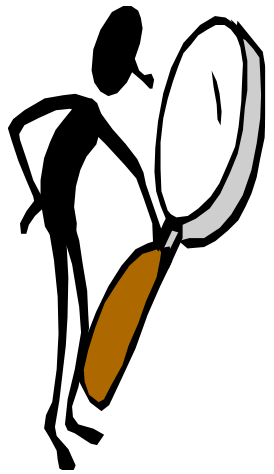
AUDITORIA INFORMATICA

Introducción

Esta es una breve introducción a las funciones de la Auditoria Informática

Es un resumen de diferentes documentos que hablan de la función de auditoría informática.



Evaluación durante la operación del sistema de cómputo

El ingeniero en informática debe de asegurarse que durante la operación del sistema de cómputo:

- Cumpla con los requerimientos del usuario.
- Se sigan las normas, políticas y procedimientos de seguridad.
- Se mantenga actualizado tecnológicamente
- Se efectúen auditorias informáticas programas y eventuales.

Auditoria en Informática

- Revisión analítica a la suficiencia de controles establecidos en el ámbito informático, con la finalidad de disminuir los riesgos y garantizar la seguridad, confiabilidad y exactitud de la información**.**

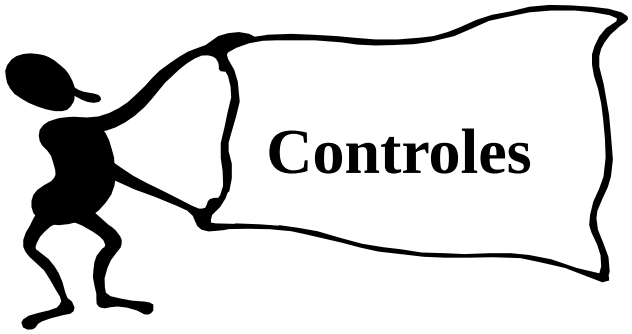
- La función del auditor va encaminada a prevenir y vigilar el control de la función del procesamiento de datos, apoyar en el establecimiento de estándares en la empresa y pugnar por la conservación de los activos informáticos de la misma.

- Se parte de la existencia de normas, políticas y procedimientos que rigen a la función informática y delimita el nivel de congruencia con el ejercicio de los mismos.

Auditoria en Informática

Su función es descubrir fraudes, robo electrónico, alteración o modificación de programas, difamación, etc..., riesgos que repercuten en daños económicos.

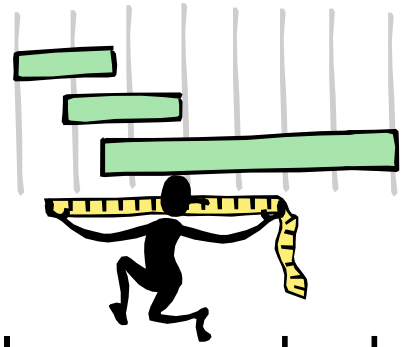
La auditoria tiene como apoyo a los controles para mantener la seguridad de los sistemas de información.



Importancia

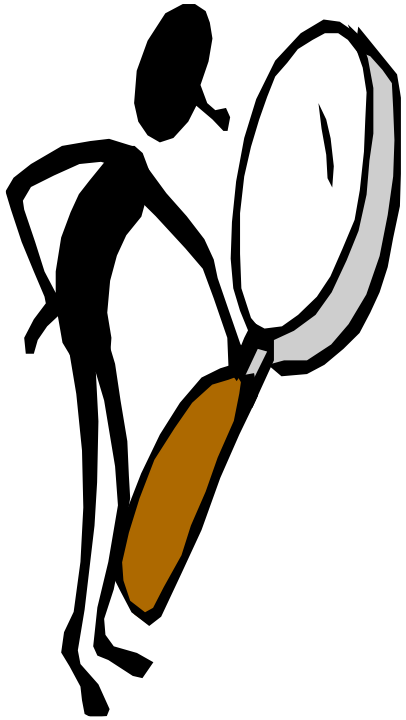
Un sistema de información se constituye por un conjunto de procedimientos manuales y computarizados.

