UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN

ESCUELA DE CONTABILIDAD SUPERIOR

"AUDITORIA DE LA SEGURIDAD DEL CENTRO DE COMPUTO DE LA FACULTAD DE INGENIERIA DE LA UNIVERSIDAD DE CUENCA"

MONOGRAFÍA PREVIA A LA OBTENCIÓN DEL TÍTULO DE CONTADORA PUBLICA AUDITORA

DIRECTOR: ING. JORGE ESPINOZA IÑIGUEZ

AUTORA: ROCIO CABRERA PROAÑO

CUENCA – ECUADOR
2006

Las ideas y expresiones expuestas en esta Monografía son de exclusiva responsabilidad de su autora.

Rocío Cabrera P.

DEDICATORIA

A mi esposo e hijos: por ser la razón de mi vida e inspiración diaria.

A mis padres: por su apoyo y ayuda constante.

Rocío

AGRADECIMIENTO

A mi familia por su comprensión y apoyo en mis estudios.

A mi maestro y amigo, Director de esta monografía por su paciencia y acertada dirección.

A la Ing. Ma. Fernanda Granda, Directora del Centro de Computo de la Facultad de Ingeniería y al Ing. Fabián Jaramillo, Decano de la Facultad de Ingeniería de la Universidad de Cuenca, por su generosa colaboración en el desarrollo de esta monografía.

Rocío

CONTENIDO

Introducción…….. VII

Capitulo 1. La Auditoría …….. 2

1.1.- Introducción. Conceptos básicos de Auditoría…….. 2
1.2.- Definición general de Auditoría…… 3
1.3.- Tipos de Auditoría…… 3
1.4.- Objetivos de la auditoría…… 4
1.5.- Normas generales de Auditoría…… 5
1.6.- Métodos, técnicas, herramientas y procedimientos de Auditoría…… 7
1.7.- Conclusiones del capítulo…….. 9

Capitulo 2. La Auditoría de Sistemas y la Auditoría sobre la seguridad de sistemas computacionales…….. 11

2.1.- Introducción. Concepto de Auditoría de Sistemas…… 11
2.2.- Marco esquemático de la Auditoría de Sistemas…… 11
2.3.- Objetivos específicos de la Auditoría de Sistemas…… 14
2.4.- División de la Auditoría de sistemas computacionales…… 15
2.5.- Auditoría sobre la seguridad de los sistemas computacionales…….. 15
2.6.- Metodología para realizar la auditoría sobre la seguridad de los sistemas computacionales…… 16
2.7.- Conclusiones del capítulo…… 22

Capitulo 3. Auditoría de la Seguridad del Centro de Cómputo de la Facultad de Ingeniería de la Universidad de Cuenca…… 24

3.1.- Introducción. …… 24
3.2.- Objetivo de la Auditoría…… 24
3.3.- La Facultad de Ingeniería de la Universidad de Cuenca…….. 25
3.4.- Explicación del desarrollo de la Auditoría…… 28
3.5.- Documentos de trabajo…….. 29
3.6.- Explicación y justificación del dictamen final…….. 41
3.7.- Presentación del Informe de Auditoría…… 57
3.8.- Conclusiones del capítulo…….. 78

Conclusiones y Recomendaciones…… 80

Bibliografía…… 82

INTRODUCCIÓN

El acelerado avance tecnológico en los últimos años, ha incrementado el uso de sistemas computacionales en todas las áreas y además la inmensa cantidad de información que se procesa día a día ha obligado a todas las empresas a buscar métodos que le permitan controlar y validar dicha información, y sobretodo analizar si ésta es la correcta y si está adecuadamente procesada y almacenada.

Con este antecedente el proceso normal de las actividades económicas y financieras de los negocios requiere de una constante vigilancia y evaluación, por lo tanto toda empresa requiere de una opinión de preferencia independiente que les ayude a evaluar sus actividades y el cumplimiento de sus objetivos. Esta evaluación consiste en una revisión metódica, periódica de sus transacciones, procesos y resultados de la empresa, con lo que se busca diagnosticar el comportamiento general de la empresa. Esto es lo que conocemos como auditoría.

Al inicio la auditoría se basaba en la revisión y la evaluación de las operaciones netamente contables de los negocios, avanzando a los aspectos financieros y administrativos, llegando el alcance de la misma a una revisión integral. En la actualidad se han realizado evaluaciones especializadas de algunas áreas y actividades; entre algunas de estas encontramos, auditoría del desarrollo de proyectos de mercadotecnia, auditoría de proyectos económicos y la auditoría de sistemas computacionales, motivo de estudio de esta monografía.

Esta monografía esta dividido en tres capítulos, en el primero *la Auditoría,* en donde presento antecedentes, conceptos generales, normas y los métodos que más se utilizan en el campo de la auditoría general, avanzando al segundo capítulo, donde expondré los objetivos específicos de las Auditorías Computacionales, división de dicha auditoría y explicaré la metodología para seguir la misma.

El tercer capítulo, comprende la parte práctica, donde desarrollaré una Auditoría de la Seguridad del Centro de Cómputo de la Facultad de Ingeniería de la Universidad de Cuenca, hasta elaborar el Dictamen de la misma.

CAPITULO I

LA AUDITORÍA

CAPITULO I
LA AUDITORÍA

1.1 Introducción.

El desarrollo de este capítulo será el análisis de los aspectos más relevantes de la auditoría, iniciando desde los conceptos básicos, hasta llegar a una definición general de la auditoría, de igual manera tratando de describir los tipos de auditoría y sobretodo enfatizar en los objetivos de la misma.

Destacaré los métodos, técnicas y las herramientas más relevantes que se utilizan dentro de cualquier tipo de auditoría que se realice, de igual manera enfatizaré en las normas de auditoría generalmente aceptadas, base fundamental en el comportamiento ético y profesional de un auditor.

El propósito de este marco teórico es mostrar los elementos que cimientan la existencia de la disciplina de la auditoría

Conceptos Básicos de Auditoría.

"En tiempos históricos, auditor era aquella persona a quien le leían los ingresos y gastos producidos por un establecimiento (de ahí su raíz latina del verbo audiré, oír, escuchar), práctica muy utilizada por civilizaciones muy antiguas (...)" ([1])

Podemos decir que la primera auditoría nació el momento que nació la necesidad de rendir cuentas de algún negocio y verificar que estas fueran correctas, esta función fue evolucionando junto con el crecimiento de las transacciones mercantiles. De acuerdo con los primeros antecedentes de la auditoría se dice que nación antes de la teneduría de libros en el siglo XV y se profesionalizó con la contabilidad financiera recién en el siglo pasado.

La verdadera necesidad del auditor surge cuando el capital se expande y emigra y aparece el inversionista ausentista, quien reclama de tiempo en tiempo, informes imparciales y sin prejuicios acerca de sus inversiones y de los resultados de la empresa.

Así los auditores siguen al capital británico que invierte en los EEUU de Norteamérica a fines del siglo XIX, y al extenderse la expansión financiera norteamericana hacia América Latina, la auditoría también se extiende a nuestro continente.

[1] Diccionario Enciclopédico Universal SALVAT, Ediciones Salvat, España, 1988. Tomo III, Pág. 130

1.2 Definición General De Auditoría:

Los campos de aplicación de la auditoría han evolucionado mucho, desde su uso netamente contable, hasta el uso en áreas especiales como es la ingeniería, medicina y los sistemas computacionales. Junto con este progreso, también se ha desarrollado las técnicas, métodos, procedimientos y herramientas que se utilizarán en cada uno de estos tipos de auditoría.

Debido a estos constantes cambios citaré de forma general, la definición que se propone para la auditoría:

"Es la revisión independiente de alguna o algunas actividades, funciones específicas, resultados operaciones de una entidad administrativa, realizada por un profesional de la auditoría, con el propósito de evaluar su correcta realización y, con base en ese análisis, poder emitir una opinión autorizada sobre la razonabilidad de sus resultados y el cumplimiento de sus operaciones." ([2])

1.3 Tipos de Auditoría:

La auditoría se puede clasificar desde varios enfoques, sin embargo las más importantes clases las constituyen:

1. Dependiendo de quien las ejecuta:
    - Auditoría Interna: Cuando los exámenes son ejecutados por una unidad dependiente de una empresa.
    - Auditoría Externa: Cuando los exámenes son efectuados por una persona natural o jurídica altamente especializada y que es contratada por una empresa.

2. Dependiendo del tipo de examen:

    - Auditoría Financiera: Cuando los exámenes son realizados para comprobar la razonabilidad de los estados financieros.
    - Auditoría Operativa: Cuando se realizan análisis de los procesos, que tan seguros y ágiles se encuentran.
    - Auditoría Administrativa: Cuando los exámenes se realizan a las estructuras organizacionales.
    - Auditoría de Sistemas: Cuando los exámenes se realizan al procesamiento de datos, su rapidez, precisión, seguridad y economía.
    - Autoría Tributaria: Un examen que se realiza a los impuestos, tasas y gravámenes de las empresas.
    - Auditoría de calidad ISO 9000 o 14000
    - Auditoría Ambiental

[2] Auditoria en Sistemas Computacionales, Carlos Muñoz Razo, editorial, Pearson Educación, México, 2002, Pág. 11

- Auditoría de Imagen y eficiencia de los servicios
- Auditoría social.

