INTRODUCCIÓN

A finales del siglo XX, los Sistemas Informáticos se han constituido en las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización tanto pública como privada. Consecuentemente con lo mencionado el ejercicio de nuestra profesión, no puede ser una excepción en cuanto a utilizar la Auditoría Informática para evaluar y controlar la eficiencia y la eficacia de los sistemas computarizados y el adecuado uso de los recursos informáticos en una institución.

La Auditoría Informática vela por la correcta utilización de los amplios recursos que la organización pone en juego para disponer de un eficiente y eficaz Sistema de Información. Claro está, que para la realización de una Auditoría informática efectiva, se debe entender a la entidad en su más amplio sentido, ya que una Universidad, un Ministerio o un Hospital son instituciones que deben funcionar y prestar servicios como una Sociedad Anónima o empresa Pública. Todas estas utilizan la informática para gestionar sus "actividades" de forma rápida y eficiente, con el fin de que las instituciones puedan obtener beneficios económicos y reducción de costes, de igual manera las entidades brindar un servicio que realmente este acorde a las exigencias y necesidades de los pueblos.

El resultado del presente trabajo es la aplicación de una metodología para realizar una auditoría informática en los departamentos que cuentan con equipos informáticos de la Universidad Técnica de Cotopaxi Edificio Matriz y Ceypsa mediante la utilización de la Metodología Cobit.

El trabajo propuesto está estructurado de la siguiente manera: El capítulo I da a conocer los conceptos de Auditoría, Informática, Control Interno y Metodología Cobit lo que permite tener un conocimiento científico para fundamentar adecuadamente la propuesta de investigación.

El capítulo II expone el trabajo de campo realizado en la Universidad Técnica de Cotopaxi, contiene el levantamiento de información que permite tener un conocimiento del espacio de estudio, en este capítulo se presenta información referente a: Entorno de la Universidad, Estructura Organizacional General, Conocimiento de la Organización y aplicación de los instrumentos dirigidas a todos los involucrados de la presente investigación, cuya información permitió la comprobación y verificación de la hipótesis.

En el capítulo III se presenta el Informe de Auditoría Informática, el mismo que contiene los resultados que son entregados a la Universidad como un aporte del grupo investigador. En cambio en el Capítulo IV se indica las conclusiones y recomendaciones finales del presente trabajo investigativo y finalmente se incluye algunos Anexos que contiene información referente a normas, reglamentos, modelos de encuestas, papeles de trabajo, detalle de los procesos de la Metodología Cobit y otros que han permitido fundamentar y desarrollar de mejor manera el trabajo realizado.

Este trabajo de investigación representa la conclusión de los estudios realizados en el campo de la Auditoría Informática la misma que constituye una herramienta que permite detectar las falencias en la administración de recursos informáticos.

La Universidad debe asumir este tipo de procesos en beneficio de todos los entes que conforman esta institución y así, aprovechar los recursos y avances tecnológicos con los que cuenta. Por ésta y muchas razones nuestra preocupación como estudiantes de la Universidad Técnica Cotopaxi ponemos a consideración este trabajo de investigación para que en un futuro no muy lejano se ponga en práctica y se aproveche el presente documento.

CAPITULO I

FUNDAMENTACIÓN TEÓRICA

1.1 GENERALIDADES

1.1.1 INTRODUCCIÓN A LA AUDITORÍA

La información ocupa cada vez más un lugar preponderante en la escala de valores institucionales. Sobre todo, a medida que crece la organización y se dividen y especializan sus funciones. Entendemos por información el conjunto de datos que sirven para tomar una decisión.

En consecuencia, su necesidad es evidente tanto en la planificación estratégica a largo plazo como en la fijación de estándares para la planificación a corto plazo. La información también es necesaria para el estudio de las desviaciones y de los efectos de las acciones correctoras; es un componente vital para el Control.

Finalmente, la incorporación de la informática en la organización, al igual que en los demás aspectos de la sociedad, va a introducir un enfoque nuevo del tratamiento de los datos que cambiará en alto grado las funciones que actualmente existen en las organizaciones. Cabe aclarar que la Informática no gestiona propiamente la organización, ayuda a la toma de decisiones, pero no decide por sí misma.

Por ende, debido a su importancia en el funcionamiento de una organización, existe la Auditoría Informática.

1.1.2 FUNCIÓN DE AUDITORÍA

1. Estudiar y actualizar permanentemente las áreas susceptibles de revisión.
2. Apegarse a las tareas que desempeñen las normas, políticas, procedimientos y técnicas de auditoría establecidas por los organismos generalmente aceptados a nivel nacional e internacional.
3. Evaluación y verificación de las áreas requeridas por la alta dirección o responsables directos de la Universidad.
4. Elaboración del informe de auditoría (debilidades y recomendaciones).
5. Otras recomendaciones para el desempeño eficiente de la auditoría.

1.1.3 AUDITORÍA INTERNA

En la página web:

http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml nos dice que: "Constituye una función de evaluación independiente. Sin embargo, existe en el seno de una entidad y bajo la autorización de la dirección con el ánimo de examinar y evaluar las actividades de la entidad. La función principal del auditor interno es ayudar a la dirección en la realización de sus funciones, asegurando:

- La salvaguardia del inmovilizado material e inmaterial de la entidad.
- La exactitud y fiabilidad de los registros contables.
- El fomento de la eficiencia operativa.
- La adhesión a las políticas de la entidad y el cumplimiento de sus obligaciones legales".

