UNIDAD 8
AUDITORIA DE LOS SISTEMAS DE INFORMACIÓN

INTRODUCCION

La naturaleza especializada de la auditoria de los sistemas de información y las habilidades necesarias para llevar a cabo este tipo de auditorias, requieren el desarrollo y la promulgación de Normas Generales para la auditoria de los Sistemas de Información.

La auditoria de los sistemas de información se define como cualquier auditoria que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes.

Para hacer una adecuada planeación de la auditoria en informática, hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características de área dentro del organismo a auditar, sus sistemas, organización y equipo.

A continuación, la descripción de los dos principales objetivos de una auditoria de sistemas, que son, las evaluaciones de los procesos de datos y de los equipos de cómputo, con controles, tipos y seguridad.

¿QUE ES AUDITORIA DE SISTEMAS?

La auditoria en informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

La auditoria en informática deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La auditoria en informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo (informática, organización de centros de información, hardware y software).

PLANEACIÓN DE LA AUDITORÍA EN INFORMÁTICA

Para hacer una adecuada planeación de la auditoria en informática, hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características de área dentro del organismo a auditar, sus sistemas, organización y equipo.

En el caso de la auditoria en informática, la planeación es fundamental, pues habrá que hacerla desde el punto de vista de los dos objetivos:

1. Evaluación de los sistemas y procedimientos.
2. Evaluación de los equipos de cómputo.

Para hacer una planeación eficaz, lo primero que se requiere es obtener información general sobre la organización y sobre la función de informática a evaluar. Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas, con base en esto planear el programa de trabajo, el cual deberá incluir tiempo, costo, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la misma.

INVESTIGACIÓN PRELIMINAR

Se deberá observar el estado general del área, su situación dentro de la organización, si existe la información solicitada, si es o no necesaria y la fecha de su última actualización.

Se debe hacer la investigación preliminar solicitando y revisando la información de cada una de las áreas basándose en los siguientes puntos:

- **ADMINISTRACIÓN**

Se recopila la información para obtener una visión general del departamento por medio de observaciones, entrevistas preliminares y solicitud de documentos para poder definir el objetivo y alcances del departamento.

Para analizar y dimensionar la estructura por auditar se debe solicitar a nivel del área de informática

1. Objetivos a corto y largo plazo.
2. Recursos materiales y técnicos
3. Solicitar documentos sobre los equipos, número de ellos, localización y características.
4. Estudios de viabilidad.
5. Número de equipos, localización y las características (de los equipos instalados y por instalar y programados)
6. Fechas de instalación de los equipos y planes de instalación.
7. Contratos vigentes de compra, renta y servicio de mantenimiento.
8. Contratos de seguros.
9. Convenios que se tienen con otras instalaciones.
10. Configuración de los equipos y capacidades actuales y máximas.
11. Planes de expansión.
12. Ubicación general de los equipos.
13. Políticas de operación.
14. Políticas de uso de los equipos.

- **SISTEMAS**

Descripción general de los sistemas instalados y de los que estén por instalarse que contengan volúmenes de información.

1. Manual de formas.
2. Manual de procedimientos de los sistemas.
3. Descripción genérica.
4. Diagramas de entrada, archivos, salida.
5. Salidas.
6. Fecha de instalación de los sistemas.
7. Proyecto de instalación de nuevos sistemas.
8. En el momento de hacer la planeación de la auditoria o bien su realización, debemos evaluar que pueden presentarse las siguientes situaciones.
9. Se solicita la información y se ve que:

No tiene y se necesita.
No se tiene y no se necesita.
Se tiene la información pero:
- No se usa.
- Es incompleta.
- No esta actualizada.
- No es la adecuada.
- Se usa, está actualizada, es la adecuada y está completa.

En el caso de *No se tiene* y *no se necesita*, se debe evaluar la causa por la que no es necesaria. En el caso de No se tiene pero es necesaria, se debe recomendar que se elabore de acuerdo con las necesidades y con el uso que se le va a dar. En el caso de que se tenga la información pero no se utilice, se debe analizar por que no se usa. En caso de que se tenga la información, se debe analizar si se usa, si está actualizada, si es la adecuada y si está completa.

éxito del análisis crítico depende de las consideraciones siguientes:

1. Estudiar hechos y no opiniones (no se toman en cuenta los rumores ni la información sin fundamento)
2. Investigar las causas, no los efectos.
3. Atender razones, no excusas.
4. No confiar en la memoria, preguntar constantemente.
5. Criticar objetivamente y a fondo todos los informes y los datos recabados.

PERSONAL PARTICIPANTE

Una de las partes más importantes dentro de la planeación de la auditoria en informática es el personal que deberá participar y sus características.

Uno de los esquemas generalmente aceptados para tener un adecuado control es que el personal que intervengan esté debidamente capacitado, con alto sentido de moralidad, al cual se le exija la optimización de recursos (eficiencia) y se le retribuya o compense justamente por su trabajo.

Con estas bases se debe considerar las características de conocimientos, práctica profesional y capacitación que debe tener el personal que intervendrá en la auditoria. En primer lugar se debe pensar que hay personal asignado por la organización, con el suficiente nivel para poder coordinar el desarrollo de la auditoria, proporcionar toda la información que se solicite y programar las reuniones y entrevistas requeridas.

Éste es un punto muy importante ya que, de no tener el apoyo de la alta dirección, ni contar con un grupo multidisciplinario en el cual estén presentes una o varias personas del área a auditar, sería casi imposible obtener información en el momento y con las características deseadas.

También se debe contar con personas asignadas por los usuarios para que en el momento que se solicite información o bien se efectúe alguna entrevista de comprobación de hipótesis, nos proporcionen aquello que se esta solicitando, y complementen el grupo multidisciplinario, ya que se debe analizar no sólo el punto de vista de la dirección de informática, sino también el del usuario del sistema.

Para completar el grupo, como colaboradores directos en la realización de la auditoria se deben tener personas con las siguientes características:

1. Técnico en informática.
2. Experiencia en el área de informática.
3. Experiencia en operación y análisis de sistemas.

4. Conocimientos de los sistemas más importantes.

En caso de sistemas complejos se deberá contar con personal con conocimientos y experiencia en áreas específicas como base de datos, redes, etc. Lo anterior no significa que una sola persona tenga los conocimientos y experiencias señaladas, pero si deben intervenir una o varias personas con las características apuntadas.

Una vez que se ha hecho la planeación, se puede utilizar el formato señalado en el anexo 1, el figura el organismo, las fases y subfases que comprenden la descripción de la actividad, el número de personas participantes, las fechas estimadas de inicio y terminación, el número de días hábiles y el número de días/hombre estimado. El control del avance de la auditoria lo podemos llevar mediante el anexo 2, el cual nos permite cumplir con los procedimientos de control y asegurarnos que el trabajo se está llevando a cabo de acuerdo con el programa de auditoria, con los recursos estimados y en el tiempo señalado en la planeación.

El hecho de contar con la información del avance nos permite revisar el trabajo elaborado por cualquiera de los asistentes.

PASOS A SEGUIR

Se requieren varios pasos para realizar una auditoria. El auditor de sistemas debe evaluar los riesgos globales y luego desarrollar un programa de auditoria que consta de objetivos de control y procedimientos de auditoria que deben satisfacer esos objetivos. El proceso de auditoria exige que el auditor de sistemas reúna evidencia, evalúe fortalezas y debilidades de los controles existentes basado en la evidencia recopilada, y que prepare un informe de auditoria que presente esos temas en forma objetiva a la gerencia. Asimismo, la gerencia de auditoria debe garantizar una disponibilidad y asignación adecuada de recursos para realizar el trabajo de auditoria además de las revisiones de seguimiento sobre las acciones correctivas emprendidas por la gerencia.

INFORME

En si todos los encuestados respondieron la totalidad de las preguntas. Todos tienen la misma respuesta en la pregunta sobre la inteligencia artificial, todos dicen prácticamente lo mismo acerca de lo que es la auditoria de sistemas en que es un sistema de revisión, evaluación, verificación y evalúa la eficiencia y eficacia con que se está operando los sistemas y corregir los errores de dicho sistema. Todos los encuestados mostraron una características muy similares de las personas que van a realizan la auditoria; debe haber un contador, un ingeniero de sistemas, un técnico y que debe tener conocimientos, práctica profesional y capacitación para poder realizar la auditoria.