3. Según el alcance o profundidad de los exámenes:

    - Auditoría Integral: Cuando abarca todos los estados financieros o toda la organización.
    - Auditoría Parcial: Cuando su extensión cubre una parte financiera u organizativa
    - Auditoría Especial: Cuando su ejecución obedece una situación de fuerza mayor o por pedido de los más altos niveles directivos.

4. Auditorías especializadas en áreas específicas:

    - Auditoría al área médica (Evaluación médico-sanitaria)
    - Auditoría al desarrollo de obras y construcciones (evaluación de ingeniería)
    - Auditoría Fiscal
    - Auditoría Laboral
    - Auditoría de proyectos de inversión
    - Auditoría a la caja chica o caja mayor (arqueos)
    - Auditoría al manejo de mercancías (inventarios)

5. Auditoría de sistemas computacionales:

    - Auditoría informática
    - Auditoría con la computadora
    - Auditoría sin la computadora
    - Auditoría a la gestión informática
    - Auditoría al sistema de cómputo
    - Auditoría alrededor de la computadora
    - Auditoría de la seguridad de sistemas computacionales
    - Auditoría a los sistemas de redes
    - Auditoría integral a los centros de cómputo.
    - Auditoría ISO-9000 a los sistemas computacionales
    - Auditoría outsourcing
    - Auditoría ergonómica de sistemas computacionales

1.4 Objetivos de la Auditoría:

A continuación enunciaré los objetivos de la auditoría, aclarando que los mismos son de carácter general, los cuales pueden ser adaptados al tipo de auditoría que se vaya a realizar; cabe resaltar que antes de iniciar una evaluación de cualquier índole, se deben plantear los objetivos que se pretenden cumplir y los que se seguirán plenamente a lo largo de la auditoría:

- Realizar una revisión independiente de las actividades, funciones o áreas de una institución, para emitir un dictamen profesional sobre la razonabilidad de sus operaciones y resultados.
- Realizar una revisión especializada y autónoma sobre los aspectos contables, financiero, operacional de todas las área de una empresa.
- Evaluar el cumplimiento de normas, procedimientos, políticas que regulan la actividad de los empleados, así también evaluar las actividades que se realizan en sus áreas y planta administrativa.
- Dar un dictamen imparcial y profesional sobre los resultados obtenidos por la empresa, así como también el cumplimiento de sus objetivos y operaciones.

La importancia de estos objetivos radica principalmente en que constituyen un instrumento de interés e información para los accionistas de una empresa, sus administradores, los inversionistas, financistas y proveedores, incluso para las entidades fiscales y organismos de control, y organismos laborales.

1.5 Normas Generales de Auditoría.

Los auditores se rigen por normas y criterios generalmente aceptados, (NAGA) que son emitidos por el **AICPA**[3] y constituyen medidas relativas a la calidad en la ejecución de los actos de evaluación y a los objetivos que pretenden alcanzarse mediante el uso de diversos procedimientos de auditoría. El propósito de señalar estas normas es que nos sirvan de referencia para tomar en cuenta los aspectos fundamentales del estudio de la auditoría como disciplina en el actuar en todo tipo de evaluación.

Las Normas de Auditoría Generalmente Aceptadas (NAGA) se dividen en tres grandes grupos:

- Generales o Personales
- Relativas a la ejecución del trabajo, y
- Relativas a la preparación de informes.

Generales o Personales.- Se refieren generalmente a la calidad de trabajo y a las cualidades que el Auditor debe tener para poder analizar.

- Entrenamiento y capacidad profesional.- El examen debe ser efectuado por personas que tienen entrenamiento técnico adecuado y capacidad profesional como Auditor.
- Esmero Profesional.-: El Auditor debe ejercer el debido cuidado profesional en la ejecución del examen aplicando destrezas, técnicas, prácticas y procedimientos de auditoría.

[3] American Institute Certified Public Accounting; Instituno Estadounidense de Contadores Públicos Certificados

- Independencia de criterio.- En todo los asuntos relacionados con el examen del Auditor debe tener independencia de criterio, es decir imparcial, objetiva y sin ningún compromiso personal.

Normas relativas al trabajo de campo.-Son los elementos básicos fundamentales en la ejecución de trabajo que constituye la especificación particular por lo menos un grado indispensable de la exigencia del cuidado y dirigencia de parte del Auditor. Se subdividen en:

- Planeamiento y Dirección Profesional (Supervisión Adecuada).-: El examen debe ser planeado con anticipación y el trabajo de los asistentes del Auditor, si los hay debe ser debidamente supervisado.
- Estudio y Evaluación del Control Interno.- El Auditor debe estudiar y evaluar apropiadamente el sistema de control interno, como base para determinar el grado de confianza que merece y consecuentemente por determinar el alcance de las comprobaciones que deben efectuarse mediante los procedimientos de Auditoría.
- Evidencia, Suficiencia y Competencia.- el Auditor debe obtener una evidencia adecuada en grado suficiente mediante la inspección, observación, indagación, confirmación para contar una base que nos permita dar una operación de los Estados Financieros sujetos al examen.

Normas relativas a la elaboración del informe de Auditoría.-Es uno de los documentos más importantes del procedimiento del trabajo realizado.

- Aplicación de los Principios de Contabilidad Generalmente Aceptados.- El Auditor en su dictamen debe expresar si los estados financieros están presentados de acuerdo a los principios de la Contabilidad generalmente aceptados.
- Uniformidad en la aplicación de los Principios de Contabilidad Generalmente Aceptados.- El informe debe expresar si tales principios han sido observados consistentemente en el periodo examinado de los estados financieros en relación con el ejercicio anterior.
- Revelación suficiente de los Estados Financieros.-Equivale a que los Estados Financieros deben reflejar los acontecimientos y resultados importantes de una empresa.
- Opinión e informe del auditor.- Dado el grado de responsabilidad del auditor el informe contendrá la expresión de una opinión sobre los estados financieros examinados, tomados en su integridad o la aceleración de que no puede expresar una opinión, en este ultimo se indicara las razones que se lo impide. En consecuencia la opinión podrá ubicarse en las siguientes alternativas:

    - dictamen limpio o sin salvedades.
    - dictamen con salvedades.
    - dictamen adverso.
    - dictamen con abstención de emitir opinión.

1.6 Métodos, técnicas, herramientas y procedimientos de Auditoría.

Las técnicas son las herramientas de las que se vale el Auditor para obtener la evidencia de su examen y con la finalidad de fundamentar su opinión profesional Las técnicas se clasifican en:

- Oculares
- Verbales
- Escritas
- Físicas

Técnicas oculares:

- Observación.- Consiste en cerciorarse en forma ocular de ciertos hechos o circunstancias o de apreciar la manera en que los empleados de la compañía llevan a cabo los procedimientos establecidos.
- Comparación.- Es el estudio de los casos o hechos para igualar, descubrir, diferenciar, examinar con fines de descubrir diferencias o semejanzas.
- Revisión.- Consiste en el examen ocular y rápido con fines de separar mentalmente las transacciones que no son normales o que reviste un indicio especial en cuanto a su originalidad o naturaleza.
- Rastreo.-consiste en seguir una transacción o grupo de transacciones de un punto u otro punto del proceso contable para determinar su registro contable.

Técnicas verbales:

- Indagación.- Consiste en obtener información verbal de los empleados de la entidad a través de averiguaciones y conversaciones. En esta técnica hay que tener mucho cuidado cuando se pregunta, hay que saber hacerla.

Técnicas escritas:

- Análisis.-Consiste en separar las partes con relación con el todo en consecuencia el análisis de una cuenta tiene por finalidad lo siguiente:

    - Determina la composición o contenido del saldo, se refiere a descomponer el saldo de la cuenta de mayor de acuerdo a los respectivos auxiliares.
    - Determina las transacciones de las cuentas durante el año y clasificarlas en forma ordenada, se refiere a establecer los débitos y créditos de una cuenta durante un período.

- Consolidación.- Consiste en hacer que concuerde dos cifras independientes. Ejemplo. conciliación bancaria, etc.
- Confirmación.- Consiste en cerciorarse de la autenticidad de las operaciones, estas pueden ser de dos clases: Negativa.-se puede optar por este método

cuando el saldo del cliente es poco significativos y positiva.- cuando el cliente protesta su saldo, su conformidad, son de dos clases:

- directa.- cuando suministramos de su saldo para que una vez rectificada con su registro proporcione respuesta sobre su conformidad o disconformidad.
- indirecta.- cuando no se le da el saldo al cliente y se solicita informe sobre el mismo para confirmarlo.

Técnicas Físicas:

- Inventarios.- esta forma de recopilación de información consiste en hacer un recuento físico de lo que se está auditando, a fin de comprobar si el número de algún producto es igual a lo detallado en los documentos en la misma fecha. Está técnica se utiliza principalmente en las auditorías de carácter financiero, operativo y administrativo, aunque también se puede utilizar en otro tipo de auditoría.

