9

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

CAMPUS
A R A G O N

"CONSIDERACIONES EN EL DISEÑO DE UN SISTEMA DE AUDITORIA PARA CENTROS DE COMPUTO. "

TESIS PROFESIONAL

QUE PARA OBTENER EL TITULO DE

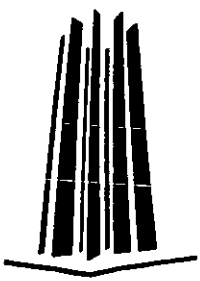
INGENIERO EN COMPUTACION

P R E S E N T A

DANIEL BAÑOS HERNANDEZ

ASESOR:

ING. MANUEL MARTINEZ ORTIZ



ENEP ARAGON

MEXICO, 2004.

INDICE

INTRODUCCION

Estamos inmersos en profundos cambios de todo tipo que nos llevará al próximo siglo XXI. Las empresas y organizaciones dependen de los órdenes económicas, industriales y sociales en los que se encuentran inmersos, por lo que, si las tendencias tecnológicas y los entornos económicos e industriales cambian, deben adoptarse rápidamente a las nuevas circunstancias para sobrevivir. Una de las tendencias actuales más significativas es la que se dirige desde una Sociedad Industrial hacia la llamada Sociedad de Información.

Este cambio es muy rápido, está afectando al mundo entero, y su compresión es fundamental para las organizaciones de todo tipo, particularmente en el contexto de los Sistemas y Tecnología de Información. Aunque los avances tecnológicos de los últimos cinco años se ha producido una verdadera revolución tecnológica de gran calado e impacto para la propia industria informática, así como de consecuencias importantes para el resto de sectores.

Cada vez un mayor número de organizaciones considera que la **información** y la **tecnología** asociada a ella representan sus activos más importantes. De igual modo que se exige para los otros activos de la empresa, los requerimientos de calidad, controles, seguridad e información son indispensables. Los gerentes de las empresas deben establecer un sistema de control interno adecuado, de ahí la importancia que de la Auditoría Informática.

El presente trabajo tiene como objetivos Diseñar un Sistema de Auditoría aplicable a un centro de cómputo.

En el primer capítulo se establecen los conceptos fundamentales de la auditoría con el propósito de tener conocimientos que serán utilizados en el diseño de un sistema que determine la Auditoría de un centro de cómputo.

En el segundo capítulo se mencionan algunos conceptos de Seguridad Informática, con la finalidad de poder aplicarla a los centros u oficinas especializadas en Servicios de Cómputo.

Y el último capítulo hace referencia a un sistema que determina la Auditoría de un Centro de Cómputo, de acuerdo a las reglas, métodos y planeaciones antes mencionadas.

Por todo lo anterior, es importante decir, que la Auditoría en Informática es de gran ayuda, tanto en los Centros de Cómputo como en las oficinas actuales, que cuentan con gran cantidad de equipos o hardware, así como, de software o paquetería a la cual los usuarios tienen acceso. La Auditoría Informática nos va ha servir para identificar con cuantos elementos contamos y que tan ordenado y organizado tenemos los Centro de Cómputo.

CAPITULO I. ASPECTOS GENERALES DE LA AUDITORIA

Objetivo: Definir los conceptos y técnicas básicas de la auditoría con el propósito de contar con herramientas reales dentro de está área a través de los diferentes enfoques de Auditoría.

I.1. CONCEPTO DE AUDITORÍA

Conceptualmente la auditoría, toda y cualquier auditoría es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/ó cumple las condiciones que le han sido prescritas.

Podemos descomponer este concepto en los elementos fundamentales que a continuación se especifican:

1. Contenido	Una opinión
2. Condición	Profesional
3. Justificación	Sustentada en determinados procedimientos
4. Objeto	Una determinada información obtenida en cierto soporte.
5. Finalidad	Determinar si presenta adecuadamente la realidad o ésta responde a las expectativas que le son atribuidas, es decir, su fiabilidad.

TIPOS DE AUDITORIA

Los elementos de "objeto" y "finalidad" distinguen de qué clase o tipo de auditoría se trata. El objeto sometido a estudio, sea cual sea su soporte, por una parte y la finalidad con que se realiza el estudio, definen el tipo de auditoría de que se trata.

Con base en los anteriores elementos podemos mencionar diferentes clases de auditoría entre otras como:

- Financiera
- Informática
- De Gestión
- De Cumplimiento.

I.2. AUDITORIA INFORMATICA

"Auditoría en Informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática, equipos de cómputo, así como su utilización, eficiencia y seguridad de la organización que participa en el procesamiento de la información". Lo anterior, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información, que sirva de base para una adecuada toma de decisiones.

La Auditoría Informática se define como: "El proceso de examinar el área informática de una empresa en general, desde su planeación, organización, operación y control, en forma particular en lo referente a la utilización de los recursos humanos, software, hardware; con el propósito de que el auditor evalúe las debilidades e irregularidades existentes en los procesos y proponga soluciones que mejoren el servicio, funciones, condiciones de operación y desarrollo y haga las recomendaciones pertinentes."

La Auditoría Informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema computarizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos. De este modo la Auditoría Informática sustenta y confirma la consecución de los objetivos tradicionales de la Auditoría:

- Objetivos de Protección de Activos e integridad de datos.
- Objetivos de Gestión que abarcan, no solamente los de protección de activos sino también los de eficacia y eficiencia.

La auditoría informática es la revisión exhaustiva que se realiza a los sistemas de computo, instalaciones, mobiliario, equipos y periféricos de apoyo con el propósito de evaluar el adecuado procesamiento de su información, gestión informática, eficiencia de sus recursos, medida preventivas y planes de contingencia establecidos dentro de un centro o área de computo.

I.3. PLANEACION DE LA UDITORIA EN INFORMATICA

La planeación en Auditoría es indispensable, ya que por medio de ella vamos a tener un punto de partida. Se establecerán normas y lineamientos a cumplir en el desarrollo del trabajo.

Decidir cuales son los procedimientos convenientes que han de emplearse y que extensión se les dará a las pruebas, la oportunidad para su aplicación, que personal intervendrá en el trabajo así como la calidad profesional del mismo.

Planear nos conduce a realizar las siguientes preguntas:

¿Qué vamos a hacer?
¿Qué será lo más conveniente?
¿Cómo y cuándo los vamos a elaborar?
¿Quién lo va a elaborar?.

Debemos tener presente las condiciones y características propias de lo que estamos planeando, las limitaciones que pueden presentarse en el desarrollo del propio trabajo.

La Planeación en Auditoría debe ser elaborada por una persona suficientemente competente y de preferencia que conozca la empresa en donde se ha de realizarse el trabajo.

El enfoque que se le dará a la planeación del trabajo, dependerá del objetivo que se persiga.

A través de una investigación preliminar se sabe que el trabajo de Auditoría puede planearse no solamente bajo el buen juicio y experiencia, sino que también puede auxiliarse de otras técnicas o métodos.

A continuación mencionaremos algunas técnicas de recopilación de información:

Cuestionario:

Es la recopilación de información, mediante la aplicación de cédulas con preguntas impresas, en donde el encuestado responde de acuerdo a su criterio con información que es útil para el investigador. El cuestionario tiene la ventaja de poder recopilar información en gran escala, debido a que busca respuestas por medio de preguntas sencillas. Tiene la facilidad de poder seleccionar entre dos tipos de preguntas:

Preguntas Abiertas.- Son aquellas preguntas en donde el encuestado tiene múltiples opciones de respuestas a lo que le interroga, no existiendo ninguna limitación para la expresión de las ideas y opiniones, ni en tamaño ni en profundidad.

Preguntas Cerradas.- Son interrogantes en donde el encuestado tiene la oportunidad de elegir, de entre alguna de las opciones presentadas, aquellas respuestas que estén de acuerdo con su opinión.

Observación:

Se puede definir como el análisis detenido de los diferentes aspectos de un fenómeno, a fin de estudiar sus características, conductas y comportamientos dentro del medio ambiente en donde se desenvuelve el fenómeno.

La observación tiene varias formas y aspectos que se utilizan según las necesidades de la propia investigación.

Tipos de Observación:

Directa: Es la inspección de un fenómeno que se hace directamente dentro del medio ambiente en donde se representa el hecho que sea de observar, a fin de contemplar todos los aspectos inherentes a su comportamiento, conductas y características dentro de ese campo.

Indirecta: Es la inspección del fenómeno en estudio, pero sin entrar en contacto directo con el mismo, sino a través de métodos específicos que permitirán hacer observaciones indirectas, según las necesidades establecidas por la propia investigación.

Oculta: Cuando por las necesidades de la investigación se requiere que el observador permanezca oculto y observe el fenómeno sin que sea notada su presencia, se dice que se trata de una observación oculta.

Participativa: Es aquella en la cual el observador tiene la oportunidad de formar parte del fenómeno observado, participando en él, como si fuera una componente del mismo.

No Participativa: Es aquella en la cual el observador evita participar en el fenómeno, a fin de no impactar con su presencia la conducta, característica y desenvolvimiento del propio fenómeno.

Entrevista:

Es la recopilación de información en forma directa, cara a cara, es decir, el entrevistador interroga y obtiene información directamente del entrevistado, siguiendo una guía con una serie de preguntas preconcebidas y adaptándose a las circunstancias que se le presentan.

Tipos de Preguntas durante la Entrevista:

Preguntas Abiertas: Son aquellas en que el entrevistado tiene la libertad absoluta de expresar su opinión sin limitación alguna, salvo la respuesta a la pregunta.

Preguntas Cerradas: Se realizan, con el propósito de limitar, concentrar y/o cerrar las respuestas al entrevistado hacia el tema básico sobre el cual se está cuestionando.

Preguntas de Sondeo: Se utiliza para determinar el medio en el que se desenvuelven el entrevistador y el entrevistado, preguntas y/o toda la entrevista.

Preguntas de Cierre: Es importante realizar las preguntas de cierre, las cuales se lanzan para determinar el cuestionario y también como forma de obtener información adicional, que se dice en último momento.

Preguntas Mixtas: Es la combinación de dos o más preguntas anteriores, tratando de hacer más ágil y eficiente la recopilación de información.

A continuación se presentan los elementos para analizar y dimensionar el área a auditar.

- **A NIVEL ORGANIZACIÓN TOTAL**

  Objetivos a corto y largo plazo.

  Manual de la Organización.

  Antecedentes o Historia del organismo.

  Políticas generales.

- **A NIVEL DEL AREA DE INFORMATICA**

  Objetivos a corto y largo plazo.

  Manuales de organización.

  Manual de política, reglamentos internos y lineamientos generales.

  Número de personas y puestos en el área.

  Procedimientos administrativos del área.

  Presupuestos y costos del área.

- **RECURSOS MATERIALES Y TECNICOS**

  Estudios de viabilidad.

  Números de equipos, localización, características y fechas de instalación.

  Plan de mantenimiento, contratos de estos y de seguro.

  Configuración de los equipos.

  Políticas de operación.

Políticas de uso de equipo.

- **SISTEMAS**

  Descripción general de los sistemas instalados y de los que están próximos a instalarse, estos deben de tener la siguiente información.

  Manuales de operación y procedimientos.

  Descripción general del sistema.

  Diagrama general del sistema y de proceso.

  Fecha de instalación.

DETERMINACION DE OBJETIVOS

La eficiencia del área de informática se puede lograr si los objetivos de ésta están integrados a los de la organización a la que pertenece. El buen funcionamiento del área de informática se logra si los objetivos, los ejecutivos y los usuarios de los sistemas toman parte activa en la dirección, conducción y utilización de los sistemas en forma adecuada, definiendo a los responsables de dichos sistemas y que estos cooperen conjuntamente.

Para los usuarios el área de informática es una herramienta más para incrementar la eficiencia de su trabajo, ya que lo visualiza como un área de servicio, sin tomar en cuenta el costo beneficio de sus requerimientos a nivel organizacional.

I.4. EVALUACION DEL EQUIPO DE COMPUTO

I.4.1. EVALUACION DEL HARDWARE

Este punto trata de algunos componentes del hardware instalados en una organización, asegurando su buena utilización, su óptimo funcionamiento, la continuidad en su operación y su actualización tecnológica.

El **hardware** es el conjunto de todos los elementos físicos (dispositivos).

Algunos elementos a considerar del hardware:

- **Diagrama general del hardware instalado**: Tiene como función principal esquematizar el equipo de cómputo, así como, las comunicaciones existentes de manera local o remota.
- Elaboración de planos de distribución física del equipo instalado. Este plano físico nos va a permitir planear rutas de instalación de nuevos dispositivos.
- Identificación de la configuración base del equipo instalado. Estas características determinar la configuración inicial con la cual va a operar el equipo en condiciones reales de trabajo.
- Identificación de espacio en disco ocupado por el sistema operativo y las aplicaciones de producción. Se debe tomar la norma de documentar el espacio en disco ocupado por cada una de las aplicaciones instaladas, así como, el espacio ocupado por la información de cada aplicación.
- Control del mantenimiento del equipo de cómputo instalado.

- Tener un control total de los equipos en aspectos tales como la periodicidad en los mantenimientos preventivos y correctivos.

La existencia de componentes internos en los equipos, se lleva a cabo a través de la comparación física existente de cada una de las partes internas de los equipos, cotejando éstas contra la factura de compra de los mismos. De esta forma podremos darnos cuenta de los faltantes o sobrantes que se encuentren alojados en el interior de cada equipo de cómputo, actividad no sencilla de realizar.

1.4.2. EVALUACIÓN DEL SOFTWARE

Este punto trata de los recursos lógicos instalados en una organización, asegurando su buena utilización, su óptimo funcionamiento, la continuidad en sus operación y su actualización tecnológica.

El **software** es un conjunto de programas que unidos y relacionados entre si, cumplen con un objetivo establecido.

Algunos elementos a considerar del **software** son:

- Identificación de la versión del sistema operativo.
- Identificación del número de bibliotecas y/o archivos que conforman el sistema operativo.
- Inventario del software instalado.

- Documentación. Se refiere a cada uno de los manuales con que cuenta la aplicación al ser adquirida, como lo son: el manual de usuario técnico y la disponibilidad de esta documentación.
- Identificación del número de bibliotecas que conforman cada aplicación, esta actividad va a determinar el número y tamaño de las bibliotecas que conforman cada aplicación.
- Normalización del software instalado.

1.4.3. EVALUACION DE LAS COMUNICACIONES

Antes de proceder a analizar en que consiste la evaluación de las comunicaciones, es importante saber los componentes de una red de comunicaciones, a fin de situar el propósito de la evaluación:

RED: Es un conjunto de computadoras, periféricos y otros recursos interconectados entre sí, para ser utilizados en forma conjunta o independiente, que cuenta con un conjunto de direcciones, las cuales permiten compartir recursos de hardware ó Software, además de recibir, transmitir e intercambiar información entre ellas.

Los elementos básicos de una red, según los diversos criterios son:

- **SERVIDOR DE ARCHIVOS.** Dispositivo que permite compartir todos los recursos que se encuentran en su ó sus discos duros.

- **ESTACION DE TRABAJO.** Son todas aquellas microcomputadoras que están integradas a la Red y desde las cuales un usuario puede utilizar los recursos disponibles en la misma.

- **MEDIO FISICO DE INTERCONEXION.** Este medio físico realiza una interconexión e interfaz con la Red por medio de un cable que permita a las estaciones de trabajo y a los servidores integrarse a una Red y comunicarse entre sí.

- **TARJETAS DE INTERFACES DE RED**. En cada nodo de Red, ya sea estación de trabajo o servidor, se debe contar con una tarjeta de red la cual realiza la función principal de trabajar como una interfaz entre los diferentes nodos de la Red.

- **SISTEMA OPERATIVO LOCAL.** Este sistema operativo administra los recursos de las estaciones de trabajo.

- **SISTEMA OPERATIVO DE RED.** Es el encargado de administrar los recursos de la Red.

La seguridad está relacionada con la comunicación interna y externa de los sistemas.

Algunos de los elementos a evaluar en la protección de las comunicaciones son:

- Diseñar protocolos y rutinas de comunicación y verificación de transmisiones.
- Establecer los medios formales de comunicación de datos, ya sean internamente o por medio de redes de cómputo.
- Mantenimiento periódico de los medios de comunicación.
- Utilización de los sistemas de comunicaciones necesarios, de acuerdo a con los requerimientos del sistema y los medios de transmisión.
- Identificar problemáticas de recepción/transmisión de datos y medios para corregirlos.
- Prevenir la entrada de virus informático, mediante la recepción de datos.
- Rutinas y protocolos de autentificación de protocolos de comunicación, dispositivos de transmisión y envío de información.

I.5. METODOLOGIA DE AUDITORIA INFORMATICA

Según el diccionario de la Lengua Real Académica Española, **METODO** es el "**modo de decir o hacer con orden una cosa".** Asimismo define el diccionario la palabra **METODOLOGIA** como **"Conjunto de métodos que se siguen en una investigación científica o en una exposición doctrinal".** Esto significa que cualquier proceso científico debe de estar sujeto a una disciplina de producción definida con anterioridad que llamaremos Metodología.

Se tiene la idea de que la Informática es una materia compleja en todos sus aspectos, por lo que se hace necesaria la utilización de las metodologías en cada una de sus áreas que la componen, desde su diseño de ingeniería, hasta el desarrollo del software, y desde luego, **la auditoría de los sistemas de información.**

Las metodologías usadas por un profesional dicen mucho de su forma de entender su trabajo, y están directamente relacionados con su experiencia profesional acumulada como parte del comportamiento humano de "acierto/error".

Asimismo una metodología es necesaria para que un equipo de profesionales alcance un resultado homogéneo tal como si lo hiciera uno sólo, por lo que resulta habitual el uso de metodologías en las empresas auditoras/consultoras profesionales, desarrolladas por los más expertos, para conseguir resultados homogéneos en equipos de trabajo hetereogéneos.

Las únicas metodologías que podemos encontrar en la auditoría informática son dos familias distintas: **las auditorías de Controles Generales** como resultado estándar de las auditorias profesionales, que son una homologación de los mismos, a nivel internacional y **las Metodologías de los Auditores Internos.**

El objetivo de las auditorías de controles generales es "dar una opinión sobre la fiabilidad de los datos de la computadora para auditoría financiera". El resultado es un escueto informe como parte del informe de auditoría, donde se

destacan las vulnerabilidades encontradas. Están basados en pequeños cuestionarios estándares que dan como resultado informes muy generales.

Las metodologías están muy desprestigiadas, pero no porque sean malas en sí mismos, sino porque dependen mucho de experiencia de los profesionales que los usan y existe una práctica de utilizarlos profesionales sin ninguna experiencia.

Algunas metodologías no usan ayudas de contramedidas, llegando a la aberración de que se utilizan metodologías de análisis de riesgo para hacer auditorías.

Todas estás anomalías nacen de la dificultad que tiene un profesional sin experiencia aun la función de auditar y busca una fórmula fácil que le permita empezar su trabajo rápidamente. Esto es una utopía. El auditor informativo necesita una larga experiencia tutelada y una gran formación tanto auditora como informática. Y esta formación debe ser adquirida mediante el estudio y la practica supervisada.

Llegamos el punto en el que es necesario decir que la metodología del auditor interno debe ser diseñada y desarrollada por el propio auditor, y esta será de su grado de experiencia y habilidad.

A continuación se propone una metodología de Auditoría Informática.

I.5.1. ESTUDIO PRELIMINAR

Para obtener una idea del trabajo a realizar, estimar el riesgo, planificar y ejecutar una auditoría efectiva y eficiente, es indispensable que obtengamos una compresión clara del negocio del cliente, lo cual requiere un contacto preliminar para:

- Obtener datos que nos permitan percibir rápidamente las estructuras fundamentales.

- Detectar diferencias principales entre el organismo a auditar y otras organizaciones que se hayan investigado anteriormente.

- Identificar las áreas significativas de auditoría, incluyendo aquellas que pueden presentarnos problemas.

- Juzgar el entorno del control.