Todos los encuestados conocen los mismos tipos de auditoria, Económica, Sistemas, Fiscal, Administrativa.

Para los encuestados el principal objetivo de la auditoria de sistemas es Asegurar una mayor integridad, confidencialidad y confiabilidad de la información mediante la recomendación de seguridades y controles.

Mirando en general a todos los encuestados se puede ver que para ellos la auditoria de sistemas es muy importante porque en los sistemas esta toda la información de la empresa y del buen funcionamiento de esta depende gran parte del funcionamiento de una empresa y que no solo se debe comprender los equipos de computo sino también todos los sistemas de información desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La auditoria de los sistemas de informática es de mucha importancia ya que para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad.

Auditoria Interna y Auditoria Externa:

La auditoría interna es la realizada con recursos materiales y personas que pertenecen a la empresa auditada. Los empleados que realizan esta tarea son remunerados económicamente. La auditoría interna existe por expresa decisión de la Empresa, o sea, que puede optar por su disolución en cualquier momento.

Por otro lado, la auditoría externa es realizada por personas afines a la empresa auditada; es siempre remunerada. Se presupone una mayor objetividad que en la Auditoría Interna, debido al mayor distanciamiento entre auditores y auditados.

La auditoría informática interna cuenta con algunas ventajas adicionales muy importantes respecto de la auditoría externa, las cuales no son tan perceptibles como en las auditorias convencionales. La auditoría interna tiene la ventaja de que puede actuar periódicamente realizando Revisiones globales, como parte de su Plan Anual y de su actividad normal. Los auditados conocen estos planes y se habitúan a las Auditorias, especialmente cuando las consecuencias de las Recomendaciones habidas benefician su trabajo.

En una empresa, los responsables de Informática escuchan, orientan e informan sobre las posibilidades técnicas y los costes de tal Sistema. Con voz, pero a menudo sin voto, Informática trata de satisfacer lo más adecuadamente posible aquellas necesidades. La empresa necesita controlar su Informática y ésta necesita que su propia gestión esté sometida a los mismos Procedimientos y estándares que el resto de aquella. La conjunción de ambas necesidades cristaliza en la figura del auditor interno informático.

En cuanto a empresas se refiere, solamente las más grandes pueden poseer una Auditoría propia y permanente, mientras que el resto acuden a las auditorias externas. Puede ser que algún profesional informático sea trasladado desde su puesto de trabajo a la Auditoría Interna de la empresa cuando ésta existe.

Finalmente, la propia Informática requiere de su propio grupo de Control Interno, con implantación física en su estructura, puesto que si se ubicase dentro de la estructura Informática ya no sería independiente. Hoy, ya existen varias organizaciones Informáticas dentro de la misma empresa, y con diverso grado de autonomía, que son coordinadas por órganos corporativos de Sistemas de Información de las Empresas.

Una Empresa o Institución que posee auditoria interna puede y debe en ocasiones contratar servicios de auditoria externa. Las razones para hacerlo suelen ser:

- Necesidad de auditar una materia de gran especialización, para la cual los servicios propios no están suficientemente capacitados.
- Contrastar algún Informe interno con el que resulte del externo, en aquellos supuestos de emisión interna de graves recomendaciones que chocan con la opinión generalizada de la propia empresa.
- Servir como mecanismo protector de posibles auditorias informáticas externas decretadas por la misma empresa.
- Aunque la auditoria interna sea independiente del Departamento de Sistemas, sigue siendo la misma empresa, por lo tanto, es necesario que se le realicen auditorias externas como para tener una visión desde afuera de la empresa.

La auditoria informática, tanto externa como interna, debe ser una actividad exenta de cualquier contenido o matiz "político" ajeno a la propia estrategia y política general de la empresa. La función auditora

puede actuar de oficio, por iniciativa del propio órgano, o a instancias de parte, esto es, por encargo de la dirección o cliente.

Alcance de la Auditoria Informática:

El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoría informática, se complementa con los objetivos de ésta. El alcance ha de figurar expresamente en el Informe Final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas. Ejemplo: ¿Se someterán los registros grabados a un control de integridad exhaustivo*? ¿Se comprobará que los controles de validación de errores son adecuados y suficientes*? La indefinición de los alcances de la auditoría compromete el éxito de la misma.

Control de integridad de registros:

Hay Aplicaciones que comparten registros, son registros comunes. Si una Aplicación no tiene integrado un registro común, cuando lo necesite utilizar no lo va encontrar y, por lo tanto, la aplicación no funcionaría como debería.

Control de validación de errores:

*S*e corrobora que el sistema que se aplica para detectar y corregir errores sea eficiente.

Características de la Auditoria Informática:

La información de la empresa y para la empresa, siempre importante, se ha convertido en un Activo Real de la misma, como sus Stocks o materias primas si las hay. Por ende, han de realizarse inversiones informáticas, materia de la que se ocupa la *Auditoría de Inversión Informática*.

Del mismo modo, los Sistemas Informáticos han de protegerse de modo global y particular: a ello se debe la existencia de la *Auditoría de Seguridad Informática* en general, o a la auditoría de Seguridad de alguna de sus áreas, como pudieran ser Desarrollo o Técnica de Sistemas.

Cuando se producen cambios estructurales en la Informática, se reorganiza de alguna forma su función: se está en el campo de la *Auditoría de Organización Informática.*

Estos tres tipos de auditorias engloban a las actividades auditoras que se realizan en una auditoría parcial. De otra manera: cuando se realiza una auditoria del área de Desarrollo de Proyectos de la Informática de una empresa, es porque en ese Desarrollo existen, además de ineficiencias, debilidades de organización, o de inversiones, o de seguridad, o alguna mezcla de ellas.

Tipos y clases de Auditorias:

El departamento de Informática posee una actividad proyectada al exterior, al usuario, aunque el "exterior" siga siendo la misma empresa. He aquí, la *Auditoria Informática de Usuario*. Se hace esta distinción para contraponerla a la informática interna, en donde se hace la informática cotidiana y real. En consecuencia, existe una *Auditoria Informática de Actividades Internas*.

El control del funcionamiento del departamento de informática con el exterior, con el usuario se realiza por medio de la Dirección. Su figura es importante, en tanto en cuanto es capaz de interpretar las necesidades de la Compañía. Una informática eficiente y eficaz requiere el apoyo continuado de su Dirección frente al "exterior". Revisar estas interrelaciones constituye el objeto de la *Auditoria Informática de Dirección*. Estas tres auditorias, mas la auditoria de Seguridad, son las cuatro Áreas Generales de la Auditoria Informática más importantes.

Dentro de las áreas generales, se establecen las siguientes divisiones de Auditoría Informática: de Explotación, de Sistemas, de Comunicaciones y de Desarrollo de Proyectos. Estas son las Areas Especificas de la Auditoría Informática más importantes.

Áreas Específicas	**Áreas Generales**			
	Interna	Dirección	Usuario	Seguridad
Explotación				
Desarrollo				
Sistemas				
Comunicaciones				
Seguridad				

Cada Área Especifica puede ser auditada desde los siguientes criterios generales:
- Desde su propio funcionamiento interno.
- Desde el apoyo que recibe de la Dirección y, en sentido ascendente, del grado de cumplimiento de las directrices de ésta.
- Desde la perspectiva de los usuarios, destinatarios reales de la informática.
- Desde el punto de vista de la seguridad que ofrece la Informática en general o la rama auditada.

Estas combinaciones pueden ser ampliadas y reducidas según las características de la empresa auditada.

Objetivo fundamental de la auditoria informática:

Operatividad

La operatividad es una función de mínimos consistente en que la organización y las maquinas funcionen, siquiera mínimamente. No es admisible detener la maquinaria informática para descubrir sus fallos y comenzar de nuevo. La auditoría debe iniciar su actividad cuando los Sistemas están operativos, es el principal objetivo el de mantener tal situación. Tal objetivo debe conseguirse tanto a nivel global como parcial.