Existen además otras técnicas que se utilizan en la auditoría como son las encuestas y cuestionarios.

- Encuestas.-"es la recopilación de datos concretos sobre un tema específico, mediante el uso de cuestionarios o entrevistas diseñadas con preguntas precisas, para obtener las opiniones de los encuestados, que permiten luego de una tabulación realizar un análisis e interpretación de esa información." ([4])
- Cuestionarios.- "son una de las formas de recopilación de información de mayor utilidad para el auditor; pues es la recopilación de datos mediante preguntas impresas en cédulas o fichas, en las que el encuestado responde de acuerdo con su criterio; de esta manera, el auditor obtiene información útil que puede concentrar, clasificar e interpretar y dar una opinión sobre lo evaluado." ([5])

Los cuestionarios son herramientas de gran utilidad pues una de ellas es que sirven para evaluar los controles internos de las empresas; constituyen el método en el cual se plantean algunas preguntas directamente relacionadas con el cumplimiento de los principios básicos de control interno y disposiciones legales enfocados a operaciones específicos como tal.

Este formulario que constituye uno de los papeles de trabajo del auditor, está diseñado para que una respuesta negativa implique el incumplimiento de uno de estos principios.

---

[4] Auditoria en Sistemas Computacionales, Carlos Muñoz Razo, editorial, Pearson Educación, México, 2002, Pág. 348

[5] Ibedem, Pág. 340

Con el objeto de formarse un juicio sobre la validez del sistema, el auditor debe analizar la importancia y repercusión de la falta de cumplimiento de los mismos.

La aplicación del cuestionario de control interno, deberá hacerse considerando principalmente los documentos existentes en la entidad y solo en los casos en que esto no fuera posible, se procederá a entrevistarse con los funcionarios, así como se deberá incluir preguntas que a juicio del auditor sean necesarias, por su naturaleza los resultados de la aplicación de este método deberán ser evaluados de acuerdo a las características de cada una de las entidades auditadas.

Fuentes de información para la revisión de controles internos.- Las fuentes de información adecuadas para la revisión del sistema de control interno y de manera específica para la resolución del cuestionario de control interno, básicamente son:

- Organigramas
- Manuales de procedimientos
- Descripción de puestos y/o tareas
- Entrevistas con funcionarios y empleados
- Los informes, papeles de trabajo y programa de auditoría interna
- Observación personal de las prácticas y procedimientos adoptados por la entidad.
- Verificación de operaciones específicas.
- Actas de Junta General de Accionistas y del Directorio

1.7 Conclusiones del Capítulo.

Al concluir de redactar lo que es la auditoría, sus objetivos, sus normas etc., me puedo dar cuenta de la importancia de evaluar una empresa o institución, ya sea en su todo, o en un aspecto específico, pues de esta manera permite a los directores, junta de accionistas, analizar sus acciones y sobretodo en base a resultados de una auditoría tomar sus decisiones futuras.

De la misma forma puedo decir sin temor a equivocarme que la auditoría debería convertirse en un proceso obligatorio en todas las áreas de las empresas, y tipo de empresas, no solo en las públicas sino en las privadas, para mejorar cada vez más y poder alcanzar el desarrollo empresarial que tanto anhelamos.

Y en lo referente a la persona o personas que realizan las auditorías, deben poseer una preparación íntegra tanto en sus conocimientos técnicos como en su ética y moral, ya que la misma le permite dar un dictamen u opinión certera y confiable.

CAPITULO II

LA AUDITORÍA DE SISTEMAS Y LA AUDITORÍA SOBRE LA SEGURIDAD DE SISTEMAS COMPUTACIONALES

CAPITULO II

LA AUDITORÍA DE SISTEMAS Y LA AUDITORÍA SOBRE LA SEGURIDAD DE SISTEMAS COMPUTACIONALES

2.1 INTRODUCCION. CONCEPTO DE AUDITORÍA DE SISTEMAS.

Dentro del gran abanico de auditorías que enunciamos en el capítulo anterior, encontramos la auditoría de sistemas, motivada por lo especializado de las actividades de cómputo, así como por desarrollo que ha tenido estos sistemas en los últimos tiempos, y debido a este acelerado avance en los sistemas, y a la enorme información que se procesa, equipos que se manejan, personal humano, etc, se ha visto la necesidad de ampliar dicha auditoría de sistemas en diferentes ámbitos, como son la auditoría con la computadora, auditoría sin la computadora, auditoría de gestión informática, auditoría al sistema de Cómputo etc, así también encontramos la auditoría de la seguridad de los sistemas computaciones, tema de estudio de este capítulo, iniciando desde su definición, objetivos y todo el marco teórico necesario para el desarrollo de un caso práctico en la actividad profesional.

Concepto de Auditoría de Sistemas.

"*Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes. Dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad, y los bienes de consumo necesarios para el funcionamiento del centro de cómputo. El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de sus resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa*." ([6])

2.2 Marco esquemático de la Auditoría de Sistemas.

"Evaluación a:

Hardware

Plataforma de hardware

[6] Ibedem, Pág. 340

- Tarjeta Madre
- Procesadores
- Dispositivos periféricos
- Arquitectura del sistema
- Instalaciones eléctricas, de datos y de telecomunicaciones
- Innovaciones tecnológicas de hardware y periféricos.

Software

- Plataforma del software
- Sistema Operativo
- Lenguajes y programas de desarrollo
- Programas, paqueterías de aplicación y bases de datos
- Utilerías, bibliotecas y aplicaciones
- Software de telecomunicación
- Juegos y otros tipos de software

Gestión informática

- Actividad administrativa del área de sistemas
- Operación del sistema de cómputo
- Planeación y control de actividades
- Presupuestos y gastos de los recursos informáticos
- Gestión de la actividad informática
- Capacitación y desarrollo del personal informático
- Administración de estándares de operación, programación y desarrollo

Información

- Administración, seguridad y control de la información
- Salvaguarda, protección y custodia de la información
- Cumplimiento de las características de la información

Diseño de sistemas

- Metodología de desarrollo de sistemas
- Estándares de programación y desarrollo
- Documentación de sistemas

Base de Datos

- Administración de base de datos
- Diseño de base de datos
- Metodología para el diseño y programació de base de datos
- Seguridad, salvaguarda y protección de las bases de datos

Seguridad

- Seguridad del área de sistemas
- Seguridad física
- Seguridad lógica
- Seguridad de las instalaciones eléctricas, de datos y de Telecomunicaciones
- Seguridad de la información, redes y bases de datos
- Administración y control de las bases de datos
- Seguridad del personal informático

Redes de cómputo

Plataformas y configuración de las redes

Protocolos de comunicaciones

Sistemas operativos y software

Administración de las redes de cómputo

Administración de la seguridad de las redes

Administración de las bases de datos de las redes

Especializadas

Outsourcing

Helpdesk

Ergonomía en sistemas computacionales

ISO-9000

Internet/Intranet

Sistemas multimedia." ([7])

2.3. Objetivos específicos de la Auditoría de Sistemas.

La auditoría realizada a los sistemas computacionales, al desarrollo de software, a la administración del centro de cómputo, a la seguridad de los sistemas computacionales y lo relacionado con estos aspectos, serán considerados bajo los siguientes objetivos:

- "Realizar una evaluación con personal multidisciplinario y capacitado en el área de sistemas, con el fin de emitir un dictamen independiente sobre la razonabilidad de la operaciones del sistema y la gestión administrativa del área de informática.
- Hacer una evaluación sobre el uso de los recursos financieros en las áreas del centro de información, así como del aprovechamiento del sistema computacional, sus equipos periféricos e instalaciones.

[7] Ibedem, Pág. 30

- Evaluar el uso y aprovechamiento de los equipos de cómputo, sus periféricos, las instalaciones y mobiliario del centro de cómputo, así como el uso de sus recursos técnicos y materiales para el procesamiento de información.
- Evaluar el aprovechamiento de los sistemas de procesamiento, sus sistemas operativos, los lenguajes, programas y paqueterías de aplicación y desarrollo, así como el desarrollo e instalación de nuevos sistemas.
- Evaluar el cumplimiento de planes, programas, estándares, políticas, normas y lineamientos que regulan las funciones y actividades de las áreas y de los sistemas de procesamiento de información, así como de su personal y de los usuarios del centro de información.
- Realizar la evaluación de las áreas, actividades y funciones de una empresa, contando con el apoyo de los sistemas computacionales, de los programas especiales para auditoría y de la paquetería que sirve de soporte para el desarrollo de auditores por medio de la computadora." ([8])

2.4 División de la Auditoría de sistemas computacionales.

Dentro del campo de la auditoría de sistemas computacionales, y debido a la amplitud de este campo, se ha subdivido esta auditoría en auditorías especializadas, las cuales se aplican para las diferentes áreas y disciplinas de este ambiente informático. Según la propuesta de Carlos Muñoz Razo en su libro Auditoría en sistemas computacionales, esta división sería la siguiente:

- Auditoría Informática
- Auditoría con la computadora
- Auditoría sin la computadora
- Auditoría a la gestión informática
- Auditoría al sistema de cómputo
- Auditoría en el entorno de la computadora
- Auditoría sobre la seguridad de sistemas computacionales
- Auditoría a los sistemas de redes
- Auditoría integral a los centros de cómputo
- Auditoría ISO-9000 a los sistemas computacionales
- Auditoría outsourcing
- Auditoría ergonómica de sistemas computacionales.

