CAPITULO II

II. PLANEACIÓN DE LA AUDITORÍA INFORMÁTICA.

Introducción

Para hacer una adecuada planeación de la auditoría en informática, hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características del área dentro del organismo a auditar, sus sistemas, organización y equipo; con ello podremos determinar el número y características del personal de auditoría, las herramientas necesarias, el tiempo y costo, así como definir los alcances de la auditoría para, en caso necesario, poder elaborar el contrato de servicios.

Dentro de la auditoría en general, la planeación es uno de los pasos más importantes, ya que una inadecuada planeación repercutirá en una serie de problemas, que pueden provocar que no se cumpla con la auditoría o bien que no se efectúe con el profesionalismo que debe tener el desarrollo de cualquier auditoría.

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

Evaluación administrativa del área de procesos electrónicos.
Evaluación de los sistemas y procedimientos.
Evaluación de los equipos de cómputo.

Para lograr una adecuada planeación, 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 un, investigación preliminar y algunas entrevistas previas, y con base a 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

Este capitulo pretende destacar la importancia de una adecuada planeación de la auditoría informática, por lo que se incluye las lecturas, conceptos de auditoría informática y elementos que la integran de Erique Hernández y Hernández y la que nos presentan Eduardo Horacio Quinn en su obra " La auditoría informática dentro de las etapas de análisis de sistemas administrativos".

II.1 Concepto y elementos que la integran.

Fuente: Enrique Hernández. Auditoría en Informática: un Enfoque Metodológico. CECSA. 2001.

Planeación.

La función de auditoría en informática debe generar, como todas las áreas del negocio, un plan de proyectos que justifiquen su trabajo durante cierto periodo; de igual manera, cada uno de esos proyectos tendrá que contemplar un análisis costo/beneficio y la estructura de los mismos

con un enfoque metodológico con el fin de que esta función sea evaluada según su desempeño, con parámetros lo mas tangibles y mesurables posibles.

Cada proyecto de auditoría en informática respalda los objetivos y requerimientos de tres entidades del negocio en alto o bajo grado:

A) Alta dirección.

- Seguimiento a proyectos relacionados con tecnología informática.
- Verificación y aseguramiento del cumplimiento de políticas tecnología informática.
- Otros aspectos de interés para la alta dirección.

B) Auditoría.

- Apoyo en la definición, implantación y seguimiento de políticas, controles y procedimientos de auditoría financiera operativa, de créditos, fiscal, etc., relacionadas directa o indirectamente con la tecnología de informática (sistemas de información, equipos de cómputo, comunicaciones, etc.).
- Planes de capacitación en el uso y entendimiento de software de auditoría, herramientas de productividad (hojas electrónicas, procesadores de palabras, graficadores, diagramadores, etc.), base de datos (consulta de información, por ejemplo), equipos de cómputo (micros, terminales, portátiles, etc.); otros de interés para los auditores.
- Otros de interés para el desarrollo eficiente de los auditores cuando evalúen áreas del negocio que se apoyan en informática.

C) Informática.

- Apoyo en la definición, implantación y seguimiento de políticas, controles, procedimientos y estándares relativos a la organización y administración de informática, el proceso de planeación, la evaluación y adquisición de nueva tecnología, la evaluación y adquisición de servicios, el desarrollo e implantación de soluciones (EDI, CASE, base de datos, telecomunicaciones, sistemas estratégicos, multimedia, etc.) y otros de interés para informática.

Lo anterior permite concluir que es muy importante la comunicación permanente entre la función de auditoría en informática y la alta dirección, así como con las direcciones o gerencias de auditoria o informática.

Proceso de planeación de auditoría en informática.

Consta de la definición y planificación de proyectos. Abarca las actividades desarrolladas por el auditor en informática que tiene como objetivo principal elaborar y presentar un conjunto de proyectos inherentes a la función de auditoria en informática a la alta dirección, y que estarán orientados primordialmente al aseguramiento de la calidad y control de los diferentes elementos que se encuentran relacionados de manera directa o indirecta con los recursos de informática.

Proceso detallado de la planeación de la auditoría en informática.

Es importante aclara que este proceso de planeación depende en gran medida del diagnostico previo que haga el auditor en informática de la situación que prevalece en cada una de las áreas o servicios de la función de informática. También se deben considerar las necesidades o prioridades que tenga la alta dirección de auditar o evaluar un área especifica de informática.

El diagnóstico de la situación de informática previo a la planeación de ésta deberá ser breve y muy objetivo; de ninguna manera debe descuidarse el objetivo principal de esta tarea, que es determinar las áreas de mayor riesgo de la función de informática con base en criterios económicos, grado de satisfacción de la alta dirección, seguridad, calidad, productividad, vanguardia tecnológica, etcétera.

