AUDITORÍA EN INFORMATICA

LA AUDITORÍA COMO ACTIVIDAD PROFESIONAL.

Concepto universal de auditoría.

Representa el examen de los estados financieros de una entidad, con el objeto de que el contador público independiente emita una opinión profesional respecto a si dichos estados representan la situación financiera, los resultados de la operaciones, las variaciones en el capital contable y los cambios en la situación financiera de una empresa, de acuerdo con los principios de contabilidad generalmente aceptados. (IMCP)

La auditoría representa el examen de los estados financieros de una entidad, con el fin de emitir una opinión sobre la razonabilidad de las cifras que de ellos emanen.

Aunque en la actualidad se realizan diversos tipos de auditoría, todos no llevan a emitir una opinión sobre algún registro, sistema, operación o actividad en particular o con fines específicos.

1. CONCEPTO DE AUDITORÍA EN INFORMATICA:

La Auditoría en informática se refiere a la revisión práctica que se realiza sobre los recursos informáticos con que cuenta una entidad con el fin de emitir un informe o dictamen sobre la situación en que se desarrollan y se utilizan esos recursos. (José de Jesús Aguirre Bautista)

2. Clasificación de la auditoría.

Tradicionalmente se consideran dos tipos de auditoría: las internas y las externas

La auditoría interna la desarrollan personan que pueden o no depender de la entidad y actúan revisando, las más de las veces, aspectos que interesan particularmente a la administración, aunque pueden efectuar revisiones programadas sobre todos los aspectos operativos y de registro de la empresa, con el fin de emitir un informe sobre su revisión.

La auditoría externa, conocida también como auditoría independiente, la efectúan profesionistas que no dependen de la empresa, ni económicamente ni bajo cualquier otro concepto, y a los que se conoce un juicio imparcial merecedor de la confianza de terceros. El objeto de su trabajo es la emisión de un dictamen. Esta clase de auditoría es la actividad más característica del Contador Público o del Licenciado en Informática.

También existen otros tipos de auditoría como son:

Auditoría operacional, se refiere a la revisión de la operación de una empresa y se juzga la eficiencia de la operación misma.

Auditoría administrativa, se refiere a la organización y eficiencia de la estructura del personal con que cuenta la empresa y los procesos administrativos en que actúa dicho personal.

Auditoría social.-se refiere ala revisión del entorno social en que se ubica y desarrolla una empresa, con el fin de valorar aspectos externos e internos que infieran en la productividad de la misma.

	AUDITORÍA ADMINISTRATIVA	AUDITORÍA OPERACIONAL	AUDITORÍA CONTABLE	AUDITORÍA INFORMÁTICA
NATURALEZA	Técnica de Control Administrativo	Técnica de Control Administrativo	Técnica de Control Administrativo	Técnica de Control Administrativo
PROPÓSITO/ OBJETIVO	Evaluar y mejorar la administración	Promover la eficiencia en las operaciones	Dictamen a los Estados Financieros	Evaluar los recursos informáticos
ALCANCE	La eficiencia y productividad de el proceso productivo	La eficiencia de las operaciones	El sistema contable	Todas las actividades informáticas
FUNDAMENTO	La ciencia Administrativa y la normatividad de la empresa	La ciencia Administrativa y la normatividad de la empresa	Principios de contabilidad y normas de auditoría	Normatividad institucional y legal
METODOLOGÍA	Apoyado en Métodos Científicos	Técnicas y procedimientos predeterminadas	Técnicas y procedimientos predeterminadas	Técnicas y procedimientos predeterminados
APLICACIÓN	A la empresa y sus funciones básicas	A las funciones de la empresa	A los estados financieros	A todas las áreas de la empresa
PROYECCIÓN	Hacia el futuro	Hacia el futuro	Hacia el pasado	Hacia el futuro
INFORME	Amplio	Amplio	Preciso	Amplio y Preciso

3. IMPORTANCIA DE LA AUDITORÍA EN INFORMÁTICA.

Siempre ha existido la preocupación por parte de las organizaciones por optimizar todos los recursos con que cuenta la entidad, sin embargo por lo que respecta a la tecnología de informática, es decir, software, hardware, sistemas de información, investigación tecnológica, redes locales, bases de datos, ingeniería de software, telecomunicaciones, etc. esta representa una herramienta estratégica que representa rentabilidad y ventaja competitiva frente a sus similares en el mercado, en el ámbito de los sistemas de información y tecnología un alto porcentaje de las empresas tiene problemas en el manejo y control, tanto de los datos como de los elementos que almacena, procesa y distribuye.

El propósito de la revisión de la auditoría en informática, es el verificar que los recursos, es decir, información, energía, dinero, equipo, personal, programas de cómputo y materiales son adecuadamente coordinados y vigilados por la gerencia o por quien ellos designen.

Durante años se ha detectado el despilfarro de los recursos o uso inadecuado de los mismos, especialmente en informática, se ha mostrado interés por llegar por llegar a la meta sin importar el costo y los problemas de productividad.

4. ANTECEDENTES DE LA AUDITORÍA EN INFORMATICA.

Sí bien la auditoría se ha llevado a cabo desde, que el hombre hizo su aparición, esta se llevaba de manera empírica, ha sido de gran ayuda para los pueblos conquistadores, ya que tenían que conocer y dar fe de los tributos que les rendían los pueblos conquistados, en México los "oidores" de la corona española, que con el paso del tiempo se transformarían en auditores, que vigilaban el pago de quinto real a los reyes de España.

La auditoría en informática es más reciente, se tiene como antecedente más cercano a los Estados Unidos de América.

En los años cuarenta se empezaron a dar resultados relevantes en el campo de la computación, con sistemas de apoyos para estrategias militares, sin embargo, la seguridad y el control solo se limitaba a dar custodia física a los equipos y a permitir el uso de los mismos solo a personal altamente calificado.

Con el paso de los años la informática y todos los elementos tecnológicos, que la rodean han ido creando necesidades, en cada sector social y se han vuelto un requerimiento permanente para el logro de soluciones.

5. Áreas a auditar en Informática

Las áreas a auditar en donde se puede realizar la auditoría en informática, puede ser:

- A toda la Entidad.
- A un departamento.
- A un área
- A una función
- A una subfunción.

Y se pueden aplicar los siguientes tipos de auditoría:

- Auditoría al ciclo de vida del desarrollo de un sistema
- Auditoría a un sistema en operación
- Auditoría a controles generales (gestión)
- Auditoría a la administración de la función de informática.
- Auditoría a microcomputadoras aisladas
- Auditoría a redes.

Clasificación de acuerdo a José de Jesús Aguirre Bautista.

II. MUESTREO ESTADÍSTICO EN LA AUDITORIA.

1. Conceptos básicos de muestreo.

Hasta el día de hoy la Comisión de Normas y Procedimientos de Auditoría ha emitido el boletín 5020, relativo al muestreo en auditoria que comprende tanto muestreo estadístico como no estadístico.

El muestreo estadístico es aquél en el que la determinación del tamaño de la muestra, la selección de las partidas que la integran y la evaluación de los resultados, se hacen por métodos matemáticos basados en cálculos de probabilidades. (IMCP)

- Población es el conjunto de todos los elementos de interés en un estudio.
- Una muestra es un subconjunto de una población.

2. Métodos de muestreo utilizados en auditoría.

Existen varios tipos de muestras que se utilizan en auditoria, si bien el IMCP, solo menciona el muestreo de atributos y Muestreo de variables, existen otros tipos de muestreo, que depende del auditor pueden ser útiles para desarrollar los procedimientos de auditoria entre ellos encontramos:

- Muestreo aleatorio simple
- Muestreo estratificado
- Muestreo de atributos
- Muestreo de aceptación.
- Muestreo por conglomerados
- Muestreo sistemático
- Muestreo por conveniencia
- Muestreo por juicio.

2.1 Muestreo aleatorio simple

La definición de este método y el proceso de seleccionar una muestra aleatoria simple depende si la población es finita o infinita.

- Muestreo aleatorio simple (población finita)

Una muestra aleatoria simple de tamaño ***n,*** de una población finita de tamaño ***N***, es una muestra seleccionada de tal manera que cada muestra posible de tamaño ***n*** tenga la misma probabilidad de ser seleccionada.

- Muestreo aleatorio simple (población infinita)

Es aquella que se selecciona de tal forma que se satisfacen las siguientes condiciones:

- Cada elemento seleccionado proviene de la misma selección.
- Cada elemento se selecciona de forma independiente.

2.2 Muestreo Estratificado.

En este tipo de muestreo primero se dividen los elementos de la población en grupos llamados *estratos,* de tal manera que cada elemento de la población pertenece a uno y solo a un estrato. Si los estratos son homogéneos el procedimiento de muestreo estratificado producirá resultados tan precisos que como el muestreo aleatorio simple, pero con menor tamaño de la muestra.

2.3 . Muestreo por atributos **(Recomendado por el IMCP)**

El muestreo por atributos es un método estadístico que se utiliza para calcular la proporción de partidas de una población que contiene una característica o un atributo de interés. Esta proporción recibe el nombre de tasa de concurrencia o tasa de excepción y es la proporción de partidas que contienen el atributo específico en relación al número total de partidas

de la población. La tasa de ocurrencia por lo general se expresa como un porcentaje.