- Identificar transacciones inusuales o inesperadas.
- Conocer la estructura organizacional y principalmente de las funciones de procesamiento de información.

- Identificar los elementos que están siendo producidos (para establecer el grado de conformidad con las normas y especificaciones del negocio).

- La documentación, reportes y archivos. Nos permiten identificar las áreas que sean de alto riesgo y por ello puedan requerir un mayor énfasis en la auditoría, así mismo también se localizarán las áreas de bajo riesgo, en donde se minimice el esfuerzo de auditoría.

Se realizaran entrevistas preliminares, observaciones y solicitudes de documentos, para ampliar la visión general del negocio y poder definir el objetivo y alcances de este.

Uno de los primeros pasos en la planeación, es el establecer los Objetivos de la auditoría. Frecuentemente las auditorías se basan en ideas plasmadas solo en la mente, lo que no sólo provoca desperdicios de recursos si no pérdidas de sensibilidad.

Al establecer los objetivos de la auditoría, debe tomar en cuenta las siguientes preguntas:

- ¿ Se establecieron los objetivos generales de la auditoría al inicia del proceso de planeación?

- ¿Tiene la organización procedimientos para establecer los objetivos específicos de la auditoría a partir de los objetivos generales?

- ¿ Se han establecido criterios de medición para los objetivos específicos?

- Cómo parte del proceso de planeación ¿ se han hecho juicios que consideren lo que se deberá hacer si en las pruebas de auditoría quedan insatisfechos completamente los objetivos de la misma?

Los objetivos específicos de la auditoría no deben limitar la iniciativa del auditor a explorar áreas de conocimiento. Los objetivos específicos se determinan durante la planeación y pueden ser cambiados durante la implantación de la auditoría.

La documentación de un sistema deberá ser actualizada cuando sus especificaciones cambian, los objetivos específicos de la auditoría deberán ser actualizados cuando cambien los planes de auditoría durante la implantación de segmentos de está.

Algunas de las razones para usar tiempo y esfuerzo en el desarrollo de objetivos específicos para la auditoría de sistemas son:

- Ordenes para el grupo auditor.
- Análisis de datos económicos.
- Medidas de auditoria.
- Límites y alcances.
- Identificación de procesos de datos conocidos.
- Identificación de técnicas de auditoría.

La cuantificación del conocimiento o desconocimiento de los riesgos, forma las primeras bases para el establecimiento de objetivos específicos de

auditoría. Una segunda consideración en el establecimiento específico son los juicios.

Estos se basan en:

- Conocimientos del negocio
- Conocimiento de la aplicaciones computacionales.
- Discusiones que involucran al personal.
- Aplicación de historia anteriores.
- Partes concernientes a terceros o complementarias.
- Concernientes de la administración general.
- Concernientes a los usuarios.
- Intuición del auditor.
- Resultados de otras auditorías.

PROCEDIMIENTOS PARA ESTABLECER OBJETIVOS ESPECIFICOS

El proceso para establecer objetivos específicos de auditoría se muestra en los siguientes cinco pasos:

Paso 1: Identificación de riesgos incluidos en la auditoría.

Paso 2: Determinar los riegos considerados confidenciales.

Paso 3: Determinar los objetivos específicos de la auditoría.

Paso 4: Desarrollar criterios y medidas que complementen los objetivos específicos.

Paso 5: Evaluación de los objetivos específicos no alcanzados.

ALCANCES

Cada organización auditada desarrolla anualmente un plan el cual identifica las áreas auditadas y objetivos para llevar a cabo la auditoría. Los alcance se aprenden con la experiencia del auditor. Desarrolla más rápidamente cada uno de los pasos así como las políticas que deben seguir los procedimiento y métodos de procesamiento de información bajo un sistema.

Los alcances envuelven las siguientes cuatro etapas:

Bajo que situación se establecen los objetivos a auditar. El auditor necesita conocer bajo que condiciones puede llevar a cabo los objetivos y así como, la descripción de la hoja de trabajo.

- Los objetivos del auditor normalmente describen la hoja de trabajo. Estos objetivos se desarrollan para realizar auditorías anualmente.

Definir los alcances de asignación. En donde se llevará a cabo la auditoría y recomendaciones o limitaciones de la auditoría.

En los alcances de auditoría de sistemas de información hay cuatros efectos que son:

- Tiempo
- Talento
- Herramientas
- Viajes.

Reunión de Conferencia. Llevar a cabo conferencia con el auditor para determinar los requerimientos y establecer los grupos de trabajo para auditar.

Obtener información atrasada. A través de visitas constantes, entrevistas y documentación, el auditor obtendrá información para la auditoría y la relación con las funciones de procesamiento de datos. Esta información va hacer propia del auditor para su propio negocio y perspectivas de control.

En la Auditoría en Informática los alcances del proyecto comprenden:

1. **Evaluación de la dirección de informática en lo que corresponde a:**
   - Su organización.
   - Estructura
   - Recursos humanos
   - Normas y políticas
   - Capacitación
   - Planes de trabajo
   - Controles
   - Estándares

2. **Evaluación de los sistemas**
   - Evaluación de los diferentes sistemas en operación (flujo de información, procedimientos, documentación, redundancia, organización de archivos, estándares de programación, controles, utilización de los sistemas).

- Evaluación de avance de los sistemas en desarrollo y congruencia con el diseño general.
- Evaluación de prioridades y recursos asignados (humanos y equipos de cómputo).
- Seguridad física y lógica de los sistemas, su confidencialidad y respaldos.

3. Evaluación de los equipos

- Capacidades
- Utilización
- Nuevos proyectos
- Seguridad física y lógica
- Evaluación física y lógica.

ESTRATEGIAS

Cuando en una instalación se encuentren operando sistemas avanzados de computación como procesamiento en línea, bases de datos, sistemas avanzados de computación y procesamiento distribuido, se podría evaluar el sistema empleando técnicas avanzadas de auditoría. Estos métodos requieren un experto y por lo tanto, pueden no ser apropiados si el departamento auditamiento no cuenta con el entrenamiento adecuado. Otra limitante, incluyendo el costo, puede ser la sobrecarga del sistema y la degradación en el tiempo de respuesta. Sien embargo, cuando se usan apropiadamente, estos métodos superan la utilización en una auditoría tradicional.

MÉTODOS DE AUDITORÍA

- **PRUEBAS INTEGRALES.** Consiste en el procesamiento de datos de un departamento ficticio, comparando estos resultados con otros predeterminados. En otras palabras, las transacciones iniciadas por el auditor son independientes de la aplicación normal, pero son procesadas al mismo tiempo. Especial cuidado se debe tener con las participaciones que se está utilizando en el sistema para prueba de la contabilidad o balance a fin de evitar situaciones anormales.

- **SIMULACION.** Consiste en desarrollar programas de aplicación para determinar pruebas y comparar los resultados de la simulación con la aplicación real.

- **EVALUACION DE UN SISTEMA CON DATOS DE PRUEBA.** Esta verificación consiste en probar los resultados producidos en la aplicación con datos de prueba contra los resultados que fueran obtenidos inicialmente en las pruebas del programa (solamente aplicable cuando se hacen modificaciones a un sistema).

- **REGISTROS EXTENDIDOS.** Consiste en agregar un campo de control a un registro determinado como un campo especial a un registro extra, que pueda incluir datos de todos los programas de aplicación que forman parte del procesamiento transacción, como en los siguientes casos.

- **TOTALES ALEATORIOS DE CIERTOS PROGRAMAS.** Se consiguen totales en algunas partes del sistema para ir verificando su exactitud en forma parcial.

- **SELECCIÓN DE DETERMINADOS TIPOS DE TRANSACCION COMO AUXILIAR EN EL ANALISIS DE UN ARCHIVO HISTORICO.** Por medio de este método podemos analizar en forma parcial el archivo histórico de un sistema, el cual sería casi imposible de verificar en forma total.

- **UNO O MAS DE LOS MANUALES DE PROCEDIMIENTOS QUE CONTIENEN INFORMACION RELATIVA A LAS TRANSACCIONES DEL SISTEMA.** Estos manuales guían a la gente en la circulación y proceso de las transacciones. En las aplicaciones automatizadas, pueden ser listados de programas de computadora, listados de diccionarios de datos y documentación de proveedores.

Otra técnicas que se utilizan son:

- Lluvia de ideas.
- Lote de datos prueba.
- Datos de prueba integrados a los sistemas en producción.
- Simulación paralela.
- Procesamiento duplicado
- Evaluación de casos base
- Imagen del contenido de la memoria.

- Imagen del contenido de la memoria.
- Módulos de auditoría integrados.
- Prueba de sistemas en línea.
- Seguimiento o rastreo
- Libro diarios o consecutivo
- Exploración/balance de archivos.
- Verificación del estudio de los programas mediante el estudio de los propios programas.
- Correlación.

I.5.2 ADMINISTRACION

REQUERIMIENTOS

Recursos Materiales

- Documentación
- Políticas de uso de equipos
- Políticas de operación.
- Inventario de los equipos características y localización de cada uno de ellos
- Contratos vigentes de compras, renta, servicio de mantenimiento y de seguros.

Instalaciones

- Ubicación general de los equipos (mapas de distribución).
- Un área reservada para el trabajo del grupo auditor.

Hardware

- Configuración de los equipos y capacidades actuales y máximas.
- Fechas de instalación de los equipos y planes de instalación.

Software

- Los sistemas en desarrollo
- Los sistemas desarrollados y que están en operación

Recursos Humanos

Elementos de gran importancia en cualquier área de una empresa, y especialmente en el AREA INFORMATICA, ya que los conocimientos del personal contratado en la empresa, dependerá de que tan eficientes y eficaces sean. A continuación se proponen los puestos que podrían formar un centro de cómputo.

DIRECTOR (A) DEL AREA DE INFORMATICA

OBJETIVOS

Dirección y control de informática y el establecimiento de las necesidades de la información a corto plazo.

FUNCIONES

- Definir y controlar el presupuesto y los medios necesarios para el área.
- Interpretar las necesidades y la política de la dirección, sugerir los campos de aplicación útiles para el organismo y dar a conocer el plan de desarrollo a largo plazo.

- Preparar los proyectos con los usuarios, vigilando que los trabajadores se integren de un modo apropiado.

SECRETARIA

OBJETIVOS

Construir el apoyo eficaz para el desarrollo de las tareas administrativas dentro del área.

FUNCIONES

- Controlar la correspondencia de la unidad y canalizar a quien corresponda.
- Atender a las personas que se dirijan a la unidad.
- Control de la documentación de la unidad a través de un archivo actualizado de expedientes.

GERENTE DE SOPORTE TÉCNICO

OBJETIVOS

- Administrar y coordinar su gerencia, administrando los recursos humanos disponibles para el desarrollo adecuado de sus funciones y así mismo, proporcionar la ayuda técnica necesaria a los demás departamentos en el desarrollo de sus aplicaciones.
- Supervisar y controlar el mantenimiento de las computadoras así como el desarrollo de aplicaciones que se elaboran en estas.
- Supervisar la seguridad de todos los recursos que son utilizados en el área de informática (hardware). Así mismo la correcta aplicación de los

estándares existentes para el área y vigilar la debida actualización de la documentación de cada sistema.

- Actualizar mediante manuales, instructivos, cursos internos y externos y toda la información que llegue a sus manos, relacionada con su área y con la compañía.

FUNCIONES

- Mantenerse al día en cuanto a procesos y estándares del departamento.
- Detectar y analizar inmediatamente cualquier problema a nivel, ya sea de comunicación, equipo, etc.
- Auxiliar en la selección, capacitación e inducción del personal del área y los costos, asegurándose que su personal los conoce y acepta.

JEFE DE SECCION DE PRODUCCION

OBJETIVOS

Coordinar y supervisar el procesamiento de los sistemas implementados.

FUNCIONES

- Establecer los estándares y los procedimientos del funcionamiento del equipo.
- Verificar la calidad y la eficacia.
- Aprobar las necesidades para la ejecución de cada trabajo. Rechazar aquellos que no respondan a las especificaciones inicialmente previas.

- Planificar la carga de las máquinas y el trabajo del personal de ejecución, a fin de obtener el máximo rendimiento del equipo y proporcionar el mejor servicio a los usuarios.

JEFE DE TELEPROCESO Y TELECOMUNICACIONES

OBJETIVOS

Coordinar y supervisar el mantenimiento y comunicación entre las computadoras y terminales para lograr que el servicio sea congruente en los horarios establecidos.

FUNCIONES

- Elaborar un plan de mantenimiento detallado d la computadora y sus periféricos para obtener la máxima disponibilidad.
- Elaborar un plan de mantenimiento específico para mantener la computadora en condiciones óptimas ambientales y de limpieza.
- Establecer las estrategias de operación, tanto del computador principal como de sus periféricos y determinar los turnos de servicio.

PROGRAMADOR DE SISTEMAS "A"

OBJETIVOS

Implementación del software y hardware.

FUNCIONES

- Realizará diseños prácticos de cómo el software propuesto debe ser implementado.
- Debe desarrollar software mediante el uso de manuales que sirvan como guía de desarrollo para los programadores. Debe además específicar parámetros de generación de versiones de versiones de sistemas operativos, así como sus correspondientes pruebas.

PROGRAMADOR DE SISTEMAS "B"

OBJETIVOS

Implementación de software y hardware.

FUNCIONES

- Debe manejar especificaciones internas, diagramas de flujo, preparar el código de instrucciones de operación.
- Cuando se desarrolle un nuevo software darle mantenimiento. Además debe preparar un plan de prueba, datos y resultados predeterminado para subsecuentemente probarlos.
- Catalogar procedimientos y utilerías.

GERENTE DE DESARROLLO Y MANTENIMIENTO DE SISTEMAS

OBJETIVOS

Es el responsable de mantener permanentemente la disponibilidad el software en condiciones que permitan la operatividad de las unidades usuarias, además de cumplir con la liberación de sistemas en los tiempos programados.

FUNCIONES

- Estructura los planes de servicio requeridos por los usuarios.
- Desarrollo de planes físicos considerando los espacios con los que cuentan, ubicación de equipo, configuraciones adecuadas e instalaciones físicas de acondicionamiento ambiental.
- Evaluación de la funcionalidad de los métodos de trabajo establecidos, regula las deficiencias detectadas.

JEFE DEL DEPARTAMENTO ANALISIS Y DISEÑO DE SISTEMAS

OBJETIVOS

Supervisión, coordinación en la implementación de sistemas.

FUNCIONES

- Sugerir e implementar los cambios cuando sean requeridos según el desarrollo del sistema.
- Identificar necesidades del personal y evaluar sus suministro.

- Dirigir y supervisar el análisis de los sistemas a implantar o modificar.

LIDER DE PROYECTO

OBJETIVOS

Coordinar el desarrollo de un sistema en todos sus aspectos, diseñar las partes componentes del mismo y supervisar su integración y desarrollo.

FUNCIONES

- Definir los requerimiento para crear, optimizar o reemplazar los sistemas.
- Desarrollar el diseño de los sistemas que sean requeridos.
- Supervisar la implementación de los sistemas.

ANALISTA DE SISTEMAS "A"

OBJETIVOS

Analizar los sistemas que habrán de desarrollarse e implementarse, como resultado de las necesidades existentes.

FUNCIONES

- Elaborar análisis de requerimientos.
- Elaborar el análisis general de los sistemas que se le asignen.
- Evaluar los resultados de las pruebas de los programas y revisar que se cumplan con los objetivos fijados en el sistema.

ANALISTA DE SISTEMAS "B"

OBJETIVOS

Auxiliar en las tareas de análisis y diseño de sistemas de cómputo.

FUNCIONES

- Elaborar el análisis y diseño de algunos de los módulos o subsistemas del sistema general.
- Diseñar el flujo general de los mismos, asegurándose de cumplir los estándares establecidos para todo el sistema.
- Definir " Archivos de Prueba" siguiendo las indicaciones planteadas, para revisar los módulos desarrollados.

JEFE DEL DEPARTAMENTO DE MANTENIMIENTO DE SISTEMAS

OBJETIVOS

Supervisión, coordinación y auditoría de sistemas.

FUNCIONES

- Sugerir e implementar los cambios cuando sean requeridos según el desarrollo del sistema.
- Identificar necesidades del personal y evaluar sus suministro.
- Estimar los requerimientos humanos y técnicos para el desarrollo de los proyectos.

JEFE DE CAPTURA

OBJETIVOS

Coordinar y supervisar la captura de datos.

FUNCIONES

- Establecer y revisar los estándares en cuanto a captura de datos.
- Rechazar a aquellos que no respondan a las especificaciones inicialmente previstas.
- Planificar la carga de trabajo, a fin de obtener el máximo rendimiento para la captura de datos.

CAPTURISTA "A"

OBJETIVOS

Realizar la captura de la información.

FUNCIONES

- Cumplir con los estándares en cuanto a captura de datos.
- Registrar los trabajos desarrollados, su tiempo de recepción y entrega.
- Capturar la información y anotar las anomalías que detecte tanto en la información como en el equipo utilizado.

CAPTURISTA "B"

OBJETIVOS

Colaborara en las tareas de captura de información.

FUNCIONES

- Cumplir con los estándares en cuanto a captura de datos.
- Capturar la información que le sea asignada y registrar dicha captura.

JEFE DEL DEPARTAMENTO DE DOCUMENTACION DE SISTEMAS

OBJETIVO

Coordinar y supervisar la captura de datos.

FUNCIONES

- Establecer y revisar los estándares en cuanto a captura de datos, seguridad, desarrollo de sistemas, normatividad, etc.
- Documentación de sistemas liberados.
- Actualización de manuales de acuerdo a las modificaciones realizadas en los sistemas.

OPERADOR DE SOFTWARE "A"

OBJETIVOS

Es responsable de operar cada sistema de acuerdo con el control establecido.

FUNCIONES

- Documentar los sistemas mediante manuales bien estructurados y ejemplificados con las gráficas necesarias para la mejor interpretación de los sistemas por parte de los analistas.
- Llevar el control de las modificaciones realizadas a cada uno de los sistemas, fecha y autor de la modificación.

NORMAS DE AUDITORIA

Generalidades

La auditoría es una actividad profesional. En este caso implica, al mismo tiempo, el ejercicio de una técnica especializada y la aceptación de una responsabilidad pública.

La dificultad que representa resolver el problema de la calidad del trabajo profesional mediante establecimientos mínimos obligó a las organizaciones profesionales que tienen relaciones con la actividad profesional de los auditores, a buscar otro camino por el cual fuera posible asegurar el suministro del servicio de auditor sobre bases mínimas de calidad satisfactorias para las personas que dependerían de los servicios del auditor independiente. Sobre esa corriente de ideas se llegó al convencimiento de que, si bien no es posible establecer procedimientos uniformes mínimos para la auditoría, sí en cambio, existen ciertos fundamentos que son la base e inspiración de los propios procedimientos de auditoría y que pueden ser definidos en términos generales. A estos fundamentos básicos del trabajo de auditoría se les llama: **"Normas de Auditoría".**

DEFINICION

"Las normas de auditoría son los requisitos mínimo de calidad relativos a la personalidad del auditor, al trabajo que desempeñan y a la información que rinden como resultado de este trabajo".

NORMAS DE AUDITORIA

Las normas de auditoría se clasifican en:

a) Normas Personales
b) Normas de ejecución del trabajo
c) Normas de Información.

- **Normas personales**

Las normas personales se refieren a las cualidades que el auditor debe tener para poder asumir, dentro de las exigencias que el carácter profesional de la auditoría impone, un trabajo de este tipo. Dentro de estas existen cualidades que el auditor debe tener preadquiridas antes de poder asumir un trabajo profesional de auditoría y cualidades que debe mantener durante el desarrollo de toda sus actividad profesional.

Entrenamiento técnico y capacidad profesional

El trabajo de auditoría, cuya finalidad es la de rendir una opinión profesional independiente, debe ser desempeñado por personas, que teniendo título profesional legalmente expedido y reconocido, tengan entrenamiento técnico adecuado y capacidad profesional como auditores.