La operatividad de los Sistemas ha de constituir entonces la principal preocupación del auditor informático. Para conseguirla hay que acudir a la realización de *Controles Técnicos Generales de Operatividad* y *Controles Técnicos Específicos de Operatividad*, previos a cualquier actividad de aquel.

- Los Controles Técnicos Generales son los que se realizan para verificar la compatibilidad de funcionamiento simultaneo del Sistema Operativo y el Software de base con todos los subsistemas existentes, así como la compatibilidad del Hardware y del Software instalados. Estos controles son importantes en las instalaciones que cuentan con varios competidores, debido a que la profusión de entornos de trabajo muy diferenciados obliga a la contratación de diversos productos de Software básico, con el consiguiente riesgo de abonar más de una vez el mismo producto o desaprovechar parte del Software abonado. Puede ocurrir también con los productos de Software básico desarrolla-dos por el personal de Sistemas Interno, sobre todo cuando los diversos equipos están ubicados en Centros de Proceso de Datos geográficamente alejados. Lo negativo de esta situación es que puede producir la inoperatividad del conjunto. Cada Centro de Proceso de Datos tal vez sea operativo trabajando independientemente, pero no será posible la interconexión e intercomunicación de todos los Centros de Proceso de Datos si no existen productos comunes y compatibles.

- Los Controles Técnicos Específicos, de modo menos acusado, son igualmente necesarios para lograr la Operatividad de los Sistemas. Un ejemplo de lo que se puede encontrar mal son parámetros de asignación automática de espacio en disco* que dificulten o impidan su utilización posterior por una Sección distinta de la que lo generó. También, los periodos de retención de ficheros comunes a varias Aplicaciones pueden estar definidos con distintos plazos en cada una de ellas, de modo que la pérdida de información es un hecho que podrá producirse con facilidad, quedando inoperativa la explotación de alguna de las Aplicaciones mencionadas.

Parámetros de asignación automática de espacio en disco:

Todas las Aplicaciones que se desarrollan son super-parametrizadas , es decir, que tienen un montón de parámetros que permiten configurar cual va a ser el comportamiento del Sistema. Una Aplicación va a usar para tal y tal cosa cierta cantidad de espacio en disco. Si uno no analizó cual es la operatoria y el tiempo que le va a llevar ocupar el espacio asignado, y se pone un valor muy chico, puede ocurrir que un día la Aplicación reviente, se caiga. Si esto sucede en medio de la operatoria y la Aplicación se cae, el volver a levantarla, con la nueva asignación de espacio, si hay que hacer reconversiones o lo que sea, puede llegar a demandar muchísimo tiempo, lo que significa un riesgo enorme.

Revisión de Controles de la Gestión Informática:

Una vez conseguida la Operatividad de los Sistemas, el segundo objetivo de la auditoria es la verificación de la observancia de las normas teóricamente existentes en el departamento de Informática y su coherencia con las del resto de la empresa. Para ello, habrán de revisarse sucesivamente y en este orden:

1. 1. Las Normas Generales de la Instalación Informática. Se realizará una revisión inicial sin estudiar a fondo las contradicciones que pudieran existir, pero registrando las áreas que carezcan de normativa, y sobre todo verificando que esta Normativa General Informática no está en contradicción con alguna Norma General no informática de la empresa.
2. Los Procedimientos Generales Informáticos. Se verificará su existencia, al menos en los sectores más importantes. Por ejemplo, la recepción definitiva de las máquinas debería estar firmada por los responsables de Explotación. Tampoco el alta de una nueva Aplicación podría producirse si no existieran los Procedimientos de Backup y Recuperación correspondientes.
3. Los Procedimientos Específicos Informáticos. Igualmente, se revisara su existencia en las áreas fundamentales. Así, Explotación no debería explotar una Aplicación sin haber exigido a Desarrollo la pertinente documentación. Del mismo modo, deberá comprobarse que los Procedimientos Específicos no se opongan a los Procedimientos Generales. En todos los casos anteriores, a su vez, deberá verificarse que no existe contradicción alguna con la Normativa y los Procedimientos Generales de la propia empresa, a los que la Informática debe estar sometida.

AUDITORÍA INFORMÁTICA DE EXPLOTACIÓN:

La Explotación Informática se ocupa de producir resultados informáticos de todo tipo: listados impresos, ficheros soportados magnéticamente para otros informáticos, ordenes automatizadas para lanzar o modificar procesos industriales, etc. La explotación informática se puede considerar como una fabrica con ciertas peculiaridades que la distinguen de las reales. Para realizar la Explotación Informática se dispone de una materia prima, los Datos, que es necesario transformar, y que se someten previamente a controles de integridad y calidad. La transformación se realiza por medio del Proceso informático, el cual está gobernado por programas. Obtenido el producto final, los resultados son sometidos a varios controles de calidad y, finalmente, son distribuidos al cliente, al usuario.

Auditar Explotación consiste en auditar las secciones que la componen y sus interrelaciones. La Explotación Informática se divide en tres grandes áreas: Planificación, Producción y Soporte Técnico, en la que cada cual tiene varios grupos.

Control de Entrada de Datos:

Se analizará la captura de la información en soporte compatible con los Sistemas, el cumplimiento de plazos y calendarios de tratamientos y entrega de datos; la correcta transmisión de datos entre entornos diferentes. Se verificará que los controles de integridad y calidad de datos se realizan de acuerdo a Norma.

Planificación y Recepción de Aplicaciones:

Se auditarán las normas de entrega de Aplicaciones por parte de Desarrollo, verificando su cumplimiento y su calidad de interlocutor único. Deberán realizarse muestreos selectivos de la Documentación de las Aplicaciones explotadas. Se inquirirá sobre la anticipación de contactos con Desarrollo para la planificación a medio y largo plazo.

Centro de Control y Seguimiento de Trabajos:

Se analizará cómo se prepara, se lanza y se sigue la producción diaria. Básicamente, la explotación Informática ejecuta procesos por cadenas o lotes sucesivos (Batch*), o en tiempo real (Tiempo Real*). Mientras que las Aplicaciones de Teleproceso están permanentemente activas y la función de Explotación se limita a vigilar y recuperar incidencias, el trabajo Batch absorbe una buena parte de los efectivos de Explotación. En muchos Centros de Proceso de Datos, éste órgano recibe el nombre de Centro de Control de Batch. Este grupo determina el éxito de la explotación, en cuanto que es uno de los factores más importantes en el mantenimiento de la producción.

Batch y Tiempo Real:

Las Aplicaciones que son Batch son Aplicaciones que cargan mucha información durante el día y durante la noche se corre un proceso enorme que lo que hace es relacionar toda la información, calcular cosas y obtener como salida, por ejemplo, reportes. O sea, recolecta información durante el día, pero todavía no procesa nada. Es solamente un tema de "Data Entry" que recolecta información, corre el proceso Batch (por lotes), y calcula todo lo necesario para arrancar al día siguiente.

Las Aplicaciones que son Tiempo Real u Online, son las que, luego de haber ingresado la información correspondiente, inmediatamente procesan y devuelven un resultado. Son Sistemas que tienen que responder en Tiempo Real.

Operación. Salas de Ordenadores:

Se intentarán analizar las relaciones personales y la coherencia de cargos y salarios, así como la equidad en la asignación de turnos de trabajo. Se verificará la existencia de un responsable de Sala en cada turno de trabajo. Se analizará el grado de automatización de comandos, se verificara la existencia y grado de uso de los Manuales de Operación. Se analizará no solo la existencia de planes de formación, sino el cumplimiento de los mismos y el tiempo transcurrido para cada Operador desde el último Curso recibido. Se estudiarán los montajes diarios y por horas de cintas o cartuchos, así como los tiempos transcurridos entre la petición de montaje por parte del Sistema hasta el montaje real. Se verificarán las líneas de papel impresas diarias y por horas, así como la manipulación de papel que comportan.

