración mayor es el espacio/tiempo. Para una evaluación adecuada, el espacio/tiempo escogido debe fallar por un mínimo, el cuál incluye el tiempo total usado en el esfuerzo de sistemas y el primer año normal de ejecución del Centro de Cómputo y un máximo que no exceda la suma del total del tiempo gastado en el esfuerzo de sistemas y el tiempo de vida económica esperada del Centro de Cómputo.

La vida económica de un nuevo Centro, es de especial importancia cuando el impacto del Centro en la organización del usuario es esperada para manifestarse por sí mismo en forma gradual, y no directamente en el primer año de operación.

El cálculo del proyecto para el espacio/tiempo seleccionado debe tomarse dentro de la cuenta de costos iniciales o no recurrentes conectado con el esfuerzo de sistemas, el cuál con la instalación de nuevo hardware, y con la implementación de nuevos procedimientos y corridas.

Este método permite ajustes en forma ascendente o descendente de los costos de operación esperados o recurrentes sobre los años de la operación actual del Centro, para encontrar su respectivo crecimiento, o incrementar en eficiencia y experiencia.

Esto permite también una evaluación integrada de todos los costos y beneficios concernidos, no respectivos del año en el cuál ocurrieron o son realizados.

El requerimiento mínimo impuesto en el departamento de contabilidad de la organización es que este deberá guardar registros separados precisos de todos los puntos del proyecto.

El resultado final de la evaluación es un resumen de todos los costos y beneficios sobre el espacio/tiempo escogido. Esta configuración debe mostrar un balance favorable de costos y beneficios omitidos sobre nuevos costos antes de que el proyecto pueda ser considerado satisfactorio.

## Selección del Equipo.

### Criterios para la selección de equipo.

Una vez que un Comité de Decisiones ha estudiado las diferentes alternativas para satisfacer los requerimientos de Centros de Cómputo y ha tomado la decisión de adquirir uno de ellos, es conveniente que antes de realizar la operación, analice las características específicas de las disponibles en el mercado.

- Que el Comité de Decisiones convoque a concurso de una manera oficial, o solicitar cotizaciones a las empresas proveedoras de sistemas de cómputo existentes en el mercado.
- Proporcionar a cada proveedor participante, la información suficiente para la elaboración de su propuesta, misma que debe contener más de una alternativa en configuración, soporte y tipo de operación, renta, compra, renta con opción a compra, etc..
- Que se establezcan las condiciones de presentación y fecha límite para la entrega de propuestas.
- Analizar y evaluar cada una de las propuestas en forma detallada documentando los resultados parciales y totales del análisis y evaluación.
- Seleccionar las propuestas que en todos sus aspectos cumpla plenamente con las condiciones requeridas.

Este análisis se ha considerado dividirlo en cuatro partes :

a. Equipo Físico ( Hardware ).

El análisis de la configuración propuesta y las características particulares de sus componentes, debe realizarse en función de los requerimientos de las aplicaciones, por lo que es útil controlar los siguientes puntos :

- CPU ( Unidad Central de Proceso ).

Su composición, organización, capacidades posibles, capacidad propuesta, requerimientos del sistema operativo y paquetes adicionales, capacidad libre disponible, forma de incremento real, formas de extensión virtual o dinámica; niveles de multiprogramación, protección de memoria, capacidad de terminales y periféricos, etc..

- Unidades de Entrada.

Cantidad y tipo de las unidades comprendidas en la configuración.

Lectoras Opticas de Caracteres.
Tipo y tamaño de documentos, velocidad de lectura, renta o costo, etc..

- Unidades de Salida.

Tipo y número de estas unidades.

Impresoras.
Modelo y serie, renta o costo, velocidad de impresión en líneas por minuto, etc..

Graficadores.
Tipo de graficación, mecánica de graficado, renta o costo, etc..

- Unidades de Entrada y Salida.

Tipos diferentes y cantidades de cada tipo que se consideraron en la configuración propuesta.

Terminales de Rayos Catódicos, o Pantallas.
Tipo y serie, renta o costo por unidad, capacidad de línea por pantalla, sistema de memoria, tipo de transmisión, etc..

Consolas de Impresión o Teletipos.
Velocidad de impresión y de procesamiento; caracteres por línea, tipo, renta o costo, etc..

Terminales de Audio-Respuesta.
Capacidad de palabras, validación, tipo de diálogo, líneas de comunicación, renta o costo, etc..

- Unidades de Almacenamiento.

Tipos y número de unidades incluídas en la configuración.

Cinta Magnética.
Códigos de representación, número de canales de grabación, pies de longitud, renta o costo, etc..

Disco Magnético, Acceso Directo.
Número propuesto de unidades por línea, discos fijos o removibles, mecanismos de acceso, costo o renta de paquetes y unidades, etc..

Equipos de Digitación.
Este puede ser de diversos tipos :
Grabadoras de cinta fuera de línea.
Grabadoras de disco fuera de línea.

Grabadoras de Cinta.
Número y tipos de teclado por unidad, tipo de carretes, unidad de grabación, indicación de errores, costo o renta, etc..

Grabadoras de Disco.
Estaciones por unidad, capacidad de disco, sistema de verificación, longitud de registros, velocidad de conversión, costo o renta, etc..

- Entrada Directa.

Tipo de dispositivo de digitación, requerimientos de interfase, tiempo de transferencia, consumo de memoria principal, costo o renta, etc..

- Equipo Especial.

De acuerdo a las circunstancias particulares de la instalación, pueden ser utilizados dispositivos especiales para la digitación, almacenamiento, cuyas características son dependientes de las necesidades y condiciones de la institución.

b. Sistemas de Programación ( Software ).

Los sistemas de programación propuestos, deben ser afines al equipo físico en el que van a operar, de tal manera que se logre el rendimiento óptimo de todo el sistema. Algunos puntos importantes a estudiar, con respecto a lo anterior son :

- Sistema Operativo.

Su composición en programas y rutinas, programas de control (si es que existen y sería muy bueno) y programas de servicio en la ejecución de tareas, compatibilidad con el equipo físico, consumo de memoria y espacio en disco, etc.

- Lenguajes de Programación.

Básicos, técnicos, científicos y de negocios, nivel, grado de depuración, etc..

- Programas de Servicio.

De control de cargas, de distribución de memoria, bibliografía, etc..

- Paquetes Especiales.

Paquetes científicos, de telecomunicación, para manejo de datos, para control de proyectos, de contabilidad, posibilidad de uso, nivel de desarrollo, grado de eficiencia, costos adicionales, etc..

c. Soporte.

Generalmente los proveedores del equipo suministran el soporte necesario en materia de operación, mantenimiento preventivo y correctivo de equipo y sistemas, etc., con o sin costo adicional; aún cuando lo anterior debe ser formalizado al tiempo de la contratación, es conveniente que en esta etapa sean negociadas las condiciones requeridas por el usuario y se analizen las características de calidad, cantidad y oportunidad de los servicios en el lugar de residencia del usuario.
Algunos puntos significativos podrían ser :

Características del Proveedor.

En lo referente a personalidad jurídica, nivel de responsabilidad, capacidad técnica, grado de cumplimiento, experiencia, reputación en el mercado, suficiencia de recursos de soporte, eficiencia de servicios, confiabilidad en general del equipo y sistemas, etc..

Asistencia Técnica.

Tiempo y tipo de asistencia técnica, apoyo en suministro de conceptos de análisis, programación, servicios de instalación, documentación de equipo y sistemas de programación, asesorías en el desarrollo de aplicaciones, organización, disponibilidad para asesorías, etc..

Asistencia Educacional.

Ayuda y tipos de adiestramiento al personal, planes de adiestramiento o capacitación, número de personas de cada área que capacitará, bibliografía que proporciona, número de manuales por instalación, cursos de capacitación, seminarios de actualización, tiempo de máquina para prácticas y laboratorios, fechas y duraciones de cursos, etc..

Soporte en Mantenimiento.

Características de mantenimiento preventivo y correctivo del equipo y sistemas, existencia en refacciones, periodicidad de mantenimiento preventivo, tiempos de atención a reportes de fallas, disponibilidad de personal, políticas de reemplazo de equipos y sistemas, etc..

Soporte de Máquina.

Respaldo de máquina con otros equipos durante el tiempo de entrega y en caso de fallas, tipo de descuentos por uso de máquina del proveedor en casos de exceso de trabajo, etc..

Los puntos tratados hasta ahora en el análisis de selección, deberán ser proporcionados por los proveedores participantes ya sea mediante bibliografía, documentos económicos o algún otro medio, de modo que permita, como mínimo, el análisis superficial de componentes y características de los mismos para evaluar las diferencias y ventajas de las propuestas.

d. Evaluación de Alternativas para seleccionar la mejor propuesta.

El proceso de evaluación estriba en determinar lo conveniente que es una alternativa con respecto a los demás.

Es importante aclarar que el proceso de evaluación no busca establecer si una alternativa es conveniente o no, desde un punto de vista económico, sino que debe reportar una calificación que refleje el grado de superioridad que tiene dicha alternativa, en relación a los otras para satisfacer los requerimientos preestablecidos.

Actualmente, se aplican diversas técnicas para la evaluación de propuestas, tales como : ponderación de factores, relación de costo/beneficio, de costo/valor, etc.

Es deseable que en la mayoría de los conceptos se realizen evaluaciones en equivalentes económicos, en tanto sea práctico y veraz asignarles un valor de este tipo en cada alternativa.

Es claro que, dentro de las posibles previsiones, habrá de tomarse en cuenta el costo de las extensiones o ampliaciones al Centro de Cómputo para cubrir las necesidades futuras. Esto formará parte de la evaluación económica y podrá eventualmente hacer menos deseable una propuesta, desde otros puntos de vista, atractiva actualmente por limitaciones en su crecimiento futuro o por el alto costo del mismo.

Contratación o Arrendamiento del Equipo.

- Especificación del Contrato.

La práctica de contratación en este campo no está bien establecida, los contratos estándar ofrecidos por el proveedor no son útiles y generalmente no protegen al usuario y en ocasiones al mismo proveedor de desacuerdos y malos entendidos.

Por lo que es recomendable elaborar un contrato específico o un anexo a un contrato estándar, y es conveniente proporcionar las especificaciones antes de la selección , pero una vez que los costos y detalles técnicos se conocen es cuando se hace el contrato definitivo.

- Contratación del equipo.

. Una vez que ha sido aprobada la adquisición del equipo, se formalizarán las tareas referentes a su contratación; es importante considerar los siguientes puntos :

Determinación de las condiciones de contratación con el proveedor seleccionado, en base a las cláusulas del Contrato Tipo para la Administración Pública Federal o uno de forma similar.

Existen diversas operaciones para la contratación o adquisición de equipo, las más comunes son las siguientes :

- Compra.
- Arrendamiento Total.
- Arrendamiento Total con Opción de Compra.
- Maquila, etc..

Cada una de ellas deberá ser analizada y discutida con el proveedor con objeto de :

- Seleccionar la más apropiada para el usuario y
- Conocer lo importante que es la forma de pago, para tramitar la autorización presupuestal.

Se hace notar que la maquila sólo será objeto de este contrato, siempre y cuando no exista alguna posibilidad de obtenerla dentro del mismo organismo, en el sector o en la Administración Pública Federal.

Posteriormente a las negociaciones y autorización presupuestal, tomada ya una decisión, se establecerán las condiciones del contrato, especificando las responsabilidades y derechos de ambas partes en base al:

" Clausulado mínimo que deberán contener los contratos que en materia de informática se celebren entre las dependencias y entidades de la Administración Pública federal y los diferentes proveedores de bienes y servicios ".

Tipos de contratos para el Sector Público.

- Compra-Venta de Bienes Informáticos.
- Mantenimiento a Bienes Informáticos.
- Compra-Venta de Equipo Periférico.
- Mantenimiento a Equipo Periférico.

- Compra-Venta de Microcomputadoras.
- Mantenimiento a Microcomputadoras.
- Arrendamiento de Programas para Microcomputadoras.

Para los contratos en el Sector Privado no existen y sería buena referencia tomar los del otro sector para tener un marco de referencia adecuado en los contratos de este otro tipo.

**Modelos a seguir y su Control.**

Básicamente existen dos modelos a seguir, el de Centralización y Descentralización.

Centralización.

Es un modelo en el cual todos los recursos del proceso de información dentro de toda la organización dependen de un solo individuo, sin ir a otros miembros cuyas responsabilidades están mas allá del Centro de Cómputo. Los recursos que reportan a él, no necesariamente deben estar localizadas geográficamente bajo el Director, sin embargo hay una relación directa de dependencia a un Gerente Central de Procesamiento de Datos. La organización centralizada envuelve la concentración de autoridad y responsabilidad en los niveles más altos de la organización.

Ventajas para la Centralización.

La razón mas frecuente utilizada para la Centralización de operaciones es la " Economía de Escala " y ésta, resulta de varios factores :

- Decentralizar computadoras pequeñas puede traernos capacidad sin uso. La Centralización en una computadora de gran tamaño, podría eliminar el costo de tal capacidad sin uso.
- Las pequeñas computadoras individuales pueden ser sobrecargadas generando presión para el ascenso del equipo o permitiendo tiempo de servicio muy caro. La Centralización en una gran computadora podría absorver esta carga contra la capacidad sin uso de otras microcomputadoras.
- En términos de espacio de piso, electricidad, aire acondicionado y sistemas de seguridad; una gran instalación es menos costosa que múltiples instalaciones pequeñas.
- El número de personal del área, es menor para una gran instalación que para muchas pequeñas.
- Una gran instalación requerirá menos personal ejecutivo que una pequeña.
- Una gran computadora es mas efectiva en costo que una microcomputadora.

Las grandes computadoras tienen además otras ventajas además de la Economía de Escala, que son :

- Mayor Velocidad Interna.
- Mayor Memoria Principal.
- Mayor Capacidad de Canales.

que pueden hacer ciertas aplicaciones prácticas que una minicomputadora no podría hacer.

La Centralización permite el diseño y uso de bases de datos de bases comunes, así como de estándares comunes para la inserción de datos y la variación de las entradas permite también, la facilidad de utilizar técnicas de desarrollo y control de proyectos que resultan en beneficios específicos para la institución.

Algunos de estos beneficios son la capacidad de :

- Implementar un Diccionario de Datos, ahorrando un tiempo considerable en, la búsqueda ó localización para una modificación del sistema.
- Establecer y reforzar documentación de estándares del sistema para asegurar mantenimiento permanente para los sistemas y programas.
- Regularizar estándares, para la documentación del usuario, considerando la facilidad de archivos, los beneficios óptimos del sistema.
- Establecer y revisar las técnicas apropiadas de programación para minimizar el uso ineficiente de las facilidades del sistema.
- Evaluar el desarrollo de proyectos, estableciendo prioridades, conductas de costo/beneficio, análisis, etc..
- Evitar desarrollo redundante de sistemas similares para diferentes divisiones de la compañía.
- Aplicar buenas técnicas de control de proyectos, asegurándose que los proyectos se completan bajo los tiempos requeridos y bajo los límites de costo/beneficio.

**Desventajas de la Centralización.**

- Tendencias a sacrificar los requerimientos y necesidades de los usuarios en favor de las necesidades y objetivos de la organización.
- Tendencia a formar un conjunto de analistas y programadores que no estén familiarizados lo suficiente con los requerimientos del usuario en forma específica, para el desarrollo de sistemas de información efectiva.
- El tener un sistema de cargos equitativo que a su vez lleve a un uso de los recursos de cómputo equitativamente.
- Establecimientos inadecuados de prioridades entre los usuarios.

- Dificultad para la planeación a largo plazo porque los planes de los usuarios no están lo suficientemente detallados o toman en cuenta los requerimientos de cómputo.
- Aumento en los gastos de transmisión, cuando existe dispersión geográfica.

Decentralización.

Un modelo de organización de este tipo es lo contrario del modelo anterior, esto implica que los recursos para procesamiento de datos reportan a varios elementos y la organización, en estos recursos pueden estar fraccionados geográficamente. La Decentralización genera la desconcentración de autoridad y responsabilidad en los niveles de la organización.

En los últimos años se ha desarrollado este modelo, con el incremento de microcomputadoras, un potencial de ahorro.

Las microcomputadoras son programadas para una aplicación específica; por lo tanto es usada como una máquina de oficina que no necesita el soporte técnico de programación y operación de una máquina de propósito general.

La decentralización implica también que cada usuario importante de una organización tenga su propio Centro de Cómputo y que las unidades decentralizadas tengan también sus propios servicios de cómputo. Este enfoque es conveniente para organizaciones con numerosos subsidios en distintas actividades o para organizaciones con grandes unidades y con distintas localizaciones geográficas.

Es posible transferir información de un lugar a otro usando equipos económicos de comunicación de datos ó enviando papeles, cintas, diskettes o cassetes.

Ventajas de la Decentralización.

- Los sistemas definidos para la organización usuaria sirven óptimamente las necesidades del usuario y satisfacen totalmente los objetivos del usuario, independientemente de los objetivos de la institución que también necesitan ser satisfechos.

- Los grupos operativos tienen control directo de su organización en el proceso de información, lo que es deseable para las operaciones diarias de la alta prioridad.

- Se fortalece la responsabilidad ya que cada usuario es directamente responsable de sus costos por el proceso de información.

- Por el conocimiento que tienen sus requerimientos, la instalación requiere el número de equipos y recursos.

- El control directo por parte del usuario facilita una planeación a largo plazo, mas directa que la hecha de manera indirecta.

Desventajas de la Decentralización.

- No hay Economía de Escala en el uso del equipo y de otros recursos.
- Es a veces imposible o al menos muy difícil integrar áreas de aplicación a lo largo de diferentes usuarios.
- Es muy difícil estandarizar las prácticas políticas del proceso de datos a lo largo de la organización.
- Los gastos generales fijos referentes al proceso de datos se repiten en cada una de las organizaciones, por lo tanto puede conducir a costos excesivos.
- Es difícil reclutar gente para el proceso de datos centralmente para muchas organizaciones diferentes.
- Puede haber competencia en la contratación de personal tanto interno como externo.
- El tener varias y diferentes organizaciones hace que no contribuyan de la mejor manera posible a alcanzar los objetivos generales de la institución.

**Proyectos de Sistemas.**

Contiene todos los proyectos que el usuario y la Gerencia de Sistemas ven para los siguientes años (2 a 5). Los proyectos pueden ser divididos en categorías. Los Proyectos Planeados son tentativamente catalogados.

Los proyectos propuestos son listados, los usuarios pueden borrar, agregar o cambiar en los proyectos planeados y propuestos. Cada proyecto debe seguir un desarrollo de sistemas estándar en su metodología con puntos de chequeo y revisarlos al final de cada fase.

Estos planes deberán estar a un año, firmes, a tres años razonablemente firmes, a cinco años, generales y a diez años estimados en una forma muy general. Así, el auditor puede planear mejor su trabajo, puede practicar también con una aproximación de diagnóstico/preventivo o manejar un papel de consultor en el cuál puede detectar puntos problema y enderezar el camino de la planeación.

### 3.1.2 CONTROL DEL PERSONAL.

**Reclutamiento y Selección de Personal.**

Todo administrador de un Centro de Cómputo debe tener presente la importancia que representa su personal en el logro de los objetivos de la institución.

Selección del Personal.

- Personal de la propia empresa.
  - Convocatoria a oposición, en dónde se fijan los requerimientos del puesto.
  - Exámenes de Suficiencia.
  - Erradicación del área de trabajo actual, para dedicarse al nuevo puesto en tiempo completo.
  - Capacitación técnica.

- Personal externo a la empresa.
  - Procedimientos tradicionales.
    No incurrir en el error de caer en alguna de las formas tradicionales, sino preferir la metodología estrucurada de selección. (Ver Técnicas de Reclut. y Selección)
  - Las recomendaciones.
    Se coloca al recomendado en un puesto cualquiera sin prestar atención a los conocimientos o aptitudes. Son producto de la amistad y el compadrazgo. Obviamente esto se debe evitar.

- Empleado Inexperto.

Las solicitudes difieren en atributos físicos, capacidad, temperamento, intereses, actitud, etc.. Debido a estas diferencias, no hay dos solicitantes que aprendan o se desempeñen exactamente igual, aunque la investigación realizada en el campo del personal de computación nos permite establecer directrices para formular, con mayor confianza, juicios para contratar empleados inexpertos.

Partiendo de la forma de solicitud o de datos básicos del personal, más una entrevista, se pueden hacer varios juicios razonables de la capacidad para aprender que tenga el solicitante inexperto en el campo de la computación, su capacidad para llevarse bien con otros, su grado de madurez y también si será estable en su empleo.

Además por medio de pruebas psicológicas se puede obtener mayor información acerca de la inteligencia general del solicitante, sus intereses y aptitudes para empleos en el campo de procesamiento de datos. Mediante pruebas de inteligencia se obtiene un índice de la capacidad general que tiene un solicitante para aprender, independientemente de su nivel educativo. Este índice puede ayudar a seleccionar solicitantes que pueden aprender un trabajo, como programación de computadoras, aunque no hayan tenido educación muy superior. Con las pruebas se puede evaluar la competencia del personal de computadoras experimentado y, al mismo tiempo, predecir la actuación en el trabajo de solicitantes que no hayan tenido experiencia previa.

- Empleado Experimentado.

En este caso, independientemente a la cantidad de datos personales que reunan y de lo difícil que es la prueba de conocimientos que se utilice, el factor más importante para predecir como se desempeñó anteriormente. Esta regla es más válida a medida que aumenta la semejanza del trabajo anterior con el que se desempeñará en el futuro.

A pesar de lo expuesto aquí, para seleccionar al personal del Centro de Cómputo es recomendable seguir técnicas las cuales nos lleven a reclutar personal calificado.

La calidad del personal como en cualquier otra área de la organización debe ser efectiva y operacional y para seleccionarla y reclutarla necesitamos lo siguiente :

Técnicas de Reclutamiento y Selección.

El control del buen personal incluye el emplear a la gente correcta en primer lugar. Los siguientes aspectos deben ser considerados :

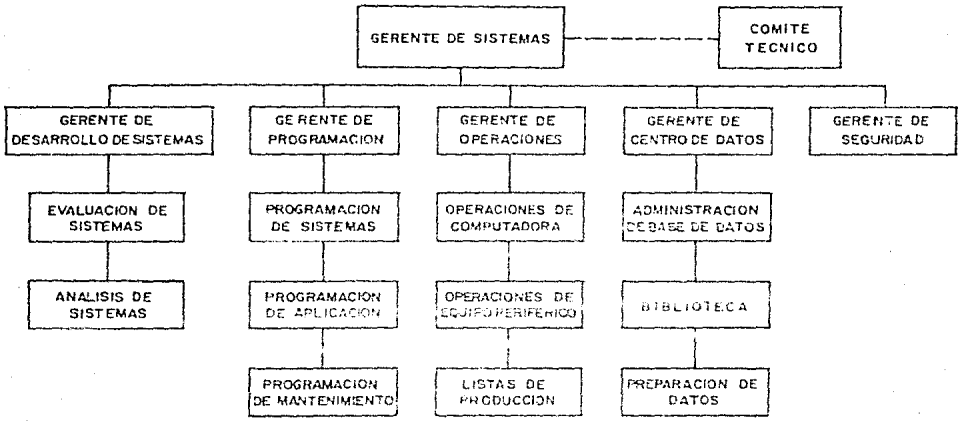
- La habilidad técnica es fundamental. Uno no puede contratar gente a menos que tenga la capacidad técnica para realizar las tareas.
- El carácter y la estabilidad emocional son factores clave.
- La experiencia anterior debe ser investigada. Si su pasado es inadecuado o sucio hay una oportunidad muy pequeña de que ahora será diferente.
- La habilidad de la persona para manejar sus propios asuntos, especialmente financieros, ayuda a indicarnos el nivel de riesgo en emplear a una persona en particular. Los problemas financieros pueden provocar a las personas a que cometan fraude.
- Una investigación de los lugares dónde han sido rechazados, puede ayudar a identificar a una persona indeseable.
- Ver su escolaridad que tenga relación con el procesamiento electrónico de datos como un estándar mínimo.

Funciones y Responsabilidades.

El éxito o falla de un sistema de información está primeramente en la calidad de su gente. Probablemente el galardón mas grande de la administración es la de reclutar, entrenar, retener y manejar efectivamente personal calificado .

Un problema adicional al auditor es que el personal del Centro de Cómputo no se siente familiarizado con él y no puede entonces relacionar sus convenciones tradicionales de contabilidad y auditoría. La gente de sistemas los ve como alguien que está obstruyendo su trabajo.

La figura 3 presenta un diagrama de organización que ilustra la variedad de tipos de puestos que existen en un Centro de Cómputo.




F I G U R A 3

Organigrama Típico de un Centro de Cómputo

La administración de las categorías en este diagrama es responsabilidad de :

a. Gerente de Sistemas
b. Desarrollo de Sistemas
c. Programación
d. Operaciones
e. Centro de Datos
f. Seguridad

a. El Gerente de Sistemas debe poder unificar lo diverso y suboptimizar los departamentos de la organización por medio de un flujo de información imparcial a todos los usuarios. El, por lo general tiene un puesto alto y debe tener una administración fuerte, como también un respaldo técnico. Sus actividades deben ser neutrales e independientes de otros ejecutivos en la organización. No debe avocarse a ningún departamento y debe ser responsable solamente de la alta gerencia, directores, y/o dueños de la organización.
Las funciones de esta persona incluyen :
- Planear y controlar todas las actividades en el Centro de Cómputo.

Esto incluye planes a corto plazo para desarrollo de sistemas, adquisición de software y equipo, y operaciones de la computadora incluyendo a su vez, manejo de estándares, monitoreos y evaluaciones de operación, realizaciones en software y hardware, y actividades personales.
En esta función se incluye un programa de seguridad diseñado para salvaguardar al personal, programas, base de datos, hardware y equipos periféricos .

- Actuar como punto de unión del sistema con los usuarios. Esto incluye comunicación con la alta gerencia y con los usuarios del sistema de los planes y actividades del sistema, programas educacionales y de capacitación de estos usuarios.
- Administrar al personal. Incluyendo selección, capacitación y manejo del personal de Centro de Cómputo.
- Administración General incluye algunas políticas presupuestales y análisis de costo/beneficio. Tener prioridades y la carga de usuarios al sistema para manejo de costos incluye también mantener relación adecuada con vendedores y proveedores, y mantener un sistema de evaluación en la adquisición de hardware y software y otras facilidades.

b. La categoría de desarrollo de sistemas incluye el análisis, diseño, evaluación, e implementación de los sistemas de información para los usuarios de la organización. La planeación y la evaluación presente y sistemas de hardware y software propuestos resultan en recomendaciones para modificaciones y/o adquisiciones de hardware y software. En algunos sistemas esta parte puede ser soportada por especialistas en comunicaciones de datos quienes diseñan e implementan redes de comunicación, incluyendo el software, terminales, modems, etc.
Esta categoría de desarrollo de sistemas puede utilizar también los servicios de un analista de métodos y procedimientos para el desarrollo de métodos, procedimientos, formas, como parte del desarrollo de un nuevo sistema.

c. Este Gerente supervisa al personal de programación quienes son los responsables para el desarrollo y mantenimiento del software lógico.
Se dividen en tres categorías :

- Un programador de sistemas quien desarrolla y mantiene al sistema operativo y otro software técnico que son los que controlan las funciones básicas de la computadora.
Debe ser una persona altamente capacitada y tener habilidad para el software y hardware. Las instrucciones son escritas en lenguaje ensamblador o en lenguaje de máquina.

- Un programador de aplicación quien diseña, codifica, prueba e implementa programas de computadora para aplicaciones específicas, y son escritos en un lenguaje de alto nivel.
- El programador de mantenimiento quien hace cambios y correciones a programas de aplicación existentes.

d. Este supervisa a los operadores del equipo y a las listas de trabajp através del sistema. Su trabajo es igual al de un capataz en un proceso de producción. Monitorea y controla a la computadora por medio de la consola de la computadora central. Los operadores de equipo periférico asisten al operador con el manejo de cintas, discos, impresoras, etc. El encargado de la producción de trabajos (jobs,tasks), coordina y controla la mezcla de trabajos para alcanzar la optimización en el uso del equipo y el servicio a usuarios. Mantiene registro de trabajos y de utilización de equipos. Los dependientes de esta persona son quienes ensamblan archivos y proporcionan el material necesario para el procesamiento de datos de acuerdo a las especificaciones del trabajo (job), y existen los empleados de control que se encargan de revisar el trabajo y de su distribución.

e. El Gerente del Centro de Datos (Data Center) supervisa el manejo de datos que son procesados en el sistema. Existen tres áreas mayores de esta categoría que son :

- El administrador de la base de datos quien diseña y controla la base de datos del sistema. El conjunta y efectúa estándares para el uso, control y seguridad de todos los archivos en la base de datos.
- La biblioteca de datos es una estructura bien construída (a prueba de incendios ) y es utilizada para guardar archivos importantes de datos, programas, documentación y otros materiales. Esto se hace bajo el control de una persona, referido a veces al bibliotecario de operaciones, quien controla la recepción y acomodo del material contenido en la biblioteca .
- La preparación de datos requiere dispositivos para convertir datos en formas procesables por la computadora. Esta área incluye operadores de equipo de entrada de datos quienes convierten datos en documentos fuente dentro de una forma leíble por la computadora y usando formas en cinta, en disco, en terminales, etc. En sistemas mas avanzados los usuarios meten sus datos sin ayuda de un operador, esto necesita otro tipo de controles que se verán adelante.

f. El Gerente de Seguridad supervisa una variedad de oficiales de seguridad para proveer seguridad completa al sistema. En un Centro de Cómputo la integración de funciones de procesamiento en un sistema concentrado con poco personal incrementa el riesgo de accesos no-autorizados, fraudes, sabotajes, robo y destrucción.

La seguridad contra esto es incluir monitores de T.V., procedimientos de identificación y de checar entradas/salidas, entrada por una sola puerta, etc.

**Establecimiento de Estándares.**

No solo se deberían establecer los estándares, sino que son acompañados de arreglos que reportan a la Gerencia cualquier desviación significativa de los estándares. Las bases medibles para estándares comprenden procedimientos, calidad, cantidad, tiempo y dinero. Y se relacionan con el personal, el software, el hardware y las bases de datos.

Estándar de Operaciones de Computadora.

Los Gerentes y Auditores raramente tienen el entendimiento técnico para controlar efectivamente las operaciones de la computadora utilizando métodos tradicionales y confían unicamente en el control presupuestal.

Sin embargo, los presupuestos operativos de las computadoras en muchas organizaciones se han incrementado significativamente año con año sin una ganancia relativa en efectividad. Obviamente, el Control Presupuestal no es suficiente si es utilizado por sí mismo.

En años recientes, algunos Gerentes han intentado ganar un control efectivo por medio de un control presupuestario suplementario realizándolo con sus herramientas de evaluación.

Estas herramientas generan reportes que reflejan las tendencias en capacidad disponible y la utilización de esta capacidad.

Tres de estas herramientas de evaluación que proveen estas clases de reportes son monitores de hardware, monitores de software y paquetes de contabilidad. Estas herramientas, especialmente el paquete, también es aplicado a las técnicas de auditoría.

Estándar de Sistemas y Trabajo de Programación.

Este punto a diferencia de las operaciones de la computadora, no depende de las características físicas de la máquina, sino que depende, de la creatividad por naturaleza. Sin embargo, la combinación de dos procedimientos nos ayudará a manejar nuestro trabajo y son :

- Estimar tiempo para las tareas del proyecto.

  Una vez que el analista de sistemas o el programador determinen las tareas apropiadas para el proyecto, el debe determinar cuanto tiempo se requiere para realizar cada uno, por ejemplo, una tarea de sistemas es entrevistar, y los analistas de sistemas pueden estimar que esto tomará seis días de trabajo completarla. O un programador que le tomarán dos días probar un módulo de un programa en particular.

- Listando y controlando las tareas del proyecto.

  Una vez que se han estimado los tiempos de las tareas, con diagramaje de Gantt y las técnicas de red (CPM, PERT, etc.) deben de utilizarse para el mejor manejo de nuestros recursos y controlar los sistemas y el trabajo de programación.

Estándares de Procesamiento de Datos Generales.

Los siguientes estándares generales pueden incrementar sustancialmente la administración y el control de un Centro de Cómputo.

- Estándar de definición de datos y nombres.

  La definición de datos y los nombres en su consistencia ayudan a realizar operaciones del sistema, mas efectivo y armonioso. La inconsistencia crea confusión. Por ejemplo, si las cuentas por cobrar son llamados CU-P-COB en una rutina y CTAS-X-COB en otra y estas rutinas son utilizadas juntas en un trabajo, para la computadora y para el usuario los dos nombres pueden tomarlos tan diferentes como blanco y negro.

- Estándar en los lenguajes de programación.

  No hay razón para gastar miles de horas-hombre desarrollando programas escritos en algún lenguaje obscuro solamente para encontrarse mas tarde con que no se está manteniendo por el proveedor o es incompatible con el nuevo equipo. Un lenguaje estándar tal como COBOL, BASIC, debe ser utilizado. Esto no es totalmente independiente de la máquina, pero es mejor que la mayoría de los lenguajes.

- Programación Estructurada, Modular y Top-Down.

  La programación es el arte de partir un programa grande en módulos que pueden estar trabajando y probándose por separado. Esta técnica es muy buena, pues en cambios al programa es mas fácil corregir un módulo que el programa completo.
  La programación estructurada Top-Down es una técnica utilizada por los programadores para escribir programas que pueden ser leídos de arriba a abajo sin brincar atrás para un párrafo o instrucción. En esta programación, hay un intento para tener un punto de entrada y un punto de salida y eliminar los "GO TO". Esta técnica incrementa la eficiencia de los programadores y simplifica el mantenimiento.

Administración de Personal.

Una vez que el personal ha sido contratado y debe ser administrado apropiadamente. Controlando un Centro de Cómputo es básicamente una manera de controlar al personal de cómputo. Este personal debe ser provisto de una clara responsabilidad y autoridad y debe ser conciente de las metas de la organización. Los métodos administrativos tradicionales deberían ser establecidos para determinar si las metas están siendo alcanzadas.

El personal administrativo debe ser seleccionado para la acción de administrar, aunque obviamente debe tener conocimientos técnicos.

No toda la gente que maneja un programa de software eficientemente puede manejar un proyecto entero.

Establecimiento de Metas y Políticas.

En el pasado y aún hoy en día, mucha gente inteligente y competente ha introducido el campo de la computadora porque fueron atraídos por el glamour, por el reto, y la mística de la computadora. Muchos de ellos tienen mas lealtad a la computadora que a la organización. Toda esta gente está desinteresada en políticas de control, de presupuesto, de administración, y las metas de la organización son vistas como una interferencia con sus objetivos personales, pero eso sí, utilizando las últimas novedades en equipo.

Las metas de la organización deben ser muy claras y los métodos para alcanzarlas deben ser integrados.

Revisiones periódicas del personal hacen una contribución significativa para saber que se lleva de trabajo y quien lo está haciendo.

Separar Areas Funcionales.

Una línea debe ser dibujada entre el personal que autoriza una transacción, aquellos quienes producen la entrada, aquellos quienes procesan los datos, aquellos quienes manejan los datos y aquellos quienes utilizan la salida.

Las áreas funcionales que deberían ser separadas en el Centro de Cómputo son :

- Grupo de Analistas de Sistemas.
- Grupo de Programación.
- Operadores de Computadora.
- Bibliotecarios de Cintas, Discos, y Documentos.
- Responsables de Entrada y Conversión de Datos.

La separación anterior divide apropiadamente las actividades de operación y desarrollo. Sin embargo, donde la gente debe trabajar conjuntamente debe ser puesta en grupos de trabajo de tres, cualquier cosa mal hecha es reportada usualmente por la "tercera" persona.

Otras formas de separación de las áreas funcionales son :

Rotación del personal y vacaciones asignadas por la gerencia. La rotación del personal previene a cualquier empleado de dominar una área. Mas aún, esto provee no solamente un chequeo cruzado, sino que reduce la propensión de confiar a un empleado donde otro puede hacer ese mismo trabajo. Al menos dos semanas consecutivas de vacaciones deben ser requeridas de todo el personal clave. Un número de abusos y errores han sido enfrentados durante los perfodos de vacaciones, porque la persona realiza un fraude o algunos otros abusos que no fueron controlados.

Programa de Capacitación .

Sin una selección y capacitación adecuada al personal, es muy difícil, no imposible, desarrollar un Centro de Cómputo efectivo y viable. Aún mas, la responsabilidad de la administración del Centro de Cómputo, debe establecer programas de capacitación para nuevos empleados para su orientación y entrenamiento. Sin olvidar actualizar al personal experimentado.

Como parte importante de la capacitación, se deben incluir los siguientes puntos :

- Asistencia a Universidades y Colegios.
- Asistencia a Escuelas de Computación reconocidas.
- Seminarios profesionales, conferencias y cursos.
- Programas de capacitación interna.
- Asignaciones especiales de trabajo con los cuales se van a ir capacitando.

Cada compañía debería tener un programa de capacitación interno ya que si este existe será todo su peso en oro, esto hará que se tenga un personal altamente calificado. Si existiera este programa de capacitación desde el punto de vista de los empleados, incrementará su motivación y empezarán a comprender tareas y trabajos más complejos.

Por lo tanto es mas fácil para una organización reclutar nuevo personal si este tiene un programa de capacitación.

Además sería conveniente instalar una biblioteca técnica para el personal de sistemas, la biblioteca debería incluir publicaciones de la industria actual, toda la documentación del sistema(s), los manuales del control del proyecto(s), manuales de estándares y manuales de capacitación y referencia. Esta lista crecerá conforme a las necesidades del crecimiento del procesamiento de datos.

### 3.1.3 CONTROL DEL PRESUPUESTO.

El proceso de presupuestación es de suma importancia; en este se integran los diferentes elementos participantes, como son recursos humanos, materiales y erogaciones necesarias para la implantación total del servicio, lo que permite la visión integral de la situación,

reforzando con ello la base de la decisión.

Es importante considerar para su desarrollo, que el resultado es la expresión financiera de un plan programado de acción, en el cuál deberán ser previstos todos los conceptos indicados, los calendarios de aplicación del gasto y los resultados esperados en el tiempo.

Generalmente, los recursos económicos de una institución, resultan limitados para la satisfacción de sus necesidades, por lo que la aplicación de un gasto insuficiente para tener un requerimiento puede dar origen a nuevas y mayores demandas; es recomendable por lo tanto, evaluar el costo real y total de las implicaciones y generar en todo caso diferentes opciones con respecto al tiempo, puntualizando las metas fijadas.

Es recomendable que este tipo de funciones sean realizadas por especialistas en la materia.

Algunos de los principales aspectos por considerar en términos monetarios se mencionan a continuación :

Recursos Humanos.

- Personal de Dirección.
- Personal de Supervisión.
- Personal Técnico.
- Personal Administrativo, de Apoyo, etc..

Recursos Materiales. Renta o Compra.

- Local y Acondicionamiento del mismo.
- Sistema de Cómputo, sus componentes y accesorios.
- Mobiliario y Equipo de Oficina.
- Equipos Complementarios de Emergencia y Soporte Ambiental.
- Material de Oficina y Bienes de Consumo.
- Material Didáctico y Publicaciones, etc..

Otros Gastos.

- Gastos de Instalación.
- Gastos de Mantenimiento de Equipo.
- Gastos de Energía Eléctrica.
- Impuestos.
- Gastos de Importación de algún bien.
- Gastos de Transportación y hospedaje del personal.
- Gastos de Capacitación de Recursos Humanos.
- Gastos de Asesoría y Consultoría, etc..

Las etapas en que puede ser desarrollado son :

- Integración de la información de recursos humanos y materiales requeridos.
- Investigación y Cotización actual de recursos y servicios necesarios.
- Determinación de gastos directos necesarios.
- Formulación y Revisión del presupuesto.
- Documentación y presentación para el análisis del mismo.

**Prueba de los Sistemas Propuestos.**

Una vez identificadas las características e implicaciones de los diferentes sistemas de cómputo, es conveniente realizar una serie de pruebas BENCHMARK, sobre la productividad de los mismos en tiempo de proceso, con la ejecución de una mezcla de aplicacciones que sean representativas de las necesidades del usuario tanto en condiciones de procesamiento como en volumen.