Actividades sugeridas para el proceso: elaboración, documentación, autorización y difusión formal del plan de auditaría en informática

Es importante identificar el nivel de riesgo de cada uno de los elementos que integran la función de informática en el negocio a través del diagnóstico de la situación actual en informática.

Las áreas que serán diagnosticadas pueden variar de acuerdo con el tamaño y estructura del negocio. Estos pueden ser empresas que dependan de un corporativo o Holding; asimismo, el giro de la empresa y el número de sucursales o subsidiarias originan en ocasiones que el auditor en informática tenga que evaluar productos y servicios de informática con un enfoque centralizado o descentralizado, según sea el caso.

Algunos de los siguientes servicios se mencionan de manera ilustrativa, esto es, no son limitativos o totalitarios para empresa alguna, ya que será el propio, perfil y sus características los que definan el alcance de la función de informática:

- Sistemas de información en operación
- Administración de hardware y software
- Desarrollo de sistemas de información
- Soporte a usuarios (capacitación, asesoría, entre otros)
- Administración de telecomunicaciones
- Investigación y desarrollo tecnológico
- Otros

El auditor deberá utilizar todos los parámetros de medición y evaluación posibles, sin caer en un análisis detallado, para detectar la problemática principal de cada área.

Si este proceso mostrara anomalías de considerable importancia en alguno de los elementos evaluados, se tomarán acciones inmediatas orientadas a minimizarlas o eliminarlas.

Determinar el nivel de riesgo que existe en cada una de las áreas de la función de informática: cada área, producto o servicio de informática es susceptible de evaluación y control para asegurar que se desarrolle de acuerdo con los estándares, políticas y procedimientos específicos que le han sido asignados según su función.

Consideraciones que se deben tomar en cuenta al diagnosticar la situación actual para la obtención de la matriz de riesgos: el auditor en informática ha de conocer de manera aceptable los aspectos relativos a auditoría e informática que deben tener cada una de las áreas de informática. Lo anterior es un requisito indispensable, ya que tendrá que basarse en su experiencia y dominio de la auditoría en informática para efectuar un diagnóstico objetivo y contundente; además, se apoyará en la visión de los principales usuarios del negocio y del responsable de informática.

Diagnóstico de la situación actual de los sistemas información en operación.

Dado que los sistemas de información en operación son un elemento primordial dentro del funcionamiento formal de cualquier negocio (aquí se manejan los datos de las áreas financieras, productivas y administrativas para la toma de decisiones), conviene recalcar las consideraciones y criterios más importantes que ha de tomar en cuenta el auditor en informática.

El diagnóstico general de esta área se puede llevar a cabo de la siguiente manera:

a) Se obtiene una lista de los principales sistemas de información y de los usuarios principales de cada uno (se establece cuáles fueron desarrollados por la empresa y cuáles comprados a terceros, para saber cuál será la fuente principal de estudio si alguno requiriese mayor evaluación).
b) Se toman como base los comentarios positivos o negativos de los principales usuarios de cada sistema de información que se encuentre en operación a fin de establecer los volúmenes de transacciones promedio.
c) Se registran las fallas o regularidades más comunes del sistema o equipo de cómputo, así como las prioridades de operación.
d) Se recaban los informes de desempeño hechos con anterioridad a los usuarios principales, a los analistas de sistemas y al personal de producción (oportunidad, calidad, confiabilidad).
e) Se anota la fecha de liberación de los sistemas y la última vez que se auditaron. Esto permite valorar la posibilidad y grado de riesgo.
f) Se revisa la configuración del equipo donde se encuentre instalado (en una microcomputadora aislada, en una red local, en una mini computadora, etcétera).
g) Se estudia su integración a otros sistemas de información.
h) Se valoran otros de interés propio del auditor en informática para la empresa que evalúe en ese momento.

Debilidades que pueden motivar la auditoría de un sistema información

Primero: que el sistema no haya sido liberado formalmente, lo que puede traer como consecuencia el desconocimiento real por parte de los usuarios y del personal de auditoría de las debilidades y fortalezas del mismo. .

Segundo: que el sistema no haya sido auditado. Esto sugiere la alternativa de auditarlo de inmediato, sobre todo si es un sistema básico para la alta dirección (un sistema de cheques en un banco, un sistema de ventas en una empresa comercial o un sistema de manufactura en una empresa de giro industrial); en caso de no ser un sistema fundamental, se programa su revisión en los proyectos intermedios o finales de la auditoría.

Clasificación del nivel de riesgo que representa el uso de hardware y software en la organización

Lo que se desea determinar en este punto es que los sistemas de información computarizados y los datos sean procesados en un ambiente tecnológico confiable, seguro y eficiente. Aquí se pueden auditar los equipos o paquetes de software que dan soporte. a los sistemas primordiales del negocio; o bien se audita de manera periódica el mantenimiento y uso que se hace de la tecnología dentro del equipo y software (herramientas de productividad) en la organización.