Centro de Control de Red y Centro de Diagnosis:

El Centro de Control de Red suele ubicarse en el área de producción de Explotación. Sus funciones se refieren exclusivamente al ámbito de las Comunicaciones, estando muy relacionado con la organización de Software de Comunicaciones de Técnicas de Sistemas. Debe analizarse la fluidez de esa relación y el grado de coordinación entre ambos. Se verificará la existencia de un punto focal único, desde el cual sean perceptibles todos las líneas asociadas al Sistema. El Centro de Diagnosis es el ente en donde se atienden las llamadas de los usuarios-clientes que han sufrido averías o incidencias, tanto de Software como de Hardware. El Centro de Diagnosis está especialmente indicado para informáticos grandes y con usuarios dispersos en un amplio territorio. Es uno de los elementos que más contribuyen a configurar la imagen de la Informática de la empresa. Debe ser auditada desde esta perspectiva, desde la sensibilidad del usuario sobre el servicio que se le dispone.

No basta con comprobar la eficiencia técnica del Centro, es necesario analizarlo simultáneamente en el ámbito de Usuario.

Auditoria Informática De Desarrollo De Proyectos O Aplicaciones:

La función de Desarrollo es una evolución del llamado Análisis y Programación de Sistemas y Aplicaciones.

A su vez, engloba muchas áreas, tantas como sectores informatizables tiene la empresa. Muy escuetamente, una Aplicación recorre las siguientes fases:

- Prerrequisitos del Usuario (único o plural) y del entorno
- Análisis funcional
- Diseño
- Análisis orgánico (Reprogramación y Programación)
- Pruebas
- Entrega a Explotación y alta para el Proceso.

Estas fases deben estar sometidas a un exigente control interno, caso contrario, además del disparo de los costes, podrá producirse la insatisfacción del usuario. Finalmente, la auditoria deberá comprobar la seguridad de los programas en el sentido de garantizar que los ejecutados por la maquina sean exactamente los previstos y no otros.

Una auditoria de Aplicaciones pasa indefectiblemente por la observación y el análisis de cuatro consideraciones:

Revisión de las metodologías utilizadas: Se analizaran éstas, de modo que se asegure la modularidad de las posibles futuras ampliaciones de la Aplicación y el fácil mantenimiento de las mismas.

Control Interno de las Aplicaciones: se deberán revisar las mismas fases que presuntamente han debido seguir el área correspondiente de Desarrollo:

- Estudio de Vialidad de la Aplicación. [importante para Aplicaciones largas, complejas y caras]
- Definición Lógica de la Aplicación. [se analizará que se han observado los postulados lógicos de actuación, en función de la metodología elegida y la finalidad que persigue el proyecto]
- Desarrollo Técnico de la Aplicación. [Se verificará que éste es ordenado y correcto. Las herramientas técnicas utilizadas en los diversos programas deberán ser compatibles]
- Diseño de Programas. [deberán poseer la máxima sencillez, modularidad y economía de recursos]
- Métodos de Pruebas. [Se realizarán de acuerdo a las Normas de la Instalación. Se utilizarán juegos de ensayo de datos, sin que sea permisible el uso de datos reales]
- Documentación. [cumplirá la Normativa establecida en la Instalación, tanto la de Desarrollo como la de entrega de Aplicaciones a Explotación]
- Equipo de Programación. [Deben fijarse las tareas de análisis puro, de programación y las intermedias. En Aplicaciones complejas se producirían variaciones en la composición del grupo, pero estos deberán estar previstos]

Satisfacción de usuarios: Una Aplicación técnicamente eficiente y bien desarrollada, deberá considerarse fracasada si no sirve a los intereses del usuario que la solicitó. La aquiescencia del usuario proporciona grandes ventajas posteriores, ya que evitará reprogramaciones y disminuirá el mantenimiento de la Aplicación.

Control de Procesos y Ejecuciones de Programas Críticos: El auditor no debe descartar la posibilidad de que se esté ejecutando un módulo que no se corresponde con el programa fuente que desarrolló, codificó y probó el área de Desarrollo de Aplicaciones. Se ha de comprobar la correspondencia biunívoca y exclusiva entre el

programa codificado y su compilación. Si los programas fuente y los programa módulo no coincidieran podríase provocar, desde errores de bulto que producirían graves y altos costes de mantenimiento, hasta fraudes, pasando por acciones de sabotaje, espionaje industrial-informativo, etc. Por ende, hay normas muy rígidas en cuanto a las Librerías de programas; aquellos programas fuente que hayan sido dados por bueno por Desarrollo, son entregados a Explotación con el fin de que éste:

1. 1. Copie el programa fuente en la Librería de Fuentes de Explotación, a la que nadie más tiene acceso
2. Compile y monte ese programa, depositándolo en la Librería de Módulos de Explotación, a la que nadie más tiene acceso.
3. Copie los programas fuente que les sean solicitados para modificarlos, arreglarlos, etc. en el lugar que se le indique. Cualquier cambio exigirá pasar nuevamente por el punto 1.

Como este sistema para auditar y dar el alta a una nueva Aplicación es bastante ardua y compleja, hoy (algunas empresas lo usarán, otras no) se utiliza un sistema llamado U.A.T (User Acceptance Test). Este consiste en que el futuro usuario de esta Aplicación use la Aplicación como si la estuviera usando en Producción para que detecte o se denoten por sí solos los errores de la misma. Estos defectos que se encuentran se van corrigiendo a medida que se va haciendo el U.A.T. Una vez que se consigue el U.A.T., el usuario tiene que dar el Sign Off ("Esto está bien"). Todo este testeo, auditoría lo tiene que controlar, tiene que evaluar que el testeo sea correcto, que exista un plan de testeo, que esté involucrado tanto el cliente como el desarrollador y que estos defectos se corrijan. Auditoría tiene que corroborar que el U.A.T. prueba todo y que el Sign Off del usuario sea un Sign Off por **todo**.

Auditoría Informática De Sistemas:

Se ocupa de analizar la actividad que se conoce como Técnica de Sistemas en todas sus facetas. Hoy, la importancia creciente de las telecomunicaciones ha propiciado que las Comunicaciones, Líneas y Redes de las instalaciones informáticas, se auditen por separado, aunque formen parte del entorno general de Sistemas.

Sistemas Operativos:

Engloba los Subsistemas de Teleproceso, Entrada/Salida, etc. Debe verificarse en primer lugar que los Sistemas están actualizados con las últimas versiones del fabricante, indagando las causas de las omisiones si las hubiera. El análisis de las versiones de los Sistemas Operativos permite descubrir las posibles incompatibilidades entre otros productos de Software Básico adquiridos por la instalación y determinadas versiones de aquellas. Deben revisarse los parámetros variables de las Librerías más importantes de los Sistemas, por si difieren de los valores habituales aconsejados por el constructor.

Software Básico:

Es fundamental para el auditor conocer los productos de software básico que han sido facturados aparte de la propia computadora. Esto, por razones económicas y por razones de comprobación de que la computadora podría funcionar sin el producto adquirido por el cliente. En cuanto al Software desarrollado por el personal informático de la empresa, el auditor debe verificar que éste no agreda ni condiciona al Sistema. Igualmente, debe considerar el esfuerzo realizado en términos de costes, por si hubiera alternativas más económicas.

Software de Teleproceso (Tiempo Real):

No se incluye en Software Básico por su especialidad e importancia. Las consideraciones anteriores son válidas para éste también.

Tunning:

Es el conjunto de técnicas de observación y de medidas encaminadas a la evaluación del comportamiento de los Subsistemas y del Sistema en su conjunto. Las acciones de tunning deben diferenciarse de los controles habituales que realiza el personal de Técnica de Sistemas. El tunning posee una naturaleza más revisora, estableciéndose previamente planes y programas de actuación según los síntomas observados. Se pueden realizar:

- ✓ Cuando existe sospecha de deterioro del comportamiento parcial o general del Sistema
- ✓ De modo sistemático y periódico, por ejemplo cada 6 meses. En este caso sus acciones son repetitivas y están planificados y organizados de antemano.