2.5 Auditoría sobre la seguridad de los sistemas computacionales.

Se puede definir a esta auditoría de la manera siguiente:

"Es la revisión exhaustiva, técnica y especializada que se realiza a todo lo relacionado con la seguridad de un sistema computacional, de sus áreas y personal, así como a las actividades, funciones y acciones preventivas y correctivas que contribuyan a salvaguardar la seguridad de los equipos computacionales, de las

[8] Ibedem, Pág. 40

bases de datos, redes, sistemas, instalaciones y usuarios del mismo. Es también la revisión de los planes contra contingencias y medidas de protección para la información, los usuarios y los propios sistemas computacionales, y en salvaguarda del buen funcionamiento del área de sistematización, sistemas de redes o computadoras personales, incluyendo la prevención y erradicación de los virus informáticos". ([9])

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional. Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos. En la actualidad y principalmente en las computadoras personales, se ha dado otro factor que hay que considerar: el llamado "virus" de las computadoras, el cual, aunque tiene diferentes intenciones, se encuentra principalmente para paquetes que son copiados sin autorización ("piratas") y borra toda la información que se tiene en un disco. Al auditar los sistemas se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus. El uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos. La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica:

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

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

2.6 Metodología para realizar la auditoría sobre la seguridad de los sistemas computacionales.

Con el propósito de explicar la metodología para realizar una auditoría de la seguridad de los sistemas computacionales, ésta se encuentra dividida en tres etapas, las mismas que pueden ser aplicadas en cualquier auditoría dentro del campo de sistemas, las etapas son las siguientes:

1. Planeación de la auditoría de la seguridad de sistemas computacionales
2. Ejecución de la auditoría de la seguridad de sistemas computacionales.

[9] Ibedem, Pág. 610

3. Dictamen de la auditoría de la seguridad de sistemas computacionales.

2.6.1 Planeación de la Auditoría.

Lo relevante en este punto de la auditoría es, planificar todas las actividades a desarrollar; es decir se deben identificar las razones por la que se va a realizar la auditoría y sobretodo determinar el objetivo de la misma, también se deben trazar los métodos, técnicas y procedimientos a utilizar en la evaluación.

En esta etapa se deben elaborar los planes, programas y presupuestos del trabajo de evaluación.

Existen varios métodos y técnicas de planeación, por lo tanto a continuación explicaré los puntos más importantes a ser tomados en cuenta en esta primera etapa de una auditoría y que pueden variar de acuerdo a la experiencia o examen a realizar, los cuales son:

a. Identificar el origen de la auditoría
b. Realizar una visita preliminar al área que será evaluada
c. Establecer los objetivos de la auditoría
d. Determinar los puntos que serán evaluados en la auditoría
e. Elaborar planes, programas y presupuestos
f. Identificar y seleccionar los métodos, procedimientos, instrumentos y herramientas necesarias.
g. Asignar los recursos y sistemas computacionales para la auditoría.

a. Identificar el origen de la auditoría.- como primer paso al iniciar una auditoría, es el averiguar el por qué? de la evaluación, los motivos que llevaron a la empresa a solicitar la auditoría, pues para el responsable de la misma, le proporciona elementos necesarios para realizar una buena planeación del reconocimiento, le ayuda a enfocar la manera de revisar; además le permite saber los aspectos primordiales en los que debe trabajar, Dentro de una auditoría de sistemas se encuentran las siguientes causas:

- Por solicitud expresa de procedencia interna.
- Por solicitud expresa de procedencia externa.
- Como consecuencia de emergencias y condiciones especiales.
- Por riesgos y contingencias informáticas.
- Como resultado de los planes de contingencia.
- Por resultados obtenidos de otras auditorías.
- Como parte del programa integral de auditoría.

b. Realizar una visita preliminar a la área que será evaluada.- realizar una visita preliminar es casi indispensable en una auditoría de seguridad de un centro de cómputo, pues le permite tener un contacto con el personal de dicha área, cuántos y cuáles son los equipos que están operando en el centro de cómputo, y

sobretodo cuáles son las medidas de seguridad visibles que existen y conocer de cerca lo que va a auditar, y para lograr este objetivo se sugiere realizar lo siguiente:

- Visita preliminar de arranque
- Contacto inicial con funcionarios y empleados del área.
- Identificación preliminar de la problemática de sistemas.
- Prever los objetivos iniciales de la auditoría.
- Calcular los recursos y personas necesarias para la auditoría.

c. Establecer los objetivos de la auditoría.- como siguiente paso, el auditor debe es establecer los objetivos, ajustándose a las necesidades de la evaluación. El propósito es dejar claro lo busca en este tipo de trabajo. Se puede establecer por ejemplo:

- Objetivo general.- es el fin global que se pretende lograr en el desarrollo de la auditoría, este objetivo será el fundamento en la realización de la evaluación.
- Objetivos particulares.- son los fines particulares que se pretende lograr en el desarrollo de la auditoría, ya sea de un área específica o de alguna función.
- Objetivos específicos de la auditoría de la seguridad.- es la limitación en forma detallada de los fines que se pretenden alcanzar con a auditoría de la seguridad.

d. Determinar los puntos que serán evaluados en la auditoría.- dentro de la auditoría de la seguridad, tema de esta monografía, se da la necesidad de evaluar en los accesos al centro de cómputo, en el ingreso y utilización de los propios sistemas y en la consulta y manipulación de información, de la misma manera la seguridad de las instalaciones, del personal y los usuarios del sistema, así como de todo lo relacionado a la salvaguarda de los sistemas computacionales.

Para esclarecer un poco qué aspectos se deben evaluar en una auditoría de la seguridad se sugieren los siguientes:

- Evaluación de la seguridad física de los sistemas.
- Evaluación de la seguridad lógica del sistema
- Evaluación de la seguridad del personal del área de sistemas
- Evaluación de la seguridad en el acceso y uso del software.
- Evaluación de la seguridad en la operación del hardware.
- Evaluación de la seguridad en las telecomunicaciones.

e. Elaborar planes, programas y presupuestos para realizar la auditoría de la seguridad.- es la elaboración del plan formal de la auditoría, donde se plasma los planes, programas y presupuestos para la auditoría, así como también los tiempos de ejecución para cumplir los objetivos, además se deben asignar los costos de los recursos que serán utilizados.

f. Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría.- este paso sirve para definir los documentos y medios con los cuales se llevará a cabo la revisión a la seguridad de las empresas, logrando por medio de la elaboración de los métodos, procedimientos y herramientas. Todo esto con el fin de que el auditor sepa lo que debe utilizar para evaluar el punto que se indica, así como la manera de efectuar la evaluación.

En la auditoría de la seguridad se evalúan todos los aspectos relacionados con la salvaguarda de la información, del personal de sistemas, y de todo lo relacionado con los bienes informáticos de las áreas de sistemas de la organización que contribuyen al mejor desempeño de la administración y control de las actividades y operaciones de la función informática en la empresa.

En este tipo de auditoría se recomienda el uso de entrevistas, cuestionarios y encuestas, elaborados con preguntas acordes con las necesidades de su evaluación sobre la seguridad, protección y salvaguarda de activos, información y personal informáticos, así como las medidas preventivas y correctivas relacionadas con la seguridad de un centro de cómputo.

Además el auditor puede utilizar como una gran herramientas los inventarios, con el fin de hacer un recuento de los bienes informáticos del área de sistemas. A continuación se sugiere utilizar las siguientes herramientas, observación, revisión documenta, la matriz de evaluación, una guía de evaluación, una lista de chequeo, o utilizar las técnicas de muestreo.

g. Asignar los recursos y sistemas computacionales para la auditoría.- el siguiente paso es asignar los recursos que serán utilizados para realizar la auditoría, conforme a la planificación anterior; estos recursos pueden ser humanos, informáticos, tecnológicos o cualesquiera otros que se hayan establecido par ala auditoría.

Los responsables de realizar la auditoría son los recursos humanos especializados en informática y auditoría, ya que serán los encargados de realizar todas las actividades programadas.