La capacidad de los equipos, cantidad de unidades (discos, cintas, terminales, etc.), los tipos (microcomputadoras, redes, mini computadoras, mainframes), distribución física y reportes de desempeño de los mismos, son datos que pueden ayudar a determinar la secuencia y grado de intensidad con que se auditará el hardware.

El uso y propósito de los paquetes de software, la existencia de procedimientos y políticas en la evaluación y adquisición del mismo, así como la estandarización de paquetes, apoyan al auditor en la programación de los proyectos de auditoría.

Evaluación del nivel de riesgo que representa el uso inadecuado de los productos. y servicios por el personal de informática y usuarios dentro de la organización.

Esto se refiere básicamente al grado de conocimientos que se tiene sobre el uso de los servicios, software y equipos.

La información que puede ser de apoyo en este punto para el auditor son los organigramas, la descripción de puestos, procedimientos y políticas que se relacionen con los productos y servicios de informática (si no existen, es probable que se estén utilizando de manera limitada las bondades de la informática; asimismo, el conocimiento de los sistemas y equipos puede no ser el más adecuado, lo que motiva al auditor a profundizar posteriormente en este punto. La presencia de catálogos de productos y servicios (hardware, software, proveedores, precios, tipos de asesorías y sus costos por hora), manuales para usuarios, manuales de sistemas, manuales de operación y la distribución y uso de los mismos, así como bitácoras de cursos de capacitación, es de gran relevancia para establecer el grado de confianza que existe por parte del personal involucrado en el manejo de los sistemas, paquetes de software y equipo.

Otros aspectos: telecomunicaciones, EDI (intercambio electrónico de datos), automatización de procesos, CASE

Estos se deben evaluar con base en estándares comúnmente aceptados a nivel internacional y según la proyección de uso que piensa darle el negocio a corto, mediano y largo plazo. Además, hay que considerar los comentarios o asesorías de personal especializado en esta área ya sea gente externa o de la función de informática de la empresa en evaluación.

Clasificación de los riesgos según criterios establecidos por la función de auditoría en informática.

- Cumplimiento de estándares comúnmente aceptados a nivel nacional e internacional.
- Cumplimiento formal de políticas y procedimientos. Grado de satisfacción de la alta dirección y del personal usuario.
- Prioridades de la alta dirección.

- Prioridades de la función de informática.
- Prioridades de la función de auditoría en informática.
- Otros de interés específico del auditor en informática en el momento de llevar a cabo la evaluación.

Elaboración de una matriz de riesgos que muestre las áreas de la función de informática susceptibles de una revisión por parte de auditoría en el siguiente periodo.

Dicha matriz muestra resultados en orden descendente. Esto implica que el área con el valor más alto es la entidad con mayor riesgo; por lo tanto, será la primera auditada y así sucesivamente, hasta conocer las áreas de menor riesgo.

Elaboración de un plan consolidado de proyectos.

Este plan ha de contar al menos con la siguiente información:

- Fechas de inicio y terminación de cada auditoría
- Etapas de cada auditoría
- Tareas principales de cada etapa
- Equipo de trabajo (auditor [es], representante de informática y representante de las áreas usuarias)
- Requerimientos (recursos, apoyo de la dirección, capacitación, material de auditoria en informática, entre otros)

Revisión de la matriz de riesgos y el pronóstico de proyectos de auditoría en informática con la gerencia o dirección a la que reporta directamente la función de auditoría en informática.

Se ejecutará de manera oportuna y formal con el fin de que se dé el visto bueno o se lleven a cabo las adaptaciones o mejoras que se consideren pertinentes, antes de presentarlo a la alta dirección de la organización.

El plan se elabora cubriendo al menos los siguientes aspectos:

- Área por auditar
- Prioridad
- Fechas de inicio y término
- Involucrados
- Responsables
- Fechas de revisión formales e informales
- Otros de interés particular del auditor en informática en el momento de efectuar esta tarea

Presentación del plan de proyectos de la función de auditoría en informática a la alta dirección.

Lo anterior tiene como finalidad los siguientes propósitos:

- Conocer los proyectos de auditoría en informática antes de que inicie el año Fiscal.

- Verificar que las áreas que considere fundamentales para el buen funcionamiento del negocio hayan sido contempladas en el plan de auditoría en informática y en la matriz de riesgos para su debida reorganización antes de que sea autorizado.
- Que la alta dirección se comprometa de manera permanente a apoyar a los auditores en el desarrollo de cada uno de los proyectos.
- Obtener la aprobación formal de la planeación de auditoria en informática por parte de la alta dirección.

