UNIDAD V. NORMATIVIDAD Y AUDITORIA EN LA FUNCIÓN INFORMÁTICA

5.1 DEFINICIÓN DE AUDITORIA INFORMÁTICA

Es una función que ha sido desarrollada para asegurar la salvaguarda de los activos de los sistemas de computadoras, mantener la integridad de los datos y lograr los objetivos de la organización en forma eficaz y eficiente (Ron Weber)

Es la revisión y evaluación de los controles, sistemas y procedimientos de la informática; de los equipos de cómputo, su utilización, eficiencia y seguridad; de la organización que participa en el procesamiento de la información, a fin de que por medio de señalamientos logre una utilización más eficiente (José Antonio Echenique)

Es el proceso que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas. Permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes (wikipedia.com)

5.2 OBJETIVOS

- El control de la función informática
- El análisis de la eficiencia de los Sistemas Informáticos
- La verificación del cumplimiento de la Normativa en este ámbito
- La revisión de la eficaz gestión de los recursos informáticos.

La auditoría informática sirve para mejorar ciertas características en la empresa como:

- Desempeño
- Fiabilidad
- Eficacia
- Rentabilidad
- Seguridad
- Privacidad

5.3 TIPOS

- **Auditoría de la dirección informática:** la contratación de bienes y servicios, documentación de procesos, políticas y normas, elección de modelos, etc.

- **Auditoría de desarrollo de proyectos o aplicaciones:** conocido también como Análisis y Programación de Sistemas y Aplicaciones. Engloba muchas áreas, las más importantes son:
  - Prerequisitos del Usuario (único o plural) y del entorno
  - Análisis funcional
  - Diseño
  - Desarrollo (Preprogramacion y Programación)
  - Pruebas
  - Entrega a Explotación y alta para el Proceso.
- **Auditoría de sistemas:** encierra el uso, funcionamiento y desempeño tanto del sw de sistemas (sistemas operativos, utilerías, controladores, etc.) como del sw de aplicación (procesadores de texto, gráficos, matemáticos, de productividad, etc.).
- **Auditoría de los datos**: clasificación de los datos, estudio de las aplicaciones y análisis de los flujogramas.
- **Auditoría de las bases de datos**: controles de acceso, de actualización, de integridad y calidad de los datos.
- **Auditoría de la seguridad**: referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.
- **Auditoría de la seguridad física**: referido a la ubicación de la organización, evitando ubicaciones de riesgo, y en algunos casos no revelando la situación física de esta. También está referida a las protecciones externas (arcos de seguridad, CCTV, vigilantes, etc.) y protecciones del entorno.
- **Auditoría de la seguridad lógica**: comprende los métodos de autenticación de los sistemas de información.
- **Auditoría de las comunicaciones y redes**. se refiere a la auditoria de los procesos de autenticación en los sistemas de comunicación.
- **Auditoría de la seguridad en producción**: frente a errores, accidentes y fraudes.

5.4 AUDITORÍA INTERNA VS AUDITORÍA 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 auditorías 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 auditorías, 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 auditorías 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 auditoría interna puede y debe en ocasiones contratar servicios de auditoría 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 auditorías informáticas externas decretadas por la misma empresa.
- Aunque la auditoría interna sea independiente del Departamento de Sistemas, sigue siendo la misma empresa, por lo tanto, es necesario que se le realicen auditorías externas como para tener una visión desde afuera de la empresa.

La auditoría 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.

Importancia

5.5 SÍNTOMAS DE NECESIDAD DE UNA AUDITORÍA INFORMÁTICA

Las empresas acuden a las auditorías externas cuando existen síntomas bien perceptibles de debilidad. Estos síntomas pueden agruparse en clases:

- **Síntomas de descoordinacion y desorganización:**
  a) No coinciden los objetivos de la función informática de la compañía y de la propia compañía.
  b) Los estándares de productividad se desvían sensiblemente de los promedios conseguidos habitualmente.

- **Síntomas de mala imagen e insatisfacción de los usuarios:**
  a) No se atienden las peticiones de cambios de los usuarios. Ejemplos: cambios de software en los terminales de usuario, refrescamiento de paneles, variación de los ficheros que deben ponerse diariamente a su disposición, etc.
  b) No se reparan las averías de hardware ni se resuelven incidencias en plazos razonables. El usuario percibe que está abandonado y desatendido permanentemente.
  c) No se cumplen en todos los casos los plazos de entrega de resultados periódicos. Pequeñas desviaciones pueden causar importantes desajustes en la actividad del usuario, en especial en los resultados de aplicaciones críticas y sensibles.

- **Síntomas de debilidades económico-financiero:**
  a) Incremento desmesurado de costos.
  b) Necesidad de justificación de Inversiones Informáticas (la empresa no está absolutamente convencida de tal necesidad y decide contrastar opiniones).
  c) Desviaciones presupuestarias significativas.
  d) Costos y plazos de nuevos proyectos (deben auditarse simultáneamente a Desarrollo de Proyectos y al órgano que realizó la petición).

- **Síntomas de Inseguridad: Evaluación de nivel de riesgos**
  a) Seguridad Lógica
  b) Seguridad Física
  c) Confidencialidad: los datos son propiedad inicialmente de la organización que los genera. Los datos de personal son especialmente confidenciales.
  d) Continuidad del Servicio: es un concepto aún más importante que la seguridad. Establece las estrategias de continuidad entre fallos mediante planes de contingencia totales y locales.
  e) Centro de Proceso de Datos fuera de control: si tal situación llegara a percibirse, sería prácticamente inútil la auditoría. Esa es la razón por la cual, en este caso, el síntoma debe ser sustituido por el mínimo indicio.