OBJETIVOS AUDITORÍA INTERNA

- Revisión y evaluación de controles contables, financieros y operativos.
- Determinación de la utilidad de políticas, planes y procedimientos, así como su nivel de cumplimiento.
- Custodia y contabilización de activos.
- Examen de la fiabilidad de los datos.
- Divulgación de políticas y procedimientos establecidos.
- Información exacta a la gerencia.

1.1.4 AUDITORÍA EXTERNA

En la página web:

http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml manifiesta que:

"Constituye una función de evaluación independiente y externa a la entidad que se examina. En la mayoría de las empresas, se contrata anualmente la realización de una Auditoría Externa para investigar el costo de un sistema para lo cual se debe considerar con una exactitud razonable, el costo de los programas, el uso de los

equipos (compilaciones, programas, pruebas, paralelos), tiempo, personal y operación, cosa que en la práctica son costos directos, indirectos y de operación de los estados financieros por parte de un contador público independiente, bien voluntariamente o bien por obligación legal".

OBJETIVOS AUDITORÍA EXTERNA

- Obtención de elementos de juicio fundamentados en la naturaleza de los hechos examinados.
- Medición de la magnitud de un error ya conocido, detección de errores supuestos o confirmación de la ausencia de errores.
- Propuesta de sugerencias, en tono constructivo, para ayudar a la gerencia.
- Detección de los hechos importantes ocurridos tras el cierre del ejercicio.
- Control de las actividades de investigación y desarrollo.

1.1.5 NECESIDAD DE LA AUDITORÍA INFORMÁTICA

En la dirección electrónica: *http://www.rociolopez.8m.com/* nos dice que: "Las organizaciones acuden a las auditorías externas cuando existen síntomas bien perceptibles de debilidad. Estos síntomas pueden agruparse en clases:

<u>Síntomas de descoordinación y desorganización:</u>

- No coinciden los objetivos de la Informática de la organización y de la propia organización.

- Los estándares de productividad se desvían sensiblemente de los promedios conseguidos habitualmente.

Síntomas de mala imagen e insatisfacción de los usuarios:

- No se atienden las peticiones de cambios de los usuarios. Ejemplos: cambios de Software en los terminales de usuario, variación de los ficheros que deben ponerse diariamente a su disposición, etc.
- No se reparan las averías de Hardware ni se resuelven incidencias en plazos razonables. El usuario percibe que está abandonado y desatendido permanentemente.
- 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:

- Incremento desmesurado de costes.
- Necesidad de justificación de Inversiones Informáticas (la entidad no está absolutamente convencida de tal necesidad y decide contrastar opiniones).
- Desviaciones Presupuestarias significativas.
- Costes 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

- Seguridad Lógica
- Seguridad Física
- Confidencialidad
- 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.

- 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".

1.1.6 DEFINICIÓN DE AUDITORÍA INFORMÁTICA

En la dirección electrónica *https://siaa.ucbcba.edu.bo/siaa/reptesispublico.asp* al respecto nos indica que: "Es el conjunto de técnicas, actividades y procedimientos, destinados a analizar, evaluar, verificar y recomendar en asuntos relativos a la planificación, control eficacia, seguridad y adecuación del servicio informático en la empresa, por lo que comprende un examen metódico, puntual y discontinuo del servicio informático, con vistas a mejorar en:

- Rentabilidad
- Seguridad
- Eficacia ”

La Auditoría Informática verifica la utilización eficiente de los recursos informáticos disponibles o por disponer, en función de las estrategias de la organización y de los objetivos previstos.

1.1.7 AUDITORÍA INFORMÁTICA INTERNA

La Auditoría Informática Interna cuenta con algunas ventajas adicionales muy importantes, 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.

1.1.8 OBJETIVOS DE LA AUDITORÍA INFORMÁTICA

Según la dirección electrónica:

http://www.cstconsultores.com/Publicaciones/Auditoríainf.htm

“Objetivo fundamental de la auditoria informática**:** *Operatividad*

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 simultáneo del Sistema Operativo y el Software de base con todos los subsistemas existentes, así como la compatibilidad del Hardware y del Software instalados.

- Los Controles Técnicos Específicos, 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".

1.2 CONTROL INTERNO Y AUDITORÍA INFORMÁTICA

1.2.1 INTRODUCCIÓN AL CONTROL INTERNO INFORMÁTICO

Básicamente todos los cambios que se realizan en una organización someten a una gran tensión a los controles internos existentes. Cuando un auditor profesional se somete a auditar una organización, lo primero que se le viene a la cabeza es mejorar todos los procesos que se llevan en la misma para buscar la eficiencia total.

1.2.2 CONTROL INTERNO INFORMÁTICO

En la página web*: http://aabbccddee.galeon.com/Metodo.htm* manifiesta que:
"Cumplen funciones de control dual en los diferentes departamentos, que puede ser normativa, marco jurídico.