El objetivo de la auditoría es asegurar que la información que producen los sistemas sea confiable, útil y oportuna entre otras.



Para lograrlo se ayuda de los controles.

Auditoria Informática.

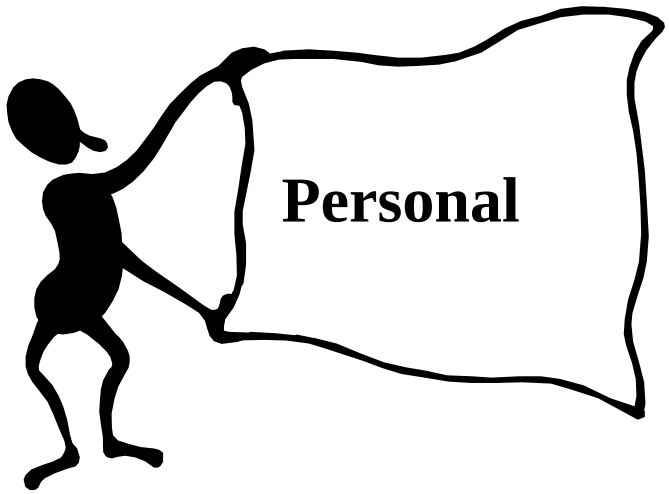


- Monitorea el cumplimiento del programa de seguridad informática.
- Revisa el acatamiento y el apego a las políticas y normas.

Objetivos particulares

Personal.- Contar con personal altamente calificado para la realización de su función.

- Cuerpo de gerentes
- Supervisores
- Técnicos
- Operadores

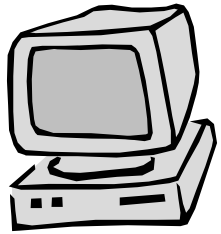


Objetivos particulares

Personal de la institución.

- Cumple con lo establecido en las políticas y normas de seguridad.
- Reporta excepciones al coordinador de seguridad.
- Participa en los programas de concientización.

Objetivos particulares



Grupo de emergencia ante contingencias.

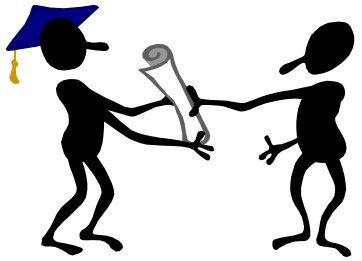
- Apoyan ante la presencia de fallas de en la seguridad.
- Diagnostican problema,
- Corrigen fallas y ajustan las tecnologías de protección.
- Notifican la problemática a otras áreas técnicas a fines.

Objetivos particulares

Grupo de instrucción detección

(Tiger Teams).

- Evalúan nivel de seguridad en la organización.
- Detectan riesgos y fallas presentes en las tecnologías y aplicaciones.
- Documentan problemáticas y proponen acciones de solución.



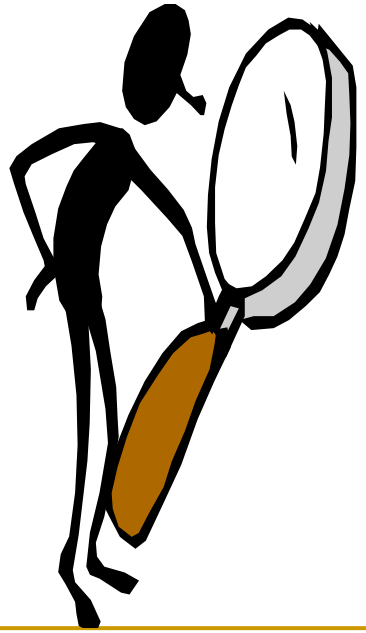
Objetivos particulares

Administradores

(Firewalls).

- Aplican políticas de seguridad establecidas.
- Parametrizan el firewall.
- Dan seguimiento a situaciones de excepción.
- Generar respaldos periódicos.
- Dan apoyo ante afectación del servicio.

Funciones Generales del Auditor



Funciones generales

- Diseñar, establecer (si no existe) y verificar que se lleve a cabo métodos de respaldo y control que garanticen la continuidad de los servicios a los usuarios.