5.6 HERRAMIENTAS Y TÉCNICAS PARA LA AUDITORÍA INFORMÁTICA

Cuestionarios

Las auditorías 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 habitual el comenzar solicitando el llenado 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. 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 el cumplimiento sistemático de sus cuestionarios, de sus Checklists.

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

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.

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

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.

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.

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 alguna 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

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. 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.

5.7 METODOLOGÍA

1.- ***Alcance y Objetivos de la Auditoría Informática*.** 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.

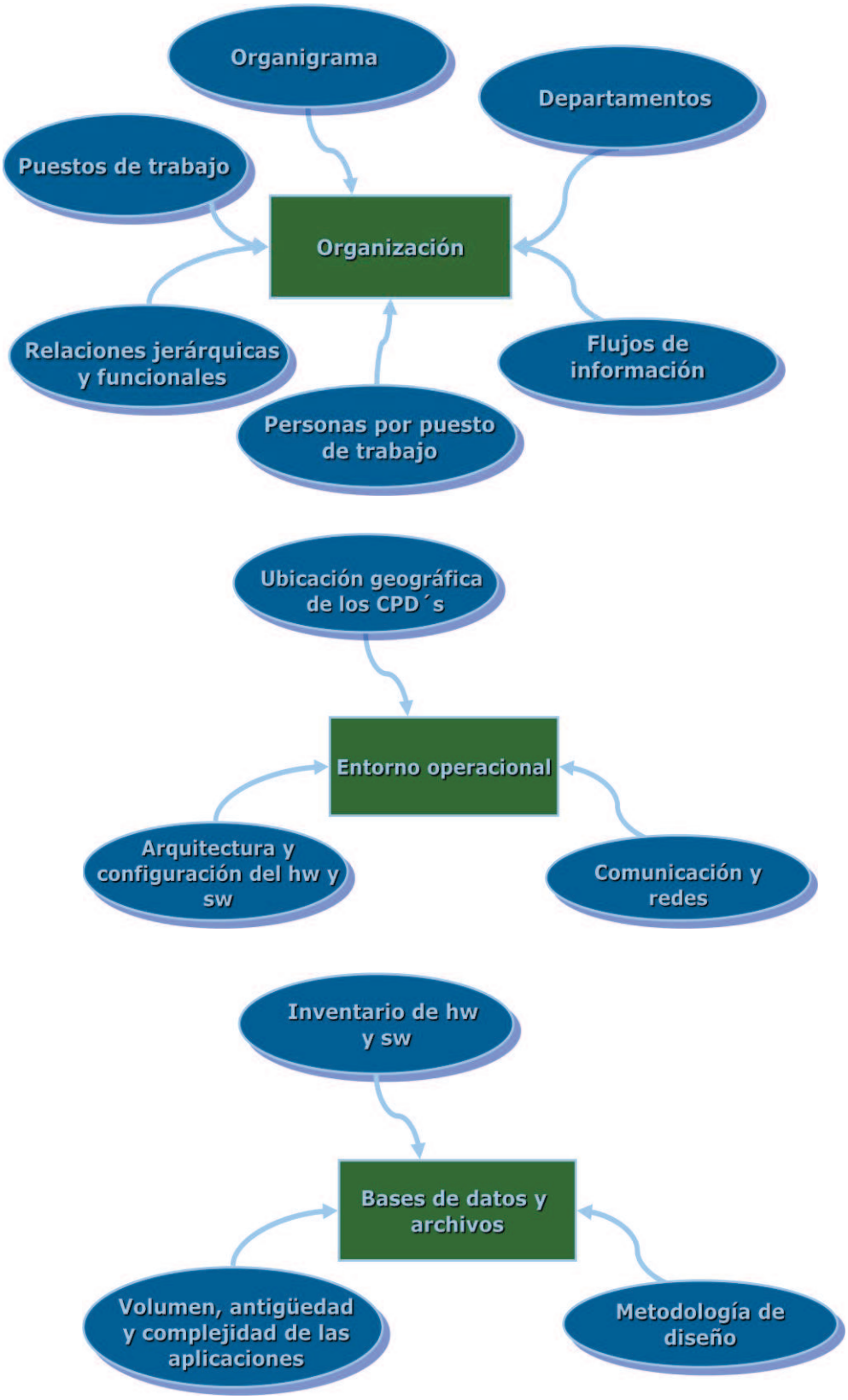
A los efectos de acotar el trabajo, resulta muy beneficioso para ambas partes expresar las excepciones de alcance de la auditoría, es decir cuales materias, funciones u organizaciones no van a ser auditadas.

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 toda auditoría Informática.

2.- ***Estudio inicial del entorno auditable.*** Se enfoca en la obtención de información preliminar que nos arroja la situación presente de la organización en torno a sus recursos informáticos. Se centra en tres áreas esenciales:



3.- ***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.

i. **Recursos materiales**: Es muy importante su determinación, por cuanto la mayoría de ellos son proporcionados por el cliente.

   Se clasifican en dos tipos:

   a. *Recursos materiales Software*. 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.

   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 cual habrá de convenir, tiempo de máquina, espacio de disco, impresoras ocupadas, etc.

ii. **Recursos Humanos:** La cantidad de recursos depende del volumen auditable. Las características y perfiles del personal seleccionado depende 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.