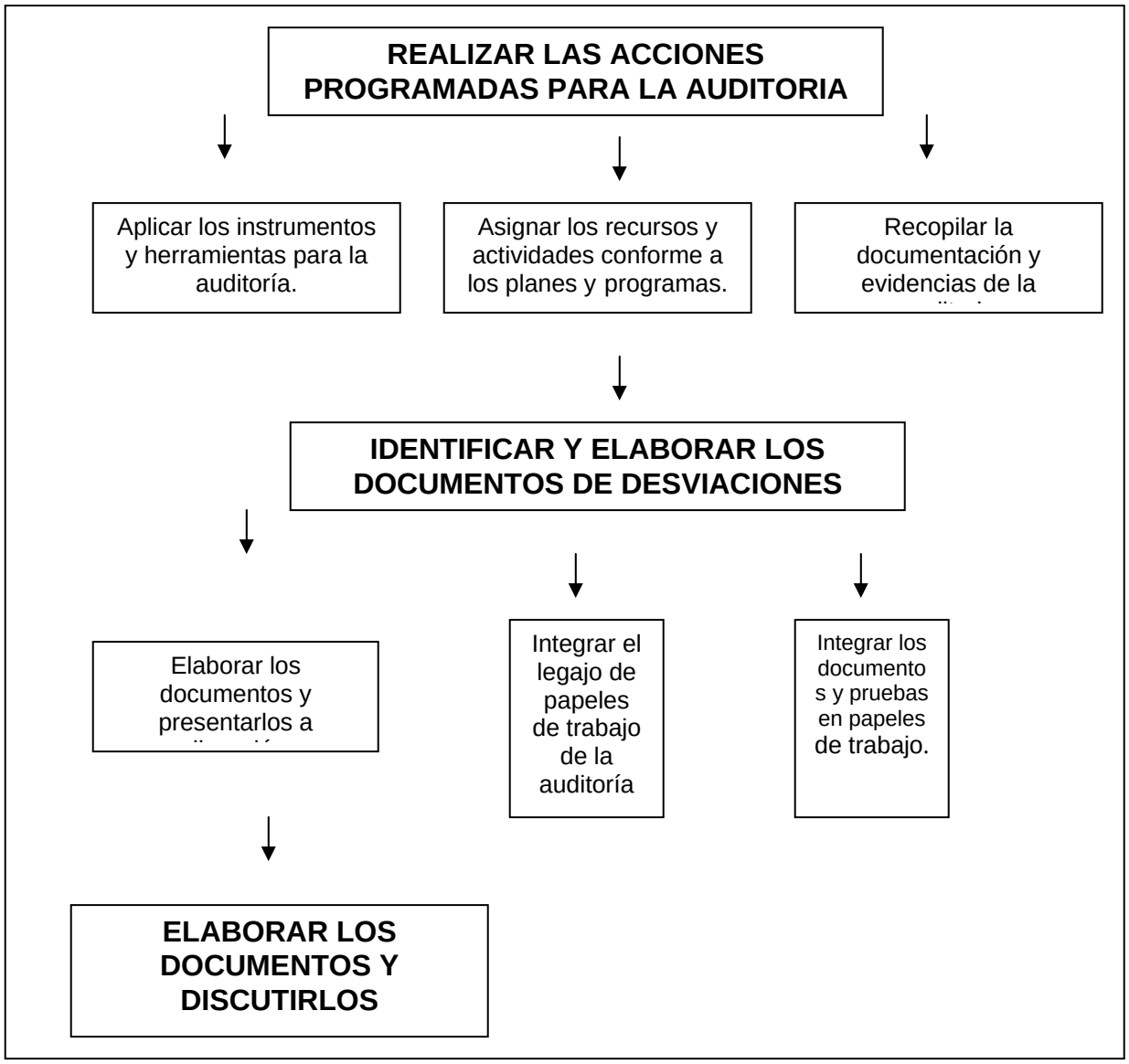
Así como se asignaron los recursos humanos para la auditoría, también se tienen que asignar los recursos informáticos y tecnológicos que se requieren, (herramientas de trabajo), Los mismos que pueden ser sus propios sistemas, sus componentes y periféricos, además los programas, paquetes y utilerías especializadas de evaluación..

Existen otros insumos necesarios para el desarrollo de una auditoría, que pueden ser desde disquetes, cintas, papelería, equipos de oficina, etc.

2.6.2 Ejecución de la Auditoría.

El paso siguiente a la planeación es su ejecución, la cual se da de acuerdo a los requerimientos y puntos que se dieron en la primera etapa.

En esta parte de la auditoría se indican los puntos más importantes y de acuerdo a las características específicas de la auditoría que se trate. Los principales puntos se especifican en el siguiente cuadro:



Realizar las acciones programadas para la auditoría.- se refiere a todo lo programado en la planificación, cumpliendo programas, cronogramas, con el único propósito de cumplir los objetivos de la auditoría.

Aplicar los instrumentos y herramientas para la auditoría.- de la misma manera se refiere a utilizar uno a uno los instrumentos diseñados en la etapa anterior cualquiera de ellas que se ha elegido utilizar.

Identificar y elaborar los documentos de desviaciones encontradas.- este punto es muy importante, pues el auditor luego de la recopilación de datos, tiene que analizar y buscar las posibles salvedades, anotarlas y encontrar la causa y la posible solución, así mismo como los responsables de los mismos; y plasmarlas en documentos de salvedades.

Elaborar el dictamen preliminar y presentarlo a discusión.- una vez culminada la evaluación, está en la obligación de redactarlas todas las salvedades una a una, o en conjunto y como primer paso tratarlas con los responsables de las mismas, buscar el origen y encontrar las posibles soluciones inclusive con fecha para corregirlo.

Integrar el legajo de papeles de trabajo de la auditoría.- todo auditor tiene la obligación de guardar todo documento que utilizó en la auditoría, como respaldo en caso de necesitarlo posteriormente.

2.6.3 Dictamen de la auditoría.

En esta última etapa encontramos tres pasos, los mismos que son:

- Analizar la información y elaborar un informe de situaciones encontradas.
- Elaborar el dictamen final.
- Presentar el informe de auditoría.

Analizar la información y elaborar un informe de situaciones encontradas.- el paso fundamental en la elaboración del dictamen de auditoría es el análisis de los papeles de trabajo junto con la elaboración de un borrador de las salvedades encontradas, para luego discutirlas con las personas involucradas y finalmente realizando las correcciones que fueran necesarias o no, elaborar el informe final. Todo este proceso podemos subdividirlo en los siguientes pasos:

- Analizar los papeles de trabajo
- Señalar las situaciones encontradas
- Comentar las situaciones encontradas con el personal responsable.
- Realizar correcciones necesarias.
- Elaborar un borrador con elementos relevantes.

Elaborar el dictamen final.- en la elaboración del informe final de una auditoría de sistemas junto con la opinión del auditor, se da luego de una entrevista con los auditados, advirtiendo que el fin de una auditoría no es encontrar culpables, sino ayudar a mejorar situaciones que se están manejando de una manera incorrecta o mejorarlas.

Presentar el informe de auditoría.- como último paso tenemos es presentar el informe a los más altos directivos de la empresa, la misma que se debe realizar con mucha formalidad, con una elaboración correcta y profesional, el mismo que debe contener lo siguiente:

- La carta de presentación.
- El dictamen de la auditoría.
- El informe de situaciones relevantes
- Anexos y cuadros adicionales.

En la elaboración del informe el auditor debe demostrar experiencia, conocimientos y la más alta profesionalidad posible, pues lo debe realizar tomando en cuenta lo conversado con los directivos, con las salvedades y los papeles de trabajo.

Este dictamen y el informe de auditoría no debe tener un solo error, su redacción sobre las salvedades debe ser clara y concreta.

La presentación física del informe es una reunión plenaria con el nivel directivo más alto, en este instante ya no existen comentarios ni aclaraciones, sólo es la lectura o entrega física de los documentos. Es una entrega formal y protocolaria.

Luego de la presentación la empresa auditora debe integrar perfectamente los papeles de trabajo, los mismos que servirán en caso de aclaraciones posteriores y para dar seguimiento a las salvedades encontradas.

2.7 Conclusiones del capítulo.

Al culminar el estudio de la metodología de una auditoría de la seguridad de los sistemas computacionales, me puedo dar cuenta de lo delicado y complejo que puede llegar a ser la realización de una evaluación de este tipo, pero el éxito depende de una adecuada planificación, del uso apropiado de las herramientas que se utilicen en cada evaluación, y para no fallar en estas decisiones depende de la capacidad y buen criterio del auditor responsable. La aplicación de uno u otra herramienta o método, depende también de las características de la empresa o centro de cómputo a examinar, inclusive de los objetivos planteados en la misma.

Con todo lo expuesto, existe muchos métodos teóricos para realizar auditorías, el uso de uno u otro depende insisto, en la experiencia del auditor, de la empresa a auditar y de los objetivos planteados. Inclusive la manera de presentar el informe de la auditoría puede variar de uno a otro por los mismos puntos expuestos con anterioridad.

CAPITULO III

AUDITORÍA DE LA SEGURIDAD DEL CENTRO DE CÓMPUTO DE LA FACULTAD DE INGENIERIA DE LA UNIVERSIDAD DE CUENCA

CAPITULO III

Auditoría de la Seguridad del Centro de Cómputo de la Facultad de Ingeniería de la Universidad de Cuenca.