Finalmente deberán analizarse los resultados obtenidos y seleccionar aquellas propuestas que cumplan correctamente con los requisitos.

**Selección de propuestas para evaluación.**

El proceso de selección de las propuestas que pasarán a la evaluación final, puede apoyarse en el uso de tablas comparativas como las que han sido elaboradas por la Sociedad Mexicana de Computación Electrónica, A.C.

**Conclusión del Análisis de Propuestas.**

Como resultado del análisis particular de cada propuesta, deberá formularse un documento que justifique la selección respectiva y presentar ésta ante un Comité de Decisiones con la descripción de los criterios de eliminación utilizados.

## 3.2 CONTROLES OPERACIONALES.

**Introducción.**

Los controles operacionales directamente relacionados a las operaciones diarias de procesamiento de datos incluyen:

1. Controles de entrada.
2. Controles del sistema operativo.
3. Controles del procesamiento.
4. Controles en programas de aplicación.
5. Controles del sistema de manejo de base de datos.
6. Controles integrados a la computadora.
7. Controles para la operación de la computadora.
8. Controles de biblioteca y base de datos.
9. Controles de salida.

### 3.2.1 CONTROLES DE ENTRADA.

Se divide en cuatro áreas:

- Códigos de entrada
- Preparación de la entrada
- Verificación de la entrada

- Terminación de la entrada

**Códigos de Entrada.**

Los sistemas de información actuales no pueden tolerar significados ambiguos o la entrada de datos erróneos en registros computarizados tales como tarjetas de crédito , archivos personales, archivos de inventario, formas de impuestos, ventas, reservaciones en aerolíneas, etc.. Antes de autorizar la entrada de datos se debe identificar, clasificar y definir los elementos de datos involucrados.

En cualquier organización, los elementos de los datos (documentos de transacción, campos, registros, archivos etc. ) representan gente, eventos, objetos, etc..

Todos estos elementos individuales son datos para ser grabados y procesados. Por ejemplo, los empleados o bienes en una tienda de departamentos pueden considerarse como datos a capturar, introducirlos al sistema y procesarlos. Es importante que todos los datos procesados por la computadora sean representados apropiadamente e identificados de forma única.

Los códigos proveen una estructura abreviada para clasificar e identificar en forma única datos en la entrada, en la comunicación, proceso, y/o recuperación. El uso de las computadoras ha dado un fuerte ímpetu a la utilización de codigos, especialmente códigos numéricos y de barra para un control y procesamiento efectivos. Las siguientes son algunas de las más conocidas estructuras de código:

a. Códigos secuenciales.

Representa un asignamiento consecutivo de números de artículos tales como chequeras, números de cuenta, artículos de inventario, ordenes de compra, empleados, etc. Es de uso simple, identifica de manera única, es muy útil en muchas aplicaciones de control y puede usarse como código estructurado. Los documentos básicos como cheques, bonos, ordenes de venta, compra y facturas deben tener números secuenciales preimpresos. Los documentos deben mantenerse fuera del Centro de Cómputo y cederlos para su procesamiento. Después del procesamiento , las formas deben regresar al área de control responsable. Cualquier forma de dato que no esté bajo control debe rastrearse inmediatamente.

b. Códigos en bloque.

Clasifica artículos dentro de ciertos grupos donde los bloques de número se asignan a clasificaciones particulares. El bloque que representa una clasificación debe situarse sobre la base de una utilización máxima esperada de ese bloque. Por ejemplo, revisar la estructura de código de bloque representado a continuación:

| número del código \ | código de posición | | |
|---|---|---|---|
| 1 | escritorio | arrendamiento | contabilidad |
| 2 | silla | comprar | mercadotecnia |
| 3 | librero | rentar | producción |
| 4 | copiadora | --- | --- |

Si un elemento de los datos se introduce en el sistema con un código 421, significa que una copiadora que se ha comprado se asignó al departamento de contabilidad.

Este código también es aplicable al área de contabilidad, donde letras y dígitos pueden representan entre otras cosas la identificación de un artículo, su ubicación en el almacén, el departamento de usuario, etc..

c. Códigos de barra.

Las diferentes configuraciones de barra mostradas en la figura 3 son llamados códigos de barra. La de la parte superior se usa en la industria de los comestibles.

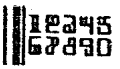
Los símbolos se pueden leer fácilmente por la computadora y convertirlos en números que representen el código. Cambiando el espesor de las barras y el espacio entre ellas, pueden identificarse de forma única todas las variaciones de productos y tamaños.

Este código requiere el uso de equipo sofisticado conectado a una computadora. Los artículos conteniendo el código de barra se pasan por un scanner láser, el cual lee el código y le transfiere a la computadora información como precio correcto, tipo, tamaño y otros datos , los cuales son presentados en pantalla e impresos en un boleto de compra al mismo tiempo . El proceso de entrada y contar un artículo toma una fracción de segundo.

Este código permite reducir el tiempo de chequeo, actualiza el control de inventarios, elimina el etiquetar los precios y cambiar precios en cada artículo. Reduce la probabilidad de errores humanos, los hurtos y los fraudes en la manipulación de las cajas registradoras.

LITTON

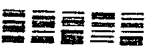
IBM



SCANNER

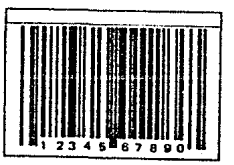
0123456789
CHARECOGN

PITNEY-BOWES



SINGER

RCA



THE SELECTED UPC CODE

F I G U R A 4

Códigos de Barra

**Preparación de la Entrada.**

La preparación de documentos de entrada y transacciones siempre deben ser manejados por personas autorizadas fuera del Centro de Cómputo. Para asegurar una preparación de entrada apropiada, deben implementarse los siguientes procedimientos:

- Todas las transacciones deben codificarse ( por códigos aprobados ) por un departamento autorizado.

- Donde sea posible, debe prepararse un control de totales por parte del departamento de origen.

- Formas confidenciales como libretas bancarias, cheques, registros de accionistas deben ser prenumerados y controlados fuera del Centro de Cómputo.

**Verificación de la Entrada.**

La introducción de documentos preparada por un empleado debe verificarse o corregirse por otro cuando el resultado de los datos requiere un alto grado de exactitud. La verificación es una operación duplicada y por tanto incrementan el costo de la entrada de datos. Para reducir este costo se pueden verificar unicamente los datos críticos tales como totales y números de cuenta, ignorando nombres, direcciones, sexo, etc..

Debe quedar bien claro que la verificación no implica la detección de todos los errores de transcripción. De hecho, los errores se reducen pero no se eliminan totalmente.

**Terminación de la Entrada.**

Terminar la entrada, significa que toda la entrada que se supone presente y procesada está, lo esté en verdad. Para asegurarse de ello se deben usar controles como los siguientes:

- Control total de la cantidad.

  Se usa para determinar los resultados de algunos cálculos. Se establece normalmente para batch's de un tamaño conveniente tal como un departamento, locación, cuenta o división. Cada batch de registros puede balancearse conforme se procesa. Una acción correctiva si es necesario puede aplicarse a pequeños batch's fácilmente checables que un gran total. Por ejemplo, en un almacén de departamentos, se graba el total de artículos vendidos y también se hace por departamento; la suma de estos últimos debe coincidir con el total del almacén, sino, algún dato está mal.

- Control total del conteo grabado.

Involucra la incorporación de todos los datos de entrada. Por ejemplo, si hay 100 registros a ser procesados y sólo 99 son encontrados, obviamente hay una pérdida; similarmente si hay 100 registros para procesar y el resultado arroja 110, también es erróneo. Después de que se han contado los registros, el número total de registros se lleva como un control total al inicio y al final del archivo, cambiándose si hay registros añadidos o borrados, balanceando este nuevo total contra el original o el total ajustado. Si el recuento está de acuerdo con el control total, se acepta como prueba de que todos los registros han sido procesados.

- Control total hash.

Se aplica a cantidades no monetarias. Generalmente es añadiendo un control extra. Por ejemplo, en una nómina, la adición de números a los números de empleados, a los números de Seguro Social o a los números del departamento.

### 3.2.2 CONTROLES DEL SISTEMA OPERATIVO.

El auditor debe tener una comprensión básica de la secuencia lógica de eventos que afectan al programa en uso. La interacción principal es entre el programa y el sistema operativo. En un intento de familiarizar al auditor con los sistemas operativos se dan las siguientes descripciones operativas.

Desde el momento que se hace la captura de datos hasta que ha finalizado la impresión , una serie de programas integrados conocidos como sistema operativo interactúa con el programa. El sistema operativo es un paquete integrado por programas muy complejos y sofisticados; es el software más poderoso utilizado por la computadora; controla enteramente la operación del hardware y mantiene control de todas las operaciones que ocurren dentro de la computadora. Desde la posición de un auditor, se debe tener en cuenta que el sistema operativo tiene la capacidad de suprimir registros en archivos, insertar módulos en programas, correr rutinas de seguridad y modificar paquetes auditores de la computadora, los cuales pueden dar la impresión de que está operando correctamente.

No se han desarrollado procedimientos auditores que prueben el sistema operativo, entre las razones primordiales, podrían incluirse la complejidad y el tamaño del sistema en sí, además generalmente están escritos en lenguaje de bajo nivel el cual es mucho más detallado que un lenguaje de alto nivel.

No obstante que no haya paquetes de software específicos para auditar un sistema operativo, hay herramientas dentro del propio sistema operativo que auxilian al auditor. Corresponde al auditor aprender el uso de estas herramientas y familiarizarse con los procedimientos para utilizarlos apropiadamente, algunas las tenemos a continuación.

Programas de Aplicación.

Es una serie de instrucciones escritas en un lenguaje de programación; se diseña para ejecutar una tarea. Sin un control, los programas pueden diseñarse para efectuar tareas fraudulentas. El programador de un programa de aplicación tiene el potencial de crear un desastre intencional o no, debido a que entiende la tecnología de la computadora y está ligado a la aplicación. Hay muchas instancias en las cuales los programadores han escrito programas que efectúan tareas que no están de acuerdo con los principios aceptados por la organización, intencional o no intencionalmente.

Compilación - Traducción de Lenguaje.

Compilación puede definirse como la traducción de un programa fuente escrito en algún lenguaje a un programa objeto o ejecutable. Ordinariamente, no pueden hacerse cambios al programa en esta etapa.

Etapa de preprocesador.

Durante esta etapa, el programador puede efectuar tres funciones con respecto al programa antes de que pase a ser programa objeto:

- Se puede cambiar el nombre de cualquier variable que aparezca en el listado original. Para el auditor, significa que cualquier variable que vea en el listado del programa fuente, puede en efecto, no ser la variable que está usando el programa objeto.

- Requerir una compilación adicional, lo cual, permitiría al programador identificar aquellas porciones del programa que no quizo fueran compiladas. Al ejecutar una función auditora, el programador podría desactivar esa sección al no incluirla en el programa objeto simplemente especificando que la sección bajo auditoría no será compilada.

- Series de textos que aparezcan en la biblioteca de un usuario o en un sistema de biblioteca, pueden ser incorporadas al programa, de tal manera que son compiladas y vienen a tomar una parte operativa del programa compilado. Para el auditor esto significa que un programador puede incluir módulos parciales o totales, que ejecuten cualquier función que el programa estime conveniente.

Etapa de procesador.

La salida del preprocesador es compilada y ya se tiene el programa objeto. Las computadoras ejecutan un código objeto, el cual es difícil de utilizar con eficiencia y facilidad. Por tanto los lenguajes de programación han sido desarrollados para que los humanos interactúen facilmente con la computadora. El compilador produce un programa objeto en un formato estándar. Esto permite combinar partes de un programa escrito en un lenguaje con porciones del mismo programa escrito en otro lenguaje. El resultado es un singular programa listo para ser cargado en la memoria principal para su ejecución.

**Editor de Ligación.**

El trabajo de este editor es un paso necesario que sigue a la compilación del programa si éste se encuentra en algún problema. Una de sus funciones más importantes es la solución de todas las referencias externas. Por ejemplo, una referencia externa, puede ser una subrutina a la cual el programa objeto requiere ejecutar. Un programador que desee calcular las medias, las desviaciones estándar y correlaciones, puede ejecutar todas estas operaciones sin tener que programar la lógica. CORRE es el nombre de una subrutina del SSP que ha sido diseñada para calcular medias, desviaciones estándar y correlaciones. El paquete SSP que es una colección de subrutinas estadísticas y matemáticas; consiste en bloques construídos separadamente, pueden aplicarse para solucionar problemas en ciencia, ingeniería y negocios.

El programador solo necesita llamar CORRE y se ejecutarán todas las operaciones deseadas. Cuando el programa fuente es compilado, el llamado a CORRE es considerado una referencia externa no resuelta. Esto implica que CORRE es un módulo externo al programa fuente y el sistema operativo debe encontrarlo y añadir el módulo al programa fuente. Esta acción resolverá la referencia externa.

Durante la edición, el dispositivo de almacenamiento apropiado, es revisado para la subrutina CORRE; cuando la subrutina se ha ubicado, se incluye en el programa objeto.

Un problema potencial para el auditor, es el hecho de que pueden incluirse tareas fraudulentas en el programa de la misma manera. El programa solo necesita hacer la llamada al módulo fraudulento y éste será incluido y el listado de esta subrutina no aparecerá en la impresión, unicamente aparecerá el llamado a la subrutina.

Otra tarea del editor es la de asignar jerarquías conforme a instrucciones de control y quizá la más importante para los auditores, pues traza la historia del procesamiento de un programa. El trazo de esta historia de procesamiento es simplificada por los registros de identificación de la sección de control que son creados y mantenidos el editor de ligación y puede contener datos, que describan: 1. El leguaje traductor utilizado, su nivel y la fecha de compilación de cada sección de control; 2. El procesamiento más reciente efectuado por el editor de ligación; 3. Las modificaciones hechas al código ejecutable de cualquier sección de control.

**Supervisor.**

El supervisor prevee recursos que pueden ser necesarios , si el programa tiene algún problema. Los recursos están ubicados de tal manera que se maximiza la eficiencia de su utilización. Después que se cargó el módulo, el programa de control automáticamente lo introduce a la memoria principal. Si el programa requiere datos, se genera una interrupción. El programa va a un estado de espera. La palabra que indica el estatus del programa ( PSW ) se modifica para indicar el estado de espera; además contiene la información requerida para una ejecución adecuada del programa. Generalmente , el PSW, controla la secuencia de instrucciones e indica el estatus del sistema en relación a la ejecución del programa.

El programa de control busca entonces el dispositivo que contiene los datos que requiere el programa. Cuando se localiza ese dispositivo, los datos se introducen en un buffer y se modifica el PSW y el programa de control sabe que el programa en estado de espera puede ahora continuar su ejecución.

Una vez terminada la ejecución, la salida es conducida al dispositivo de salida apropiado, como a una impresora por ejemplo. Una vez terminada la impresión, el sistema se libera de ese programa en particular.

**Observaciones Respecto a los Sistemas Operativos.**

Las modificaciones inapropiadas o no autorizadas a los sistemas operativos pueden dañar seriamente el procesamiento, así también desactivando sus paquetes de software de auditoría. El poder de penetración y la vulnerabilidad del sistema operativo son incuestionables. El auditor debe tener a su disposición el conocimiento y las herramientas que serán valiosas dentro de una auditoría.

El auditor puede utilizar la información de los registros de la sección de control como una herramienta efectiva para averiguar la información pertinente a un programa específico. Requerirá de la utilización en un paquete de software para auditoría.

El sistema operativo es preparado por un vendedor, generalmente el mismo que fabricó el CPU. Sería propio asumir que el vendedor no está tratando de tener acceso a información importante de los usuarios.

Un factor de beneficio para el auditor es la utilización de pseudocódigo que permitirá prevenir de individuos que modifiquen el sistema operativo, ya que las modificaciones requerirán el reemplazo de firmware. Los componentes que modifican el sistema operativo, están disponibles unicamente con el vendedor del CPU.

### 3.2.3 CONTROLES DEL PROCESAMIENTO.

Consisten en una variedad de técnicas incorporadas en los programas de aplicación para ayudar a asegurar que unicamente los datos válidos o correctos están siendo procesados como se prescribe. Se dividen en dos grupos:

- Checadores de edición.
- Controles operativos del programa.

**Checadores de Edición.**

Los checadores de edición ponen en la pantalla de la computadora, errores no detectados causados por omisión, entradas inválidas y otras. Estos checadores se listan a continuación:

a. Checadores numéricos, alfabéticos y de caracteres especiales.

Evitan la entrada de caracteres incorrectos en el procesamiento. Por ejemplo, la identificación de cierto departamento está formado por los siguientes dígitos: 97865. Si por alguna razón se transcribe 97B65, un checador numérico detectaría el error antes de efectuar el procesamiento. Otro ejemplo podría ser con los nombres, donde Salmón fué metido como Salmóm.

b. Checadores de signos.

En un sistema de cómputo hay dos tipos de signos: positivo (+) y negativo. Si el resultado de una operación aritmética es negativo, en algunos sistemas, sin una edición apropiada, este valor podría aparecer sin signo, durante las demás operaciones.

c. Checadores de validez.

Los chequeos se hacen contra tablas u otros datos que aseguren que los datos de entrada son válidos. Por ejemplo, una tabla de vendedores que la compañía coloca en un archivo en disco magnético bajo estricto control. Cada vez que se paga al vendedor, al dar el número del vendedor, debe encender un número en la tabla de vendedores válidos. Este control de validez, ayuda a reducir la probabilidad de que los pagos se hagan a falsos vendedores.

d. Checadores de límite y razonamiento.

Se usa para identificar datos que tienen un valor más alto o más bajo que el límite predeterminado. Estos límites estándares altos o bajos se determinan y establecen antes del procedimiento. Este control detecta unicamente aquellos datos que caen fuera de estos límites. Ejemplos de como puede usarse esta técnica son: un empleado no puede ganar más de $999.99 a la semana; no puede haber un número de cuenta menor de 87265-78.

e. Checadores de secuencia.

Los archivos frecuentemente están acomodados en una secuencia ascendente o descendente. Las instrucciones escritas en el programa de procesamiento compara la situación secuencial del registro o transacción precedente. Con esta técnica, cualquier registro fuera de secuencia puede detectarse y el archivo o si no será procesado con formas incorrectas.

f. Checadores aritméticos.

Varias rutinas pueden diseñarse dentro de programas de procesamiento para validar el resultado de otros procesos o el valor de campos de datos. Un método de prueba aritmética adiciona o resta dos o más campos y el cero balancea este resultado con el resultado original.

g. Dígito autochecador.

Cuando un número de cuenta es asignado, un dígito autochecador se prepara usando una operación aritmética y anexándolo al número de cuenta. Cada vez que el número de cuenta es introducido para procesamiento, se efectúa el mismo cálculo en la computadora. Si el dígito derivado no es igual al introducirlo al sistema, entonces hay un error. Por ejemplo, un dígito autochecador para el número de cuenta 12314 se podría calcular como sigue:

| | | | | | | |
|---|---|---|---|---|---|---|
| número de cuenta | 1 | 2 | 3 | 1 | 4 | |
| | x | x | x | x | x | |
| números primos | 17 | 13 | 7 | 5 | 3 | |
| resultado de multiplicar | 17 | 26 | 21 | 5 | 12 | |
| suma de resultados | 17 | + 26 | + 21 | + 5 | + 12 | = 81 |

restar 81 del múltiplo superior de 11: 88 - 81 = 7

El número de cuenta con el dígito autochecador anexado es: 12314-7

h. Checadores de overflow.

Protege contra la pérdida de dígitos si se presenta una condición de overflow durante el proceso. Por ejemplo, en COBOL, si el valor 1000.09 se toma como PICTURE 999V9, el resultado es 000.0 o un simple cero. Para prevenir esta clase de errores, debe incluirse la opción ON SIZE ERROR en todas las operaciones aritméticas.

i. Checadores de etiquetas.

La etiqueta inicial, la cual incluye al menos el nombre del archivo, debe checarse antes de iniciar el procesamiento. Sin embargo, las cintas pueden tener etiquetas antes y después de los archivos de datos. Las etiquetas de disco pueden aparecer en cualquier sitio del volumen del disco, donde el usuario especifique donde se localizará.

j. Checadores run-to-run.

Utiliza los controles de salida que son resultado de un proceso que establece controles totales en la entrada y sobre el proceso subsecuente.

Controles Operativos del Programa.

Además de la rutina de procesamiento y los checadores de edición, deben haber también otras instrucciones operativas en los programas. Los programas deben contener rutinas que muestren todas las condiciones de error o excepcionales que resulten de los chequeos de edición además de cualquier error o condición no válida.

Normalmente el sistema debe operar sin interrupión y cualquier condición de error debe ser escrita en un archivo de errores para su corrección subsecuente. Unicamente en circunstancias raras, el programa detendría el trabajo.

Por ejemplo, un checador de etiqueta no prende cuando debería indicar que se ha montado una cinta errónea. Las instrucciones deben ser desplegadas en pantalla al operador para saber que hacer cuando ocurran estas interrupciones.

Otro control en la operación de programas muy importante se refiere a procedimientos de reinicio y puntos de chequeo que son rutinas programadas que se ejecutan en puntos de chequeo o intervalos del procesamiento. Su propósito es determinar que procesamiento ha sido ejecutado correctamente sobre un punto designado. Si el procesamiento es correcto, el estatus del job se graba en cinta mágnetica o disco. El procedimiento normal del job continúa hasta que se alcanza el siguiente punto de chequeo.

El punto de chequeo tiene el efecto de dividir un job largo en una serie de fragmentos. Por ejemplo, el sistema de cómputo se dedica durante largos períodos de tiempo a la demanda de procesamientos de depósitos contables o de nóminas grandes. Una vez definidas las porciones de un job grande se corren como partes separadas e independientes, y cada parte se checa después de completarse. Si el chequeo es correcto, la información se copia a disco o cinta mágnetica para hacer posible el regreso al último punto de chequeo con un mínimo de dificultades si ocurriera algún error o interrupción.

El uso apropiado de los procedimientos de inicio y los puntos de chequeo en un programa, constribuyen a la eficiencia operativa de un sistema de cómputo. Si hay una falla en la energía o si ocurren desperfectos serios en el equipo, estos procedimientos proveen una forma de rearranque inicialmente a una pequeña parte de un job sin tener forma de reiniciar un job entero. La aplicación de estos procedimientos pueden significar el salvar muchas horas del equipo y el pago de muchas horas extras.

Los procedimientos de reinicio también permiten la interrupción de un job para programar otros job's que necesitan atención inmediata. Entonces cualquier job puede ser interrumpido, intencionalmente por el operador y remplazado con otro job cuando es necesario.

Finalmente el procedimiento de reinicio prepara una interrupción en la operación de la computadora para reparaciones de emergencia o mantenimiento no programado.

### 3.2.4 CONTROLES EN PROGRAMAS DE APLICACION

Los controles de los programas consisten en:

- Desarrollo del programa
- Documentación del programa
- Cambios en el programa
- Ayudas al programa.

**Desarrollo del Programa.**

Los programas en algunas organizaciones crecen sin ningún control. Frecuentemente los programadores siguen metodología de desarrollo no muy bien definida; algunos tratan de codificar antes de que los objetivos estén bien comprendidos y definidos. La metodología para el desarrollo de un programa que debe seguirse se describe a continuación:

- Diseño de lógica.

Antes de hacer cualquier intento para escribir las instrucciones de un programa, la lógica del sistema a programar debe ser comprendida por el programador y aceptado por el usuario. Esta lógica, generalmente se prepara con el uso de diagramas de flujo, formatos y tablas de decisión.

- Codificación.

El programador debe convertir la lógica preparada en diagramas de flujo a la sintaxis apropiada de un lenguaje de programación. Selecciona las instrucciones apropiadas y las coloca en secuencia de acuerdo a la lógica descrita en el diagrama de flujo. Cuando la lógica se ha codificado, entonces el programa debe probarse para errores sintácticos y lógicos.

- Pruebas.

Los errores del programador son más difíciles de evitar de lo que podría esperarse. Es raro el programa que trabaje correctamente la primera vez que se maneja con datos de prueba. En la mayoría de los casos deben hacerse varias corridas de prueba antes de encontrar y corregir todos los errores. El compilador encuentra por sí mismo la mayoría de los errores durante la compilación. La prueba real, debe asegurar que el programa no tiene errores lógicos y que es capaz de producir salidas correctas.

- Implementación.

Después de efectuarse los tres primeros pasos, se prepara el programa y se instala para ser operado.

- Catalogamiento.

El último paso es catalogar el programa en la librería bajo estricto control. No debe permitir el acceso o cambios al programa sin autorización apropiada.

Documentación del Programa.

Sirve como una referencia que describe todos los aspectos de un programa particular. La documentación mínima debe incluir lo siguiente:

a. Descripción narrada.

Esta descripción debe dar una visión amplia de lo que trata el programa y su propósito.

b. Nombre y número de identificación.

Es simplemente para identificar el programa; dá una forma de localizar el programa en la biblioteca.

c. Lógica del programa.

Incluye los diagramas de flujo mas las tablas de decisiones si es que hubo.

d. Listados del programa.

Es una copia, generalmente en papel de todas las instrucciones usadas en la codificación del programa.

e. Fecha de prueba y aprobación final.

Fechas de prueba y aprobación, adicionalmente los nombres de las personas que efectuaron las pruebas y el de la persona que las aprobó.

f. Resultados de pruebas.

Los resultados o el listado de la ejecución de pruebas.

g. Formatos de archivos y grabación.

Estas formas describen todas las entradas y salidas.

h. Instrucciones de operación.

Estas instrucciones se despliegan al operador de la computadora, por ejemplo " Montar la cinta No. XXXXXX".

i. Instrucciones para la distribución de la salida.

Estas instrucciones le dicen al personal operativo quién está autorizado para recibir los reportes.

j. Programas autodocumentados.

Esto es quizá lo más importante que debe ser escrito en un programa, de tal manera que permita su fácil comprensión, esto es, deben usarse nombres de las variables que tienen una relación lógica con los datos que están siendo manejados.

Cambios en el Programa.

Los cambios no autorizados en un programa representan una de las más significativas amenazas a los sistemas. Es imperativo que cualquier cambio en un programa se haga de acuerdo a procedimientos estrictos de aprobación de cambios y supervisándolos, si estos son aprobados. Si se realizan cambios autorizados sobre un programa, éste debe probarse para asegurar que hace lo que se supone que tiene que hacer. Una desviación de este procedimiento conduce facilmente a errores.

Ayudas al Programa.

Estas ayudas no solo incrementan la eficiencia del programa, sino que también incrementan el control.

a. Abreviaturas.

Abreviación de palabras en la programación. Por ejemplo, en COBOL, en vez de escribir PICTURE cada vez que se necesite, solo se escribe PIC.

b. Tablas de decisión.

Apoyan el diseño de un programa modular y ayuda a aclarar la lógica del programa a los usuarios y a los encargados del mantenimiento de los programas.

c. Generadores de datos de prueba.

Se puede producir un número infinito de combinaciones y permutaciones de condiciones de prueba por algún método, ya que es difícil y tardado prepararlas manualmente y son muy importantes para las pruebas.

d. Biblioteca.

Esta ayuda provee mejores controles. Un programa de mantenimiento se ejecuta con más facilidad porque la documentación es mejor. Algunas de ellas pueden ser: un sistema de directorios y reportes de quién ha usado que programa, indica el status del programa, estado activo o de prueba, etc.

Los paquetes de librerías no deben restringirse al uso de programas de aplicaciones. Se han desarrollado paquetes de software para ayudar en el manejo de sistemas operativos altamente vulnerables. El Programa para Modificaciones de Sistemas (SPM), fué desarrollado por IBM para registar y publicar cualquier cambio hecho en la computadora. En la actualidad hay gran cantidad de paquetes de software para una amplia gama de utilidades.

### 3.2.5 CONTROLES DEL SISTEMA DE MANEJO DE BASE DE DATOS

Los sistemas que manejan la base de datos se están convirtiendo en parte integral del procesamiento de datos. El auditor eficiente debe tener conocimientos de este sofisticado software.

Una base de datos puede verse como una colección generalizada, común e integrada de datos que satisfacen los requerimientos de datos de todas las aplicaciones con acceso a ellos. Adicionalmente, los datos dentro de esa base de datos debe ser estructurada como módulo de la relación de datos que existe en una compañía.

Las nociones de bases de datos y manejadores de base de datos, pueden definirse apropiadamente sobre una base individual. Sin embargo existe una relación funcional entre la base de datos y su sistema de manejador de base de datos asociado, lo cual demanda que se consideren los dos conceptos en conjunto.

Los datos dentro de una base de datos están archivados con técnicas especificadas, esto es, el tamaño de los registros, los formatos específicos de esos registros, etc.. La creación de una base de datos integra y compleja lleva asociada un costo sustancial. Una organización no dedicaría sumas grandes de dinero a la creación de una base de datos que no tenga un sistema de manejo de base de datos creado sobre esa base de datos.

**Sistemas de Manejo de Base de Datos.**

Los sistemas de manejo están emergiendo con una pequeña y común base de operación, pero tiene problemas de incompatibilidad. Los programas fuente pueden transferirse de una máquina a otra, o sean son transportables, mientras que los archivos sobre los cuales operan los programas no tienen una técnica estándar de almacenamiento.

Se tienen dos tipos básicos de sistemas que están asociados con la base de datos: sistemas con capacidad para un lenguaje huésped y sistemas con capacidad autocontenida. Un lenguaje huésped implica la necesidad de usar un lenguaje de procedimiento y la capacidad autocontenida no implica la conexión con un lenguaje huésped.

Capacidad para un lenguaje huésped.

Un sistema de este tipo se construye sobre las facilidades de un lenguaje de procedimiento tales como COBOL, PL/1 o lenguaje ensamblador. La interfase entre el lenguaje huésped y las capacidades de lenguaje huésped es através de una instrucción determinada.

El "construído sobre" utilizado, no debe confundirse con "construído con" ya que en general el lenguaje huésped y su compilador permanecen intactos. En resumen, las capacidades del lenguaje huésped deben verse simplemente como nuevas herramientas para el programador.

Capacidad autocontenida.

En sistemas que ofrecen estas capacidades, las definiciones de los datos en los registros reside en una forma codificada con los datos. En efecto, estos pueden ser almacenados, tanto en un catálogo de varias definiciones de datos o con el archivo de datos.

Un sistema autocontenido provee capacidades para el acceso a la base de datos y para el despliegue de datos en pantalla através del uso de un lenguaje de alto nivel simplificado, diseñado para ser usado por quien no es programador. El lenguaje es considerablemente menos flexible que los comunes, sin embargo es más sencillo aprenderlo y usarlo.

En resumen, las capacidades autocontenidas son herramientas tanto para los programadores como para los que no lo son.

**Subfunciones de los Sistemas de Manejo de la Base de Datos.**

Un sistema de manejo de base de datos, comprende una o mas de las siguientes subfunciones: manejo de archivos, dudas y generadores de programa.

Abarca las operaciones para la creación de la base de datos, su supresión y su dada de alta. Sin embargo, se afirma que la independencia y relación de datos, la no redundancia, integridad, compresión, seguridad y la auditoría sobre el sistema son también funciones del manejo de archivos.

a. Independencia de los datos.

Implica la capacidad de archivar y recuperar datos sin un formato de datos específico. Comunmente, los datos deben ser formateados cuando son archivados.

b. Relación de datos.

Implica la construcción de una base de datos con relaciones lógicas entre los inter-registros grabados además de asociaciones consistentes y lógicas. Por ejemplo, es lógico tener la información concerniente a un individuo dentro de un registro como sigue:

| | | |
|---|---|---|
| posicion de bytes | 01-25 | nombre |
| | 26-50 | dirección |
| | 51-73 | ciudad |
| | 74-75 | estado |
| | 76- n | otros datos relevantes |

La relación inter-registro significa el uso de técnicas de dirección tales como encadenar o invertir archivos de tal forma que registros con información similar pueden obtenerse sin necesidad de revisar el archivo entero. Las relaciones que pueden existir entre los datos que están en la base de datos deben quedar claramente especificadas para que se puedan derivar las asociaciones deseadas.

c. No redundancia de datos.

Implica el almacenamiento de los mismos datos en más de una locación de un dispositivo de almacenamiento. Es costosa, no unicamente desde el punto de vista de una utilidad deficiente de espacio almacenado, sino desde el punto de vista del procesamiento, ya que más información irrelevante debe manejarse durante el procesamiento. Por tanto, desde el punto de vista del costo de almacenaje y tiempo de máquina, la base de datos debe evitar la redundancia de datos.

d. Integridad de los datos.

Implica datos libres de error. Una base de datos implica a muchos usuarios y es de extrema importancia que el sistema sea capaz de prevenir la contaminación de los datos, en el tiempo de captura. Es importante recordar que los errores se hacen tanto en la captura de nuevos datos, como en datos que serán dados de alta. Numerosas técnicas para reducir errores están disponibles. Estos incluyen el uso de dígitos verificadores, validación del tamaño, etc.

e. Compresión de datos.

Un compresor es un software o hardware que abrevia la longitud de la cadena de bits. Un descompresor, expande la cadena abreviada devolviendole su forma original. El resultado es una utilización más eficiente de los dispositivos de almacenamiento. Por ejemplo, en una cadena de caracteres que tiene el apellido de un individuo la variable que contiene el nombre, puede declararse con una longitud de 20 caracteres. Si el apellido es Zorrilla, solo 8 de los 20 caracteres contienen información, los 12 restantes solo ocuparán espacio en almacenamiento. Un compresor puede tomar la cadena de caracteres y determinar que hay 12 espacios. Una nueva cadena puede formarse con "Zorrilla12"; el número de espacios en blanco se ha incorporado a la nueva cadena y unicamente 10 caracteres son archivados. Esta técnica podría tener un efecto sustancial en el costo. Los compresores de datos son algoritmos altamente sofisticados que pueden operar a un nivel bit lo cual permitirá una utilización mas eficiente del espacio de almacenamiento.

f. Seguridad de los datos.

La dificultad de tener acceso a los datos debe ser función de la confidencialidad de los datos y la autoridad del usuario. Se debe dar seguridad hasta en el nivel más elemental.

La prevención del acceso no autorizado a los datos es solo una de las múltiples facetas de la seguridad. La probabilidad de pérdida de datos debido a robos, fuego, etc; es grande.

g. Auditoría sobre el sistema.

Poder hacer una auditoría sobre el sistema se convierte en un aspecto extremadamente importante en los sistemas que manejan base de datos, ya que los auditores deben verificar que todas las transacciones se están recibiendo apropiadamente, además de que la entrada y todos los datos que residen en la base de datos se han modificado apropiadamente.

Estos sistemas generalmente tienen capacidades auditoras internas, las cuales pueden servir a los auditores. Por ejemplo, IMS ( el controlador de la base de datos de IBM ) tiene procedimientos que registran todas las entradas y salidas, así como imágenes de antes y después de los registros modificados en la base de datos.

### 3.2.6 CONTROLES INTEGRADOS A LA COMPUTADORA.

La mayoría de los vendedores ofrecen computadoras con una gran variedad de características de control que son internas y automáticas y que ayudan a asegurar que operen apropiadamente. Estos controles consisten en:

- Controles de hardware.
- Controles de software.

Muchas características de los controles están estandarizadas; donde esto no ocurre, su manejo podría requerir que le sean incorporados antes de que la computadora sea instalada.

**Controles de Hardware.**

Están construidos dentro de los circuitos para la detección de errores que pueden resultar de la manipulación, cálculo o transmisión de datos por los varios componentes del sistema de cómputo. Estos controles del equipo se requieren para asegurar que solo un pulso electrónico es transmitido através de un canal durante una fase, que los datos se han codificado o decodificado correctamente, que los dispositivos específicos están activados y que los datos recibidos en una locación son los mismos que los transmitidos por otra. Algunas características del control del equipo son:

a. Chequeo de paridad.

Para asegurar que los datos que se introdujeron inicialmente al sistema, se han transmitido correctamente, un checador interno se incorpora. En los bytes usados para representar datos, la computadora usa un bit llamado de paridad. Se usa para detectar errores en los circuitos los cuales podrían ocasionar la pérdida, adición o destrucción de un bit debido a un mal funcionamiento del equipo. El bit de paridad hace que el número de bits en código binario sea non o par.

b. Chequeo de validez.

Los números y caracteres se representan por combinación de dígitos binarios. La representación de estos datos por medio de símbolos es efectuada por varios esquemas codificados, manejados por los circuitos del sistema de cómputo. Por ejemplo, los caracteres en código Hollerith de una tarjeta perforada son convertidos a código BCD o EBCDIC o ASCII, o sea el código de comunicación entre la computadora y sus componentes. Por tanto, un mensaje si es válido, se está transmitiendo o recibiendo através de una operación de codificación y decodificación, y que es aceptada para el envío o recepción del dispositivo en cuestión.

c. Chequeo de duplicación.

Este chequeo de control requiere que dos componentes independientes ejecuten la misma operación y comparen resultados. Si hay alguna diferencia entre las dos operaciones, se indica una condición de error.

d. Chequeo de repetición.

Autentifica la transmisión de datos de y hacia los componentes del sistema de cómputo. La transmisión de datos se verifica rebotando las señales recibidas por el componente comparándolos con el origen de los datos. Por ejemplo, el CPU, transmite un mensaje a una impresora para ejecutar una operación. La impresora envía un mensaje hacia el CPU, donde es automáticamente checado para ver si se ha activado el dispositivo correcto.

d. Chequeo de variedad de errores.

Adicionalmete a los chequeos nombrados anteriormente, el sistema de cómputo debe hacer detecciones como diferentes instrucciones no válidas, sobre flujo de datos, signos perdidos, división entre cero y componentes defectuosos.

e. Controles de firmware.

Las instrucciones de firmware, a diferencia de las instrucciones de software, no pueden modificarse. La nueva tecnología permite colocar muchas instrucciones de firmware en un solo chip. Por ejemplo, las calculadoras de bolsillo que ejecutan funciones como la raíz cuadrada tienen la lógica del cálculo permanentemente en un chip; la lógica no puede modificarse con software convencional, solo se consigue alterando el chip o reemplazándolo.

El concepto de firmware es extremadamente importante debido a que quita al programador la capacidad de alterar programas, incluyendo sistemas operativos altamente vulnerables. Conforme se incrementa la complejidad y sofisticación de los sistemas de cómputo, debe darse mayor confianza al control interno de la computadora.

Al avanzar la tecnología, métodos más eficientes de transferir algoritmos a circuitos integrados, están haciendo inevitables los programas de firmware. Los auditores deberán requerir que los procedimientos de auditoría dentro de las computadoras sean con firmware.

Controles de Software.

Algunos de estos controles son los siguientes:

a. Error de lectura o escritura.

Con este error , la máquina detendrá el programa y permitirá al operador investigar el error. Por ejemplo, una impresión intentada con la cabeza de impresión defectuosa o si la impresora tiene mal colocado el papel.

b. Chequeo de la longitud de registros.

En algunas instancias los bloques de registros son colocados de tal manera que son demasiado largos para la entrada del área del buffer de la computadora. Este control por tanto, asegura que los registros de datos leídos por la computadora de cintas o discos, sean de una longitud correcta.

c. Rutina de chequeo de etiquetas.

Hay dos clases de etiquetas, las del encabezado y las del final. Como mínimo la etiqueta de encabezado, debe contener el nombre del archivo y la del final, el fin del archivo. Por ejemplo, si es una entrada de archivo, la etiqueta de encabezado se usa para checar que el archivo es el especificado por el programa. La etiqueta del final, para determinar si todos los datos del archivo fueron procesados correctamente.

d. Control de acceso.

Se presenta una condición de error cuando la referencia es hecha en un dispositivo de almacenamiento que no está en estado READY.

e. Control para comparar las direcciones.

Se presenta un error cuando una dirección de cierto almacenamiento es referida por un componente y estas no concuerdan. Por ejemplo, la dirección del centro de almacenamiento, no concuerda con la dirección referida por un drive.

f. Control de paquetes comerciales.

Actualmente, las microcomputadoras ( PC's ) están teniendo un fuerte impacto en los Centros de Cómputo grandes y pequeños.