Cuidado y diligencia profesionales

El auditor obligado a ejercitar con cuidado y diligencias razonables en la realización de su trabajo y en la preparación de su dictamen o informe.

Independencia

El auditor está obligado a mantener una actitud de independencia mental en todos los asuntos relativos a su trabajo profesional.

- **Normas de ejecución del trabajo**

Aún cuando es difícil definir lo que en cada tarea puede representar un cuidado y diligencia adecuadas, existen ciertos elementos que por su importancia, deben ser cumplidos. Estos elementos básicos, fundamentales en la ejecución del trabajo, que constituyen la especificación particular, por lo menos al mínimo indispensable, de la exigencia de cuidado y diligencia, con los que constituye las normas denominadas de ejecución del trabajo.

Planeación y supervisión

El trabajo de auditoría debe ser planeada adecuadamente y si se usan ayudantes, éstos deben ser supervisados y capacitados en forma apropiada.

Estudio y evaluación del control interno

El auditor debe efectuar un estudio y evaluación adecuados del control interno existente, que le sirven de base para determinar el grado de confianza que va a depositar en él; así mismo, que le permita determinar la naturaleza, extensión y oportunidad que va a dar a los procedimientos de auditoría.

Obtención de evidencia suficiente y competente

Mediante sus procedimientos de auditoría, el auditor debe de obtener comprobatoria suficiente y competente en el grado que requiera para suministrar una base objetiva para su opinión.

- **Normas de Información**

El resultado final del auditor es su dictamen o informe. Mediante él, pone en conocimiento de las personas interesadas los resultados de su trabajo y la opinión que se ha formado a través de su examen. El dictamen o informe del auditor es en lo que va a reposar la confianza de los interesados de la empresa. Por último, es principalmente, a través del informe o dictamen, como el público y el cliente se dan cuenta del trabajo del auditor y en muchos casos, es la única parte de dicho trabajo que queda a su alcance.

PERSONAL PARTICIPANTE

AUDITOR LIDER

Es aquel individuo calificado cuya experiencia y entrenamiento le permiten organizar y dirigir una auditoría, reportar deficiencias o desviaciones, así como evaluar y orientar acciones correctivas. En el caso de auditorías efectuadas por un grupo, además de ser el responsable de la auditoría.

AUDITOR EN ENTRENAMIENTO

Es aquel individuo aspirante a obtener la clasificación de auditor, el cual acompaña y auxilia al grupo auditor durante todas las etapas de una auditoría y

recibe la orientación y entrenamiento adecuado para tal fin, mediante la coordinación y dirección de un auditor líder.

GRUPO AUDITOR

Es el conjunto de individuos que se integran para realizar una auditoría de calidad bajo la dirección de un auditor líder.

Actualmente se cuenta con más elementos para definir el conjunto de conocimientos y habilidades que es necesario desarrollar por los individuos que pretenden integrarse a esta especialidad.

El paquete de conocimientos básicos que debe tener un auditor en informática se deberá ampliar constantemente de acuerdo con las características de la misma empresa, ya que el grado de tecnología, la centralización de las funciones de sistemas, el medio ambiente y muchos factores más, fijan las áreas de conocimiento requerido así como su profundidad y especialización.

I.5.3. NEGOCIACION

CONTRATO

Una vez que se haya establecido como se va a llevar a cabo la auditoría, se estará en posibilidad de presentar el plan de trabajo.

Es importante que exista un claro entendimiento tanto del auditor como de su cliente, de los términos y alcances de cualquier trabajo de auditoría, con objeto de evitar, hasta donde sea posible, confusiones o malas interpretaciones

respecto de los derechos y obligaciones de cada una de las partes. Una carta del auditor a su cliente documentada, confirma la presentación del servicio, el objeto y alcance del mismo, el grado de responsabilidad que asume y clase de informes que debe proporcionar.

Generalmente se llega a un primer acuerdo con el cliente en una reunión en donde se comentan los detalles del servicio que prestará. Posteriormente es recomendable que el acuerdo inicial se confirme por medio de una carta que el auditor envíe a su cliente.

OBJETIVO

El objetivo es auxiliar al auditor en la preparación de cartas para confirmar a sus clientes la presentación de sus servicios de auditoría.

CONTENIDO DE LA CARTA

Generalmente se conoce como carta compromiso de auditoría y su forma y contenido puede variar en cada caso particular, sin embargo, deberá hacer referencia a los siguientes aspectos:

- El objetivo y alcance de la auditoría incluyendo una referencia a los pronunciamientos.
- Solicitud al cliente que confirme su aceptación del servicios en los términos de la carta firmando y regresando al auditor una copia de la misma.
- Los informes que el auditor emitirá como resultado de su trabajo.
- Bases sobre las cuales se calcularán sus honorarios y gastos, su importe y arreglos en cuanto a su forma de pago.

- El hecho de que los procedimientos de auditoría no están diseñados específicamente para descubrir errores e irregularidades.
- Participación de especialistas en ciertos aspectos de la auditoría.
- El estudio y evaluación del control interno como parte de la auditoría.
- El estudio y evaluación del control interno como parte de la auditoría.
- Fechas acordadas para desarrollar el trabajo, entrega de informes, etc.
- El libre acceso a los registros, documentación y cualquier información relacionada con la auditoría, incluyendo la utilización de equipo de cómputo.
- Descripción de otros informes y cartas que espera emitir.

Cuando el auditor de la empresa tenedora o principal es también auditor de alguna entidad relacionada, deberá tomar en cuenta los factores que a continuación se indican para determinar si procede enviar una carta de compromiso por separado a la entidad relacionada.

- Quién designa al auditor de la entidad relacionada.
- Si se va a emitir un dictamen por separado de la entidad relacionada.
- El alcance de cualquier trabajo efectuado por otros auditores.

ALCANCES Y LIMITACIONES

Esto se refiere exclusivamente a los procedimientos de auditoría que se puede aplicar cuando se decide utilizar el trabajo de especialista. Un especialista es la persona o firma que posee conocimientos técnicos y

experiencia en un determinado campo de acción y puede ser contratado tanto por el cliente o por el auditor.

No es aplicable a la utilización del trabajo de un especialista que forma parte del equipo profesional del auditor, ya que este caso queda cubierto en las disposiciones normativas relativas al de calidad y planeación y supervisión del trabajo de auditoría.

Para establecer los procedimientos de auditoría que se consideran adecuados para la revisión del trabajo de especialista son los siguientes:

a) Conocer los eventos o transacciones que hayan requerido o requerirán del trabajo de un especialista, dando consideración a :
   - Cualquier evidencia de auditoría con que ya se cuente.
   - La naturaleza y complejidad del asunto, incluyendo el riesgo de error inherente.

Control Interno

La revisión, estudio y evaluación de la efectividad del control interno deberá dirigirse principalmente a los siguientes aspectos:

a) **Aprobación por parte de la administración del especialista seleccionado.** Es responsabilidad de la administración la selección y designación del especialista que estará autorizado para desempeñar determinado trabajo, así como de que éste cuente con la capacidad necesaria que garantice resultados satisfactorios.

b) **Comunicación con el especialista.** Debe existir un claro entendimiento, preferentemente por escrito sobre la naturaleza del trabajo de este último cubriendo entre aspectos, siguientes:

- Objetivos y alcances de trabajo.
- Forma y contenido del producto terminado que permita evaluarse y servir como evidencia del evento o transacción involucrado.

Métodos y supuestos que se aplicarán, en su caso, consistencia con los empleados en el año anterior.

c) **Independencia del especialista.** Es altamente deseable que el especialista sea una persona o firma independiente del cliente, a fin de obtener mayor confianza de que su trabajo será ejecutado con total imparcialidad; sin embargo, cuando las circunstancias no lo permitan, se puede usar el trabajo de un especialista que tenga relaciones con el cliente, pero el auditor debe de considerar la necesidad de aplicar los procedimientos adicionales de auditoría en la relación a parte o la totalidad de los supuestos métodos o resultados del trabajo del especialista para determinar que los resultados sean razonables o contratar un especialista para tal propósito.

d) **Revisión o análisis de los resultados.** Dado que los resultados del trabajo de un especialista podrían repercutir en la información, la empresa tiene la obligación de comprobar que el trabajo se desarrollo conforme a lo acordado y que, en su caso, el especialista se basó en los datos o elementos objetivos suministrados por la empresa.

I.5.4. RESULTADOS

INFORME

Es la presentación de las conclusiones de la auditoría y podrá realizarse en la siguiente forma:

a) **INFORME EJECUTIVO.** Es "una breve descripción de la situación actual en la cual se reflejen los puntos más importantes", a través de cuadros estadísticos, gráficas, matrices de decisión, etc. "Se debe romper la resistencia a la lectura que tienen algunos ejecutivos por medio de conclusiones concretas que sean sencillas (se procurará que se entiendan los términos técnicos y si es posible, usar técnicas audiovisuales).

b) **INFORME DETALLADO**

El cual comprende:

- Los problemas detectados
- Posibles causas, problemas de fallas que originaron la situación presentada.
- Repercusiones que pueden tener los problemas detectados.
- Alternativas de solución.
- Comentarios y observaciones de la dirección de informática y de los usuarios sobre las soluciones propuestas".

- Si se opta por alguna alternativa de solución, cuáles son las repercusiones, ventajas y tiempo estimado para efectuar el cambio.

c) **SOPORTE.** Si se detectaron problemas, presentar los documentos como evidencia comprobatoria.

DICTAMEN DEL AUDITOR

El dictamen del auditor es el documento formal que describe el mismo conforme a las normas de su profesión, relativo a la naturaleza, alcance y resultado del examen realizado del que se trate. La importancia del dictamen en la práctica profesional es fundamental, ya que usualmente es lo único que el público conoce de su trabajo. El público como proveedores, acreedores, autoridades, etc. Conocen las formas usuales de dictámenes de los auditores, de modo que una desviación sustancial de esos modelos requiere una explicación clara del motivo que la origina.

La opinión del auditor, por ser independiente a la administración de la empresa, es el resultado de la aplicación de normas que controlan la calidad que debe reunir la información que emite.

OBJETIVOS

Es establecer la forma y contenido del dictamen que debe rendir al auditor al término de su examen practicado con las normas de auditoría generalmente aceptadas y describir las modificaciones a dicho documento cuando exista limitaciones en el alcance del trabajo y/o desviaciones. Así mismo, se refiere a aquellos casos en que el auditor considera necesario incluir un párrafo de énfasis en su dictamen.

- **Pronunciamiento generales relativos al dictamen**
  - A quién debe dirigirse el dictamen.
  - Redacción y firma del dictamen.
  - Fecha del dictamen.

- **Pronunciamientos relativos a asuntos que originan dictámenes**

En ocasiones el auditar no se encuentra en condiciones de expresar un dictamen sin salvedades, ya sea por existir desviaciones en la aplicación. Al existir cualquier excepción de importancia relativa, el auditor deberá emitir, según sea el caso, una opinión con salvedades, una abstención de opinión o una opinión negativa.

- **Dictamen de salvedades**

Cuando el auditor expresa una opinión con salvedades debe revelarse en uno o más párrafos, dentro del cuerpo del dictamen, todas las razones de importancia que las originaron e indicar inmediatamente después de la expresión "en opinión, la frase" excepto por" o su equivalente, haciendo referencia a dichos párrafos. Anexando los documentos que respalden las razones indicadas.

- **Dictamen con abstención de opinión**

El auditor debe abstenerse de expresar una opinión cuando el alcance de su examen haya sido limitado en forma tal, que procede la emisión de un dictamen con salvedades. En este caso, deberá indicar todas las razones que dieron lugar a dicha abstención.

- **Dictamen Negativo**

  El auditor debe expresar una opinión negativa o adversa cuando, como consecuencia de su examen. El hecho de expresar una opinión negativa, no eximirá al auditor de la obligación de mencionar todas las salvedades derivadas de limitaciones que hayan tenido en el alcance de su trabajo.

CAPITULO II. LA SEGURIDAD INFORMATICA

Objetivo: Definir los conceptos básicos de la auditoría de la seguridad dentro del entorno informativo con el propósito de integrarlos de manera armónica a las áreas.

II.1. CONCEPTOS GENERALES

Seguridad

"Calidad de seguro, locución que se aplica a un ramo de la Administración Pública cuyo fin es velar por el bien. Se aplica a ciertos mecanismos que aseguran el buen funcionamiento de algo".

Los sistemas de procesamiento y equipos de cómputo en general, el concepto de seguridad de informática o seguridad en los sistemas de información puede ser muy variado, incluso no existe un concepto generalizado y aceptado.

Seguridad Informática

Es la función de control o supervisión que permite a una corporación o institución conservar las características de integridad, confidencialidad y disponibilidad de sus sistemas de información junto con los otros recursos y tecnologías empleadas para reducir las únicas variables que afectan el escenario de seguridad: La amenaza y la vulnerabilidad convertidas en riesgos.

II.2. OBJETIVOS DE LA AUDITORIA EN SEGURIDAD

- Verificar la existencia de planes, políticas y procedimientos costo/beneficio de los controles y procedimientos de seguridad antes de ser implantados.
- Comprobar que los planes y políticas de seguridad y de repercusión sean difundidos y conocidos por la alta dirección.

- Asegurar que las políticas y procedimientos brinden confidencialidad a la información manejada en el procesamiento de datos electrónicos en su operación y mantenimiento.
- Asegurar que se brinde la seguridad necesaria a los diferentes equipos de cómputo existentes.
- Comprobar que existen contratos de seguro necesario para el hardware y software de la empresa requeridos para el funcionamiento continuo de las aplicaciones básicas.

II.3. CARACTERISTICAS DE LA SEGURIDAD INFORMATICA

Con base en las siguientes características de la seguridad en informática, podremos determinar que la información este segura.

II.3.1. Integridad

La integridad es básicamente el aseguramiento de que el sistema este funcionando correctamente y que se encuentre completo.

Los procedimientos de integridad también se aplican durante el procesamiento simultáneo de trabajos. El sistema deberá funcionar de tal forma que después de que se complete un trabajo autorizado, la información de dicho trabajo quede saneada (p. ej. borrada, tachada) de manera que las personas no autorizadas no la pueden leer.

Sin estos procedimientos de saneamiento, la información confidencial puede quedar expuesta a un acceso no autorizado en diversos puntos durante su procesamiento.

II.3.2. Confidencialidad

Es la necesidad de guardar información que no debe ser pública. Si todos los datos de las organizaciones y su información pudiera publicarse sin problemas, entonces no se tendría ninguna necesidad de guardar confidencialidad respecto a la información almacenada.

La confidencialidad permite asignar privilegios y facultades a los usuarios para consultar o procesar información de acuerdo a sus funciones y responsabilidades.

En ambientes de negocios, la confidencialidad asegura la protección de información, tales como datos de nómina, datos corporativos sensibles, tales como memorandúm internos y documentos de planeación estratégica.

II.3.3. Disponibilidad

Un sistema de cómputo seguro debe guardar información y mantenerla disponible a sus usuarios. La disponibilidad significa entonces que el hardware y software del sistema de cómputo trabajen eficientemente y que el sistema se puede recuperar rápida y completamente si un desastre ocurre.

Lo opuesto de la disponibilidad es la negociación del servicio. Esto significa que los usuarios del sistema estarán inhabilitados de los recursos que

ellos necesitan. La computadora pudo haberse saturado, en este caso no habrá suficiente memoria para procesar o para ejecutar un programa. Los recursos para almacenar en discos, grabar o las impresoras, pueden no estar disponibles.

II.4. PARTICIPANTES EN LA SEGURIDAD

ADMINISTRADOR DE RED

Debe de responsabilizarse de la óptima operación de la red, y ser capaz de determinar el impacto inmediato que puede tener si alguna amenaza se materializa. Además serán los responsables de asegurar que en las políticas de seguridad desarrolladas se lleven a cabo adecuadamente. Así como identificar y recomendar software para detección y limpieza del virus.

RESPONSABLES DE CADA AREA

Debe ser responsable de que la gente se dedique específicamente a las funciones que le han sido asignadas:

❖ PROPIETARIO

- Es la persona del área que apoye sus actividades de trabajo en cierta información.
- Deberá clasificar el nivel de importancia de la información.
- Deberá de identificar, de acuerdo a las políticas y normas establecidas, las medidas de seguridad a implementar.
- Deberá definir quien tiene acceso a su información.
- Deberá vigilar que el custodio con sus responsabilidades como:
    1. Evaluar y clasificar necesidades.

2. Definir controles.
3. Automatizar aplicaciones.
4. Monitorear y Validar aplicaciones.

- **CUSTODIO**

Deberá salvaguardar, manejar y distribuir la información de acuerdo a lo establecido por el propietario de la misma.

Sus responsabilidades deberán ser:

1. Salvaguardar la información.
2. Aplicar las medidas de seguridad establecidas por el propietario de la información.
3. Otorgar acceso y distribuir información de la manera pactada.
4. Dar asistencia técnica.
5. Administrar y proveer recursos.

- **USUARIO**

Deberá estar encargado de dar tratamiento y uso a la información de acuerdo a lo establecido por el dueño de la misma y conforme a sus funciones.

Sus responsabilidades deberán ser:

1. Utilizar la información de acuerdo a su responsabilidad y facultades otorgadas.
2. Proteger la información conforme a su nivel de clasificación y acorde a los expresado en las normas y políticas generales.
3. Reportar desviaciones o situaciones de excepción provocadas por un uso no autorizado de la información.

- Desde el diseño de la aplicación se deberá establecer un compromiso entre propietario y custodio para que las necesidades, condiciones, características, propuestas y avances consten por escrito.
- Toda aplicación deberá incluir controles y validaciones de seguridad en la etapas de entrada, procesamiento, salida, almacenamiento y recuperación de información.
- Toda las aplicaciones deberán ser auditables, cumpliendo con las características:
    1. Manuales de usuario y programador
    2. Toda la documentación que se genere en el desarrollo del sistema (necesidades, propuestas y avances).
    3. Lenguaje de alto nivel.
    4. Estándares y disciplinas de programación.
    5. Mantenimiento de datos prueba.
    6. Registro de seguridad.
- Toda aplicación deberá contar con los procedimientos de recuperación de errores en entrada, procesamiento, salida, almacenamiento y recuperación de la información.
- En todos los reportes impresos deberán numerarse las bajas y en la última de ellas, alguna leyenda que indique que es el final del trabajo.
- Toda aplicación debe ser capaz de comunicar cualquier mal funcionamiento anunciándolo debidamente en pantalla y/o reporte.
- Todos los procesos al terminar deberán mandar un mensaje indicando su terminación normal en pantalla.
- Toda aplicación debe identificarse con nombre y versión.

II.5. CONTROL INTERNO

"El control interno se refiere a las reglas y procedimientos que sigue alguien con el fin de mantenerse la integridad y seguridad de los datos, registros, activos financieros y otros de la organización".

Basándose en procedimientos que se tienen implantados de apoyarse con personal con que cuente, para lograr sus objetivos.

II.5.1. OBJETIVOS

El control interno consiste en el conjunto de medidas empleadas por la empresa con el propósito de:

- Prevenir fraudes.
- Descubrir robos y malversaciones.
- Obtener información administrativa, contable y financiera confiable y oportuna.
- Localizar errores administrativos, contables financieros.
- Proteger y salvaguardar los bienes, valores, propiedad y demás activos de la empresa.
- Promover la eficiencia del personal.
- Detectar desperdicios innecesarios de materiales, tiempo, etc.
- Mediante su evaluación, graduar la extensión del análisis, comprobación y estimación de las cuentas sujetas a auditoría.

II.5.2. IMPORTANCIA DEL CONTROL INTERNO

Todas las empresas públicas, privadas y mixtas, ya sean comerciales, industriales o financieras, deben de contar con instrumentos de control administrativos, tales como un buen sistema de contabilidad, apoyado por un catálogo de cuentas eficiente y práctico, deben de contar, además con un sistema de control interno, para confiar en los conceptos, cifras, informes y reportes de los estados financieros.