Realización de cada uno de los proyectos de acuerdo con el plan de auditoría en informática.

Este punto entraña la ejecución de actividades de seguimiento y revisión formal de cada proyecto.

Integración y formalización de equipos de trabajo

Los equipos estarán integrados por:

a) Gerente(s) de las áreas usuarias que se evaluarán
b) Gerente de la función de informática
e) Líder del proyecto de la función de auditoría en informática

Aprobación formal de la alta dirección del informe final de la auditoría en informática realizada.

Por último, se dará seguimiento oportuno y formal a cada una de las recomendaciones contempladas en dicho informe; se aplicarán políticas y controles estandarizados a nivel internacional, y la implantación de este proceso de planeación de auditoría en informática será permanente.

Resumen.

Hay que considerar el proceso de planeación en cualquier organización como el pilar de todas las actividades que se ejecuten en ella. La desestimación o informalidad en los planes ha provocado importantes decepciones en todos los que pregonan que planear es una pérdida de tiempo y un recipiente de buenos deseos.

En todas las organizaciones los proyectos al vapor causan retrasos en la entrega de resultados, costos superiores a los estimados al inicio y calidad cuestionable en los entregables.

Un problema común en proyectos de mediano o largo plazo es la alta rotación de los encargados. Al no tener definidos su función, responsabilidad, tiempos ni resultados, este personal es el candidato perfecto para convertirse en culpable cuando aumentan los costos del proyecto, los tiempos de soluciones se alargan o simplemente cuando los usuarios olvidan los requerimientos originales.

La planeación se entiende como un proceso formal donde al menos se encuentran los siguientes elementos:

- Etapas.

- Tareas.
- Actividades.
- Costos/beneficios.
- Resultados esperados por actividad, tarea y etapa.
- Responsables de cada actividad o tarea.
- Involucrados o participantes.
- Revisiones formales e informales.
- Técnicas para ejecutar actividades.
- Herramientas para realizar cada una de las actividades del proyecto.

Se puede sobrevivir trabajando en base a las crisis de la empresa y no de acuerdo con estrategias y objetivos de la dirección; es factible seguir dando resultados temporales de "úsese y tírese" en vez de brindar al negocio resultados duraderos y congruentes con sus necesidades; asimismo, es posible trabajar al día. Sin embargo, también es importante planear, estimar y esperar antes de actuar. Hay muchos beneficios de planeación, pero el más importante es poder asegurar con alto grado de credibilidad a ejecutivos y empresarios cuánto invertirán y cuánto obtendrán de beneficio por cada proyecto.

No hay que subestimar lo que tantos hombres de negocio prominentes pregonan con el ejemplo: el que planea sabe a dónde va y cuándo llegará; dejemos de depender de la buena suerte.

Se puede dejar el proceso de la auditoría en informática como un proceso informal, pero en cada uno de los proyectos es pronosticable la presencia de problemas o irregularidades imprevistas. Si no se planea el trabajo es lógico pensar que tampoco se planean las anomalías y decepciones que el desarrollo de dicho trabajo acarreará.

No se vive de buenos deseos sino de metas claras, medibles y factibles. El auditor de informática y la función o área que la administre deben considerar la importancia y relevancia que tiene, para su éxito como parte del negocio, contar con un plan formal que contemple los proyectos de auditoría así como los diferentes planes relacionados con la informática.

No hay que perder de vista la relación directa entre el grupo responsable de la función de auditoría en informática y los procesos de planeación del negocio, la auditoría tradicional y la función o área de informática.

Se entiende por planeación del negocio la actividad que contempla el planteamiento, elaboración y formalización de los proyectos de cada área o dirección de una organización, encaminados a satisfacer las estrategias y objetivos de los accionistas, dueños o responsables directos del negocio a corto, mediano y largo plazo.

Para fines prácticos, se entiende por planeación de auditoria tradicional todas las actividades de los auditores tradicionales orientadas al planteamiento, .elaboración y formalización de proyectos relativos a la revisión y dictamen de los aspectos administrativos, operativos, financieros, etc., de una organización de acuerdo con prioridades y necesidades propias de cada negocio.

Se entiende por planeación de informática el proceso que llevan a cabo los responsables de esa área con el fin de plantear, elaborar y formalizar el conjunto de proyectos de corto, mediano y largo plazo que darán soporte estratégico, táctico y operativo al negocio.

Por último, se define como planeación de auditoria en informática el proceso que consiste en plantear, elaborar y formalizar una serie de proyectos de corto, mediano y largo plazo orientados a la evaluación y revisión oportuna de todos los componentes inherentes a la informática, según prioridades propias de la empresa y con una orientación de apoyo directa a los planes mencionados.