Para muchos usuarios, las microcomputadoras los han liberado de la falta de atención por parte del Departamento de Sistemas, que en frecuentes ocasiones retarda y frustá sus deseos de capacidades adicionales automatizadas. Pero, si se habla de Software Comercial, nos encontramos con que no se sabe como poder controlar el ritmo en el desarrollo que se tiene en la actualidad, que es demasiado rápido y cambiante.

Las versiones de un producto duran como " lo último " muy poco tiempo, y cuando se ha puesto la mayoría de su capacidad en uso, nos enteramos que ya existe una nueva versión que es mas poderosa, con mas opciones, mas barato en algunas ocasiones y que nos proporcionará mayores alternativas de aplicación y por lo tanto, mayores beneficios.

Pero todo esto, no debe sembrar dudas con respecto a lo que se tiene en existencia, porque la adquisición debió realizarse en base a un estudio de factibilidad y a la recopilación de información de las necesidades específicas de la institución, en cuanto a efectividad, disponibilidad, capacidad, recursos y una relación de costo-beneficio entre otros. No se debe caer en la preocupación de que en poco tiempo, aparecerá un producto mejor, con capacidad de transferencia de información de nuestro paquete al nuevo.

Se debe pensar en un nuevo paquete, cuando la vida útil del actual esté por llegar; si actuamos de otra manera, nos pondremos en una situación en la que nuestros recursos serán sobrepasados por la velocidad que tiene la tecnología de software.

Así que podemos decir entonces, que esta sería la mejor manera de controlar los Paquetes Comerciales, controlando la ambición de estar " en lo que dicta la moda " sin dejar de tener información para estar concientes del avance para el momento de pensar en una nueva adquisición.

Si se usa el software de control de fábrica o si la manufactura tiene su propio paquete software de control, el auditor debe conocer estas técnicas de verificación y manejo de errores.

### 3.2.7 CONTROLES PARA LA OPERACION DE LA COMPUTADORA

La computadora es uno de los componentes clave en el sistema de información. Es por tanto, importante que tenga su control y mantenimiento apropiados. Mas aún, es imperativo que el personal que opera el equipo de cómputo, esté sujeto a los mismos controles estrictos. Esta área de controles se divide en dos grupos:

- Controles físicos.
- Controles de procedimiento.

**Controles Físicos.**

Estos controles conciernen al medio en que está instalado el Centro de Cómputo. El sentido común y el establecimiento de controles físicos simples, pueden ayudar a prevenir muchos errores y contratiempos.

Sitio de la Computadora

La ubicación y construcción del Centro de Cómputo son fundamentales; la construcción debe ser de alta calidad y con material a prueba de fuego.

Control del Medio

Deben instalarse sistemas de medidores de humedad relativa y humificadores adecuados; también necesitan un gran sistema de aire acondicionado para operar apropiadamente. Los circuitos integrados y componentes de la computadora, son muy sensibles a las fluctuaciones de la temperatura. Irregularidades de estos sistemas, pueden causar problemas serios en varias formas incluyendo corrosiones en los contactos eléctricos. La humedad relativa no controlada, puede generar electricidad estática y ésta es muy dañina para el funcionamiento correcto de los circuitos integrados.

Sistemas de Energía Ininterrumpibles

Se debe instalar una fuente de energía emergente. Las computadoras, como la mayoría de los sistemas altamente sofisticados, dependen de la operación ininterrumpible de sus subsistemas tributarios. Un subsistema obviamente importante es la energía eléctrica.

Una energía eléctrica deficiente, implica apagones pasajeros e inestabilidad en la línea; por ejemplo, fluctuaciones en el voltaje y/o en la frecuencia de la electricidad.

Para asegurar la disponibilidad continua de energía eléctrica, se han desarrollado sistemas de energía ininterrumpibles (UPS). Si la instalación de la computadora, es muy sensible, es apropiado considerar la adición de generadores de motor emergentes con el fin de tener energía durante interrupciones prolongadas.

Controles de Procedimiento.

Estos se refieren a la supervisión para verificar si las tareas en el sistema se están ejecutando apropiadamente.

Supervisión del Cuarto de Cómputo

Todos los equipos en un Centro de Cómputo, especialmente los operadores, deben estar bajo supervisión directa. Los supervisores deben establecer las prioridades de trabajo y una bitácora para cada día de trabajo debiéndola firmar todos los operadores al inicio y final de su turno. El uso extra de la computadora debe limitarse.

Los supervisores deben demandar reportes de la utilización del equipo y llevar registros precisos de control del trabajo referido al tiempo de la computadora, incluyendo producción, listados de programas, reprocesos y tiempo que está parada la máquina. El auditor debe revisar periódicamente estos reportes.

Los supervisores deben revisar los trabajos en proceso y los terminados para asegurar la calidad y la correcta disposición de la salida. La impresión de información confidencial que no se uitilizará debe ser destruída por seguridad.

Todas las bitácoras de operación deben revisarse diariamente por los supervisores. Estas bitácoras deben incluir todos los mensajes hacia y desde la computadora através de la consola de la computadora, ya que es usado por el operador para mantener y controlar las operaciones de la computadora. La bitácora puede tener la forma de un papel de forma continua proveniente de la impresora conectada a la consola; en otras instalaciones, puede ser registrada en cintas o discos magnéticos.

La consola generalmente consiste de un panel de control y un teclado. Con la consola, además de la impresora, la pantalla, switches y botones del panel de control, facilitan al operador el introducir comandos o mensajes y recibir información directamente del CPU. Utilizando todo lo anterior, el operador puede:

- Iniciar, detener o cambiar la operación de todo o parte del sistema de cómputo.
- Introducir, modificar y desplegar datos manualmente.
- Determinar el estatus de los interruptores internos electrónicos.
- Determinar el contenido de ciertos registros.
- Alterar el modo de operación cuando ocurre un mal funcionamineto o una condición inusual y continuar después de que se ha corregido.
- Cambiar la selección de los dispositivos de entrada/salida.
- Ejecutar programas y rutinas.

La intervención o manipulación no autorizada por parte del operador debe reducirse con varias técnicas de control. Por ejemplo, la impresora que se usa para las intervenciones del operador más los resultados de las operaciones durante un período definido, registra la fecha y hora de ejecución; esta puede ser revisada periódicamente por el administrador del Centro de Cómputo y el auditor. El operador debe dar razón de todo el tiempo de operación de la computadora en su turno.

Unicamente los operadores deben operar el equipo, pero la intervención del operador durante el procesamiento debe ser limitada. Más aún, el acceso de los operadores a cintas, discos, programas y documentación confidenciales deben ser estrictamente controlados.

Deben establecerse procedimientos de mantenimiento preventivo, para evitar el deterioro de los componentes de la computadora por medio de un sistema preventivo, detectivo y correctivo. Lo básico de un mantenimiento preventivo es un inventario de repuestos; es tonto que se detenga la operación de un sistema de millones de pesos por una refacción de miles de pesos. Todo el servicio que se da al equipo, debe ser hecho por ingenieros de servicio calificados.

Las facilidades de acceso al cuarto de cómputo debe restringirse a personal autorizado unicamente. Las técnicas de control administrativas incluyen chequeos a fondo, vacaciones, rotación de turnos y rotación de deberes de todos los operadores.

Controles de la interfase programador/base de datos.

El objetivo general de los buenos controles de procedimiento es aislar datos confidenciales de los programadores, reduciendo la probabilidad de un acceso no autorizado o de la modificación de datos.

Comunmente, un programador, recibe la orden de generar un programa que ejecutará una tarea específica. Una vez completado éste y las pruebas subsecuentes que aseguren su funcionamiento apropiado, el programador coloca el producto terminado en la biblioteca de programas del sistema. Pero en sí, el programador no debe ser el que coloque la copia final del programa en la biblioteca; debe hacerlo el administrador de la base de datos.

Este administrador tiene a su disposición dos técnicas para limitar el acceso del programador a los datos:

- Facilidades del tiempo de compilación.
- Lenguaje de control de los job's.

a. Facilidades del tiempo de compilación.

Si una compañía está utilizando un sistema para manejo de base de datos, el auditor debe considerar los pasos que ocurren durante la compilación del programa. El uso de un sistema para manejo de base de datos con capacidad para un lenguaje huésped permite tener acceso a la base de datos através de una instrucción de llamado a la base de datos.

Cuando un programador ha concluído su programa, incluyendo pruebas, es tiempo de tener una compilación final del programa que pueda ser guardada en forma de módulo en un dispositivo de almacenamiento de acceso directo. Sin embargo, en lugar que el programador someta su programa al operador, el someterá el programa fuente al administrador de la base de datos. El administrador deberá conocer cual es el propósito del programa y los datos que son permitidos usar en ese programa provenientes de la base de datos; deberá también colocar una serie de comandos que cambiarán los nombres de variables estándar a una representación codificada que pueda aceptar la base de datos. De esta manera, si el programador trata de utilizar datos que no forman parte de su programa durante la etapa de procesamiento, esas variables no serían transformadas a valores reconocibles. Tal condición evita la ejecución del programa.

Por la delicadeza de su trabajo, el administrador de la base de datos debe ser seleccionado cuidadosamente y establecer procedimientos de control, suficientes para asegurar que el sistema operará apropiadamente.

Estos procedimientos tienden a desalentar a las personas de utilizar datos no autorizados. También previene que un individuo escriba un programa no autorizado para utilizar datos confidenciales, ya que sin la conversión del procesador, ningún programa podría usar ningún dato proveniente de la base de datos.

b. Lenguaje de control de jobs (JLC).

Podría aplicarse en un medio donde está operando un sistema sin manejador de base de datos. En la actualidad, las tarjetas de definición de datos (DD) son un componente del JLC. Las tarjetas DD, actúan como una interface entre el usuario del programa y el sistema operativo; tienen información concerniente al nombre de la sección de datos, el tipo de dispositivo de almacenamiento ( disco, cinta, etc), el número de serie del almacenamiento y otra información importante.

El administrador de la base de datos podría desarrollar un procedimiento que prohíba a los programadores el uso de tarjetas DD para la producción de un programa y de ésta manera ya no sabrían donde están los datos o cualquier otra información vital acerca de la sección de datos o archivos.

Tarjetas de reemplazo

La utilización de tarjetas de reemplazo (REP), permite hacer cambios a los programas objetos, pero hay muchos problemas si se utilizan; por tanto se deben instituir controles para su utilización.

La modificación de un programa objeto no implica la actualización de un programa fuente; el resultado es que cuando el programa fuente debe ser recompilado, los cambios hechos con tarjetas REP repentinamente vuelven a su estado original. La razón es que el defecto fué corregido con tarjeta REP y el programa fuente aún tiene la lógica inapropiada.

La utilización de las tarjetas REP se debe limitar a instalaciones que usan lenguaje ensamblador como el principal de programación, debido a que hay una relación 1:1 entre una instrucción ensamblada y el código objeto generado.

### 3.2.8 CONTROLES DE BIBLIOTECA Y BASE DE DATOS

La biblioteca y la base de datos representan la base del sistema de información y deben ser controlados. Si hay pérdida o destrucción deben haber sido establecidos procedimientos preplaneados para reproducir cualquier dato perdido. Se dividen en dos grupos:

- Físicos.
- De procedimiento.

**Controles Físicos.**

El fuego, inundaciones, robos, empleados resentidos, motines y plagas entre otros, representan peligro para la información vital de una organización. Un almacén seguro para ésta información es de gran importancia para la operación continua de cualquier cuestión. Los dispositivos para la protección como anillos protectores para cintas magnéticas, deben usarse para prevenir borraduras accidentales. Todos los dispositivos de almacenamiento, deben mantenerse libres de contaminantes ambientales, así como controlarse estrictamente las condiciones de humedad y temperatura.

**Controles de Procedimiento.**

Todos los archivos deben guardarse en una biblioteca aún cuando no se usen. La biblioteca debe tener un registro completo de todos los archivos en una lista de inventario, a que persona están asignados los archivos, el estatus y cuando han sido regresados. Todos los archivos deben contener etiquetas externas para su identificación, las cuales deben estar en clave e indescifrables. La limpieza y reparación deben hacerse regularmente a cintas y discos magnéticos. Tal procedimiento minimiza los errores de lectura/escritura y asegura un suministro adecuado de medios de almacenamiento.

de archivos recomendable para archivos secuenciales, se ilustra en la fig. 5. Este sistema de respaldo se denomina normalmente como Abuelo-Padre-Hijo. Con este procedimiento tres versiones del archivo están disponibles en cualquier momento. El archivo A (padre) en el ciclo I, produce el archivo B (hijo). En el ciclo II, el archivo B (ahora padre) produce el archivo C (hijo de B). En este ciclo, el archivo A se convirtió en abuelo. La ventaja de este procedimiento es que siempre es posible la recuperación.

Por ejemplo, si el archivo C contiene errores, el job podría repetirse usando el archivo B con las transaccion de datos desde el archivo 2 de transacción. Si tanto el archivo B como el C, están dañados o destruídos, el archivo A (guardado fuera del sitio de trabajo) está adn disponible y con el archivo 1 de transacción puede crear el archivo B, el cual puede a su vez usarse para crear el archivo C.

Con dispositivos de almacenamiento de acceso directo como discos y cintas magnéticas, es recomendable que los contenidos sean escritos periódicamente y en un archivo de respaldo y almacenados en otro sitio. Adicionalmente debe llevarse una bitácora de transacciones por dos razones: una, porque constantemente hay transacciones y la bitácora puede enlazar un respaldo con el siguiente; y dos, al escribir sobre un disco o cinta magnética, se cubre lo que había.

Si por algún motivo, los archivos en la base de datos se destruyen o se modifican incorrectamente, debe haber un método disponible para reconstruir el archivo. En la fig. 6 se ilustra un plan para la reconstrucción de archivos de acceso directo. En este ejemplo, asumimos que el archivo de acceso directo (archivo maestro) es destruido durante el periodo II. Con el respaldo A, el cual es una copia del archivo maestro al final del periódo I y con la bitácora de transacción 2, la cual registro todas las transacciones durante el periodo 2 hasta la destrucción del archivo maestro, puede reconstruirse un nuevo archivo maestro en disco. Todos los datos del archivo maestro, el respaldo A, son escritos sobre el nuevo archivo maestro en disco. Así todas las transacciones de la bitácora de transacciones 2 están propiamente grabadas, llevando el archivo maestro a un estado correcto.

### 3.2.9 CONTROLES DE SALIDA

Los controles de salida se establecen como un chequeo final sobre la información procesada. Estos procesos son:

a. Las salidas deben encausarse inmediatamente a una área controlada y distribuirse unicamente a personas autorizadas por personas autorizadas.

b. Los controles totales de salida deben ser compatibles con los controles totales de entrada para asegurar que no hay datos que se hayán perdido o añadido durante el procesamiento o la transmisión.

c. Todas las formas de control deben ser prenumeradas y contadas,

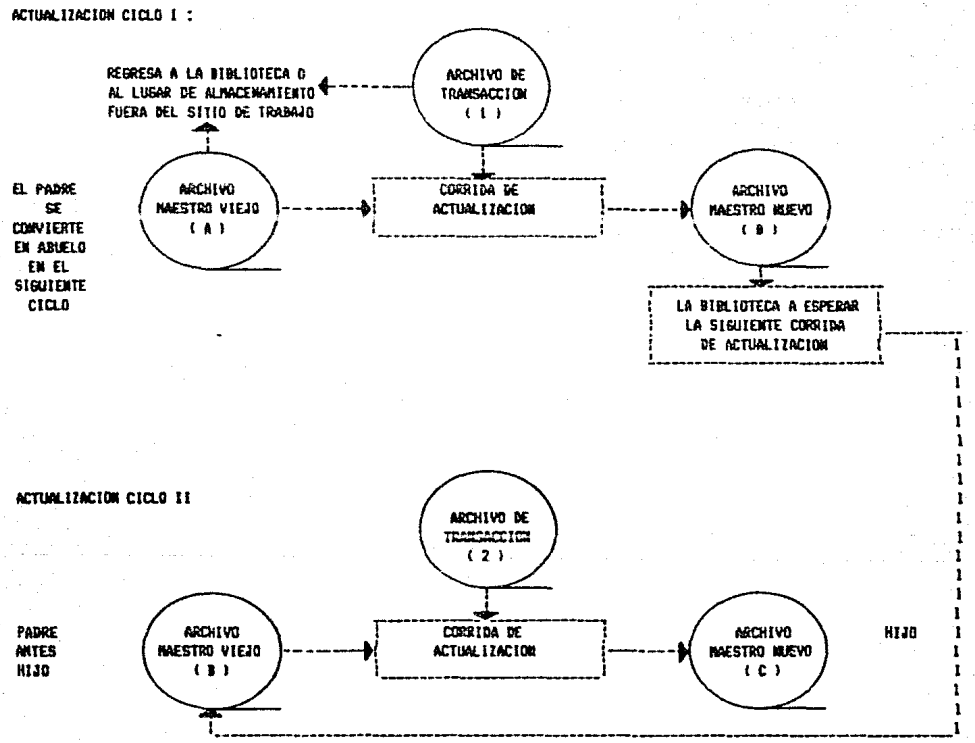

ACTUALIZACION CICLO I :
REGRESA A LA BIBLIOTECA O AL LUGAR DE ALMACENAMIENTO FUERA DEL SITIO DE TRABAJO
ARCHIVO DE TRANSACCION ( 1 )
EL PADRE SE CONVIERTE EN ABUELO EN EL SIGUIENTE CICLO
ARCHIVO MAESTRO VIEJO ( A )
CORRIDA DE ACTUALIZACION
ARCHIVO MAESTRO NUEVO ( B )
LA BIBLIOTECA A ESPERAR LA SIGUIENTE CORRIDA DE ACTUALIZACION
ACTUALIZACION CICLO II
ARCHIVO DE TRANSACCION ( 2 )
PADRE ANTES HIJO
ARCHIVO MAESTRO VIEJO ( B )
CORRIDA DE ACTUALIZACION
ARCHIVO MAESTRO NUEVO ( C )
HIJO

FIGURA 5

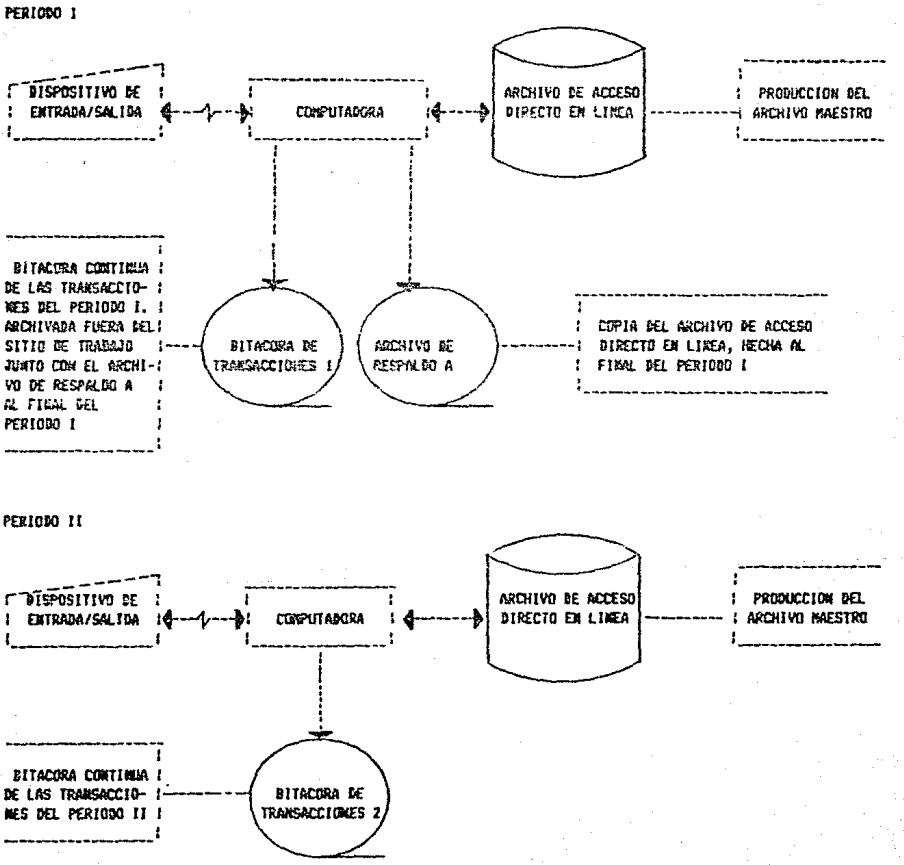

PERIODO I
DISPOSITIVO DE ENTRADA/SALIDA
COMPUTADORA
ARCHIVO DE ACCESO DIRECTO EN LINEA
PRODUCCION DEL ARCHIVO MAESTRO
BITACORA CONTINUA DE LAS TRANSACCIONES DEL PERIODO I. ARCHIVADA FUERA DEL SITIO DE TRABAJO JUNTO CON EL ARCHIVO DE RESPALDO A AL FINAL DEL PERIODO I
BITACORA DE TRANSACCIONES 1
ARCHIVO DE RESPALDO A
COPIA DEL ARCHIVO DE ACCESO DIRECTO EN LINEA, HECHA AL FINAL DEL PERIODO I
PERIODO II
DISPOSITIVO DE ENTRADA/SALIDA
COMPUTADORA
ARCHIVO DE ACCESO DIRECTO EN LINEA
PRODUCCION DEL ARCHIVO MAESTRO
BITACORA CONTINUA DE LAS TRANSACCIONES DEL PERIODO II
BITACORA DE TRANSACCIONES 2

FIGURA 6

c. Todas las formas de control deben ser prenumeradas y contadas, como ejemplo, los cheques de pago.

d. Cualquier salida de alta confidencialidad que no deba ser accesible al personal del Centro de Cómputo, debe generarse através de un dispositivo de salida; por ejemplo, una impresora en una locación segura fuera del cuarto de cómputo.

e. A pesar de todas las precauciones tomadas se dan errores. El mejor punto de control para detectar errores es el usuario. Por tanto, los procedimientos deben establecerse por un auditor que coloque un canal entre el usuario y el grupo de control para el reporte sistemático de errores o impropiedades. El diseño de tales sistemas utilizaría un loop de retroalimentación en el cual los usuarios reportan todos los errores al grupo de control y este a su vez tomaría la acción para corregir cualquier inexactitud e inconsistencia que pueda presentarse. Hay otros controles de salida, tales como los chequeos manuales sistemáticos, muestreo estadístico, conteos físicos de inventario. Puede observarse muchos métodos de control de salida, pero el nivel de control debe estar en función de la confidencialidad de la salida.

Hemos conocido los controles operativos los cuales se diseñan para asegurar el apropiado funcionamiento del sistema total. Específicamente, para mantener la eficiencia y la interacción apropiada del personal, el hardware, el software y la base de datos.

Algunos efectos que pueden presentarse en los sistemas de cómputo que no están controlados apropiadamente son:

- Pérdida de dinero.
- Pérdida de inmobiliario, equipo, software e información.
- Daños personales.

La degradación de uno de los controles puede ocasionar que se comprometa el sistema entero. Por tanto el auditor debe estar alerta y evaluar cuidadosamente cada uno de los controles operativos.

## 3.3 CONTROLES DE DOCUMENTACION.

La documentación adecuada de los sistemas de computadora, los programas, la operación y otros procedimientos relativos, son necesarios para la comprensión completa y exacta de las actividades de procesamiento en computadora y del impacto de tal procesamiento en los grupos usuarios.

La documentación se utiliza para proporcionar a la gerencia las bases para entender claramente los objetivos del sistema, los conceptos y los resultados y para asegurar que las políticas se cumplan, con objeto de servir como base para la revisión de la contabilidad y de los controles internos, por parte de los auditores internos y externos, y proporcionar una referencia conveniente, a los analistas de sistemas y a los programadores responsables del mantenimiento de los sistemas y de los programas existentes.

Mientras que la necesidad de la documentación es generalmente aceptada, su cumplimiento en la práctica varía considerablemente, existiendo desde organizaciones en donde todo queda archivado en la memoria de los programadores, hasta aquellos que no permiten el inicio de un nuevo proceso, antes de que la documentación completa haya sido elaborada y verificada.

La preparación de un mínimo de documentación requiere una cantidad apreciable de tiempo y esfuerzo por parte de los analistas de sistemas y programadores, lo que, al enfrentarse a presiones en la realización de su trabajo, frecuentemente resulta el primer obstáculo. Sin embargo estas economías han sido frecuentemente excedidas en comparación con los costos de las modificaciones de los programas, en circunstancias en las cuales no se encontró en forma disponible la documentación necesaria.

En la práctica, las modificaciones a los programas, en los casos en que la persona que lo describió no está disponible y no existe la documentación adecuada, con frecuencia significa una lenta y costosa reconstrucción de la lógica del programa seguida por una revisión del programa o inclusive la vuelta a planear y codificar el mismo.

Si en una organización, la documentación de sus procesos en computadora debe de cumplir con estos objetivos, no solamente deberá estar completa, sino que también deberá ser consistente para todos los sistemas, independientemente de quién la preparó, por ejemplo, esta debe ser preparada de acuerdo con estándares pre-determinados. A causa del alto índice de problemas que pueden presentarse y la variedad de equipo y lenguajes de programación existentes, no se cuenta con estándares de documentación completos y universales. Muchas de las ayudas o técnicas utilizadas para la documentación, han sido sujeto de estudio en varios países, que concluyeron en la publicación de diferentes estándares, por ejemplo, el empleo de símbolos para diagramación. Por consiguiente, toda la organización que este planeando la introducción del procesamiento en computadora, deberá establecer estándares adecuados de documentación previos a la iniciación del diseño y la programación de los sistemas.

## Objetivos de Control

Los objetivos principales de control, que deben cumplir los controles sobre documentación, son los siguientes:

1. Asegurar que la documentación adecuada exista y sea controlada con efectividad.

   El entendimiento adecuado del procesamiento en computadora, no será posible si no se cuenta con la documentación adecuada. Los procesos adicionales y las revisiones al procesamiento, serán difíciles de introducir sin amplios conocimientos de los sistemas en existencia, los programas y los procedimientos. Los controles acerca de la documentación, deberán asegurar que la documentación sea elaborada, revisada, autorizada y actualizada, según se requiera.

2. Asegurar que todos los sistemas sean documentados adecuadamente.

Las operaciones de procesamiento en computadora pueden ser introducidas, y pudieran dejar de cumplir con los objetivos del usuario, o pudieran resultar ineficientes o antieconómicas. Los controles de documentación deben asegurar que los requerimientos de los usuarios y sus problemas de procesamiento, en conjunto con el sistema de computadora propuesto, cuenten con controles adecuados y hayan sido establecidos con claridad, en forma tal que pueden ser revisados previamente antes de permitir el inicio de la programación y el procesamiento.

3. Para asegurar que todos los programas son documentados adecuadamente.

Un programador puede comenzar a trabajar en un programa, el cual por diferentes razones tendría que ser terminado por otro programador; en la misma forma las revisiones a un programa pudieran tener que hacerse por un programador distinto del que inicialmente lo escribió. La administración y los auditores, con frecuencia desearán examinar la lógica y los controles incorporados en un programa. Los controles de documentación, deberán asegurar que estén disponibles los detalles suficientes para la completa comprensión de cualquier programa.

4. Asegurar que las instrucciones a todo el personal de procesamiento de datos y del usuario, sean documentadas adecuadamente.

Con frecuencia los operadores de la computadora deberán de utilizar cientos de programas en el desempeño de sus funciones y no se puede esperar que recuerden los requisitos de operación de cada uno de ellos. Los controles de documentación deberán asegurar la existencia de información suficiente para:

a) Permitir a los operadores preparar y procesar cada operación y reaccionar adecuadamente ante errores en los datos, los programas o el equipo, los cuales pudieran detener el proceso de las operaciones.

b) Permitir a otros grupos de personas involucrados directamente en el procesamiento en computadora (por ejemplo, encargados de biblioteca, de conversión de los datos, de control y usuarios) adquirir la información necesaria para el cumplimiento de sus deberes, según se requiera.

Los estándares específicos de control, así como las técnicas de control se detallan bajo los cuatro encabezados anteriores.

### 3.3.1 ASEGURAR QUE LA DOCUMENTACION ADECUADA EXISTA Y SEA CONTROLADA CON EFECTIVIDAD

**Estándares Mínimos de Control.**

- Deberá existir algún método que asegure que se preparó toda la documentación de acuerdo con los estándares predeterminados.

  Los estándares en el Centro de Cómputo, son las normas bajo las cuales deben de trabajar los analistas de sistemas, programadores, operadores de computadora y demás personas involucradas con el procesamiento en computadora.

  Cada organización deberá establecer sus propios estandares de procesamiento de datos que reflejen sus requerimientos y circunstancias propias. Sin embargo en determinadas áreas, tales como las gráficas de flujo y la presentación de las tablas de decisiones, todos los usuarios de computadora deberán seguir normalmente los estándares de la industria o lo que la práctica haya establecido. Todos los estándares decididos por una organización, deberán publicarse para formar parte de un Manual de Estándares, del cual se deberán de distribuir copias a todo el personal interesado, por ejemplo, analistas de sistemas, programadores, operadores de la computadora, departamentos usuarios, administradores y auditores.
  Las personas que sean responsables de la elaboración de la documentación, deberán hacerlo de acuerdo con estos estándares, los cuales deberán de ser respaldados por algún sistema de revisión de la documentación.
  Los estándares deberán ser revisados regularmente y modificados cuando resulte necesario, con el fin de asegurar que reflejen con exactitud las políticas en uso.
  El responsable de la elaboración de la documentación será normalmente:

| | |
|---|---|
| Diseño de sistemas | -Analista |
| Programación | -Programador |
| Procedimientos de operación | -Programador |
| Biblioteca | -Analista |
| Perforación | -Analista |
| Control | -Analista |
| Usuario | -Analista |

  A pesar de que la asignación de responsabilidades se determine en la forma que se menciona, los departamentos usuarios y otros, pudieran participar en la elaboración de la documentación.

Técnicas de Control.

* Se deberán establecer, publicar y poner en práctica los estándares de documentación.

  Los estándares que normalmente se aplican en la elaboración de la documentación de sistemas serán algunos de los siguientes:

  a) Formato y contenido de la documentación de sistemas,
  b) Revisiones previstas.
  c) Normas establecidas para los diagramas de flujo.
  d) Normas establecidas para las tablas de decisiones.
  e) Normas establecidas para la codificación, nombres y abreviaturas estándar, codificación alfabética estándar, números y caracteres especiales.

  f) Terminología - explicación de términos especiales, peculiares de la industria, o la instalación.

* Los estándares de documentación de la programación, deberán ser establecidos, publicados y puestos en práctica.

  Los estándares que normalmente deberán de aplicarse en la elaboración de la documentación de los programas, serán algunos de los siguientes:

  a) Contenido y formato de la documentación de los programas.
  b) Calendario para las revisiones de la documentación.
  c) Normas para los diagramas de lógica.
  d) Normas para las tablas de decisiones.
  e) Normas para la codificación.
  f) Terminología.

* Deberán establecerse, publicarse y ser puestos en práctica estándares acerca de la documentación de operación.

  Los estándares que normalmente se aplicarán en la elaboración de la documentación de las operaciones, serán algunos de los siguientes:

  a) Formato y contenido.
  b) Métodos para la revisión de la documentación.
  c) Normas sobre mensajes y procedimientos en casos de detención.
  d) Procedimientos estándar para reconstrucción y reinicio.
  e) Procedimientos estándar de terminación de proceso.

  Estos estándares para la documentación individual de programas se aplican en forma adicional a los estándares generales de operación para actividades como el manejo de las cintas magnéticas, operación de la máquina, mantenimiento del equipo y otras actividades normales de operación.

* Deberán de establecerse, publicarse y ponerse en práctica, estándares de documentación. Unos de estos son:

  a) Contenidos y formato.
  b) Metodología para la revisión de la documentación.
  c) Formato de las etiquetas externas para archivos en cinta, disco y tarjetas.
  d) Formato del registro histórico de cintas o discos.
  e) Método de numeración de archivos.
  f) Método para fechar.
  g) Método para el almacenamiento de archivos o convencionalmente por orden secuencial de su contenido.

* Estándares para perforación u otra forma de conversión de datos.

  a) Formato y contenido.
  b) Métodos para revisar la documentación.
  c) Códigos de identificación para registros legibles para la máquina.
  d) Reglas concernientes al llenado de ceros a la izquierda, signos algebráicos, señales de fin de campo y fin de registro, cuando se utiliza la perforación en forma libre, etc.

* Se deberán establecer estándares de documentación para la preparación de instructivos para las personas que se responsabilicen del control sobre los datos de entrada y salida de la computadora (grupo de control y grupos de usuarios).

  a) Formato y contenidos.
  b) Metodología para la revisión de la documentación.
  c) Corrección, realimentación y control de los errores detectados.
  d) Períodos para la depuración de los errores.

### 3.3.2 ASEGURAR QUE TODOS LOS SISTEMAS SEAN DOCUMENTADOS ADECUADAMENTE

**Estándares Mínimos de Control.**

- Deberá haber algún método, para asegurar que un problema que debe ser resuelto, sea establecido en forma clara y exacta.

  El diseño de sistemas de procesamiento en computadora, sólo podrá ser controlado efectivamente cuando haya una definición clara y confiable de los requerimientos y objetivos de procesamiento del área en revisión.

- Deberá haber algún método para garantizar que un sistema diseñado con el fin de resolver un problema sea presentado en forma clara y exacta.

Normalmente los sistemas comerciales de procesamiento de datos, son diseñados por analistas de sistemas, que carecen de experiencia en los departamentos usuarios y que en el mejor de los casos no se sentirán responsables por llevar adelante el sistema. Un control efectivo acerca de nuevas soluciones a los problemas de procesamiento, se obtendrá sólo haciendo que el analista de sistemas produzca la documentación de los componentes del sistema, en forma que el mismo pueda ser revisado por la gerencia, los usuarios potenciales, así como los auditores.

- Deberá haber algún método, que garantice que las funciones de control y responsabilidad acerca de cualquier sistema fueron definidas claramente y que los procedimientos de control relativos fueron documentados en forma clara y completa.
La elaboración de información confiable, válida y completa, realizada con oportunidad solamente se podrá obtener mediante el diseño y cumplimiento de procedimientos adecuados de control.

Técnicas de Control.

* Se deberá hacer una difusión del problema para cada problema de procesamiento o área de aplicación general.

La elaboración de una definición del problema, proporcionará un medio por el cual la administración y otros grupos interesados, puedan revisar la definición del problema y así saber de antemano que cambios de política podrá llevar aparejada la instrucción del procesamiento en computadora, y también servirá para evitar que se realicen diseños de sistemas sin autorización.
Al fin de obtener consistencia en el diseño y la totalidad de los datos, se deberá de predeterminar y cumplir con el siguiente formato, que normalmente comprenderá las siguientes secciones:

- Solicitud del proyecto.
- Términos de referencia del proyecto.
- Aprobación del proyecto.
- Asignación de responsabilidad del proyecto.
- Correspondencia diversa y minutas de las juntas relacionadas en el estudio.
- Descripción del problema.

La descripción general del problema deberá comprender por ejemplo:

a) Probables modificaciones en la organización que pudieran ser necesarias.
b) Reasignación de responsabilidades.
c) Descripción de los requerimientos de procesamiento de datos.

d) Descripción de los posibles cómputos especiales.
e) Estimación de los tamaños de archivos y volúmenes de transacciones.
f) Personal actual, descripción general de labores, costos de salarios.
g) Descripción del equipo usado y costo aproximado.
h) Estimación total de los costos al utilizar procesamiento en computadora.

* Se deberá preparar la documentación de sistemas para cada aplicación.
La documentación de sistemas, normalmente es preparada para un sistema completo o un sub-sistema bien definido mas que para un programa de cómputo individual, deberá comprender los siguientes requerimientos:

a) Deberá cumplir con los estándares de sistemas establecidos.
b) Deberá proporcionar a todos los grupos interesados una comprensión clara y confiable del sistema, incluyendo sus objetivos, métodos, soluciones a problemas, archivos de datos, flujo de la información a través del sistema, pasos del procesamiento, programas de la computadora y resultados del sistema.
La documentación de los sistemas, deberá incluir normalmente los elementos siguientes:

- Página de título.
- Página de revisiones.
- Indice.
- Definición y descripción general del problema.
- Descripción general de los sistemas.
- Gráfica general de los sistemas, mostrando el flujo de la información a través del sistema y la interrelación entre los pasos del procesamiento y los procesos en la computadora.
- Tratamiento especial en caso de excepciones.
- Listado de los programasa que componen el sistema.
- Especificaciones de programas.
- Descripción de los documentos fuente.
- Constantes, códigos y tablas.
- Formato de entradas y descripciones.
- Formatos de salida y descripciones.
- Controles de procesamiento y consideraciones acerca de la validación de los datos.
- Procedimientos de control de archivos.
- Pistas administrativas y de auditoría.
- Especificaciones de los datos de prueba.
- Programas y procedimientos de conversión.
- Instrucciones al usuario de departamento de origen y grupo de control.

* La documentación de los sistemas deberá incluir descripciones de las funciones de control, de los procedimientos y de las responsabilidades, en forma clara y completa.

Los controles de procesamiento sólo podrán funcionar en forma adecuada, cuando los procedimientos de control hayan sido documentados convenientemente y comprendidos por las personas responsables de su implantación. Se requerirán procedimientos de control para:

a) Registro inicial de datos.
b) Transmisión de datos.
c) Conversión de datos a una forma que capte el equipo.
d) Procesamiento de los datos en la computadora.
e) Control, corrección y realimentación de errores.
f) Conciliación de las salidas contra las entradas.
g) Distribución de las salidas.

Los procedimientos deberán detallar:

- Persona o personas responsabilizadas.
- Naturaleza de las operaciones que deben realizarse.
- Cuando deben de realizarse las operaciones.
- Descripción de las condiciones de error.

### 3.3.3 ASEGURAR QUE TODOS LOS PROGRAMAS SEAN DOCUMENTADOS ADECUADAMENTE

**Estándar Mínimo de Control.**

- Deberá haber algún método, para asegurar que se preparen todos los documentos y registros necesarios para la comprensión completa de cada programa.

Los programas, una vez terminados pudieran no producir los resultados que se desean debido a que el programador no entendió debidamente el problema o a errores u omisiones. Un control efectivo sobre las correcciones y revisiones a los programas, así como proveer un medio aceptable para revisiones por otros grupos interesados, solamente se podrá obtener si existe una documentación aceptable.

**Técnica de Control.**

- Para cada programa se deberá elaborar la documentación adecuada de la programación.

Una instalación de computadora debe proporcionar las facilidades para revisarla y, cuando resulte necesario, revisar los programas. La descripción del programa, de los registros y las instrucciones para operación, debe completarlas el programador, quien es responsable en un programa, en forma tal que otro programador pueda entender el mismo y realizar las modificaciones a éste. Esto solamente se podrá realizar con la propiedad indispensable si cada programa cuenta con la documentación adecuada.

La documentación del programa normalmente deberá comprender:

- Título o nombre del programa.
- Página de revisión.
- Indice.
- Especificaciones del programa.
- Descripción del programa en forma narrativa.
- Diagrama de lógica y/o tablas de decisión.
- Constantes, códigos y tablas.
- Formato de entrada y salida.
- Formatos y descripciones de los archivos.
- Listado de programa fuente.
- Listado de memoria.
- Instrucciones de operación.

### 3.3.4 ASEGURAR QUE LAS INSTRUCCIONES A TODO EL PERSONAL DE PROCESAMIENTO DE DATOS Y PERSONAL DEL DEPARTAMENTO USUARIO, SEAN DOCUMENTADAS ADECUADAMENTE

**Estándares Mínimos de Control.**

- Deberá haber algún método para asegurar la disponibilidad de toda la información requerida por el operador de la computadora para el cumplimiento de sus responsabilidades.

  Normalmente los operadores de una computadora, trabajan con muchos programas elaborados por distintos programadores. El resultado correcto de la ejecución de estos programas no deberá depender de que el operador tenga en su memoria los requerimientos acerca de la operación de cada uno de ellos. Unicamente se alcanzará un control efectivo sobre las operaciones de la computadora cuando existan instrucciones de operación adecuadas, preparadas de acuerdo con estándares predeterminados.

- Deberá existir algún método para asegurar que se encuentre disponible toda la información necesaria para entender completamente las operaciones de mantenimiento y protección de errores.