- Elaborar (si no existe) y verificar que sea adecuado el plan de contingencia de todo el procesamiento electrónico de datos.
- Establecer los controles adecuados que garanticen la completa protección de todos los recursos de cómputo.

Funciones generales

•Investigar , estudiar y proponer la adquisición y utilización de nuevos equipos de cómputo.

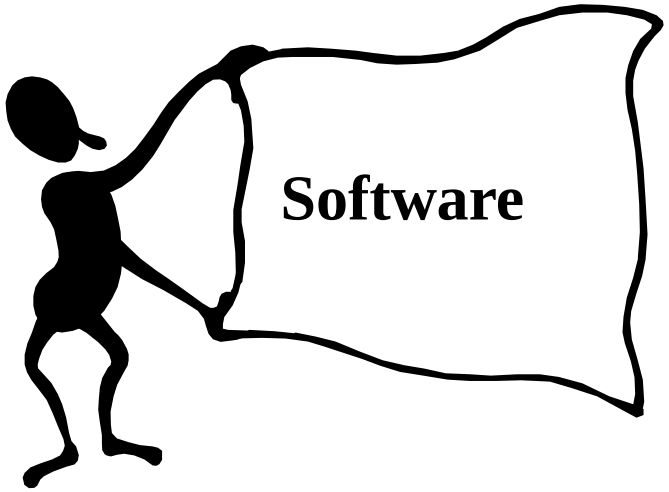
•Mantener y actualizar la configuración de los equipos electrónicos y redes de comunicación para satisfacer las necesidades de crecimiento, implantación de nuevas aplicaciones y niveles de servicio ofrecidos a los usuarios.

Objetivos particulares

Software

Verificar que se este a la vanguardia en tecnología de software:

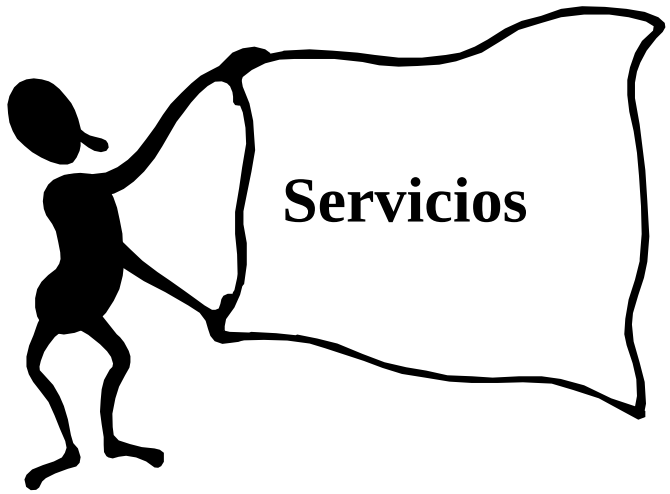
- Sistema operativo
  - Utilería
  - Métodos de acceso
  - Lenguajes
- Software de comunicaciones
- Software de base de datos



Objetivos particulares

Servicio a usuarios.- Mejorar y mantener los niveles de servicio al usuario en sus necesidades.

- Consultas
- Capacitación
- Documentación
- Implementación



Objetivos particulares

Red de comunicaciones

Mejorar y mantener una red de comunicaciones que integre todos los niveles de procesamiento, cubriendo las siguientes características:

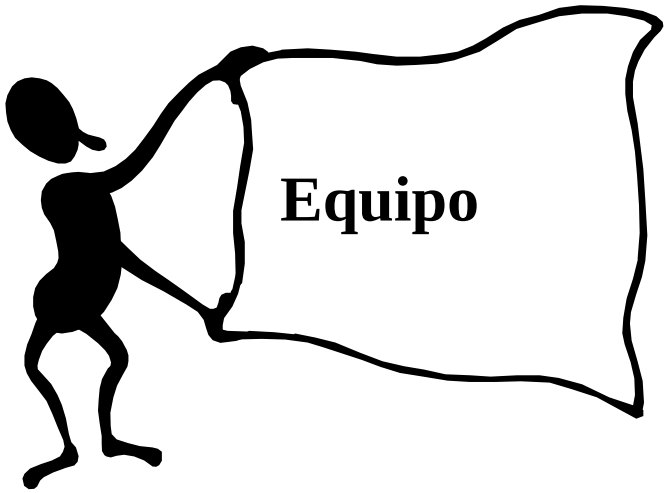
- Confiable
- Segura
- Estándar
- Flexible
- Integrada