El auditor realiza un estudio y evalúa en forma adecuada el control interno existentes, que sirve de base determinar el grado de confianza que va a depositar en él.

II.5.3. ESTUDIO Y EVALUACION DEL CONTROL INTERNO

En el estudio del control interno existen dos posibilidades de determinar el alcance del estudio, cuando se efectúa una auditoría por primera vez a una empresa resulta conveniente efectuarlo totalmente abarcando todas los aspectos posibles en relación con el trabajo de auditoría en subsecuentes auditorías puede prepararse un plan, examinando en un año unos aspectos y en el año siguiente los aspectos restantes, completando siempre con ratificaciones generales a los aspectos en los que no se profundiza por el conocimiento anterior, o en los que hubiese mostrado cambios.

II.5.4. CONTROLES INTERNOS DE ENTRADA

Los recursos activos son aquellos que deben de revisarse durante el control de entradas.

- **DISPOSITIVOS DE ENTRADA.** Indica uno o todos los dispositivos de entrada usados para interconectar en el sistema de cómputo .

- **PROCEDIMIENTOS OPERATIVOS.** Señalan a los procedimientos escritos a seguirse durante la creación de, la preparación de, y la alimentación de datos al sistema de cómputo.

- **PERSONAL.** Indica a los individuos responsables de preparar y alimentar los datos, operar y mantener el equipo, seguir los procedimientos operativos, y ejecutar cualesquiera otras operaciones durante la alimentación de los datos al sistema de cómputo.

- **ARCHIVOS.** Señala los archivos manuales de los documentos fuente y a los datos una vez que éstos se almacenan en dispositivos magnéticos tales como cintas o discos magnéticos.

- **ALMACEN DE REGISTROS.** Señala el archivo a largo plazo de los documentos fuente o de otros tipos de datos o bien programas que pueden ser necesarios en determinado momento o en le futuro. Este recurso también incluye el almacenamiento a largo plazo de datos registrados en microformas.

- **FORMAS.** Indica cualesquiera de las formas especialmente preimpresas o diseñadas que pueden ser utilizadas antes o durante la alimentación de los datos al sistema de cómputo.

II.5.5. CONTROLES INTERNOS DE SALIDAS

Los siguientes recursos activos son aquellos que deben de ser comprobados, durante la revisión de los controles de las salidas.

- **DISPOSITIVOS DE SALIDA.** Son los dispositivos periféricos conectados al sistema de la computadora central y se refieren también a las clases de errores que se pueden cometer por este equipo. Todos los controles deben de revisar los dispositivos de salida, su uso normal, y cualquier documentación escrita que se refiera a ellos.

- **PERSONAL.** Hace referencia a los individuos responsables de conciliar los datos de salida, de operar y mantener los dispositivos de salida de escribir los procedimientos operativos, y de administrar la función de control de calidad de las salidas. Esto puede incluir también a los usuarios del departamento de personal.

- **ALMACENAMIENTO Y PRESCRIPCION DE LOS REGISTROS.** Indica el medio de almacenamiento de los datos de salida (copias o microfilms) así como la prescripción de los datos. Esto incluye la revisión de las técnicas de almacenamiento y disposición de los datos.

- **PROCEDIMIENTOS OPERATIVOS.** Son los procedimientos escritos que se refieren al cómo obtener los datos, a su verificación, conciliación, y a todos los aspectos del envío de los datos de salida del proceso (ya sea centralizado o distribuido) a los usuarios.

II.5.6. CONTROL DE SEGURIDAD FISICA

Elementos que deben de comprobarse durante la revisión del control físico.

- **ACTIVA ADMINISTRATIVA.** Señala la actitud de la administración con respecto a la seguridad a varios niveles y alrededor del servicio de proceso de datos.

- **CONSTRUCCION DE SERVICIOS.** Hace referencia la construcción de los servicios que rodean al recurso de proceso de datos y a los diversos componentes internos de tal servicio los cuales, tomados colectivamente, hacen que la operación de proceso de datos sea segura.

- **GENERADORES Y MOTORES ELECTRICOS.** Indica el suministro eléctrico para las operaciones de proceso de datos incluyendo a generadores especiales.

- **AIRE ACONDICIONAMIENTO Y AGUA HELADA.** Señala las capacidades de clima artificial para el sistema de cómputo. Como es sabido

un cambio en el clima artificial en algunos casos puede: inutilizar temporal o permanentemente, las operaciones de procesos de datos.

- **PLANES DE CONTIGENCIA.** Son los planes y las pruebas de los planes que se han de utilizar si hay una interrupción o desastre mayor, o una interrupción temporal del procesamiento.

- **PROGRAMAS DE ENTRENAMIENTO.** Se refiere al entrenamiento continuo de los empleados en la seguridad y confidencialidad.

- **PERSONAL.** Son los individuos responsables de las operaciones de proceso, programación, desarrollo y la corrida del sistema computarizado.

- **SEGURO.** Señala la cobertura del seguro que debe de adquirirse para compensar a la organización en caso de que ocurra un siniestro mayor u otra perturbación.

II.5.7. CONTROL DE COMUNICACIÓN DE DATOS

- **SOFTWARE DEL SISTEMA OPERATIVO.** Es el software total que maneja el sistema de cómputo. Este recurso incluye al sistema operativo suministrado por el proveedor de la computadora e incluye específicamente a los programas supervisores del sistema, los programas de carga e inicio del sistema, y cualquiera otro tipo de programas de software que se utilicen en el sistema de cómputo.

- **SOFTWARE DE COMUNICACIÓN DE DATOS.** Indica los programas de software que se utilizan para correr la porción de comunicación de datos del sistema. A los programas que conciernen específicamente a los métodos de acceso de las telecomunicaciones, a los monitores de telecomunicación que deben supervisar la función total de comunicación de datos y cualquier software de algún procesador frontal.

- **SOFTWARE OPERATIVO.** Este recurso se encamina específicamente a paquetes de software que están distribuidos en los extremos de los eslabones de comunicación de datos; pero estos paquetes no incluyen los aspectos de comunicación de datos; solamente incluyen a la inteligencia distribuida para los lugares remotos de proceso distribuido.

- **SOFTWARE DE LOS SISTEMAS ADMINISTRATIVOS DE BASE DE DATOS.** Es el software administrador de la base de datos que reside en la computadora central, en una computadora de respaldo, o en un lugar distribuido remoto (base de datos distribuidos) y específicamente a los controles que accesan de la base de datos.

- **POLITICAS ADMINISTRATIVAS.** Señalan a las políticas, procedimientos y recursos que conciernen al desarrollo de, al control de, y al almacenamiento de cualesquiera de los paquetes de software.

- **DOCUMENTACION.** Indica la revisión documental de cualquier de los paquetes de software.

- **PERSONAL DE SOFTWARE DEL SISTEMA.** Señala los controles específicos que deben de colocarse para asegurar que los programadores del sistema y otro personal altamente técnico realicen sus labores de una manera eficiente y segura, además de asegurarse que no hagan trabajos extraños que puedan ser dañinos a la organización.

II.5.8. CONTROL DE RED DE COMUNICACIONES

- Asegurar que exista una función formal de administración de las redes.
- Asegurar la existencia de procedimientos y controles de:
    1. La instalación de las redes locales
    2. La administración de las redes de locales.
    3. Mantenimiento de las redes locales.
    4. La operación y seguridad de las redes locales.

- Evaluar el grado de soporte que se brinda a los usuarios.
- Detectar el grado de confianza y satisfacción del desempeño de las redes.
- Determinar si existen los controles suficientes.
- Asegurar que sólo se encuentren el software legalizado en redes.
- Comprobar que se cuente con un software de apoyo para el monitoreo u auditoría de los elementos de una red.

II.5.9. CONTROL DE SEGURIDAD LOGICA

La seguridad lógica es la seguridad de la información. El propósito de la seguridad de la información es "asegurar a la comunidad de las operaciones y minimizar el daño a las mismas".

La información toma muchas formas. Esta puede estar almacenada en las computadoras, transmitirse a través de las redes de trabajo, fuera de impresión o bajo escritura en papel y en conversaciones, desde la perspectiva de seguridad, la protección apropiada deberá estar aplicada a todas las formas de la información, incluyendo papeles, bases de datos, películas, documentos de opiniones, módulos, cintas, disquetes, conversaciones y algunos otros métodos de uso para transmitir conocimientos o ideas.

- **CONTROLES DE ACCESO**

Las reglas de control de acceso pueden expresarse en términos de privilegios o restricciones. Un privilegio es un derecho o poder especial. En sistemas de computación este término es frecuentemente usado para describir funciones de control especial la operación de un sistema en un sitio privilegiado de procesos y el manejo de sistemas es frecuentemente un privilegio de usuario.

Se debe controlar adecuadamente el acceso, por medio de claves a recursos. Lo anterior con la finalidad de reducir el riesgo de transferencia, modificación, pérdida o divulgación accidental o internacional de la información confidencial.

- **ESTANDARES DE NORMATIVIDAD**

La unidad orgánica que tenga la responsabilidad sobre la seguridad de los datos deberá conocer la información de la institución que necesita estar protegida y el grado de protección que dicha información requerirá.

- Deberá definirse que seguridad de datos es necesaria, para la activación y mantenimiento de las claves de acceso y de instruir al personal respectivo sobre la importancia de la seguridad.
- Es necesario que se registre en una bitácora todos los accesos ocurridos, exitosos o no.
- Registrar el apagado de la computadora principal cuando la sesión es finalizada.
- Seguridad de PC´s o terminales por cierre de llaves o su equivalente a control de acceso de password, cuando no este en uso.
- Los usuarios deberán tener conocimiento del uso de los equipos.
- Los usuarios deberán tener disciplinas, contar con experiencia y no tener atavismos culturales.
- Los usuarios deberán tener cuidado con los virus.
- Deberá contarse con sistemas antivirus.
    - Detectores de acciones sospechosas
    - Detectores de virus conocidos.
- Deberá darse capacitación a los usuarios:
    - Cursos y pláticas
    - Manuales
    - Soporte técnico a usuarios.
    - Difusión de normas y procedimientos.

- Deberá tenerse prohibidos los programas piratas.

- **ADMINISTRACION DE LAS CLAVES DE ACCESO**

- Las claves de acceso podrán ser cambiadas directamente por los usuarios, lo cual es apropiado ya que este conoce la información que esta manejado.
- Se debe garantizar el cambio periódico en las claves de acceso.
- Deberá contarse con un esquema factible para usuarios de base de datos o entradas centralizadas.

- **DESCENTRALIZADA**

- Las claves de acceso podrán ser cambiadas directamente por los usuarios, lo cual es apropiado ya que este conoce la información que esta manejado.
- Se debe garantizar el cambio periódico en las claves de acceso.
- Deberá contarse con un esquema factible de sistemas de tiempo compartido y distribuido.

- **USO DE LAS CLAVES DE ACCESO**

- El uso de las claves podrán tener un alcance de:

Datos	Dispositivos y equipos de cómputo.
Registros	CPU´s
Programas	Discos
Archivos	Terminales y PC´s
Aplicaciones	Impresoras
Directorios	Controladores de comunicaciones
Procesos	Encriptores
Mensajes	Usuarios

comunicaciones

- Deberá existir políticas y reglas para la administración de claves de acceso.
- Hacer cambios periódicos de las claves de acceso.
- Es necesario contar con una jerarquización para el control de las claves de acceso.
    - Administración de seguridad.
    - Usuarios privilegiados.
    - Dueños de grupos.
    - Usuarios normales.

- Prohibir el uso de usuarios sin clave de acceso.
- Encriptar las claves de acceso durante su almacenamiento y transmisión a través de la red de comunicaciones.
- Proteger el archivo de usuarios, claves de acceso y atributos a recursos de cómputo.
- Proteger en la pantalla la digitación de la clave de acceso.
- Controlar con la clave de acceso al usuario así como las terminales.
- Respaldar periódicamente el archivo de claves de acceso del sistema.
- Restringir sólo el acceso del archivo de claves de acceso del sistema al administrador de seguridad.
- Avisar al usuario previamente el vencimiento de su clave de acceso.
- La clave de acceso y el usuario, sólo podrán estar activos en una terminal y no en varias a la vez.
- Para programas o transacciones sensitivas o vitales utilizar doble clave de acceso diferente.

- Una clave de acceso que caduque no deberá ser utilizada de nuevo.
- No permitir el uso de claves de acceso cortas.
- Los procedimientos deben ser cubiertos por todas las estrategias en el ciclo de vida de acceso desde los registros iniciales de nuevos usuarios hasta el final.
- Garantizar la redundancia de identificadores de usuarios no reimpresión de otros usuarios.
- En los sistemas multiusuarios deberán separarse de programas y datos.
- Separar la capacidad de escribir en directorios de programas de la de ejecutar.
- Deberá realizarse una revisión de la integridad del sistema.

- **ALTAS**

- Deberá establecerse controles de acceso con las siguientes características:
    - Identificar al usuario.
    - Asignaciones de clave personal para cada usuario.
    - Marcar una vigencia de acceso al sistema.

Sobre las claves de acceso (password):

- Almacenaje y transmisión encriptada.
- Ningún usuario sin clave.
- Protección de digitación en pantalla de texto y posiciones.
- Actualización de password cada 60 días, o cada vez que se requiera.
- Claves adicionales según se eleve el grado de confidencialidad.

- Deberá registrarse el acceso por subdirectorio, bibliotecas, archivos y programas por medios de privilegios.
- Deberá identificarse el tipo de acceso permitido (consultas, creación, modificación y eliminación).
- Se deberá contar con un archivo encriptado en donde se registre la información de cada usuario, tal como:
    - Nombre
    - Area a la que pertenece
    - Tipo de acceso
    - Privilegios.
    - Vigencia de acceso.
    - Password.

- Manejar un rango de longitud de la clave de acceso entre 1-8 caracteres.

- La clave de acceso debe ser personal e intransferible.
- Los controles de acceso deberán ser auditables.
- Deberá implementarse un software de seguridad, que permita el control y monitoreo del estado de los procesos y usuarios, reporte de tentativas de acceso no autorizadas, etc.
- Deberá haber un esquema de administración de red contra virus:
    - Directorio de programas con atributos de sólo ejecución.
    - Directorios de datos con atributos de solo escritura.
    - El que ejecuta no escribe,. El que escribe, no ejecuta.
    - Instalación de software antivirus.

- Obligar el uso de claves de acceso con enlace a través de la red de comunicaciones.
- No definir la clave de acceso igual que el identificador del usuario.

- **BAJAS**

- Deberá darse de baja a los usuarios que hagan mal usos de los recursos asignados.
- Deberá darse de baja a los usuarios que no cumplan con las políticas y controles autorizados.
- Deberá darse de baja al usuario que intente o instale algún software no permitido.
- Deberá darse de baja a los usuarios que alteren la información.

- **CAMBIOS**

- Cambiar la clave de acceso si esta se cree ya del conocimiento del dominio de otros.
- Cambiar inmediatamente el derecho de acceso de los usuarios cuando tienen cambios de trabajo o contrarios a la institución.
- Deberá cambiarse la clave del usuario en el tiempo establecido por la Dirección General de Informática.

- **BLOQUES**

- Bloquear el acceso a los "N" intentos no validos.
- El sistema deberá bloquear el acceso del usuario en la fecha que deba cambiar su password.

- Deberá bloquearse la cuenta de los usuarios en caso de que se descubra que hay virus.

- **USO DE PASSWORD**

La técnica más popular para controlar el acceso a la información es hoy en día la de password.

Un password es un conjunto de números, caracteres o combinaciones de ellos, que se asignan a un usuario o recurso de un sistema de cómputo.

Todos los proveedores que desarrollan software en la actualidad, ya contemplan el uso de las claves en su operación, por lo cual para su utilización es recomendable establecer las políticas de uso y aprovechar el grado de automatización que nos brinda.

Por lo tanto:

- Deberá haber una asignación individual de password para mantener la contabilidad.
- Guardar los password confidencialmente.
- Evitar guardar los password registrados en papel a menos que está pueda almacenarse en una parte segura.
- Selección del password con un mínimo de longitud de 8 caracteres.
- Evitar basarse en password de :
    - Mes del año, días de la semana o también otros aspectos de fecha
    - Nombres de familia, iniciales o números de registros de carros.

- Números telefónicos o similares, todos los números de grupos.
- Identificador de usuario, nombre de usuario, identificador de grupo u otros sistemas identificadores.
- Más de dos caracteres identificadores consecutivos.
- Todos los números o todos los grupos alfanuméricos.

- Deberá hacerse cambios de password en intervalos regulares aproximadamente 30 días y evitar recursos o ciclos de password viejos.
- Cambio de password por conteo de privilegios, estos con acceso a las utilidades del sistema central más frecuente.

- **SOFTWARE DE SEGURIDAD**

El objetivo es dar a conocer una herramienta de control de acceso de los datos que pueda ser usada para fortalecer la seguridad de la información en el Sistema de Información, así como, las funciones principales que debe ser capaz de realizar y los beneficios que se obtienen de su instalación.

Consideraciones del Software de Seguridad.

- Un paquete de seguridad de software debe proporcionar no sólo el control para tener acceso al sistema de procesamiento de datos, sino también para el acceso a una gran variedad de información contenida en los recursos computacionales.
- En caso de pérdida, divulgación o modificación de información el sistema deberá proporcionar la información suficiente para identificar el suceso o actividad no autorizada.

- Deberán considerarse los recursos a proteger como son:

Archivos

- ❖ En discos
- ❖ En cintas

Transacciones

- ❖ Internas
- ❖ Externas

Terminales

Programas

Identificadores de Usuario

Base de Datos

Bibliotecas

- ❖ Procedimientos
- ❖ Parámetros
- ❖ Tablas.

Registros

Campos

Sistemas Operativos

- Deberá considerarse una secuencia de actividades para seleccionar un paquete de seguridad de software.
- Es necesario establecer una estrategia de implantación debido a que existen diferentes actividades por realizar.
- Deberá definirse la estructura organizacional adecuada para la correcta interrelación de las funciones de las áreas usuarias con las funciones del paquete.

- Deberá darse presentación a las áreas de sistemas afectadas sobre las características y funciones del paquete.
- Es necesario una presentación a las áreas e identificar los recursos a proteger
- Establecer la prioridad de protección.
- Probar exhaustivamente la protección y desprotección de los recursos a través de los comandos propios del paquete.
- Documentar los procedimientos, políticas e instructivos en relación con el funcionamiento del paquete.
- Capacitar a los usuarios sobre el funcionamiento de paquete.
- Proteger los recursos en el orden previamente establecido.
- Controlar, administrar y dar mantenimiento al paquete.

Desarrollo de Aplicaciones

En lo referente a los programas y aplicaciones que se lleven acabo, se identificará perfectamente a las entidades.

- **ENCRIPTACION**

El rápido avance en la tecnología de cómputo, ha traído como consecuencia un incremento en la posibilidad de que sean accesados (con o sin fines de fraude), los sistemas de cómputo actuales, por muy complejos que estos puedan parecer.

Datos estadísticos en los Estados Unidos de Norteamérica señalan pérdidas en sistemas de cómputo por 3 billones de dólares al año. Cada día, las

Instituciones que cuentan con algún equipo de cómputo, son más conscientes de los riesgos existentes en el acceso no autorizado a su información, ya que no existe forma de conocer e identificar a las personas que pueden utilizar sus conocimientos técnicos para realizar un fraude.

Según el FBI, aproximadamente un 95% de los fraudes realizados por computadora no son detectados. A la fecha, la mejor defensa contra accesos no autorizados a la información procesada de Centros de Cómputo, consiste en implantar medidas de seguridad, tanto físicas como lógicas, que reduzcan la probabilidad de que ocurra un evento, el cual puede repercutir en una pérdida para la instalación.

En el ambiente de teleproceso, la criptografía es una técnica de protección disponible para proteger la información sensitiva, que se transmite a través de la red; aunque también puede ser usada para proteger información almacenada en dispositivos.