A los auditores les interesa la ocurrencia de los siguientes tipos de excepciones en las poblaciones de datos contables:

- Desviación de los procedimientos del control establecido por el cliente.
- Errores o irregularidades monetarias en los datos de las operaciones.
- Errores o irregularidades monetarias en los detalles de los saldos en las cuentas.

El auditor llegara a la conclusión que la tasa de excepción de la muestra es el calculo mas probable de la tasa de excepción de la población.

Dado que se basa en una muestra, sin embargo, existe una probabilidad significativa que en la tasa de excepción de la muestra y la tasa de excepción de la población real difieran. Los métodos estadísticos permiten al auditor indicar la medida en que los dos índices de excepción probablemente difieran y la confiabilidad del cálculo. Lo primero recibe el nombre de precisión y lo segundo riesgo de muestreo. Así pues una vez que se calcula el índice de excepción de la muestra, el auditor determinara la precisión del cálculo, lo sumara y lo restara del índice de excepción de la población. El auditor llegara a la conclusión que el calculo del intervalo contiene el índice de excepción real de la población en determinado riesgo de muestreo.

El Universo

Se llama así al cuerpo de datos en donde el auditor desea extraer muestras para llegar a una conclusión, e auditor deberá determinar que el universo en donde extrae la muestra es apropiado para el objetivo específico de la auditoría.

Las partidas individuales que componen el universo se conocen como unidades de muestreo para obtener una muestra efectiva y eficiente que le permita alcanzar el objetivo particular de auditoría.

Riesgo y certidumbre

Al programar la auditoría, el auditor utiliza su criterio profesional para determinar el nivel de riesgo de auditoría apropiado.

Los riesgos de auditoría incluyen:

- El riesgo de que ocurrirán errores importantes también conocidos como riesgo inherente.
- El riesgo de que el sistema de control interno contable del cliente no prevenga ni corrija tales errores también conocido como riesgo de control.
- El riesgo de cualquier otro error importante no sea detectado por el auditor también, conocido como riesgo de detección.

El objetivo del auditor debería ser el reducir el riesgo fuera del muestreo a un nivel mínimo por medio de un planeación, dirección, supervisión y revisión adecuada.

Error Tolerable

Es el error máximo en el universo que el auditor estaría dispuesto a aceptar y a pesar de eso concluir que el resultado del muestreo ha alcanzado su objetivo de auditoría. El error tolerable es considerado durante la etapa de planeación y se relaciona con el juicio preliminar del auditor respecto a la importancia. A menos grado de error tolerable, será mayor el tamaño e la muestra que requerirá el auditor.

En los procedimientos de cumplimiento el error tolerable es el porcentaje máximo de desviación de un procedimiento de control prescrito que el auditor estaría dispuesto a aceptar sin alterar el grado de confianza que tenía planeado depositar en el control que esta probando. En el caso de procedimientos sustantivos, el error tolerable es el error monetario máximo en el saldo de una cuenta o transacción que el auditor estaría dispuesto aceptar de manera que al considerar los resultados de todos los procedimientos de auditoría, este en posición de concluir con razonable seguridad, que la información financiera no contiene errores importantes.

Error esperado en el universo

Si el auditor espera la presencia del error, normalmente tendrá que examinar una muestra mayor para concluir que el valor del universo esta razonablemente presentado dentro del error tolerable estimado o que la confianza que se había planeado depositar en un control importante esta justificada, las muestras de mayor tamaño se justifican cuando se esperan que el universo se encuentre libre de errores. Al determinar el error esperado en un universo, el auditor deberá considerar asuntos tales como niveles de error identificados en auditorías previas, cambios en los procedimientos de los clientes y evidencia disponible de su evaluación del sistema de control interno contable y de los resultados de procedimientos de revisión analíticos.

III. METODOLOGÍA GENERAL PARA LA AUDITORIA EN INFORMÁTICA.

1.- Introducción

Metodología es una secuencia de pasos lógica y ordenada de proceder para llegar a un resultado. Generalmente existen diversas formas de obtener un resultado determinado, y de esto se deriva la existencia de varias metodologías para llevar a cabo una auditoria informática.

- Planeación. Esta consiste en la elaboración de los programas de trabajo que se llevaran acabo durante la revisión a la entidad auditada.

  - Trabajos preliminares.- Consisten básicamente, de una serie de entrevistas con nuestro cliente, las cuales tienen como objetivo dejar en claro las características básicas del trabajo que se va a realizar, que es lo que quiere el cliente y que hará, en términos generales, el auditor.

  - Diagnóstico Administrativo - El Diagnóstico Administrativo tiene por objetivo, proporcionarnos una panorámica de cómo la empresa percibe y practica la Administración.

  - Investigación Previa.- Aquí conoceremos la empresa y de ser posible validaremos la problemática que nos fue expuesta por el cliente. Después de esta fase se estará en posibilidades de hacer una mejor estimación del tiempo y de los honorarios, si es que no lo pudo hacer en la primera fase.

  - Elaboración del programa de la AI.- Todo buen administrador debe planear sus actividades y el auditor no debe ser la excepción, el programa señala

las actividades que han de realizarse, fechas de inicio y término, así como los tiempos.

- Obtención de la Información:

  - En esta fase se obtendrá toda la información pertinente sobre el caso estudiado, pudiendo recurrir a herramientas como: entrevistas, encuestas, observación, etc., dependiendo el tipo de información que necesite.

- Análisis, clasificación y evaluación de la información:

  - El análisis y clasificación de la información podrá realizarse por métodos estadísticos
  - Evaluación es aquí en donde se pone a prueba el talento del auditor, por que para entender e interpretar la información y continuar con el siguiente paso.

- Informe, elaboración y presentación del informe final.

  - En él se informará de manera clara y concisa, sobre los resultados de la AI. No debemos olvidar que a los ojos de nuestro cliente él paga por recibir un informe, y en él debe encontrar valiosas recomendaciones que habrán de mejorar su administración., el informe aunque es escrito, debe presentarse apoyado en una exposición verbal.

  - Implementación y seguimiento: Algunos autores consideran esta fase como opcional, que no corresponde al auditor realizarla, sino a la empresa, yo considero que el auditor debe participar, para que se interpreten correctamente sus recomendaciones y no haya lugar a desvíos en las mismas.

Etapas de la Metodología

l método de trabajo del auditor pasa por las siguientes etapas:

Alcance y Objetivos de la Auditoría Informática

Estudio inicial del entorno auditable

Determinación de los recursos necesarios para realizar la auditoría

Elaboración del plan y de los Programas de Trabajo

Actividades propiamente dichas de la auditoría

IV. AUDITORÍA DE SISTEMAS

La experiencia de la mayoría de las empresas nos indica que los resultados obtenidos del proceso de desarrollo de los sistemas de información son deficientes. Mencionaré algunos problemas como ejemplo:

- Costos en una proporción inadecuada a los beneficios.
- Incremento en la escala del proyecto.
- Sistemas no integrales o aislados.
- Deficiente comunicación entre usuarios y personal del P.E.D. (Proceso Electrónico de Datos); desconocimiento del papel / responsabilidad de usuarios y dirección.
- Escasez de personal profesional.
- Expectativas no cumplidas, insatisfechas de los usuarios.
- Ausencia de pistas de auditoría.
- Falta de revisiones técnicas a detalle.
- Entrenamiento deficiente.
- Carencia o incompleta documentación de sistemas (documentación técnica), de operación y/o de usuario.
- Carencia de metodología, o bien de metodología incompleta y no estándar, para el desarrollo de los sistemas, en la que se señalen con precisión actividades, tiempo estimado y responsable
- Administración insuficiente de los proyectos.
- Inoportunidad en la transferencia de sistemas en desarrollo a operación normal.
- Desaprovechamiento tecnológico.
- Pruebas del sistema incompletas, inadecuadas, desorganizadas, sin documentar y/o mal diseñadas, las cuales garanticen que los errores e irregularidades se detectan oportunamente por sistema. Pruebas no siempre controladas por usuario.

Cabe destacar que es sumamente importante que el auditor esté involucrado desde el plan maestro del sistema.
Fundamentalmente al auditor del ciclo de vida de desarrollo de sistemas le interesa:

- Que exista una metodología.
- Que la metodología sea la adecuada al entorno tecnológico de la entidad, sea estándar, completa, al día, aprobada, y comunicada a todo el personal.
- Que la metodología se cumpla en el caso de un sistema de información, en particular o en general.

El auditor no siempre ha participado en el ciclo de vida de desarrollo de los sistemas pues teme "ser juez y parte", pero es conveniente que el auditor esté consciente de que él no representa un factor para la toma de decisiones, sino más bien juega un papel de control que contribuye a disminuir riesgos, no a evitarlos. En otras ocasiones la falta de su participación se debe a la escasez de tiempo o personal en cuanto a prioridades.

La mayoría de las organizaciones destinan enormes recursos al desarrollo de nuevos sistemas o a la modificación de los mismos. A la luz del incremento en el porcentaje de fallas en las fechas de terminación, costos estimados y la satisfacción del usuario, las organizaciones deben seguir un enfoque estructurado para el desarrollo de nuevos sistemas y el mantenimiento de los mismos. La combinación de técnicas efectivas de administración del proyecto, la participación activa del usuario y especialistas, y la utilización de una metodología estructurada para el desarrollo de sistemas puede minimizar los riesgos en cuanto a aplicaciones inapropiadas, erróneas, con datos sin uso o bien a las que se efectúan cambios injustificados: "el gran salto hacia delante se logra con pequeños saltos".