  Los archivos pueden destruirse, mantenerse más allá del plazo debido o extraviarse, salvo que se proporcione a las personas que se responsabilicen de los mismos, instrucciones claras y completas referentes a procedimientos tales como: control de archivos, fechas de vigencia, disponibilidad, reconstrucción y requisitos de seguridad de los mismos.

- Deberá implantarse alguna metodología que asegure la disponibilidad de toda la información que requieran las personas encargadas de las operaciones de conversión de los datos.

Los datos que deberá procesar la computadora, normalmente deberán ser transcritos de tal forma que el equipo capte a partir de los documentos fuente. Un control efectivo sobre las operaciones de conversión de datos, se obtendrá mediante el cumplimiento de instrucciones claras y completas.

- Deberá haber algún método para asegurar la disponibilidad de toda la información necesaria para las personas que se responsabilicen de controlar las entradas y las salidas de la computadora.

  Deberán documentarse las responsabilidades del grupo de control, acerca de cada sistema. Las instrucciones deberán de ser claras y completas y seguirse en todos los casos.

- Deberá haber algún método que asegure que este disponible toda la información requerida por los departamentos que proporcionan datos o que reciben información de la computadora.

  El exito de procesamiento en la computadora, dependerá de la puntualidad con que se efectúe la recepción de los datos de entrada, de que los mismos sean confiables y de que estén completos. Sólo se obtendrá un control efectivo acerca de los datos de entrada, mediante la adopción de instrucciones claras y completas a los departamentos interesados y su cumplimiento.

Técnicas de Control.

- Para cada programa deberán elaborarse instrucciones de operación.

  Deberá ser posible para cualquier operador llevar a cabo las operaciones de procesamiento de cualquier programa a pesar de no tener experiencia previa acerca del programa en particular. Esto será posible únicamente, asegurándose de que las instrucciones de operación adecuada las elaboren los programadores por todos los programas que reciban.
  La documentación de operación normalmente deberá comprender los elementos siguientes:

  * Número y nombre del programa.
  * Breve descripción de la finalidad del programa.
  * Esquema de la operación, que muestre las entradas y su secuencia; tarjetas, archivos en cinta o discos, salidas, y la asignación de dispositivos de entrada y salida.
  * Formato de entrada y de salida.
  * Instrucciones especiales de operación relativas a la preparación de la operación de la computadora y los procedimientos finales de operación.
  * Listado de las detenciones programadas y los mensajes en caso de haberlos, y la acción correctiva correspondiente, para proseguir el proceso.

* Procedimientos de recuperación y reinicio a seguir, al encontrarse con una falla del equipo.
* Instrucciones de "terminación del trabajo", que gufen al operador acerca del etiquetado y disposición de las entradas, archivos de salida y reportes, procedimientos de verificación de proceso a proceso y otros requisitos generales de terminación del proceso y limpieza de la máquina.
* Estimación de tiempo normal del procesamiento y límite máximo permitido de tiempo de proceso.

- Se deberán elaborar instrucciones detalladas de operación, para cada instalación de la computadora.

Además de las instrucciones de operación individuales para cada programa, los operadores de la computadora deberán contar con instrucciones detalladas acerca de sus responsabilidades en general y las acciones que deben emprender bajo circunstancias especiales.
Estas instrucciones detalladas, normalmente cubrirán lo siguiente:

* Condiciones adecuadas del medio ambiente, tales como temperatura, humedad y limpieza del aire y qué acción emprender en caso de que no pudieran mantenerse estas condiciones.
* Seguridad de los datos y de los programas. Las instrucciones deberán indicar las personas que puedan tener acceso al cuarto de la computadora y a los programas.
* Acción que deberá emprenderse en casos de emergencia tales como incendio, inundación, fallas de energía eléctrica, actos de guerra o desórdenes civiles.
* Operaciones de respaldo que comprenden dónde se debe de realizar el trabajo, arreglos especiales para la transferencia del sistema operativo, catálogo de programas, programas, archivos, datos, etc., a la instalación de respaldo; así como las condiciones de operación de la instalación de respaldo.
* Registro de los tiempos de procesamiento en la bitácora de tiempo.
* Disposiciones de las hojas de bitácora de la consola.
* Mantenimiento del equipo. Las instrucciones deberán indicar la política general acerca del mantenimiento preventivo y los procedimientos que deben seguirse en casos de falla del equipo.
* Limpieza de las cintas.
* Etiquetas externas de los archivos.
* Procedimientos para la manipulación de cintas y discos, utilización de anillos para la protección de archivos, anillos para el sellado de cintas y cubiertas de almacenamiento.

- Se deberán preparar instrucciones acerca del control de los archivos de cada sistema, y ponerlas a la disposición de la persona encargada de la salvaguarda de los archivos.

  La documentación de los sistemas deberá comprender una sección acerca de los procedimientos de control de archivos, una copia de la cual deberá estar disponible en la biblioteca.
  Los procedimientos deberán de especificar para cada archivo:

  a) Nombre y número del archivo.
  b) Autorización para la creación del archivo (ejemplo, en el caso de archivos de acceso restringido).
  c) Ciclo de actualización.
  d) Ciclo o fecha de retención.
  e) Tamaño del archivo y tamaño del bloque.
  f) En el caso de archivos en disco y otro dispositivo de acceso al azar, cuando se debe copiar en otro medio para fines de respaldo, por ejemplo, en otro disco, cinta, tarjeta o reporte impreso.
  g) Cómo los archivos deben reponerse en caso de que se dañen o destruyan.
  h) Cómo serán almacenados los archivos, en la biblioteca, bóveda especial, área de almacenamiento fuera de la instalación.

- Se deberán preparar instrucciones precisas para la protección de los archivos, en cada Centro de Cómputo que se instale.

  Las personas que asumen la responsabilidad de la custodia y seguridad de los archivos, deberán contar con instrucciones por escrito claras y completas, que comprendan los siguientes conceptos:

  a) Condiciones del medio ambiente necesarias en el área de la biblioteca.
  b) Protección contra incendios requerida en el área de la biblioteca.
  c) Ubicación y utilización de las áreas de almacenamiento fuera de la instalación.
  d) Requisitos de etiquetado de archivos en cinta, discos y tarjetas, procedimientos para numeración seriada.
  e) Procedimientos generales para la creación de archivos.
  f) Cómo y cuándo registrar datos históricos en archivos en cinta o disco en la tarjeta de registro histórico.
  g) Políticas de retención física, aplicables a cintas, discos, etc.
  h) Procedimientos para el mantenimiento y la limpieza de las cintas magnéticas.

- Se deberán elaborar instrucciones acerca de la conversión de datos por cada uno de los sistemas y hacerlas del conocimiento de las personas encargadas de estas operaciones.

La documentación de los sistemas deberá contener una sección acerca de la conversión de los datos, la cual deberá ser del conocimiento de las personas que se responsabilicen de estas operaciones. Las instrucciones acerca de la conversión de los datos, deberán comprender.

- En los documentos fuente, se deberá establecer cuáles son los datos que se deberán de incluir y en qué secuencia.
- En el medio de alimentación, se deberá establecer el formato de los datos de entrada, cualquier código especial que deba emplearse, el uso del llenado de ceros a la izquierda en registros fijos, la utilización de símbolos para fin de campo y fin de registro, tratándose de registros de formato libre, caracteres que deben ser dejados en blanco, forma de registrar las cantidades negativas, especificaciones acerca de campos de contenido solamente numérico, solamente alfabético o mixtos, datos alfanuméricos, o caracteres especiales.
- Registros de control, deberá indicarse el método y el formato para registrar datos de control.

- Se deberán elaborar instrucciones sobre control de los datos por cada sistema y hacerlas del conocimiento de las personas encargadas del control de los datos.

Las personas encargadas del control de los datos de entrada y salida pudieran estar en un grupo de control separado, en el grupo de operaciones de la computadora, o tratarse de empleados de los departamentos usuarios. Independientemente de quien realice la función, las instrucciones necesarias deberán formar parte de la documentación del sistema y hacerse del conocimiento de la persona apropiada.
Las instrucciones deberán cumplir los siguientes puntos:

- Origen y descripción de los datos de entrada.
- Muestra de las salidas.
- Conciliación y/o verificación de las salidas contra las cifras de control.
- Condiciones de error previstas y acción que debe emprenderse al respecto.
- Disposición de salidas.

- Se deberán elaborar instrucciones por cada sistema al departamento usuario y hacerlas del conocimiento de los departamentos interesados.

Se requieren instrucciones para asegurar que los departamentos usuarios conozcan:

- Qué datos o documentos deberán enviar para su procesamiento en la computadora.
- Qué controles deberán establecer sobre los documentos o los datos.
- A qué deberán sujetarse los programas de explotación.

* Códigos especiales que deberán usar.
* Procedimientos de depuración que deberán seguir.
* Reportes e información que deberán recibir.
* Cédula de reportes.
* Qué pasos deberán seguir para realizar la verificación general de los reportes o de la información, por ejemplo:

  - Periodo correcto.
  - Corrección de los totales de arrastre.
  - Los totales del periodo actual, total de los datos enviados.

## 3.4 CONTROLES DE SEGURIDAD.

Introducción.

Generalmente, los controles de seguridad no afectan el procesamiento apropiado y preciso de transacciones tanto como los controles anteriores.

Conceptualmente, un sistema seguro es uno que está a prueba de todo. Los controles de seguridad ayudan a protegerlo contra fallas de hardware, software y gente. La ausencia de estos controles, puede incrementar la probabilidad de errores, tales como:

- Operaciones degradadas.
- Sistema comprometido.
- Pérdida de servicios.
- Pérdida de activos.
- Pérdida de declaraciones no autorizadas de información especial.

Los controles de seguridad, también como todos los controles expuestos antes, se aplican a pequeños Centros de Cómputo, grandes y sofisticados sistemas de cómputo y otros servicios de computadoras. Estos controles son un punto clave, pues ellos no pueden ser rechazados por el auditor.

El control de seguridad está dividido en tres categorías:

- Peligros.
- Técnicas de seguridad física.
- Técnicas de procedimiento de seguridad.

### 3.4.1 PELIGROS.

Un peligro representa un riesgo de pérdida o una oportunidad de daño. Lo opuesto al peligro es la seguridad. En los sistemas de información como en otros sistemas, hay usualmente una jerarquía de peligros. Proporcionaremos las jerarquías de peligros y las metas de control contra estos.

Jerarquías de Peligros.

Las jerarquías de peligro en un Centro de Cómputo están dadas por su probabilidad de ocurrencia y su impacto. Estas jerarquías están basadas en la investigación, intuición y generalización; pero esta sujeta al debate. Además, en cualquier sistema en particular, la manera en que se representan estos peligros es muy diferente.

a. Malfunciones.

Los errores de la gente, el software y del hardware, provocan los problemas mas grandes. Actos de omisión, negligencia e incompetencia, causan mas daño que todas las áreas juntas.

b. Fraudes y accesos no autorizados.

Este peligro es el logro de algo através de lo deshonesto, del engaño o embuste. El fraude puede ocurrir por:

- Infiltración y espionaje industrial.
- Bloqueando las líneas de comunicación de datos.
- Recepción de datos de receptores parabólicos.
- Curiosear archivos de usuarios en terminales.
- Entrar al sistema con clave de otro usuario.
- Confiscación física de archivos y otros documentos.

c. Energía y fallas de comunicación.

En algunos lados, este peligro puede ocurrir con gran frecuencia, más que otros peligros. Para un gran alcance, la factibilidad y confiabilidad de la energía y las facilidades de comunicación, son una función de la localidad. Los apagones ocurren frecuentemente en época de lluvias y esto se debe contemplar. Si el suministro de la energía no es el conveniente, puede quemar los componentes y dañar la computadora. Este peligro puede ser facilmente controlado con un regulador de voltaje y con un sistema de energía ininterrumpible.

También, durante las horas de trabajo, los canales de comunicación están a veces ocupados y/o con ruido.

d. Fuegos.

Los incendios ocurren con más frecuencia de lo que se piensa y pueden ser desastrosos. Se deben considerar los fuegos causados accidentalmente así como los premeditados.

e. Sabotaje y motín.

Se ha tenido casos donde los Centros de Cómputo instalados en áreas urbanas decadentes han sido dañados. Pero la ubicación no es siempre un factor clave; también lo pueden ser bombas y de ahí resultar pérdidas económicas y hasta vidas humanas.

f. Desastres naturales.

Los terremotos, huracanes, inundaciones, trombas, rayos, etc., son devastadores. El sentido común y la planeación ayudarán a reducir el daño que puedan causar. Como se vió el 19 de Septiembre de 1985, fecha que todo México recuerda con tristeza y que debido al terremoto, también para el aspecto computacional fué fatal para el sector público, puesto que sus Centros de Cómputo, estaban instalados en las áreas más afectadas y que a la fecha no se han podido recuperar totalmente.

g. Peligros generales.

Esta categoría cubre peligros aleatorios que son difíciles de definir y anticipar. Normalmente, el sentido común y las seguridades generales disminuirán su ocurrencia. Por ejemplo, un accidente cerca del local del Centro de Cómputo se remediaría con una buena planeación del sitio donde se implantará el Centro de Cómputo.

**Metas de los Controles de Seguridad contra los Peligros.**

Las metas de los controles de seguridad contra los peligros pueden ser vistos como una serie de niveles de controles. Esto es, si un nivel falla, entonces otro nivel lo toma y así sucesivamente, y el impacto en el sistema se reduce.

1o. Disuadir. En este nivel, la meta es la de prevenir cualquier pérdida o desastre que pueda ocurrir.

2o. Detectar. La meta es la de establecer métodos de monitoreo y observación para los peligros y reportarlos para la acción correctiva.

3o. Minimizar el impacto de desastre o pérdida. Si un accidente o desgracia ocurre, deberá haber procedimientos establecidos y facilidades que ayuden a reducir las pérdidas. Por ejemplo, un respaldo del archivo maestro nos ayudará a reducir la destrucción del archivo maestro principal.

4o. Investigación. Si una pérdida ocurre, se debe hacer una investigación inmediatamente para determinar que sucedió. La información obtenida de la investigación puede ser usada para la planeación de la seguridad a futuro.

5o. Recuperación. Debe haber un plan de acción para recuperar desde la pérdida y comenzar operaciones tan pronto como sea posible.

### 3.4.2 TECNICAS DE SEGURIDAD FISICA.

**Incluyen dispositivos y localización física de las facilidades de cómputo que ayuden a resguardarse contra los peligros. Estas técnicas son:**

- **Acceso Físico Controlado.**
- **Posición Física.**
- **Dispositivos de Protección Física.**

Acceso Ffsico Controlado.

La protección de control de acceso es básica para un sistema de seguridad. Si personal no autorizado no puede entrar a las facilidades de la computadora, entonces la oportunidad de perjuicio es reducida considerablemente. Los siguientes puntos ayudan a controlar el acceso.

- Guardias y escolta especial.

Los guardias deben ser localizados en puntos de entrada estratégicos del Centro de Cómputo. Todos los visitantes que tengan permiso para entrar deben ser acompañados por una persona designada.

- Registros de entrada/salida.

Todas las personas deben firmar un registro indicando la fecha, nombre, hora de entrada y salida, propósito de la visita y firma.

- Gafetes.

Codificados por color, con una fotografía en lugar visible y es utilizado para identificar personal autorizado y a visitantes.

- Tarjetas de Entrada/Salida.

El control de tarjeta en su equipo, es usado solo o en conjunción con otras medidas, es probablemente el dispositivo de acceso mas eficiente. Las puertas del Centro de Cómputo se abrirán con tarjetas codificadas óptica o magnéticamente. La autorización de entrada puede ser controlada dinámicamente por puertas individuales, tiempo del día, día de la semana y clasificación de seguridad de los individuos a quienes se les fué dada la tarjeta. Las autorizaciones pueden ser fácilmente aumentadas , borradas, y las actividades de entradas son puestas en un reporte para un control oficial. Los estados de abierto y cerrado de las puertas pueden ser monitoreadas, e intentar una entrada no autorizada, puede ser detectada inmediatamente y una alarma sonará.

- Monitores de Circuito Cerrado.

Los dispositivos de monitores de circuito cerrado de t.v. y cámaras son conectadas a un panel de control, para ser vigiladas por personal de seguridad, estas ya son muy populares. Son muy efectivos para controlar una área muy grande concentrándolos en puntos de entrada y salida.

- Papel Destrozado.

Los reportes nunca deben arrojarse al bote de la basura. En un sin fin de casos, los ladrones pudieron robar información confidencial obteniéndolos del depósito de basura. Cualquier reporte si se va a tirar, se debe triturar; en caso de no tener máquina trituradora se debe despedazarlo hasta hacerlo confeti y así no podrá ser reconstruído.

- Entrada con Doble Puerta.

La primera puerta permite el acceso a los servicios de cómputo, la segunda puerta tiene que ser abierta para entrar al cuarto dónde se encuentra la máquina.

- Puertas de Emergencia abatibles en un sólo sentido.

Los dispositivos antes mencionados pueden ser combinados con otros medios de seguridad. Por ejemplo, la tarjeta puede ser combinada con un identificador de geometría de manos.

Posición Física.

La posición del Centro de Cómputo es una consideración importante en la planeación de la seguridad. Debe tener los siguientes lineamientos :

- Posición Remota.

El sitio de la computadora debe ser localizado lejos de aeropuertos, equipos eléctricos (radares, micro-ondas), áreas urbanas decadentes, tráficos pesados, calentadores de vapor, etc.. Si el sitio no puede estar tan remoto como sea deseable, se puede localizar en un punto dónde se tenga un radio de 60 a 100 metros y que no tenga nada que ver con el exterior instalando alrededor de él, reflectores y una cerca en su perímetro.

- Edificio Separado.

Muchos especialistas en seguridad recomiendan que el Centro de Cómputo sea encasillado en un edificio separado; cuando ocupa un edificio separado, el control de acceso es más fácil, y hay menos riesgo de peligros generales. Por ejemplo, hay menos riesgo de daños de agua o provocados por fuego de productos inflamables utilizados por otros ocupantes. La desventaja de un edificio separado es que un ataque deliberado en la fuente de poder, líneas de comunicación, y suministros de agua pueden ser más fáciles porque el Centro de Cómputo está encasillado en una estructura específica. Si el Centro de Cómputo, no está encasillado, entonces debe estar en el centro del edificio, lejos de paredes y no se ubicará en las plantas alta y baja. No debe ser hecho como un aparador o una vitrina.

- Identificación.

El sitio de la computadora no debe contener ningún signo que lo identifique al exterior.

- Control del Equipo Accesorio.

La energía y las líneas de comunicación deben ser localizadas bajo tierra. Los dispositivos de tomas de aire, compresoras y torres de enfriamiento deben ser protegidas con barreras y/o localizadas en alturas que no puedan ser alcanzadas fácilmente.

- Posición de las Facilidades de Respaldo.

El respaldo juega un papel muy importante en muchas áreas del sistema total de control. El respaldo es el elemento clave de recuperación. Las facilidades de respaldo deben estar lo suficientemente lejos del centro principal para salvarse de los mismos peligros, poderse recuperar rápidamente y ser útil. El sitio donde se localizarán los respaldos debe ser confidencial.

Dispositivos de Protección Física.

Los dispositivos adicionales de protección deben ser considerados en un plan de protección general con los puntos siguientes :

- Drenajes y Bombas de Agua.

Algunas veces los tubos de agua se revientan o el agua en la extinción de un fuego o inundación amenazan a un Centro de Cómputo. Para ayudar a reducir el impacto de estos percances, los drenajes y bombas de agua deben ser instaladas.

- Energía de Emergencia.

De nueva cuenta, el respaldo juega una parte importante en el control. Los UPS (Uninterrumpible Power System) que significa Sistema de Energía Ininterrumpible, éste, debe ser instalado para respaldo de energía para proveer procesamiento continuo. Esto depende hasta de la frecuencia y naturaleza de las variaciones de energía y el efecto que tienen en el Centro de Cómputo. Las fallas de energía o variaciones pueden ir de pocos milisegundos a etapas de gran tiempo. Estas fluctuaciones de energía pueden resultar en pérdidas de datos, errores en el procesamiento, tiempo perdido, mal funcionamiento del equipo, daños, etc..

Un estudio completo de fallas de energía deben ser hechas para determinar las causas de cualquier variación, para Centros de Cómputo menores se pueden eliminar con un equipo generador de energía, o con reguladores de voltaje. Pero hay que recordar que cualquier interrupción puede ser crítica y producir muchos efectos no deseados.

Aunque una UPS no puede ser justificada en algunos lugares estables, en un futuro pueden fallar.

- Cubiertas.

Todos los equipos deben ser protegidos con cubiertas de plástico cuando no se utilicen. En muchos casos los daños por agua en equipo de cómputo se reducen durante un fuego porque el equipo fué tapado y no penetró en él, el agua.

- Control de fuego.

Existen 3 clases de fuego:

Clase A - Celulosa.
Clase B - Líquidos flamables.
Clase C - Eléctrico.

Por lo general, el Centro de Cómputo maneja las clases A y C, por lo que, necesitan detectores de humo y métodos de extinción.

Se recomiendan los siguientes extinguidores en base a costo y tamaño del Centro de Cómputo:

* Extinguidores portátiles de Bióxido de Carbono o HALON.
* Gas fluorido.
* Sistemas con HALON ( no provoca daños a humanos y es el mejor de todos los medios de extinción, preferencialmente el 1301 ).
* Sistemas con CO2 ( con bióxido de carbono, es el indicado para la clase C, pero puede sofocar al personal ).
* Rociadores de agua.
* Sistemas de extinción de humo ( a veces es un gran problema, más que el fuego, porque el material que se quema es tóxico como el plástico y el vinil ).

Para los sistemas de extinción, el personal debe percatarse de que realmente es importante el fuego y encender el sistema en el panel de control y habiéndose encendido las alarmas audibles y visibles para comunicarse además con la Central de Bomberos.

- Seguridad del edificio en general.

Las paredes del edificio deben ser construídas con concreto. Paredes y techos deben tener al menos un rango de una hora de soporte al fuego directo. El número de puertas debe ser limitado, no tendrá ventanas y debe contener ductos de humo.

### 3.4.3 TECNICAS DE PROCEDIMIENTO DE SEGURIDAD.

Es difícil precisar la división entre técnicas de seguridad física y por procedimientos, porque hay mucho de común entre los dos. Una técnica puede trabajar en conjunción con otra, y engrandecer la efectividad de las demás. En mayor instancia, una técnica de seguridad por procedimiento es nada más que el uso de una técnica de seguridad física.

En dónde las técnicas de seguridad físicas traten con fuegos, desastres naturales, etc., y las técnicas de seguridad por procedimiento son casi exclusivamente para el control de acceso, se requerirán de las siguientes técnicas de seguridad física:

- Integridad.
- Aislamiento.
- Identificación.

- Autorización.
- Autenticidad.
- Monitoreo.

**Integridad**

Significa que el sistema es honesto y dependiente. Como un concepto en los controles de seguridad, la integridad es básicamente el aseguramiento de que el sistema está funcionando en forma completa y correcta. La ausencia de integridad ocasionará que los demás conceptos no sean efectivos.

**Aislamiemto**

En los Centros de Cómputo, el aislamiento debe ser mantenido entre los usuarios y la información. También entre los recursos, el hardware, el software y los procesos.

Este concepto reconoce y trata con el incremento de compartimiento simultáneo de facilidades y procesos y el uso extensivo de redes de comunicación de datos en los sistemas de cómputo de hoy en día.

El procesamiento concurrente de muchos usuarios direrentes, requiere la separación y protección de información individual y de los procesos de trabajo. El incremento en el uso de redes de comunicación de datos ha abieto otras exposiciones que deben ser protegidas. Muchos procedimientos de protección que afectan el aislamiento son los siguientes:

- Desconexión y separación. Una forma de que el aislamiento se alcance por distribución geográfica y lógica en la cual no hay conexiones entre ciertos elementos del sistema. Aunque existen relaciones que deben permanecer como las de operador / consola, operador / programa, programador / computadora, analista/programas, usuario / terminal, etc. Por lo tanto, para tener aislamiento debemos evitar cierto tipo de combinaciones.

- Acceso de privilegio mínimo. El privilegio asignado debe ser apropiado para el usuario y tener la autoridad mínima de acceso necesario para realizar los procesos requeridos y no más.

- Ofuscación. Este procedimiento sirve para aislar por confusión, aturdimiento, obscurecimiento u ocultamiento de una penetración potencial en el sistema. Esto se podría hacer, ocultando algunos archivos que no sean desplegados en el listado de archivos, inhibir el despliegue de la entrada en el "user name" y en el "password". Un procedimiento que ayuda a reducir la vulnerabilidad inherente en comunicación de datos es comunmente referida a una encriptación o criptografía. Los sistemas de encriptación comunes envuelven:

  * Sustitución. El cual es la relocalización de mensajes de caracteres con otros caracteres por medio de tablas.

* Transformación. El cual es la conversión de caracteres en un mensaje por un procedimiento aritmético.
* Transposición. La cual cambia el orden de caracteres en un mensaje.

Se pueden instalar cajas de encriptación entre una terminal y el modem. El más común de los métodos es el de cambiar caracteres por letras y números en el mensaje original.

## Identificación

Si un sistema instala procedimientos de aislamiento, entonces los sistemas deben tener también la habilidad para identificar interfases autorizadas y apropiadas. El sistema debe tener la habilidad de distinguir entre aquellos usuarios que su acceso es permisible y aquellos quienes no lo tienen. Dependiendo en el nivel de seguridad requerido, ya sea la persona, la terminal, el archivo, y/o el programa deben ser identificados, para que el derecho de uso pueda ser verificado, y el usuario pueda ser contablemente autorizado. Los métodos para efectuar esta identificación son los siguientes:

- Algún usuario tiene. Un usuario es identificado por algo que el tiene en su posesión. Los puntos de identificación puden consistir de:

  * Códigos (también llamados passwords).
  * Claves para asegurar.
  * Gafetes.
  * Cintas magnéticas o tarjetas ópticas.
  * Números telefónicos.
  * Número de terminal.
  * Claves de encripción.

  La principal desventaja de estos puntos de identificación es que la probabilidad es relativamente alta de que ellos puedan obtener estos puntos y usarlos en su contra.

- Algún usuario conoce. Un usuario es identificado sobre la base de que él sabe algo y solo él lo conoce. Ejemplos de estos puntos son:

  * Códigos personalizados que son cambiados regularmente.
  * Secuencias donde las respuestas del usuario son un conjunto predispuesto de preguntas, por ejemplo, dirección anterior, lugar de nacimiento, color de los ojos de la esposa, etc.. La efectividad de este punto de identificación está directamente relacionada al rango de cambio.

- Características del usuario. El usuario es identificado sobre la base de que algo es parte de él y unicamente suyo. Estas características pueden dividirse en dos categorías:

* Neuromuscular, tal como una firma y escritura.
* Genética. La categoría de genética cubre lo siguiente:
  - Geometría del cuerpo (identificación de la geometría de la mano está siendo utilizado en muchos casos).
  - Huellas digitales.
  - Patrones de respuesta de voz.
  - Apariencia facial (el uso primario está en el gafete, no está todavía disponible comercialmente para identificación por computadora).
  - Iris del ojo y retina.
  - Impresiones del labio.
  - Patrones de onda del cerebro.

Las características arriba mencionadas son características especiales que distinguen a una persona de otras. Sin embargo, la tecnología de cómputo no está disponible comercialmente para esta clase de identificaciones aún.

- Posición de terminales. Sobre la base de posición, las terminales pueden ser dadas en diferentes clasificaciones y niveles de seguridad.

Autorización

Una vez que una persona ha sido identificada como un usuario válido, viene la pregunta, que autoridad tiene ? , esto es, que poder tiene o que derechos ?, por ejemplo en la seguridad de archivos en una base de datos los procedimientos deben ser arreglados para determinar quién tiene acceso a que archivos, quienes tienen el derecho de agregar y borrar, y quien es el reponsable de administrar esos archivos. Los siguientes puntos ayudan a tratar el concepto de autorización.

- Categorizar la autorización. Este paso determina la autoridad específica de usuarios, programas, y hardware. Las clases de autoridad pueden incluir usuarios para documentar, usuarios para equipar, usuarios para programar, usuarios para archivar, terminal para programar, programa para archivar, programa para programar, etc.. Esas actividades que deben ser designadas en conjunción con tipos de autoridad son leídas, escritas agregadas, cambiadas, borradas, copiadas, creadas y apendizadas, etc.

- Uso de códigos. Los códigos (también llamados claves) son ligados a una tabla de autorizaciones. La tabla de autorizaciones es turnada a una tabla de identificaciones, esto es, el usuario es identificado primero como válido. Entonces esto determina que puede hacer el usuario. Aún mas, los códigos pueden ser asignados no solamente a archivos sino que pueden llegar a nivel de registro y si es necesario a campos.

- Programa de seguridad. El Centro de Cómputo por sí mismo debe ser programado no solamente para identificar usuarios válidos sino asegurarse que la autoridad apropiada ha sido otorgada.
  En suma, el programa de seguridad debe tener la habilidad de cambiar la identificación y autorización también como los cambios en los requerimientos de seguridad basados en la hora del día, día de la semana, fines de semana, días festivos, etc.. Por ejemplo, ciertos usuarios deberían perder su autoridad en fines de semana, vacaciones, o días festivos. Incluído en el programa, debe también tener una rutina que reporte la fuente de cualquier violación intentada inmediatamente.

**Autenticidad**

Los procedimientos de autenticidad son requeridos para mostrar que algo es válido o genuino. Aunque alguna o algunas facilidades pueden ser identificadas apropiadamente y autoridad dada para accesar algo o para realizar alguna actividad, el sistema no puede asegurar que el usuario es válido, especialmente si el usuario es identificado sobre la base de "que tiene" o "que conoce". Periódicamente, durante la utilización de archivos sensitivos (también como otros recursos), la validación de los usuarios debe ser confirmada. Esta confirmación puede incluir uno o todos los procedimientos de autenticidad siguientes:

- Observación física; enviar a alguien a la fuente de emisión para confirmar que el usuario es quien lo está reclamando.
- Desconexiones periódicas y procedimientos de volver a llamar, por ejemplo, una terminal es desconectada y conectada nuevamente para ver si la terminal apropiada responde.
- Solicitudes periódicas para mayor información o re-verificación del usuario.

**Monitoreo**

Monitoreo es el hecho de observar, checar, o vigilar algo. Este concepto reconoce que mas tarde o mas temprano, o en forma accidental o intencional, los controles ya mencionados serán neutralizados o rotos. Algunas capacidades del sistema específicos soportan los procedimientos de monitoreo incluyendo lo siguiente.

- Detección de violaciones de seguridad; un sistema de seguridad debe ser instalado para detectar cualquier violación de seguridad tan pronto como éste ocurra. Ejemplos de violaciones son, desuniones de usuarios de códigos de identificaciones de terminal, y solicitudes no autorizadas para un archivo.

- Asegurando el sistema; si ciertas violaciones de seguridad son serias, el sistema debe asegurar automáticamente el sistema de uso.
- Reporte de Excepciones; todas las condiciones excepcionales deben ser reportadas al auditor para su revisión. Los auditores deben ser escépticos si ellos no reciben los reportes. La ausencia de cualquier intento de violación puede indicar que los usuarios están saltándose los controles.
- Reportes de tendencia; el sistema debe colectar los datos concernientes a todos los accesos del usuario. Los datos típicos en este reporte deben incluir:
  * Usuario, terminal, etc.
  * Tipo de procesamiento (demostración, entrenamiento, prueba, operaciones normales).
  * Fecha.
  * Hora del día.
  * Puntos accesados (por ejemplo, nombre del archivo). Estos reportes deben ser revisados sistemáticamente por auditores y oficiales de seguridad.

# AUDITORIA

# AUDITORIA

## 1. INTRODUCCION.

Esta es la segunda parte de la tesis, con la misma importancia que la primera que se refiere a Control. Se puede decir que es la parte complementaria, ya que para que exista una Auditoría en Centros de Cómputo necesitamos tener algo que controlar y viceversa. En este tema daremos una introducción al mundo de la auditoría comenzando con su definición y continuando con las áreas de aplicación hasta llegar a los Centros de Cómputo que es la parte interesada y su relación con las demás.

### 1.1 DEFINICION.

La palabra Auditoría viene del latín "auditorius", que significa "que tiene la virtud de oír". El diccionario la define como "revisión de cuentas colegiado".

La auditoría es la acción del auditor, por lo que, el auditor debe estar encaminado a un objetivo específico que es el de evaluar los controles, para que por medio de señalamientos dé cursos alternativos de acción, tomar decisiones que permitan corregir los errores, en caso de que existan o bien mejorar las formas de acción.

La auditoría no es una actividad que implique la aplicación de 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 seguirse y estimar los resultados obtenidos.

La palabra auditoría se ha mal empleado y se considera como una evaluación con el único fin de detectar errores y señalar fallas, por eso se ha llegado a usar la frase "tiene auditoría" como un sinónimo de que desde antes de realizarse ya se encontraron fallas y por lo tanto se está haciendo la auditoría. El concepto de auditoría debe ser más amplio, no solo detectar errores, sino que sea un exámen crítico que se realiza con el objetivo de evaluar los controles de un departamento o de una organización completa.

### 1.2 AREAS DE APLICACION.

La auditoría tiene un campo de acción muy amplio, que podemos observar y analizar en la ejecución de diversas actividades que vienen realizándose desde el siglo XV. Entre las diversas áreas en las que de una manera u otra se han venido aplicando funciones de auditoría se encuentran:

- Auditoría de Guerra

La realiza un funcionario del Cuerpo Jurídico Militar que informa sobre la interpretación o aplicación de las leyes y propone la resolución correspondiente a procedimientos judiciales y otros instruidos por el ejército o región militar donde tiene su destino.

- Auditoría de la Rota

La puede realizar cada uno de los doce prelados del tribunal Romano de la Rota, pues cada uno, tiene jurisdicción sobre las causas eclesiásticas de todo el orbe católico.

- Auditoría en la Marina

La debe realizar un funcionario del Cuerpo Jurídico Militar de la Armada que tiene funciones análogas a las del Ejército.

- Auditoría Militar

La realiza un funcionario del Cuerpo Jurídico Militar, que no ha tenido facultades jurisdiccionales, asesorando a las autoridades judiciales militares y dirigiendo las diversas tramitaciones judiciales.

- Auditoría Contable

La realiza un contador público que examina los estados financieros de una organización con el fin de dictaminar sobre su razonabilidad.

- Auditoría Administrativa

La persona encargada debe realizar un exámen objetivo, metódico y completo de una organización, así como de sus métodos de control, medios de operación y empleo de recursos.

- Auditoría en Centros de Cómputo

La persona que la realiza tiene por objetivos la evaluación y revisión de los controles en el Centro de Cómputo; siendo más explícitos, es un exámen completo y constructivo del Centro de Cómputo de una organización, en los aspectos de hardware, software y gente; con el fin de descubrir deficiencias e irregularidades, con proposiciones para mejorar el servicio, funciones, condiciones de operación, crecimiento y desarrollo del Centro de Cómputo.

## 1.3 TIPOS DE AUDITORIA RELACIONADOS CON UN CENTRO DE COMPUTO.

**Auditoría Interna.**

La Auditoría Interna es una actividad independiente de evaluación, mediante la revisión de contabilidad, finanzas y otras operaciones que sirven de base a la administración de empresas. Es un control gerencial cuyas funciones es la medición y evaluación de los controles. Sus objetivos están orientados al equipo de cómputo y los sistemas, para lo cual se requieren conocimientos de contabilidad, finanzas, recursos humanos, administración y computación esencialmente.

**Auditoría Contable.**

Las personas dedicadas a la Auditoría Contable con conocimientos de computación podrán obtener revisiones más eficientes ya que les reduce el tiempo y el arduo trabajo requerido para: selección de transacciones y su verificación, selección e impresión de solicitudes de conformidad de saldos, realización de papeles de trabajo, comparación de datos entre registros, determinación de antiguedad de saldos, etc..

En el caso de la Auditoría Contable, la computadora es una gran herramienta para que el auditor automatice algunos de los procedimientos de auditoría, y pueda hacer uso de esta herramienta de trabajo para comprobar los registros que se conservan en la computadora como parte de la evaluación de los registros de una empresa.

**Auditoría Administrativa.**

Es el exámen comprensivo y constructivo de la estructura de una empresa, de una institución, una sección del gobierno o cualquier parte de un organismo, en cuanto a sus planes y objetivos, sus métodos y controles, su forma de operación y sus recursos humanos y financieros.

Se lleva a cabo una revisión y consideración de la organización con el fin de precisar las pérdidas y deficiencias, los mejores métodos, mejores formas de control, operaciones más eficientes y mejor uso de los recursos humanos y financieros.

La Auditoría Administrativa pretende ayudar a complementar a la administración en determinadas áreas que requieren economías y prácticas mejores.

Cualquier empresa de cualquier índole, tiene áreas generales sujetas a investigaciones y que permiten obtener una evaluación de la administración.

La Auditoría Administrativa es la revisión objetiva, metódica y completa de la satisfacción de los objetivos institucionales, con base a los niveles jerárquicos de la empresa en cuanto a su estructura y la participación individual de los integrantes de la institución.

## 2. EL AUDITOR EN CENTROS DE COMPUTO.

### 2.1 CARACTERISTICAS.

El auditor en Centros de Cómputo debe convertirse en un "Doctor" que practique "medicina preventiva", es decir, debe hacer un diagnóstico preventivo a su trabajo. El auditor de Centros de Cómputo debe poder revisar y evaluar los controles y las técnicas de auditoría en cómputo que son fundamentales. Debe estar envuelto en el desarrollo de sistemas para asegurarse que el sistema está controlado apropiadamente y que está diseñado para proveer al auditor de una interfase auditable para monitorear, probar y capturar información confidencial que fluya através del sistema.

La involucración del auditor en la fase de desarrollo es la más importante, porque los sistemas de procesamiento eventual son tan complejos que un retroajuste de controles e interfases auditables podrían ser extremadamente difíciles, o si no impracticables.

El auditor debe tener el derecho de aplicar técnicas de auditoría de cómputo, para recuperar cualquier dato, en cualquier formato deseable desde la base de datos sin interferencias del personal de sistemas. Debe tener la autoridad para asegurar que los programadores utilizan los procedimientos apropiados, la documentación y las ayudas de programación. Debe ver los cambios de software monitoreados y controlados. Debe asegurar que los equipos y software adquiridos tengan control estándar y características de seguridad. El auditor puede aplicar monitores, para colectar y reportar datos operacionales, debe tener la autoridad para ver que los administradores de base de datos y la seguridad se empleen cuando y dónde el lo considere necesario.

En cualquier momento, el auditor puede reportar variaciones significativas a personas de jerarquía mayor quienes tienen la responsabilidad y autoridad para tomar acciones de corrección.

El auditor debe tener un conocimiento firme de Centros de Cómputo, sistemas de información, sistemas de controles y técnicas de auditoría en cómputo. Debe entender diagramas de flujo y tablas de decisión. Debe poder escribir programas y correr, moderadamente, programas de aplicación en al menos un lenguaje de programación. Debe poder obtener independencia del personal de sistemas, seleccionando y aplicando programas de auditoría generalizados. No debe dudar cuando realice una auditoría en la operación de la computadora ni del flujo de trabajo.

El debe poder revisar, comprender y probar un sistema completo de controles y saber como revisar programas de computadora; con todo lo anterior, se puede tener un mejor control y resultados auditables que en un sistema manual.

Debe revisar también la seguridad y confiabilidad de los controles en la estructura de la organización, así como la revisión de la aplicación y evaluación de confiabilidad de controles de manera completa y a tiempo.

El auditor quien actúa como un guardián, debe primero que todo, ser independiente del personal de sistemas. Además debe ser persistente y escéptico, y fusionar ambos atributos con una buena dosis de sentido común. Y en resumen a su experiencia en el campo del control de computadoras y de la auditoría, el debe ser creativo e imaginativo para adaptar condiciones dinámicas.

La oportuna participación del auditor puede detectar posibles debilidades de control pudiendo tomar así medidas adecuadas. Es más problemático modificar un control cuando éste ya se encuentra operando.

## 2.2 PROBLEMAS A LOS QUE SE ENFRENTA EL AUDITOR.

Una computadora es una herramienta potente que puede ser una contribución significativa a las organizaciones y a la sociedad en general . Pero su potencial puede ser distorsionado, porque puede ser utilizado para propósitos fraudulentos.