III. EL DISEÑO DE SISTEMAS DE COMPUTO

Objetivo: Especificar algunas consideraciones fundamentales del análisis y diseño de sistemas de cómputo, con el propósito de contar con elementos técnicos que nos ayuden en el diseño de un programa de Auditoría para Centros de Cómputo.

III. DISEÑO DE SISTEMAS DE CÓMPUTO

III.1. INTRODUCCIÓN AL DISEÑO DE SISTEMAS

El proceso de desarrollo del software contiene tres fases genéricas, independientemente de la metodología o proceso que se haya elegido para realizar su seguimiento. Las tres fases, **definición, desarrollo** y **mantenimiento,** se encuentran en todos los desarrollos de software, independientemente del área de aplicación, del tamaño del proyecto o de la complejidad.

La fase de **definición** se centra en **qué.** Esto es, durante la definición, el que desarrolla el software intenta identificar qué información ha de ser procesada, qué función y rendimiento se desea, qué interfaces han de establecerse, qué restricciones de diseño existen y qué criterios de validación se necesitan para definir un sistema correcto. Por tanto, han de identificarse los requisitos clave del sistema y del software. Aunque los métodos aplicados durante la fase de definición variarán dependiendo de la metodología aplicada, de alguna forma se producirán tres pasos específicos:

- **Análisis del Sistema:** El análisis del sistema define el papel de cada elemento de un sistema informático, asignando finalmente al software el papel que va a desempeñar.

- **Planificación del proyecto de software:** Una vez establecido el ámbito del software, se analizan los riesgos, se asignan los recursos, se estiman los costos, se definen las tareas y se planifica el trabajo.

- **Análisis de requisitos:** El ámbito establecido para el software proporciona la dirección a seguir, pero antes de comenzar a trabajar es necesario disponer de una información más detallada del ámbito de información y de función del software.

La fase de **desarrollo** se centra en el **cómo**. Esto es, durante esta fase, el que desarrolla el software intenta descubrir cómo han de diseñarse las estructuras de datos y la arquitectura del software, cómo han de implementarse los detalles procedimentales, cómo ha de traducirse el diseño a un lenguaje de programación (o lenguaje no procedimental) y cómo ha de realizarse la prueba. Los métodos aplicados durante está fase también variarán, pero de alguna forma se producirán pasos concretos como:

- **Diseño del Software:** El diseño traduce los requisitos del software a un conjunto de representaciones (algunas gráficas y otras tabulares o basadas en lenguajes) que describen la estructura de los datos, la arquitectura, el procedimiento algorítmico y las características de la interfaz.

- **Codificación:** Las representaciones del diseño deben ser traducidas a un lenguaje artificial (un lenguaje de programación convencional o un lenguaje no procedimental (Técnicas de 4ª. Generación o herramientas CASE)), dando como resultado unas instrucciones ejecutables por la computadora. Este paso es el que lleva a cabo esa traducción.
- **Prueba del Software:** Una vez que el software ha sido implementado en una forma ejecutable por la máquina, debe ser probado para descubrir los

defectos que puedan existir en la función, en la lógica y en la implementación.

La fase de **mantenimiento** se centra en el **cambio** que va asociado a la corrección de errores, a las adaptaciones requeridas por la evolución del entorno del software y a las modificaciones debidas a los cambios de los requisitos del cliente dirigidos a reforzar o a ampliar el sistema. La fase de mantenimiento vuelve a aplicar los pasos de las fases de definición y de desarrollo, pero en el contexto del software ya existente. Durante la fase de mantenimiento se encuentran diferentes cambios:

- **Corrección:** Incluso llevando a cabo las mejores actividades de garantía de calidad, es muy probable que el cliente descubra defectos en el software. El mantenimiento correctivo cambia el software para corregir los defectos.

- **Adaptación:** Con el paso del tiempo es probable que cambie el entorno original (p. Ej. , la CPU, el sistema operativo, los periféricos) para el que se desarrolló el software. El mantenimiento adaptativo consiste en modificar el software para acomodarlo a los cambios de su entorno externo.

- **Mejora:** Conforme utilice el software, el cliente/usuario puede descubrir funciones adicionales que podría interesar que estuvieran incorporadas en el software. El mantenimiento perfectivo amplía el software más allá de sus requisitos funcionales originales.

Las fases y sus pasos descritos anteriormente, se complementan con varias actividades "protectoras": Las revisiones que se realizan durante cada paso

para asegurar que se mantiene la calidad. La documentación que se desarrolla y controla para asegurar que toda la información sobre el sistema y el software estará disponible para un uso posterior. El control de los cambios se instituye de una forma que puedan ser mejorados y registrados.

El método para cada paso puede variar dependiendo de la técnica o metodología que se ocupe, pero el enfoque global que exige la definición, el desarrollo y el mantenimiento, permanece invariable. Uno puede realizar cada fase con disciplina y métodos bien definidos o de forma completamente desordenada. Pero habrá que realizarlos de alguna manera.

III.2. METODOLOGIAS DE DESARROLLO

Una metodología para el análisis y desarrollo de sistemas es el proceso para la producción organizada de software, mediante el uso de un conjunto de técnicas predefinidas y de una notación adaptada como convención, además es un instrumento útil para poder definir con el usuario final los requerimientos del proyecto, de manera simplificada.

Toda metodología se basa en un modelo, el cual es una abstracción de la realidad, que debe absorber los elementos indispensables de la problemática presentada. No se trata de plasmar todos los detalles, debe ser una representación simplificada.

La elección de una metodología se lleva a cabo de acuerdo con la naturaleza del proyecto y de la aplicación, los métodos y herramientas a usar y

los controles y entregas requeridos. Algunas metodologías más comunes las mencionaremos continuación.

III.2.1. ANALISIS ESTRUCTURADO

La metodología de análisis estructurado es considerada como una de las más modernas herramientas en el análisis de sistemas; así como también es considerada como la técnica más segura dentro de la prevención de fallas de diversa índole por medio de una concepción amplia del sistema, de su funcionalidad y de las relaciones que existan en todas y cada una de las entidades establecidas de acuerdo a las necesidades del sistema.

Antes del análisis estructurado, no existía una metodología formal, por lo que el analista de sistemas simplemente escribía a manera de novela los requerimientos y necesidades de los usuarios. A menudo, se duplicaban las peticiones y más aún, se repetía la información en diferentes partes del documento.

El análisis de sistemas tradicional presenta las siguientes deficiencias:

1. Dificultad y ambigüedad en la interpretación de las ideas plasmadas por el analista.

2. El documento final de análisis es redundante.

3. Debido a las redundancias, al presentarse una modificación solicitada por el usuario, esta se debe efectuar en todas las partes del documento en donde aparezca.

A través del tiempo, y de una forma gradual, se han ido depurando las técnicas de análisis de sistemas, lo que ha dado como resultado el nacimiento de nuevas tecnologías, entre ellas el Análisis Estructurado, que permiten que las especificaciones funcionales de un sistema sean más claras y cumplan con las siguientes características:

1. Gráficas – compuestas de una variedad de diagramas, apoyados por material textual.

2. Particionadas – de tal manera que se puedan leer independientemente porciones individuales de la especificación.

3. Mínimamente redundantes.

Etapas de la Metodología

Fase 1: Estudio de Factibilidad

Esta actividad también se conoce como estudio inicial de negocios. Generalmente, comienza cuando el usuario solicita que una o más partes de su sistema se automaticen. Los principales objetivos de esta etapa son:

Identificar, a los usuarios responsables y crear un campo de actividad inicial. Esto suele lograrse a través de una serie de entrevistas para determinar qué usuarios estarán comprendidos ó serán afectados por el proyecto. Se puede desarrollar además un diagrama inicial de contexto, en el cual se representa el sistema completo como un solo proceso.

Identificar las deficiencias actuales en el ambiente del usuario. Comprende la lista de funciones que hacen falta o que se están llevando a cabo de manera insatisfactoria en el sistema actual.

Establecer metas y objetivos para el sistema nuevo. Puede ser una simple lista narrativa que contenga las funciones existentes que se deben reimplantar, las nuevas y los criterios de desempeño del nuevo sistema.

Determinar si es factible automatizar el sistema, y de ser así, sugerir escenarios aceptables. Implica estimaciones de tiempo y costo necesarios para construir un sistema nuevo, así como los beneficios que se derivarán de ello. En esta etapa tan temprana del proyecto, será muy difícil determinar tiempos y costos con menos de un 50% de porcentaje de error.

Preparar el esquema que se usará para guiar el resto del proyecto. Incluirá toda la información listada anteriormente, además de que se deberá identificar al administrador responsable del proyecto, y describir los detalles del ciclo de vida que seguirá el proyecto.

Fase 2: Análisis del Sistema

El propósito de la actividad de análisis es transformar las dos entradas principales: las políticas de usuario y el esquema del proyecto en una especificación estructurada. Esto implica que se deberá modelar el ambiente del usuario con diagramas de flujo de datos, diagrama de entidad-relación, diagramas de transición de estados y demás herramientas.

El proceso de análisis implica el desarrollo de un modelo ambiental, y el desarrollo de un modelo de comportamiento, los cuales se combinan para formar el modelo esencial, que representa una descripción formal de lo que el nuevo sistema debe hacer, independiente de la naturaleza de la tecnología que se use para cubrir los requerimientos.

A continuación se describen con mayor detalle los modelos producidos en esta fase.

Modelo Ambiental

El modelo ambiental define la frontera entre el sistema y el resto del mundo. Además de determinar qué está en el interior del sistema y que en el exterior, también es de importancia crítica definir las interfaces entre el sistema y el ambiente. Se necesita saber que información entra al sistema desde el ambiente exterior, y que información produce como salida al ambiente externo.

Otro aspecto importante del modelo ambiental consiste en identificar los acontecimientos que ocurren en el ambiente al cual debe responder el

sistema. Sólo preocuparán aquellos acontecimientos que ocurren afuera y requieren una acción del sistema.

El Modelo de Ambiente consta de tres componentes:

1. Declaración de propósitos – Declaración textual breve y concisa del propósito del sistema, dirigida al nivel administrativo superior, administración de los usuarios, y otros que no están directamente involucrados con el desarrollo del sistema. Esta declaración puede constar de varias frases, pero no deberá ser demasiado extensa, ya que la intención no es proporcionar una descripción completa y detallada del sistema.

2. Diagrama de contexto – Esta parte del modelo ambiental comienza a contestar a algunas preguntas que surgen a raíz de la declaración de propósitos. El diagrama de contexto es un caso especial del diagrama de flujo de datos, en donde una sola burbuja representa todo el sistema. El diagrama de contexto enfatiza varias características importantes del sistema Personas, organizaciones y sistemas con los que se comunica el sistema, los cuales se conocen como terminadores.

   - Los datos que el sistema recibe del mundo exterior y deben procesarse de alguna forma.
   - Los datos que el sistema produce y que se envían al mundo exterior.
   - Los almacenamientos de datos que el sistema comparte con los terminadores.

- La frontera entre el sistema y el resto del mundo.

3. Lista de acontecimientos – Es una lista narrativa de los "estímulos" que ocurren en el mundo exterior a los cuales el sistema debe responder.

4. Como parte adicional del modelo ambiental, se puede contar con:

   - Diccionario de datos inicial, que define todos los flujos y almacenamientos externos.
   - Modelo Entidad-Relación de los almacenamientos externos.

Modelo de Comportamiento

Este modelo describe el comportamiento que del sistema se requiere para que interactúe de manera exitosa con el ambiente. Este modelo consiste de diagramas de flujo de datos, de entidad-relación, de transición de estados, diccionarios y especificaciones del proceso.

1. **Diagrama de flujo de datos** – Esta es una herramienta que permite visualizar un sistema como una red de procesos funcionales, conectados entre sí por conductos y almacenamiento de datos. Esta es una de las herramientas más comúnmente usadas, sobre todo por sistemas operacionales en los cuales las funciones del sistema son de gran importancia y más complejas que los datos que éste maneja. Brevemente se enumeran los componentes de un DFD:
   - Proceso – El proceso muestra una parte del sistema que transforma entradas en salidas; se representa gráficamente como un círculo, aunque

algunos analistas prefieren usar un rectángulo con esquinas redondeadas, ó un óvalo. (El círculo suele asociarse a la escuela Yourdon/DeMarco, así como el óvalo se asocia a menudo con la escuela Gane/Sarson). El proceso se describe con una sola palabra, frase u oración que describirá lo que hace el proceso.

- Flujo – Se representa gráficamente por medio de una flecha que entra o sale de un proceso. El flujo se usa para describir el movimiento de bloques de información de parte del sistema a otra. Los flujos representan datos en movimiento.
- Almacenamiento – Se utiliza para modelar una colección de paquetes de datos de reposo. Se denota por dos líneas paralelas.
- Terminador – Representan entidades externas con las cuales el sistema se comunica. Se representa como un rectángulo.

2. **Diagrama de Entidad – Relación** – Es un modelo que describe con alto nivel de abstracción la distribución de datos almacenados en un sistema. Es importante debido a que las estructuras de datos y sus relaciones pueden ser tan complejas que es necesario enfatizarlas y examinarlas independientemente del proceso que se llevará a cabo. Los componentes de un E-R son:

   - Entidades – Cosas del mundo real que se identifican de manera única dentro del sistema
   - Relaciones – Conexiones entre entidades.

3. **Diagramas de Transición de Estados** – Este diagrama se conoce como DTE, y enfatiza el comportamiento dependiente del tiempo del sistema.

Sus principales componentes son estados y flechas que representan los cambios de estado.

4. **Diccionario de Datos** – Es un listado organizado de todos los datos pertinentes al sistema, con definiciones precisas. Un diccionario de datos:

   - Describe el significado de los flujos y almacenamiento que se muestran en el DFD.
   - Describe la composición de los datos que se mueven a lo largo de los flujos
   - Describe la composición de los datos que se encuentran en los almacenamientos.
   - Describe los detalles de las relaciones especificadas en el E-R.

Además del modelo del sistema, generalmente se prepara un conjunto de presupuestos y cálculos de costos beneficios más precisos y detallados.

Fase 3: Diseño

La Actividad de diseño se dedica a la creación de una jerarquía apropiada de módulos de programas y de interfaces entre ellos para implantar la especificación creada en la fase de análisis. Además, la actividad de diseño se ocupa de la transformación de modelos de datos de entidad-relación en un diseño de base de datos.

En esta etapa se desarrolla además el modelo de implantación del usuario. Este modelo contiene una descripción completa de lo que el sistema debe

hacer para satisfacer al usuario. En su elaboración, el usuario proporcionará información que involucra cuestiones de implantación como:

1. Frontera de automatización – cuáles partes del sistema se van a implantar con la computadora y cuáles se van a realizar manualmente por personal de la organización.
2. Formato de entradas y salidas del sistema – Es de suma importancia para un usuario la organización y distribución de la información en sus reportes y pantallas de captura, así como tipos de mensajes de error que generará la aplicación y mecanismos de ayuda.
3. Identificación de actividades de apoyo manual adicional – El usuario podría decidir qué módulos del sistema automatizado requieren algún proceso adicional de control de errores operacionales que el personal pudiera cometer. Estas actividades de apoyo adicional se representarían como nuevos procesos.
4. Especificación de restricciones operacionales – El equipo de implantación deberá decidir la combinación de hardware, sistema operativo, equipo de comunicaciones, lenguaje de programación y estrategia de diseño para implantar mejor los requerimientos. Pero esto será difícil de lograr si no se tiene una declaración de restricciones operativas, las cuales involucran:
   - Volumen de datos: El usuario especificará los volúmenes de transacciones de entrada y el tamaño requerido de los almacenamientos de datos.
   - Tiempo de respuesta: Esto suele indicarse en términos de probabilidades ó de límites de tiempo.

- Restricciones políticas sobre modalidades de implantación: El usuario podía especificar la marca de hardware que se usará, el lenguaje de programación, ó los proveedores de telecomunicaciones.

- Restricciones ambientales: En este rubro se consideran las restricciones de temperatura, humedad, interferencia eléctrica, consumo de energía, limitaciones de tamaño, peso o emisiones eléctricas, contaminación, ruido, radiación y otras restricciones ambientales.

- Restricciones de seguridad y confiabilidad: El usuario puede especificar un tiempo promedio entre fallas, así como tiempo promedio necesario para la reparación.

- Restricciones de seguridad: Estas restricciones están enfocadas a minimizar el uso no autorizado del sistema, esto incluye números y claves para cada usuario; así como mecanismos para evitar el acceso no autorizado a datos confidenciales.

Además de lograr los objetivos que se especifican en el modelo de implantación de usuario, el diseñador también se ocupa de la calidad global del diseño. La capacidad que los programadores exhiban para implantar un sistema de alta calidad y libre de errores depende en gran medida de la naturaleza del diseño. El campo del diseño estructurado ofrece guías para ayuda al diseñador a determinar los módulos que conformarán el sistema.

Las dos reglas más importantes que se establecen son:

- Cohesión: Se define como el grado en el cual los componentes de un módulo son necesarios y suficientes para llevar a cabo una sola función bien definida. Esto significa que el diseñador debe asegurarse de no fragmentar los procesos esenciales en módulos, y también debe asegurarse de no juntar procesos no relacionados en módulos sin sentido.

- Acoplamiento: Grado en el cual los módulos se interconectan o se relacionan entre ellos. Entre más fuerte sea el acoplamiento entre módulos en un sistema, más difícil es implantarlo y mantenerlo, pues entonces se necesitará un estudio más cuidadoso para la modificación o cambio de algún módulo.

Fase 4: Implantación

Esta actividad incluye la codificación y la integración de módulos en un esqueleto progresivamente más completo del sistema final. Como analista, se deberá estar al tanto de que la productividad, la eficiencia, la portabilidad y fácil mantenimiento del software desarrollado sean cuestiones clave en la programación de sistemas:

- Programación Estructurada – Se debe seguir un enfoque de programación estructurada, en el que la lógica del programa (decisiones y ciclos) se organiza en combinaciones anidadas de construcciones IF THEN y DO WHILE.

- Módulos pequeños – Es esencial que los programas se organicen en pequeños módulos.

- Sencillez de estilo – Seguir ciertas reglas para la escritura de programas sencillos, que un programador promedio pueda entender, y que se pueda pasar fácilmente de un programador a otro para su mantenimiento.

Fase 5: Generación de Pruebas de Aceptación

La especificación estructurada debe contener toda la información para definir un sistema que sea aceptable desde el punto de vista del usuario. Por eso, una vez generada la especificación, se pueden comenzar a producir conjuntos de casos de pruebas de aceptación.

Existen distintas estrategias de prueba, las dos más comunes se conocen como prueba ascendente y descendente. El enfoque ascendente empieza por probar módulos individuales pequeños separadamente (esto es conoce comúnmente como prueba de unidades, prueba de módulos, o prueba de programas). Luego, los módulos individuales se combinan para formar unidades cada vez más grandes que se probarán en masa (lo cual se conoce como prueba de subsistemas). Finalmente todos los componentes del sistema se combinan para probarse.

El enfoque de prueba descendente empieza con un esqueleto del sistema, la estrategia de prueba supone que se han desarrollado los módulos de alto nivel, pero que los de bajo nivel existen como módulos vacíos.

Además de estos conceptos, se tienen los siguientes tipos de pruebas:

Prueba Funcional: Su propósito es asegurar que el sistema realiza sus funciones normales de manera correcta.

Prueba de Recuperación: Asegurar que el sistema pueda recuperarse adecuadamente de diversos tipos de fallas.

Prueba de desempeño: Asegurar que el sistema pueda manejar el volumen de datos y transacciones de entrada especificados, y que tenga el tiempo de respuesta requerido.

Fase 6: Garantía de Calidad

Se conoce también como la prueba final ó prueba de aceptación. Esta fase se ocupa de verificar que el sistema tenga el nivel apropiado de calidad.

Fase 7: Descripción del Procedimiento

Es la generación de una descripción formal de las partes del sistema que se harán, en forma manual, así como la descripción de cómo interactuarán los usuarios con la parte automatizada del nuevo sistema. El resultado de esta fase es un manual de usuario.