Los sistemas de información se deben desarrollar para servir al usuario, proporcionándole capacidades para el proceso de datos y reportes.

Cada sistema de información tiene cuatro principales áreas o fases sujetas a control durante el proceso del ciclo de vida del desarrollo de sistemas:

- Planeación
- Análisis y Diseño
- Desarrollo
- Implantación

El reconocer que hay un ciclo de vida para el desarrollo de sistemas es el primer paso para su control el hecho de dividir el desarrollo en fases permite predecir el proyecto integro, analizar y evaluar cada parte con mayor concentración y monitorear continuamente la calidad y avance del trabajo. Cada área de control se divide en fases que involucran diversas actividades, responsabilidades y productos finales. Los proyectos de desarrollo se estructuran como acumulativos, cada actividad o etapa descansa en la precedente. Las actividades del proyecto deben ser evaluadas conforme se realizan y tomar la decisión de continuar con la asignación de recursos y con el programa de trabajo o detenerse a tiempo.

La revisión del ciclo de vida del desarrollo de sistemas parte de los estándares o metodología requerida para el desarrollo de los nuevos sistemas y las modificaciones a los mismos. El propósito de la revisión efectuada por el auditor de sistemas de información es asegurar que la organización tiene y usa la metodología adecuada de desarrollo.

Adicionalmente el auditor de sistemas de información está interesado en asegurar que el proceso de desarrollo se adhiera a los estándares establecidos por la metodología. Su participación puede ser durante el desarrollo del sistema o una vez ya concluido.

OBJETIVOS DE AUDITORÍA

La meta es verificar que se desarrollen sistemas útiles, seguros, auditables, mantenibles y controlables, lo cual produzca resultados consistentes para satisfacer los requerimientos del usuario.

FASES DEL CICLO DE VIDA DEL DESARROLLO DE SISTEMAS

PLANEACIÓN

1. Requisición de servicios
2. Estudio de factibilidad

DISEÑO

3. Diseño general del sistema
4. Diseño detallado del sistema

DESARROLLO

5. Programación
6. Prueba modular y prueba del sistema integral
7. Desarrollo de manuales
8. Entrenamiento

IMPLANTACIÓN

9. Conversión
10. Revisión de la post-implantación

PLANEACIÓN

1. REQUISICIÓN DE SERVICIOS

- Justificación.
- Ambiente.
- Alcance.
- Restricciones.
- Beneficios.
- Integración del equipo de trabajo y sus responsabilidades.
- Definición de requisitos de información, nuevos y existentes.
- Aprobación del proyecto.

2. ESTUDIO DE FACTIBILIDAD

- Estudio de los procedimientos existentes.
- Formulación de cursos alternativos de acción.
- Factibilidad tecnológica (métodos aplicables de P.E.D.), disponibilidad de la tecnología que satisfaga las necesidades del usuario, actualización o complemento a los recursos actuales.
- Factibilidad económica
- Costos actuales contra costos de cada alternativa (personal de desarrollo, equipo software, entrenamiento, preparación de la entrada, conversión de archivos de prueba, operación, costo del software, etc.).
- Identificación y cuantificación de beneficios.
- Factibilidad operativa. Determinar qué se operará, utilizará; tomando en cuenta factores como la resistencia al cambio, características del personal, ubicación de las instalaciones, etc.
- Plan maestro del proyecto (puntos de control y calendarización de actividades).
- Estado general de la función de desarrollo.
- Aprobación del proyecto.

3. DISEÑO GENERAL DEL SISTEMA

- Estructura general del sistema.
- Definición y documentación de los requisitos de salida del sistema.
- Contenido y formato de los informes.
- Frecuencia de producción de reportes.
- Lista de distribución de reportes.
- Periodos de retención de informes.
- Controles sobre la salida.
- Definición y documentación de los requisitos de entrada.
- Requisitos de edición y validación (control).
- Revisiones de seguridad para la protección de la exclusividad.
- Controles sobre la entrada.
- Definición y documentación de los requisitos de archivos
- Definición de los tipos de registros o estructuración de bases de datos.
- Métodos de organización.
- Niveles de seguridad y controles de acceso.
- Periodos de respaldo y retención.
- Definición y documentación de los requisitos de procesamiento (manual y computarizado).
- Especificación de procedimientos programados de cálculo, clasificación, etc.
- Estimación de tiempos de respuesta.
- Normatividad.
- Interfases.
- Niveles de seguridad.
- Diseño de documentos fuente.

En esta parte se determinan las especificaciones del usuario, es decir todo aquél que dentro del contexto de la organización se relaciona con el sistema. Existen usuarios primarios y usuarios secundarios.

Usuario primario: Es aquél que usa directamente en sus tareas los resultados del sistema de información.

Usuario secundario: Es aquél que introduce datos al sistema.
El analista de sistemas debe comprender las responsabilidades, limitaciones, necesidades del usuario, las acciones que deberá tomar el usuario, las reglas de decisión a aplicarse y los itinerarios de interacciones. Las especificaciones del usuario involucran el diagnóstico de la problemática y las especificaciones de solución. Estas tienen la fuerza de un contrato o compromiso entre el usuario y el personal de P.E.D.: tiempo de desarrollo, nivel de desempeño. Las especificaciones de usuario son los antecedentes para todo el equipo de desarrollo. Deben responder a las preguntas, ¿Cómo?, ¿Por qué?, por tanto se deberán quedar diagramados los procedimientos actuales y los esperados.

Las decisiones que tienen que tomar los usuarios de un sistema de información se pueden dar a 3 niveles:

1) Nivel de Administración Estratégica:
Guían al nivel medio y operativo de administración, actúan en un clima de incertidumbre. Postulan metas, estrategias y políticas.
2) Nivel Medio de Administración:
Toman decisiones sobre planeación y control a corto plazo, trabajan en un ambiente de baja certidumbre y las decisiones carecen de alto grado de estructuración.
3) Nivel Operativo de Administración:
Apoyan sus decisiones en reglas pre-establecidas, operan en nivel de alta certidumbre y fundamentalmente, consiste en la supervisión de detalles operativos.

NIVEL DE DIRECCION ESTRATÉGICA	CARACTERÍSTICAS	NIVEL DE CONTROL OPERATIVO
AMPLIA	VISION DE LA INFORMACIÓN	ESTRECHA
GENERAL	NIVEL DE DETALLE	MUY DETALLADA
RESUMIDO	NIVEL DE RESUMEN	DATOS PRIMARIOS
ANTIGUA	ANTIGÜEDAD DE LA INFORMACIÓN	MUY ANTIGUA
ESTIMACIONES	PRECISIÓN DE LA INFORMACIÓN	PRECISIÓN
CUALITATIVA	TIPO DE INFORMACIÓN	CUANTITATIVA
PRINCIPALMENTE		PRINCIPALMETE
EXTERNA		FUENTE INTERNA

Otro factor importante a considerar son las relaciones humanas, ya que los sistemas de información pueden cambiar las relaciones interpersonales y las interacciones.

Se debe comprender el estilo organizacional, tomar la organización como un todo, identificar el grado de apertura / restricción:
Permeabilidad. Es necesario identificar si el estilo de liderazgo es autócrata o demócrata.

La recopilación de datos involucra la investigación documental, la realización de entrevistas y la observación., ¿Qué se examinará?, ¿A quiénes se entrevistará?

Principales objetivos de los formatos / pantallas de captura:

- Precisión.
- Facilidad de uso y sencillez.
- Consistencia.
- Controlables (flujo).

Principales objetivos de las salidas:

- Satisfacción del objetivo planteado.
- Adaptada al usuario.
- Adecuada cantidad de información.
- Oportunidad.
- Medio apropiado.
- Medición del grado de confidencialidad.

“Es mucho menos costoso corregir problemas cuando éstos se encuentran en sus etapas iniciales, que esperar a que se expresen mediante quejas de usuarios o aparición de crisis”.

4. DISEÑO DETALLADO DEL SISTEMA

- Diseño de documentos fuente.
- Especificaciones de programas y controles programados (costo-beneficio).
- Diseño de pistas de auditoría.
- Estándares de documentación de programas.
- Nombre de la aplicación.
- Diagrama del sistema (menú jerárquico).
- Aspectos generales del programa.
- Formatos de archivos de entrada.
- Formatos de archivos de salida.
- Diseño y muestra de reportes.
- Diseño y muestra de pantallas.
- Descripción detallada de los principales procedimientos de cálculo, clasificación, etc., incorporados al programa.
- Criterios de selección.
- Procedimientos de conexión de cifras.
- Instrucciones de corrida y listado de procedimientos de ejecución.
- Medio de almacenamiento y localización del programa.
- Requerimientos de equipo.
- Listado del programa fuente (última compilación, con comentarios a la lógica).
- Estándares para la prueba de programas y del sistema total.
- Procedimiento para establecer datos de prueba.
- Asignación de responsabilidades para la preparación de datos y evaluación de los resultados.
- Autorización y aceptación escrita.