Los requisitos mínimos para que la planeación de auditoría en informática sea formal, permanente y exitosa son:

Involucramiento directo del auditor en informática en el proceso de planeación estratégica del negocio para:
Entender requerimientos, tiempos y prioridades de cada proyecto del negocio a fin de poder evaluar, revisar o asesorar a las áreas involucradas

b) Compromiso del responsable de auditoría en informática con cada proyecto del plan de informática para implementar un esquema de control y seguridad preventivo y completo.
c) Participación del auditor en informática en el proceso de planeación de auditoría tradicional para hacer en controles y medidas correctivas.

Los beneficios surgidos de la participación entrañan la supresión de:

- Riesgos de no planear la auditoría.
- Responsables de tareas inadecuados.
- Falta de compromiso de los involucrados en el proyecto.
- Aparición de costos imprevistos. Retrasos en la obtención de beneficios.
- Mala calidad en los resultados.
- Rotación del personal clave.
- Inadecuada segregación de tareas y actividades.
- No alineación con planes de negocio, auditoría o informática.
- Errores en la disposición de las cargas de trabajo.
- Tensión y falta de motivación en los participantes.
- Uso impropio o no utilización de técnicas y herramientas apropiadas.
- Falta de una estructura sólida para los proyectos (etapas, secuencias, tiempos)

II.2 Metodología de trabajo en la auditoría informática.

Fuente: (http://www.monografias.com/trabajos5/audi/aUdi2.shtml#traba) Horacio Quinn Eduardo.

Una vez definida la Auditoría Informática, sus fines y utilidades, así como expuestas sus clases y tipos, procedemos a describir el método de trabajo que el equipo auditor ha de seguir, desde la contratación por parte del cliente o la orden de la Dirección (según que la auditoría sea externa o interna), hasta la confección y entrega por escrito del Informe final. Toda la función auditora se comprendía en la entrega del mencionado Informe a quien lo solicitó.

El método de trabajo auditor pasa por las siguientes fases, a saber:

1. Alcance y Objetivos de la Auditoría Informática.
2. Estudio inicial del entorno auditable.

3. Determinación de los Recursos necesarios para efectuar la Auditoría.
4. Elaboración del Plan y de los Programas de Trabajo.
5. Actividades propiamente dichas de la Auditoría (Análisis, entrevistas, etc.).
6. Confección y Redacción del Informe Final.
7. Redacción de la "Carta de Introducción" o "Carta de Presentación" del Informe Final.

Definición de alcances y objetivos

Como su propio nombre indica, el alcance de la Auditoría expresa los límites de la misma. Debe existir un acuerdo muy preciso entre autoridades y clientes sobre las funciones, las materias y las organizaciones auditadas.

Así, por ejemplo, en la auditoría de una Explotación deberá fijarse previamente si ha de incluirse o no la función de Soporte Técnico, dependiendo de su ubicación en el organigrama.

Del mismo modo, se fijaría de antemano si ha de auditarse la percepción de los usuarios, o solamente la eficiencia interna de Explotación, etc.

Especial importancia tendría la determinación del ámbito de la auditoría cuando se incluyan áreas no informáticas de la empresa u Oficinas de Servicios Informáticos ajenos a la misma, Soporte de la firma constructora, etc.

A estos efectos, resulta muy beneficioso para ambas partes expresar las excepciones de alcance de la auditoría, es decir, manifestar por escrito cuáles materias o funciones no van a ser auditadas.

Tanto el alcance de la auditoría como las excepciones del mismo, han de figurarse al comienzo del documento final.

Auditoría ha de conocer con la mayor precisión los objetivos que sus acciones pretenden. Debe comprender con exactitud los deseos y pretensiones, del cliente, de forma que los objetivos perseguidos sean susceptibles de ser cumplidos.

Bien determinados los objetivos, en lo sucesivo llamados objetivos específicos, el auditor tendrá siempre presente que éstos se añadirán a los dos objetivos generales y comunes a toda auditoria informática: La Operatividad de los Sistemas y los Controles de Gestión Informática.

Por lo demás, los objetivos más habituales pueden ser: Evaluación de funcionamiento de áreas informáticas, aumentos de Seguridad y Fiabilidad, Conectividad, Compatibilidad, aumento de Calidad, Costos y Plazos, etc.

Dentro de este apartado de Alcance y Objetivos debe incluirse la fijación de los interlocutores del equipo auditor.

El concepto de interlocución comprende la determinación previa de las personas que tienen poder de decisión y de validación dentro de la empresa.

Igualmente, los auditores conocerán con exactitud la persona o personas destinatarias del Informe.

Estudio inicial

La metodología de trabajo del equipo auditor comporta un estudio inicial de la situación general, aun en el caso de que la auditoria a realizar sea solamente sectorial.