Más aún, los datos pueden ser almacenados en bases de datos, en donde la confidencialidad de éstos puede ser maliciosamente utilizada.

El auditor por su propia voluntad, através del sistema legal, debe interesarse en el abuso de la computadora, especialmente cuando se relaciona con fraudes e invasión de privacías. Los individuos que tienen un interés especial en el control de la computadora por el abuso son de administración, accionistas, acreedores, consumidores y el gobierno. Todos ellos quieren asegurarse que el sistema de cómputo no vendrá a ser un vehículo para actos delictivos. La mejor persona que estarán buscando para esto, es al Auditor.

Hay un número de maneras en las cuales la computadora puede estar desaprovechada o, por un abuso, provoca errores, administración pobre, sabotaje, etc.. Sin embargo, nos interesamos en dos abusos mayores : Fraude e Invasión de Privacía.

## 2.2.1 FRAUDE.

Fraude es el acto de obtener algo o diversas ventajas através de la mala representación de la verdad y engaños.

Algunas autoridades estiman que las pérdidas por fraude son mas grandes que los robos y siniestros.

Los auditores quienes consiguen un "soplo" acerca de un fraude deben tomar ciertos pasos para resolver completamente sus sospechas, aunque no son detectives, y a veces no hay manera que una auditoría pueda resolver sus sospechas.

La posición histórica del auditor, es que el fraude no está dentro de su responsabilidad y probablemente no es sostenible. Hay muchos casos de fraude administrativo, donde la parte administrativa obscureció la realidad de la actividad corporativa del auditor. No hay duda que el auditor hoy, está siendo esperado para asumir un gran papel.

Los auditores tendrán que cambiar su actitud de decir "esta no es mi responsabilidad", y tomar una visión mas profesional y analizar sus actividades auditables .

Todos los auditores deben utilizar técnicas de auditoría y control que están disponibles. Si ellos no los utilizan, serán presionados duramente para defenderse por ellos mismos en el caso de que una organización fuera víctima de un fraude.

Las responsabilidades de los auditores se han incrementado grandemente en los últimos 20 años. El auditor se debe mover rápidamente dentro del medio para difundirse y provocar un interés público.

Hay seis maneras básicas en las cuales el fraude es cometido en relación a la computadora, estas son :

1. Desaprovechar el tiempo de computadora o robar recursos computarizados.
2. Utilizar la computadora como un "chivo expiatorio".
3. Manipular datos de entrada o introducir intencionalmente datos incorrectos.
4. Alterar o copiar los registros de la base de datos.
5. Modificar el software o sustituir programas inválidos para validar algunos.

6. Interceptar datos transmitidos sobre los sistemas de comunicación.

El fraude es usualmente detectado por accidente o por una equivocación hecha por el defraudador. Los tipos de gente que han cometido fraude son, directores, subdirectores, encargados de préstamos, cajeros, analistas de sistemas, programadores, auditores y operadores de computadoras.

La gente comete fraude por ellos mismos, por sus amigos, o para impresionar a alguien. Hay siempre una oportunidad de quien comete fraude para percibir grandes ganancias de su "cliente" por información confidencial del Centro de Cómputo. El pensamiento de ser atrapado es usualmente suprimido. Se piensa que el fraude es mas fácil de realizar en un sistema de cómputo porque los cambios pueden hacerse o pueden ser copiados de la base de datos sin dejar ninguna pista .

**Fraude en el Desarrollo de Sistemas.**

En relación al desarrollo de sistemas es muy poco probable que un sistema fraudulento haya sido montado alguna vez con esta idea en mente en el momento del diseño. El fraude es siempre algo que se piensa después de que el sistema está en operación. En efecto, de todos los fraudes que han salido a la luz, pocos han sido llevados a cabo por el analista de sistemas; la mayoría han sido perpetrados por el usuario.

La principal tarea es asegurar que la operación del sistema no se deteriorará más adelante, hasta el punto de que se pueda cometer un fraude. Muchos de los aspectos que controlan la precisión también sirven para controlar el fraude, ya que este tipo de actos tiende a desequilibrar las relaciones o a crear situaciones que son difíciles de justificar. Cuando se encuentra una de estas situaciones, el auditor debe profundizar en ella lo suficiente para concluir que se trata de un fraude o de un resultado poco común que puede tener explicación.

**Fraude en las Operaciones del Centro de Cómputo.**

Los casos publicados sobre fraude por computadora muestran que pocos de ellos han sido detectados por un auditor. Aparentemente el fraude se detecta por accidente o debido a una avaricia excesiva de parte del ladrón. En vista de que la tasa de detecciones no ha mejorado considerablemente en los últimos años, parecería no haber muchas instrucciones específicas que puedan darse al auditor para resolver este problema. No obstante, hay algunas sugerencias que pueden ser de utilidad.

Un punto de partida es determinar si todas las entradas y salidas son controladas hasta el punto de que al operador de la computadora se le dificulte agregar una entrada u obtener para sí algún informe sin ser visto. Suponga que el control de entrada y salida cuenta los datos de entrada; suponga también que los programas tienen un paso que cuenta los datos procesados por la computadora. En ese caso, concilie los dos totales para asegurarse que no se han añadido datos entre esos dos puntos.

Hay muchos casos de sistemas que empiezan el control en el punto donde los datos entran por primera vez a la computadora, no antes, donde debiera comenzar.

El punto importante es que cualquier diferencia, por pequeña que sea, debe ser investigada exhaustivamente para conocer su causa. Por ejemplo, un fraude en una nómina consistió en tomar un centavo de la liquidación de cada persona y transferir el total a la cuenta del estafador. Cuando un empleado preguntó el porqué de la diferencia de un centavo en su pago, la administración respondió (sin ninguna investigación de por medio) que se debía a un error de aproximación de la computadora y "usted sabe la cantidad de problemas que hemos tenido con la computadora".

El fraude más común en las computadoras parece ser el robo de servicios; específicamente, desarrollar trabajos de computadora a terceros para beneficios del ladrón. En un caso clásico, se usó todo un tercer turno con este propósito. La compañía defraudada pagó por el espacio, la computadora, el operador de la computadora y la mayoría de los suministros. El único elemento suministrado por el ladrón fué la papelería que utilizó para cobrarles a sus clientes.

Aun si la gerencia puede ser inducida a creer que la organización necesita tres turnos en la computadora cuando solo hay trabajo para dos, el auditor debe estar en condiciones de detectar un problema es esa área. Con seguridad hay, o al menos debe haber, suficientes horarios de trabajo, tandas de entrada y salida, y registros de la operación de la computadora para indicar discrepancias de esta dimensión. Este tipo de fraudes también pueden descubrirse y, aún mejor, evitarse mediante visitas inesperadas a horas no usuales de parte de los auditores y de la misma administración.

Otro fraude que ha llamado la atención es la venta de copias de archivos importantes. Un ejemplo podría ser una lista de correo de clientes potenciales. Puesto que es difícil registrar a los empleados para asegurarse de que no están sacando parte o toda una copia de un archivo, tal vez sea mejor dificultar lo más posible la obtención de tales copias.

Aunque hacer copias de los archivos es un procedimiento normal, el procedimiento puede controlarse en el sentido de cuántas copias se obtienen, quién las obtiene y cuándo. Es posible aun tener una alarma que se encienda cuando determinado archivo está siendo duplicado. La revisión del registro de utilización de la computadora en el programa de copia debe indicar cuándo hubo un intento no autorizado de obtener copia de un archivo. El solo hecho de que se sepa que hay algunos controles y procedimientos de seguimiento establecidos de que habrá acciones disciplinarias, ayuda en alguna forma a evitar el fraude.

La mayoría de los comentarios anteriores son válidos cuando solo una persona está implicada en el fraude. Si varias personas deciden aunarse en detrimento de la organización, es mucho más difícil tener defensa contra ello. Una técnica útil es determinar si todos los libros y las cuentas están cuadradas. Si no lo están, se debe hacer una investigación para descubrir la causa de ello.

**Fraude en la Generación y Conversión de Datos.**

En principio parece relativamente fácil que una persona que está en el área de los datos de entrada creé una transacción cuyo propósito sea el de causar fraude a la empresa para la cual trabaja. Por lo tanto, el sistema debe incluir ciertos controles que dificulten tal acción. Lo que se requiere es dedicar cierto tiempo durante el diseño del sistema a pensar cómo podría alguien tratar de registrar transacciones falsas. Generalmente, el sistema debe diseñarse para que haya una clara separación de deberes, es decir, ninguna persona debe tener control total sobre una función específica.

Un buen sistema de autorizaciones, firmas y doble verificación debe dificultar la preparación de un documento falso, y un buen control de documentos fuente y de los programas de computadora puede dificultar que el operador de conversión de los datos cree un registro en la computadora para un documento de entrada que no existe.

Sin embargo, el auditor que está buscando un posible fraude no debe preocuparse solo por lo que es obvio.

Podría darse el caso de que una persona deseara defraudar a la empresa para la cual trabaja, sin estar pensando en algún beneficio personal. Es posible, por ejemplo, en el caso de un empleado descontento que desee crearle problemas a la empresa. Esto podría hacerse mediante varias acciones que lleven a la empresa a incrementar el inventario más de lo conveniente, a perder clientes, etc.

Algunos auditores creen que la tan mencionada mística de la computadora tiene muchas ventajas como para cometer fraude. La computadora es percibida por algunas gentes como omnipotentes y cualquier salida generada por esta "cosa-sabelo-todo" sin preguntas, debe ser exacta.

Estudios realizados predicen que el abuso de la computadora crecerá con el incremento en el número de instalaciones de computadoras, y fraudes mayores sucederán otra vez y serán cometidos por medio del firmware.

## 2.2.2 INVASION DE PRIVACIA.

Definimos la privacía individual como:

- El deseo individual para ejercitar control sobre la colección de información acerca de uno mismo.

- El deseo individual de ejercitar alguna medida de control sobre el uso de la información acerca de uno mismo, una vez que ésta es recabada.

El punto de privacía individual no es nada nuevo. Esto concierne también al personal de cómputo en sistemas tales como crédito del cliente, personal, seguros y bases de datos mantenidos por un huésped de las dependencias del gobierno.

Los manejos complejos, aparentemente sin solución, llegan a organizaciones, personal de cómputo y auditores dónde los legisladores y juristas se mueven de la filosofía abstracta y teorías de invasión de privacía a provisiones específicas de estatutos detallados y llegan a ser interpretaciones constitucionales .

Ciertamente, el área de problema el cuál acompaña la privacía individual, la confidencialidad de los datos y la seguridad de los Centros de Cómputo es altamente explosiva y fría, si no se negoció con propiedad, se volverá una reacción en cadena, como también es posible hacer daño a los controles de muchas aplicaciones de la tecnología .

Al mismo tiempo, si el problema es tratado claramente por el poder legislativo o jurídico, si la industria no acarrea y pone en práctica sus obligaciones al público y si la comunidad científica se desasocia por sí misma de los apuntalamientos de la tecnología del problema, entonces la tecnología de computadora y de las comunicaciones podrá ser víctima de intrusos e individuos hasta sus propios derechos como ciudadanos y consumidores. Entonces, el problema de invasión de privacía es tan complejo que cualquier solución de progreso depende de los esfuerzos coordinados y de la cooperación del gobierno convertidos en reglamentos y leyes contra este gran problema.

La protección de la privacía en lo individual está fundada en leyes, reglamentos e interpretaciones que rigen las áreas legislativa y judicial; por lo cual es una responsabilidad de la Procuraduría General de la República, interpretar y proveer lineamientos para su manejo y del auditor para las interpretaciones de estas leyes e interpretaciones judiciales y como evitar conflicto entre ellas.

Esta es una gran responsabilidad de los fabricantes de equipo que tienen que trabajar con otras empresas y con el gobierno, para plantear e implantar la seguridad de la tecnología y sus dispositivos relacionados. Características muy desarrolladas en capacidad y seguridad deben ser incorporadas en el hardware y software y especialmente en los sistemas operativos.

Dar elementos de monitoreo y prueba al sistema, que deben ser incluídos en el diseño. La complejidad en los sistemas operativos prohibe las pruebas y como resultado, los procedimientos de prueba indican frecuentemente la existencia de errores o desusos, pero no su ausencia.

El sistema operativo debe asegurar que los usuarios no puedan interferir con las operaciones del sistema, tomar el control del sistema, o estrechar o alterar los sistemas de seguridad. El sistema operativo debe asegurar que el usuario no pueda tener acceso sin autorización a datos de otros usuarios o interferir con programas de otros usuarios.

Esta es la responsabilidad del auditor para asegurar que el sistema de control está en su lugar para asegurar que el Centro de Cómputo sea complaciente con los requerimientos legislativos y judiciales de la privacía.

Aún sin una legislación, como en México, el auditor debe averiguar el efecto de las normas existentes. Cada auditor debe revisar el sistema de controles y las políticas de administración de su organización y decidir que legislación y reglamentación tuvieron y deberán tener.

El auditor debe balancear las finalidades del Centro de Cómputo, el cual se incrementa accesiblemente, contra las demandas compensadas referentes a la exactitud, integridad y confidencialidad. Una de las metas del diseño de sistemas de información es dar acceso rápido al sistema a una variedad de usuarios através de la organización. Sin un control propio, esta característica puede presentar problemas.

Es probablemente imposible encontrar requerimientos de privacía sin un sistema de control, pero un sistema con muchos controles no garantiza privacía. El acceso controlado tiene problemas con el sistema y la privacía. Pero uno puede estar controlando el acceso desde un punto de vista del sistema sin lograr privacía desde un punto de vista legal.

## 3. AUDITORIA EN CENTROS DE COMPUTO.

### 3.1 TIPOS DE AUDITORIA EN CENTROS DE COMPUTO.

La Auditoría se puede dividir en cuatro tipos:

- Auditoría externa por una firma especializada. Esta auditoría se realiza, generalmente, para que la firma obtenga evidencia sobre los estados financieros de la organización. Debido a que la mayoría de los sistemas financieros de los clientes de la firma están manejados en computadora, es necesario estudiar la computadora y ver como trabajan esos sistemas. Esta auditoría externa también se puede entender con los controles internos y la protección de los activos de la organización. Estos objetivos se pueden alcanzar normalmente en forma más efectiva al auditar el sistema y no los datos.

- Auditoría externa hecha por las oficinas de impuestos, o por algún ente de la industria, como, por ejemplo, el banco estatal o una aseguradora. El propósito de esta auditoría es similar a la auditoría que hace una firma especializada. Como el cliente ha entregado cierta información financiera y como muchos clientes del negocio están pendientes de su operación, la auditoría se realiza para asegurar que la compañía tiene lo que dice tener. De nuevo, se hace énfasis en los controles internos para estar seguros de que los activos están protegidos.

- Auditoría externa por la oficina de Hacienda, que se preocupa por la exactitud de los cálculos de la deuda por concepto de impuestos. Esta oficina se basa principalmente en los datos sobre retención, consignados por los contribuyentes en un formulario procesable en computadora.

- Auditoría interna por empleados especialmente designados para ello (auditores internos o auditores de Centros de Cómputo) o por expertos externos en auditoría, contratados por corto tiempo. El propósito de este tipo de auditoría puede ser uno de los siguientes:

  * Asegurar exactitud (con un relativo margen de error) en todas las fases de la operación. Se relaciona directamente con el control interno y la protección de los activos. Es de esperar que una alta precisión permita obtener mejores resultados.

* Verificar la efectividad del sistema. Están los usuarios obteniendo lo que necesitan o lo que creyeron que iban a obtener ?

* Asegurar la efectividad del sistema o del uso de los recursos sobre la base de costo-beneficio. Eficiencia y efectividad no deben considerarse iguales. Un sistema puede llevar a resultados muy valiosos (ser efectivo), pero a un costo injustificado (es decir, ineficiente). Por otro lado, un sistema puede operar eficientemente, a un bajo costo, pero producir resultados de poco valor.

* Asegurarse de que se están cumpliendo las políticas y los procedimientos establecidos. Los sistemas se diseñan para operar en una forma específica y la auditoría es un método para verificar que lo hagan. Por ejemplo, un sistema puede diseñarse para seguir una secuencia específica de pasos en el desarrollo de una escala de créditos para un nuevo cliente o para cambiar la existencia de un antiguo cliente.
En el curso de una auditoría interna, se puede encontrar que este procedimiento preestablecido se ha alterado inadvertidamente , debido, tal vez, a los problemas de la operación diaria. (Este aspecto de la auditoría puede involucrar ciertos requisitos legales que deben ser tomados en cuenta)

* Proteger la reserva. Con todas las actitudes y leyes relacionadas con la violación de la reserva, puede ser necesario auditar el sistema para determinar si se ajusta a la ley.

* Proteger la propiedad de los datos y/o programas. Es probable que la gerencia desee verificar periódicamente las medidas de seguridad sobre los datos y los programas para segurarse de que no caigan en manos de los competidores o de cualquiera que los pueda usar en deterioro del propietario.

* Velar por la seguridad de las personas, los datos, los programas y el equipo. Esto se refiere a los métodos usados para evitar su pérdida o destrucción por causas debidas al fuego, a inundaciones y a eventos similares que puedan atentar seriamente contra la normal operación del sistema. Un aspecto de importancia es la habilidad para recuperarse de las pérdidas cuando ellas ocurren.

* Cualquier otro punto que la gerencia o la auditoría quieran verificar.

Gran parte del trabajo de la auditoría interna puede tener impacto significativo sobre cualquier auditoría externa que se vaya a realizar en el mismo período. Una auditoría interna bien realizada puede ser muy útil para un auditor externo y puede además ayudar a reducir el costo de una auditoría externa apreciablemente.

Así mismo, la auditoría interna, cuando se le orienta en forma práctica, puede conducir a que se hagan sugerencias útiles para mejorar las operaciones.

La figura 1 resume los intereses de los cuatro grupos diferentes de auditores.

| | Firma de Auditores | IRS | Agencia del Gobierno | Auditoría Interna |
|---|---|---|---|---|
| Precisión | G | G | G | G |
| Efectividad | M | - | M | G |
| Eficiencia | M | - | - | G |
| Seguimiento de Políticas y Procedimientos | G | M | M | G |
| Revisión de Resultados | - | - | - | G |
| Fraude | M | - | M | G |
| Reserva | - | M | M | G |
| Propiedad | - | - | - | G |
| Seguridad | M | M | M | G |

G = Gran interés M = Moderado interés - = Poco o no interés directo

F I G U R A 1

## 3.2. OBJETIVOS Y PROCEDIMIENTOS DE AUDITORIA.

Al juzgar el significado de la función del Centro de Cómputo de una compañía, el auditor tiene primero que determinar el grado en que se utiliza el Centro de Cómputo para procesar la información que respalda los estados financieros que va a examinar y si hay algunas aplicaciones que requieran atención especial de auditoría. Su objetivo primario es recabar información que puede usarse para tomar decisiones respecto de cuánto se necesita hacer para lograr los objetivos de auditoría en un área determinada, así como la manera en que podrían ser logrados efectivamente. Si lo que encuentra preliminarmente indica que la función del Centro de Cómputo, o algunas de sus aplicaciones, son importantes desde un punto de vista de auditoría, entonces el auditor puede encontrar que es necesario hacer una revisión más extensa de los procedimientos y controles en vigor en las operaciones del Centro de Cómputo y, quizá, continuar con revisiones y pruebas detalladas de ciertas aplicaciones específicas.

La naturaleza y extensión de las revisiones y pruebas del auditor respecto de la función del Centro de Cómputo deben ser coordinadas con otros segmentos de la auditoría para asegurar que el alcance global de la auditoría es adecuado y evitar duplicación de esfuerzos por parte de los varios miembros del grupo de auditores. Como parte de su exámen, el auditor revisará y evaluará los procedimientos y controles en varias áreas. Cuando se usa el Centro de Cómputo para procesar una información en una o más de esas áreas, debe tomarse en cuenta al establecer el plan de auditoría para cada una de ellas. El grado hasta el cual las pruebas se dirigen específicamente a controles y rutinas de procesamiento del Centro de Cómputo dependerá del criterio del auditor en cuanto al modo más efectivo de cumplir con sus objetivos.

El objetivo de evaluar los controles es predecir la confiabilidad del proceso que se está controlando. Una metodología sólida de auditoría establece que, antes de probar el cumplimiento de los controles, es necesario determinar:

1. Que existan normas relativas a los controles.
2. Que estas normas sean adecuadas para proporcionar el grado de confiabilidad deseado.

### 3.2.1 NECESIDAD DE QUE EXISTAN NORMAS.

El principal requisito para la utilización consistente de los controles es que existan normas que las requieran. Si los controles que se examinan y evalúan no han de usarse también en el futuro, la predicción basada en su exámen no resulta válida. Sin la existencia de normas para las operaciones, el auditor no tiene fundamento alguno que le sirva de base para hacer una predicción.

### 3.2.2 PROPOSITO DE NORMAS.

Las normas relativas a los sistemas de información describen las operaciones y los requisitos para todas las actividades y resultados de dichos sistemas. Las normas se desarrollan y se aplican a funciones tanto manuales como computarizadas. En efecto, una norma es una aseveración formal, por escrito, de "como se hacen aquí las cosas".

Actualmente la mayoría de los Centros de Cómputo tienen o están desarrollando algún tipo de documentación formal respecto a las normas. Vale la pena hacer notar esta tendencia, aun cuando la calidad de los controles que se expresan en las normas varía ampliamente y con frecuencia tiende a ser menos que adecuada.

Las normas de sistemas cubren todas las actividades de los Centros de Cómputo y se aplican a un nivel tanto lógico como técnico. Las normas técnicas son necesarias para la programación y la operación de las computadoras. Sin embargo, las normas a nivel lógico proporcionan la clave para el control y la auditoría de las aplicaciones en Centros de Cómputo.

### 3.2.3 LAS NORMAS COMO AYUDA PARA LA AUDITORIA.

El contar con normas formales por escrito para los sistemas, facilita y mejora el proceso de conocimiento, evaluación, y prueba de la confiabilidad de los sistemas. Observando la operación y los resultados del procesamiento del sistema, el auditor puede determinar si las acciones y los controles especificados en las normas de sistemas realmente existen en los procedimientos implantados. La documentación requerida para la comunicación entre los usuarios y los especialistas en sistemas también le resulta útil al auditor.

Además, el valor de la actividad de auditoría se incrementa debido a que el nivel de conocimientos del auditor respecto a las funciones y la operación del sistema va más allá de lo que sería posible de no existir las normas de sistemas. Al contar con documentación, el auditor puede planear su trabajo para revisar simultáneamente la confiabilidad de los sistemas y la adhesión de los controles tanto a las normas de las aplicaciones como a las de la instalación.

En el pasado, las normas documentadas eran una rareza. Sin embargo, un número cada vez mayor de gerentes generales y de sistemas están reconociendo que las descripciones precisas de los sistemas se pagan por si mismas al:

- Mejorar los controles.
- Reducir los costos.
- Facilitar la ejecución de las revisiones de auditoría.
- Minimizar las interrupciones causadas por las actividades de auditoría.

En muchos casos, este requerimiento respecto a la documentación durante una auditoría debe servir de aliciente para la preparación de normas.

Cualquier trabajo de auditoría que incluya el exámen de sistemas de cómputo en los cuales el auditor pretenda confiar, deberá presuponer que antes de llevar a cabo una revisión de las aplicaciones, el auditor se familiarizará con las normas relativas. La ausencia de estas normas o el que sean inadecuadas es motivo de comentarios por parte del auditor y modificaciones al alcance planeado para los procedimientos de auditoría sustantivos. La habilidad para revisar la documentación del sistema a nivel lógico es probablemente el requisito más importante en la auditoría de aplicaciones del Centro de Cómputo.

Esta área de actividad presenta toda una nueva dimensión de oportunidades para los auditores. Con la documentación apropiada de las aplicaciones, el auditor puede comprender las alternativas y el razonamiento que respaldan las reglas de decisión utilizadas en las aplicaciones, y evaluar su efectividad. En efecto, a la función tradicional de dictaminación que efectúa el auditor, se agregará una nueva dimensión de auditoría operacional. Por lo tanto, en las situaciones en que existan normas adecuadas, la presencia de una computadora aumentará, más que disminuir, su auditabilidad.

Las normas de sistemas son la base apropiada para auditar los controles sobre los sistemas de cómputo. La presencia, ausencia o grado de control se relacionan directamente con el alcance, la integridad y la comprensibilidad de la documentación.

Una auditoría más significativa respecto al cumplimiento de los controles sólo podrá tener lugar después de haberse establecido las normas adecuadas.

Para obtener la información que necesita, con objeto de hacer una evaluación de la función del Centro de Cómputo, con el propósito de decidir acerca del enfoque y alcance de la auditoría, el auditor puede proceder de la siguiente forma:

### 3.2.4 REVISION PRELIMINAR.

Cada compañía es única y su singularidad debe ser reconocida en la manera como es auditada. Por lo tanto, antes de poder tomar una decisión respecto al alcance requerido en una situación específica, el auditor debe determinar el grado en que el Centro de Cómputo se usa y que tan importante es desde el punto de vista de la auditoría. Una revisión preliminar dirigida hacia esos objetivos debe ser diseñada para determinar:

- Cómo se usa el Centro de Cómputo para procesar datos financieros.
- La ubicación de las principales instalaciones del Centro de Cómputo y los tipos de equipo usados.
- Los tipos de transacciones contables procesadas y las aplicaciones efectuadas.
- El significado para auditoría de las transacciones contables procesadas.
- Los tipos de controles de entrada-salida establecidos fuera de la función del Centro de Cómputo para facilitar la exactitud de la información procesada.
- Las reacciones de los usuarios respecto de lo oportuno, completo y exacto de la información recibida del departamento de cómputo y su documentación.

- La solidez aparente de la organización del Centro de Cómputo en número e idoneidad del personal en lo adecuado de su administración y en sus funciones de seguridad.

La revisión preliminar del Centro de Cómputo unicamente necesita ser lo suficientemente profunda para suministrar un entendimiento del significado de la función del Centro de Cómputo dentro del sistema total de procesamiento de datos. La información obtenida, tiene entonces que combinarse con la evaluación del auditor de los procedimientos y controles relacionados con la parte no incluída en el Centro de Cómputo, del sistema total de procesamiento de información, con el fin de decidir la naturaleza y extensión de su actividad de auditoría que debe relacionarse específicamente con la función del Centro de Cómputo. Debe él entonces decidir si puede obtener el grado requerido de seguridad de auditoría fuera del ambiente de sistemas, sin evaluación adicional de la propia función del Centro de Cómputo.

3.2.5 REVISION GENERAL DE PROCEDIMIENTOS Y CONTROLES.

Esta revisión debe determinar que los procedimientos y controles relacionados con la función del Centro de Cómputo son adecuados y compatibles con otros procedimientos y controles dentro de la organización financiera de la compañía. Se presenta a continuación un bosquejo de las áreas principales que el auditor debe considerar para su revisión.

3.2.6 REVISION DE LAS APLICACIONES ESPECIFICAS.

Cuando el auditor llega a la conclusión de que necesita hacer una revisión detallada de aplicaciones específicas, debe entonces tratar más señaladamente con los varios controles en los que estos se relacionan con las aplicaciones respectivas.

Sobre las base de lo que encuentre durante la revisión general, normalmente estará en posición de evaluar fácilmente los elementos de control que son importantes para sus objetivos y el grado en el cual tienen que practicar pruebas específicas para llegar a satisfacerse de la efectividad de tales elementos durante el período en que está examinando.

Pueden también necesitar procedimientos de auditoría para determinar que los respectivos programas de la computadora y rutinas de procesamiento y servicios del Centro de Cómputo no logran aquello para lo que fueron diseñados. Esto puede requerir una revisión detallada de las formas y documentación usadas para controlar el flujo de información a través de la aplicación, una revisión de documentación que respalde los programas de la computadora y pruebas específicas para determinar que los programas de la computadora están funcionando adecuadamente.

Los procedimientos usados por el auditor en su revisión de las aplicaciones específicas deben coordinarse de cerca con las pruebas usadas en la parte del exámen que no queda dentro del procesamiento de información, para las áreas de auditoría a las cuales se refieren esas aplicaciones y así asegurar un esfuerzo balanceado de auditoría.

Debe ser obvio que este tipo de revisión del Centro de Cómputo puede ser complejo y requerir estar familiarizado con los conceptos y controles de la programación. En muchos casos, será necesaria la ayuda de un especialista en sistemas.

### 3.2.7 PROGRAMAS DE AUDITORIA Y DOCUMENTACION PARA LOS PAPELES DE TRABAJO.

Para llevar a cabo una revisión efectiva, ya sea preliminar o general, de la función del Centro de Cómputo, es deseable que el auditor prepare un cuestionario detallado para asegurar que la revisión logre el grado de interrogación penetrante que las circunstancias requiera. Este cuestionario debe ser lo suficientemente detallado para permitir al personal que ejecuta la revisión tener, un claro entendimiento de los objetivos. (Ver 4.3 RECOPILACION DE INFORMACION)

Cuando el auditor llega a la conclusión de que es necesario revisar aplicaciones específicas, debe combinar las actividades de auditoría en esa área, la revisión de la aplicación manejada en el procesamiento de información con la parte no incluída.

Cuando el auditor utiliza los servicios de especialistas en sistemas, debe controlar la revisión, y en ninguna circunstancia debe emprenderse la revisión por los especialistas hasta que el auditor haya establecido por escrito su plan y objetivos de auditoría y ambas partes claramente entiendan con exactitud lo que debe hacerse.

La forma y contenido de los programas de auditoría variarán significativamente, dependiendo del alcance de la actividad del auditor en lo que se relaciona con la función del Centro de Cómputo. Los procedimientos de auditoría que deban seguirse dependerán de las circunstancias de la organización que está siendo revisada, y el gerente de auditoría tiene la responsabilidad de precisar el enfoque de la auditoría.

Es importante notar que raramente podrá un auditor obtener, o aún buscar, completa satisfacción de pruebas dirigidas solamente a determinar la efectividad de una aplicación específica del Centro de Cómputo. A menudo, la actividad de auditoría hacia el Centro de Cómputo será solamente una pequeña parte del esfuerzo total de auditoría.

Al concluir una revisión del Centro de Cómputo, el auditor debe preparar un escrito que describa los resultados de la revisión y, cuando sea apropiado, las pruebas de las aplicaciones específicas del Centro de Cómputo. Si bien la extensión de la revisión puede variar de un año a otro, al completar cada exámen el auditor debe estar en posibilidad de contestar preguntas en lo que atañen a las áreas de importancia.

## 4. DESARROLLO DE LA AUDITORIA.

Para poder realizar la auditoría es necesario llevar una secuencia de pasos que nos lleven a la evaluación final del Centro de Cómputo, y al cumplimiento de los objetivos de la empresa con respecto a los servicios de cómputo.

Los siguientes pasos deben reflejar los puntos mas importantes en el desarrollo de la auditoría, puede ser que existan mas o menos, pero eso depende del enfoque global o particular de cada auditor. Para esta tesis los pasos son los siguientes:

4.1 Areas de Auditoría.
4.2 Definición de Objetivos.
4.3 Recopilación de Información.
4.4 Evaluar los Controles.
4.5 Diseñar y Efectuar Pruebas y Procedimientos.
4.6 Evaluación General.

Los cuales se ampliarán a continuación para poder evaluar finalmente la situación en la que se encuentra el Centro de Cómputo.

## 4.1 AREAS DE AUDITORIA .

Dentro de la auditoría debemos manejar todas las áreas correspondientes al Centro de Cómputo, que vienen a ser generalmente, el Personal, el Equipo y los Programas que a fin de cuentas son las áreas de Administración, Operación, Documentación y Seguridad (en las cuales se le puede dividir) mismas que las Areas de Control para su conjunción y entendimiento.

### 4.1.1 ADMINISTRATIVA .

Una revisión general de la estructura de la organización del departamento del Centro de Cómputo, junto con un entendimiento de los deberes y responsabilidades asignados a las diversas unidades dentro del departamento, proporcionará al auditor conocimiento de cómo se planean y controlan las actividades del departamento.

Consecuentemente el auditor puede:

- Revisar la estructura de la organización del departamento de cómputo, incluyendo líneas de autoridad y responsabilidad para las actividades clave.

- Revisar la razonabilidad de los niveles de escalafón e idoneidad del personal del Centro de Cómputo.

- Determinar que existe una segregación apropiada de trabajo para las funciones clave.

- Determinar que existe una coordinación apropiada entre la función del Centro de Cómputo y otros departamentos afectados dentro de la organización.

- Se han tomado en consideración procedimientos de mantenimiento preventivo y se han hecho arreglos para contar con equipo de respaldo.

Los controles de la organización en un ambiente de procesamiento electrónico de información deben proporcionar un control efectivo sobre el departamento de sistemas y sobre la utilización de los servicios de la computadora por toda la organización.

Una revisión de la estructura de la organización del departamento de cómputo, junto con un entendimiento de los deberes y responsabilidades asignados a las varias unidades dentro del departamento, suministrarán un entendimiento de cómo se planean y controlan las actividades del departamento. La presencia o ausencia de organigramas, descripciones de tareas y manuales de políticas y procedimientos pueden ser indicadores importantes de los controles globales en vigor.

El procesamiento electrónico de información toca a todas las partes de una empresa y la variedad de problemas que puede generar hace que sean esenciales prácticas definidas de organización y administración. La existencia de una estructura de organización sana y la bondad de políticas y procedimientos administrativos no garantizarán que los datos serán debidamente manejados; pero la ausencia de esos factores bien puede indicar que no están siendo debidamente manejados. Hay muchos factores que el auditor debe considerar para determinar si existe un plan efectivo de organización y un clima dentro de la compañía que tenga probabilidad de dar por resultado procedimientos y controles de administración sanos.

Esta sección delinea los factores que deben considerarse en la evaluación de los aspectos de la organización del departamento de cómputo o de sistemas.

El departamento de sistemas debe ser independiente de los departamentos de operación para los cuales procesa información.

La mayoría de las instalaciones de Centros de Cómputo tienen responsabilidad conjunta y participan hasta cierto grado con los usuarios en la preparación, procesamiento y mantenimiento de datos y registros relativos. Una separación de las siguientes funciones es un procedimiento básico de control que debe establecerse en todos los sistemas y organizaciones para impedir que un solo grupo de individuos tengan control completo sobre una transacción entera:

- Iniciación y autorización de las transacciones.

- Registro de las transacciones.

- Custodia de los activos.

El departamento de sistemas normalmente actúa en calidad de unidad de servicio para otros departamentos y su papel debe limitarse al procesamiento de información. Los documentos fuente normalmente se originan en (y deben ser autorizados por) algún departamento fuera del Centro de Cómputo.

Por ejemplo, cuando se procesan datos financieros, los empleados del departamento de contabilidad no deben intervenir directamente en las operaciones reales del departamento de cómputo.

Muchas compañías proporcionan esta segregación de responsabilidades mediante:

- La asignación al departamento que proporciona la información de entrada de la responsabilidad de su autenticidad, exactitud e integridad. El departamento de sistemas, a través del uso de su equipo, puede ayudar en esta responsabilidad mediante la comparación de la información de entrada con los controles por batch sometidos junto con esa información por el departamento en que se origina.

- El establecimiento del departamento de sistemas como una unidad separada, independiente, desde el punto de vista de organización, de los departamentos de operación y previendo que no tenga acceso a, o control sobre los activos y libros de contabilidad. Si bien el departamento de sistemas normalmente procesa las nóminas, desembolsos y otra información que genera como resultado la expedición de cheques de la compañía, etc., no debe permitírsele que inicie transacciones o cambie los datos fuente pues entonces el personal de cómputo podría estar colocado en una posición en que pudiera desviar activos de la compañía para su propio beneficio.

- El requisito de quien recibe y usa la información procesada ejecute procedimientos de comprobación para fines de control.

El departamento de sistemas debe reportar a la alta gerencia.

El departamento de sistemas puede procesar datos para varios departamentos en la organización, y debe estar en posibilidad de tratar objetivamente con esos departamentos. Para hacer esto efectivamente, y para poder mantener su independencia, el departamento de sistemas debe estar bien dirigido y contar con el grado necesario de respaldo y autoridad de la alta gerencia. Frecuentemente, esto requerirá que el departamento reporte a un ejecutivo de cuando menos el mismo rango de los gerentes de los departamentos para los cuales procesa información.

La supervisión en el departamento de sistemas debe ser adecuada para asegurar observancia de los procedimientos de operación preescritos y para permitir que el departamento sea debidamente dirigido.

El mejor diseño de los sistemas no funcionará si la gente que lo usa no sigue los procedimientos preescritos. Es responsabilidad de la gerencia ver que el sistema trabaje mediante una supervisión cuidadosa. Para determinar que todo el personal del departamento de sistemas está llevando a cabo sus tareas de una manera satisfactoria, el gerente del Centro de Cómputo o algún otro supervisor debe, entre otras cosas:

- Determinar que el trabajo de sistemas y programación esté adecuadamente planeado, revisado, probado y documentado.

- Revisar varios reportes preparados durante el procesamiento, tales como bitácoras de utilización de máquinas y listados de la consola, y aprobar las acciones tomadas respecto de paros de la máquina y correcciones de errores.

- Observar a los operadores en acción en varios momentos para determinar que están siguiendo las instrucciones.

- Estar al tanto de la naturaleza de los problemas y dificultades que van encontrándose, y satisfacerse de que se están tomando los pasos apropiados para tratarlos. Tales problemas pueden incluir equipo, programas, horarios de trabajo, calidad de datos, comparación de cifras y control.

Los factores fundamentales que el auditor debe considerar en su evaluación de la función gerencial del departamento de sistemas, son similares a los de otras áreas del negocio. Como son dirección, uso de técnicas apropiadas, buen personal, capacitación, disciplina.

Debe existir un organigrama para el departamento de sistemas en el cual estén claramente definidas las líneas de responsabilidad y la obligación de rendir cuentas. (Ver Controles de Personal)

Es deseable que las descripciones y responsabilidades del trabajo estén especificadas por escrito.

Deben prepararse descripciones de trabajo para todos los empleados del Centro de Cómputo y el plan de organización debe estar expuesto explícitamente para establecer la responsabilidad básica. Aunque los títulos pueden variar en diferentes compañías, las descripciones referidas en Funciones y Responsabilidades son comúnmente las que se encuentran en la mayoría de las instalaciones de cómputo.

En general, el analista de sistemas requiere el más alto grado de adiestramiento y los antecedentes más amplios. Los programadores siguen al analista en el nivel requerido de aptitud. Los operadores de máquinas requieren menos antecedentes y adiestramiento que el analista o el programador.

Nuevamente, una de las claves para el éxito en cualquier organización es el nivel de competencia y calidad de su personal. Como en cualquier otro campo de esfuerzos, el nivel de adiestramiento y experiencia que un individuo tenga en cada uno de los puestos mencionados será una buena indicación de su idoneidad.

Las responsabilidades dentro del departamento de sistemas deben prever una segregación apropiada de funciones.

Es deseable que las siguientes funciones dentro del departamento de sistemas estén separadas para lograr una división de funciones apropiadas:

- Análisis y Diseño de Sistemas.
- Programación.
- Operaciones.
- Función de Control.

El analista de sistemas diseña el sistema, el programador lo traduce a programas de computadora, el operador procesa los datos a través del sistema que usa los programas y las instrucciones de operación preparadas por el programador, y el grupo de control vigila el flujo de datos procesados por el departamento de sistemas. La segregación de estas funciones separa a aquellos individuos que tienen el mayor conocimiento del sistema (analistas de sistemas y programadores) de los que operan el equipo y manejan los datos reales. También suministra un control independiente (función de control) sobre el flujo de datos que entran al departamento de sistemas y salen de él. En compañías con instalaciones de Centro de Cómputo, no siempre es práctico lograr la segregación deseada de funciones dentro del departamento; en tales situaciones, los controles fuera de la actividad del Centro de Cómputo deben establecerse tomando esto en cuenta.

Al personal de diseño de sistemas y de programación debe prohibírsele operar la computadora para corridas regulares de procesamiento y a los operadores de la computadora debe negárseles acceso a la documentación de sistemas y programas.