En esta etapa se definen las especificaciones técnicas, es decir las características y definiciones técnicas y operativas del sistema, lo cual es responsabilidad del líder de proyecto en informática. Las especificaciones técnicas incluyen:

- Instrucciones para programación.
- Itinerario para el desarrollo de programas / módulos.
- Matrices de archivos / programas, módulos / programas.
- Selección de los lenguajes de programación.
- Controles del operador.
- Instrucciones al operador en caso de interrupciones.
- Procedimientos de respaldo, reinicio y recuperación.

DESARROLLO

5. PROGRAMACIÓN

- Desarrollo y elaboración de la documentación de programas.

6. PRUEBA MODULAR Y PRUEBA DEL SISTEMA INTEGRALMENTE

Se deben ejercer presiones para hacer fallar el sistema. Las pruebas deben efectuarse con volúmenes de datos y bajo condiciones reales de operación. Cualquier error detectado debe ser cuidadosamente analizado y corregido, preparándose un reporte de excepciones: problema, causa y solución, indicando la fecha de corrección. La prueba debe estar bien dirigida, organizada, ser exhaustiva y eficiente, involucrando:

- Los procedimientos manuales, incluyendo al área de mesa de control.
- Los programas de cómputo y procedimientos de ejecución.
- Archivos de prueba.
- Al personal.

Es importante que se documenten las pruebas y se muestre en ellas la aprobación del usuario.

Plan de instalación.

En el caso de proyectos grandes conviene desarrollar un plan de instalación piloto o por módulos, asignando responsabilidades.

7. DESARROLLO DE MANUALES

De Operación:

- Representación gráfica de la estructura del sistema.
- Función de cada programa.
- Requerimientos de equipo.
- Tamaño estimado de archivos (normal y máximo).
- Explicación de los mensajes de la consola, junto con la respuesta adecuada del operador.
- Instrucciones de corrida y listado de procedimientos de ejecución.
- Calendarización de procesos.
- Parámetros a alimentar.
- Creación de salida y su distribución.
- Identificación adecuada de las etiquetas de los archivos de salida.
- Puntos de reinicio y recuperación.
- Procedimientos para notificar errores o condiciones defectuosas.
- Procedimientos para casos de emergencia.

De Usuario:

- Representación gráfica de la estructura del sistema.
- Procedimientos de preparación de datos.
- Asignación de prioridades.
- Tiempo probable de respuesta y recepción de productos finales.
- Especificaciones de diseño de entrada de datos (formatos y pantallas de captura).
- Especificaciones de diseño de salida de datos (reportes / pantallas de consulta).
- Controles de usuario.
- Procedimientos para resolver errores e incongruencias.
- Controles sobre la entrada y salida.

Del Sistema:

- Representación gráfica de la estructura del sistema.
- Documentación de cada programa de cómputo.

La revisión de la documentación de una aplicación involucra identificar su existencia, analizar su contenido y juzgar su oportunidad y disponibilidad. La calidad del mantenimiento de sistemas depende en gran medida de la calidad de la documentación. Además de la claridad y organización de la documentación, debe dedicarse especial atención al tipo al tipo de personas a quien va dirigido.

8. ENTRENAMIENTO

- Métodos de la enseñanza.
- Mecanismos para evaluación del aprendizaje.

IMPLANTACIÓN

9. CONVERSIÓN

- Identificación de fuentes de información.
- Recopilación de información.
- Revisión de la exactitud de los documentos previos a la conversión.
- Evaluación de los resultados de la conversión.

La etapa de conversión significa abandonar el sistema actual, manual o computarizado, para emigrar a uno nuevo y, conciliar los resultados.
Los controles en la etapa de conversión persiguen el asegurar que los archivos iniciales proporcionan un punto de arranque adecuado, marcando: itinerarios, compromisos, condiciones de éxito.

Normalmente la conversión requiere del desarrollo de programas de conversión de archivos de un formato a otro.

10. REVISIÓN DE LA POST-IMPLANTACIÓN

La revisión post-implantación es una revisión formalmente planeada, que debe realizarse después de transcurridos 3 o 6 meses de la instalación definitiva. La revisión post-implantación normalmente involucra:

- Evaluación del cumplimiento de las necesidades de usuario.
- Análisis de costo-beneficio.
- Efectividad de los controles.
- Control de modificaciones al sistema.

Mantenimiento del Sistema

Debido a que lo único constante en sistemas es el cambio, en esta etapa se analiza y evalúa como ha sido el mantenimiento de sistemas para proteger a la instalación de cambios incorrectos, no autorizados o decisiones equivocadas.
"El primer cambio surge el día que se instala el sistema".

El mantenimiento de sistemas se origina por los siguientes factores:

- Cambios en normatividad interna y externa a la entidad.
- Desarrollo tecnológico.
- Comportamiento del entorno, competencia.
- Costos excesivos.

Normalmente los cambios obligatorios se efectúan con menos controles, por la presión implícita, mientras que los cambios por mejoras (refinamiento, creatividad, ventajas tecnológicas) se atienden más controladamente.

Al auditor le preocupa que haya un sistema para administrar los cambios, por ejemplo hacer los cambios por grupos o lotes pertenecientes a un mismo módulo/programa. La documentación de los cambios debiera mostrar:

- Control numérico.
- Fecha de implantación.
- Persona solicitante.
- Persona que efectuó el cambio.
- Justificación.
- Descripción narrativa.
- Documentación de las pruebas.
- Autorización formal.

Todo cambio debiera originar la actualización de la documentación correspondiente.

La conciencia de la calidad, seguridad y control, debe iniciarse en las áreas de desarrollo, contemplando un balance adecuado con la productividad de los sistemas.

Área de Control | Planeación de Sistemas.

Los objetivos de control del proceso de planeación de sistemas son el asegurar que:

1- Los proyectos de desarrollo de sistemas de información son planeados con la suficiente anticipación.
2- Las necesidades y objetivos son definidas adecuadamente.
3- Se evalúan adecuada y suficientemente las desventajas, los aspectos económicos, técnicos, humanos, políticos y de operación.
4- Los sistemas son planeados de acuerdo a estándares.

“Si no se puede planear tampoco se podrá hacer”.

Área de Control | Diseño de Sistemas.

Los objetivos de control del proceso de desarrollo de sistemas son asegurar que:

1- Los programas son construidos de acuerdo con las especificaciones aprobadas por el usuario en la etapa de diseño del sistema.

2- Los programas son desarrollados en base a especificaciones detalladas por programa.

3- Los sistemas son verdaderamente probados / documentados.

4- Los usuarios son adecuadamente entrenados.

5- El sistema está de acuerdo a estándares.

La participación del autor de sistemas de información en el proceso de desarrollo se basa en la siguiente afirmación:

"La detección y corrección de controles inadecuados o incompletos durante la fase de diseño ahorrará tiempo y dinero cuando el sistema está operando".

V. AUDITORÍA DEL EQUIPO DE CÓMPUTO.

Una de las áreas de auditoria mas conflictivas y sensibles en una Institución es la función de adquisiciones que, tratándose de recursos informáticos se vuelve por demás interesente y muy sensible, debido a que se tiene que establecer los procedimientos de adquisición de los bienes informáticos, que van desde una compra simple, hasta una licitación en forma, ya sea por adjudicación directa, por invitación restringida, por licitación nacional o internacional, si se requiere.

Entre los aspectos importantes que tenemos que observar al realizar la auditoria se encuentran:

- Economía y factibilidad del posible proyecto de inversión, para la solución de los requerimientos planteados por la entidad evaluando su efectividad de acuerdo a las metas y objetivos previamente planeados.
- Se debe tener bien establecida la responsabilidad de los proveedores

Equipo / software

A partir del análisis y definición de requerimientos se deberán explorar las diferentes alternativas de solución, realizando un estudio de factibilidad que comprendan los siguientes elementos.

- Factibilidad económica. (estudio de costo-beneficio) involucrando los costos asociados a la adquisición, considerando no solo el desembolso inicial sino los costos por entrenamiento al personal y mantenimiento de los equipos.
- Factibilidad operativa, orientado a evaluar si el equipo tendrá la capacidad de procesar la información con posibilidades de crecimiento probadas.

- Factibilidad tecnológica, por las restricciones que esto pudiera tener para aprovechar íntegramente la inversión que esta realizando. Existen muchos casos en que se obliga a la institución a adquirir otro tipo de dispositivos para poder hacer operativo el equipo inicialmente contratado.

Es importante tomar en cuenta la facilidad que tiene el proveedor para dar mantenimiento en el propio lugar en que se encuentra instalado el equipo o los programas. Ya que esto puede entorpecer la operación en caso de que el proveedor no ofrezca esta posibilidad. Esta condición es aun más importante cuando nos referimos a software especializado.

En base a lo anterior se iniciara el siguiente paso del proceso que es el envió de solicitudes de propuestas a diferentes proveedores.

En la práctica se solicita la cotización, abriéndose esta en una fecha determinada ante la presencia de todos los concursantes a fin de que no existan favoritismos en la asignación del periodo y este se canalice hacia la mejor alternativa para la institución.

Estas solicitudes de propuestas deberán incluir todas las especificaciones técnicas y operativas que deberán cumplir para estar en posibilidades de concursar.

Con estas propuestas se realizara la evaluación de los equipos y programas y se realizaran las pruebas de aceptación previas.

Se sugiere que los resultados de las pruebas se alimenten a un sistema que asignara calificaciones y en forma automática, señalara el ganador del concurso.