La funciones del control interno es la siguientes determinar los propietarios y los perfiles según la clase de información, permitir a dos personas intervenir como medida de control, realizar planes de contingencias, dictar normas de seguridad informática, controla la calidad de software, los costos, los responsables de cada departamento, control de licencias, manejo de claves de cifrado, vigilan el cumplimiento de normas y de controles, es clara que esta medida permite la seguridad informática".

1.2.3 DEFINICIÓN Y TIPOS DE CONTROLES

De acuerdo al sitio web: *http://alarcos.inf-cr.uclm.es/doc/Auditoria/auditoria.htm* define al control interno como: "Cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para lograr o conseguir sus objetivos.
Los controles internos se clasifican en los siguientes:

- **Controles preventivos:** Para tratar de evitar el hecho, como un software de seguridad que impida los accesos no autorizados al sistema.

- **Controles detectivos:** Cuando fallan los preventivos para tratar de conocer cuanto antes el evento.
- **Controles correctivos:** Facilitan la suelta a la normalidad cuando se han producido incidencias".

1.2.4 FUNCIÓN DE CONTROL INTERNO Y AUDITORÍA INFORMÁTICA

"Control interno informático; Cumplen funciones de control dual en los diferentes departamentos, que puede ser normativa, marco jurídico.

En la auditoría Informática; esta tiene función de vigilancia y evaluación mediante dictámenes, los auditores tienen diferentes objetivos, que los de cuentas, ellos evalúan eficiencia, costos y la seguridad con mayor visión, y realizan evaluaciones de tipo cualitativo".

1.2.5 FUNCIÓN DE CONTROL INTERNO INFORMÁTICO

Según la dirección electrónica:

http://www.ucpr.edu.co/auditores/estandares%5Cindex.htm expresa que: "La función del control interno informático es asegurarse de que las medidas que se obtienen de los mecanismos implantados por cada responsable sean correctas y válidas.

Como principales objetivos podemos indicar los siguientes:

- Controlar que todas las actividades se realicen cumpliendo los procedimientos y normas fijados, evaluar su bondad y asegurarse del cumplimiento de las normas legales.
- Asesorar sobre el conocimiento de las normas.
- Colaborar y apoyar el trabajo de auditoría informática, así como de las auditorías externas al grupo.
- Definir, implantar y ejecutar mecanismos y controles para comprobar el logro del servicio informático".

1.2.6 FUNCIÓN DE AUDITORÍA INFORMÁTICA

Según: *HERNÁNDEZ, Hernández Enrique, (1996); Auditoría en Informática, México.* Considera como:

"**Funciones Mínimas:**

- Evaluación y verificación de los controles y procedimientos relacionados con la función de informática dentro de la Entidad.
- La validación de los controles y procedimientos utilizados para el aseguramiento permanente del uso eficiente de los sistemas de información computarizados y de los recursos de informática dentro de la Entidad.
- Evaluación, verificación e implantación oportuna de los controles y procedimientos que se requieren para el aseguramiento del buen uso y aprovechamiento de la función de informática.

- Aseguramiento permanente de la existencia y cumplimiento de los controles y procedimientos que regulan las actividades y utilización de los recursos de informática de acuerdo con las políticas de la entidad.
- Desarrollar la auditoría en informática conforme normas y políticas estandarizadas a nivel nacional e internacional.
- Evaluar las áreas de riesgo de la función de informática y justificar su evaluación con la alta dirección de la entidad.
- Elaborar un plan de auditoría en informática en los plazos determinados por el responsable de la función.
- Obtener la aprobación formal de los proyectos del plan y difundirlos entre los involucrados para su compromiso.
- Administrar o ejecutar de manera eficiente los proyectos contemplados en el plan de la auditoría en informática". (pág.36)

1.2.7 CLASES DE AUDITORÍA INFORMÁTICA

La Auditoría puede clasificarse desde diversos puntos de vista. Pasamos a desarrollar estos aspectos:

En la página web: *http://www.auditoriadesistemas.com/modules/news/* se encuentra la siguiente clasificación

- Auditoría de la dirección.
- Auditoría del desarrollo o aplicaciones.

- Auditoría de la explotación.
- Auditoría informática de sistemas.
- Auditoría de la seguridad informática.
- Auditoría informática de comunicaciones y redes.

1.2.7.1 AUDITORÍA DE LA DIRECCIÓN

"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 entidad.

Una informática eficiente y eficaz requiere el apoyo continuado de su dirección frente al "exterior". Revisar estas interrelaciones constituye el objeto de la *Auditoría Informática de Dirección*.

1.2.7.2 AUDITORÍA DEL DESARROLLO 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 organización. Muy escuetamente, una aplicación recorre las siguientes fases:

- Prerequisitos del Usuario (único o plural) y del entorno.

- Análisis funcional.
- Diseño.
- Análisis orgánico (Preprogramación 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.

1.2.7.3 AUDITORÍA DE LA 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.

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".

1.2.7.4 AUDITORÍA INFORMÁTICA DE SISTEMAS

Según el sitio web: *http://www.eduardoleyton.com/Audcomp_R.html* nos dice que: "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".