Objetivos particulares

Equipo

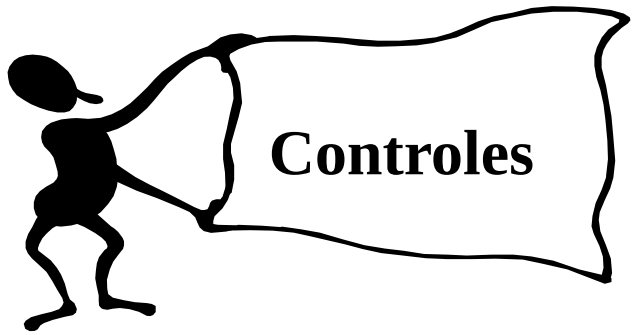
Contar con la tecnología más avanzada en materia de equipo de computo para:

- Centros de cómputo
- red de comunicaciones
- Terminales
- Captura de datos
- Microcomputadoras



Objetivos particulares

La auditoria tiene como apoyo a los controles para mantener la seguridad de los sistemas de información



Tipo de controles

Preventivos	Evitan que ocurran errores o irregularidades
Detectivos	Emiten una señal (sonido, mensaje, etc.) cuando un error o irregularidad ha ocurrido
Correctivos	Contribuyen a la corrección cuando un error o irregularidad ha ocurrido.

La auditoria se apoya más de los controles detectivos y correctivos

Los controles como apoyo de la auditoria

El uso de controles hace que tiendan a disminuir los riesgos en la frontera del sistema: entrada de datos, procesamiento de datos y la salida de información.

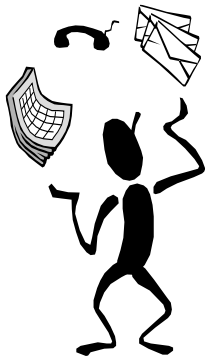
Los controles ofrecen una razonable seguridad de que las operaciones básicas funcionen y se ejecuten tal y como fueron diseñadas, que ña seguridad de los datos se mantenga y que los errores se detecten oportunamente

Software de auditoría en el mercado

En el mercado existen todo tipo de software para auxiliar al auditor para hacer sus funciones, desde simples hojas de calculo hasta sofisticados sistemas.

El objetivo será seleccionar la herramienta apropiada basandose en el tipo de sistema a auditar y la funcionalidad y resultados que se esperan obtener.

Software de auditoría en el mercado



Algunas herramientas, programas o software se ubican en dos o más categorías, esto implica que son más completas, frecuentemente este software esta dividido en módulos y cada uno corresponde a una de las categorías.

1. Facilitan el entendimiento del auditor de sistemas dentro de la organización
2. Facilitan la recolección de pruebas sobre la calidad e integridad de los datos
3. Permiten evaluar la calidad y robustez de la programación
4. Recolectan información sobre la eficiencia (productividad) de una instalación.

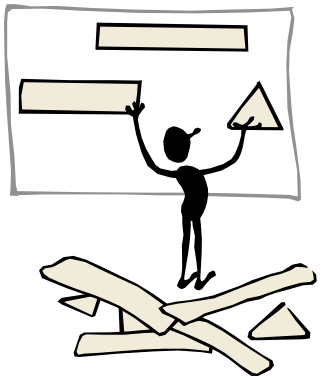
Software de auditoría en el mercado

- La eficiencia del auditor depende de su capacidad de entender los programas y los datos en un tiempo mínimo.
- Esto se complica si no se tienen especificaciones robustas, estándares, programación estructurada o archivos planos.