Para asegurar que la segregación de funciones indicada antes es efectiva, es esencial que los individuos que intervienen en estas funciones tengan la prohibición de llevar a cabo las funciones de los otros. No debe permitirse al personal de sistemas y programación operar la computadora durante el procesamiento de información real puesto que su conocimiento íntimo de los programas de computadora puede proporcionarles la posibilidad de manipular la información.

Por las mismas razones, los operadores de la computadora no deben tener acceso a la documentación de los programas. Sin la documentación correspondiente sería muy difícil para los operadores alterar el procesamiento de los datos en forma significativa. Deben prepararse hojas de instrucción de operaciones especiales para cada programa e incluirse en el manual del operador para cada aplicación.

Los operadores asignados a rutinas específicas de procesamiento deben rotarse o alternarse periódicamente para evitar que se familiaricen demasiado con los programas y para permitir a la compañía tener más de un operador disponible para correr varias rutinas de procesamiento y así cubrir vacaciones y otros períodos de ausencia de los operadores.

4.1.2 OPERATIVA.

- Se han establecido controles para asegurar que las aplicaciones específicas estén convertidas a procesamiento de datos de una manera efectiva y eficiente y solamente después de que lo haya autorizado la gerencia.

- Han sido diseñados los sistemas y procedimientos de acuerdo con estándares apropiados, y que la documentación parece adecuada para proporcionar un entendimiento del sistema y de sus aplicaciones.

- Se han aprobado debidamente y sujetado a prueba los programas de la computadora y sus modificaciones antes de darlos efecto, y que la documentación parece adecuada para proporcionar un entendimiento de su lógica y de las rutinas de procesamiento.

Un sistema efectivo de control incluirá procedimientos y controles que principalmente se apliquen a la eficiencia de las operaciones y a la observancia de las políticas gerenciales. Frecuentemente son una parte importante del sistema global de control interno. Esta sección esboza aquellos procedimientos y controles que pudieran encontrarse en un Centro de Cómputo.

Diseño y Desarrollo de Sistemas.

El diseño y desarrollo de sistemas de procesamiento electrónico de información requieren los esfuerzos combinados del personal del departamento de sistemas y de otros departamentos de toda la organización. La manera en la cual la gerencia, los funcionarios contables, los departamentos usuarios, los diseñadores de sistemas y los programadores coordinan sus esfuerzos durante el diseño y desarrollo de nuevos sistemas y programas, tendrá un impacto importante en la efectividad y confiabilidad permanente del sistema y de los programas durante su operación posterior. La gerencia debe obtener la seguridad de que su inversión en el desarrollo de sistemas, en programación y en "hardware" están usándose para cumplir su cometido y que tanto los controles controlables sobre los activos como los registros son confiables. Hay que asegurarse de que:

- Las aplicaciones específicas se convierten a procesamiento electrónico de información sólo después de que se determine que ese curso de acción será una forma económica, efectiva y eficiente para manejar la aplicación.

- Los sistemas desarrollados son efectivos y representan lo realmente autorizado por la gerencia.

- Se mantienen adecuadamente los sistemas y programas y solamente se hacen cambios debidamente autorizados una vez que llegan a ser operantes.

Un sistema de procesamiento electrónico de información proporciona el enlace entre los datos de la fuente original y la información resumida o reportes para uso de la gerencia y de otras personas para operar el negocio. El diseño e implantación de un sistema o aplicación de procesamiento electrónico de información debe tener la aprobación y autorización por escrito de un nivel apropiado de la gerencia. Las modificaciones a los sistemas existentes generalmente deben ser autorizadas y aprobadas de manera similar. Si bien el grupo de sistemas y el personal interesado en la información de salida normalmente tomarán parte en el establecimiento de los procedimientos y controles que hayan de ser incorporados a una aplicación específica del Centro de Cómputo, el producto final debe ser revisado antes de la implantación por el deparatamento usuario, por el personal contable y, cuando sea apropiado, por los auditores internos para asegurarse de que la aplicación contiene procedimientos adecuados de control y un rastro para auditoría.

A medida que las aplicaciones de procesamiento electrónico de información lleguen a ser más complejas y refinadas, el auditor interno puede encontrar que es necesario revisar los procedimientos y controles en nuevas aplicaciones importantes antes de que sean puestas en práctica, para asegurarse que proporcionan controles adecuados y un rastro efectivo para auditoría. Frecuentemente no es práctico hacer cambios en sistemas complejos después de que estén en operación.

Programas de la Computadora.

Los programas y sus modificaciones deben ser autorizados y aprobados por personal adecuado de la gerencia. Deben revisarse y probarse antes de ponerlos en práctica para determinar si contienen controles adecuados.

Los procedimientos y controles que deben seguirse en el desarrollo y preparación de programas de computadora son similares a los que se requieren en el diseño y desarrollo de la aplicación del sistema del cual forma parte un programa.

Un programa de computadora es un juego de instrucciones que exponen los pasos detallados de procesamiento que la computadora debe seguir para procesar información de la manera descrita por el sistema. Los programas individuales generalmente son parte de un grupo de programas que pertenecen a una aplicación dada y tienen que ser compatibles uno con otro. Los programas nuevos, o las modificaciones a los mismos, hechos por programadores que no tienen un entendimiento de la aplicación global, o de la interacción detallada de los programas, pueden tener un efecto adverso sobre la información procesada a través del sistema.

Consecuentemente, todos los programas y los cambios a los mismos deben ser adecuadamente revisados, probados y aprobados por niveles apropiados de la gerencia. Frecuentemente es deseable que los auditores internos revisen las especificaciones del programa, la lógica y las subrutinas que afectan la información antes de darles efecto para determinar que se han incluído controles adecuados.

Los programas deben ser probados con información real y especial que represente condiciones verdaderas, incluyendo transacciones diseñadas específicamente para violar los procedimientos de control incorporados en el programa.

Cuando se incluyen varios programas en un sistema, deben ser probados en su secuencia real, así como independientemente.

Puesto que una computadora puede ejecutar solamente las funciones expuestas en el programa, este debe contener todos los pasos necesarios para tratar todas las posibles situaciones y condiciones que encontrará. Para lograr esto, es esencial que todos los programas incluídos en una aplicación de sistemas se sujeten a pruebas completas con información real, así como información de prueba especialmente construida que considere todas las posibles situaciones. Las pruebas finales deben incluir todos los programas en la aplicación del sistema en su secuencia normal para asegurar que se obtienen los resultados deseados, para asegurar la aceptabilidad de la información de salida de un programa como entrada al siguiente, y para asegurar que los archivos creados por el sistema para uso en ciclos posteriores serán aceptables como entrada en el siguiente ciclo.

Una característica significativa de todos los programas de computadora es la naturaleza y grado de los controles que pueden incorporarse en ellos para ser aplicados por la computadora a la información que recibe, o a los resultados de su procesamiento de la información, o ambas. Estos controles forman una parte integral del sistema global de control, y deben probarse para asegurar que operan y son efectivos.

Los programas deben comprobarse periódicamente en cuanto a exactitud de ejecución mediante el procesamiento de información de prueba.

Los controles incorporados al sistema deben comprobarse periódicamente para asegurar que son operantes y continúan realizando el trabajo para el cual fueron desarrollados. Son frecuentes las modificaciones a los programas y la forma y contenido de la información fuente varía de acuerdo con los negocios de la empresa. Como resultado de esto, los controles programados pueden llegar a ser inoperantes o anticuados y dejar de estimular la acción deseada cuando aparecen violaciones.

**Otras Consideraciones Generales.**

Deben utilizarse procedimientos de mantenimiento preventivo para reducir al mínimo las fallas del equipo.

El departamento de sistemas puede ser un "cuello de botella" alrededor del cual no puede darse un rodeo. La responsabilidad de establecer y llevar a cabo una política de mantenimiento preventivo es pesada y generalmente descansa sobre la gerencia del departamento de cómputo. El tiempo programado para mantenimiento del equipo no debe sacrificarse por conveniencia para ponerse al corriente en un atraso de procesamiento o por otras causas aparentemente justificables. El mantenimiento debe llevarse a cabo por individuos competentes que hayan tenido un buen adiestramiento para el trabajo y que estén familiarizados con el equipo al que se está dando servicio.

Para una operación confiable y satisfactoria de las computadoras generalmente se requiere que estén bajo condiciones determinadas de temperatura y humedad. Por lo tanto, la mayoría de los Centros de Cómputo operan bajo condiciones controladas mediante el uso de acondicionadores de aire y eliminadores de humedad.

Deben hacerse arreglos para equipo de respaldo en previsión de fallas del equipo.

Un medio de reducir el efecto de descomposturas prolongadas del equipo o de fallas de energía es tener disponible equipo de respaldo. Puesto que tener un equipo de reserva propio sería muy costoso, normalmente se establece algún arreglo con otros usuarios de computadora. Pueden usarse centros de procesamiento de los fabricantes para proporcionar servicio de respaldo o, lo que es más común, dos compañías pueden tener un arreglo recíproco mediante el cual el equipo de una puede ser usado por la otra como equipo de respaldo y viceversa.

Ningún arreglo de respaldo es completamente satisfactorio a menos que haya la seguridad de que los dos sistemas son verdaderamente compatibles. La única manera de asegurar la compatibilidad del equipo es procesar información de prueba en el equipo de respaldo en volumen suficiente y a través de un número suficiente de ciclos para cubrir todas las rutinas de procesamiento importantes. Una vez que se haya hecho esta prueba, debe repetirse siempre que se hagan modificaciones a la configuración del equipo de respaldo.

El control operacional comprende un plan de organización y todos los métodos y medidas coordinados dentro de un negocio para salvaguardar sus activos, comprobar la exactitud y confiabilidad de sus datos, promover la eficiencia operativa y alentar la observancia de las políticas gerenciales preescritas. Los controles operacionales generalmente se consideran relacionados principalmente con la salvaguarda de activos y con la confiabilidad de los registros.

Los controles operacionales en una organización de procesamiento electrónico de información podrían considerarse que incluyen aquellos controles cuyo propósito es asegurar que:

- Los datos de entrada son exactos y están debidamente aprobados para procesamiento.

- No hay pérdida de datos o falta de procesamiento de los mismos.

- Los programas de computadora están procesados en los archivos apropiados.

- El procesamiento logra el resultado deseado y se ejecuta sin error.

- La información de salida es distribuida en forma apropiada al personal autorizado.

Los controles operacionales deben ser evaluados por el auditor para identificar los puntos fuertes y débiles en el sistema global de control y para permitirle determinar el alcance del exámen que se requiere en una situación particular. Este proceso de evaluación requiere no solamente un conocimiento de los procedimientos y métodos preescritos, sino también seguridad mediante pruebas selectivas de que tales procedimientos están operando efectivamente.

Esta sección esboza varios factores que deben ser considerados por el auditor en su evaluación de los controles operacionales y de los procedimientos de procesamiento que pueden encontrarse en una instalación de Centro de Cómputo. También trata los controles usados para salvaguardar los registros de procesamiento electrónico de información y los rastros de auditoría.

## La Función de Control.

El departamento de sistemas normalmente actúa en calidad de departamento de servicio y tiene como responsabilidad primaria el procesamiento de datos para otros departamentos en la organización. Una función separada, comúnmente conocida como la función de control, debe establecerse para ver que toda la información se recibe, procesa y entrega por el departamento de sistemas. Esta función debe determinar que toda la información de entrada está debidamente autorizada, es exacta y completa y que oportunamente es enviada a, y despachada por, el departamento de sistemas. Esta función también debe:

- Controlar la acumulación y transmisión de la información de entrada al departamento de sistemas. Esto incluye el desarrollo de información de control (totales de batch) para cotejarla contra el procesamiento posterior.

- Controlar el flujo de datos que pasan a través del departamento.

- Conciliar los datos de control con la información desarrollda durante el procesamiento y con la salida.

- Controlar la distribución de la información de salida a personal autorizado.

- Controlar errores notados durante el procesamiento para asegurar que son reportados, corregidos y reprocesados.

Como se vió anteriormente es importante que las transacciones procesadas por el Centro de Cómputo se originen, aprueben y controlen por personal fuera del departamento de sistemas . En la práctica, la función de control usualmente se ejecuta por dos grupos. (Ver punto 3.3.1 Estudio de Factibilidad)

**Controles de Entrada.**

El controlar la confiabilidad de la información de salida procesada por el Centro de Cómputo comienza con la preparación de la información fuente que servirá como entrada para el sistema. Si bien la confiabilidad del equipo del Centro de Cómputo es generalmente buena, la confiabilidad de los datos de entrada solamente depende del cuidado ejercido por los responsables de su preparación y revisión.

Un sistema de cómputo bien diseñado debe incluír medidas para asegurar una entrada al sistema exacta y completa. El auditor debe tener conocimiento de las fuentes de errores y las técnicas que pueden emplearse para evitarlos y detectarlos. Pueden ocurrir errores porque la información de entrada esté:

- Registrada incorrectamente u omitida en el punto de iniciación.

- Indebidamente revisada y aprobada.

- Incorrectamente convertida a forma legible por la máquina.

- Pérdida durante su manejo.

- Incorrectamente procesada al ser leída por la computadora.

Se han desarrollado varias técnicas para controlar la confiabilidad de la información de entrada, y pueden establecerse controles en cualquier número de puntos en el sistema total de procesamiento de información. Puede también establecerse control sobre la entrada mediante revisiones apropiadas de la información de salida. Muchas de las técnicas usadas para controlar datos de entrada no serán aplicables en todas las situaciones o pueden no suministrarse al control deseado en una aplicación determinada. Cada situación deber ser evaluada en términos del riesgo y de la presencia de otros controles relacionados con ella.

Los procedimientos y técnicas que pueden utilizarse para asegurar una buena entrada son similares en muchos aspectos a los usados en sistemas manuales. Puede hacerse mucho para reducir la posibilidad de errores en el registro inicial de información, simplificando y estandarizando las formas, formulando instrucciones específicas, usando formas previamente codificadas, suministrando elementos visuales de registro mecánico (perforación por teclas) y prenumerando los documentos. También deben establecerse disposiciones para la revisión y aprobación de la información inmediatamente antes de su entrada al departamento de sistemas. Algunas de las técnicas más comúnmente usadas para controlar la información de entrada son:

- Controles de Batch - la mayor parte del procesamiento de información actualmente está controlada por técnicas de procesamiento en batch. Siempre que sea posible, deben establecerse totales de batch antes de que la información sea enviada al departamento de sistemas. Esto puede hacerse en el departamento que los origina.
  Estos totales de controles no necesitan restringirse a importes o cantidades, sino que pueden ser recuentos de transacciones o totales arbitrarios de números de código. La preparación de esta información de control suministra un control importante sobre las operaciones del departamento de sistemas. Los datos de control de batch debe conservarlos el departamento que establece los controles para comparación posterior con los batch equivalentes de control determinados durante el procesamiento por la computadora. Sin embargo, la práctica más generalizada es suministrar los totales del control en batch a un grupo de control en el departamento de sistemas, y ver que se haga una comparación de esos totales con los derivados del procesamiento de los datos por la computadora.

- Recuento de transacciones - otras variantes de la técnica de control en batch emplean recuentos de transacciones, partidas o documentos. Una técnica similar es usar los números primero y último de cada secuencia de números de documentos contenidos en batch como control de que entró en el sistema de cómputo el número correcto de documentos.

- Documentos que regresan - el uso de documentos que regresan, como formas previamente perforadas de remesas, para suministrar datos de entrada al departamento de sistemas, puede reducir considerablemente el riesgo de error en el registro y entrada de datos. Los documentos que regresan, los cuales contienen todos los datos necesarios, no requieren procesamiento intermedio en el que es probable que ocurran errores, pérdidas o alteraciones. Por lo tanto, los controles de batch de información de entrada usualmente se aplican a procesos en batch mucho mayores y frecuentemente se limitan a un total en importe o a un recuento de partidas.

La conversión de los datos de entrada a una forma legible por la máquina, cinta magnética, debe comprobarse por alguna combinación de procedimientos tales como verificación de claves, dígitos autoverificadores, totales de batch, etc.

La conversión de información fuente a una forma legible por la máquina puede hacerse en varias etapas y es sumamente importante que la conversión se haga apropiadamente para asegurar la exactitud del procesamiento posterior, así como la de la información de salida final.

Ningún sistema puede producir una salida confiable si los datos de entrada no están correctos. Al convertir los datos a forma legible por la máquina, la exactitud de la conversión puede probarse de varios modos.

Un procedimiento puede usarse para el registro en cinta magnética, en el cual un codificador de tecla a cinta magnética se usa para registrar los datos directamente en la cinta. Este dispositivo puede también usarse para verificar los datos.

La verificación es una operación duplicada y el grado en que deba usarse depende de la importancia de los datos que están siendo convertidos. En algunos casos se verifican solamente los datos críticos y en otros no se lleva a cabo verificación alguna.

Otro enfoque para comprobar la exactitud de los datos es el dígito autoverificador. Los números incorrectos tales como números de cuenta, números de productos, y números de empleados pueden detectarse con un alto grado de confiabilidad, haciendo ciertos cálculos matemáticos predeterminados con los dígitos en el número básico y comparando el dígito en la posición inferior del resultado con un dígito de comprobación incluído como un sufijo en el número de identificación. Esta comprobación normalmente se hace como una prueba programada durante las primeras etapas del procesamiento. El uso del programas de computadora para comparar la exactitud de los totales de los datos de entrada con algún total de control de batch prestablecido, es otro método común y efectivo para comprobar la exactitud de la conversión de los datos.

La información debe comprobarse después de que los datos de entrada han sido convertidos a forma legible por la máquina y conciliados con controles preestablecidos antes de comenzar el procesamiento.

Los totales de control en batch para datos de entrada, deben comprobarse mediante un paso del programa de la computadora tan pronto como sea posible después de que los datos se hayan convertido a la forma legible por la máquina, y antes de que se haga ningún procesamiento por la computadora. Si hay algo erróneo en los datos de entrada, es deseable encontrar esto tan pronto como sea posible y no después de que hayan sido usados en una corrida compleja de procesamiento. Los procedimientos correctos de control requieren que se comprueben los totales de control en cada punto conveniente durante el procesamiento por la computadora.

Deben establecerse controles sobre los datos leídos dentro de la computadora para probar su validez, corrección y secuencia.

Cuando se leen los datos dentro de la computadora, el programa puede utilizarse para comprobar las etiquetas de archivo y ver que se está usando el archivo apropiado para determinar que los campos de datos que están siendo leídos son válidos y para establecer y comprobar los procesamientos en batch. También para determinar que se están usando los archivos de transacciones o los archivos maestros apropiados y que se está procesando un archivo completo, registros especialmente codificados conocidos como etiquetas internas de archivo; estas se usan generalmente al principio y al final de los archivos para registrar identificación y controlar información. La etiqueta al principio del archivo se llama "registro de encabezado" y se usa para identificar el archivo, mientras que la etiqueta al final del archivo se llama "registro zaguero" e indica el recuento del bloque, los totales de control y el código del fin de archivo.

Una vez que la información ha sido leída por la computadora, puede sujetarse a ciertas rutinas de edición para suministrar alguna seguridad en cuanto a su validez. Algunas pruebas que pueden utilizarse dentro de la computadora para comprobar la validez de los datos a procesar se anotan a continuación. Estas rutinas de edición usualmente se practican en una corrida preliminar de procesamiento y las excepciones se reportan al departamento fuente o al grupo de control para investigación y corrección.

- Código válido - si hay un número limitado de códigos válidos, el código incluído en los datos de entrada se comprueba para ver que sea válido.

- Carácter válido - cuando solamente ciertos caracteres se usan en un campo de datos específicos, puede hacerse una prueba para ver que no se usan los caracteres no válidos.

- Tamaño, signo y composición válidos del campo - pueden hacerse pruebas para verificar que el número de dígitos en un campo determinado no excede el tamaño del campo, que el signo en un campo determinado es positivo o negativo como se especifica, y que solamente caracteres numéricos o alfabéticos se usan en un campo determinado.

- Transacción válida - generalmente hay un número limitado de transacciones que pueden ser procesadas con un archivo determinado y la computadora puede ser programada para comprobar la validez del código para las transacciones que hayan de ser procesadas.

- Combinación válida de campos - pueden probarse las combinaciones de datos cuando las combinaciones permisibles están claramente especificadas.

- Prueba de datos faltantes - puede hacerse una comprobación para determinar que todos los campos de datos necesarios para registrar una transacción contienen datos.

- Prueba de secuencia - los datos procesados en un sistema de procesamiento por batch tienen que ser arreglados en una secuencia específica que pueda ser fácilmente probada en la computadora.

- Prueba de límites o razonabilidad - los datos de entrada pueden compararse con límites predeterminados para asegurar que no han sido reportados montos en exceso de límite.

Los totales de control de entrada y los totales de corrida a corrida para cada aplicación deben comprobarse por alquien que no sea el operador del equipo.

Los totales de control se usan como un método básico para asegurar el manejo correcto y el descubrimiento de errores. Este método requiere que la cifra de control se desarrolle antes del procesamiento y que la corrida de procesamiento recalcule esta cantidad para que puedan compararse los dos totales. Para asegurar que tales cifras de control están comparadas apropiadamente, las comparaciones deben hacerse o verificarse por el grupo de control, el originador de los datos o el usuario de los datos. Esta función puede también manejarse internamente por la computadora. Esto es preferible en ciertos casos cuando la salida de una corrida se convierte en la entrada de otra corrida. Cuando la computadora se usa para esta función, los totales de control se leen dentro de la computadora como datos de entrada y la computadora se programa para acumular totales independientes de control y hacer comparaciones. Debe imprimirse un mensaje confirmando la comparación y mostrando los totales aún si éstos coinciden.

**Controles de Procesamiento.**

Deben usarse controles programados para detectar errores en programas defectuosos de computadora.

Los programas que hayan sido apropiadamente depurados y probados deben presentar pocos problemas. Sin embargo, con programas complejos, nuevos o modificados, existe la posibilidad de que haya errores latentes que puedan no ser descubiertos por algún tiempo después de que el programa haya estado en uso porque alguna condición determinada de procesamiento no puede ocurrir frecuentemente. Pueden incorporarse características de control en programas de computadora para descubrir ciertos tipos de errores que pueden permanecer sin detectarse durante la preparación, modificación y depuración del programa.

Tales controles pueden ser relativamente sencillos pero muy efectivos para descubrir errores en lógica, procesamiento incompleto y errores introducidos por cambios en el programa. Los controles programados también pueden detectar determinados tipos de errores del operador, tales como alimentación de archivos incorrectos de datos.

Varios tipos de controles programados que pueden usarse para probar el procesamiento de computadora se describen a continuación:

- Prueba de límites y razonabilidad - las instrucciones programadas que prueban la razonabilidad de los resultados del procesamiento comparándolos con límites determinados.

- Prueba de sumas horizontales - la información procesada por la computadora puede comprobarse de una manera similar a la prueba de sumas horizontales usada en un sistema manual. Las partidas individuales se totalizan independientemente por la computadora durante el procesamiento y se obtiene un total de sumas horizontales.

- Cifras de control - los montos obtenidos de la misma manera que los totales de control de entrada pueden usarse para probar los datos procesados por la computadora. Las cifras de control obtenidas durante el procesamiento deben estar, cuando son relevantes, en una forma en que puedan compararse con los totales de control de entrada relativos.

Los programas de computadora deben contener rutinas para comprobar las unidades de cinta y las unidades de almacenamiento de discos antes de procesar los datos.

Los operadores pueden introducir errores en el procesamiento, alimentando archivos o procesos en batch de transacciones incorrectos, o poniendo archivos de transacciones en una pieza equivocada del equipo. Los controles de programa normalmente están diseñados para reducir errores del operador mediante la inclusión de instrucciones en el programa, que hacen pruebas a efecto de que se utilice el equipo y se procesen los archivos apropiados.

Un operador de computadora debe siempre recibir instrucciones detalladas del programa, especificando el equipo que debe ser usado, archivo que debe ser alimentado, etc. Los mensajes de la consola pueden ser generados por el programa, que describa los pasos que deben ejecutarse por el operador durante la corrida del programa. El programa debe requerir verificación por vía de la consola en el sentido de que se han seguido las instrucciones.

Un programa de computadora debe suministrar información al final de cada fase mayor del procesamiento, que pueda ser usada para verificar que los datos procesados siguen de acuerdo con las cifras de control.

Los programas de computadora pueden ser bastante complejos y requerir un largo procesamiento. En tales casos los programas deben requerir una comparación periódica de los datos que están siendo procesados contra controles previamente establecidos, o contra totales en batch determinados al final de una etapa previa en el procesamiento. Si cualquier dato se omite inadvertidamente en algún paso en el procesamiento o se procesa mas de una vez, es esencial que el error en el procesamiento se descubra tan pronto como sea posible después de que ocurra. El costo de encontrar un error después de que los datos han sido procesados frecuentemente excede en valor al costo de incorporar comprobaciones periódicas de cifras de control en el programa que está siendo utilizado.

Los cambios en los archivos maestros pertinentes requieren controles especiales.

Los cambios en los archivos maestros que afectan cómputos clave tales como el cálculo de nóminas deben ser estrechamente controlados por el departamento que inicia los cambios. Debe suministrarse al departamento que los inicia un aviso o registro de todos los cambios procesados para verificar que tales cambios fueron hechos apropiadamente y para sujetar los cambios a su revisión. Los archivos maestros completos que contienen información financiera clave deben imprimirse regularmente para ser revisados y actualizados tanto por el departamento que los origina como por el que los usa.

Los controles sobre los cambios a esos archivos maestros que tienen significado para auditoría pueden requerir una revisión cuidadosa por parte del auditor.

Controles sobre Errores y Datos Rechazados.

Los controles de computadora deben prever la preparación de un registro de todas las transacciones incluídas en paros del programa e intervenciones del operador.
Debe mantenerse control sobre los datos rechazados o incorrectos para asegurar su procesamiento futuro.

Se escriben programas efectivos para que el procesamiento no se vea interrumpido por errores.

Un procedimiento de errores escrito dentro del programa puede proporcionar identificación y listado de ciertas clases de transacciones erróneas. Debe prepararse un reporte de rechazos o errores durante cada rutina de procesamiento y, cuando el error está en los datos originales, debe devolverse al departamento fuente para corrección y reposición. Actuar de otra manera sería eludir al control interno básico sobre el procesamiento de datos. La información rechazada o incorrecta debe ser controlada de manera que se apliquen los remedios apropiados, y los operadores de computadoras no deben tener facultad de iniciar correcciones.

Es importante dar cuenta apropiadamente de los datos rechazados y corregidos en sistemas de procesamiento por batch, de manera que los totales preestablecidos de batch puedan continuar usándose para controlar la entrada y la salida durante todo el procesamiento. La responsabilidad de obtener las correcciones necesarias y asegurar el reprocesamiento de los datos debe ser delegada al grupo de control.

Los controles sobre datos que son rechazados durante una corrida normal de procesamiento y los procedimientos usados para corregir errores, son una parte importante de los procedimientos de control y deben ser revisados cuidadosamente por el auditor.

Debe prepararse un registro de todos los errores anotando su naturaleza, frecuencia y efecto sobre la exactitud de la información de salida. Muchos errores son únicos y no pueden ser remediados por cambios de procedimientos o de personal. Sin embargo, los errores recurrentes pueden indicar deficiencias básicas en algún punto del sistema, tales como manejo inadecuado de la información de entrada en los departamentos fuente. Los errores recurrentes pueden indicar también un número poco satisfactorio de equivocaciones en el procesamiento por parte de un determinado operador de la computadora.

Sin importar el patrón mostrado por el análisis de errores, el significado general de todos los errores debe evaluarse periódicamente para determinar su efecto sobre la confiabilidad de la información de salida del sistema de procesamiento en conjunto, y deben hacerse esfuerzos prontamente para eliminar su causa. Las estadísticas de errores deben revisarse periódicamente por personas independientes del departamento de sistemas, tales como los auditores.

Deben establecerse procedimientos para manejar y controlar transacciones dispares.

Cuando se procesan datos que no pueden ser equiparados, la computadora no hará nada con los datos dispares a menos que el programa contenga instrucciones adecuadas para cubrir esta situación. Usualmente los programas contienen un paso que requiere el rechazo e impresión de un listado de datos dispares para su rastreo posterior por departamento, que suministró los datos fuente. La documentación del programa debe tener un directorio de las provisiones para errores que hayan sido incorporadas en un programa.

**Controles de Salida.**

Toda la información de salida debe ser entregada al grupo de control del departamento de sistemas para su revisión y comparación, con totales de control externos predeterminados siempre que esto sea posible.

Toda la información de salida debe ir directamente al grupo de control después de completar el procesamiento. Este grupo debe ser responsable de revisar la información en cuanto a que sea rezonable y esté completa y para comprobar cualesquiera de los totales de control que hayan sido establecidos previamente.

Para hacer esto efectivamente el grupo de control debe tener un conocimiento general del propósito fundamental de la rutina de procesamiento y debe saber lo que requieren los usuarios así como lo que posteriormente hacen con la información de salida.

Deben establecerse procedimientos adecuados para controlar la distribución de informes.

La distribución de la información de salida debe ser controlada para asegurar que solamente personal autorizado la reciba, puesto que muchos de los datos procesados por el departamento de sistemas pueden ser confidenciales. Para asegurar que la información se distribuye apropiadamente, el grupo de control del departamento de sistemas debe mantener un programa de todos los datos a procesar por el departamento, los informes resultantes, el número de copias que deben prepararse y su distribución.

La información procesada debe ser revisada por el usuario o por el departamento que controla los datos de entrada para determinar su razonabilidad.

Las personas que reciben la información de salida del departamento de sistemas son una parte integral del sistema de control y representan una fuente importante de descubrimiento de errores. Debe hacerse provisión para la retroalimentación de la información de errores proveniente de los usuarios de datos, quienes deben tomar la responsabilidad final de toda la información recibida del Centro de Cómputo. Esas personas deben satisfacerse de que la información está completa, exacta y en forma aceptable antes de usarla. Para lograr estos objetivos toda la información de salida debe ser revisada en cuanto a su razonabilidad por un empleado responsable dentro del departamento usuario, y esta revisión debe hacerse además de la revisión hecha por el grupo de control.

Todas las preguntas de personas de afuera respecto a lo exacto o apropiado de los datos procesados deben dirigirse a alguien independiente del departamento de sistemas para investigarlas, puesto que los errores detectados pueden ser indicios de manipulación deliberada de los datos procesados.

Un rastro para auditoría para un sistema de cómputo generalmente se refiere a los medios para identificar los pasos dados al procesar los datos que permiten seguir el rumbo de transacciones y datos de la fuente, a través del sistema de procesamiento hasta el total final de salida o tomar un total final y seguir el rumbo hacia atrás, hasta los datos originales de los cuales se derivó. El rumbo de la auditoría también suministra los medios por los cuales el auditor puede satisfacerse de que los datos han sido adecuadamente compilados y resumidos y si han sido procesados exactamente o no.

Como la computadora puede tener un impacto considerable sobre el rumbo de la auditoría, el auditor debe considerar cuidadosamente las siguientes características de cada aplicación de cómputo que tengan significado para la auditoría:

- Después de que los documentos fuente se transcriben en forma legible por la máquina, esos documentos ya no se usan en el ciclo de procesamiento y, por lo tanto, pueden archivarse de manera que dificulte su acceso posterior.
- En algunos sistemas los documentos fuente tradicionales pueden eliminarse por el uso de dispositivos de entrada indirecta.

- Los listados de transacciones o los detalles de los datos procesados pueden no ser preparados o retenidos durante un período adecuado.

- Pueden mantenerse archivos en medios de computadora sin listados detallados de los registros históricos.

- La secuencia de los registros y rutinas de procesamiento pueden ser difíciles de observar porque están contenidas dentro de la computadora.

Al diseñar un sistema de procesamiento de datos, deben observarse cuidadosamente ciertos principios para asegurar que el sistema suministrará rastros de auditoría apropiados. Deben existir:

- Medios para establecer la cuenta en la cual se asienta cualquier transacción.

- Medios para seguir el rumbo hacia atrás de totales resumidos a los elementos individuales de transacciones para todas las cuentas.

- Medidas para localizar información en los registros necesarios para contestar preguntas.

Deben mantenerse registros, documentación y rastros de auditoría adecuados para satisfacer las necesidades de la gerencia, del auditor y de las autoridades fiscales.

Una consideración importante en cualquier sistema de cómputo, es el problema de determinar cuánto tiempo debe guardarse cierta información. Deben considerarse las necesidades tanto operativas como legales.

La retención de registros es especialmente importante para el auditor puesto que necesita estar en posibilidad de examinar documentos fuente y ver que coincidan con los datos resumidos durante el curso de su exámen. Si los datos que tienen significado para la auditoría no están siendo conservados como política establecida, el auditor debe tomar medidas para ver que se retengan hasta que termine su trabajo.

Si bien, el advenimiento del procesamiento de datos ha traído cambios en la forma del rastreo de auditoría tradicionalmente encontrado por el auditor en los sistemas manuales, la sustancia del rastreo de auditoría ha sido conservada en la mayoría de los sistemas de cómputo principalmente por motivo de las necesidades de información para la gerencia.

4.1.3 DOCUMENTAL.

Los sistemas y procedimientos deben diseñarse de acuerdo con estándares apropiados.

Un departamento de sistemas bien manejado debe usar un manual de sistemas y procedimientos que prescriba procedimientos estándar apropiados a la naturaleza del trabajo. Un manual de sistemas y procedimientos debe cubrir cuando menos los siguientes tópicos:

- Procedimientos estándar para describir sistemas y especificaciones.

- Convenciones y procedimientos de programación estándar, incluyendo glosario, procedimientos de depuración y métodos de documentación para programación. La política de la compañía debe requerir que todos los programadores sigan las mismas convenciones.

- Procedimientos estándar de operación estableciendo las prácticas y procedimientos que deben seguirse al manejar el equipo del Centro de Cómputo, incluyendo especificaciones para la operación de la máquina, registros de utilización de la máquina, conservación de archivos, mantenimiento de registros y procedimientos de emergencia.

Todos los sistemas deben estar adecuadamente documentados para permitir el conocimiento completo del sistema en conjunto y de sus varias aplicaciones.

La documentación adecuada del diseño de sistemas, de los programas y de los procedimientos operativos es esencial para un entendimiento completo de las aplicaciones específicas del Centro de Cómputo y del impacto de tales aplicaciones sobre los departamentos usuarios. La documentación debe proporcionar:

- Un entendimiento claro de los objetivos e información de salida de una aplicación dada de sistemas, y evidencia de que la política de la compañía está siendo seguida.

- Una base para la revisión y evaluación de procedimientos y controles incluídos en una aplicación dada.

- Una referencia para los analistas de sistemas y programadores que son responsables de mantener el sistema y los programas después de que se han puesto en práctica.

La preparación de documentación adecuada puede requerir una cantidad considerable de tiempo y algunas veces es descuidada por analistas de sistemas y programadores.

Es importante que se prepare documentación adecuada en cada etapa del proceso de diseño y desarrollo si han de revisarse y aprobarse adecuadamente las aplicaciones de sistemas y los programas. Cuando se requiere una modificación posterior y la aplicación original de sistemas no ha sido debidamente documentada, la modificación puede tomar mucho tiempo y esfuerzo, puede ser necesario reconstruir la lógica de la aplicación original y los programas de respaldo. Esto es probable cuando los analistas y programadores que prepararon el material original ya no trabajan en la empresa o han sido asignados a otro trabajo.

Es importante que la documentación sea completa y consistente para todas las aplicaciones de sistemas en una compañía determinada, sin importar quién las haya preparado. En vista de la amplia gama de problemas que pueden surgir y de la variedad de equipo y lenguajes de programación que existen, normalmente no hay estándares universales de documentación. Sin embargo, el auditor puede esperar que se encuentre la siguiente documentación en la mayoría de los sistemas:

- Descripción narrativa del sistema, identificando los objetivos de aplicación, el volumen y tipo de datos procesados, frecuencia de procesamiento, información de salida del sistema y requisitos de tiempo o de horario.

- Uno o más niveles de diagramas de flujo del sistema, indicando la fuente y naturaleza de toda la información de entrada, operaciones de la computadora y manuales, y la naturaleza y distribución de toda la información de salida, en sus varios grados de detalle.

- Descripción del formato y contenido de los registros de entrada y salida, identificando los datos que hayan de ser procesados y el producto final resultante. Deben incluirse muestras de formas.

- Especificaciones detalladas para la preparación de programas de computadora necesarios para procesar la información en el sistema en particular. Deben usarse tablas de decisiones, pues éstas proporcionan una base sólida para documentar las especificaciones de los programas.

- Procedimientos de control de información y corrección de errores que especifiquen los controles por utilizar para determinar errores y los pasos requeridos para corregirlos.

- Aprobación escrita del sistema y de las modificaciones posteriores.

Los programas de computadora deben estar adecuadamente documentados para proporcionar un entendemiento de la lógica y rutinas necesarias para llevar a cabo su función.

La documentación adecuada de los programas de computadora es esencial para un entendimiento de las funciones de las rutinas específicas de procesamiento. Tal documentación sirve para los siguientes propósitos:

- Simplifica la modificación suministrando detalles que describen la lógica de los programas vigentes.

- Proporciona la información necesaria para contestar preguntas en cuanto a la operación del programa.

- Proporciona la base para mantener al corriente las instrucciones de operación.

- Sirve como base para evaluar los controles de procesamiento.

Un programa puede consistir en varios módulos o subrutinas, escritos por varios programadores. Las modificaciones a un programa pueden tener que hacerse por un programador que no escribió el programa original. Sería difícil para otro programador modificar un programa sin suficiente documentación que exponga los detalles necesarios para suministrar un entendimiento de la lógica y técnicas de programación que fueron usadas en la preparación del programa original. La documentación adecuada también proporciona los medios por los cuales la gerencia y otros interesados, tales como el auditor (con ayuda técnica cuando sea necesario), pueden revisar lo adecuado del programa y los controles que contiene. Si bien el grado de la documentación puede variar, las siguientes partidas serán siempre necesarias:

- Extracto del programa - descripción del propósito del programa.

- Diagrama de flujo del programa - un diagrama de los pasos de procesamiento y lógica del programa de computadora. Este debe respaldar el diagrama de flujo de sistemas que delinea el flujo de trabajo, documentos y operaciones de la aplicación de la cual forma parte el programa.

- Formato de los registros - diagrama que muestre el tamaño, posición y composición de las partidas de información que componen cada tipo de registro que es procesado.

- Narrativo del programa - descripción de los módulos clave de procesamiento, listando cada subrutina y función ejecutada. También deben describirse los controles de procesamiento y los procedimientos para manejar errores.

- Listado del programa - un listado detallado de la codificación contenida en el programa.

- Información de prueba - datos fuente usados para probar los cambios en el programa.

- Instrucciones al operador - información requerida por los operadores de la computadora para correr el programa.

- Registro de aprobaciones y cambios - documentación que respalda cambios en el programa.

La documentación del programa debe contener instrucciones explícitas para los operadores de la computadoras.

Aunque el operador de la computadora no debe tener acceso a la documentación completa del programa que está procesando debe suministrársele suficiente información para permitirle operar el equipo y correr los programas. Esta información debe permitirle al operador establecer y procesar cada operación y reaccionar apropiadamente respecto a errores en la información, paros en los programas o fallas en el equipo durante el procesamiento.

4.1.4 SEGURIDAD.

La presencia o ausencia de procedimientos y controles de seguridad claves pueden establecerse preliminarmente durante esta fase de la revisión. Para este propósito el auditor normalmente se cerciorará de que:

Han sido establecidos controles de procedimiento y procesamiento, los cuales aparentemente aseguran que:

- La información de entrada es exacta y está debidamente aprobada para procesamiento

- No hay pérdida o falta de procesamiento de información.

- Los programas de la computadora son procesados con los archivos apropiados.

- El procesamiento logra el resultado deseado y se ejecuta sin error.

- La información de salida se distribuye en forma apropiada al personal autorizado.

- Se han establecido políticas y procedimientos para salvaguardar apropiadamente los registros y archivos del Centro de Cómputo.

- No existen oportunidades para fraudes o errores importantes por parte del personal del Centro de Cómputo.

- La naturaleza y extensión del trabajo de los auditores internos en el área del Centro de Cómputo es razonable en relación con la importancia de la función.