1.2.7.5 AUDITORÍA DE LA SEGURIDAD INFORMÁTICA

De acuerdo con la dirección electrónica:

http://www.monografías.com/trabajos/seguinfo/seguinfo/shtml

"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 el acceso de los usuarios a la información".

1.2.7.6 AUDITORÍA INFORMÁTICA DE COMUNICACIONES Y REDES

En el sitio web: http://www.sedisi.es/05_Estudios/guia01.htm considera que: "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".

1.3 HERRAMIENTAS Y METODOLOGÍAS DE CONTROL Y AUDITORÍA INFORMÁTICA

1.3.1 INTRODUCCIÓN A LAS METODOLOGÍAS EN CONTROL Y AUDITORÍA

El nacimiento de metodología en el mundo de la auditoría y el control informático se puede observar en los primeros años de los ochenta, naciendo a la par con la informática, la cual utiliza la metodología en disciplinas como la seguridad de los sistemas de información, la cual la definimos como la doctrina que trata de los riesgos informáticos, en donde la auditoría se involucra en este proceso de protección y preservación de la información y de sus medios de proceso.

La informática crea unos riesgos informáticos los cuales pueden causar grandes problemas en entidades, por lo cual hay que proteger y preservar dichas entidades con un entramado de contramedidas, y la calidad y la eficacia de la mismas es el

objetivo a evaluar para poder identificar así sus puntos débiles y mejorarlos, siendo esta una función de los auditores informáticos.

1.3.2 HERRAMIENTAS DE CONTROL Y AUDITORÍA INFORMÁTICA

De: *HERNÁNDEZ, Hernández Enrique, (1996); Auditoría en Informática, México.* Se extrae: "Las herramientas de control, son de dos tipos físicos y lógicos.

Como herramientas de control físico podemos citar a los cifradores y las del punto lógico son programas que brindan seguridad, las principales herramientas son las siguientes; seguridad lógica del sistema, seguridad lógica complementaria del sistema, seguridad lógica en entornos distribuidos, control de acceso físico, control de copias, gestión de soporte magnéticos, gestión de control de impresión y envío de listados por red, control de proyectos y versiones , gestión de independencia y control de cambios.

1.3.3 FUNCIONALIDAD DE LAS HERRAMIENTAS

La informática crea unos riesgos informáticos los cuales pueden causar grandes problemas en entidades, por lo cual hay que proteger y preservar dichas entidades con un entramado de contramedidas, la calidad y la eficacia de la mismas es el objetivo a evaluar para poder identificar así sus puntos débiles y mejorarlos de ahí que se puede utilizar herramientas para la obtención de la información requerida".

1.3.3.1 ENTREVISTAS

En el sitio web: http*://www.cstconsultores.com/Publicaciones/Auditoriainf.htm* define a: “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.

1.3.3.2 CHECKLISTS

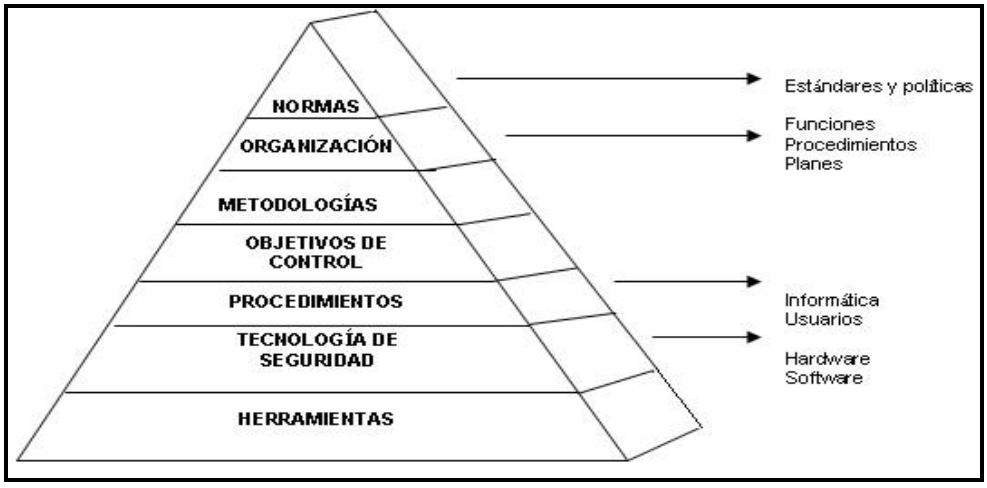
El auditor conversará y hará preguntas “normales”, que en realidad servirán para la complementación sistemática de sus Cuestionarios, de sus Checklist.
El auditor deberá aplicar los Checklist de modo que el auditado responda clara y escuetamente. Se deberá interrumpir lo menos posible a éste, y solamente en los casos en que las respuestas se aparten sustancialmente de la pregunta”.

1.3.4 METODOLOGÍA DE AUDITORÍA INFORMÁTICA Y CONTROL INFORMÁTICO

En la dirección electrónica *http://www.criptored.upm.es/guiateoria/gt_m142a.htm* nos dice que: “La informática crea unos riesgos informáticos de los que hay que proteger y preservar a la entidad con un entramado de contramedidas y la calidad y la eficacia de las mismas es el objetivo a evaluar para poder identificar así sus puntos débiles y mejorarlos.