Para realizar dicho estudio han de examinarse las funciones y actividades generales de la informática siguientes, a saber:

2.a) Organización.
2.b) Entorno Operacional.
2.c) Aplicaciones Informáticas, Base de Datos y Archivos.

2a) Organización.

Para el equipo auditor, el conocimiento de quién ordena, quién diseña y quién ejecuta es fundamental. No podrá realizar su misión sin conocer con bastante aproximación la estructura organizativa de la Informática sujeta a auditoria. Al menos, se deberán fijar los conceptos que siguen:

Organigrama: El organigrama expresa inicialmente la estructura oficial de la organización a auditar. El propio equipo auditor dibujará el organigrama oficial con todo detalle, sin omitir las casillas que realicen funciones auxiliares o complementarias no informáticas. Si el número de niveles es elevado, se fraccionará. Los textos de los recuadros del organigrama deberán ser auto explicativos.

Obsérvese que se ha hecho referencia al organigrama oficial. El auditor podrá comprobar con facilidad la identidad que debe existir entre lo oficial y lo real.

Si se descubriera a través de los flujos de información y de las relaciones funcionales y jerárquicas, que existe un organigrama fáctico diferente al oficial, se pondrá de manifiesto tal circunstancia y las derivadas de ella.

Departamentos: Se entienden ahora como departamentos los órganos qu siguen inmediatamente tras la Dirección. El equipo auditor describirá breve y claramente las funciones más importantes de los recuadros del organigrama que constituyen cada uno de ellos, y los que dependen directamente de éste.

Relaciones jerárquicas y funcionales entre órganos de la Organización:

Además del organigrama y de las funciones principales de cada Departamento, el equipo auditor verificará si se cumplen las relaciones funcionales y jerárquicas previstas, o por el contrario, detectará, por ejemplo, si algún empleado tiene dos jefes.

Las relaciones de jerarquía implican la correspondiente subordinación. Las funcionales, por el contrario, indican relaciones de naturaleza complementaria y no estrictamente subordinales. Estas relaciones deben estar bien definidas por el nivel inmediato superior, el cual nivel deberá informar a sus propios grupos horizontales de la existencia de tales relaciones, así como de cualquier variación en ellas.

En principio, las relaciones no jerárquicas contribuyen a proporcionar mayor flexibilidad a las estructuras. Sin embargo, y también como principio, deberán restringirse al máximo las "dependencias funcionales".

Como veremos enseguida al referimos a "flujos de información", las dependencias funcionales, significan imprecisiones organizativas de diversa importancia y género, aceptables tan sólo en circunstancias excepcionales, y siempre que esté prevista su desaparición a plazo fijo.

Flujos de información:

Además de las corrientes verticales intradepartamentales y de las directrices de la Dirección, 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 y aun imprescindibles 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 de información alternativos se producen porque hay pequeños o grandes fallos en la estructura y en el organigrama que los representa.

Se ha dicho con verdad que no existe el organigrama perfecto, por lo que puede resultar inevitable la existencia de flujos de información no deseados, pero esta realidad no debe excusar la proliferación de dichos flujos.

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.

Particular importancia tienen los llamados "puenteos" en el vocabulario empresarial, sobre todo cuando está involucrada la propia Dirección.

Número de puestos de trabajo:

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

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

Esta situación pone de manifiesto deficiencias estructurales; los auditores pondrán de manifiesto tal circunstancia y expresarán el número de Puestos de Trabajo verdaderamente diferentes.

Piénsese que difícilmente existen más de 5 o 6 Puestos operativos distintos por cada rama informática, mientras que en muchas organizaciones aparecen hasta 10 o 12 denominaciones por rama.

Número de personas por puesto de trabajo:

Es un parámetro que los auditores informáticos deben considerar. La inadecuación del personal o la falta de plantilla en algunas secciones y la sobran en otras, determina que el número de personas que realizan las mismas funciones rara vez coincida con la estructura oficial de la organización.

Los auditores deberán exponer el número de empleados reales de cada sección auditada. De este modo, se ponen de manifiesto una distribución ineficiente de recursos o la necesidad de un reorganización para modificar la estructura oficial.

2b) Entorno operacional

El equipo de auditoria informático debe poseer una adecuada referencia del entorno en el que ha de desenvolverse.

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

1. Situación geográfica de los sistemas

Se determinará la ubicación geográfica de los Centros de Proceso de Datos distintos de la empresa. De acuerdo con dicha ubicación, se verificará la existencia de responsables por cada uno de ellos, así como el uso de los mismos estándares de trabajo.

2. Arquitectura y configuración de hardware y software

Sobre todo cuando existen varios Centro de Proceso de Datos, es fundamental la configuración elegida para cada uno de ellos en tanto deben constituir un Sistema compatible e intercomunicado. La configuración de los Sistemas está muy ligada a las políticas de Seguridad Lógica Informática de las Compañías.