3.1 Introducción.

El Centro de Cómputo de la Facultad de Ingeniería de la Universidad de Cuenca, es un Centro de Cómputo dedicado principalmente a cubrir las necesidades académicas de la Facultad, no tiene dentro de sus responsabilidades el procesamiento de información, ni desarrollo de software; da soporte a tres áreas a saber: plataforma informática acorde a las necesidades académicas para que los estudiantes puedan recibir sus cátedras; otra plataforma para el desenvolvimiento de las actividades administrativas de la Facultad; y una tercera, que es el sistema informático donde se mantiene la información académica de los estudiantes y profesores. Estas tres áreas son conocidas como laboratorios de cómputo, red administrativa y sistema académico, respectivamente.

En este capitulo evaluaré y explicare el desarrollo de la Auditoría de la seguridad realizada en este Centro de Cómputo según los atributos particulares de éste, los mismos que se señalaron en el párrafo anterior. Esta auditoría se concentra en los aspectos hardware, software y ambiente.

.

3.2 Objetivo de la Auditoría.

Los objetivos generales de la auditoría planteada al Centro de Cómputo de la Facultad de Ingeniería de la Universidad de Cuenca consistieron en realizar una revisión independiente de los sistemas computacionales, las áreas, el proceder de los usuarios y la forma de trabajar del personal del Centro de Cómputo del punto de vista de la seguridad del hardware, software y ambiente.

Para poder cumplir este objetivo se plantearon otros específicos que consistieron en:

- Evaluar:
    - Condiciones e instalaciones físicas y medio ambiente.
    - Protección y seguridad de los espacios físicos de las instalaciones de Cómputo.
    - Seguridad en los sistemas computacionales.
    - Seguridad del hardware.
    - Seguridad del software.
    - Mantenimiento preventivo y correctivo del software y el hardware.

- Recaudar información y elaborar un informe de situaciones detectadas.

- En base a la información recaudada en entrevistas, cuestionarios y encuestas elaborar un análisis de sustento al informe final.
- Elaborar el dictamen final.
- Elaborar y presentar el informe de auditoría.

3.3 La Facultad de Ingeniería de la Universidad de Cuenca.

A continuación citaremos algunos aspectos que nos ayuden a conocer mejor el estamento donde se aplicó la auditoría.

3.3.1 Reseña Histórica.

La Universidad de Cuenca tiene su sede en la ciudad del mismo nombre, fue creada por decreto legislativo del 15 de octubre de 1867. Se denominó inicialmente Corporación Universitaria del Azuay.

En 1887, se crea las cátedras aplicadas (química industrial, botánica, zoología, geología, ingeniería, litografía y grabado) bajo la conducción de profesores alemanes contratados con este propósito.

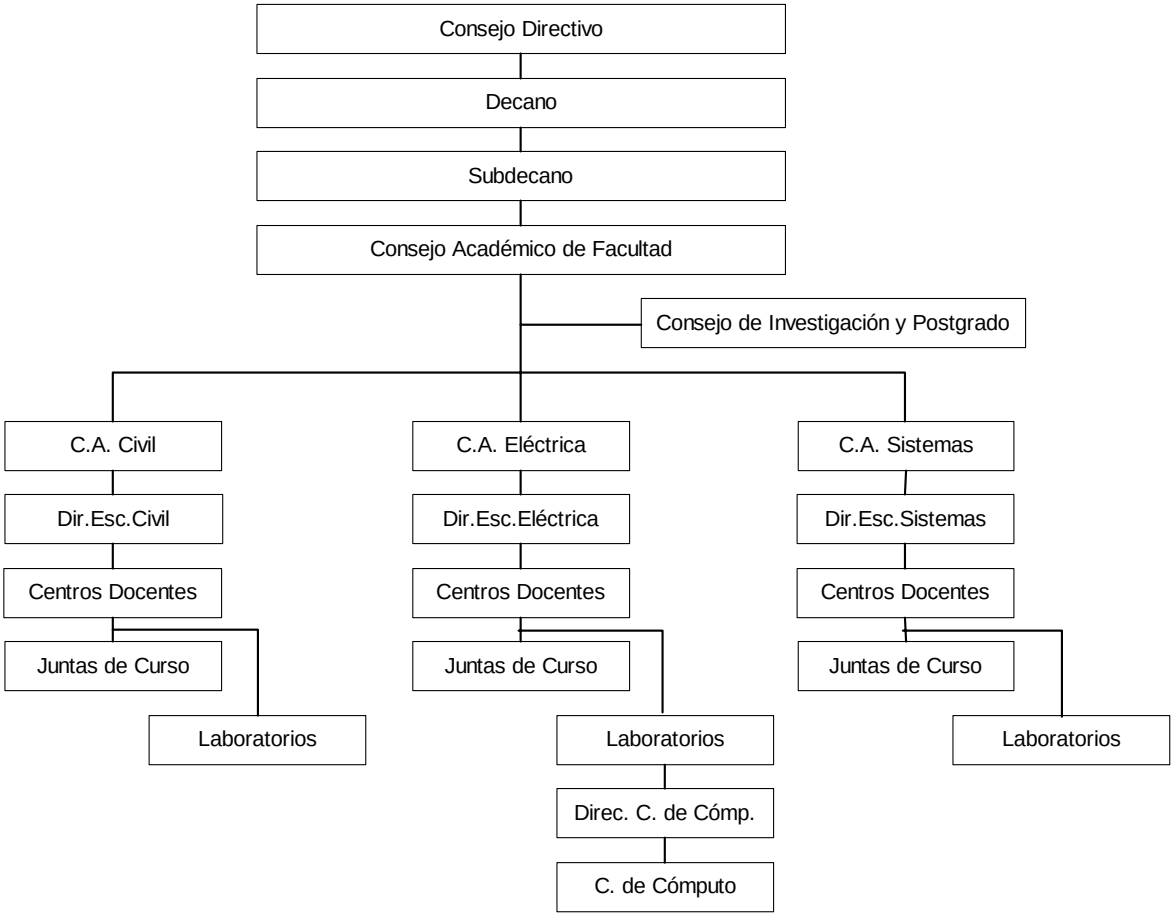
En 1890 se organiza la Facultad de Ciencias, donde se desarrolla la enseñanza de las matemáticas puras y aplicadas, y de las ciencias físicas y naturales. En 1895 bajo el impacto de la Revolución Liberal, se promulga la ley de Instrucción Pública en junio de 1897 y se consagra el reconocimiento de la condición propiamente universitaria de la Corporación del Azuay, que por un tiempo se llama Universidad del Azuay.

Desde 1926, toma su nombre definitivo de Universidad de Cuenca. En 1940, y teniendo siempre en la mira el desarrollo de la región, la Universidad crea la Escuela Superior de Minas (1935), y la Facultad de Ciencias Matemáticas y Físicas (1939) con la Escuela de Ingeniería Civil.

En 1972, se crea la Escuela de Ingeniería Eléctrica que hasta la fecha ha preparado a más de 400 profesionales en el ámbito de la Energía y Potencia, Electrónica y Telecomunicaciones.

Posteriormente y como una respuesta oportuna la globalización de los medios de comunicación, se inicia en 1990, la carrera de Programación y Computación que en un año más daría origen a la carrera de Ingeniería de Sistemas con la creación de Escuela de Informática

3.3.2 Estructura Organizacional del Centro de Cómputo dentro de la Facultad de Ingeniería.



3.3.3 Visión.

"Ser una Facultad competitiva, con excelencia académica, que propicie la investigación y el desarrollo técnico – científico, con una plana docente altamente calificada; que responda de manera proactiva a las necesidades de desarrollo local, regional y nacional que forme profesionales emprendedores con calidad humana, iniciativa, liderazgo, y se constituya en un referente de opinión y orientación de la sociedad." ([10])

[10] Plan estratégico de la Facultad de Ingeniería, documento, Universidad de Cuenca, febrero 2005

3.3.4 Misión.

La Facultad de Ingeniería al pertenecer a un estamento educativo superior, como todas sus iguales tiene por misión cumplir de la mejor manera su gestión académica a través de conseguir profesionales con los siguientes perfiles:

"Perfil Profesional Ingeniero Civil.

La Escuela de Ingeniería Civil, reconocida por su elevado nivel académico, entrega a la sociedad ecuatoriana profesionales suficientemente capacitado para resolver en forma individual o formando grupos interdisciplinarios, proyectos de diseño, fiscalización y construcción de obras de Ingeniería relacionadas con:

•Vías de comunicación,
•Obras Hidrosanitarias e Hidráulicas.
•Estructuras de edificios, puentes, etc.
•Saneamiento y protección ambiental.
•Además, completa la formación integral y humanística con enseñanzas en idiomas, sociología, investigación, y destrezas gerenciales."([11])

"Perfil profesional Ingeniero Eléctrico.