Por tanto, debemos profundizar más en ese entramado de contramedidas para ver qué papel tienen las metodologías y los auditores en el mismo. Para explicar este aspecto diremos que cualquier contramedida nace de la composición de varios factores expresados en la figura adjunta. Todos los factores de la pirámide intervienen en la composición de una contramedida**".**

GRÁFICO 1.1 METODOLOGÍA DE CONTROL INTERNO Y AUDITORÍA INFORMÁTICA



FUENTE: Piattini , Mario G.; Del Peso, Emilio. "Auditoría Informática: Un enfoque práctico". 1998
ELABORADO POR*: Marco León y Silvia Manotoa*

1.3.5 METODOLOGÍA DE TRABAJO DE AUDITORÍA INFORMÁTICA

Para el desarrollo de la presente Auditoría Informática en la Universidad Técnica de Cotopaxi se ha seguido la siguiente metodología de trabajo, la misma que comprende las siguientes fases:

FASE 1 CONOCIMIENTO PRELIMINAR

1. Alcance y Objetivos de la Auditoría Informática de la Universidad Técnica de Cotopaxi.

2. Estudio inicial del entorno auditable: Universidad Técnica de Cotopaxi.

3. Determinación de los recursos necesarios para realizar la Auditoría en la Universidad Técnica de Cotopaxi.

FASE 2 PLANIFICACIÓN

1. Elaboración del Programa de Trabajo. (Ver anexo # 3)

FASE 3 EJECUCIÓN

1. Elaboración de los Papeles de Trabajo. (Ver Anexo # 4)

2. Aplicación de los Papeles de Trabajo. (Ver Anexo # 5)

3. Aplicación de las encuestas a los usuarios potenciales. (Ver Anexo # 6)

4. Análisis de la información recopilada a través de las encuestas realizadas.

5. Elaboración del primer borrador de Auditoría Informática.

FASE 4 COMUNICACIÓN DE RESULTADOS

1. Lectura del Informe.

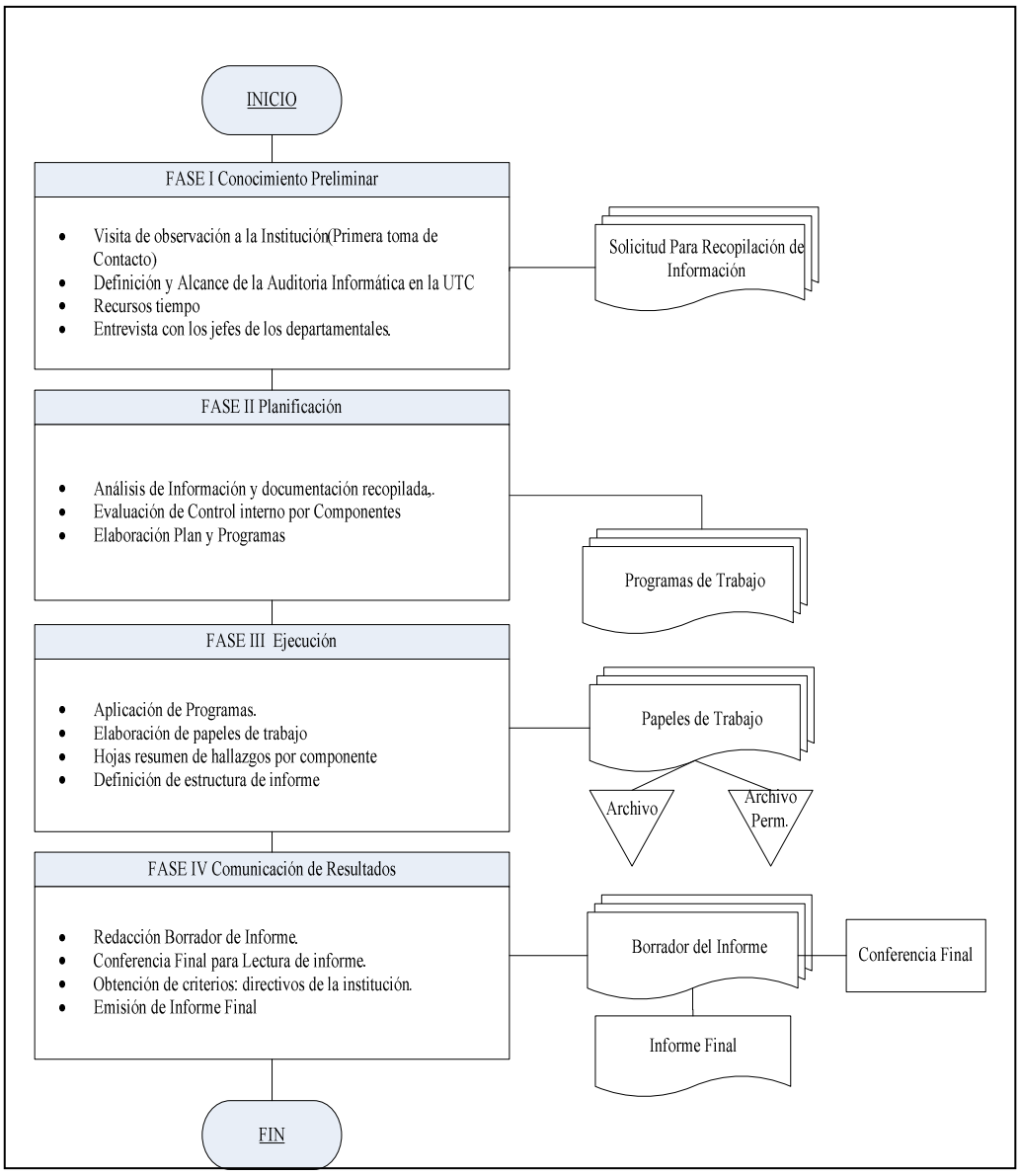
2. Obtención de Criterios por parte de los encargados de los departamentos inmersos en la presente Auditoría Informática.