Es necesaria una revisión minuciosa del contrato con el proveedor. Es recomendable solicitar la opinión del departamento legal de la institución o en su ausencia de un especialista externo, que valide la formulación del mismo.

En el caso de adquisición de software es importante definir el nivel de modificaciones (customización) que requiere para hacerlo operativo en la realidad. Aceptando que los paquetes responden a necesidades generales pero que requerirán de este proceso de adecuación razonable para hacerlos operativos.

Estos trabajos deberán declararse en forma detallada dentro de los contratos respectivos.

Al término de esta actividad se autoriza la compra mediante la aprobación de la gerencia y se iniciara un sistema de seguimiento del proyecto de tal manera que este se cumpla dentro de las estimaciones de costo y tiempo definidas.

Otro aspecto importante a señalar es la capacitación requerida y ofrecida por el proveedor, tanto en hardware como en software, que también tendrá que formar parte de la propuesta inicial para tener un panorama real de la inversión necesaria.

Es necesario tener claramente especificado de que activos se trata, de que manera y cuales serán los requisitos de autorización necesarios, los cuales pasaran a formar parte de la evaluación del auditor.

Para finalizar, es necesario realizar un seguimiento de los resultados que se obtengan al utilizar las nuevas adquisiciones a fin de comparar las expectativas contra los resultados reales y estar en posibilidades de realizar los ajustes necesarios.

Objetivos de la revisión

- Que los recursos y el capital sean efectivas y eficientemente aplicados.
- Que se cumpla con las políticas y procedimientos establecidos por la institución.

Aspectos de las adquisiciones.

- Determinación del presupuesto
- Consideraciones financieras
- Requisitos de la aplicación / prioridades
- Selección de posibles proveedores
- Petición formal de propuestas
- Demostraciones
- Referencias/ pruebas
- Características de las licencias de uso de software
- Comparación de propuestas evaluación de riesgos
- Planificación del local (instalaciones)
- Plan de instalación
- Planificación de la conversión
- Plan de implantación

Tema 2. Sistema operativo

Implantación

Típicamente el sistema operativo lo proporciona el fabricante del computador, pero el trabajo de implantación abarca el seleccionar las opciones apropiadas del sistema operativo y "generar un sistema" que cumpla con los requerimientos específicos de la institución, tomando en cuenta factores como:

- Configuraciones de equipos de computo (capacidades de memoria, periféricos en uso etc.)
- Modo de procesamiento (batch o en línea)
- Otras facilidades que se requieren (comunicaciones)

Este trabajo puede ejecutarse por el proveedor, por cuenta de la entidad o por la entidad misma. En cualquiera de los casos deberán verse involucrado, como responsable. Un funcionario de procesamiento

electrónico de datos que ayude a determinar que las opciones se han de seleccionar, probar documentar e implantar apropiadamente.

El sistema operativo que resulte deberá probarse acuciosamente bajo la supervisión del funcionario responsable, para determinar que se ejecuta de conformidad con los requerimientos de la entidad y que se han implantado apropiadamente todas las rutinas, facilidades y capacidades autorizadas.

Mantenimiento de sistemas operativos

Deben establecerse formalmente los procedimientos para dar mantenimiento de los sistemas operativos, al igual que en las aplicaciones. Un procedimiento conveniente pudiera incluir el que se prepare, revise y autorice adecuadamente una forma estándar de requisición de cambio antes de que se haga la modificación.

Una vez efectuado el cambio deberán estar en vigor procedimiento de revisión. A este efecto de asegurar que la documentación se actualiza de acuerdo a las normas de la entidad.

Después de que los programas modificados se han catalogado, un funcionario de procesamiento electrónico de datos (personal calificado en soporte técnico) deberá cerciorarse de que se han seguido los procedimientos apropiados para garantizar que se han considerado los aspectos mas importantes como son la ejecución del sistema operativo y los cambios que afectan a los usuarios, así mismo se deberán obtener las aprobaciones requeridas y cerciorarse de que el personal implicado ha sido notificado por escrito respecto a la fecha en que entrara en vigor la versión modificada del sistema operativo.

Algunos de los aspectos a incluir en la revisión del sistema operativo son:

- Documentación
  - Tablas de configuración del sistema operativo, guías, procedimientos, etc.

- Procedimientos
  - Carga inicial del sistema
  - Aplicación de actualizaciones o modificaciones.
  - Retención del registro de la actividad en consola y contabilidad del trabajo (job accounting)
  - Restricciones para el uso de comandos críticos

- Ejecución del sistema (software para monitoreo)
  - Tiempo de respuesta en línea
  - Costos/gastos excesivos.
  - Sistema operativo.

Tema 3 auditoria a la seguridad física

Seguridad física

La información y los recursos informáticos son activos que deben ser protegidos del acceso no autorizado. La manipulación y la destrucción. La seguridad física debe establecerse para prevenir accesos innecesarios y/o no autorizados y registrar los hechos.

La auditoria a la seguridad física se re refiere a la revisión de las medidas de control orientadas a la continuidad del servicios y dependen en gran parte de;

- Los fenómenos naturales: incendio, terremoto, huracanes, tormentas, severas, inundación, fallas de corriente, picos de voltaje, falla de aire acondicionado y cortos circuitos.

- Actos intencionales de ex-empleados, empleados notificados de despido, huelga, empleados adictos al alcohol o drogas, ladrones profesionales, empleados con problemas económicos o descontentos

Por lo anterior la entidad corre el peligro de:

- Entrada no autorizada
- Daño de equipo
- Vandalismo
- Robo de equipo y documentos
- Copias, consulta y/o divulgación de información confidencial
- Alteración de equipos sensible.
- Cambio no autorización de datos

La seguridad física debe proteger principalmente las áreas de

- Sala de computo
- Consola del operador
- Impresoras
- Equipo de teleproceso
- Fuentes de poder
- Lugar donde se guardan las cintas o discos magnéticos
- Bóvedas de respaldos
- Oficina de control de entradas y salidas
- Closet de comunicaciones
- Microcomputadoras y terminales remotas
- Área de programación

La revisión principalmente abarca la verificación de controles sobre:

- Ubicación del equipo
- Facilidad de acceso. Las áreas extremadamente visibles son muy vulnerables.
- Alimentación de energía eléctrica

- Líneas telefónicas privadas de respaldo, sobre todo en el caso de teleproceso
- Índice de delincuencia.
- Empresas vecinas altamente contaminantes
- Índice de fenómenos naturales: sismos, tormentas, etc.

- Material de construcción y mobiliario
  - materiales de construcción. Las paredes, techos y pisos deben estar construidas de material difícil de romper, resistente al fuego y no combustibles y que además no genere partículas de polvo, ya que pueden dañar los recursos informáticos
  - evitar las alfombras ya que causan electricidad estática, sobre todo cuando la humedad es baja.
  - Se debe mantener al mismo el numero de puertas y ventanas
  - El centro de cómputo debe instalarse dentro de un edificio lejos de ventanas y paredes que den a la calle.
  - No deben existir grandes árboles u otras estructuras que pongan en peligro el área de computo
  - Bóvedas resistentes al calor y humedad
  - Barreras para cortar o aislar incendios.
  - Se deben vigilar la instalación de detectores y controles de acceso. Los detectores pueden ser de: humo, calor, agua, combustión, controles de temperatura, controles de humedad, sistemas de detección de intrusos.
  - El lugar debe acatarse a los códigos de seguridad
  - Debe evitarse el uso de ventiladores en las áreas en donde se encuentra ubicado el equipo, ya que es un elemento para propagar el polvo con el riesgo de dañar los equipos.
  - El mobiliario debe ser resistente al fuego y no se debe permitir fumar alrededor o cerca de dañar los equipos
  - El mobiliario debe ser resistente al fuego y no se debe permitir fumar alrededor o cerca de los equipos.

Control de acceso

- Control de puertas. El acceso solo debe permitirse a aquellas personas que opriman la secuencia correcta de botones, sistema de tarjetas, sistemas de gafetes, etc. Tratándose de sistemas digitales generalmente la secuencia es de 6 dígitos. Lo cual proporciona un millón de combinaciones diferentes.
- Guardias de seguridad.
- Cerraduras de combinación, electrónicas o biométricas.
- Cerraduras para terminales
- Circuito cerrado de televisión
- Alarmas
- Puertas blindadas bajo sistemas de doble puerta
- Registro de visitante y gafetes de identificación
- Uso de credenciales-gafetes con fotografías

Algunas consideraciones en la selección del sistema de control de acceso son:

- Margen de error. Determinar el porcentaje tolerable de error del sistema a seleccionar; es decir, hasta cuantas veces se aceptara que el sistema niegue el acceso a una persona autorizada o lo permita a una que no lo esta.
- Protección en caso de fallas en el suministro de energía eléctrica.
- Resistencia a la manipulación o sabotaje
- Mantenimiento del sistema en buen estado
- Flexibilidad para crecer en relación al crecimiento institucional.
- Sencillez en su operación desde su instalación hasta su puesta en marcha
- Cantidad y frecuencia de acceso de acuerdo al trafico de entradas y salidas

Prevención contra fuego y agua

- Existencia mínima de material combustible
- Existencia adecuada de trituradora de papel
- Evitar cables sueltos y contactos en mal estado
- Detectores y alarmas de fuego, humo y humedad
- Extinguidores de agua (áreas administrativas y almacenes) y gas (áreas de equipo) carga, peso, ubicación, cantidad y capacidad.
- Tuberías adecuadamente aisladas para evitar filtraciones.
- Apagadores automáticos de incendio en ductos de aire acondicionado.
- Fundas para los equipos

Extras

- Salidas de emergencias
- Planta de energía, reguladores de voltaje y sistema "no-break"
- Respaldos
- Contratos de mantenimiento preventivo y correctivo a todos los equipos e instalaciones del área de informática.