Considerando el campo ocupacional del medio, se ha estructurado un pénsum de estudios de forma que nuestros profesionales, obtengan buenos conocimientos en las áreas de potencia, telecomunicaciones, electrónica y control.
Además, completa la formación integral y humanística con enseñanzas en idiomas, sociología, ecología, etc.
Actualmente nuestros egresados se están desenvolviendo con mucho éxito en los campos de:

- Potencia (Empresas Eléctricas de todo el País y Organismos de Regulación)
- Telecomunicaciones (Empresas de telecomunicaciones nacionales, internacionales y Organismos de Regulación)
- Electrónica y Control (varias Industrias del país).
- Libre Ejercicio Profesional (a través de asociaciones, o en forma individual, han formado sus oficinas, para dar asesoramiento, realizar diseños y construcciones eléctricas y telefónicas). " ([12])

[11] Presentación de la Facultad de Ingeniería. Documento electrónico en Power Point. Ing. Fabián Jaramillo P. 2006

[12] Ibedem

"Perfil profesional del ingeniero de sistemas.

La escuela de Sistemas forma profesionales de alto nivel académico en las Ciencias de la Computación con una formación humanística y científica capaces de aplicar sus conocimientos en diferentes disciplinas y de diseñar y desarrollar Sistemas de Información de propósitos diversos. El profesional conocerá la teoría y los métodos de las ciencias de la computación así como sus aplicaciones en otras disciplinas y su vinculación con la sociedad. La formación de este profesional deberá capacitarle para:

- Identificar problemas relacionados con las Ciencias de la Computación.
- Proponer diferentes alternativas de solución del problema ya identificado.
- Evaluar estas alternativas con el fin de escoger la más congruente con los recursos disponibles.
- Colaborar en la implementación de la solución escogida o dirigir la misma.
- Participar en la conformación de equipos de trabajo interdisciplinarios en los que se requiera la contribución de un consultor de alto nivel en la rama de la Informática." ([13])

3.4 Explicación del desarrollo de la Auditoría.

Con la finalidad de cumplir los primeros aspectos formales de la Auditoría realicé una primera visita a la Facultad, donde con previa cita me entrevisté con el Sr. Decano, Ing. Fabián Jaramillo, a quien le impuse del plan de trabajo previsto a realizar en coordinación con la directora del centro de Cómputo, quien autorizó el plan y adicionalmente me facilitó la documentación de la Facultad. Más tarde me entreviste informalmente con la directora del Centro de Cómputo, Ing. María Fernanda Granda, con quien discutimos y coordinamos el plan de trabajo, además me mostró las instalaciones físicas y me dio a conocer los detalles necesarios para poder formular los cuestionarios y encuestas necesarias.

Con este cúmulo de información planifiqué las visitas necesarias para levantar la información y las técnicas a utilizar.

Se elaboraron cuestionarios de control interno, los mismos que fueron aplicados a la Directora de Cómputo y al instrumentista, custodio de los equipos y encargado de mantener en orden el recinto de Cómputo, el mismo que contestó a mi parecer con demasiada celeridad, y que al momento de cruzar información encontré diferencias que me obligaron a preparar y realizar una nueva entrevista con la Directora de Cómputo para descubrir los motivos de las divergencias en algunas respuestas, las mismas que fueron solventadas y que personalmente me preocupe de corroborarlas

[13] Ibedem

para asegurarme de que las incongruencias entre las dos partes fueran expuestas según la realidad.

Como parte probatoria de esto, a más de la conversación sostenida y registrada para mi análisis, se tomaron fotos que muestran evidencias de cómo se encuentran algunas de las situaciones del Centro de Cómputo.

En la visita, donde apliqué los cuestionarios antes señalados, también se realizó una encuesta a una muestra significativa de usuarios, los mismos que se dividieron en dos tipos: alumnos y personal administrativo y docente. Estas fueron tabuladas y expuestas en forma de cuadros estadísticos para poder realizar el respectivo análisis, pero para que las respuestas estuvieren sustentadas en la realidad, solicite una nueva visita donde permanecí por un tiempo prudencial que me permitió verificar si las tendencias mayoritarias en las respuestas coincidían con la realidad, dicha confrontación y sus conclusiones, junto con los datos de los cuestionarios, se mencionaran en el análisis y se reflejarán en el informe de Auditoría.

3.5 Documentos de Trabajo

El trabajo se sostuvo metodológicamente en el cronograma de actividades que sirvió como Plan de Auditoría. Esta planificación realizada al inicio, ya en la ejecución sufrió pequeñas modificaciones dado que había que “acomodarse” a los horarios y tiempos disponibles de las personas y usuarios con quien había que conversar, pero en general sirvió como guía para cubrir y conseguir los objetivos, estos cambios se explican en el punto anterior donde se menciona con detalle como se procedió. El cronograma inicial fue:

P/T #1
AUDITOR: RCP
PERIODO: 08-2006

Tareas	Semana 1					Semana 2					Semana 3					Semana 4					Semana 5					Semana 6					Semana 7					Semana 8				
	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Definición del tipo de pruebas																																								
Elaboración de Encuestas y cuestionarios																																								
Entrevistas individuales																																								
Entrevista grupal																																								
Procesamiento de la información																																								
Elaboración del dictamen preliminar																																								
Discusiones del documento y modificaciones Elaboración del informe de situaciones encontradas																																								
Análisis de los papeles de trabajo																																								
Elaboración del dictamen final																																								
Elaboración y preparación del informe de auditoría																																								
Presentación del informe de auditoría																																								

Los controles internos aplicados se dividieron en cuatro cuestionarios que cubrieron los asuntos de: seguridades y controles físicos; seguridades y controles en programas de aplicación; seguridades y controles en la organización; y, operación, seguridad y mantenimiento, los mismos que a continuación se anotan:

RCP

C-001
AUDITOR: RCP
PERIODO: 08-2006

AUDITORÍA DE LA SEGURIDADES AL CENTRO DE CÓMPUTO DE LA FACULTAD DE INGENIERIA DE LA UNIVERSIDAD DE CUENCA

CUESTIONARIO DE CONTROLES INTERNOS
ASUNTO: SEGURIDADES Y CONTROLES FISICOS

PREGUNTA	SI	NO	N/A	OBSERVACIONES
1. ¿La alimentación eléctrica para los servidores cuenta con algún tipo de protección a la variación de voltaje?				
2. Si la respuesta a la pregunta anterior es si, ¿Está funcionando correctamente?				
3. ¿Cuenta el sistema con una fuente de poder capaz de dar energía al computador cuando se suprime la corriente eléctrica?				
4. Si la respuesta a la pregunta anterior es sí, ¿Está funcionando adecuadamente? Indique en observaciones cuánto tiempo de energía que brinda al sistema.				
5. ¿Existe en el centro de cómputo un extintor contra incendios?				
6. Si la respuesta a la pregunta anterior es sí, ¿Está dentro del período de carga y con la presión adecuada?				
7. ¿Cuenta el Centro de Cómputo con un equipo de aire acondicionado?				
8. ¿Se mide con frecuencia la temperatura y la humedad?				
9. ¿Se mide con frecuencia la tensión e intensidad de la corriente eléctrica?				
10. ¿Las acometidas eléctricas de alimentación para los equipos del Centro de Cómputo son independientes del resto de la instalación eléctrica?				
11. La instalación eléctrica del Centro de Cómputo tiene conexión a tierra?				
12. ¿Existe algún sistema de detección de incendios?				
13. ¿Existe algún letrero o indicador de que está prohibido fumar, convenientemente escrito o difundido?				

14. ¿Está restringido el acceso al Centro de Cómputo? 15. ¿Existe algún sistema de alarma que permita detectar intrusos en el Centro de Cómputo? 16. ¿Tiene el Centro de Cómputo alguna puerta de escape? 17. Si la respuesta a la pregunta anterior es sí, ¿puede ésta ser usada como entrada? 18. ¿Existe algún equipo de control de acceso al Centro de Cómputo? Si existe alguno, descríbalo brevemente en observaciones. 19. ¿Existe algún plan de seguridad de emergencias escrito y aprobado? 20. ¿Se ha contratado alguna póliza de seguros? 21. Si la respuesta a la pregunta anterior es sí, ¿Cubre ésta todo riesgo? 22. ¿Se limpia regularmente el Centro de Cómputo? 23. Si la respuesta es sí, ¿se controla a la persona de limpieza? 24. ¿Se hace mantenimiento periódico a los equipos de computación? 25. ¿Se destruye adecuadamente todo papel, listado, etc. Al que no se va a dar uso? 26. ¿Cuenta el Centro de Cómputo con una destructora de papeles? 27. Si la respuesta a la pregunta anterior es sí. ¿Funciona correctamente? 28. ¿Existe algún manual o reglamento que trate acerca de la seguridad física del Centro de Cómputo? 29. ¿Existe algún tipo de estantería con llave para guardar los manuales y documentación así como la recepción de los mismos? 30. ¿Se controla la entrega de dichos manuales y documentación así como la recepción de los mismos? 31. ¿Existe un inventario actualizado de los manuales y documentación de los programas y aplicaciones? 32. ¿Se guarda en algún lugar fuera de la empresa una copia de los manuales y documentación? 33. Si la respuesta a la pregunta anterior es sí, ¿Se encuentra estas copias bajo llave y custodia? 34. ¿Están los discos, cintas y cualquier otro medio magnético convenientemente almacenados en salas o armarios especiales? 35. ¿Se guarda en una localidad distinta a la de la empresa una copia de los discos y cintas? 36. Si la respuesta a la pregunta anterior es sí ¿Se encuentran estas copias bajo llave y custodia? 37. ¿Está restringido para personal ajeno del centro de cómputo el acceso a manuales,				