3. Redacción del Informe Final.

4. Estructuración y presentación del Informe Final.

FLUJOGRAMA DE LA METODOLOGÍA DE TRABAJO DE AUDITORÍA INFORMÁTICA A APLICARSE EN LA UNIVERSIDAD TÉCNICA DE COTOPAXI

Gráfico 1.2: Metodología de Trabajo



Fuente: Manuales de Auditoría Informática
Elaborado por: Marco León y Silvia Manotoa

1.3.6 CLASIFICACIÓN DE INFORMACIÓN Y PROCEDIMIENTOS DE CONTROL

Clasificación de información: determinar que la información es reservada o confidencial.

1. Los datos confidenciales son datos de difusión no autorizada. Su uso puede suponer un importante daño a la organización.
2. Los datos restringidos son datos de difusión no autorizada. Su utilización iría contra los intereses de la organización y/o sus clientes. (Datos de clientes, programas o utilidades, software, datos de inventarios, etc.).
3. Los datos de uso interno no necesitan ningún grado de protección para su difusión dentro de la organización. (Organigramas, política y estándares, listín telefónico interno, etc.).
4. Los datos no clasificados no necesitan ningún grado de protección para su difusión. (Informes anuales públicos, etc.).

Los Procedimientos de control de la información se pueden dividir en los siguientes tipos:

- Física
- Lógica
- Organizativo – Administrativa
- Jurídica

1.3.7 PLAN DEL AUDITOR INFORMÁTICO

En el sitio web: *http://gratistodo.8m.com/capiaudi6.htm* nos dice que: "Un plan del auditor informático deben contener al menos lo siguiente:

1. *Funciones.* Ubicación de la figura en el organigrama de la empresa. Deben describirse las funciones de forma precisa, y la organización interna del departamento, con todos sus recursos.

2. *Procedimientos para las distintas tareas de las auditorías*. Entre ellos están el procedimiento de apertura, el de entrega y discusión de debilidades, entrega de informe preliminar, cierre de auditoría, redacción de informe final, etc.

3. *Tipos de* auditoría*s que realiza.* Metodologías y cuestionarios de las mismas. Existen tres tipos de auditoría según su alcance: la completa de una área; limitada a un aspecto y correctiva que es la comprobación de acciones de auditorías anteriores.

4. *Sistema de evaluación y los distintos aspectos que evalúa*. Independientemente de que exista un plan de acciones en el informe final, debe hacerse el esfuerzo de definir varios aspectos a evaluar como nivel de gestión económica, gestión de recursos humanos, cumplimiento de normas.

5. *Nivel de exposición*. Permite en base a la evaluación final de la última auditoría realizada sobre ese tema definir la fecha de la repetición de la misma auditoría".

1.3.8 NORMAS APLICADAS EN LA AUDITORÍA INFORMÁTICA

A) MODELO POR DOMINIOS COBIT (OBJETIVOS DE CONTROL PARA TECNOLOGÍA DE INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS).

COBIT (Objetivos de Control para Tecnología de Información y Tecnologías Relacionadas.) ha sido desarrollado como un estándar generalmente aplicable y aceptado para la práctica del control de Tecnología Informática, está basado en los Objetivos de Control existentes de la Information Systems Audit and Control Foundation (ISACF) mejorados con los estándares internacionales existentes y emergentes técnicos, profesionales, regulatorios y específicos de la organización.

Misión

Investigar, desarrollar, publicar y promover un conjunto internacional, autorizado y actual de objetivos de control en tecnología de información generalmente aceptados para el uso cotidiano de gerentes de empresa y auditores.

Esta metodología se divide en tres niveles:

Dominios: Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.

Procesos: Conjunto de actividades unidas con delimitación o cortes de control.

Actividades: Acciones requeridas para lograr un resultado medible.

Estos procesos están agrupados en cuatro grandes dominios que se detallan a continuación junto con sus procesos:

1. DOMINIO: (PO) PLANIFICACIÓN Y ORGANIZACIÓN

A través de este dominio se comprende las decisiones estratégicas y tácticas que definen la manera en que la TI ayuda de mejor forma al logro de los objetivos de la institución.

2. DOMINIO: (AI) ADQUISICIÓN E IMPLEMENTACIÓN

Con este dominio se identifica soluciones de TI, adquirirlas o desarrollarlas, y por supuesto hacerlas operativas integrándolas como procedimientos del día a día lo que permite ser mejores y tener una continuidad operativa.