Tema 4 auditoria a la seguridad lógica

Nunca ha sido tan grande la demanda de la identificación de los usuarios en todos los niveles. En la actualidad, cada vez más existe la tendencia a que los usuarios compartan los recursos de cómputo, por lo tanto el auditor debe preocuparse por:

- Determinar el mecanismo de acceso autorizado es capaz de prevenir accesos no autorizados a los recursos.
- Dadas las capacidades del mecanismo del control de acceso a los sistemas de información, determinar si es suficiente.

Los controles de frontera o controles de acceso establecen la interfase entre el usuario de un sistema y en computador mismo. Su propósito primario es establecer la identificación y la autenticación del que pretende ser usuario del sistema, para lo cual se necesitar un mecanismo de control.

Es una realidad que cada vez más los recursos informáticos: equipo, programas y datos, son compartidos por un gran número de personas físicamente dispersas lo cual hace necesario implantar controles que garanticen que el acceso a ellos se realiza de acuerdo al nivel jerárquico y funciones del personal. Protegiendo a la instalación de:

- Destrucción accidental o intencional
- Mal uso
- Consulta no autorizada de datos

La seguridad lógica se lleva a cabo a través de programas de acceso a:

- Equipos
- Programas
- Comunicaciones
- Datos
- Facilidades

Las acciones sobre el acceso sobre los datos y programas deben restringirse en cuanto a:

- Creación
- Modificación
- Copiado
- Eliminación
- Consulta
- Ejecución

La identificación puede definirse como el proceso de distinguir en forma única a un usuario de los demás mientras que la autentificación consiste en determinar si el individuo es quien dice ser. Es autentico para efectos de la seguridad lógica, un usuario lo constituye cualquier persona que utiliza los recursos informáticos ya que pertenezca a la área de informática o no.

La identificación, autentificación y autorización de los accesos del personal se logran mediante el uso de:

- Información memorizada "passwords" o contraseñas. ¿que conoce el usuario?
- Objetos, tarjetas plásticas con bandas magnéticas, llaves, etc. ¿que posee el usuario?
- Características personales: voz, huella digital, retina del ojo, etc.

El medio mas común para el control de accesos es la información memorizada o palabras calves; "passwords" y debe reunir las siguientes características:

- No menores de cuatro caracteres
- Alfanuméricos para incrementar el numero de combinaciones
- No debe tener el nombre del usuario o cualquier dato personal asignados por el propio usuario
- Debe ser intransferible. Cada usuario es responsable del buen o mal uso.
- No debe permitirse usar palabras anteriormente utilizadas
- Fáciles de recordar, difíciles de recordar
- Numero limitado de intentos
- Internamente transformados en un código secreto "encriptados"
- No desplegables en pantalla
- Cambiados periódicamente y de manera automática por el sistema

El sistema de control de accesos mediante passwords debe establecer perfiles de usuarios que incluyan los siguientes datos.

- Nombre del usuario
- Identificador del usuario “USER ID”
- Área a que pertenece
- Privilegios dentro del sistema
- Vigencia de acceso al sistema

El archivo en donde reciben los passwords deber ser protegidos con su respectiva contraseña

Cobra una gran importancia el concienciar al personal para que no rebelen los passwords. Enfatizando lo que estos representan en la reducción de riesgo de transferencia, modificación, perdida o divulgación, accidental o intencional de información confidencial

Normalmente los sistemas computarizados para seguridad proporcionan una bitácora de las actividades efectuadas en el proceso electrónico de datos. Constituyendo pistas de auditoria que pueden analizarse periódicamente y tomar decisiones en esta bitácora deben quedar registrados todos los accesos ocurridos y los intentos de acceso no autorizados a fin de que se puedan tomar las medidas pertinentes cuando el numero de incidencias es relevante: en que Terminal ocurre, a que hora, cuantas veces, que persona la utiliza, etc.

Los datos que pueden ser útiles como pistas de auditoria son:

- Identificación del usuario
- Información dada para autentificación
- Recursos requeridos
- Acciones privilegiadas (derechos) requeridas
- Identificación del dispositivo (Terminal)
- hora de inicio y terminación del acceso
- numero de intentos de acceso
- recursos proporcionados o negados
- acciones privilegiadas (derechos) otorgadas o negadas

Controles mediante criptografía

La criptografía derivada de dos palabras griegas: “kriptos” (oculto o secreto) y “grafos” (escritura). Es un método de protección de información mediante un proceso en el cual datos entendibles o legibles son transformados en códigos secretos (criptogramas) para prevenir accesos no autorizados y mantener la privacidad de la información por o tanto la criptografía convierte los datos originales en mensajes que no tienen significados para los que no conocen el sistema para recobrar los datos iniciales.

El análisis criptográfico se refiere a las técnicas para recobrar legalmente datos crípticos incorporados en criptogramas. Los términos de encripcion y decripcion son sinónimos descifrados.

Existen básicamente tres métodos para transformación de informaron:

Sustitución: mediante este método se conserva la posición original de los caracteres del mensaje y esconde su identidad pues los remplaza por otros caracteres de acuerdo a una tabla de códigos equivalentes ya sean numéricos o alfabéticos.

Transposición o permutación. Consiste en cambiar el orden de los caracteres del mensaje original.

Hibrido. Este método combina las características de los métodos de sustitución y de transposición.

Con el objeto de estandarizar la forma de encriptar. Se diseño un algoritmo llamado “des” (data enryption standard) basado en la técnica de sustitución o transposición de datos; el cual fue adoptado por la “nbs” (national bureau of standards) de, los estados unidos de Norteamérica.

La seguridad no puede depender de un solo elemento como lo es un algoritmo de encripción. Pues la persona que quisiera acceder información confidencial protegida, lo único que tendría que hacer es enfocar sus esfuerzos a descubrir los detalles de dicho algoritmo. Es por esto que se requiere de un segundo elemento llamado “llave de encripcion”, que es un numero generado en forma aleatoria con el objeto de mantener su confidencialidad.

El concepto de encripcion por hardware se aplica cuando se utiliza un dispositivo eléctrico denominado encriptor para transportar datos que viajan a través de un medio de comunicación. Se dice que la encripcion es vía software, cuando se utilizan una serie de programas para transformar los datos independientemente de que estos se encuentren almacenados o viajando a través de cables, líneas telefónicas, etc.

Aspectos importantes para evitar cambios no autorizados a los programas y datos.

- Segregación de funciones
  - Diferentes personas
  - Diferentes bibliotecas y directorios en disco (para producción desarrollada)

- Adecuado sistema de medios de identificación por ejemplo palabras claves (passwords) definición de autorizaciones, frecuencia de cambios estructurales, etc.

- Supervisión.

Tema 5. Plan de contingencias.

Ha existido mucha dificultad para la plantación y prevención de desastres durante los últimos años. Un buen punto de inicio fue el reconocimiento del poder de las comunicaciones (teléfono, fax MODEM, etc.) y como afecto a los centros de computo el temblor de de septiembre de 1985 en México, DF. El impacto mayor no es en muchas veces el desastre mismo, sino las acciones que se tomen en el momento del desastre.

Recordando los desastres pueden ser naturales, humanos y materiales. Normalmente se piensa en los fenómenos naturales, pero no en lo de todos los días. Roedores, fugas de agua, etc. Y eso muchas veces es lo primero a controlar. Otro ejemplo es el que cualquiera puede llegar a las instalaciones, a recursos vitales como las comunicaciones.

- Se entiende como:

    - Desastre: accidente, tragedia, emergencia.

    - Recuperación: sanar, reponer, ganar de nuevo.

Se puede definir un plan de recuperación como la habilidad de una organización para continuar sus operaciones diarias, a pesar de que ocurra un desastre, por medio de una serie de acciones coordinadas y planeadas con el conocimiento y el apoyo gerencial. El gerente de informática debe ser el líder del plan. Pero debe involucrarse seriamente el director de finanzas.

Para que u plan de recuperación ante contingencias funcione deben ser del conocimiento y reconocimiento de todos los involucrados. Para obtener un mayor convencimiento se puede recurrir a fuentes externas. Es una póliza de seguro diferente.

En general los planes de contingencia pueden definirse como un elemento de control interno que es establecido para asegurar la disponibilidad de datos valiosos y los recursos del computador en el caso de un evento que ocasione la interrupción de operaciones.

Un buen plan de contingencia y recuperación detallada los procedimientos para emigrar a una situación de emergencia en el menor tiempo posible y con el menor grado de riesgo así como regresar a la operación normal de la misma forma.

La preparación de los planes de contingencia no es una tarea simple y realizable por un solo individuo. Es una actividad compleja y multifacético que requiere la involucración de toda una organización. Por lo que resulta necesaria la creación de un comité que administre todo lo relacionado con el plan de contingencias: recursos humanos y financieros aunque el desarrollo del plan requiere de la cooperación de todas las áreas de la institución, una persona debe tener la responsabilidad de coordinar, complementar y dar mantenimiento al plan. A esta persona se le conoce como líder del proyecto.