Fase 8: Conversión de Base de Datos

En algunos proyectos, la conversión de base de datos involucraba más trabajo y planeación que el desarrollo mismo del nuevo sistema. En otros casos puede que no exista una base de datos previa por convertir. En el

caso general esta actividad requiere como entrada la base de datos actual del usuario, así como la especificación de diseño del sistema nuevo.

Fase 9: Instalación

La actividad final es la instalación, sus entradas son el manual de usuario producido en la fase 7, la base de datos convertida de la fase 8, y el sistema producido por la fase 6. En algunos casos la instalación puede significar un cambio de la noche a la mañana, en otros, puede ser un proceso gradual, en el que un grupo tras otro de usuarios van recibiendo manuales y entrenamiento para usar el sistema.

III.2.2. METODOLOGIA DE PROTOTIPOS

III.2.2.1. El ciclo de vida de protipos

Se ha vuelto popular en los últimos años este ciclo, popularizado por Bernard Board, James Martín y otros. Este enfoque consiste en capturar un conjunto inicial de necesidades e implantarlas rápidamente con la intención de expandirlas y refinarlas iterativamente al ir aumentando la comprensión que del sistema tiene el usuario y quien los desarrolla. La definición del sistema se realiza mediante el descubrimiento evolutivo y gradual.

El enfoque de prototipos generalmente requiere de los siguientes tipos de herramientas de software:

- Diccionario de datos integrado
- Generador de pantallas

- Generador de reportes no guiado por procedimientos
- Lenguaje de programación de cuarta generación
- Lenguaje de consultas no guiado por procedimientos
- Medios poderosos de administración de bases de datos

El ciclo de vida de prototipos involucra el desarrollo de un modelo funcional, que luego se descarta y se remplaza con un sistema de producción. Existe un peligro considerable de que el usuario o el equipo que desarrolla el sistema traten de convertir al prototipo mismo en un sistema de producción. Esto no suele resultar, pues el prototipo no puede trabajar eficientemente con grandes volúmenes de transacciones, y porque carece de detalles operacionales tales como recuperación de errores, auditorías, documentación para el usuario y procedimientos de conversión.

Si se descarta el prototipo y se reemplaza con el sistema de producción, existe el peligro real de que pudiera concluirse el proyecto sin dejar un registro permanente de los requerimientos del usuario. Esto probablemente dificulte cada vez más el mantenimiento con el paso del tiempo.

III.2.3. METODOLOGIA ORIENTADA A OBJETOS

III.2.3.1. El Enfoque de Orientación a Objetos

La metodología de modelos y diseño orientada a objetos es una nueva forma de enfocar problemas, utilizando modelos que se elaboran alrededor de conceptos del mundo real. La construcción fundamental es el objeto, el cual combina una estructura de datos y comportamiento, en una sola entidad. Estos modelos resultan útiles para la comprensión de problemas, la comunicación con los expertos, para la preparación de documentación y el diseño tanto de programas como de base de datos.

Los métodos más conocidos y utilizados hasta el momento dentro del tema de Orientación a Objetos son desarrollados por Ivan Jacobson (OOSE), James Rumbaugh y Grady Booch (OMT), y actualmente el UML ó Método Unificado, que consiste en una fusión y mejoras sobre los mencionados anteriormente.

El término de orientación a objetos se refiere a la organización del software como una colección discreta de objetos, con datos y comportamiento. Este concepto se contrapone con la programación convencional, donde la estructura de datos y el comportamiento sólo están vagamente conectados.

Un enfoque orientado a objetos debe contener:

- **Identidad:** Los datos se encuentran organizados en entidades discretas, distinguibles y únicas llamadas objetos.

- **Clasificación:** Varios objetos que presenten los mismos atributos e igual comportamiento, se agrupan en clases. Se entiende por objeto a la instanciación de una clase. Ej. Clase Pieza de Ajedrez, al ser instanciada tiene los objetos: Peón, Alfil, Rey, etc.

- **Polimorfismo:** Significa que una misma operación se puede comportar de distinta forma en diferentes clases. Ej. La operación movimiento tiene un comportamiento diferente en la clase ventana y en la clase pieza de ajedrez.
- **Herencia:** Mecanismo que permite a las clases compartir sus atributos y funciones con otras clases relacionadas, que pertenecen a niveles inferiores.

La metodología orientada a objetos involucra todo el ciclo de desarrollo de software: análisis, diseño e implementación. La esencia del método es la identificación y organización de los conceptos que componen el dominio de la aplicación, y no la idea de la representación final en un lenguaje de programación.

La Técnica de Modelado de Objetos (OMT Object Modeling Technique) es una de las metodologías más difundidas hoy por hoy, siguiendo las etapas que se muestran a continuación:

- Análisis: Inicia en la definición del problema, el analista construye un modelo de la situación real, mostrando sus propiedades importantes. El modelo que se obtenga es una abstracción de lo que el sistema va a hacer, no de cómo lo va a hacer. Los objetos del modelo son conceptos del dominio de la aplicación, y no conceptos de la implementación computacional.

- Diseño del Sistema: Durante esta etapa, el diseñador toma las decisiones de la arquitectura general del sistema, el cual se organizará en subsistemas, buscando estrategias para atacar cada problema, características que se optimizarán, y colocación de recursos, así como protocolos de comunicación, estrategias de manejo de memoria, etc.

- Diseño de Objetos: El diseñador construye un modelo de diseño, basado en el modelo del análisis, pero que contiene detalles de implementación. Es decir, se diseñan las estructuras de datos y algoritmos necesarios para la implementación de cada clase. Las clases definidas en el análisis se complementan con sus estructuras computacionales y sus algoritmos de ejecución de funciones. Además se definen nuevas clases, asociadas al diseño computacional, que coexistirán con las clases originales de la aplicación, pero en un distinto plano conceptual.
- Implementación: Las clases y relaciones desarrolladas son traducidas a un lenguaje particular de programación, base de datos o implementación en hardware.

La metodología orientada a objetos explota al mejor nivel la modularidad de programación. Un objeto por sí mismo constituye un módulo completo.

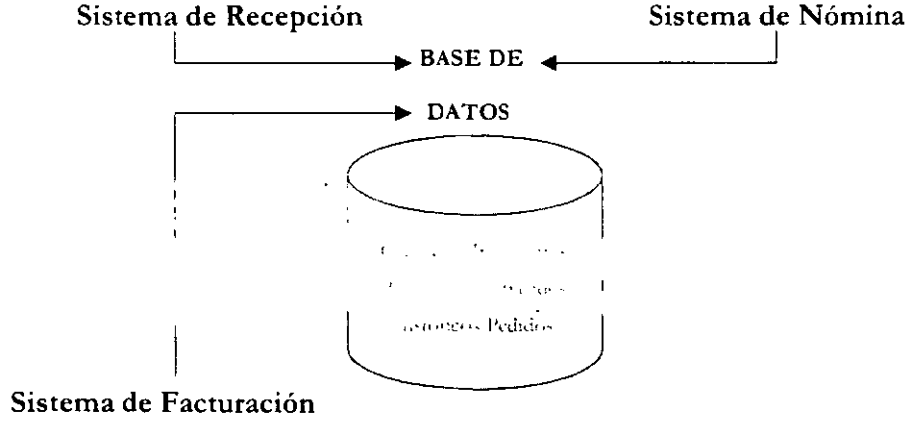
III.3. LAS BASES DE DATOS RELACIONALES

III.3.1. ASPECTOS GENERALES

Una base de datos es una colección integrada de objetos, en donde cada persona y cada programa puede accesar la información que contiene, siempre y cuando tenga autorización de hacerlo. De la misma forma, los datos pueden ser modificados por usuarios que reciban una autorización previa.

Es importante resaltar que una base de datos bien diseñada minimiza la cantidad de información redundante en un sistema de información.

Gráficamente, se podría representar el enfoque de base de datos de la siguiente manera:



Este enfoque permite:

- Controlar la redundancia: no permitir que la misma información, se encuentre en varias partes.

- Mantener la consistencia: la información es la misma, para cualquier usuarios que la vea desde cualquier aplicación.

- Lograr la integración de los datos.

- Compartir los datos entre las diferentes aplicaciones: la información, se encuentra en la base de datos y cualquier programa que sea parte de una aplicación puede accesarla.

- Cumplir con los estándares.

- Facilidad en el desarrollo de aplicaciones.

- Uniformar los controles de la información.

- Independencia entre los datos y los programas: la información, se encuentra en la base de datos, mientras que los programas pueden tener cualquier ubicación y accesar la base desde de cualquier lugar.

- Reducir el mantenimiento a los programas: esta característica se desprende de la anterior, como los programas y los datos son independientes, no hay

alteración del código cuando un dato cambia, y de la misma forma, el cambio en el programa no implica cambio en los datos.

Un DBMS (Sistema Manejador de Base de Datos) es un programa de software que:

- Almacena, recupera y modifica datos
- Mantiene la consistencia de la información
- Resuelve problemas de concurrencia: en los casos en que varios usuarios accesan un mismo dato a la vez; el manejador se ocupa de permitir el acceso a un usuario, y mantener en espera a otros, para evitar problemas de consistencia de la información.

- Permitir una interfaz universal con los datos: Cualquier aplicación puede consultar la base de datos con sólo establecer la conexión, utilizando un lenguaje estándar de manejo de la información.

- Regula el acceso a la información. Controla usuarios y privilegios sobre la información.

Las características principales de un manejador de bases de datos relacional son:

1. Representación de los datos en forma de tablas

2. Utilización de un lenguaje de cuarta generación (4GL), el cual: maneja sintaxis no procedural, y es muy parecido al inglés.

3. Manejo de todos los operadores relacionales

4. Facilidad en la modificación de los datos y de sus estructuras.

En una base de datos relacional, la información está organizada en forma de tablas, donde las categorías de información están listadas a lo largo de la parte superior de cada tabla, y los casos individuales están listados hacia abajo. De esta manera, se puede visualizar y comprender la información en forma muy sencilla.

Cada columna contiene un tipo de información que caracteriza a la tabla. Cada renglón está por tanto compuesto de varias columnas que contienen cada una, un valor.

La información de una tabla no necesariamente se encuentra aislada, puede relacionarse con la información de otra tabla.

La habilidad del diseñador de la base de datos para relacionar información de una tabla con otra permite organizar los datos en unidades independientes y mucho más fáciles de manejar. Esta independencia no representa ningún problema en cuanto al manejo de la información, ya que se pueden relacionar los datos por medio de una consulta de unión de tablas. Los valores comunes de las tablas relacionadas son los que permiten estas consultas de unión (join).

III.3.2. MODELO ENTIDAD – RELACIÓN

Este modelo permite la representación gráfica del problema real. Es una técnica para definir las necesidades de información de cualquier lugar. Involucra los objetos de principal importancia del mismo, a los cuales se le denomina Entidades, mientras que a las características básicas de cada objeto se les denomina Atributos, y a la forma en que los distintos objetos interactúan, se les conoce como Relaciones.

Estos conceptos se modelan en esquemas gráficos, que resultan comprensibles a los usuarios y les permiten visualizar sus necesidades de información.

A continuación se describen en forma más detallada los elementos del modelo:

Entidad: Es una persona, cosa o lugar que tenga importancia dentro del dominio del sistema, y sobre la cual el sistema deba mantener y relacionar información.

Las entidades se representan por medio de una caja con las esquinas redondeadas, dentro de esta caja se escribe el nombre, el cual siempre debe de estar en singular.

Cada entidad tiene un nombre único en el sistema.

Una entidad corresponderá a una tabla de la base de datos, donde el nombre de la tabla corresponderá a la entidad, utilizando ya el plural. Cada tabla contendrá atributos que la caractericen (constituyen las columnas), de los cuales una columna o grupo de columnas deberá identificar de forma única a cada renglón. Esta columna (o grupo) recibe el nombre de llave primaria y no puede contener valores nulos, ni duplicados.

Relación: Una relación requiere de una o más entidades, que asociarán su respectiva información. Las relaciones se presentan en varias modalidades:

- Uno a uno: Una fila de la entidad A se relaciona con una fila de la entidad B. Puede ser obligatoria a opcional, opcional a opcional y obligatoria a obligatoria.

- Uno a muchos: Una fila de la entidad A se relaciona con muchas filas de la entidad B. Puede ser obligatoria a opcional, opcional a opcional, obligatoria a obligatoria y opcional a obligatoria.

- Muchos a muchos: Muchas filas de la entidad A se relaciona con muchas filas de la entidad B. Puede ser obligatoria a opcional y obligatoria a obligatoria. (Esta entidad se debe descomponer para su manejo en la base de datos).

Relaciones recursivas: Combinación de muchas a uno, opcional a opcional ó uno a uno opcional a opcional. Una fila de la entidad A se puede relacionar con una o muchas otras filas de la misma entidad A.

La manera de leer las relaciones es:

"Cada elemento de la entidad A debe o puede relacionarse con uno y sólo uno (o muchos) elemento(s) de la entidad B".

Atributos: Un atributo es una característica de una entidad que cae dentro del dominio del sistema, los atributos se escriben dentro de la entidad. En la base de datos se representan por medio de columna de la tabla.

III.3.3. REGLAS DE INTEGRIDAD RELACIONAL

Cualquier base de datos se compone de alguna configuración de valores de los datos, la cual refleja la realidad, es decir, es un modelo o representación de algún fragmento del mundo real.

Algunas configuraciones de valores no tienen sentido, debido a que no representan ningún estado del mundo real. Por lo tanto, es necesario ampliar una definición de base de datos, para incluir ciertas reglas de integridad, cuyo propósito es informar al Sistema Manejador de Base de Datos de ciertas restricciones en el mundo real para que pueda impedir la ocurrencia de tales valores.

La mayor parte de las reglas de integridad son específicas a la base de datos a la que se aplican. Sin embargo, el modelo relacional incluye dos reglas generales relacionadas principalmente con la Llave Primaria y llave foránea o secundaria, que se aplican a cualquier base de datos que se apegue a este modelo.

Llave Primaria

La llave primaria de una entidad es el identificador único para ésta. Esta llave puede ser compuesta (formada por varios atributos de la entidad) o simple.

También es posible que un entidad tenga más de un identificador único, esta característica no es muy usual, pero en tales casos, se dice que la entidad tiene varias llaves candidatas, y una sola de ellas será seleccionada como llave primaria, mientras que las demás serán llaves alternas.

Toda relación deberá tener una llave primaria. Estas llaves constituyen el mecanismo de direccionamiento, a nivel de filas básico en un sistema relacional. Es decir, el único modo garantizado por el sistema, de localizar una fila o tupla específica es por el valor de su llave primaria.

Regla de Integridad 1

La primera regla general de integridad es la regla de las entidades, y se refiere a que ningún componente de la llave primaria de una entidad puede aceptar nulos o información faltante por alguna razón. Algunas justificaciones de la existencia de esta regla son:

- Las entidades corresponden a "cosas" del mundo real. Estas entidades son distinguibles, o sea que se les puede identificar de alguna manera. Por tanto, los representantes de las entidades dentro de la base de datos deben ser distinguibles también.
- Las llaves primarias realizan esta función de identificación única en el modelo relacional. Si uno de los atributos de esta llave fuera nulo, esto equivaldría a decir que en el mundo real existe un ente sin identidad.

Esta regla se aplica únicamente a llaves primarias, y no a las llaves alternas.

Llaves Foráneas

Una llave foránea es un atributo (que puede ser simple o compuesto) de una entidad 2 cuyos valores deben concordar con los de la primaria de alguna entidad 1. Un valor de llave foránea representa una referencia a la fila donde se encuentra el valor correspondiente de la llave primaria.

Regla de Integridad 2

La segunda regla general de integridad del modelo relacional es la llamada regla de integridad referencial. Esta se refiere a que la base de datos no debe de contener valores de llave foránea sin concordancia.

La justificación de esta llave es simple: así como los valores de llave primaria representan referencias a entidades. La regla de integridad referencial dice tan sólo que si B hace referencia a A, entonces A debe de existir.

La integridad referencial exige concordancia de las llaves foráneas específicamente con llaves primarias, no con llaves alternas de otra entidad.

La regla de integridad referencial implica la validación de ciertos estados de la base de datos. Cualquier estado que no satisfaga la regla será incorrecto.

Sin embargo, se deben tomar en cuenta en el diseño las acciones a seguir con el fin d evitar, o bien de manejar la existencia de estados incorrectos.

Una posibilidad es que el sistema rechace cualquier operación que produzca un estado ilegal. Pero en la mayoría de los casos la alternativa preferible sería que el sistema aceptara la operación pero realizara ciertas operaciones de compensación con objeto de garantizar un estado legal.

Por ejemplo, si el usuario solicita eliminar una tupla o registro de una entidad 1, debería ser posible hacer que el sistema elimine también el de la entidad 2 el registro relacionado por medio de una llave foránea, sin necesidad de acciones adicionales por parte del usuario (efectos de eliminación en cascada). Cualquier diseño de base de datos deberá especificar cuáles operaciones han de rechazarse, y cuáles han de aceptarse, y en este último caso, cuáles operaciones de compensaciones debe realizar el sistema.

III.3.4. ALGEBRA RELACIONAL

El álgebra relacional consiste es un conjunto de operadores de alto nivel que operan sobre entidades. En principio, sería posible definir una gran cantidad de operadores que se ajustan a esta definición, Codd definió un conjunto específico de ocho operadores, divididos en dos grandes grupos:

- Operadores Tradicionales de conjuntos: Unión, intersección, diferencia y producto cartesiano.

- Operadores relacionales especiales: Restricción, proyección, reunión y división.

III.3.5. REGLAS DE CODD

En la década de los 80´s, Codd estableció una serie de reglas que debía de cumplir un Sistema Manejador de Base de Datos para poder afirmar que era completamente relacional. Desde su publicación, estas reglas se han estado revisando, ampliando y aclarando, y sin duda han sido criticadas en varios aspectos técnicos; no obstante, es innegable que han tenido una influencia importante en el mercado.

En este caso solo se mencionarán algunas de las más importantes:

Regla de Información. Toda la información se presentará en la base de datos de una manera y sólo una, mediante valores en posiciones de columnas, dentro de filas de tablas.

Regla de Acceso Garantizado. Debe ser posible obtener la dirección de cada valor individual en la base de datos especificando el nombre de la tabla que lo contiene, el nombre de la columna que lo contiene, y el valor de la llave primaria de la fila que lo contiene.

Manejo Sistemático de Valores Nulos. El sistema manejador de base de datos (DBMS) debe de manejar una representación de la información faltante y de la no aplicable, que sea sistemática y distinta de todos los valores normales, por ejemplo "distinta de cero o cualquier otro número".

III.3.6. NORMALIZACIÓN

La teoría de la Normalización tiene como fundamento el concepto de formas normales. Se dice que una entidad está en una determinada forma normal si satisface un cierto conjunto de restricciones.

Se han definido un gran número de formas normales. Originalmente, Codd definió la primera, segunda y tercera formas normales.

Las principales se comentan a continuación:

Primera forma normal: Cada posición de fila y columna dentro de una entidad contendrá un valor atómico, es decir, siempre hay uno y sólo un valor de datos, nunca un conjunto de múltiples valores.

Segunda forma normal: Una entidad está en segunda forma normal si y sólo si, está en primera forma normal y todos los atributos dependen por completo de la llave primaria.

Tercera forma normal: Una entidad está en tercera forma si y sólo si, los atributos que no forman parte de la llave son dependientes por completo de la llave primaria (segunda forma normal), y mutuamente independientes.

CAPITULO IV. UNA PROPUESTA PARA LA AUDITORIA DE CENTROS DE COMPUTO

Objetivo: Generar un Sistema de Auditoria para Centros de Cómputo, a través de una base de datos relacional (Acces) y generación de un Front-End (Visual Basic) que permita la entrada, actualización y consulta de la información en línea, representación gráfica y reportes de información, con el fin de controlar los recursos tanto materiales como humanos con los que cuenta un Centro de Cómputo .