Facilitan el entendimiento del auditor dentro de la organización

Software de auditoría en el mercado

Para entender la lógica y relaciónes entre programas y datos el auditor se basa en las mismas herramientas que auxilian al diseñador del sistema



Herramientas - Diagramas

- Contexto
- Jerarquía HIPO Entrada-Proceso-Salida.
- Estructura de la base de datos
- Transición de estados (distintos estados que puede estar un modulo o función)
- Estado o autómatas (describen protocolos o gramáticas de transición a nivel muy bajo)
- Flujo de datos

Software de auditoría en el mercado

Herramientas Generales

- Diccionario de datos.
- Reglas de negocio
- Referencias cruzadas entre Bases de Datos
- Analizador del perfil de transacciones (frecuencia con la que se actualizan los datos y los índices que mantienen la integridad).
- Cartas descriptivas (flujo de datos y control de cada programa, modulo o función).
- Pantallas o Guis (Pantallas de captura y presentación de datos).
- Reportes de Salida
- Mapas de ejecución
- Listado de referencias cruzadas

Software de auditoría en el mercado

Diagramas de la programación basada en objetos

- De especificaciones del comportamiento de los objetos definidos por el usuario
- De herencia
- De llamadas entre objetos
- De relación con el Back-end
- De especificaciones del comportamiento de los objetos.

Herramientas generales basada en objetos

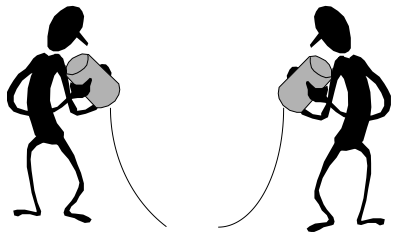
- Catalogo de objetos
- Tablas declarativas

Software de auditoría en el mercado

Este software apoya al auditor como:

Generador de limites o parámetros frontera de pruebas (los valores frontera son los que se alimentaran al generador de datos prueba).

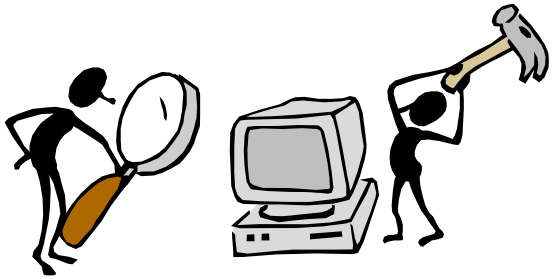
- Generador de datos de prueba.
- Trace o Debugger
- Monitoreo de ejecución (Rastreo del camino de ejecución, para poder detectar con mayor facilidad la fuente de error).
- Simulador de entradas y salidas (Simular la comunicación con otros programas o sistemas para poder detectar fallas de comunicación).



Software de auditoría en el mercado

Este software apoya al auditor como:

- Diagramador de pruebas (actúa como agenda de las prueba, registra las pruebas efectuadas y las faltantes, las anomalías detectadas y procesos correctos).
- Monitor de concurrencias (evalúa el performance del sistema y cuanto tiempo ocupa de CPU).
- Comparación de código (compara los programas que se dejaron para instalación y los que están en producción).



Software de auditoría en el mercado

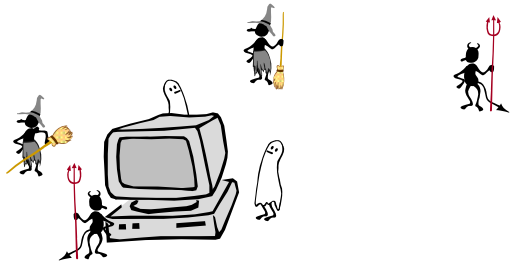
Este software apoya al auditor como:

- Utilización del CPU (detecta errores y limites).
- Utilización de memoria expandida (detectar errores y limites).
- Utilización de almacenamiento (Que tanto se almacena en disco y que tanto se utiliza).
- Utilización de canales de comunicación (detectar fuentes de envío, destino y si un elemento extraño esta haciendo uso del sistema).
- Utilización de periféricos (Proporciona estadísticas del uso de los periféricos).