Una parte del proceso de planeación para los casos de contingencia es la determinación de los desastres potenciales de la organización. Diferenciándose un desastre de una falla operativa. La clave para la determinación efectiva de los planes de contingencia es el entendimiento de los requerimientos de procesamiento y sus prioridades.

A continuación se indican algunos puntos a considerar dentro de un plan de contingencia. :

- Tener un mejor entendimiento de la entidad. “lo importante no es ser informático sino pertenecer a una entidad en particular”.

- Ver las cosas no con una perspectiva simplemente tecnológica, sino de protección y seguridad. Muchos problemas se van generando paulatinamente y en un momento se convierten en desastre, diariamente pasan inadvertidos.

- Imposición de sanciones (penalizaciones y multas) por violaciones o infracciones a las reglas de seguridad por empleados irresponsables o descuidados. Por ejemplo, en el caso de cortes de cables.

- Realizar un inventario de todos los sistemas. Facilidades y recursos de cómputo incluye a las personas que están operando enfermedades que parecen limitaciones emocionales, Accesibilidad y responsabilidad, empleados valiosos, mobiliario, aire acondicionado, puertas, cerraduras, necesidades de usuarios y fijar prioridades.

- Analizar todos los conflictos legales y laborales considerados como potenciales en caso de desastre, con empleados accionistas, clientes, proveedores, etc.

- Cuidar la coordinación cuando se comparte el inmueble con otras instituciones. Fincando responsabilidad compartida, también es el caso de construcciones y remodelaciones vecinas.

- Auxiliarse de documentos modelos y preparar un plan preliminar, en términos de negocios.

- Incluir procedimientos detallados iniciales de avisos y acciones. Lo más importante es proteger la vida humana. Las telecomunicaciones en muchos casos son críticas en caso de desastres. El seguir las instrucciones ordenadamente puede evitar que un desastre se convierta en una catástrofe. Puede darse el caso de tener la necesidad de reemplazar trabajadores valiosos que renuncian como resultado de tener sentimientos de inseguridad o percibir un alto riesgo para sus vidas.

- Lista de personas que deben arrancar el plan contra desastres, que deben ser informadas de manera inmediata y de los coordinadores responsables de la centralización y diseminación de la información durante la emergencia.

- Clasificar los recursos informáticos de acuerdo a su importancia.

- Requerimientos de personal para recuperación.

- Procedimientos de seguridad que deberán tenerse en cuenta al trasladar los recursos informáticos.

- Direcciones y teléfonos de:

    - Centro alterno de proceso de datos.
    - Proveedores.
    - Clientes.
    - Doctores.
    - Policía.
    - Servicios de emergencia, bomberos, hospitales, etc.
    - Agencias de personal para nuevas contrataciones
    - Personal activo.

- Rutas de transportación primaria y alterna en el caso de que resulte necesario enviar empleados a su domicilio.
- Procedimiento en caso de amenaza de bombas
- Procedimientos para activar el equipo de soporte
- Mecanismo de notificación y control de actividades.
- Operaciones a procesar en el centro de apoyo o facilidades alternas.
- Prioridades de operación de sistemas.
- Planes de evacuación y planes alternos en caso de fuego, bomba o explosión.
- Procedimientos para solicitar asistencia de la policía y los bomberos.
- Procedimiento para recuperación, conmutación telefónica y restauración de los servicios del centro de procesos de datos.
- Reporte y evaluación de riesgos existentes.
- Copiad de contratos y seguros de mantenimiento y respaldos.
- Mecanismos de respaldo existentes. Guardando la versión “abuelo” de los archivos en medios magnéticos en un lugar seguro y fuera de la zona en que se ubique el centro de proceso de datos.
- Convenios con otras instalaciones para formalizar soporte de equipo en caso de catástrofes.

- Existencia del manual de contingencias en el lugar en que se encuentre la bóveda de respaldos.

- Los procedimientos deben funcionar siempre por lo que es importante efectuar una revisión periódica de ellos y actualizar los ejemplares que se tengan del manual por el comité de contingencias cada vez que ocurran cambios en:

    - Personal.
    - Equipo o instalación propia y/o soporte.
    - Teléfonos.
    - Usuarios.
    - Contratos de mantenimiento y respaldo.

VI. AUDITORÍA ADMINISTRATIVA PARA EL ÁREA DE CÓMPUTO.

ADMINISTRACIÓN DE LA FUNCIÓN INFORMÁTICA

REQUERIMIENTOS A SOLICITRA PARA LA REVISIÓN

P L A N E A C I Ó N

Dentro de esta etapa vamos a considerar la determinación de objetivos, políticas, procedimientos y programas, además de la elección de los cursos de acción para lograrlos con base en la investigación y elaboración de programas de trabajo que incluya. La creación y función del comité u órgano interno de cómputo que debe ser el encargado de administrar los bienes informáticos.

SOLICITAR

- Manuales de Organización donde se identificó:
    - Funciones, personal y equipo del área.
    - Objetivos del área.
    - Objetivos particulares de cada departamento.
    - Políticas del área.
    - Procedimientos del área.
    - Programas.

O R G A N I Z A C I Ó N

En esta etapa se deberá considerar el establecimiento de la estructura necesaria, para la optimización de los recursos a través de la determinación de jerarquías y agrupación de actividades con el fin de realizar y simplificar las funciones del área.

SOLICITAR

- Organigrama general y particular del área de cómputo.

I N T E G R A C I Ó N

Dentro de esta etapa se verifica la función a través de la cual el encargado de la administración de la función informática elige y se allega de los recursos humanos necesarios para cumplir con los objetivos previamente establecidos.

SOLICITAR

- Planes y programas de trabajo respecto a:

- Reclutamiento.
- Selección.
- Inducción.
- Capacitación.
- Desarrollo.

D I R E C C I Ó N

En esta etapa se consideró si existe supervisión y coordinación de las actividades desarrolladas por el personal del área de cómputo.

SOLICITAR

- Documentos que establezcan:
  - Frecuencia con que se realiza.
  - Quién es el responsable de realizarla.
  - Formas en que se realiza.

C O N T R O L

En esta etapa se verifica si se cumplió con los objetivos planeados, analizando los resultados obtenidos.

SOLICITAR

- Informe anual de actividades del jefe de la División de Informática.

- Ultimo informe de cada departamento con la finalidad de verificar su existencia y periodicidad de realización.

- Registros y bitácoras de actividades desarrolladas por todas y cada una de las personas del área.

Aplicación de los cuestionarios desarrollados en el proceso administrativo, auxiliados de las metodologías, ya se sea de William P. Leonard, O del análisis Factorial del Banco de México, o por desarrollado por José de Jesús Aguirre, que se explicarán en clase. Y que son aplicables a la estructura orgánica de la empresa, al personal, a costos, presupuestos y controles de asignación de trabajo.

VII. INTERPRETACIÓN DE LA INFORMACIÓN.

Se cuenta en la actualidad con numerosas herramientas para interpretar la información que recopilamos durante la auditoria previamente planeada, después viene la fase de la ejecución del trabajo en donde, para realizar un trabajo suficiente y competente nos auxiliamos de las técnica de auditoria emitida por el IMCP, y que podemos adaptar a nuestras revisiones en informática, no obstante podemos adherir las técnicas propias de la informática, a continuación mencionaremos las técnica emitidas por el IMCP.

Clasificación de las Técnicas de Auditoria

La comisión de normas y procedimientos de Auditoria del Instituto Mexicano de Contadores Públicos, en su boletín 5010-procedimientos de auditoría ha propuesto la siguiente clasificación:

- Estudio General
- Análisis.
- Inspección.
- Confirmación.
- Investigación.
- Declaraciones
- Certificación.
- Observaciones.
- Cálculo.

- **Estudio General**

Es la apreciación y juicio de las características generales de la empresa, las cuentas o las operaciones, a través de sus elementos mas significativos para concluir se ha de profundizar en su estudio y en la forma que ha de hacerse.

- **Análisis**

Es el estudio de los componentes de un todo para concluir con base en aquellos respecto de este. Esta técnica se aplica concretamente al estudio de las cuentas o rubros genéricos de los estados financieros.

- **Inspección**

Es la verificación física de las cosas materiales en las que se tradujeron las operaciones, se aplica a las cuentas cuyos saldos tienen una representación material, (efectivos, mercancías, bienes, etc.).

- **Confirmación**

Es la ratificación por parte de una persona ajena a la empresa, de la autenticidad de un saldo, hecho u operación, en la que participo y por la cual esta en condiciones de informar validamente sobre ella.

- **Investigación**

Es la recopilación de información mediante platicas con los funcionarios y empleados de la empresa.

- **Declaraciones y Certificaciones**

Es la formalización de la técnica anterior, cuando, por su importancia, resulta conveniente que las afirmaciones recibidas deban quedar escritas (declaraciones) y en algunas ocasiones certificadas por alguna autoridad (certificaciones).

Observación

Es una manera de inspección, menos formal, y se aplica generalmente a operaciones para verificar como se realiza en la practica.

Cálculo

Es la verificación de las correcciones aritméticas de aquellas cuentas u operaciones que se determinan fundamentalmente por cálculos sobre bases precisas.