IV.1. INTRODUCCIÓN

En este capítulo hablaremos del análisis donde se definen los alcances del sistema y de un diseño de las formas principales del sistema, en las cuales se pueden visualizar de forma clara las funciones del sistema, relaciones y uso de las tablas contenidas en la base de datos, para la implantación de un sistema.

IV.2. ANÁLISIS DEL SISTEMA DE AUDITORIA PARA UN CENTRO DE CÓMPUTO.

Todas las empresas cuentan con un centro de cómputo que por pequeño que sea lleva a la necesidad de un control particular al estar constituido por recursos tanto materiales como humanos.

El control puede llevarse a través de un sistema automático, que despliegue información gráfica y reportes informativos. Este tipo de sistema esta desarrollado en un lenguaje de programación orientado a objetos (Visual Basic) y tiene la ventaja de que la información se almacena en una base de datos relacional como lo es Access lo que facilitará el manejo de la información además de estar estandarizado para ser implantado en cualquier centro de cómputo.

Para el desarrollo de este sistema se deben de considerar los siguientes puntos:

Para Recursos Materiales:

Tipo de recurso (Hardware, Software, etc.)
Status en los que se encuentra los recursos (Operación, Obsoleto, Ext.)
Descripción del recurso

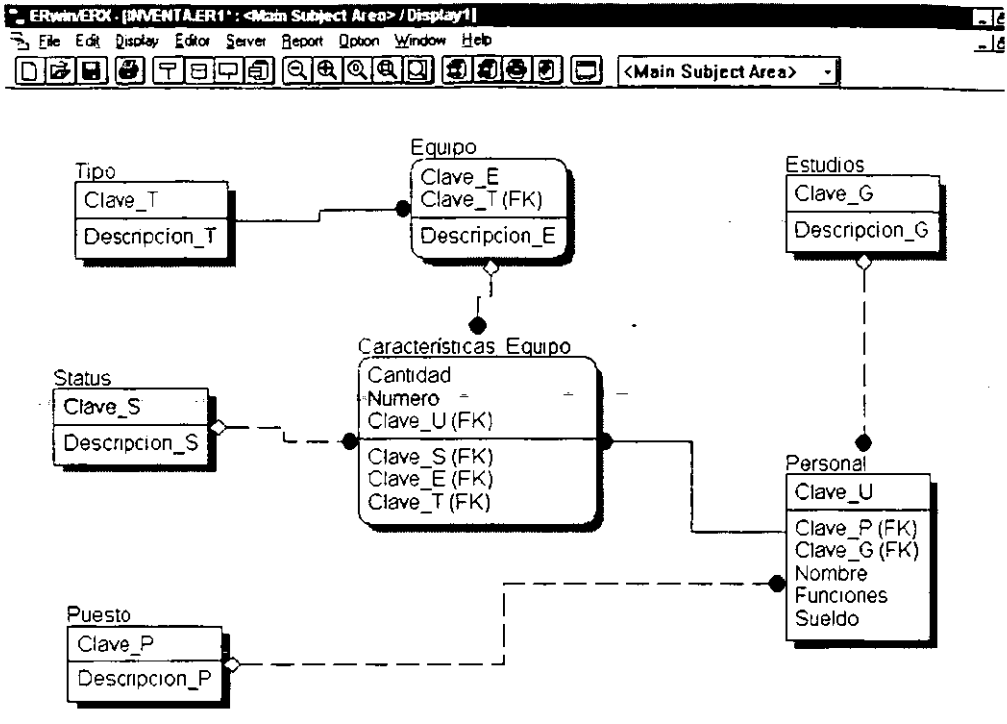
Para Recursos Humanos:

Escolaridad (Técnico Programador, Licenciado en Informática, etc.)
Puesto (Director General, Gerente de Informática, Líder de Proyecto, etc.)
Nombre del recurso
Funciones desarrolladas en la empresa
Sueldo que percibe

IV.3. DISEÑO DEL SISTEMA DE AUDITORIA.

El diseño de la base de datos es parte principal para el desarrollo de un sistema, de esta depende la funcionalidad del sistema.

A continuación se muestra un diagrama de la estructura de la base de datos con cada tabla y sus campos correspondientes que se encuentran involucrados en el sistema de auditoria.



La tabla principal del sistema es la llamada *Status_Equipo*, porque ahí es donde se encuentra la relación de los campos de otras tablas.

A continuación se muestran las tablas contenidas en la base de datos, sus campos correspondientes y sus relaciones con las otras tablas.

Tipo

Campo	Tipo De Llave	Tabla De Relación	Tipo De Dato	Longitud
Clave_T	Primaria	Equipo, Status de Equipo	Texto	1
Descripcion_T	N/A	N/A	Texto	8

Equipo

Campo	Tipo De Llave	Tabla De Relación	Tipo De Dato	Longitud
Clave_E	Primaria	Status de Equipo	Texto	10
Clave_T	Foranea	Status de Equipo	Texto	1
Descripcion_E	N/A	N/A	Texto	50

Estudios

Campo	Tipo De Llave	Tabla De Relación	Tipo De Dato	Longitud
Clave_G	Primaria	Personal	Texto	6
Descripcion_G	N/A	N/A	Texto	50

Puesto

Campo	Tipo De Llave	Tabla De Relación	Tipo De Dato	Longitud
Clave_P	Primaria	Personal	Texto	3
Descripcion_P	N/A	N/A	Texto	50

Personal

Campo	Tipo De Llave	Tabla De Relación	Tipo De Dato	Longitud
Clave_U	Primaria	Status de Equipo	Texto	4
Clave_P	Foranea	Personal	Texto	3
Clave_G	Foranea	Personal	Texto	6
Nombre	N/A	N/A	Texto	50
Funciones	N/A	N/A	Memo	
Sueldo	N/A	N/A	Long Integer	

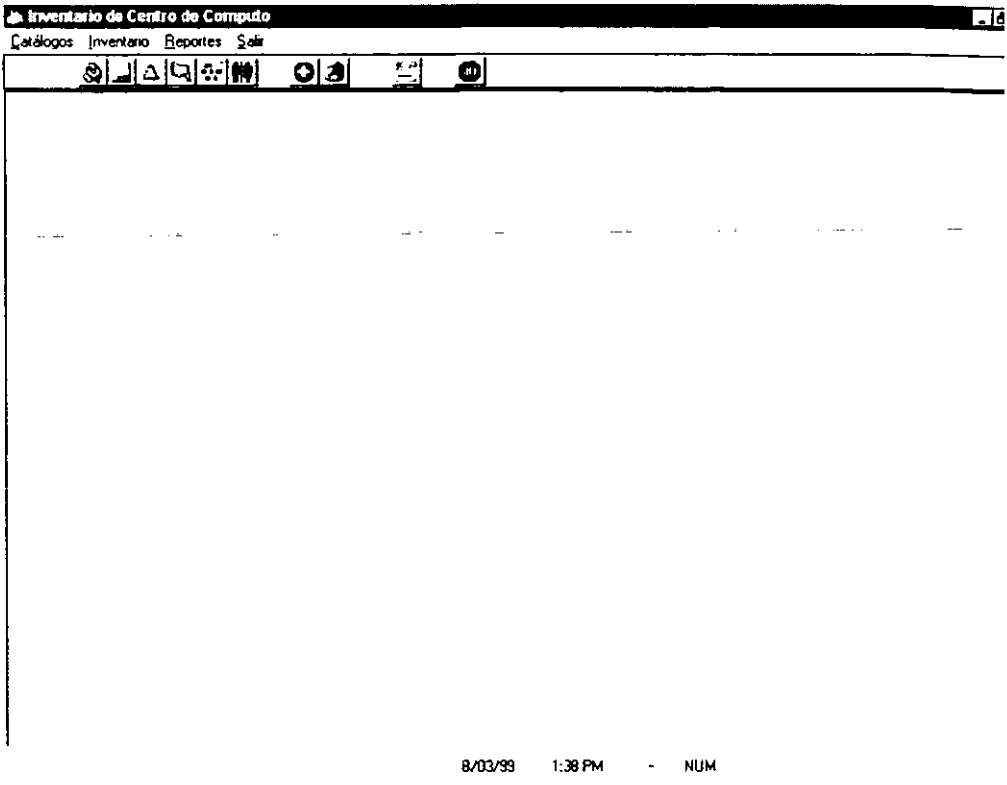
Status

Campo	Tipo De Llave	Tabla De Relación	Tipo De Dato	Longitud
Clave_S	Primaria	Status_Equipo	Texto	3
Descripcion_S	N/A	N/A	Texto	18

Status_Personal

Campo	Tipo De Llave	Tabla De Relación	Tipo De Dato	Longitud
Cantidad	Primaria	N/A	Integer	
Numero	Primaria	N/A	Texto	50
Clave_U	Foranea	Personal	Texto	4
Clave_S	Foranea	Status	Texto	3
Clave_E	Foranea	Equipo	Texto	10
Clave_T	Foranea	Equipo. Tipo	Texto	1

El diagrama que se muestra a continuación es la forma que aparece cuando se ejecuta el sistema



Como podemos ver en la figura los comandos en el menú del sistema son:

Catálogos

Inventario

Reportes

Salida

IV.3.1. CATALOGOS

Dentro de los catálogos se realiza el mantenimiento de *Alta*, *Baja*, *Cambios* y *Modificaciones* de datos que son poco variables. Dentro del sistema consideramos los siguientes catálogos:

Tipo. Clasificación del equipo por su clase

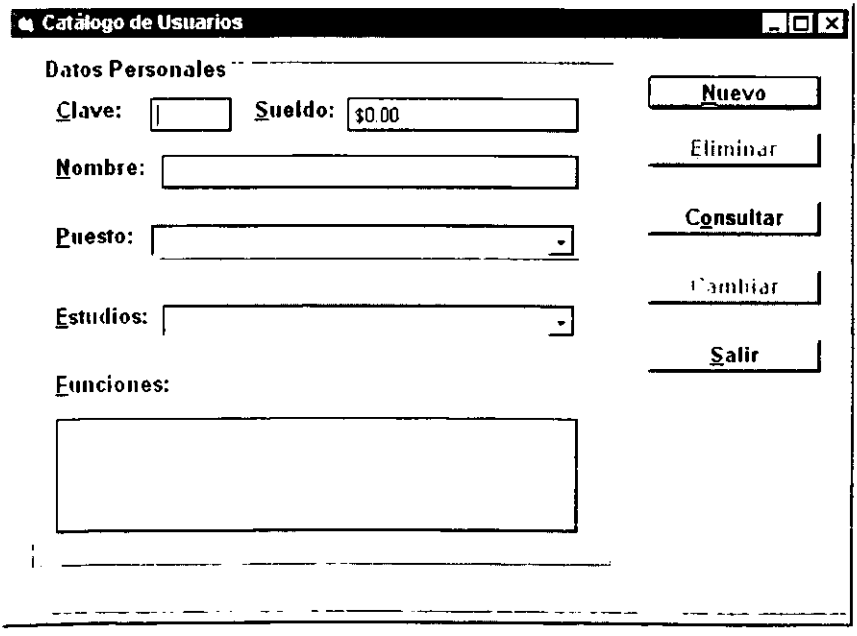
Equipo. Descripción de los recursos materiales

Estudios. Nivel de escolaridad de los recursos humanos

Puesto. Puestos establecidos por la empresa

Personal. Descripción de los recursos humanos, con el desempeño de las funciones y el sueldo percibido

La siguiente figura muestra gráficamente el *Catálogo de Personal.*

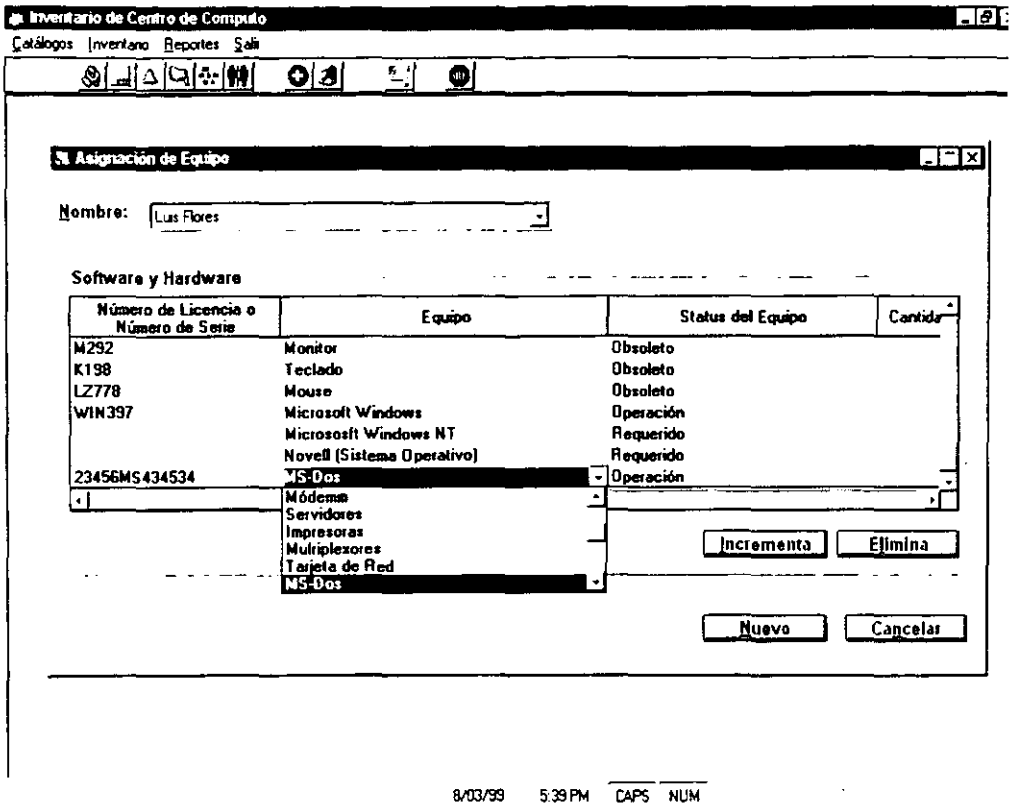


IV.3.2. INVENTARIO

En esta parte es donde se lleva la relación del los recursos materiales (llamados en el sistema el equipo) con los recursos humanos (llamados personal). Dentro de este comando tenemos las siguientes funciones:

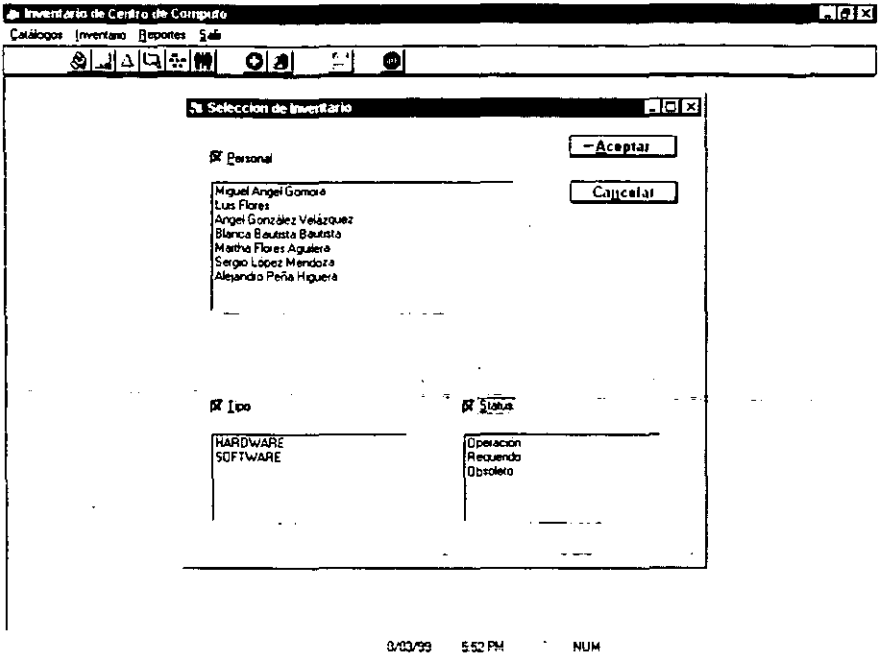
Nuevo
Consulta
Consulta de Equipo

Nuevo. Se dan de alta o se modifica los recursos humanos con los recursos materiales. A continuación se presenta la forma de *Asignación de Equipo*



Consulta. Aparecen todos los recursos humanos relacionados con los recursos materiales que se encuentran registrados en la base de datos.

La siguiente pantalla muestra las opciones de Personal, Tipo y Status que se desean consultar.



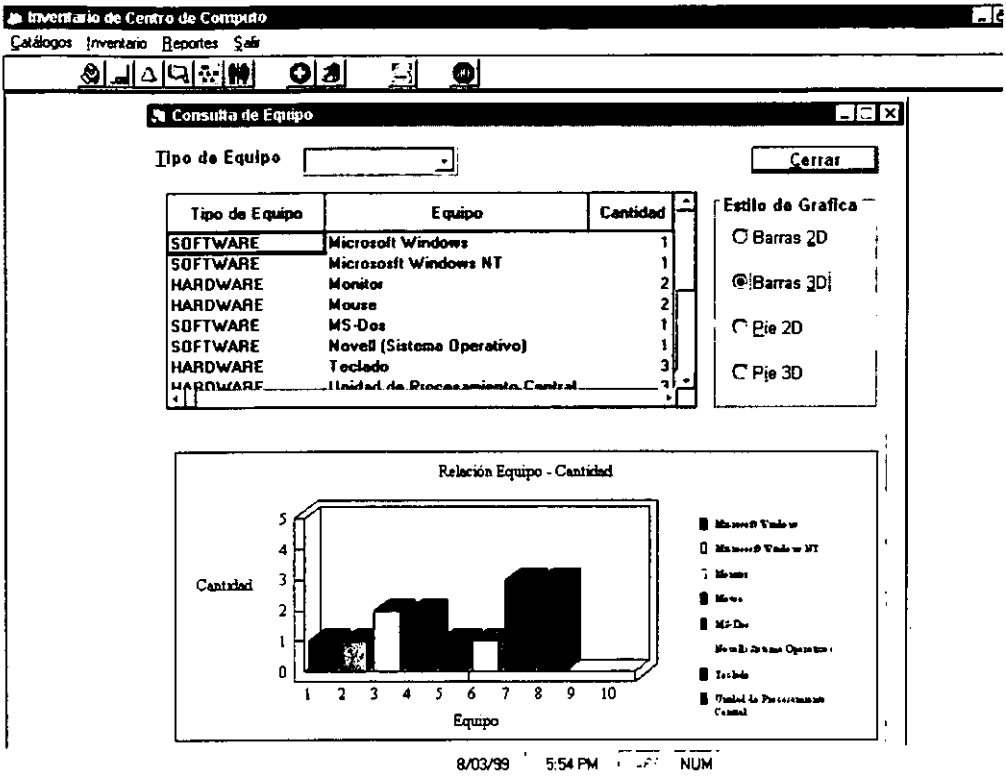
Una vez que se seleccionaron las opciones aparece la información en otra ventana como la siguiente:

Relación de Equipo Personal

Nombre	Equipo	Número de Licencia o Número de Serie	Cantidad	Status del Equipo
Miguel Angel Gomora	Unidad de Procesamiento Central	EF19A00488	1	Operación
Miguel Angel Gomora	Monitor	9177902211745018888P3K1:	1	Operación
Miguel Angel Gomora	Teclado	9152Q	1	Operación
Miguel Angel Gomora	Mouse	9702	1	Operación
Luis Flores	Unidad de Procesamiento Central	EF1988	1	Operación
Luis Flores	Monitor	K2191	1	Operación
Luis Flores	Teclado	65S00000	1	Operación
Luis Flores	Mouse	437	1	Operación
Luis Flores	Unidad de Procesamiento Central	ER34	1	Obsoleto
Luis Flores	Teclado	292	1	Obsoleto
Luis Flores	MS-Dos	345JU	1	Operación
Luis Flores	Microsoft Windows	695099	1	Operación
Luis Flores	Micrososft Windows NT	DDDD	1	Requerido

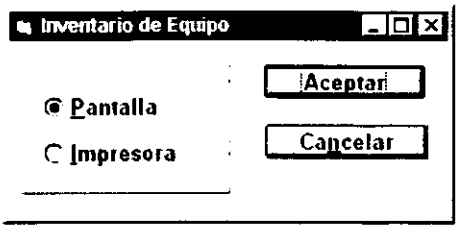
Elimina Cancelar

Consulta de Equipo. Aparece sólo el equipo que se encuentra registrado en la base de datos, Esta consulta puede ser tomando en cuenta los status o sin ser considerados.