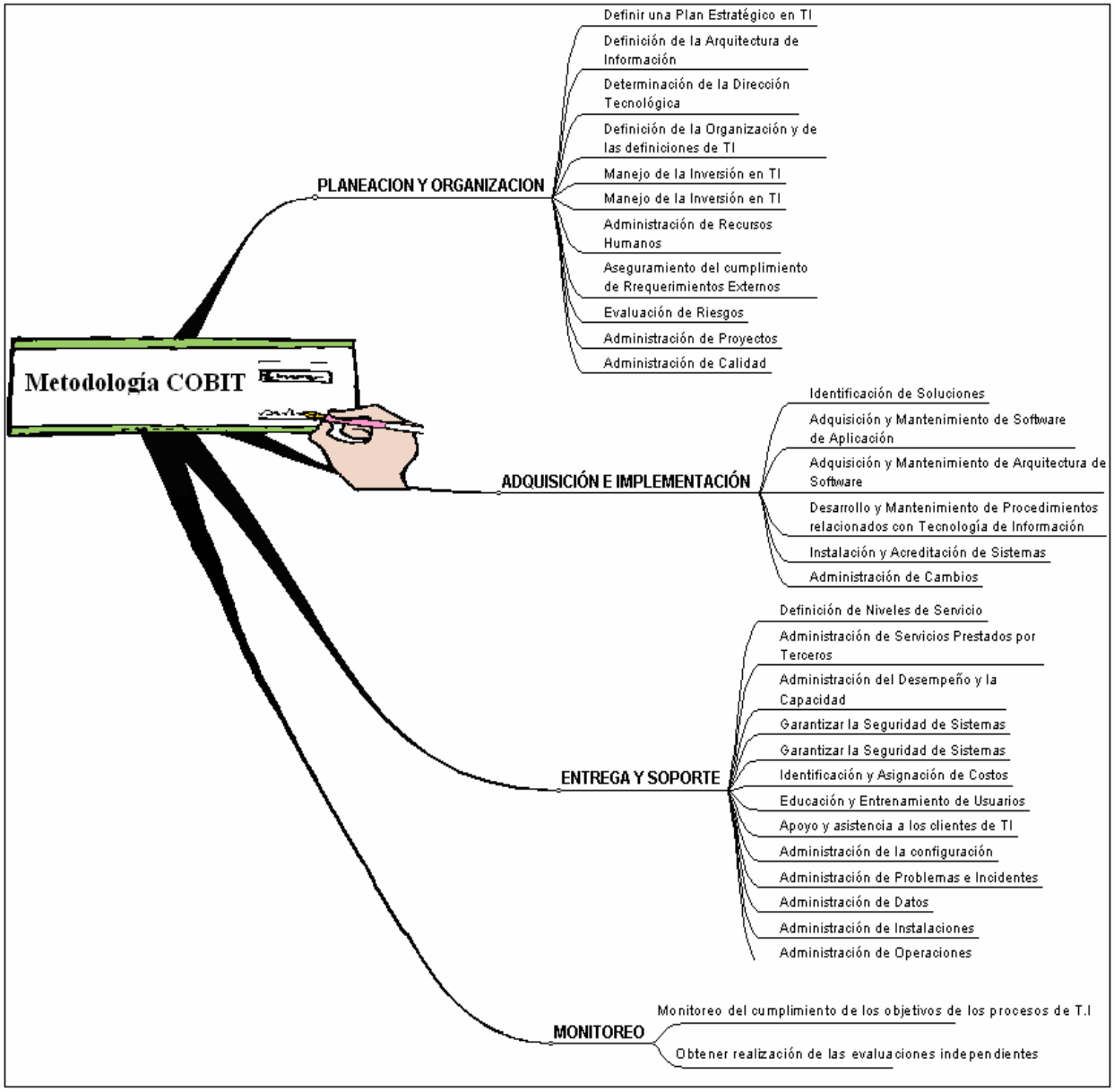
3. DOMINIO: (DS) ENTREGA Y SOPORTE

Mediante este dominio se llegó a comprender las actividades de Soporte a los sistemas en producción. En esta área se incluye el procesamiento de los datos por sistemas de aplicación.

4. DOMINIO: (M) MONITOREO

Mediante este dominio todos los procesos de TI deben ser evaluados regularmente, tanto en cuanto a su calidad, como al cumplimiento de los requerimientos de control.

GRÁFICO 1.3 METODOLOGÍA COBIT



FUENTE: http://www.unap.cl/~setcheve/pe.htm
ELABORADO POR: Marco León y Silvia Manotoa

B) CONTRALORÍA GENERAL DEL ESTADO

Normas de Control Interno para el Sector Público de la República del Ecuador emitido por la Contraloría General del Estado. Específicamente se va a emplear la **Norma 400** (Ver Anexo # 7) la misma que se refiere a: Normas de control interno para el área de sistemas de información computarizados.

Con esta norma se busca promover la correcta utilización de los sistemas computarizados que procesan la información que generan las entidades.

C) UNIVERSIDAD TÉCNICA DE COTOPAXI

Estatuto Orgánico de la Universidad Técnica de Cotopaxi, Art. 5, Fines literal e (Ver Anexo # 8).