Software de auditoría en el mercado

Este software apoya al auditor como:

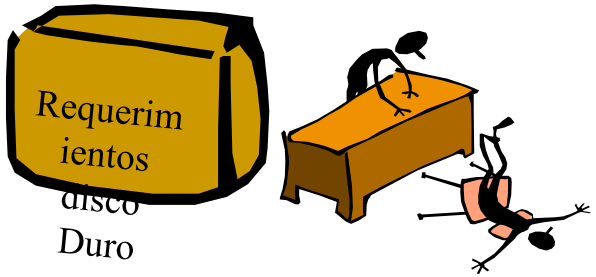
- Tiempo de respuesta (detectar la causa por la que el tiempo de respuesta es bajo o alto, si es por la comunicación o por el sistema mismo).
- Pruebas de contención (detectar el origen de la contención, identificando los accesos de todos los usuarios y disparando una alarma cuando se tenga contención).
- Largo de los querys (Identificar si usan las llaves apropiadas y si no hacen exceso de lecturas)
- Tiempos de búsqueda (Detectar si los algoritmos de búsqueda son los apropiados, que la búsqueda no sea lenta)



Software de auditoría en el mercado

Este software apoya al auditor como:

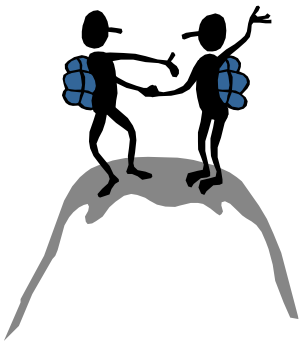
- Monitoreo de paginación (saber que aplicaciones consumen más recursos de disco).
- Frecuencia de checkpoints (Puntos de chequeo que permiten ver como andan los recursos).



Software de auditoría en el mercado

Este software apoya al auditor como:

- Pistas de auditoría.
- Uso de archivos de log.
- Utilizar de metodologías bien definidas para el desarrollo de aplicaciones.
- Uso de una estructura del sistema que permita crear ambientes de prueba.



Ejemplo de software comercial existente en el mercado para efectuar evaluaciones

Pruebas comparativas, Benchmark

Software que mide el rendimiento de una aplicación (sistema de información), computadora, componente.

Ayuda también a evaluar procesos bajo diferentes configuraciones de Hardware y Software.

Pruebas de Sistema.- Evalúan el rendimiento global o parte del sistema, ejecuta y cronometra el tiempo de respuesta.

a) **Pruebas de aplicación o Aplicación-Base (Application-based)**.- Evalúan el rendimiento de una aplicación en ejecución, como esta operando. Ejecuta y cronometra. Winstone de ZDnet

Pruebas comparativas, Benchmark

b) **Pruebas PlayBack** (Test Playback).- Usan llamadas al sistema durante actividades especificas de una aplicación y la ejecutan de forma aislada, ejemplo uso de memoria, generación de gráficos, etc. Mide como funciona una parte del sistema.(Winbench de Zdnet prueba gráficos, Cd-Rom, acceso a disco duro, etc.).

c) **Prueba sintética (Synthetic Test).-** Enlaza actividades de aplicación en subsistemas específicos. Winbench usa las pruebas de procesadores y SPEC 92, Norton SI 32*, CPUmark 32*, Indice iCOMP®2.0 (para aplicaciones de 32 bit´s).

Pruebas comparativas, Benchmark

d) Pruebas de Inspección- - Evalúan a la aplicación bajo simulación de cargas de trabajo. Verifican comportamiento, mide rendimiento operación por operación (Test Inspect WinBench de ZDnet,).

Pruebas modernas de sistema

Evalúan la ejecución de una aplicación con varias aplicaciones corriendo simultáneamente, varios procesadores, requerimiento de mucha memoria, velocidades mas rápidas de transmisión de datos en red, API`s (interfaces), reconocimiento de voz, uso intensivo de video, audio y/o gráficos. SYSmark*32 para Windows 95, SYSmark para Windows NT (32 bits, aplicaciones reales y multitarea).