El auditor deberá conocer el número de Tunning realizados en el último año, así como sus resultados. Deberá analizar los modelos de carga utilizados y los niveles e índices de confianza de las observaciones.

Optimización de los Sistemas y Subsistemas:

Técnica de Sistemas debe realizar acciones permanentes de optimización como consecuencia de la realización de tunnings preprogramados o específicos. El auditor verificará que las acciones de optimización* fueron efectivas y no comprometieron la Operatividad de los Sistemas ni el plan crítico de producción diaria de Explotación.

***Optimización:**

Por ejemplo: cuando se instala una Aplicación, normalmente está vacía, no tiene nada cargado adentro. Lo que puede suceder es que, a medida que se va cargando, la Aplicación se va poniendo cada vez más lenta; porque todas las referencias a tablas es cada vez más grande, la información que está moviendo es cada vez mayor, entonces la Aplicación se tiende a poner lenta. Lo que se tiene que hacer es un análisis de performance, para luego optimizarla, mejorar el rendimiento de dicha Aplicación.

Administración de Base de Datos:

El diseño de las Bases de Datos, sean relaciones o jerárquicas, se ha convertido en una actividad muy compleja y sofisticada, por lo general desarrollada en el ámbito de Técnica de Sistemas, y de acuerdo con las áreas de Desarrollo y usuarios de la empresa. Al conocer el diseño y arquitectura de éstas por parte de Sistemas, se les encomienda también su administración. Los auditores de Sistemas han observado algunas disfunciones derivadas de la relativamente escasa experiencia que Técnica de Sistemas tiene sobre la problemática general de los usuarios de Bases de Datos.

La administración tendría que estar a cargo de Explotación. El auditor de Base de Datos debería asegurarse que Explotación conoce suficientemente las que son accedidas por los Procedimientos que ella ejecuta. Analizará los Sistemas de salvaguarda existentes, que competen igualmente a Explotación. Revisará finalmente la integridad y consistencia de los datos, así como la ausencia de redundancias entre ellos.

Investigación y Desarrollo:

Como empresas que utilizan y necesitan de informáticas desarrolladas, saben que sus propios efectivos están desarrollando Aplicaciones y utilidades que, concebidas inicialmente para su uso interno, pueden ser susceptibles de adquisición por otras empresas, haciendo competencia a las Compañías del ramo. La auditoría informática deberá cuidar de que la actividad de Investigación y Desarrollo no interfiera ni dificulte las tareas fundamentales internas.

<La propia existencia de aplicativos para la obtención de estadísticas desarrollados por los técnicos de Sistemas de la empresa auditada, y su calidad, proporcionan al auditor experto una visión bastante exacta de la eficiencia y estado de desarrollo de los Sistemas>

Auditoria Informática De Comunicaciones Y Redes:

Para el informático y para el auditor informático, el entramado conceptual que constituyen las Redes Nodales, Líneas, Concentradores, Multiplexores, Redes Locales, etc. no son sino el soporte físico-lógico del Tiempo Real. El auditor tropieza con la dificultad técnica del entorno, pues ha de analizar situaciones y hechos alejados entre sí, y está condicionado a la participación del monopolio telefónico que presta el soporte. Como en otros casos, la auditoria de este sector requiere un equipo de especialistas, expertos simultáneamente en

Comunicaciones y en Redes Locales (no hay que olvidarse que en entornos geográficos reducidos, algunas empresas optan por el uso interno de Redes Locales, diseñadas y cableadas con recursos propios).

El auditor de Comunicaciones deberá inquirir sobre los índices de utilización de las líneas contratadas con información abundante sobre tiempos de desuso. Deberá proveerse de la topología de la Red de Comunicaciones, actualizada, ya que la desactualizacion de esta documentación significaría una grave debilidad. La inexistencia de datos sobre la cuantas líneas existen, cómo son y donde están instaladas, supondría que se bordea la Inoperatividad Informática. Sin embargo, las debilidades más frecuentes o importantes se encuentran en las disfunciones organizativas. La contratación e instalación de líneas va asociada a la instalación de los Puestos de Trabajo correspondientes (Pantallas, Servidores de Redes Locales, Computadoras con tarjetas de Comunicaciones, impresoras, etc.). Todas estas actividades deben estar muy coordinadas y a ser posible, dependientes de una sola organización.

Auditoria De La Seguridad Informática:

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. También puede ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional. Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos.

En la actualidad y principalmente en las computadoras personales, se ha dado otro factor que hay que considerar: el llamado "virus" de las computadoras, el cual, aunque tiene diferentes intenciones, se encuentra principalmente para paquetes que son copiados sin autorización ("piratas") y borra toda la información que se tiene en un disco. Al auditar los sistemas se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus. El uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos.

La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica. La seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc.

La seguridad lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

Un método eficaz para proteger sistemas de computación es el software de control de acceso. Dicho simplemente, los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden del usuario una contraseña antes de permitirle el acceso a información confidencial. Dichos paquetes han sido populares desde hace muchos años en el mundo de las computadoras grandes, y los principales proveedores ponen a disposición de clientes algunos de estos paquetes.

Ejemplo: Existe una Aplicación de Seguridad que se llama SEOS, para Unix, que lo que hace es auditar el nivel de Seguridad en todos los servidores, como ser: accesos a archivos, accesos a directorios, que usuario lo hizo, si tenía o no tenía permiso, si no tenía permiso porque falló, entrada de usuarios a cada uno de los servidores, fecha y hora, accesos con password equivocada, cambios de password, etc. La Aplicación lo puede graficar, tirar en números, puede hacer reportes, etc.

La seguridad informática se la puede dividir como Area General y como Area Especifica (seguridad de Explotación, seguridad de las Aplicaciones, etc.). Así, se podrán efectuar auditorías de la Seguridad Global de

una Instalación Informática –Seguridad General- y auditorías de la Seguridad de un área informática determinada – Seguridad Especifica -.

Con el incremento de agresiones a instalaciones informáticas en los últimos años, se han ido originando acciones para mejorar la Seguridad Informática a nivel físico. Los accesos y conexiones indebidos a través de las Redes de Comunicaciones, han acelerado el desarrollo de productos de Seguridad lógica y la utilización de sofisticados medios criptograficos.

El sistema integral de seguridad debe comprender:

- Elementos administrativos
- Definición de una política de seguridad
- Organización y división de responsabilidades
- Seguridad física y contra catástrofes(incendio, terremotos, etc.)
- Prácticas de seguridad del personal
- Elementos técnicos y procedimientos
- Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales.
- Aplicación de los sistemas de seguridad, incluyendo datos y archivos
- El papel de los auditores, tanto internos como externos
- Planeación de programas de desastre y su prueba.

La decisión de abordar una Auditoría Informática de Seguridad Global en una empresa, se fundamenta en el estudio cuidadoso de los riesgos potenciales a los que está sometida. Se elaboran "matrices de riesgo", en donde se consideran los factores de las "Amenazas" a las que está sometida una instalación y los "Impactos" que aquellas puedan causar cuando se presentan. Las matrices de riesgo se representan en cuadros de doble entrada <<Amenaza-Impacto>>, en donde se evalúan las probabilidades de ocurrencia de los elementos de la matriz. Ejemplo:

Impacto	Amenaza				1: Improbable 2: Probable 3: Certeza -: Despreciable
	Error	Incendio	Sabotaje	……..	
Destrucción de Hardware	-	1	1		
Borrado de Información	3	1	1		

El cuadro muestra que si por error codificamos un parámetro que ordene el borrado de un fichero, éste se borrará con certeza.

Herramientas y Técnicas para la Auditoría Informática:

Cuestionarios:

Las auditorias informáticas se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

Para esto, suele ser lo habitual comenzar solicitando la cumplimentación de cuestionarios preimpresos que se envían a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar.

Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación, y muy cuidados en su fondo y su forma.

Sobre esta base, se estudia y analiza la documentación recibida, de modo que tal análisis determine a su vez la información que deberá elaborar el propio auditor. El cruzamiento de ambos tipos de información es una de las bases fundamentales de la auditoría.
Cabe aclarar, que esta primera fase puede omitirse cuando los auditores hayan adquirido por otro medios la información que aquellos preimpresos hubieran proporcionado.