Los Planes de Contingencia Total que cada empresa suele buscar con fruición, rara vez tienen materialización efectiva cuando, desgraciadamente, llega la ocasión.

Las experiencias de los últimos años indican que cuando un Centro de Proceso de Datos queda inoperativo, su sustitución por otro no es una operación inmediata. Se exceptúan los servicios estratégicos principales de los Estados.

Deben tenerse en cuenta los elevados costos que para una empresa supone disponer de un Centro Informático Alternativo, que basa su utilidad potencial en la ejecución de cargas reducidas mientras llega el desastre.

En otro orden, la organización informática necesita una configuración muy flexible, facilitada en la actualidad por la versatilidad de los Sistemas.

Sobre todo, los auditores, en su estudio inicial, deben tener en su poder la distribución e interconexión de canales y discos.

3. Inventario de hardware y software

El equipo auditor recabará información escrita de la empresa, en donde figuren todos los elementos físicos y lógicos de la instalación. En cuanto a Hardware, figurarán las CPU, procesadores intermedios, unidades de control locales y remotas, periféricos de todo tipo, terminales, ordenadores personales, etc. Es conveniente que en el inventario físico figuren igualmente las líneas disponibles con los datos fundamentales de cada una de ellas.

El inventario 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.

4. Comunicaciones y redes de comunicaciones

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.

No existen inconvenientes para que toda la información de líneas y Redes figure en el mismo Inventario del punto anterior. Por el contrario, debe estimularse la construcción de un Inventario Hardware y Software único.

En todo caso, la ausencia o desactualización de los datos anteriores suponen una debilidad importante que el auditor deberá recoger con severidad.

2c) Aplicaciones bases de datos y archivos.

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.

El entorno auditable se pone de manifiesto principalmente por medio de las siguientes características:

1. Volumen, antigüedad y complejidad de las aplicaciones

El equipo de auditoría informática hallará un promedio de los conceptos epigrafiados. Se pondrá especial énfasis en la periodicidad de ejecuciones de la carga.

2. Metodología del diseño

Se calificará globalmente la existencia total o parcial de metodologías en el desarrollo de las Aplicaciones. Si se han utilizado varias a lo largo del tiempo se pondrá de manifiesto tal circunstancia.

Aún se pondrá más de relieve el hecho de que se hayan desarrollado simultáneamente varias Aplicaciones con metodologías diferentes. Esta simulación comporta un evidente desaprovechamiento de recursos.

3. Documentación

Desde el punto de vista práctico, la existencia de una adecuada documentación de las Aplicaciones proporciona beneficios tangibles e inmediatos muy importantes.

Una documentación correcta es aún más importante que la homogeneidad metodología. En efecto, la documentación de programas disminuye grandemente el mantenimiento de los mismos.

La actividad de mantenimiento de Aplicaciones es en la actualidad uno de los problemas más importantes, y representa a veces hasta un 70% del total de los recursos de Desarrollo.

4. Cantidad y complejidad de bases de datos y archivos

El auditor recabará información de tamaño y características de las Bases de Datos, clasificándolas en relacionales y jerárquicas. Hallará un promedio de número de accesos a ellas

por horas o días. Esta operación se repetirá con los archivos, 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, sobre el cual gravita el aumento de carga y las interferencias sobre el desarrollo normal de su trabajo.

Las herramientas software propias del equipo auditor van a utilizarse igualmente en el Sistema auditado, por lo que han de convenirse en lo posible las fechas y horas de uso entre auditor y cliente. .

Los recursos materiales del auditor son de dos tipos:

a) Recursos materiales Software

Programas propios de la Auditoría. Se indicó en su momento que son muy potentes y flexibles. Habitualmente, se añaden a las ejecuciones de los procesos del cliente pura verificar los recorridos
de aquellos. .

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. Es una máxima de la auditoría informática que los procesos de control deben efectuarse necesariamente en los Ordenadores del auditado.

Por tanto, habrán de convenirse, fundamentalmente, tiempo de máquina y oportunidad de fecha, hora y duración de las sesiones de medida.

Finalmente, se convendrán: Cantidad de pantallas, espacio en disco, montajes de cintas, impresoras ocupadas y líneas de comunicaciones si van a utilizarse en exclusiva.
El auditor deberá calcular con la mayor precisión posible los incrementos de carga por él generados.

- Recursos Humanos

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

Suponiendo una auditoría general, es habitual la presencia de personas no informáticas pero expertas en temas de organización y análisis de costos.

Debe resaltarse que el equipo auditor no es solamente la agregación de expertos. Por el contrario, es necesaria la cohesión entre sus integrantes. Esta suele ser proporcionada por un informático generalista.