Pruebas comparativas, Benchnark

Evalúan solamente partes especificas de la computadora. Son software de prueba que avalúa el rendimiento del procesador, acceso a memoria, etc.

Dhrystone, PowerMeter MIPS y Wintune (versión modificada de Dhrystone**).-** Prueba de rendimiento del procesador. Evalúa millones de instrucciones por minuto (MIPS).

Contiene ejemplos representativos de las operaciones requeridas por las aplicaciones, hace complicadas secuencias de instrucciones usadas por las aplicaciones. Se mide el tiempo que toma la ejecución de esas secuencias de instrucciones. Es un programa que envía cargas de trabajo al procesador.

Pruebas comparativas, Benchnark

Whestone y Wintune (versión modificada de Whestone**).-** . Prueba del rendimiento del procesador con operaciones de punto flotante. Evalúa millones de instrucciones por minuto (MFLOPS). La aritmética de punto flotante es la mas significativa para operaciones científicas, estadísticas, programas de diseño, hoja de calculo, dibujo, movimiento de imagen, etc. Este es muy utilizado para medir rendimiento del procesador. Prueba tambien operaciones con numeros enteros.

SPEC 92, SPECint*95, SPECfp*95 .- Prueba la CPU y el acceso a memoria basado en aplicaciones reales.

Pruebas comparativas, Benchnark

Benchmark de evaluación del procesador.

- Spec (System Performance evaluation Comparative).
- Stanford
- Integer
- Linpack
- Livermore_lux
- Whetstone

Benchmark para sistemas multiusuario o Benchmark de evaluación general.

- AIM III
- Masbus.
- Benchmark para ambientes de base de datos.
- TPC-A
- TPC-B
- TPC-C
- WISCONCIS'N
- AS3Ap
- SETQUERY
- BUSINESS-BENCHMARK

Establecimiento del estado del sistema de cómputo

De acuerdo con el reporte de auditoria (evaluación) el ingeniero en informática establece adecuaciones, cambios y recomendaciones.

El ingeniero en informática tiene las siguientes alternativas

- **No hay recomendaciones** – Continuar trabajando como hasta ahora.
- **Adecuaciones menores** – Efectuar pequeñas adecuaciones a procedimientos, actividades, etc.
- **Cambios o adecuaciones al sistema de cómputo** – Efectuar mantenimiento al sistema de cómputo
- **Cambios mayores al sistema de computo** – Efectuar reingeniería al sistema de cómputo
- **Sustituir el sistema de cómputo actual** – El sistema de computo actual no sirve y se requiere uno nuevo que satisfaga los requerimientos del cliente, la organización y el medio ambiente.

Sustituir el Sistema de Cómputo (S.C.) actual

- Si el resultado de la evaluación es sustituir el sistema de computo actual se inicia con el proceso de evaluación de selección. Cerrando con esto el circulo de evaluación.

Diseño de la auditoria

- La auditoria se basa en los lineamientos establecidos por las seguridad. Los datos, archivos, accesos, procesos, áreas, etc. que se debe establecer seguridad y el grado de seguridad requerida. La auditoria establece las fechas para verificar que la seguridad de la información. La auditoria se puede efectuar de dos formas programada o sorpresa.
- Se recomienda que un sistema se establezcan ambas

Nivel de seguridad

1 – Alta

2 - Media

3 – Mínima

4 – Sin seguridad

Matriz de consideraciones para la seguridad / auditoria del sistema de cómputo

Elemento(s) a establecer seguridad (datos, archivos, procesos, etc.)	Nivel de seguridad	Especificación de consideraciones y procesos de seguridad	Programación de fechas para realizar la auditoria
-------	----	--------	------
-------	----	-------	
------	----	------	

Reporte de auditoria

Una vez que se efectúa la evaluación se desarrolla un reporte con los puntos detectados. El siguiente reporte es un ejemplo la empresa o el auditor establecerá el formato que mejor se adapte a las necesidades.

Puntos detectados	En el dato, archivo, procedimiento, etc,	Recomen-daciones o correcciones	Fecha entrega o instalación de correción
-----	-----	-----	---
------	-----	-----	----