Entrevistas:

El auditor comienza a continuación las relaciones personales con el auditado. Lo hace de tres formas:

1. Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.
2. Mediante "entrevistas" en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.
3. Por medio de entrevistas en las que el auditor sigue un método preestablecido de antemano y busca unas finalidades concretas.

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

Aparte de algunas cuestiones menos importantes, la entrevista entre auditor y auditado se basa fundamentalmente en el concepto de interrogatorio; es lo que hace un auditor, interroga y se interroga a sí mismo. El auditor informático experto entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente y con pulcritud a una serie de preguntas variadas, también sencillas. Sin embargo, esta sencillez es solo aparente. Tras ella debe existir una preparación muy elaborada y sistematizada, y que es diferente para cada caso particular.

Checklist:

El auditor profesional y experto es aquél que reelabora muchas veces sus cuestionarios en función de los escenarios auditados. Tiene claro lo que necesita saber, y por qué. Sus cuestionarios son vitales para el trabajo de análisis, cruzamiento y síntesis posterior, lo cual no quiere decir que haya de someter al auditado a unas preguntas estereotipadas que no conducen a nada. Muy por el contrario, el auditor conversará y hará preguntas "normales", que en realidad servirán para la cumplimentación sistemática de sus Cuestionarios, de sus Checklists.

Hay opiniones que descalifican el uso de las Checklists, ya que consideran que leerle una pila de preguntas recitadas de memoria o leídas en voz alta descalifica al auditor informático. Pero esto no es usar Checklists, es una evidente falta de profesionalismo. El profesionalismo pasa por un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes. El profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente.

El conjunto de estas preguntas recibe el nombre de Checklist. Salvo excepciones, las Checklists deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma.

Según la claridad de las preguntas y el talante del auditor, el auditado responderá desde posiciones muy distintas y con disposición muy variable. El auditado, habitualmente informático de profesión, percibe con cierta facilidad el perfil técnico y los conocimientos del auditor, precisamente a través de las preguntas que éste le formula. Esta percepción configura el principio de autoridad y prestigio que el auditor debe poseer.

Por ello, aun siendo importante tener elaboradas listas de preguntas muy sistematizadas, coherentes y clasificadas por materias, todavía lo es más el modo y el orden de su formulación. Las empresas externas de Auditoría Informática guardan sus Checklists, pero de poco sirven si el auditor no las utiliza adecuada y oportunamente. No debe olvidarse que la función auditora se ejerce sobre bases de autoridad, prestigio y ética.

El auditor deberá aplicar la Checklist de modo que el auditado responda clara y escuetamente. Se deberá interrumpir lo menos posible a éste, y solamente en los casos en que las respuestas se aparten sustancialmente de la pregunta. En algunas ocasiones, se hará necesario invitar a aquél a que exponga con mayor amplitud un tema concreto, y en cualquier caso, se deberá evitar absolutamente la presión sobre el mismo.

Algunas de las preguntas de las Checklists utilizadas para cada sector, deben ser repetidas. En efecto, bajo apariencia distinta, el auditor formulará preguntas equivalentes a las mismas o a distintas personas, en las mismas fechas, o en fechas diferentes. De este modo, se podrán descubrir con mayor facilidad los puntos contradictorios; el auditor deberá analizar los matices de las respuestas y reelaborar preguntas complementarias cuando hayan existido contradicciones, hasta conseguir la homogeneidad. El entrevistado no debe percibir un excesivo formalismo en las preguntas. El auditor, por su parte, tomará las notas imprescindibles en presencia del auditado, y nunca escribirá cruces ni marcará cuestionarios en su presencia.

Los cuestionarios o Checklists responden fundamentalmente a dos tipos de "filosofía" de calificación o evaluación:

a. Checklist de rango

Contiene preguntas que el auditor debe puntuar dentro de un rango preestablecido (por ejemplo, de 1 a 5, siendo 1 la respuesta más negativa y el 5 el valor más positivo)

Ejemplo de Checklist de rango:

Se supone que se está realizando una auditoría sobre la seguridad física de una instalación y, dentro de ella, se analiza el control de los accesos de personas y cosas al Centro de Cálculo. Podrían formularse las preguntas que figuran a continuación, en donde las respuestas tiene los siguientes significados:

1_ Muy deficiente.
2_ Deficiente.
3_ Mejorable.
4_ Aceptable.
5_ Correcto.

Se figuran posibles respuestas de los auditados. Las preguntas deben sucederse sin que parezcan encorsetadas ni clasificadas previamente. Basta con que el auditor lleve un pequeño guión. La cumplimentación de la Checklist no debe realizarse en presencia del auditado.

-¿Existe personal específico de vigilancia externa al edificio?
No, solamente un guarda por la noche que atiende además otra instalación adyacente.

-Para la vigilancia interna del edificio, ¿Hay al menos un vigilante por turno en los aledaños del Centro de Cálculo?
Si, pero sube a las otras 4 plantas cuando se le necesita.

-¿Hay salida de emergencia además de la habilitada para la entrada y salida de máquinas?
Si, pero existen cajas apiladas en dicha puerta. Algunas veces las quitan.

-El personal de Comunicaciones, ¿Puede entrar directamente en la Sala de Computadoras?
No, solo tiene tarjeta el Jefe de Comunicaciones. No se la da a su gente mas que por causa muy justificada, y avisando casi siempre al Jefe de Explotación.

El resultado sería el promedio de las puntuaciones: (1 + 2 + 2 + 4) /4 = 2,25 Deficiente.

b. Checklist Binaria

Es la constituida por preguntas con respuesta única y excluyente: Si o No. Aritméticamente, equivalen a 1(uno) o 0(cero), respectivamente.

Ejemplo de Checklist Binaria:

Se supone que se está realizando una Revisión de los métodos de pruebas de programas en el ámbito de Desarrollo de Proyectos.

-¿Existe Normativa de que el usuario final compruebe los resultados finales de los programas?

-¿Conoce el personal de Desarrollo la existencia de la anterior normativa?

-¿Se aplica dicha norma en todos los casos?

-¿Existe una norma por la cual las pruebas han de realizarse con juegos de ensayo o copia de Bases de Datos reales?

Obsérvese como en este caso están contestadas las siguientes preguntas:
-¿Se conoce la norma anterior?

-¿Se aplica en todos los casos?

Las Checklists de rango son adecuadas si el equipo auditor no es muy grande y mantiene criterios uniformes y equivalentes en las valoraciones. Permiten una mayor precisión en la evaluación que en la checklist binaria. Sin embargo, la bondad del método depende excesivamente de la formación y competencia del equipo auditor.

Las Checklists Binarias siguen una elaboración inicial mucho más ardua y compleja. Deben ser de gran precisión, como corresponde a la suma precisión de la respuesta. Una vez construidas, tienen la ventaja de exigir menos uniformidad del equipo auditor y el inconveniente genérico del <si o no> frente a la mayor riqueza del intervalo.

No existen Checklists estándar para todas y cada una de las instalaciones informáticas a auditar. Cada una de ellas posee peculiaridades que hacen necesarios los retoques de adaptación correspondientes en las preguntas a realizar.

Trazas y/o Huellas:

Con frecuencia, el auditor informático debe verificar que los programas, tanto de los Sistemas como de usuario, realizan exactamente las funciones previstas, y no otras. Para ello se apoya en productos Software muy potentes y modulares que, entre otras funciones, rastrean los caminos que siguen los datos a través del programa.

Muy especialmente, estas "Trazas" se utilizan para comprobar la ejecución de las validaciones de datos previstas. Las mencionadas trazas no deben modificar en absoluto el Sistema. Si la herramienta auditora produce incrementos apreciables de carga, se convendrá de antemano las fechas y horas más adecuadas para su empleo.