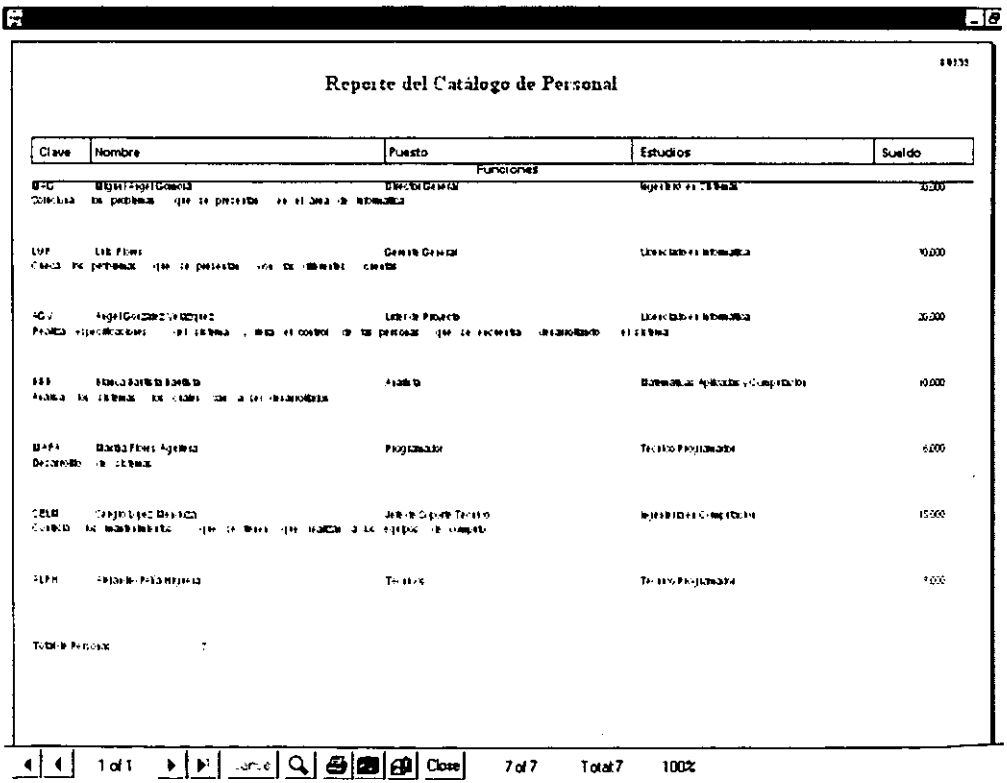
IV.3.3. REPORTES

En este comando se generan los reportes de información para el sistema. Las ventanas de generación de reportes son las semejantes, a continuación se muestra una forma de generación de reporte:

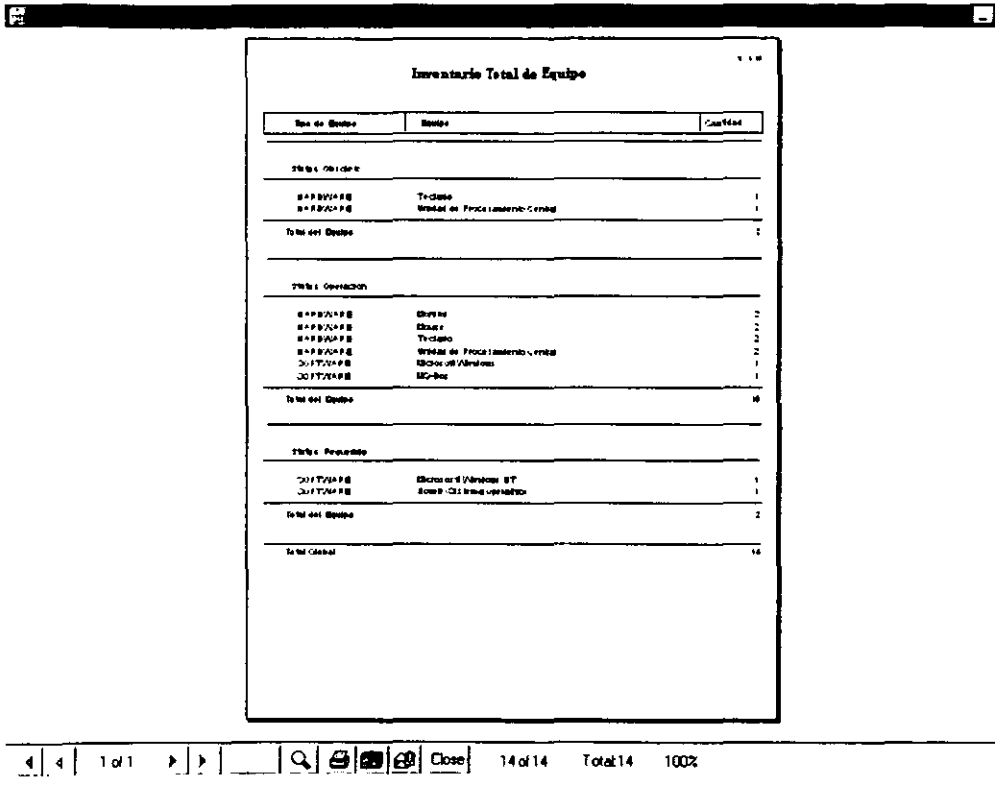


Los reportes están divididos en:

Reportes de Catálogos. Son los reportes con la información registrada en cada uno de los catálogos. Un ejemplo de reporte de catálogo es el siguiente:



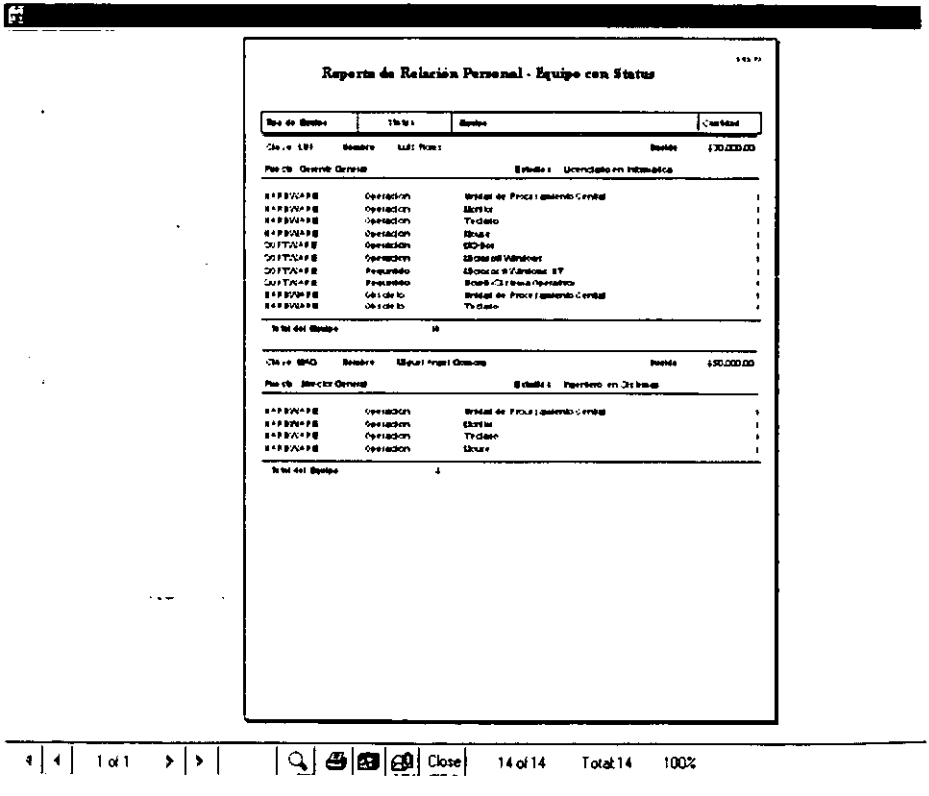
Reportes de Equipo. Son los reportes que dan información acerca del equipo, estos pueden ser total de equipo o por status con que se encuentre este. A continuación se muestra un reporte de equipo:



Reporte Relación Personal – Equipo. Este reporte contiene la información detallada de los recursos materiales que corresponde a cada uno de los recursos humanos.

Reporte Relación Personal – Equipo con Status. Este reporte contiene la misma información que el anterior con la diferencia de que divide por status los recursos materiales.

La figura que a continuación se muestra es un reporte que representa tanto a Reporte Relación Personal – Equipo y Reporte Relación Personal – Equipo con Status



IV.3.4. SALIR

Este comando es utilizado para salir del sistema.

IV.4. DESARROLLO

Una vez que se realizó el análisis y el diseño del sistema se procede al desarrollo del mismo.

El desarrollo es la parte donde se realiza la programación, y las pruebas correspondientes para la operación del sistema.

IV.4.1. CODIGO DE PROGRAMACION

Visual Basic es un lenguaje de programación orientado a objetos y a eventos sucedidos en cada objeto. A continuación se muestra la técnica de programación que se desarrollo en la forma de *Consulta de Equipo* la cual es parte del desarrollo del sistema.

```
Sub Ejecuta()
   Limpia_Spread sprEquipo
   Consulta_General
   Genera_Grafica (3)
End Sub

Function Genera_Grafica(Tipo)
   If sprEquipo.MaxRows > 1 Then
      Activa_Grafica (Tipo)
      Limpia_Grafica
      Grafica
   Else
      Inicial
   End If
   sprEquipo.Enabled = False
End Function

Sub Grafica()
   grpEquipo.YAxisMax = vfn_Valor + 2
   grpEquipo.YAxisTicks = vfn_Valor + 2
   grpEquipo.NumPoints = sprEquipo.MaxRows
   grpEquipo.AutoInc = 1
   For i = 1 To grpEquipo.NumPoints
         sprEquipo.Row = i
         grpEquipo.ThisPoint = i
         grpEquipo.LegendText = as_Equipo(i)
         grpEquipo.ThisPoint = i
         sprEquipo.Row = i
         sprEquipo.Col = 3
```

```
        grpEquipo.GraphData = Val(sprEquipo.Text)
    Next i
   grpEquipo.DrawMode = 2
End Sub

Sub Inicial()
   Me.Height = 3855
   Me.Width = 8820
   Me.Left = (Screen.Width - Me.Width) / 2
   Me.Top = ((Screen.Height - Me.Height) / 2) - 500
   spnGraficas.Visible = False
   frmGrafica.Visible = False
End Sub

Function Activa_Grafica(Tipo)
   Me.Height = 7875
   Me.Width = 8820
   Me.Left = (Screen.Width - Me.Width) / 2
   Me.Top = ((Screen.Height - Me.Height) / 2) - 500
   spnGraficas.Visible = True
   frmGrafica.Visible = True
   grpEquipo.GraphType = Tipo
   If Tipo = 1 Then
      optPie2d = True
   Else
      If Tipo = 2 Then
         optPie3D = True
      Else
         If Tipo = 3 Then
            optBarras2D = True
         Else
            optBarras4D = True
         End If
      End If
   End If
End Function

Sub Limpia_Grafica()
   grpEquipo.YAxisStyle = 2
   grpEquipo.YAxisMin = CERO
   grpEquipo.YAxisMax = CERO
   grpEquipo.YAxisTicks = 1
End Sub

Private Sub cmbTipo_Click()
   Ejecuta
End Sub

Private Sub cmdCancelar_Click()
   Habilita_Otros
   Unload Me
End Sub

Private Sub Form_Load()
   If Not Existe(T_TIPO) Then
      MsgBox "No existe información para realizar la consulta", vbInformation
      cmdAceptar.Enabled = False
      Exit Sub
   End If
   Call Llena_Combo(T_TIPO, K_CLAVE_T, 1)
   cmbTipo.AddItem NULO
   For i = 1 To vgn_Valor
      cmbTipo.AddItem ags_Descripcion(i)
   Next i
   Ejecuta
End Sub

Sub Consulta_General()
   Dim vls_Tipo As String
```

```
   Limpia_Arreglo
   sprEquipo.Enabled = True
   If cmbTipo.Text <> NULO Then
      vls_Tipo = " Where " & C_DESCRIPCION_T & " = '" & cmbTipo.Text & "'"
   Else
      vls_Tipo = NULO
   End If
   vgs_Query = "Select * From CEquipo"
   vgs_Query = vgs_Query & vls_Tipo & " Order By " & C_DESCRIPCION_E
   Set vgs_Snapshot = db_MyDataBase.OpenRecordset(vgs_Query, dbOpenSnapshot)
   If vgs_Snapshot.EOF Then
      MsgBox "No existen registros para esa consulta", vbInformation
      Exit Sub
   End If
   vgs_Snapshot.MoveLast
   vgn_Valor = vgs_Snapshot.RecordCount
   vgs_Snapshot.MoveFirst
   For i = 1 To vgn_Valor
      ReDim Preserve as_Tipo(i)
      ReDim Preserve as_Equipo(i)
      ReDim Preserve an_Cantidad(i)
      ReDim Preserve as_ClaveE(i)
      as_Equipo(i) = vgs_Snapshot(0)
      an_Cantidad(i) = vgs_Snapshot(1)
      as_Tipo(i) = vgs_Snapshot(2)
      as_ClaveE(i) = vgs_Snapshot(3)
      vgs_Snapshot.MoveNext
   Next i
   vgs_Snapshot.Close
   If vls_Tipo <> NULO Then
      sprEquipo.Col = 1
      sprEquipo.ColHidden = True
   Else
      sprEquipo.Col = 1
      sprEquipo.ColHidden = False
      sprEquipo.ColWidth(1) = 15
   End If
   sprEquipo.MaxRows = vgn_Valor
   For i = 1 To vgn_Valor
      sprEquipo.Row = i
      sprEquipo.Col = 1
      sprEquipo.Text = as_Tipo(i)
      sprEquipo.Col = 2
      sprEquipo.Text = as_Equipo(i)
      sprEquipo.Col = 3
      sprEquipo.Text = an_Cantidad(i)
      If vfn_Valor < an_Cantidad(i) Then
         vfn_Valor = an_Cantidad(i)
      End If
   Next i
End Sub

Sub Limpia_Arreglo()
   Erase as_Tipo()
   Erase as_Equipo()
   Erase as_ClaveE()
   Erase an_Cantidad()
End Sub

Private Sub optBarras2D_Click(Value As Integer)
   Genera_Grafica (3)
End Sub

Private Sub optBarras3D_Click(Value As Integer)
   Genera_Grafica (4)
End Sub

Private Sub optPie2d_Click(Value As Integer)
   Genera_Grafica (1)
```

```
End Sub

Private Sub optPie3D_Click(Value As Integer)
    Genera_Grafica (2)
End Sub
```

IV.4.1. PRUEBAS DE DESARROLLO

Para comprobar la operación del sistema se diseño un plan donde a continuación se muestra parte de ese:

Módulo/Función	Test	Tiempo	Status	Observaciones
Catálogo de Personal	Nuevo	1 ms	OK	
	Consulta	1 ms	OK	
	Elimina	1 ms	OK	
	Cambia	1 ms	OK	
	Salir	1 ms	OK	
Asignación de Equipo	Nuevo	2 ms	OK	
	Cambia	3 ms	OK	
	Elimina Renglón	1 ms	OK	
	Inserta Renglón	1 ms	OK	
Inventario de Equipo	Aceptar Pantalla	2 ms	OK	
	Aceptar Impresora	3 ms	OK	
	Cancelar	1 ms	OK	

IV.5. IMPLEMETACION

Una vez concluido el desarrollo del sistema y haciendo las pruebas necesarias del buen funcionamiento de este, se procede a la implantación del sistema. La implantación del sistema es la instalación de este en las computadoras en el cuál va a operar el sistema.

IV.5.1. REQUERIMIENTO DE OPERACIÓN DEL SISTEMA

Los requerimientos mínimos para la operación del sistema son:

Hardware

Procesador Pentium 133Mhz o superior

16 MB de memoria RAM

20 MB en Disco Duro

Mouse

Monitor VGA o Superior

Impresora

Software

Microsoft Windows 95 o Microsoft Windows NT

Excel v.97 (En el caso que se deseen exportar reportes)

IV.5.1. INSTALACIÓN DEL SISTEMA

La instalación del sistema es la puesta en operación del sistema.

El sistema cuenta con 4 discos de instalación. En estos discos se encuentran las librerías y ejecutables para que el sistema se ejecute correctamente.

El sistema se desarrollo bajo un ambiente Windows NT, Access v.7.0 y Visual Basic v.4.0 a 32 bits. La instalación del sistema se realizó en diferentes

equipos y con diferentes ambientes. En el equipo con el mismo ambiente en desarrollo no se detectó ningún problema.

En algunos equipo con Windows 95 o Windows 98 si se detectaron problemas debido a que al querer ejecutar el sistema enviaba un mensaje de error. Estos errores suceden frecuentemente por falta de librerías o diferencias de datos en ellas. Para corregir este tipo de errores se tiene que operar el sistema donde su operación sea la correcta y ejecutar el WPS. Este programa lista todas las librerías y programas que se encuentran en operación lo que ayuda a comparar librerías con otros equipos y poder sustituirlas cuando no sean las mismas.

CONCLUSIONES

En las culturas orientales el imitar a sus maestros y posteriormente superarlos, es parte de su educación. Filosofía que los a llevado a tener problemas con occidente en lo que se refiere a patentes y derechos de autor, sin embargo esta actitud los ha colocado en los primeros lugares de diferentes áreas del conocimiento humano.

Desafortunadamente no podemos decir lo mismo de nuestra gente y lo menciono por que me he dado cuenta de cómo se han desarrollado los departamentos de informática de las empresas en nuestro país, ya que en la mayoría de ellas independientemente del giro y del tamaño de las mismas, cuando tienen la necesidad de sistematizar o automatizar alguno de sus procesos adquieren uno o varios equipos de computo, contratan algunas personas que les ayude a manejarlos, compran algún paquete de software y se ponen a trabajar y la mayoría de las veces carecen de una estrategia informática y es con el paso del tiempo o debido a causas muy específicas que se llegan a preguntarse ¿con que recursos informáticos cuentan en la empresa en ese momento?. Los empresarios están preocupados en resolver las estrategias de sus negocios y prestan poca importancia a la **auditoria informática** termino poco conocido y menos aplicado en nuestra sociedad.

Pienso que ese caos administrativo se reduciría en gran medida si las empresas cuando adquieren sus equipos de computo contaran con los conocimientos básicos de la auditoria informática y con algún programa de computo para facilitar esa actividad.

BIBLIOGRAFIA

Control Interno, Auditoria y Seguridad Informática,
Cooper & Lybrand,
Madrid 1990

Datapro Reports on Information Security,
DATAPRO, McGraw Hill

El estudio y Evaluación de Interno en entornos Informatizados.
Documento número 1 del REA (Registro de Economistas Auditores)
Enero 1996

Guía de Seguridad Informática.
SEDESI, Madrid, 1997

Metodología de Auditoría AUDIFOR. Instituto de Auditores Internos de España (incluye programa informático).

Apuntes de la Asignatura de Auditoría Informática.
Fernández Sánchez, Carlos Manuel
Universidad Pontificia de Salamanca. Madrid.
Curso Académico 1996-1997.

Auditoría en Informática. Seguridad Informática, No. 17
Ramos González, Miguel Angel.
Noviembre 1995.

La Auditoría Informática. Actualidad Informática Aranzandi, No. 14
Enero 1995.

La Auditoría Informática. Métodos reglas, Normas. Masson.
Thorin M. (THOR89)
Barcelona, 1989.