	documentación, librerías, discos, cintas y medios magnéticos?				
38.	¿Está marcado o identificado perfectamente el material confidencial?				
39.	¿Se sacan suficientes copias de seguridad de los archivos principales?				
40.	¿Existe algún plan escrito para sacar copias de respaldo periódicamente?				
41.	¿Existe un inventario actualizado de cintas y discos que permita controlar su ubicación y antigüedad?				
42.	¿Se destruyen los discos y cintas que están dañados o fuera de uso?				
43.	¿Existe un stock mínimo o de seguridad de los suministros (papel, cintas, discos, etc.) en el Centro de Cómputo?				
44.	¿Existen procedimientos de operación escritos para encender y apagar el computador ya sea en operaciones normales o cuando se va la energía eléctrica?				
45.	En caso de que el equipo sufra un daño, ¿Existe un plan de contingencias para soportar la emergencia?				
46.	Si la respuesta a la pregunta anterior es sí, ¿Se ha realizado un simulacro del plan de contingencias?				
47.	¿Existe control adecuado sobre el uso de suministros en el Centro de Cómputo?				
48.	¿Se lleva un registro adecuado de averías e interrupciones en el funcionamiento del equipo de computación?				
49.	¿Se evita la operación del computador por personas no autorizadas?				
50.	¿Está el centro de cómputo alejado de zonas peligrosas?				
51.	¿El techo y suelo del centro de cómputo está construido de un material no combustible?				
52.	¿Existe algún conducto de agua que atraviese el Centro de Cómputo?				
53.	¿Pasan los cables de corriente eléctricas cerca del material combustible?				
54.	¿Las puertas del Centro de Cómputo se cierran solas mediante algún mecanismo?				
55.	¿Existe alguna alarma de incendios de activación manual?				
56.	¿Está la información en discos y cintas magnéticas correctamente etiquetadas y ordenados?				
57.	¿Existe algún mecanismo de control que permita conocer a quién se le entrega la información procesada por el computador?				
58.	¿Existe algún tipo de solicitud para la emisión de listados e información por parte del Centro de Cómputo?				
59.	¿Tiene la información y listados emitidos por el Centro de Cómputo una hoja de ruta que				

permita conocer el destino y utilización de dicha información? 60. ¿Están las ventanas del centro de cómputo protegidas contra intrusos? 61. ¿Existen cronogramas de trabajo para el uso del equipo? 62. ¿Se retienen copias de la información en el tiempo necesario para satisfacer requisitos operacionales y legales?				

AUDITORÍA DE LA SEGURIDADES AL CENTRO DE CÓMPUTO DE LA FACULTAD DE INGENIERIA DE LA UNIVERSIDAD DE CUENCA

CUESTIONARIO DE CONTROLES INTERNOS ASUNTO: SEGURIDADES Y CONTROLES EN PROGRAMAS Y APLICACIONES.

PREGUNTA	SI	NO	N/A	OBSERVACIONES
1. ¿Es adecuada la documentación de los programas?				
2. ¿Los cambios, modificaciones o nuevos programas son autorizados antes de proceder a su realización?				
3. ¿Se revisan y se prueban adecuadamente los programas antes de entregarlos a los usuarios?				
4. ¿Se documenta adecuadamente cualquier cambio o modificación de un programa?				
5. ¿Existe un plan para el desarrollo futuro de programas y aplicaciones para la adquisición del equipo necesario para ello?				
6. ¿Existen políticas en cuanto a la propiedad de datos y protección de los mismos?				
7. ¿El acceso a los programas está restringido y reglamentado para el Centro de Cómputo?				
8. ¿Se prepara manuales de cada programa para el usuario?				
9. ¿Se da mantenimiento a los programas y aplicaciones en forma regular?				
10. ¿Están integrados las aplicaciones en un todo?				
11. ¿Existe un área de control que revise que los listados e información emitidos por el computador estén correctos?				
12. ¿Existen procedimientos escritos y detallados con instrucciones concretas acerca del uso de cada programa y aplicación?				
13. ¿Está cada usuario o grupo de usuarios provisto de una palabra clave o código secreto de seguridad?				
14. ¿Se varia con suficiente frecuencia la tabla de palabras claves o códigos secretos?				
15. ¿El acceso a la tabla de palabras claves o códigos secretos está restringido?				
16. ¿Existen otros procedimientos de seguridad física adicionales, llaves, tarjetas magnéticas, etc.?				
17. ¿Las fallas de funcionamiento en los				

programas son documentadas y revisadas adecuadamente? 18. ¿Los programas y aplicaciones son autorizados por el Decanato antes de ser puestos en operación? 19. ¿Existen procedimientos escritos para descargar o restaurar información al computador? 20. ¿Emite el Centro de Cómputo un listado de control donde se especifique la hora, la fecha, el tiempo de utilización, los programas usados, por cada usuario? 21. ¿Se hacen inspecciones regulares y por sorpresa al contenido de programas y aplicaciones? 22. ¿Existen estándares establecidos para la elaboración y documentación de los programas? 23. ¿Se destruyen las pruebas de los programas? 24. ¿Existen procedimientos para probar programas modificados? 25. ¿Tienen acceso los usuarios a la documentación y a los programas de manera que puedan modificarlo? 26. ¿Existe algún contrato o convenio para procesar información fuera de las instalaciones del cliente? 27. ¿Todos los software cuentan con las licencias respectivas?				

AUDITORÍA DE LA SEGURIDADES AL CENTRO DE CÓMPUTO DE LA FACULTAD DE INGENIERIA DE LA UNIVERSIDAD DE CUENCA

CUESTIONARIO DE CONTROLES INTERNOS
ASUNTO: SEGURIDADES Y CONTROLES EN LA ORGANIZACIÓN.

PREGUNTA	SI	NO	N/A	OBSERVACIONES
1. ¿Dispone el Centro de Cómputo de un organigrama funcional? 2. ¿Existe separación de funciones y de responsabilidades en el Centro de Cómputo? 3. ¿Se selecciona adecuadamente al personal del Centro de Cómputo? 4. ¿Se capacita continuamente al personal del Centro de Cómputo? 5. ¿Se motiva adecuadamente al personal del Centro de Cómputo? 6. ¿Está el personal de operación del computador adecuadamente formado en técnicas de determinación de problemas y averías? 7. ¿Está informado el personal sobre medidas y cuidados específicos relativos a seguridad del Centro de Cómputo? 8. ¿Existe un manual de organización en el cual se describa responsabilidades de todo el personal en el Centro de Cómputo? 9. ¿Existen políticas para mantener la seguridad cuando termina la relación laboral con un empleado? 10. ¿Se evalúa y supervisa al personal del Centro de Cómputo? 11. ¿Existen políticas de vacaciones obligatorias para el personal del Centro de Cómputo?				

AUDITORÍA DE LA SEGURIDADES AL CENTRO DE CÓMPUTO DE LA FACULTAD DE INGENIERIA DE LA UNIVERSIDAD DE CUENCA

CUESTIONARIO DE CONTROLES INTERNOS
ASUNTO: OPERACIÓN, SEGURIDAD Y MANTENIMIENTO.

PREGUNTA	SI	NO	N/A	OBSERVACIONES
1. ¿Se ha efectuado la revisión de los contratos de hardware y software?				
2. ¿Se ha efectuado la evaluación del cumplimiento de los contratos por parte de los proveedores de los equipos?				
3. ¿Cuál es la cobertura de los seguros contratados?				
4. ¿Se mantiene documentación de soporte de los archivos?				
5. ¿Existe estándares para la operación del computador?				
6. ¿Se controla la eficiencia y óptima utilización del hardware?				
7. ¿Se está utilizando el equipo solamente para trabajos autorizados?				
8. ¿Se llevan reportes de utilización de hardware y software?				
9. ¿Se elabora calendarios de trabajo del área de procesamiento de datos?				
10. ¿Se mantiene un inventario pormenorizado del equipo?				
11. ¿Existe un manual de procesamiento de mantenimiento del hardware?				
12. ¿Son adecuados las condiciones ambientales de las áreas del Centro de Cómputo?				
13. ¿Se controla la distribución de los reportes?				
14. ¿Se revisan los controles de los nuevos sistemas antes de su implantación?				
15. Se ha verificado la bondad de los estándares para mantenimiento del software?				
16. ¿Se ha efectuado la verificación de los procedimientos utilizados para actualización de archivos?				
17. ¿Se ha verificado la seguridad lógica de datos y archivos de programas considerando las modificaciones efectuadas?				
18. Se ha implantado procedimientos de seguridad física?				
19. ¿Se efectúan verificaciones de los sistemas de accesos físicos?				