Por lo que se refiere al análisis del Sistema, los auditores informáticos emplean productos que comprueban los valores asignados por Técnica de Sistemas a cada uno de los parámetros variables de las Librerías más importantes del mismo. Estos parámetros variables deben estar dentro de un intervalo marcado por el fabricante. A modo de ejemplo, algunas instalaciones descompensan el número de iniciadores de trabajos de determinados entornos o toman criterios especialmente restrictivos o permisivos en la asignación de unidades de servicio para según cuales tipos carga. Estas actuaciones, en principio útiles, pueden resultar contraproducentes si se traspasan los límites.

No obstante la utilidad de las Trazas, ha de repetirse lo expuesto en la descripción de la auditoría informática de Sistemas: el auditor informático emplea preferentemente la amplia información que proporciona el propio Sistema: Así, los ficheros de <Accounting> o de <contabilidad>, en donde se encuentra la producción completa de aquél, y los <Log*> de dicho Sistema, en donde se recogen las modificaciones de datos y se pormenoriza la actividad general.

Del mismo modo, el Sistema genera automáticamente exacta información sobre el tratamiento de errores de maquina central, periféricos, etc.
[La auditoría financiero-contable convencional emplea trazas con mucha frecuencia. Son programas encaminados a verificar lo correcto de los cálculos de nóminas, primas, etc.].

Pruebas Del Sistema

Cuando los programadores enlazan sus programas para formar una secuencia, ésta ha de probarse en su conjunto para garantizar que cumple su cometido. Esta es una etapa muy importante para el sistema, en la que el auditor ha de verificar muchas cosas. La preparación de los datos de prueba deberá llevar consigo lo siguiente :

Recogida de un conjunto de datos que refleje todas las variantes de los valores y errores que puedan surgir en el sistema en cada momento.

Preparación de una implantación de los resultados que ha de producir el sistema cuando ejecute los datos de prueba.

Al principio, los auditores se ocuparán de ver si el alcance de los datos de prueba es suficiente como para verificarlo por completo y sugerirán las modificaciones que puedan complementar las pruebas para ayudar a los trabajos de auditoría. Al mismo tiempo, deberá comprobar si se han obtenido los resultados previstos, tomando muestras en varios puntos si fuera necesario. El diseño de datos de prueba a partir de los flujogramas y las especificaciones tiende a demostrar que el sistema hace lo que se diseñó que hiciera, en vez de lo que debería hacer, con lo que el diseño o se comprueba por completo.

Las pruebas reales del sistema implican una serie de pasadas de prueba en las que se vayan eliminando errores progresivamente. Quizás se necesiten varias pasadas para utilizar todos los datos de prueba porque la ocurrencia de una prueba podría excluir la posibilidad de que sucedieran otras cosas. Siempre se verificarán los resultados comparándolos con lo que se esperaban obtener. Una vez corregidos todos los errores, se hará una pasada final de prueba para demostrar que todas las correcciones se han hecho y que el sistema estará en condiciones de trabajo cuando se ponga en marcha.

Una vez verificada la preparación de los datos de prueba, el auditor se preocupará de la calidad de la verificación de los resultados, la oportunidad de las pasadas para asegurarse de que indican la posición cuando comience a utilizarse el sistema y de que las correcciones no han provocado corrupciones inesperadas en las rutinas que antes funcionaban bien.

Las pasadas de prueba no sólo se utilizarán para comprobar que los programas funcionan y que se entrelazan bien para formar sistemas, sino como función de formación en ciertas áreas y como medio de verificar que los procedimientos de control de datos y corrección de errores son adecuados y que funcionan correctamente.

****Log**:*
El log vendría a ser un historial que informa que fue cambiando y cómo fue cambiando (información). Las bases de datos, por ejemplo, utilizan el log para asegurar lo que se llaman las transacciones. Las transacciones son unidades atómicas de cambios dentro de una base de datos; toda esa serie de cambios se encuadra dentro de una transacción, y todo lo que va haciendo la Aplicación (grabar, modificar, borrar) dentro

de esa transacción, queda grabado en el log. La transacción tiene un principio y un fin, cuando la transacción llega a su fin, se vuelca todo a la base de datos. Si en el medio de la transacción se cortó por x razón, lo que se hace es volver para atrás. El log te permite analizar cronológicamente que es lo que sucedió con la información que está en el Sistema o que existe dentro de la base de datos.

Software de Interrogación:

Hasta hace ya algunos años se han utilizado productos software llamados genéricamente <paquetes de auditoría>, capaces de generar programas para auditores escasamente cualificados desde el punto de vista informático.

Más tarde, dichos productos evolucionaron hacia la obtención de muestreos estadísticos que permitieran la obtención de consecuencias e hipótesis de la situación real de una instalación.
En la actualidad, los productos Software especiales para la auditoría informática se orientan principalmente hacia lenguajes que permiten la interrogación de ficheros y bases de datos de la empresa auditada. Estos productos son utilizados solamente por los auditores externos, por cuanto los internos disponen del software nativo propio de la instalación.

Del mismo modo, la proliferación de las redes locales y de la filosofía "Cliente-Servidor", han llevado a las firmas de software a desarrollar interfaces de transporte de datos entre computadoras personales y mainframe, de modo que el auditor informático copia en su propia PC la información más relevante para su trabajo.

Cabe recordar, que en la actualidad casi todos los usuarios finales poseen datos e información parcial generada por la organización informática de la Compañía.

Efectivamente, conectados como terminales al "Host", almacenan los datos proporcionados por este, que son tratados posteriormente en modo PC. El auditor se ve obligado (naturalmente, dependiendo del alcance de la auditoría) a recabar información de los mencionados usuarios finales, lo cual puede realizar con suma facilidad con los polivalentes productos descritos. Con todo, las opiniones más autorizadas indican que el trabajo de campo del auditor informático debe realizarse principalmente con los productos del cliente.

Finalmente, ha de indicarse la conveniencia de que el auditor confeccione personalmente determinadas partes del Informe. Para ello, resulta casi imprescindible una cierta soltura en el manejo de Procesadores de Texto, paquetes de Gráficos, Hojas de Cálculo, etc.

Metodología de Trabajo de Auditoría Informática

El 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.*
- ✓ *Confección y redacción del Informe Final.*
- ✓ *Redacción de la Carta de Introducción o Carta de Presentación del Informe final.*

Definición de Alcance y Objetivos

El alcance de la auditoría expresa los límites de la misma. Debe existir un acuerdo muy preciso entre auditores y clientes sobre las funciones, las materias y las organizaciones a auditar.
A los efectos de acotar el trabajo, resulta muy beneficioso para ambas partes expresar las excepciones de alcance de la auditoría, es decir cuales materias, funciones u organizaciones no van a ser auditadas.

Tanto los alcances como las excepciones deben figurar al comienzo del Informe Final.

Las personas que realizan la auditoría han de conocer con la mayor exactitud posible los objetivos a los que su tarea debe llegar. Deben comprender los deseos y pretensiones del cliente, de forma que las metas fijadas puedan ser cumplidas.

Una vez definidos los objetivos (objetivos específicos), éstos se añadirán a los objetivos generales y comunes de a toda auditoría Informática: La operatividad de los Sistemas y los Controles Generales de Gestión Informática.

Estudio Inicial

Para realizar dicho estudio ha de examinarse las funciones y actividades generales de la informática. Para su realización el auditor debe conocer lo siguiente:

Organización:

Para el equipo auditor, el conocimiento de quién ordena, quién diseña y quién ejecuta es fundamental. Para realizar esto en auditor deberá fijarse en:

1) Organigrama:

El organigrama expresa la estructura oficial de la organización a auditar.

Si se descubriera que existe un organigrama fáctico diferente al oficial, se pondrá de manifiesto tal circunstancia.

2) Departamentos:

Se entiende como departamento a los órganos que siguen inmediatamente a la Dirección. El equipo auditor describirá brevemente las funciones de cada uno de ellos.

3) Relaciones Jerárquicas y funcionales entre órganos de la Organización:

El equipo auditor verificará si se cumplen las relaciones funcionales y Jerárquicas previstas por el organigrama, o por el contrario detectará, por ejemplo, si algún empleado tiene dos jefes.

Las de Jerarquía implican la correspondiente subordinación. Las funcionales por el contrario, indican relaciones no estrictamente subordinables.