Clasificación de los Procedimientos de Auditoria

Como ya se ha mencionado los procedimientos de auditoria son la agrupación de técnicas aplicables al estudio particular de una cuenta u operación; prácticamente resulta inconveniente clasificar los procedimientos ya que la experiencia y el criterio del auditor deciden las técnicas que integran el procedimiento en el caso particular.

Extensión o alcance de los Procedimientos

Se llama extensión o alcance a la amplitud que se da a los procedimientos, es decir, la intensidad y profundidad con que se aplican prácticamente.

Oportunidad de los Procedimientos

Es la época en que deben aplicarse los procedimientos al estudio de partidas específicas

Además de las técnicas antes mencionadas, nos ayudaremos de los cuestionarios de control interno, y cuestionarios de aplicación general y específica utilizando el modelo José de Jesús Aguirre, que hace referencia a la ponderación de cada etapa de la auditoria en informática y se le da un valor para medir, ya sea la productividad, costo-beneficio, y utilidad de la capacidad instalada, para poder emitir una opinión sobre la razonabilidad en el uso de recursos informáticos, que es finalmente el objetivo de la Auditoria en informática.

INFORME DE AUDITORIA

Elementos básicos del Informe de Auditoría

La materialización final del trabajo llevado a cabo por los auditores independientes se documenta en el dictamen, informe u opinión de auditoría. Además, para aquellas entidades sometidas a auditoría legal, este documento junto con las cuentas anuales del ejercicio forma una unidad,

El informe de auditoría independiente deberá contener, como mínimo, los siguientes elementos básicos:

- El título o identificación.
- A quién se dirige y quienes lo encargaron.
- El párrafo de "Alcance".
- El párrafo de "Opinión".
- El párrafo o párrafos de "Énfasis".
- El párrafo o párrafos de "Salvedades".
- El párrafo sobre el "Informe de Gestión".
- La firma del informe por el auditor.
- El nombre, dirección y datos registrables del auditor.
- La fecha del informe.
- El párrafo legal o comparativo

Objetivos, características y afirmaciones que contiene el informe de auditoría

El informe de auditoria en informática tiene como objetivo expresar una opinión técnica sobre el uso de los recursos informáticos, sobre si éstas muestran la imagen fiel del patrimonio informático, y su aplicación correcta dentro de la Institución que se audite.

Características del informe de auditoría

- Es un documento mercantil o público.
- Muestra el alcance del trabajo.
- Contiene la opinión del auditor.
- Se realiza conforme a un marco legal.

Principales afirmaciones que contiene el informe

- Indica el alcance del trabajo y si ha sido posible llevarlo a cabo y de acuerdo con qué normas de auditoría.
- Expresa si las cuentas anuales de gastos en los recursos informáticos y que contienen la información necesaria y suficiente y han sido formuladas de acuerdo con la legislación vigente y, también, si dichas cuentas han sido elaboradas teniendo en cuenta el principio de uniformidad.
- Se opina también sobre la concordancia de la información contable para verificar la veracidad de las cifras en el rubro de recursos informáticos.
- En su caso, explica las desviaciones que presentan los estados financieros con respecto a unos estándares preestablecidos y el plan anual de avance informático..
- Podemos sintetizar que el informe es una presentación pública, resumida y por escrito del trabajo realizado por los auditores y de su opinión sobre la situación de los recursos informáticos de una Institución.
-

Tipos de opinión

Existen cuatro tipos de opinión en auditoría:

- Opinión Favorable.
- Opinión con Salvedades.
- Opinión Desfavorable.
- Opinión Denegada.

La opinión favorable, limpia o sin salvedades significa que el auditor está de acuerdo, sin reservas, sobre la presentación y contenido de los procedimientos que se llevan a cabo par verificar la utilización adecuada en los recursos Informáticos.

La opinión con salvedades (llamada también en la jerga de la auditoría como opinión calificada o cualificada), significa que el auditor está de acuerdo con los procedimientos y utilización de los recursos informáticos, pero con ciertas reservas.

La opinión desfavorable u opinión adversa o negativa significa que el auditor está en desacuerdo con los procedimientos utilizados para el manejo de los recursos informáticos y afirma que éstos no se realizan conforme a estándares nacionales o determinados por la empresa.

Por último, la opinión denegada, o abstención de opinión significa que el auditor no expresa ningún dictamen sobre el manejo de los recursos informáticos. Esto no significa que esté en desacuerdo con ellos, significa simplemente que no tiene suficientes elementos de juicio para formarse ninguno de las tres anteriores tipos de opinión.

Observaciones

El auditor debe realizar procedimientos diseñados a obtener suficiente y apropiada evidencia de auditoria, en que puedan todos los elementos hasta la fecha del informe del auditor que puedan requerir de ajustes o exposiciones en las metodologías que, hayan sido identificados. Ciertos eventos y transacciones que ocurren después de cada fin de año, deben ser examinados como parte del trabajo normal de verificación de auditoria.

Además debe de llevar acabo una revisión completamente documentada, de eventos subsecuentes la cual tiene como objetivo de obtener una seguridad razonable, de que todos los eventos importantes han sido identificados y expuestos o registrados en las bitácoras de auditoría.

La revisión debe ser actualizada a una fecha lo más cercanamente posible a la fecha del informe de auditoria, hablando con la gerencia y realizando pruebas futuras de ser necesario.

Todos los procedimientos de auditoria emprendidos y las conclusiones alcanzadas deben estar completamente documentadas las hojas de trabajo deben incluir notas, detalladas de reuniones, incluyendo quien estaba presente, los asuntos discutidos y el resto de las discusiones.

El auditor no tiene ninguna obligación de hacer ninguna investigación relacionada con la información de los recursos informátcos, que estos hayan sido omitidos, pero antes de que la reunión general anual, el entera de información que pudo haber afectado el informe de auditoria si hubiera tenido conocimiento de ella en ese momento, nuevamente el debe discutir el asunto con los directores.

Los objetivos de los procedimientos de finalización de la auditoria para asegurar que:

- Si ha sido obtenida suficiente evidencia de auditoria para apoyar la opinión de auditoria.
- Todas las decisiones tomadas han sido documentadas.
- El archivo de auditoria ha sido complementado.
- Cualquier tema estratégico ha sido documentado y discutido con el cliente.

Las tareas claves en la terminación de la auditoria son:

- Terminación de cada área de auditoria del archivo.
- Escribir el informe al socio.
- Escribir cualquier revisión estratégica del negocio.
- Revisión de las hojas de trabajo.
- Conclusiones generales de auditoria.
- Realizar una reunión para asegurar que los secretos de la empresa no sean relevados.

Sugerencias

Los programas principales de auditoria deben mostrar claramente el objetivo de auditoria, el trabajo realizado y las conclusiones alcanzadas y ser sustentados por todos los papeles de trabajo de referencia cruzada.

Cada programa principal auditado debe ser comparado con las hojas de trabajo de auditoría relevantes y con las cifras de los recursos ejercidos en informática.

Correctivas

Conclusiones del área de Auditoria:

- Se debe obtener una conclusión para cada área de auditoria.
- Antes de obtener una conclusión, debe asegurarse que el programa de auditoria fue llevado a cabo como se planteo, o que los cambios acerca de las decisiones hechos en la etapa de la planificación están documentados.
- Las hojas de trabajo también se deben escudriñar para asegurar que todas las preguntas que surjan hayan sido claras y que todos los procedimientos y programas de auditoria planificados hayan sido completados. Se debe hacer un informe completo de todos los problemas no resueltos.
- Cualquier problema importante u otros asuntos no aclarados deben ser anotados por la gerencia o incluidos en el informe al socio. Cualquier asunto inusual, aun cuando estén aclarados, deben ser incluidos en el informe al socio en manera de información
- Cualquier debilidad u otros asuntos relacionados con el área de auditoria, que resulten apropiados reportar al cliente, deben ser resumidos e incluidos en la carta de gerencia.
- Cualquier área donde el auditor haya tenido que depender de representaciones, deben ser incluidas en la carta de representación.

Informe al socio

El informe al socio agrupan en un solo lugar, todos los asuntos que tiene un efecto en la opinión de auditoria, o que necesitan ser discutidos con al cliente.

Dependiendo de la estructura del equipo de auditoria debe ser hecho en borrador por el señor mientras la auditoria progresa y completado por el cliente.

El gerente debe evidenciar la terminación del informe al socio firmado la primera página y el socio debe refrendarlo. El gerente debe firmar una segunda vez cuando todos los puntos que surjan de la revisión del informe al socio deben entonces refrendarlo para evidenciar su satisfacción.

Aunado a todo lo anterior, el auditor en informática, debe tener en cuenta que su trabajo, es profesional y de una fuerte independencia mental ya que al realizar auditorias a información o procedimientos informáticos estos son la médula espinal de la empresa y con riesgos altos.

Y conlleva a que la fragilidad de los sistemas son de alto riesgo y que normalmente las instituciones no le dan importancia a este tipo de auditorias por que no son obligatorios, si no voluntarios y las empresas ven a la auditoria como un gasto y no como una inversión.

El auditor debe con su trabajo, motivar a que ese supuesto gasto se convierta en beneficios de la empresa y aumenta su nivel de confianza en la seguridad de sus recursos informáticos.