Cuando la seguridad de la auditoría depende de la efectividad con la cual alguno de estos procedimientos y controles han funcionado durante el período que está siendo examinado, el auditor generalmente tendrá que llevar a cabo pruebas de procedimientos para respaldar lo que inicialmente ha encontrado. Muchos de los procedimientos y controles que afectan la operación del Centro de Cómputo estarán sujetos a pruebas durante otras fases de auditoría, y las conclusiones acerca de la efectividad de los controles sobre la entrada, procesamiento y salida de información pueden depender en gran medida, por la forma en que éstos están diseñados o por otras razones, de los resultados de esas pruebas.

- Controlar el acceso al Centro de Cómputo y evitar que personal no autorizado falsifique o inadvertidamente quite o destruya información crítica.

**Resguardo de Registros y Archivos.**

Los programas clave, documentación, registros y archivos de la computadora deben ser adecuadamente protegidos.

Los registros de la computadora, incluyendo los programas y los archivos maestros activos y de transacciones, son registros cuya seguridad y resguardo son de importancia considerable para la mayoría de las compañías. Su custodia requiere procedimientos de control completos y efectivos. Las principales medidas de protección física que pueden emplearse para tales registros pueden clasificarse como sigue:

- Controles Ambientales - Como las tarjetas, cintas y discos pueden ser afectados por la temperatura y la humedad, es deseable controlar la temperatura y humedad en áreas usadas para almacenarlos. También es importante recordar que las cintas magnéticas y los discos no deben almacenarse en áreas donde pueden ser desmagnetizados.

- Protección contra el Fuego - Las tarjetas, cintas y discos, son fácilmente destruídos por el fuego y deben almacenarse en estuches y guardarse en áreas de almacenamiento a prueba de fuego.

- Protección de Seguridad - Los registros y archivos del Centro de Cómputo deben estar controlados y almacenados en locales con cerradura. Las precauciones de seguridad deben ser especialmente estrictas para registros que pueden ser rápidamente duplicados o alterados.

- Almacenamiento fuera del Establecimiento - El almacenamiento de registros a prueba de fuego solamente puede garantizar la protección de los archivos por un período limitado puesto que un fuego intenso u otro siniestro como una inundación puede destruir los registros en almacenamiento "a prueba de fuego". Como resultado de esto, la mayoría de las compañías utilizan almacenamientos fuera del establecimiento para proporcionar una resguardo adicional para registros valiosos. Los archivos duplicados que deben conservarse para este propósito se comentan más adelante.

Los programas y los archivos de datos de la computadora deben mantenerse bajo el control de un bibliotecario y entregarse a los operadores según se requiera y se autorice.

Las grandes instalaciones generalmente tienen un bibliotecario responsable de llevar cuenta y razón de los programas de la computadora, archivos de datos y sus usos. También deben emplearse buenas prácticas de biblioteca en sistemas medianos o pequeños, aún en el caso de que ningún individuo determinado sea responsable de tal función. Esas prácticas protegen contra acceso no autorizado, pérdida o destrucción de archivos, suministran procedimientos útiles para conservar el orden y ayudan a la eficiencia operativa.

Los programas de computadora y los archivos de datos deben estar adecuadamente etiquetados para identificar claramente su contenido.

Deben usarse etiquetas externas e internas en los archivos para reducir al mínimo la posibilidad de procesar datos o archivos de programas incorrectos por el error del operador. Los archivos deben ser etiquetados externamente de manera consistente y con información suficiente para identificar exactamente su contenido. La etiqueta debe identificar claramente la fecha en que un archivo fue creado para que pueda mantenerse una sección apropiada de registros. Es importante que los archivos de cintas y de discos también contengan etiquetas internas. Como se explicó anteriormente, los programas de computadora normalmente contienen instrucciones que requieren que la computadora lea las etiquetas internas de los archivos antes del procesamiento y que las compare contra información preestablecida contenida en el programa o en el almacenamiento externo.

Debe existir un programa adecuado para la retención de archivos de respaldo y reconstrucción de archivos.

Una política que requiere la retención de archivos adecuados de respaldo es un ingrediente importante en cualquier sistema de Centros de Cómputo. La mejor protección contra la total destrucción de archivos y programas importantes es la creación de duplicados que sean almacenados en áreas que no fueran afectadas por algún siniestro en el departamento de Cómputo.

Cuando esto no es práctico, como sucede con muchos archivos, deben establecerse procedimientos que proporcionen los medios por los cuales archivos importantes de información pueden ser reconstruídos en caso de accidente u otro desastre.

Puesto que la retención y reconstrucción de archivos de información están afectados por las características de los medios involucrados, debe darse consideración a la relación entre los documentos fuente y los medios usados.

- Archivos en Tarjetas Perforadas - No es posible hacer una aseveración general respecto de la retención de archivos en tarjetas perforadas. La importancia de los archivos individuales en el sistema global dicta por cuánto tiempo deben retenerse los archivos. También debe darse consideración a la frecuencia en la preparación de listados. Los archivos originales en tarjetas, usualmente se retienen hasta que los ciclos de procesamiento en los cuales se incluyen sus contenidos, son procesados y los resultados comprobados. Periódicamente deben reproducirse copias de archivos importantes después de que sean actualizados, a cuyo tiempo el archivo anterior y su respaldo deben destruirse.

- Archivos en Cintas Magnéticas - El respaldo para archivos en cintas, normalmente se logra mediante el uso del principio "abuelo, padre, hijo" con la cual se mantienen tres generaciones de archivos en cintas. La cinta "abuelo" y los datos de entrada para las últimas dos generaciones pueden almacenarse fuera del Departamemto de Cómputo o fuera del establecimiento como respaldo.

- Archivos en discos - Los datos actualizados normalmente se describen sobre el disco en el mismo lugar anteriormente ocupado por datos previamente almacenados y, aunque pueden mantenerse archivos duplicados en discos, esto va en contra de la ventaja principal del procesamiento en discos. Las políticas de seguridad generalmente incluyen vaciar el contenido de un archivo en discos, en una cinta magnética o imprimir periódicamente listas y retener los datos de transacciones en forma legible por la máquina entre vaciados. En el caso de un archivo en discos grande, y un volumen masivo de transacciones vigentes, este procedimiento puede ser engorroso y consumir mucho tiempo; sin embargo, sin esta preocupación un simple accidente puede destruir irreparablemente datos vitales. Cuando sea práctico, un listado de los registros activos en el archivo inmediatamente después de que haya sido actualizado proporcionará un rastro efectivo para auditoría.

La compañía debe tener un seguro adecuado para cubrir el equipo, los programas y los archivos de información.

Un seguro es una parte integral de cualquier plan para resguardar los activos de la compañía incluyendo los archivos del Centro de Cómputo.

Los riesgos contra los cuales la compañía debe estar protegida provienen principalmente de fuego y otros siniestros naturales, de los vinculados con el procesamiento de información incluyendo el uso de una oficina de servicio y, si se ejecuta trabajo para otros, de la responsabilidad por errores u omisiones. Esos riesgos pueden cubrirse en varios grados por seguros, y la gerencia debe revisar periódicamente la cobertura para tener la seguridad de que es adecuada a las circuntancias.

## 4.2 DEFINICION DE OBJETIVOS.

El primer paso siempre consiste en establecer claramente los objetivos específicos de la auditoría. Esto no significa que los objetivos deban ser limitados o reducidos, sino que deben establecerse metas explícitas, tangibles, a fin de que tanto el auditor como sus superiores puedan determinar posteriormente si los objetivos fueron logrados.

## 4.3 RECOPILACION DE INFORMACION.

Teniendo sus objetivos y metas en mente, el segundo paso que debe seguir el auditor consiste en obtener un conocimiento general de las normas del sistema y del flujo de las transacciones: su propósito general, su magnitud, sus funciones y sus controles. Este conocimiento general no necesita tener gran relación directa respecto a los objetivos específicos, ya que solo es un esfuerzo para adquirir una comprensión general del sistema, a fin de que los pasos subsecuentes puedan concentrarse en forma efectiva a los objetivos específicos. La información reunida debe consistir en las políticas y posiblemente alguna de las guías de orientación más importantes.

La documentación para la recopilación de información básica es más bien simple: notas sobre entrevistas, cuestionarios generales, organigramas e información similar sobre la estructura general del sistema.

Una vez que se conocen las características generales del sistema en conjunto, el auditor prosigue a obtener un conocimiento más detallado. Este difiere del conocimiento general en que implica un mayor grado de detalle, y limita ese detalle a los aspectos del sistema que se refieren únicamente a los objetivos particulares del auditor.

En este paso, el auditor deberá reunir tanto las demás guías de orientación como las normas a nivel de instrucción que sean importantes. Esta información detallada también se documenta cuidadosamente en forma de cuestionarios detallados completos, notas adicionales, ejemplos de documentos, diagramas de flujo y diagramas detallados de otros tipos.

El enfoque primario son los cuestionarios, por lo que en cada área de auditoría se elaboran preguntas que nos proporcionarán la información deseada.

Los siguientes cuestionarios servirán como una base para los Centros de Cómputo, pudiendo agrandar o disminuir el número de preguntas según las necesidades y el tamaño de la instalación.

4.3.1 ADMINISTRATIVOS.

- Se puede obtener un organigrama del Centro de Cómputo, determinando puestos, descripción de trabajo y nombre de las personas ?.

- Hay un plan escrito para cambios futuros a realizarse en el Centro de Cómputo ?.

- Es aprobada cada aplicación, respaldada por un estudio de costo-beneficio ?.

- Está apoyado en un estudio de costo-beneficio la aprobación de cada cambio que se piensa hacer ?.

- Hay una tabla de implementación, mostrando el progeso real contra el planeado ?.

- En lo referente a costos, se lleva el total presupuestado por :
  - . año fiscal actual
  - . año fiscal siguiente ?.

- En lo referente a costos actuales para el año fiscal recientemente terminado se toman en cuenta costos de :
  - . renta del CPU
  - . renta de otro equipo
  - . costo de equipo comprado
  - . mantenimiento de hardware
  - . sueldo de gerentes
  - . sueldos de capturistas
  - . sueldo de operadores
  - . sueldo de diseñadores
  - . sueldo de programadores
  - . sueldo de analistas
  - . sueldo de personal administrativo
  - . insumos
  - . contratos de conversión de datos
  - . contratos de servicios
  - . utilerías
  - . otros ?.

- El personal conoce de las metas de la compañía ?.

- Se tienen planes de crecimiento a corto, mediano y largo plazo ?.

- Se cuenta en los planes de crecimiento con estrategias, proyectos de sistemas y recursos necesarios ?.

- Se revisan periódicamente los planes de crecimiento, para su actualización ?.

- Los objetivos planteados y los resultados a ser alcanzados son adecuados y corresponden realmente a lo que se ejecuta ?.

- Existe una calendarización adecuada que contribuya eficaz y eficientemente a los objetivos establecidos por el Centro de Cómputo ?.

- Se encuentran vigentes los procedimientos establecidos para el funcionamiento del Centro de Cómputo ?.

- Es congruente la capacidad del equipo de cómputo con los planes de desarrollo del Centro de Cómputo ?.

- Hay un estudio de factibilidad, que permite tomar decisiones sobre la posibilidad y conveniencia de modificar parcial o totalmente los procedimientos actuales del Centro de Cómputo, de tal manera que los cambios resultantes lleven a la solución de los problemas detectados ?.

- En el estudio de requerimientos de equipo, tanto a largo como a corto plazo, se considera la evaluación de la computadora, tomando en cuenta la conveniencia de comprar, rentar, rentar con opción a comprar, o cualquier otra alternativa que justifique la adquisición del equipo ?.

- Se cuenta con documentos que muestran las ventajas, desventajas y costos de las soluciones, así como de la razón por la que se rechazó la selección de algún equipo ?.

- Qué tan útil ha sido el estudio de factibilidad que se realizó del Centro de Cómputo ?.

- Existen perspectivas de desarrollo del personal ?.

- Existe un programa de rotación de puestos ?.

- Existen sustitutos para apoyar un puesto clave en caso de ausencia ?.

- Está negado el acceso a la biblioteca de programas y su documentación ?.

- El personal es investigado antes de contratarse ?.

- Está el personal asegurado por alguna compañía ?.

- Existen revisiones de personal ?.

- Existe un programa de capacitación y entrenamiento formal para el personal ?.

- Como se estima el rendimiento del personal que trabaja en el Centro de Cómputo ?.

- Funcionan las técnicas de selección y reclutamiento del personal del Centro de Cómputo ?.

- Hay una segregración de tareas tales como :
  - las funciones y tareas del diseño de sistemas y de la programación, están separadas de las operaciones de la computadora
  - los programadores no operan la computadora para corridas regulares de procesamiento
  - los operadores de la computadora están restringidos en el acceso a la información de datos y programas no necesarios para realizar sus tareas asignadas
  - los empleados en el procesamiento de datos están separados de todas las tareas relacionadas a la iniciación de transacciones y a la iniciación de solicitudes para cambios a los archivos maestros ?.

- Están los operadores asignados a corridas de aplicaciones indiviaduales rotándose periodicamente ?.

- Se comparan y verifican el número de personas en cada puesto contra los autorizados ?.

- Es el departamento de sistemas, independiente de otras operaciones funcionales ?.

- Son las siguientes funciones, realizadas por individuos diferentes :
  - diseño de sistemas
  - programación
  - aceptación de pruebas
  - autorización a cambios de programas
  - aceptación de programas
  - manejo de datos fuente
  - operación de la máquina
  - mantenimiento de archivos ?.

- Existen personas y procedimientos sobre el control de recursos humanos, materiales y financieros ?.

- Los presupuestos son vigilados para su adecuado uso ?.

- Se tienen identificados los requerimientos de recursos humanos, materiales y financieros para cada proyecto del Centro de Cómputo ?.

4.3.2 OPERACIONAL.

- Existen normas que definen el contenido de los instructivos de capturación de datos ?.

- La orden de trabajo que se recibe en el área de capturación de datos contiene :

. número de folio
. formato
. fecha y hora de recepción
. nombre del documento
. departamento
. nombre del usuario
. nombre del responsable
. número de registros a capturar
. identificación del capturista
. password para capturar
. fecha y hora de entrega ?.

- Cuales de éstos controles se realizan en el área de capturación de datos :

. recepción de trabajos
. revisión del documento fuente
. prioridades de capturación
. relación de errores en la capturación
. relación de avance en los trabajos
. producción de cada capturista
. verificación de cifras de control de entrada con las salidas
. costo mensual por trabajo
. relación de trabajos atrasados
. entraga de trabajos ?.

- Cada cuando se elabora el programa de trabajo para cada turno en el área de capturación de datos ?.

- El programa de trabajo es congruente con el calendario de producción ?.

- Si el trabajo diario es mayor que el programado en capturación, se investigan sus causas ?.

- Quién y como se controla la entrada de documentos fuente ?.

- Las correcciones en los datos fuente son revisados y aprobados por personas que no pertenecen al área de sistemas ?.

- Los registros erróneos que fueron rechazados son escritos en un archivo para su revisión ?.

- Se usan los controles totales run-to-run para revisar que se haya completado el proceso ?.

- Hay controles adecuados sobre los procesos de identificación, corrección y reprocesamiento de datos rechazados por los programas?.

- Se llevan controles totales de conteo y predeterminación para controlar las transacciones rechazadas ?.

- Los registros que se llevan de la utilización del equipo de cómputo son:

- tiempo de uso del procesador central
- tiempo dedicado a compilaciones
- tiempo dedicado a pruebas
- tiempo dedicado a producción
- tiempo dedicado a operacioñn de la computadora
- tiempo dedicado a mantenimiento del sistema operativo
- tiempo dedicado a mantenimiento preventivo
- tiempo dedicado a mantenimiento correctivo
- tiempo de falla de los dispositivos de almacenamiento
- tiempo de falla de los dispositivos de entrada y salida
- tiempo de uso de los dispositivos de almacenamiento
- tiempo dedicado a reprocesamiento
- tiempo ocioso
- tiempo de fallas en el aire acondicionado, suministro de energía, etc. ?.

- Con que periodicidad se registran estos datos :
  - tiempo promedio de operación
  - promedio de compilaciones
  - promedio de programas ejecutados
  - promedio de trabajos en cola de espera de ejecución en horas pico
  - promedio de trabajos en cola de espera de dispositivos de entrada y salida en horas pico ?.

- Qué porcentajes de tiempo por turno de operación se dedica a :
  - compilación
  - pruebas
  - producción
  - ocio ?.

- La relación de uso de dispositivos de entrada y salida, con respecto al trabajo es suficiente ?.

- Si es insuficiente el trabajo de los dispositivos de entrada y salida, investigar si es conveniente:
  - incrementar el número de dispositivos
  - reestructurar las cargas de trabajo ?.

- Qué porcentaje de los programadores se dedican a dar mantenimiento a los sistemas ?.

- Que lenguajes conocen los analistas y programadores ?.

- Los analistas son también programadores ?.

- Que pasos siguen los programadores para el desarrollo de sistemas ?.

- Se utilizan los estándares establecidos para programación ?.

- Se encuentran en un manual esos estándares ?.

- Se lleva registro de la elaboración de programas por :
  - . programador
  - . programa
  - . sistema
  - . área
  - . otros ?.

- Los sistemas se están ejecutando correctamente y en forma eficiente ?.

- Los sistemas son:
  - . dinámicos
  - . estructurados
  - . integrados
  - . accesibles
  - . necesarios
  - . comprensibles
  - . oportunos
  - . funcionales
  - . estándares
  - . modulares
  - . jerárquicos
  - . únicos
  - . seguros ?.

- Se llevan a cabo revisiones periódicas de los sistemas para determinar si aún cumplen con los objetivos par los cuales fueron diseñados tanto de análisis como de programación y que acciones correctivas se toman en caso de desviaciones ?.

- Al diseñar un sistema quienes intervienen:
  - . usuarios
  - . analistas
  - . programadores
  - . operadores
  - . gerentes
  - . asesores
  - . auditores
  - . otros ?.

- La documentación que acompaña al sistema cuando se entrega contiene :
  - . descripción narrada
  - . nombre y número de identificación
  - . lógica del programa
  - . listados del programa
  - . fecha de aprobación
  - . formatos
  - . diagramas de flujo
  - . diccionario de datos ?.

- Cuales puntos se toman en cuenta para la prueba de un sistema :
  . pruebas particulares de cada programa
  . prueba por fase
  . prueba con un programa paralelo
  . otros ?.

- Existe una relación de proyectos de sistema y fechas programadas de implantación ?.

- La relación de proyectos de sistemas prevee la atención de solicitudes urgentes ?.

- La relación de proyectos de sistemas prevee un porcentaje del tiempo total de producción para reproceso o fallas de equipo ?.

- Se tiene una lista de proyectos a largo y corto plazo ?.

- Quién autoriza los proyectos ?.

- Quién interviene en la planeación de proyectos ?.

- Como se calcula el presupuesto del proyecto ?.

- Quién y como se asignan las prioridades en los proyectos ?.

- Quién controla el avance de los proyectos ?.

- Con que periodicidad se revisa el reporte de avance de proyectos ?.

- Cada cuando se estiman los costos del proyecto para compararlo con lo presupuestado ?.

- Se tienen copias de los archivos fuera, de las instalaciones del Centro de Cómputo ?.

- Con que periodicidad se realizan los respaldos ?.

- Con que frecuencia se verifica la validez de los inventarios ?.

- Se tienen procedimientos que permitan la reconstrucción de un archivo en cinta o disco, el cual fué destruido ?.

- Qué procedimiento se sigue en el remplazo de dispositivos de almacenamiento que contienen los archivos maestros :
  . se conserva la maestra anterior hasta después de la verificación de la nueva cinta
  . se utiliza la política de conservación hijo-padre-abuelo
  . otras ?

- Se depuran los medios de almacenamiento con información obsoleta ?.

- Dentro del programa de trabajo de la máquina, se tienen previstas:
  - demandas inesperadas
  - fallas de la máquina
  - respaldos generales
  - mantenimiento preventivo ?.

- Que tan frecuentemente se asigna la computadora en su totalidad, para una sola aplicación ?.

- Que elementos se utilizan para programar la carga de trabajo de la computadora ?.

- Se lleva a cabo un programa de mantenimiento preventivo para cada dispositivo de cómputo ?.

- Si los tiempos de reparación son superiores a los estipulados en el contrato, que acciones correctivas se toman ?.

- Se mantinen registros actualizados de las fallas de los dispositivos del equipo de cómputo ?.

- Se mantinen registros actualizados de las fallas de servicios en el Centro de Cómputo como aire acondicionado, sistema de energía, detectores de humo, etc. ?.

- Es posible identificar, los problemas más recurrentes o fallas mayores que afecten en forma determinante el funcionamiento del Centro de Cómputo ?.

- Tiempo de respuesta que se ha tenido del contrato de mantenimiento ?.

- Calidad de los ingenieros de servicio para mantener el equipo funcionando ?.

- Tiempo promedio que toma investigar y resolver el problema ?.

- Disponibilidad de refacciones necesarias para dar mantenimiento al equipo ?.

- Existen procedimientos formales para la operación de los sistemas de cómputo ?.

- Esos procedimientos describen detalladamente tanto la organización de la sala de máquinas así como su operación ?.

- Los instructivos de operación para cada aplicación contienen :
  - identificación del sistema
  - identificación del programa
  - periodicidad y duración de la corrida
  - etiquetas de archivos de salida
  - nombres de archivos lógicos
  - fechas de creación y expiración

- instructivos sobre materiales de entrada y salida
- detenciones programadas y acciones requeridas
- instructivos específicos a los operadores en caso de falla del equipo
- puntos de reinicio, procedimientos de recuperación para procesos de gran duración o criterios
- identificación y especificación de todos los dispositivos de la máquina a ser usados
- especificaciones de resultados ( cifras de control, registros de salida por archivo ) ?.

- Hay una justificación de los procesos en la computadora ?.

- Como programan los operadores los trabajos dentro de la sala de máquinas ?.

- Se respetan las prioridades de trabajo ?.

- Se analiza la efectividad con que se ejecutan los trabajos dentro de la sala de máquinas, tomando en cuenta equipo y operador através de inspección ?.

- Se rota a los operadores procurando un entrenamiento para evitar la manipulación fraudulenta de los datos ?.

- Cuentan los operadores con una bitácora para mantener los registros de cualquier evento y acción tomada por ellos ?.

- Como está organizado el archivo de bitácoras :
  - por fecha y hora
  - por turno de operación ?.

- Existen procedimientos para evitar ejecuciones de programas no autorizados ?.

- Se permite a los operadores el acceso a la información referente a los programas fuente fuera de la sala de máquinas ?.

- Existen procedimientos formales que se deban observar antes de que sean aceptados en operación, sistemas nuevos o modificaciones ?.

- Quién dá la aprobación formal cuando las corridas de prueba, de un sistema modificado o nuevo, están acordes a los instructivos de operación ?.

- Se catalogan los programas para producción rutinaria ?.

- Como considera el usuario el servicio del departamento de sistemas ?.

- Como consideran los usuarios, la calidad del procesamiento que se le proporciona ?.

- Hay disponibilidad de procesamiento para los requerimientos de los usuarios ?.

- Los costos de servicios de cómputo son conocidos por los usuarios ?.

- Que piensan los usuarios acerca de la seguridad en el manejo de su información ?.

4.3.3 DOCUMENTACION.

- Se preparó la documentación de acuerdo a los estándares predeterminados ?.

- Se utilizan los estándares que se establecieron para el Centro de Cómputo ?.

- Están los estándares disponibles en un manual ?.

- Se publican y ponen en práctica los estándares de documentación para programación, operación y capturación ?.

- Los responsables de la elaboración de la documentación son :
  - diseño de sistemas
  - programación
  - procedimientos de operación
  - biblioteca
  - capturación
  - usuario ?.

- La documentación para la preparación de instructivos para las personas que se responsabilizan de los datos de entrada y salida es adecuada ?.

- La documentación para cada archivo especiffca :
  - nombre y número de archivo
  - autorización para su creación
  - ciclo de actualización
  - ciclo o fecha de retención
  - tamaño de archivos y bloques
  - cuando se deben copiar los archivos para fines de respaldo
  - como se deben reponer los archivos en caso de que se dañen o destruyan
  - como serán almacenados los archivos fuera de las instalaciones ?.

- Se preparan instrucciones precisas para la protección de los archivos que comprendan los siguientes conceptos :
  - condiciones del medio ambiente necesarios para el área de almacenamiento
  - protección contra incendios requerida en el área de almacenamiento
  - ubicación y utilización de las áreas de almacenamiento fuera de la instalación
  - requisitos de etiquetado de archivos en dispositivos de almacenamiento, procedimientos para numeración seriada
  - como y cuando registrar datos históricos en archivos en dispositivos de almacenamiento en los registros históricos
  - procedimientos para el mantenimiento y la limpieza de los dispositivos de almacenamiento ?.

- La documentación de los sistemas incluye descripciones de las funciones de control, de los procedimientos y de las responsabilidades tales como :
  - registro inicial de datos
  - transmisión de datos
  - conversión de datos
  - procesamiento de datos
  - control, corrección y realimentación de errores
  - conciliación de las salidas contra las entradas
  - distribución de las salidas ?.

- Se preparan todos los documentos y registros necesarios para la comprensión completa de cada programa del sistema ?.

- La documentación del programa comprende :
  - nombre del programa
  - índice
  - especificaciones del programa
  - descripción del programa en forma narrativa
  - diagrama de lógica y/o tablas de decisión
  - constantes, códigos y tablas
  - formatos de entrada y salida
  - formatos y descripciones de los archivos
  - listado del programa fuente
  - instrucciones de operación ?.

- Se prepara la documentación del sistema para cada aplicación con el siguiente contenido :
  - nombre
  - índice
  - definición y descripción general del problema
  - descripción general del sistema
  - gráfica general de los sistemas, mostrando el flujo de la información através del sistema

- tratamiento especial en caso de excepciones
- listado de los programas que componen el sistema
- especificaciones de programas
- descripción de los documentos fuente
- constantes, códigos y tablas
- descripción de formatos de entrada y salida
- procedimientos de control de archivos
- especificaciones de los datos de prueba
- programas y procedimientos de conversión
- instrucciones al usuario
- pistas para auditoría ?.

- Se elaboran instrucciones acerca de la conversión de datos por cada uno de los sistemas, y se hacen del conocimiento de las personas encargadas de estas operaciones. Estas instrucciones contienen :
  - en los documentos fuente, se establecen cuáles son los datos que se deben de incluir y en que secuencia
  - se establece el formato de los datos de entrada, cualquier código especial que deba emplearse, el uso del llenado de ceros a la izquierda en registros fijos, la utilización de símbolos para fin de campo y fin de registro, forma de registrar las cantidades negativas, especificaciones de campos solo numéricos, solo alfabéticos o mixtos, datos alfanuméricos o caracteres especiales, etc.
  - indican el método y formato para registrar datos de control ?.

- Se elaboran instrucciones sobre control de los datos por cada sistema, haciéndolas del conocimiento de las personas encargadas del control de datos, y comprenden :
  - origen y descripción de los datos de entrada
  - muestra de las salidas
  - conciliación y/o verificación de las salidas contra las cifras de control
  - condiciones de error previstas y acción a tomarse al respecto
  - disposición de salidas ?.

- La documentación para la operación de cada programa comprende :
  - número y nombre del programa
  - breve descripción de la finalidad del programa
  - esquema de la operación, mostrando las entradas y su secuencia; archivos, salidas y la asignación de dispositivos de entrada y salida
  - descripción de formatos de entrada y salida
  - instrucciones especiales de operación relativas a la preparación de la operación de

la computadora y los procedimientos finales de operación
. listado de las detenciones programadas y los mensajes en caso de haberlos y la acción correctiva correspondiente, para proseguir el proceso
. procedimientos de recuperación y reinicio a seguir, al encontrarse con una falla del equipo
. instrucciones de terminación de trabajo, que gufen al operador acerca del etiquetado y disposición de las entradas, archivos de salida y reportes, procedimientos de verificación de procesos
. estimación de tiempo normal del procesamiento y límite máximo de tiempo de proceso ?.

- Acerca de sus responsabilidades en general y las acciones que deben emprender bajo circunstancias especiales, los operadores de la computadora, cuentan con instrucciones detalladas, tales como :
  . condiciones adecuadas de la temperatura, humedad, limpieza del aire y que hacer en caso de que no pudieran mantenerse estas condiciones
  . las instrucciones que indican, qué personas pueden tener acceso a la sala de cómputo y a que programas
  . que hacer en casos de emergencia tales como incendio, inundación, fallas de energía eléctrica, actos de guerra, desórdenes civiles o desastres naturales
  . el registro de los tiempos de procesamiento en la bitácora de operación
  . el mantenimiento del equipo indicando la política general acerca del mantenimiento preventivo y los procedimientos que deben seguirse en casos de falla del equipo
  . el mantenimiento y limpieza de los dispositivos de almacenamiento
  . etiquetas externas de los dispositivos de almacenamiento
  . los procedimientos para la manipulación de dispositivos de almacenamiento, como la utilización de anillos para el sellado de cintas ?.

- Se elaboran instrucciones para asegurarse que los usuarios conozcan :
  . que datos deben enviarse para el procesamiento en la computadora
  . que controles se establecen sobre los datos
  . códigos especiales a usar
  . procedimientos de depuración a seguir
  . reportes e información que deben recibir

. que pasos deben seguir para realizar la verificación de los reportes o informacion ?.

- Hay una supervisión en la documentación para asegurar que es adecuada ?.

- Está la documentación actualizada hasta la fecha ?.

4.3.4 SEGURIDAD.

- Como está dividida la responsabilidad de la seguridad ?.

- El personal de vigilancia en la organización se contrata :
  . directamente
  . por medio de empresas que venden ese servicio ?.

- Se investiga a los vigilantes antes de contratarlos ?.

- Se controla el trabajo en el Centro de Cómputo fuera de horario ?.

- Se registran las acciones de los operadores para evitar que realicen algo que pueda ser perjudicial para el Centro de Cómputo ?.

- Se ha instruído a estas personas sobre que medidas tomar en caso de que una persona pretenda entrar sin autorización ?.

- Se vigila la moral y el comportamiento personal, con el fin de evitar un posible fraude ?.

- Se tienen documentados los procedimientos para actuar en caso de desastre ?.

- Los procedimientos para los casos de desastre son practicados continuamente ?.

- Hay vigilancia las 24 horas en la sala de máquinas ?.

- A la entrada de la sala de máquinas existe :
  . vigilante
  . recepcionista
  . tarjeta de control de acceso
  . nadie ?.

- El edificio donde se encuentra la sala de máquinas está situado a salvo de :
  . inundación
  . terremoto
  . fuego
  . sabotaje ?

- Los vidrios de la sala de máquinas, pueden ser rotos con facilidad ?.

- Qué control existe para el personal del Centro de Cómputo en el acceso a la sala de máquinas :
  - . cerraduras de combinación
  - . identificación personal
  - . tarjeta magnética
  - . circuito cerrado de televisión
  - . otros ?.

- Son cambiados con periodicidad estos medios ?.

- De que manera son controladas las visitas y demostraciones en la sala de máquinas ?.

- Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior de la sala de máquinas para evitar daños y accidentes ?.

- Es retirado con frecuencia el polvo acumulado en el techo y piso falsos de la sala de máquinas ?.

- Se controla el acceso y préstamos en :
  - . cintoteca
  - . discoteca
  - . programoteca ?.

- Se verifica identificación para el uso de la computadora ?.

- Están separadas de la sala de cómputo, el área de almacenamiento de dispositivos de almacenamiento ?.

- Se han tomado medidas para minimizar la posibilidad de fuego :
  - . evitando artículos inflamables en la sala de máquinas
  - . prohibiendo fumar
  - . vigilando y manteniendo el sistema eléctrico en excelentes condiciones ?.

- Existen alarmas para detectar :
  - . fuego
  - . humo
  - . agua
  - . magnetos
  - . otros ?

- Se encuentran colocadas en posiciones estratégicas éstas alarmas ?.

- Con que periodicidad se da mantenimiento a todas las alarmas ?.

- Se ha adiestrado al personal para utilizar los extintores ?.

- Con que periodicidad se les da mantenimiento a los extintores ya sean automáticos o manuales ?.

- Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos ?.

- Están estrategicamente colocadas las puertas de emergencia ?.

- Se cierran las tomas de aire acondicionado en caso de detección de fuego ?.

- Están en perfecto estado el sistema de respaldo ininterrumpido ?.

- Se ha establecido que información puede ser accesada y por que persona ?

- Existen claves, passwords, autorizaciones para prevenir cambios no autorizados en los archivos ?.

- Se registra cada violación a los sistemas, con el fin de llevar estadísticas y frenar los posibles fraudes ?.

- Para la protección de los archivos, se tienen cuenta :
  - . condiciones del medio ambiente necesarioas para el área de almacenamiento
  - . protección contra incendio requerida en el área de almacenamiento
  - . ubicación y utilización de las áreas de almacenamiento fuera de la instalación
  - . requisitos de etiquetado de archivos en dispositivos de almacenamiento, procedimientos para numeración seriada
  - . como y cuando registrar datos históricos en archivos en dispositivos de almacenamiento en los registros históricos
  - . procedimientos para el mantenimiento y la limpieza de los dispositivos de almacenamiento ?.

- Se tienen copias de los archivos fuera, de las instalaciones del Centro de Cómputo ?.

- Qué seguridad y confidencialidad se tiene en ese local para los datos ?.

- Con que periodicidad se realizan los respaldos ?.

- El inventario de la programoteca, cintoteca y discoteca contiene:
  - . localización
  - . número de serie
  - . nombre y clave de usuario
  - . confidencialidad
  - . nombre del sistema que lo genera
  - . fecha de generación

. fecha de expiración
. otros ?.

- Con que frecuencia se verifica la validez de los inventarios ?.

- Se registran en el inventario, los medios de almacenamiento nuevos que se reciben ?.

- Se tienen procedimientos que permitan la reconstrucción de un archivo en cinta o disco, el cual fué destruido ?.

- Se tiene un responsable por turno de la programoteca, cintoteca y discoteca ?.

- Qué medida se toma en el caso de extravío de un medio de almacenamiento ?.

- Se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento al personal ?.

- En caso de préstamo de algún dispositivo de almacenamiento, con que información se cuenta :
  . fecha de préstamo
  . fecha en que se debe regresar
  . archivos que contiene
  . formatos
  . cifras de control
  . código de grabación
  . otros ?

- Existe una localidad con las facilidades necesarias para recurrir a ellas en caso de tener problemas con disposición de sistema de energía, aire acondicionado, piso y techo adecuados, etc. ?.

- El Centro de Cómputo a que otras instituciones les da respaldo ?.

- Qué otras instituciones proporcionan respaldo al Centro de Cómputo ?.

- Bajo que condiciones se otorga respaldo o servicio ?.

- Tiene seguro de cobertura amplia el Centro de Cómputo ?.

- Se tienen identificados los costos en caso de pérdidas ?.

## 4.4 EVALUACION DE LOS CONTROLES.

Una vez que el auditor ha entendido ampliamente el sistema, debe identificar y evaluar los controles. Esto implica, primero, la distinción entre las actividades que están sujetas a control y aquellas que proporcionan control. Una vez hecha esta diferenciación, el auditor: (1) identifica aquellos controles cuya ausencia permitirfa riesgos importantes y (2) determina los riesgos que existen en base al sistema pero que podrían eliminarse añadiendo controles adicionales. Los riesgos se limitarán a aquellos que se relacionan con sus objetivos.

Con frecuencia, este proceso de evaluación se realiza informal e intuitivamente. Existe alguna evidencia con respecto, a que, en circunstancias idénticas, aún los auditores experimentados harán evaluaciones distintas de los controles y riesgos. La evaluación mejorará sustancialmente si este paso se convierte en un proceso formal.

La documentación de esta evaluación deberá consistir en un listado de las características y deficiencias importantes del control, con una estimación global de los riesgos para el negocio.

## 4.5 DISEÑAR Y EFECTUAR PRUEBAS Y PROCEDIMIENTOS.

Durante los años en donde las computadoras se utilizaron primero en organizaciones de negocios, los auditores intentaron auditar estos sistemas de la misma manera que con los sistemas manuales. Cuando esta etapa cambió, los auditores se tuvieron que ver mas envueltos en los sistemas de cómputo.

Dentro del diseño y efecto de las pruebas para auditar se necesitan técnicas alrededor de la computadora, a través de la computadora y las pruebas de escritorio las cuales se ven a continuación:

### 4.5.1 AUDITANDO ALREDEDOR DE LA COMPUTADORA.

Muchas funciones en el proceso de auditoría son realizadas independientemente, del sistema de cómputo, tales como la verificación de inventarios físicos y manejo de efectivo.

Muchas personas argumentan que la auditoría a través de la computadora y la auditoría con la computadora son lo mismo. Teóricamente, es cierto, pero desde que empezó la auditoría en Centros de Cómputo, la auditoría a través de la computadora tiene un significado en el uso de pruebas de escritorio. Auditando con la computadora, se utilizará como un panorama mas amplio.

**Definición de la Auditoría Alrededor de la Computadora.**

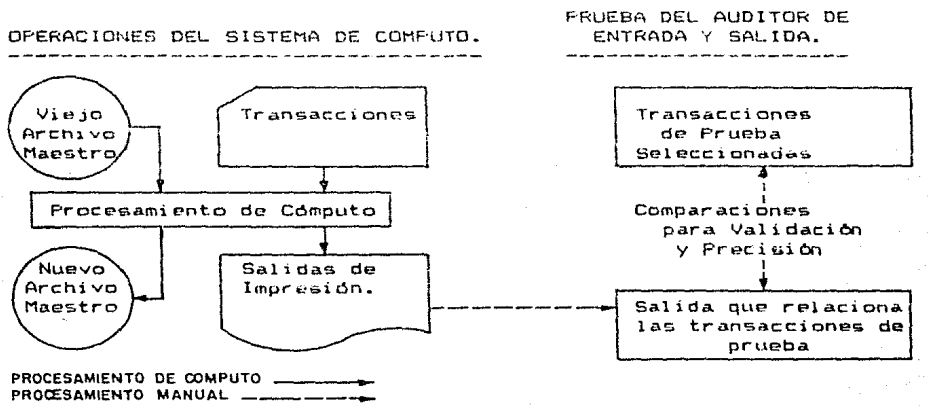
En tiempos pasados los auditores veían a la computadora como una caja negra en donde nada mas auditaban las entradas y salidas unicamente. Los controles y procedimientos usados en el procesamiento de datos fueron considerados sin importancia por el auditor tanto como la salida generada por la computadora.

El auditor seleccionó la entrada y probó contra una salida apropiada y vice-versa, y se asumió que los sistemas de control en operación trabajaban apropiadamente.

## Como Auditar Alrededor del trabajo de Cómputo.

La figura 2 muestra una aproximación a este tipo de auditoría. La auditoría se realiza seleccionando un conjunto de transacciones actuales que hayan sido procesadas. Estas transacciones son rastreadas desde su punto de origen como documentos fuente a los registros de salida o a los registros producidos.

Por ejemplo, el auditor selecciona los documentos fuente a ser procesados, tales como tarjetas checadoras, se los rastrea a través de salidas de impresión, tales como registros y cheques de pago. Ambos, la validación y precisión de las transacciones de prueba seleccionadas son verificadas. La parte racional detrás de esta aproximación es que si los documentos fuente son reflejados apropiadamente en los archivos maestros, los archivos maestros en turno son soportados por documentos fuente, y la salida producida será la correcta, entonces las funciones de procesamiento del sistema de cómputo serán los correctos.




F I G U R A 2

Ejemplo de Prueba de Transacciones de Entrada con Salidas utilizando Técnicas de Auditoría Alrededor de la Computadora.

Ventajas:

a. No hay riesgo de trampa con datos reales.
b. Poquena capacitación para el auditor.
c. Es sencilla y comprensible por cualquiera.
d. El costo es bajo.

Desventajas:

a. Muchas computadoras tienen Bases de Datos enormes para trabajar en forma manual.
b. Ignora al sistema de control y puede fallar en reconocer errores potenciales o irregularidades con el sistema.
c. Representa actuar después y no antes del error.
d. No utiliza la computadora.
e. Para todos los intentos y propósitos no se alcanzan las metas del auditor.