4) Flujos de Información:

Además de las corrientes verticales intradepartamentales, la estructura organizativa cualquiera que sea, produce corrientes de información horizontales y oblicuas extradepartamentales.

Los flujos de información entre los grupos de una organización son necesarios para su eficiente gestión, siempre y cuando tales corrientes no distorsionen el propio organigrama.

En ocasiones, las organizaciones crean espontáneamente canales alternativos de información, sin los cuales las funciones no podrían ejercerse con eficacia; estos canales alternativos se producen porque hay pequeños o grandes fallos en la estructura y en el organigrama que los representa.

Otras veces, la aparición de flujos de información no previstos obedece a afinidades personales o simple comodidad. Estos flujos de información son indeseables y producen graves perturbaciones en la organización.

5) Número de Puestos de trabajo

El equipo auditor comprobará que los nombres de los Puesto de los Puestos de Trabajo de la organización corresponden a las funciones reales distintas.

Es frecuente que bajo nombres diferentes se realicen funciones idénticas, lo cual indica la existencia de funciones operativas redundantes.

Esta situación pone de manifiesto deficiencias estructurales; los auditores darán a conocer tal circunstancia y expresarán el número de puestos de trabajo verdaderamente diferentes.

6) Número de personas por Puesto de Trabajo

Es un parámetro que los auditores informáticos deben considerar. La inadecuación del personal determina que el número de personas que realizan las mismas funciones rara vez coincida con la estructura oficial de la organización.

Entorno Operacional

El equipo de auditoría informática debe poseer una adecuada referencia del entorno en el que va a desenvolverse.

Este conocimiento previo se logra determinando, fundamentalmente, los siguientes extremos:

a) Situación geográfica de los Sistemas:

Se determinará la ubicación geográfica de los distintos Centros de Proceso de Datos en la empresa. A continuación, se verificará la existencia de responsables en cada unos de ellos, así como el uso de los mismos estándares de trabajo.

b) Arquitectura y configuración de Hardware y Software:

Cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado. La configuración de los sistemas esta muy ligada a las políticas de seguridad lógica de las compañías.

Los auditores, en su estudio inicial, deben tener en su poder la distribución e interconexión de los equipos.

c) Inventario de Hardware y Software:

El auditor recabará información escrita, en donde figuren todos los elementos físicos y lógicos de la instalación. En cuanto a Hardware figurarán las CPUs, unidades de control local y remotas, periféricos de todo tipo, etc.

El inventario de software debe contener todos los productos lógicos del Sistema, desde el software básico hasta los programas de utilidad adquiridos o desarrollados internamente. Suele ser habitual clasificarlos en facturables y no facturables.

d) Comunicación y Redes de Comunicación:

En el estudio inicial los auditores dispondrán del número, situación y características principales de las líneas, así como de los accesos a la red pública de comunicaciones.

Igualmente, poseerán información de las Redes Locales de la Empresa.

Aplicaciones bases de datos y ficheros

El estudio inicial que han de realizar los auditores se cierra y culmina con una idea general de los procesos informáticos realizados en la empresa auditada. Para ello deberán conocer lo siguiente:

a. Volumen, antigüedad y complejidad de las Aplicaciones
b. Metodología del Diseño

   Se clasificará globalmente la existencia total o parcial de metodología en el desarrollo de las aplicaciones. Si se han utilizados varias a lo largo del tiempo se pondrá de manifiesto.
c. Documentación

   La existencia de una adecuada documentación de las aplicaciones proporciona beneficios tangibles e inmediatos muy importantes.

   La documentación de programas disminuye gravemente el mantenimiento de los mismos.
d. Cantidad y complejidad de Bases de Datos y Ficheros.

   El auditor recabará información de tamaño y características de las Bases de Datos, clasificándolas en relación y jerarquías. Hallará un promedio de número de accesos a ellas por hora o días. Esta operación se repetirá con los ficheros, así como la frecuencia de actualizaciones de los mismos.

Estos datos proporcionan una visión aceptable de las características de la carga informática.

Determinación de recursos de la auditoría Informática

Mediante los resultados del estudio inicial realizado se procede a determinar los recursos humanos y materiales que han de emplearse en la auditoría.

Recursos materiales

Es muy importante su determinación, por cuanto la mayoría de ellos son proporcionados por el cliente. Las herramientas software propias del equipo van a utilizarse igualmente en el sistema auditado, por lo que han de convenirse en lo posible las fechas y horas de uso entre el auditor y cliente.

Los recursos materiales del auditor son de dos tipos:

a. Recursos materiales Software

Programas propios de la auditoria: Son muy potentes y Flexibles. Habitualmente se añaden a las ejecuciones de los procesos del cliente para verificarlos.
Monitores: Se utilizan en función del grado de desarrollo observado en la actividad de Técnica de Sistemas del auditado y de la cantidad y calidad de los datos ya existentes.

b. Recursos materiales Hardware

Los recursos hardware que el auditor necesita son proporcionados por el cliente. Los procesos de control deben efectuarse necesariamente en las Computadoras del auditado.
Para lo cuál habrá de convenir, tiempo de maquina, espacio de disco, impresoras ocupadas, etc.

Recursos Humanos

La cantidad de recursos depende del volumen auditable. Las características y perfiles del personal seleccionado dependen de la materia auditable.

Es igualmente reseñable que la auditoría en general suele ser ejercida por profesionales universitarios y por otras personas de probada experiencia multidisciplinaria.

Perfiles Porfesionales de los auditores informáticos

Profesión	**Actividades y conocimientos deseables**
Informático Generalista	Con experiencia amplia en ramas distintas. Deseable que su labor se haya desarrollado en Explotación y en Desarrollo de Proyectos. Conocedor de Sistemas.
Experto en Desarrollo de Proyectos	Amplia experiencia como responsable de proyectos. Experto analista. Conocedor de las metodologías de Desarrollo más importantes.
Técnico de Sistemas	Experto en Sistemas Operativos y Software Básico. Conocedor de los productos equivalentes en el mercado. Amplios conocimientos de Explotación.
Experto en Bases de Datos y Administración de las mismas.	Con experiencia en el mantenimiento de Bases de Datos. Conocimiento de productos compatibles y equivalentes. Buenos conocimientos de explotación
Experto en Software de Comunicación	Alta especialización dentro de la técnica de sistemas. Conocimientos profundos de redes. Muy experto en Subsistemas de teleproceso.
Experto en Explotación y Gestión de CPD´S	Responsable de algún Centro de Cálculo. Amplia experiencia en Automatización de trabajos. Experto en relaciones humanas. Buenos conocimientos de los sistemas.

Técnico de Organización	Experto organizador y coordinador. Especialista en el análisis de flujos de información.
Técnico de evaluación de Costes	Economista con conocimiento de Informática. Gestión de costes.

Elaboración del Plan y de los programas de trabajo

Una vez asignados los recursos, el responsable de la auditoría y sus colaboradores establecen un plan de trabajo. Decidido éste, se procede a la programación del mismo.

El plan se elabora teniendo en cuenta, entre otros criterios, los siguientes:

a) Si la Revisión debe realizarse por áreas generales o áreas específicas. En el primer caso, la elaboración es más compleja y costosa.
b) Si la auditoría es global, de toda la Informática, o parcial. El volumen determina no solamente el número de auditores necesarios, sino las especialidades necesarias del personal.

- ✓ En el plan no se consideran calendarios, porque se manejan recursos genéricos y no específicos.
- ✓ En el Plan se establecen los recursos y esfuerzos globales que van a ser necesarios.
- ✓ En el Plan se establecen las prioridades de materias auditables, de acuerdo siempre con las prioridades del cliente.
- ✓ El Plan establece disponibilidad futura de los recursos durante la revisión.
- ✓ El Plan estructura las tareas a realizar por cada integrante del grupo.
- ✓ En el Plan se expresan todas las ayudas que el auditor ha de recibir del auditado.

Una vez elaborado el Plan, se procede a la Programación de actividades. Esta ha de ser lo suficientemente como para permitir modificaciones a lo largo del proyecto.