Mediante este artículo se pretende vincular a la Universidad y buscar soluciones a los problemas de la sociedad.

1.3.9 PAPELES DE TRABAJO

Los papeles de trabajo son todos aquellos apuntes, datos, e información recopilada con relación a una auditoría y que conforman una documentación y evidencia del trabajo realizado por el auditor.

IMPORTANCIA

Los papeles de trabajo representan en la culminación del trabajo de auditoría, la evidencia documental del trabajo efectuado, de técnicas y procedimientos de auditoría aplicados y de las conclusiones generadas.

OBJETIVOS DE LOS PAPELES DE TRABAJO

- Proporcionar evidencia del trabajo realizado y de las conclusiones obtenidas.
- Ayudar al equipo de trabajo para que adopte una estructura ordenada y uniforme para la presentación del trabajo.
- Facilitar la supervisión y revisión del trabajo realizado, así como dejar evidencia que dicha supervisión fue hecha. ser útil en futuros trabajos o revisiones de la auditoría.
- Mantener el registro de la información para sustentar las declaraciones y los informes.
- Documentar la información que podrá ser útil en futuros trabajos o revisiones de la auditoría.
- Mantener el registro de la información para sustentar las declaraciones y los informes.

CARACTERÍSTICAS GENERALES DE LOS PAPELES DE TRABAJO

a) La información que se incluya en los papeles de trabajo debe ser clara, completa y concisa.

b) Debe dar un testimonio verídico e inequívoco del trabajo realizado.

c) Debe contener las razones que fundamenten decisiones en aspectos controvertidos.

d) Deben cumplir con los más altos parámetros de calidad y así mismo limitarse en cantidad.

e) No deben elaborarse para transcribir o copiar información ni para que los auditados los diligencien.

CONTENIDO DE LOS PAPELES DE TRABAJO

- Descripción de la tarea realizada.
- Los datos y antecedentes obtenidos durante la auditoría.
- Información relevante sobre la actividad u operación del área auditada.
- Antecedentes del ambiente de control y los Sistemas de Información.
- Debilidades y fortalezas (sin que las debilidades afecten el alcance de la auditoría).
- Conclusiones sobre el examen o las revisiones practicadas.

1.3.9.1 TIPOS DE PAPELES DE TRABAJO (VER ANEXO # 4)

- **GUÍA DE AUDITORÍA**

Es una planilla en la que se describen en detalle las actividades que el auditor debe realizar para lograr el objetivo propuesto; se recomienda que por cada objetivo específico se elabore una Guía de Auditoría en la que se relacionen

actividades que estén estrechamente relacionadas con el logro del mismo y sin desbordar los límites del alcance propuesto.

- **LISTA DE VERIFICACIÓN O DE CHEQUEO**

Una lista de verificación o de chequeo contiene una serie de actividades, en forma de pregunta cerrada, que el auditor debe realizar, en su gran mayoría corresponden a evaluaciones, verificaciones, análisis, comprobaciones y revisiones; las respuestas a éstas preguntan son de tipo falso o verdadero, sí o no.

- **CÉDULAS DE HALLAZGO O COMENTARIO**

En la medida en que se van ejecutando los programas de trabajo se deben ir elaborando las cédulas de hallazgos y recomendaciones.

1.3.10 ESTRUCTURACIÓN Y PRESENTACIÓN DEL INFORME FINAL

La función de la auditoría se materializa exclusivamente por escrito. Por lo tanto la elaboración final es el exponente de su calidad.

Resulta evidente la necesidad de redactar borradores e informes parciales previos al informe final, los que son elementos de contraste entre opinión entre auditor y auditado y que pueden descubrir fallos de apreciación en el auditor.

Es importante que el informe, antes de su emisión definitiva, sea comentado y discutido con los responsables del área auditada y en caso de discrepancia de opiniones con el área auditada, estas deberán ser incluidas en el texto final del informe.

En la presentación de resultados el equipo de auditoría, podrá auxiliarse de medios de visión electrónicos, y tendrá el siguiente contenido:

- Objetivo y Alcance de la auditoría
- Limitaciones principales para el desarrollo de la auditoría
- Resultados de auditoría
- Área Auditada (nombre)
- Observaciones
- Recomendaciones
- Conclusión General

Carta de introducción o presentación del informe final

La carta de introducción tiene especial importancia porque en ella ha de resumirse la auditoría realizada. Se destina exclusivamente a los directivos de la entidad auditada, en este caso, Rector, Director de Servicios Informáticos, Jefes de las áreas auditadas, etc.

FINALIDAD

Los informes son un factor importante en el logro exitoso de los objetivos de la auditoría.

El informe de auditoría debe, por lo tanto, ser un documento profesional que se ve y se lee como un producto de profesionales.

FORMATOS

No existe un formato de informe para todas las organizaciones de auditoría. El formato depende de:

- Las necesidades de la dirección.
- La naturaleza de la entidad y su organización (centralizada o descentralizada).

CONFIDENCIALIDAD DE LOS INFORMES

El informe tendrá el carácter de borrador, por lo que su uso será restringido, hasta la entrega del informe final a la entidad auditada por las instancias correspondientes.