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

Sin ánimo exhaustivo, y de modo sinóptico en el siguiente cuadro, se han relacionado los perfiles profesionales de lo que podría ser un equipo auditor informático para abordar una Revisión General de la Informática de una Organización.

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 Proyecto. 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 mantenimiento de BD. Conocimiento de Productos compatibles y equivalentes. buenos conocimientos de Explotación*
Experto en Software de Comunicaciones	*Alta especialización dentro de la Técnica de Sistemas. Conocimientos profundos de Redes. Muy experto en subsistemas de Teleproceso.*
Experto en Explotación y Gestión de Centro de proceso de Datos	*Responsable de algún Centro de Cómputo. Amplia experiencia en Automatización de Trabajos. Experto en relaciones humanas. Buenos conocimientos de los Sistemas.*
Técnicos de la Organización	*Experto organizador y coordinador. Especialista en el análisis de flujos de información.*
Técnico de evaluación de Costos	*Economista con conocimientos de Informática. Gestión de costos*

Elaboración del plan y de los programas de trabajo

Una vez asignadas los recursos, el responsable de la auditoría y sus colaboradores establece un plan de trabajo. Decidido éste, se procede a la programación del mismo por parte del responsable de cada sector o de cada especialista, que los reportan el mencionando responsable de la auditoría para la aprobación final.

El Plan de Auditoría se elabora teniendo en cuenta, entre otros criterios, los siguientes:

a) Si la Revisión ha de realizarse por áreas generales o áreas específicas. En el primer caso, la elaboración final es más compleja y costosa, lo cual redonda en una superior calidad

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 de 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.
- El Plan establece las prioridades de materias auditables, de acuerdo siempre con las prioridades del cliente.
- El Plan establece la disponibilidad futura del personal y de los demás recursos durante la duración de la Revisión.
- El Plan estructura las tareas a realizar por cada integrante del equipo
- 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 flexible como para permitir modificaciones a lo largo del proyecto. Los programas de trabajo son las cuantificaciones del plan.

En ellos se asignan los recursos humanos y materiales concretos para cada sector del plan. En el programa de trabajo se establece el calendario real de actividades a realizar. La auditoría informática necesita de planificación y programación detallada. Posee la naturaleza de un verdadero Proyecto, y por ello le son aplicables las reglas generales de los mismos.

Actividades de la auditoría informática

En este Apartado vamos a hacer un repaso de las acciones auditoras, las técnicas concretas que se utilizan y las herramientas de las que se ayudan.

Auditoría por temas generales o por áreas específicas

La auditoria informática general se realiza por áreas generales o por áreas específicas. El método de trabajo es diferente: Si se examina por grandes temas, por ejemplo desde el punto de vista de la seguridad, resulta evidente la mayor calidad y el empleo de más tiempo total y mayores recursos. Piénsese en que revisada la seguridad, pasaríamos luego a la identificación de la dirección con el modelo informático de la empresa en todas sus áreas, luego a la percepción de los usuarios finales respecto a la explotación, el desarrollo, etc., y finalmente al funcionamiento interno de la informática como centro de trabajo.

Por el contrario, cuando la auditoría se realiza por áreas específicas, se abarcan de una vez todas las peculiaridades que afectan a las mismas, de forma que el resultado se obtiene más rápidamente y con menor calidad.

Así, cuando se aborda la auditoría de desarrollo de aplicaciones, se tienen en cuenta todos los factores que le afectan, como la seguridad, la percepción del usuario, etc. Una vez finalizada la revisión del área de desarrollo, no es preciso volver sobre el mismo concepto, sino comenzar el análisis de otra rama específica, explotación por ejemplo.

Técnicas de trabajo

Basta con enumerarlas, ya las hemos conocido a través de los Capítulos anteriores:

- Análisis de la información recabada del auditado.
- Análisis de la información propia.
- Cruzamiento de las informaciones anteriores.
- Entrevistas
- Simulación
- Muestreos

Herramientas.

Procedamos igualmente a su enumeración:

- Cuestionario general inicial.
- Cuestionario-Checklist.
- Estándares.
- Monitores.
- Simuladores (Generadores de Datos).
- Paquetes de Auditoría (Generadores de Programas).
- Matrices de Riesgo.

Es conveniente ahondar en este último concepto. Las matrices de riesgo tienen la doble particularidad de que deben ser incorporadas al Informe Final y de que pueden considerarse también como elementos decisorios para la realización de una Auditoría Informática de Seguridad.

Bibliografía Capitulo II

Hernández, Enrique. 2001. "Auditoría Informática: Un Enfoque Metodológico". CECSA.

Horacio Quinn Eduardo. 08/11/2000. "La Auditoria informática dentro de las etapas de análisis de sistemas administrativos"
http://www.monografias.com/trabajos5/audi/aUdi2.shtml#traba