## 4.5.2 AUDITANDO A TRAVES DE LA COMPUTADORA.

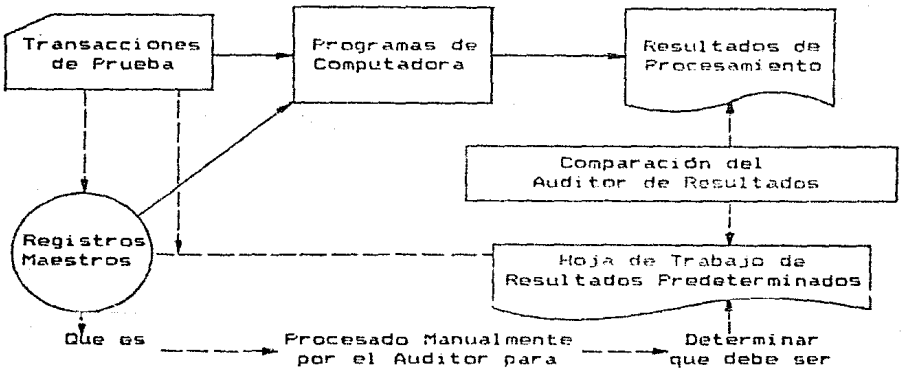
Como existen muchas limitantes para la auditoría alrededor de la computadora, se crearon nuevos y mas sofisticados sistemas de procedimiento.

En este punto se le dá un énfasis a probar y verificar lo siguiente:

a. La efectividad de los procedimientos de control sobre las operaciones de cómputo y sus programas.
b. La incorrección de los procesamientos internos.
   * Revisión y Verificación de transacciones fuente.
   * La prueba actual de la lógica del programa y sus controles.

Aquí (Ver Figura 3) el auditor asume que la computadora, por sí sola es una herramienta precisa y que cuando es programada adecuadamente producirá salidas correctas. Es más, las pruebas de auditoría deben ser pensadas para ver como probar la lógica del programa así como la precisión de la computadora.

Una de las herramientas clave en la aplicación de esta técnica es la preparación de una serie de transacciones de prueba, referidas normalmente a una prueba de escritorio. La prueba de escritorio es corrida en la computadora, utilizando los mismos programas que fueron usados para operar la aplicación particular que está siendo probada. La prueba está diseñada para asegurar la efectividad de los controles y la precisión y generalidad de los programas.




F I G U R A 3

Ej.de Pruebas al Procesamiento Interno del Sistema usando Técnicas Através de la Computadora.

Ventajas:

a. Ayuda al auditor a estar mas envuelto en el sistema, incrementa su conocimiento y su habilidad para realizar auditorías mas complejas en el futuro.
b. Trabaja como ayuda en realizar las pruebas y en la evaluación de los controles programados.
c. Incrementa el servicio a clientes porque los controles y las operaciones son checadas y al menos observadas por el auditor.
d. Los resultados de las pruebas son fácilmente identificables y pueden ser hechas como una medida de procesamiento interno seguro.
e. Esta técnica utiliza a la computadora como una herramienta realizando funciones auditoras.

Desventajas:

a. Requiere tiempo de computadora.
b. Requiere mas conocimiento técnico y mas personal de auditoría.
c. Representa una prueba limitada del sistema.
d. Representa actuar después de y antes del auditor.

### 4.5.3 PRUEBAS DE ESCRITORIO.

Son datos de prueba que son simulados y que incluyen idealmente cada tipo posible de condición, incluyendo aquellos que el sistema, por la carencia de controles apropiados, es incapaz de manejar.

Las listas de transacciones deben probarse para condiciones válidas e inválidas. Los datos simulados, son procesados con los programas del sistema de cómputo.

**Propósito de la Prueba de Escritorio.**

El auditor no puede ver físicamente las operaciones y controles en la caja negra, pero puede ver un listado de salida de los resultados de la prueba, por ejemplo, algunas transacciones que fueron supuestas para ser rechazadas o donde las condiciones de overflow causaron errores, o donde las transacciones fuera de límite fueron procesadas como si estuvieran correctas. El auditor puede determinar también que la caja negra está procesando apropiadamente las transacciones válidas. El uso de pruebas de escritorio abre las ventanas de la caja negra, porque las transacciones simuladas son procesadas através del sistema de cómputo y generan resultados que son comparados por el auditor con los resultados que ya había preparado a mano.

Antes de ejecutar la prueba de escritorio, el auditor calcula el resultado de la utilización de la prueba y entonces compara estos resultados con los resultados obtenidos durante la prueba.

**Como prepararla.**

a. El sistema completo de controles debe ser revisado.
b. Sobre esta base; las transacciones son diseñadas para probar aspectos seleccionados del sistema o del sistema entero.
c. Los datos de prueba son transcritos a las formas particulares del sistema de entrada.
d. Los datos de prueba son convertidos a una forma reconocible por la máquina, con su respectiva validación.
e. Los datos de prueba son procesados utilizando los programas regulares de producción y los Sistemas Operativos.
f. El resultado del punto anterior se comparará con los resultados predeterminados.

**Ventajas:**

- El auditor no debe tener un amplio conocimiento técnico.
- Es una buena aplicación donde la variedad posible y las combinaciones de transacciones son limitadas.
- Da una evaluación objetiva y una verificación de los controles de programa y otras operaciones en las cuales la misma valuación debe ser impracticable o imposible para acompletarse por otros medios.
- Pueden ser aplicables por sorpresa para disuadir las modificaciones no autorizadas de programas y para incrementar la efectividad general de otras pruebas realizadas.

Desventajas:

- Mucho tiempo y esfuerzo son requeridos para preparar una prueba de escritorio representativa y mantenerla. Cualquier cambio en el sistema, manejo de registros, y programas normalmente requieren que esta prueba también sea alterada o modificada.
- En algunos casos el auditor no puede probar los programas de producción del sistema real.
- En un sistema complejo, con una gran variedad de transacciones, es difícil anticipar todas las condiciones significativas y las variables que serían probadas.
- El auditor debe estar familiarizado con la lógica del programa a probar.
- Hay una alta probabilidad que la prueba no detecte una manipulación inapropiada de una cantidad o cuenta específica.

4.5.4 AUDITAR LOS PROGRAMAS DE APLICACION.

Existen numerosas razones para querer auditar este tipo de programas y son los siguientes:

- Detectar o evitar fraudes programados.
- Establecer una conformidad de los requerimientos legales y regulatorios. Ver de paso si los estándares en la programación se están llevando a cabo por el personal.
- Ver si los principios contables son seguidos.
- Evaluar la eficiencia de la programación.
- Establecer como la computadora está generando información en áreas donde de otra manera se dificultaría determinarla.
- Determinar si la documentación del programa está al corriente.
- Facilitar la revisión de modificaciones a programas subsecuentes.

Desde un punto inicial de la revisión del programa, se debe hacer lo siguiente:

- Revisar los estándares de programación y documentación que han sido establecidos por la instalación.
- Seleccionar un programa en particular o un sistema para revisión.
- Obtener una copia del listado en código del programa fuente.
- Obtener una copia de la documentación del programa.
- Determinar que archivos de entrada/salida están siendo utilizados y como son utilizados.
- Confirmar el entendimiento de los archivos y registros que ha conseguido.
- Revisar el programa y apuntar en donde se abren y se cierran los comandos.
- Ahora que los archivos están aislados, empezar a hecharle un vistazo a la lógica del programa.
- Lo siguiente en importancia son los "GO TO's".

- Ahora se está en el último tramo.
- Pon a la computadora a trabajar para ayudarte en la revisión del programa. O sea, utiliza la ayuda en los programas como son los diagramas de flujo, listas de referencia cruzada, generadores de datos de prueba, y tantas herramientas como esté a tu alcance. Sin estas ayudas se hará una tarea muy tediosa.

### 4.5.5 LAS TECNICAS DE AUDITORIA ASISTIDAS CON COMPUTADORA.

**Usando la Computadora como una herramienta de Auditoría.**

El proceso de Auditoría envuelve tres pasos:

a. Revisión del sistema de controles.
b. Evaluación y prueba del sistema de controles.
c. Verificación del contenido de los registros y generación de información evidencial de la base de datos.

Mientras que las pruebas de escritorio y las revisiones de programas son utilizadas para evaluar la calidad de los controles, procedimientos e instrucciones, otras técnicas se necesitan para determinar la calidad de la información producida por el sistema.

Las técnicas de auditoría asistida con computadora hacen posible expander el panorama de la verificación del contenido de los registros y la generación de información evidencial de la base de datos mas eficientemente.

El auditor obtiene un mejor nivel de seguridad de los establecimientos financieros y otras salidas del sistema extendiendo el panorama de su exámen e incremento del número de incisos probados.

La velocidad y prediccionalidad de la computadora permite al auditor tener mayor precisión en su información de manera económica y práctica sin ninguna de las restricciones impuestas por procedimientos de oficina.

El propósito de este punto es de realizar una confirmación para verificar la existencia o la precisión de compañías, gente, cuentas, bienes y servicios. El auditor realiza la verificación por uno o por una combinación de los siguientes procedimientos.

- Uso de una confirmación positiva.

  Esta forma de confirmación contiene el estatus y la cantidad del objetivo de confirmación (por ejemplo recepción de cuentas), es direccionando y enviando al responsable adecuado (por ejemplo, el cliente), preguntándole para confirmar directamente al auditor la precisión del reporte de confirmación (por ejemplo balance). La característica esencial de la confirmación positiva es que se hace para replicar en cada caso.

- Uso de una confirmación negativa.

  La aproximación general para la preparación de una confirmación negativa es la misma que la positiva, excepto que el contestante es solicitado para avisar al auditor solamente si la forma de confirmación tiene errores.

- Uso de una confirmación física.

  Esta aproximación es utilizada cuando el auditor actualmente va al objetivo de confirmación y observar su existencia.

A continuación se presentan lineamientos que representan una lista de las actividades a realizar por el auditor en una confirmación y la cantidad de trabajo que debe hacer con la ayuda de la computadora.

a. Preparación. La fase de preparación se maneja de la forma siguiente:

   - Arregla la Fecha. Decide una fecha específica para el trabajo, permitiendo suficiente tiempo para ensamblar equipo y personal requerido.
   - Frecuencia de Confirmación. Se confirma por lo general del 10 al 33% de las cuentas que son consideradas las menos importantes.
   - Elemento de Sorpresa. Para mayor efectividad, la verificación debe ser realizada sin avisar a ninguna persona que tenga la responsabilidad de guardar registros, seguridades, o cuentas a ser verificadas. Si la sorpresa no se lleva a cabo, la verificación puede perder su valor.
   - Separar su Apartado Postal. Si el auditor no tiene un apartado postal, debe obtenerlo. Es esencial que toda la información llegue directamente al auditor.
   - Avisar a los Clientes.
   - Determinar el Panorama.
   - Selección de Cuentas.

b. Realización.

   - Control de Registros.
   - Profundidad de las Cuentas a Verificar.
   - Registro de Solicitud Enviada.
   - Suministrando y Checando Cantidades.
   - Checar Direcciones.
   - Formas Fechadas.
   - Instrucciones de Envío Especial.
   - Envío.
   - Manejo de Envíos Inapropiados.

c. Seguimiento.

- Consecuencias de la Revisión.
- Verificando Firmas.
- Firmas Inapropiadas.
- Seguimiento de Cartas a Clientes.
- Cuentas sin Respuesta.
- Resultados en un Reporte. Este reporte debe incluir el número, y la cantidad de dinero del total de cada grupo que está siendo checado y del número de verificaciones enviadas, también como el número y la cantidad de verificaciones recibidas, junto con unos apuntes de cualquier excepción seria.

Podemos decir que la computadora puede ser utilizada para accesar y manipular datos como lo requiera el auditor, sumarizar volumenes masivos de datos, identificar discrepancias con y entre los archivos, producir información analítica, etc.

Si la computadora tiene tantos beneficios uno no puede explicarse porque no se usa con mas frecuencia. Seguramente es porque los auditores no estaban capacitados para programarlas.

Así que para resolver este problema, hay cuatro fuentes para este tipo de programas auditores.

- Programas escritos por un programador de la organización.
- Programas escritos por o bajo supervisión del auditor.
- Programas generalizados, desarrollados por empresas privadas.
- Programas de utilidad y de propósito suministrados por el proveedor.

Programas escritos por un programador de la organización.

Si no dispone de programas del proveedor o de auditoría, el auditor si no puede tampoco escribir sus propios programas, el auditor debe trabajar con el programador para el desarrollo de un programa que sirva para su propósito. La ventaja para el auditor es que ahorra tiempo y otros recursos. La mayor desventaja es que el auditor debe depender del personal de sistemas para realizar el trabajo crítico. Haciendo esto el compromete su independencia y puede perder el respeto del personal. Sin embargo de esta manera permanece la computadora como una caja negra para él.

Tipos de Programas Disponibles.

- Un programa diseñado puramente para satisfacer un requerimiento de auditoría específico, tal como una programación simple para selección de transacciones, determinación de condiciones excepcionales.

- Un programa diseñado puramente para satisfacer un requerimiento de auditoría específico, pero también puede ser útil para la administración sobre una base continua, tal como un programa para recibir cuentas o analizar inventarios y sacar los obsoletos.

- La modificación de un programa existente para acompletar una tarea de auditoría simultaneamente con operaciones de procesamiento normal, tales como impresión de la recepción de cuentas seleccionadas a la vez que estas cuentas a recibir están siendo preparadas.

- Existien programas y datos procesados bajo condiciones controladas, tales como acumulación, apreciación y extensión de inventario.

Habiéndose hecho el programa, el auditor necesitará probarlo antes de usarlo.

**Programas escritos por el Auditor.**

El principio fundamental de auditoría es la independencia del auditor. Con la instalación de mas y mas computadoras, muchos auditores han observado que su independencia ha disminuido con el incremento de la confianza en el personal de cómputo para actuar como intermediarios entre ellos y el sistema de cómputo que están auditando. Para ser efectivo, debe establecer su independencia. Una de las mejores maneras para hacer esto es que el auditor escriba su propio programa de auditoría, entonces el confiará solamente en sí mismo y en la computadora para proveerlo con información confidencial.

La manera de efectuar esta técnica puede ser la siguiente:

Escribir el programa de auditoría por sí mismo o para tener una ayuda bajo una supervisión cercana.

Para hacer esto, el auditor debe poseer un conocimiento firme del sistema de cómputo y de la competencia en un lenguaje de programación que puede ser ejecutada por el sistema de cómputo.

Algunos de los lenguajes de alto nivel al auditar son COBOL, PL/1, FORTRAN Y BASIC. Es relativamente fácil obtener un nivel moderado de competencia en cualquiera de estos lenguajes de programación. La mayoría de estos lenguajes son universales. Si el auditor por ejemplo aprende COBOL, el puede sentirse seguro que este lenguaje será compatible con un gran número de sistemas. Sin embargo, debe enfatizarse que un número de sistemas no pueden ser compatibles con un lenguaje particular que el auditor pueda escribir.

Hay que determinar cuando sí, o cuando no escribir su propio programa o el utilizar cualquiera de las otras técnicas, el auditor debe comprender los factores de procesamiento y balance contra los que debería tener para hacerlo sin el uso de una técnica de auditoría en particular, tal como escribir su propio programa de auditoría.

Estos factores son:

- El volumen de elementos de datos envueltos.
- La complejidad de las operaciones de procesamiento de datos requeridas.
- Estrecho procesamiento en el tiempo.
- Demandas computacionales.

Si el auditor va a seleccionar la técnica de auditoría apropiada, el debe comprender los cuatro elementos que tienen impacto en los objetivos.

En muchos sistemas un elemento es tan dominante que los otros tres no pueden ser cuidadosamente definidos o considerados.

En la mayoría de los sistemas estos elementos trabajan justo para hacer menos difícil a los auditores el uso de técnicas manuales. En conclusión, como el volumen de datos se incrementa, como se incrementa la complejidad, los ajustes de tiempo serán mas severos y como las demandas computacionales son mas sofisticadas, en el incremento del uso de programas de auditoría escritos por el auditor, tan bien como de otras fuentes, será garantizada.

Ventajas:

- Incrementa la independencia del auditor del personal de cómputo.
- Enaltece el respeto al auditor en Centros de Cómputo del personal.
- Incrementa la experiencia del auditor y su confidencialidad acerca de los sistemas de cómputo en general adentrándose mas en el sistema.
- Improvisar la flexibilidad del auditor permitiéndole conjuntar o formular cualquier criterio de selección que quiera.
- Dar al auditor la habilidad para auditar cualquier sistema, tanto como el lenguaje sea compatible con la computadora. Este punto es importante porque algunos programas de auditoría generalizados son compatibles en la computadora "X" pero no en la "Y". Mas aún, teniendo el conocimiento de la programación, improvisa sobre la capacidad auditable y su flexibilidad.
- Da al auditar una fuerte herramienta para tratar loa requerimientos de volumen, complejidad, tiempo y de cómputo.

Desventajas:

- Los costos no pueden ser justificados. El tiempo y dinero invertidos en el esfuerzo de escribir un programa de computadora debe ser justificado en la base del límite de recursos de auditoría y los beneficios que se obtendrán a futuro.
- Algunos programas pueden estar bien para una vez, pero no siempre funcionan para usos repetidos.
- Algunas veces el auditor puede necesitar grandes períodos de tiempo para preparar sus programas.

- Los programas una vez desarrollados, requieren normalmente mantenimiento para el cambio en las condiciones a tratar. Sin este mantenimiento, los programas se harán obsoletos rápidamente.

Uso del Programador bajo supervisión directa del Auditor.

El auditor puede sentir que su tiempo puede ser mejorado aprovechándolo en otras tareas, si el puede contratar a un programador que codifique y dé mantenimiento a los programas para auditar.

El programador debe trabajar bajo la supervisión directa del auditor. Por lo tanto el auditor debe formular el criterio de selección y objetivos de la auditoría. Debe estar envuelto en las pruebas e implantación del programa. Teniendo un programador, de ninguna manera reduce las necesidades para el auditor de tener más conocimientos de los sistemas de cómputo y la habilidad para poder escribirlos. Su experiencia en sistemas y programación debe ser tan grande que cuando el tenga un programador para escribir sus programas, debe ser como si el estuviera desarrollándolos o mejor.

Si el auditor quisiera tener un programador en una base experimental primero, puede contratar servicios externos tales como compañías de software o despachos de servicios para un programador. Esta aproximación permitirá al auditor iniciarse y ayudarle a "sentir" los programas. Esta alternativa representa un bien temporal, así que sería mejor no utilizarlo por más de un año.

Otra aproximación es contratar a un programador para el grupo auditor de tiempo completo. Las tareas del programador de auditoría deben ser las siguientes:

- Trabajar con miembros del grupo auditor para desarrollo de especificaciones y objetivos del programa.

- Revisar la documentación del cliente y definir los registros del programa.

- El diseño, la codificación, las pruebas y la implementación del programa bajo supervisión directa.

- Preparar la documentación completa de los programas.

- Desarrollar, catalogar y mantener una biblioteca de programas.

- Mantener y cambiar programas tanto como las condiciones lo requieran.
- En asuntos técnicos servir como un lazo de comunicación entre los auditores y el personal de sistemas.

- Supervisar el desarrollo, implantación y operación de las otras técnicas de auditoría.

- Actuar como consultor técnico al grupo auditor.

- Mantenerse actualizado con los cambios en la tecnología de cómputo y de programación.

**Programas de Auditoría Generalizados.**

En muchos casos, hay una barrera entre el auditor y la computadora. El advenimiento de los programas de auditoría generalizados representa un desarrollo significativo que ha ayudado a los auditores a mantener la paz en los Centros de Cómputo y disminuir los problemas básicamente, estos programas han sido diseñados para facilitarle al auditor el uso de la computadora en su trabajo. También lo ayudan a seleccionar independientemente los datos para su evaluación e interpretación. Estos programas reducen la tarea del auditor con el personal del Centro de Cómputo e incrementan su independencia.

Muy pronto los programas de auditoría generalizados facilitarán el análisis auditable de los datos computarizados, perfeccionan la realización de la auditoría y proveen mayor administración al auditor con una gran variedad de información.

Este programa se define como un programa de computadora o grupo de módulos lógicamente ligados, los cuales se diseñaron para realizar una variedad de tareas especificadas por el auditor.

**Objetivos de estos Programas de Auditoría Generalizados.**

- Aplicar el concepto de generalidad, por lo tanto el auditor puede usar el término programas de auditoría generalizados en donde sea, sin hacer caso a la aplicación o al Centro de Cómputo.

- Proveer al auditor de un alto nivel de independencia, especialmente del personal del Centro de Cómputo.

- Para perfeccionar el acceso rápido a grandes volumenes de datos codificados y convertirlos en forma legible para nosotros.

- Incrementar el número de técnicas de auditoría disponibles para el auditor.

- Minimizar las necesidades del auditor para tener un respaldo extenso en tecnología de cómputo y de programación.

En una corrida larga estos objetivos pueden trabajar contra el auditor si el depende demasiado de esta técnica.

Ventajas:

- El auditor puede hacer mas en menos tiempo.

- Cuando hay muchos problemas relacionados con el volumen, la complejidad, la computación y el tiempo, la aplicación de este tipo de programas resultará mejor de manera significativa ahorrando costos.

- La mayor confianza puede ser localizada en los resultados auditables.

- Solamente algunas semanas de entrenamiento y un mínimo conocimiento de tecnología en computadoras es requerido.

- El programa está bajo el control del auditor.

- El programa puede realizar una variedad de tareas de auditoría en diferentes sistemas.

Desventajas:

- Diversidad de lenguajes de programación, computadoras, diseño de sistemas y diferentes estructuras de datos encontrados en los sistemas del manejo de Base de Datos, que pueden hacer a los programas incompatibles en un número de situaciones.

- Algunos auditores, probablemente sin una justificación, dicen que esto requiere mucho tiempo de entrenamiento y que uno debe tener mucha experiencia para usar el programa efectivamente.

Programas de Utilería Suministrados por el Proveedor

Ahora mas proveedores de computadoras tienen un gran número de programas de utilería de propósito general en sus bibliotecas. La mayoría de estos programas no son vistos como programas de auditoría en sí. Sin embargo, debido a que las funciones de auditoría requieren extraer datos de archivos en la computadora, obteniendo medias, ordenando, copiando, analizando, probando y monitoreando procesos, y muchos de estos programas pueden realizar muchas de estas mismas funciones, y que pueden ser puestas o incluídas en las herramientas del auditor como técnicas efectivas.

La disponibilidad de estos programas para el auditor no pueden ser obvios, porque ellos no han sido empleados generalmente en un contexto de auditoría tradicional.

El auditor puede tener que hacer averiguaciones con proveedores, estimando las necesidades para programas de utilidad que pueden ser utilizados para realizar tareas de auditoría.

Las ventajas obvias de estos programas para el auditor son:

- Proveer información de auditoría significativa que puede ser difícil de obtener por otras técnicas.

- Dan al auditor seguridad de operación, porque los programas tienen ya una independencia de un tercero.

- Proveen un alto nivel de integridad porque ellos son desarrollados por un tercero.

- Generalmente soportan una buena documentación.

- Son de gran utilidad en la realización de una tarea de auditoría una vez que no justifica el desarrollo de un programa de auditoría especial.

## 4.6 EVALUACION GENERAL.

Para que el auditor pueda dar su evaluación, se debe contar ya con toda la información necesaria y haber cumplido con todos los otros pasos del desarrollo de la auditoría.

Esta evaluación consiste en un reporte que tomará en cuenta un enfoque global de la situación actual en la que se encuentre hasta el momento el Centro de Cómputo. Este reporte o informe se realizará de la siguiente manera :

Una práctica común es el que el auditor redacte su informe en borrador a medida que realiza su trabajo. Inicia la tarea provisto de los instrumentos propios de la misma y varias carpetas de archivo. Cada una de estas últimas se rotulará con un tema específico, por ejemplo las áreas de control y auditoría, que figurarán en el informe. A medida que avance la auditoría, irá colocando documentos y memorándums en sus carpetas respectivas. Al completar un sector específico de evaluación, pondrá por escrito, inmediatamente, los detalles mientras todavía están frescos en su mente, con lo que evitará la molesta posibilidad de tener que volver a recopilar los mismos datos.

La preparación cuidadosa del informe, con todos los aspectos y recomendaciones, corona el trabajo. Conviene tener presentes varios aspectos fundamentales al redactarlo y el método para organizar los hallazgos debe ser objeto de particular atención. Todos los hechos que reflejen circunstancias fuera de lo normal, deficiencias, irregularidades, embotellamientos, puntos débiles, desperdicio exagerado, pérdidas innecesarias, controles inadecuados, etc., se dispondrán en el orden de su importancia relativa. Luego vendrán los detalles de aspectos tratados con la Alta Gerencia y otros empleados. Habrá que indicar o transcribir normas vigentes y comentarios respecto a lo descubierto durante la auditoría. Finalmente, vendrán las recomendaciones formuladas por el auditor, las cuales deberán redactarse sencilla y claramente.

En la preparación del informe hay que tener presentes dos aspectos de suma importancia, que se puedan condensar en estas dos preguntas: A quién se enviará el informe ? y Cómo rendir el informe? La decisión en cuanto a quién habrá de recibir el informe no es difícil, porque eso deberá estar bien definido por la política respectiva, pero sí es algo a que el auditor tiene que atender antes de la preparación del documento. Porque quien lo reciba va a juzgar de su calidad, aceptarlo o rechazarlo, determinar si es bueno, adecuado, interesante, útil.

La respuesta a la segunda interrogante contiene varias facetas que hay que tener presentes. El auditor necesita determinar cómo rendirá su informe, porque el método de comunicación es importante. Parte de la información se proporcionará de forma oral, pero la mayor parte de la misma será por escrito. En las empresas, los informes escritos deben ser breves, claros, valiosos y pertinentes. Porque a ningún ejecutivo le gusta leer y digerir informes largos y confusos. En resumen, el auditor debe preveer las indicaciones e intereses de la dirección.

Tener ideas claras es indispensable, porque esto le da más énfasis a lo que se escribe. Un pensamiento bien organizado y una planeación inteligente, son los primeros pasos en el proceso de unificar ideas o hechos.

El esbozo de informe de auditoría establece un plan o guía para la ordenada presentación del informe. Por medio del mismo, el auditor tendrá una imagen mental de lo que busca hacer.

El informe deberá ser uniforme en cuanto a diseño, esto es, en cuanto a plan general, pero no en cuanto a contenido. Lo que importa más es que la uniformidad de diseño no provoque, por ningún motivo, una uniformidad en la forma de plantear las situaciones halladas, ni tampoco borrar la personalidad individual de quien redacte el informe.

Este deberá expresar la finalidad y alcance del desarrollo de auditoría, las limitaciones que se tuvieron o los problemas con que se tropezó y los hallazgos, opiniones, conclusiones y recomendaciones.

Toda circunstancia perjudicial, deficiencia o irregularidad, deberá ser expuesta en forma breve, pero notoria. El propósito del auditor deberá ser comunicar a quien lea el informe, todo hallazgo o hecho de importancia y demostrar por qué pueden ser de interés para el segundo.

El informe deberá estar redactado en buen español y escrito con la suficiente claridad para que no sea entendido en forma equívoca. El auditor tendrá que hacer lo más que pueda para expresar sus ideas con exactitud, concisión y cortesía.

La exactitud consiste en que lo que se dice está basado en una información definida.

La concisión implica una exposición precisa de lo que se informa.

La cortesía es el empleo de palabras y expresiones que eviten una innecesaria brusquedad en las alusiones.

Habrá que dar atención especial a la expresión, estructura de párrafos, frases y unidad correctas. Deberá tenerse especial cuidado que lo que se dice sea fácilmente comprensible. Una buena redacción presenta ciertas cualidades que no es posible desdeñar: claridad que no deje duda respecto a lo que se pretende decir, precisión que refleje verdad, variedad en la forma de expresarse que mantenga la atención del lector y sobriedad que evite demasiada palabrería.

Conviene emplear un vocabulario sencillo, evitando todo término o expresión técnica. Al escribir el informe, deberá cuidarse que los espacios entre líneas sean a doble renglón, con objeto de facilitar la inserción de correcciones. El manuscrito preliminar deberá estar en forma legible para que el revisor y mecanógrafo lo pueda leer sin dificultad. El redactor deberá prestar atención a ortografía, puntuación y aspectos gramaticales en general.

La redacción será en un estilo preciso, descriptivo, sin sensacionalismos, chocarrerías, modismos o frases hechas.

El auditor no debe saltar demasiado pronto a conclusiones, sino que debe seleccionar todo informe que pueda ser demostrado y contar con los hechos concisos.

Necesita ser veraz y cuidadoso, enfocando las cosas con rigor científico y sin pronunciamientos anticipados o prejuicios personales. Tiene que ser constructivo y positivo. Su informe deberá estar concebido en forma impersonal, utilizando en su redacción la tercera persona gramatical.

### 4.6.1 RECOMENDACIONES.

Habrá casos en que las pruebas y observaciones susciten sugerencias para mejorar la estructura orgánica, políticas y normas, procedimientos y desempeño del trabajo, desarrollo del personal, informes de operación y en otras actividades. Algunas de esas sugerencias podrán discutirse con la alta gerencia para su aprobación y puestas en obra durante la realización de la auditoría por el auditor mismo. Otras sugerencias requerirán de un trámite especial o de toda una labor de convencimiento antes de que sean aceptadas.

Desde luego, el auditor deberá pugnar porque se acepten sus recomendaciones, sin importarle las demoras que puedan ocurrir por causa de personas, problemas de organización o cualquier otra razón

Toda recomendación de importancia que pudiera surgir en las primeras fases de una auditoría, habrá de someterse a la consideración del ejecutivo correspondiente a la mayor brevedad, con objeto de conocer su opinión personal. Esto ayudará a programar el tiempo para un estudio, análisis y cambio de impresiones futuras. También servirá para que la sugerencia se ponga en obra posteriormente o lo más pronto posible.

Las recomendaciones, en términos generales, se presentarán en el informe en su orden de posible aceptación. En otras palabras, el auditor presentará a la dirección, todas aquellas ideas que parezcan tener una mayor probabilidad de aceptación, desde el punto de vista del lugar que ocupen en la lista general de recomendaciones.

Siempre que se pueda, convendrá tener una alternativa para cada recomendación fundamental, a efecto de que si no se acepta la idea original, se pueda hacer la otra proposición muy parecida a la misma. Al aceptarse las sugerencias, convendrá precisar la fecha en que serán puestas en práctica.

### 4.6.2 CON RESPECTO A LOS HECHOS PRINCIPALES.

Al redactar el informe, deberá atenderse a los siguientes puntos:

- Claridad.
- Brevedad.
- Importancia relativa de los datos.

Cada uno de los datos se expresará con claridad y todo vocablo deberá tener sólo un significado.

La brevedad es lo esencial. Sin embargo, conviene cuidar de que exista un equilibrio entre la claridad y la brevedad. Será útil, al respecto, revisar cada párrafo para ver si no presenta inexactitudes en el significado o vocablos inadecuados.

Las situaciones perjudiciales se plantearán en el orden de su importancia relativa. Nunca se insistirá demasiado en esto. Porque si al primer aspecto impresiona a la persona que lee el informe, lo que sigue de este será objeto de mayor atención que si el primer planteamiento no hubiese tenido suficiente impacto.

Además de saber cuáles son los aspectos sobresalientes relacionados con circunstancias, políticas y prácticas que directa o indirectamente afecten de una manera adversa a la empresa; a la dirección le interesa saber cómo afectan esos aspectos o situaciones a ella misma.

# CONCLUSIONES.

Podemos decir en conclusión, que los Centros de Cómputo en México, necesitan ser controlados desde el momento en que se piensa en la instalación de uno . No debemos permitir que se esté creciendo en forma desmesurada solo por decir que nuestros procesos se están automatizando con el solo hecho de adquirir una computadora.

Necesitamos aplicar otro tipo de conocimientos antes de pensar en una de ellas.

Es cierto que el Cómputo está creciendo en nuestro país en forma acelerada, pero pocos son los que están realizando una planeación estratégica, un verdadero análisis de las necesidades de procesamiento electrónico de información. No debemos olvidar que los costos de este tipo de adquisición representan un egreso muy fuerte para cualquier institución y que deben aprovecharse al máximo, pues si no fuese así, estaríamos cayendo en un fraude y posteriormente yendo a un rotundo fracaso.

Sin embargo, no hay que olvidar que un Sistema de Control debe ser directamente proporcional al tamaño de la instalación, pues será una parte muy importante en el exito de su funcionamiento.

Otra parte, es que necesitamos de algo para retroalimentar al Sistema de Control y ese algo es la Auditoría. Debemos quitar de nuestro pensamiento la idea de que la Auditoría es sinónimo de que algo está fallando. La Auditoría como hemos podido ver, es una herramienta muy útil para el encuentro con el punto óptimo de aprovechamiento del Centro de Cómputo, de su gente, de su equipo y de todo el medio que lo rodea.

Es una tarea ardua pero que rinde muchos frutos en provecho de un mejor funcionamiento del Centro de Cómputo.

Se espera que este documento sea un avance esencial, para el mejoramiento de la computación y su desarrollo.

Se tiene que buscar el apoyo de las Instituciones para la implementación de normas y reglamentos que rijan los problemas a los que se enfrenta esta tecnología, en beneficio de la comunidad computacional, tanto en Software como en Hardware pues practicamente son nulas y los auditores no tendrían, en caso de un problema mayor, a quien acudir.

Además, hay que tratar por todos los medios de mantener un orden, una secuencia y una planeación para seguir paso a paso el desarrollo de un Centro de Cómputo.

Podemos agregar también, que este documento servirá como una ayuda muy importante para la implementación de un sistema de Control y de la aplicacín de una Auditoría.

Se debe recalcar el hecho de que este documento se realizó en forma general y que existen muchos mas detalles que se han resumido por falta de espacio. Esto nos hubiera llevado a detalles excesivos, y se hubiera perdido el enfoque al que pretendíamos llegar y al propósito fundamental del documento.

# BIBLIOGRAFIA.


- INFORMATION SYSTEMS HANDBOOK ( I y II ).
  W.HARTMAN, H.MATTHES, A.PROEME
  N.V.PHILIPS, NETHERLANDS, 1984

- SOFTWARE ENGINEERING PRACTITIONERS APPROACH.
  RESEG S.PRESSMAN
  MC.GRAW HILL, NEW YORK, 1983

- INFORMATION SYSTEMS: THEORY AND PRACTICE.
  JOHN G.BURCH,JR., FELIX R.STRATER,JR.
  JOHN WILEY & SONS, U.S.A., 1985

- MANAGING THE FOUR STAGES OF EDP GROWTH.
  GIBSON,C.F., R.I.NOLAN
  HARVARD BUSINESS REVIEW, U.S.A., JAN-FEB 1974

- GUIA PARA LA ELABORACION DE ESTUDIOS DE VIABILIDAD SOBRE SISTEMAS DE COMPUTACION.
  VARIOS AUTORES
  S.P.P., MEXICO, 1981

- DESARROLLO Y ADMINISTRACION DE CENTROS DE COMPUTO.
  V.GEREZ, M.MIER, R.NIEVA, G.RODRIGUEZ
  INSTITUTO DE INVESTIGACIONES ELECTRICAS
  C.E.C.S.A., MEXICO, SEPTIEMBRE 1985

- CONTRATOS ESTANDAR PARA LA ADMINISTRACION PUBLICA FEDERAL EN MATERIA DE INFORMATICA. VOL. I y II
  I.N.E.G.I., S.P.P., MEXICO, 1986

- SISTEMA DE ORGANIZACION DE LA INFORMACION.
  SEGUROS LA PROVINCIAL, MEXICO, 1986

- PROGRAMA INSTITUCIONAL DE DESARROLLO INFORMATICO.
  GCIA.SISTEMAS E INFORMATICA, FIOSCER
  MEXICO, 1986

- CENTRALIZATION: " TO BE OR NOT TO BE ? ".
  LOUIS FRIED
  AUERBACH PUBLISHERS, U.S.A., 1976

- ADMINISTRACION Y SEGURIDAD DE UN CENTRO DE COMPUTO.
  DESARROLLO EJECUTIVO DE COMPUTACION A.C.
  MEXICO, 1985

- DATA CENTER OPERATIONS.
  A GUIDE TO EFFECTIVE PLANNING, PROCESSING AND PERFORMANCE
  HAWARD SCHAEFFER
  PRENTICE HALL, U.S.A., 1981

- CONTROL Y AUDITORIA DEL COMPUTADOR.
  W.C.MAIR, DONALD R.WOOD, KEAGLE W.DAVIS
  INSTITUTO MEXICANO DE CONTADORES PUBLICOS
  GPO.EDITORIAL PRINTAMATIC S.A., MEXICO, 1976

- PLANEACION DE INSTALACIONES PARA EL SISTEMA 360 Y 370.
  IBM DE MEXICO, MEXICO, 1984

- ADMINISTRACION DE CENTROS DE COMPUTO.
  MANUAL DE ESTUDIANTE
  HONEYWELL SISTEMAS DE INFORMACION. MEXICO, 1984

- GUIA COMPENDIADA: REVISION DEL PROCESAMIENTO ELECTRONICO DE INFORMACION.
  D.W.JERBASI
  PRICE WATERHOUSE & CO., NEW YORK, U.S.A., 1971

- EL PROCESO DE AUDITORIA PARA DESARROLLAR PROGRAMAS DE AUDITORIA.
  D.W.JERBASI
  PRICE WATERHOUSE & CO., NEW YORK, U.S.A., 1971

- BASES GENERALES DEL PROGRAMA ANUAL DE AUDITORIA 1984.
  S.E.C.O.G.E.F., MEXICO, 1984

- CENTRO DE COMPUTO INFONET.
  S.C.T., MEXICO, 1982

- CARDOX GASEOUS AGENT FIRE EXTINGUISHING SYSTEMS FOR COMPUTER FACILITIES.
  CARDOX PRODUCTS
  CHEMETRON CO., CHICAGO, ILLINOIS, U.S.A., 1985

- COMPUTER CONTROL AND AUDIT.
  A TOTAL SYSTEMS APPROACH
  JOHN G.BURCH,JR., JOSEPH L.SARDINAS,JR.
  JOHN WILEY & SONS, NEW YORK, U.S.A., 1978

- PROCEDIMIENTOS DE CONTROL EN COMPUTACION.
  INSTITUTO MEXICANO DE CONTADORES PUBLICOS
  MEXICO, 1982

- AUDITORIA EN SISTEMAS.
  MANUAL DEL SEMINARIO
  INSTITUTO MEXICANO DE AUDITORES INTERNOS
  MEXICO, 1987

- SISTEMAS DE CONTROL EN ADMINISTRACION DE PROGRAMAS.
  JOSEPH A.MACIARIELLO
  LIMUSA, MEXICO, 1981

- AUDITING INFORMATION SYSTEMS.
  IVO DE LOTTO, EARL M.WYSONG,JR.
  INTERUNIVERSITY CONSORTIUM OF LOMBARDY FOR AUTOMATIC DATA PROCESSING, MILAN, ITALY, SEP.26-29, 1978

- NORMAS Y PROCEDIMIENTOS DE AUDITORIA.
  INSTITUTO MEXICANO DE CONTADORES PUBLICOS
  MEXICO, 1981

- AUDITORIA INTERNA.
  C.P. JORGE LOZANO N.
  ECASA, MEXICO, 1983

- AUDITORIA ADMINISTRATIVA.
  WILLIAM P.LEONARD
  DIANA, MEXICO, 1983

- LA AUDITORIA ADMINISTRATIVA.
  JOSE ANTONIO FERNANDEZ
  DIEM, MEXICO, 1984

- AUDITORIA Y CONTROL DEL PROCESAMIENTO DE DATOS.
  RICHARD W.LOTT
  ED.NORMA, COLOMBIA, 1984

- COMPUTER SYSTEMS AUDITING.
  CODE GB7 STUDENT HANDBOOK
  HONEYWELL INFORMATION SYSTEMS
  MASSACHUSETTS, U.S.A., 1986

- COMPUTERS: AUDITING AND CONTROL.
  JANCURA, ELISE AND ARNOLD BERGER
  AUERBACH PUBLISHERS, U.S.A., 1973

- DPMA POLL FINDS PRIVACY STILL MOST CRITICAL ISSUE.
  ANN DOOLEY
  COMPUTERWORLD, U.S.A., DEC.13, 1976