Universidad del Azuay

Facultad de Administración de Empresas

Escuela de Ingeniería de Sistemas

"Elaboración de un software para evaluación, control y auditoría de sistemas de información, aplicado en el centro de cómputo de la Universidad del Azuay"

Trabajo de graduación previo a la obtención del título de Ingeniero de Sistemas

Autor:

Fernando Mauricio Sigüenza Sarmiento

Fernando Esteban Torres Palacios

Director: Ing. Jorge Espinoza Idrovo.

Cuenca, Ecuador

2007

DEDICATORIA

Este trabajo está dedicado con todo cariño a mi familia y de forma muy especial a mis padres por el amor, apoyo, comprensión y valores inculcados durante mi vida, sobre todo por el esfuerzo dedicación y sacrificio que realizaron día a día para que pueda alcanzar esta meta.

Esteban

DEDICATORIA

Dedico este proyecto a mi madre ya que ella ha sido mi guía y mi fuerza para conseguir esta meta, también a mi padre por su gran apoyo y confianza, a mi esposa e hijo por su amor cariño, compresión y permanente apoyo para la cristalización de este sueño, a mis hermanos, abuelos y toda mi familia por cariño y apoyo o incondicional que me han brindado

Fernando

AGRADECIMIENTOS

Agradecemos a Dios por permitirnos terminar el presente proyecto, a la Universidad del Azuay y a sus maestros por habernos recibido en sus aulas y por todos los conocimientos recibidos, a nuestro director de tesis Ing. Jorge Espinoza Idrovo por su acertada dirección y orientación, que supo proporcionarnos para la culminación exitosa del presente proyecto, al Ing. Janela Encalada Jefe del centro de cómputo de la Universidad del Azuay por el tiempo y apoyo brindado, de igual manera al Ing. Pablo Pintado por su acertada colaboración, y a todas las personas quienes fueron participes directos de la consecución de este trabajo de investigación.

ÍNDICE DE CONTENIDOS

INDICE DE ILUSTRACIONES Y CUADROS

RESUMEN

El contenido de la presente tesis tiene por objetivo la elaboración de un software para evaluación, control y auditoría de sistemas de información, para facilitar la recopilación procesamiento y generación de informes que permita mejorar las actividades de una organización.

Para el desarrollo de la aplicación utilizamos la herramienta Microsoft Visual Basic .NET 2003, con el gestor de base de datos Microsoft SQL Server 2000.

La eficiencia del software fue comprobada en el centro de cómputo de la Universidad del Azuay, dando seguimiento al proceso de compras de equipos y suministros de computación, lo que nos permitió encontrar sus falencias y plantear las recomendaciones que mejorarían a este proceso.

ABSTRACT

The objective of this thesis is develop a software to evaluate, control, and audit information system in order to facilitate the compilation, processing, and creation of databases that will allow to improve the activities within organizations.

For the development of the application, we used Microsoft Visual Basic .NET 2003 with the database software Microsoft SQL Server 2000.

The efficiency of the software was proved and tested in the Information System Department of the University of Azuay through a process of purchasing equipment and computer supplies during the month of December, 2006. This allowed us to find the system flaws and recommend solutions to improve the process.

INTRODUCCIÓN

El presente trabajo pretende mejorar la fase de recolección y procesamiento de datos de cualquier tipo de auditoría, ayudando a la persona responsable de esta tarea a realizar su trabajo de forma más rápida y segura.

El objetivo general del presente trabajo es elaborar un software para la evaluación, control y auditoría de sistemas de información, que permita el ingreso de los datos de los distintos procesos que se realizan en el área de una empresa, procesarlos y generar la información resultante para plantear las posibles recomendaciones que ayudaran a mejorar la calidad de las actividades de la empresa.

Entre los objetivos específicos propuesto para este trabajo tenemos los siguientes:

- Determinar una metodología y sus fases para el desarrollo de una auditoría.
- Conocer y aprender las herramientas a utilizar para el desarrollo de esta tesis.
- Definir la arquitectura que se utilizara para el análisis y desarrollo del software.
- Desarrollar una aplicación que sea utilizada, como un apoyo en cualquier tipo de auditoría.
- Realizar una auditoría al centro de cómputo de la Universidad del Azuay aplicado el software desarrollado.
- Presentar un informe con las conclusiones y recomendaciones de la auditoría realizada en el centro de cómputo de la Universidad del Azuay.

Para lograr los objetivos planteados hemos estructurado este trabajo en seis capítulos los cuales se indican a continuación.

En el primer capítulo daremos a conocer los conceptos y aspectos más relevantes de la auditoría y como se lleva a cabo una auditoría de sistemas, en el segundo estudiaremos las herramientas a utilizar, sus características y sus ventajas. En el tercer capítulo desarrollaremos la metodología a seguir para llevar un adecuado control, evaluación y auditoría de cualquier sistema. En el cuarto realizaremos el análisis, diseño y desarrollo del software. En quinto capítulo probaremos la eficiencia del software realizando una auditoría al centro de cómputo de la Universidad del Azuay. En el sexto y último capítulo se encuentran las conclusiones y recomendaciones del presente trabajo.

CAPÍTULO 1:

INTRODUCCIÓN Y ASPECTOS GENERALES DE AUDITORÍA

CONTENIDO

1.1 Introducción al capítulo

Hoy en día, parte del éxito de las empresas se debe no solo a la forma de administrar y disponer de sus recursos, es esencial también llevar un control y evaluación de todas las funciones y recursos que se poseen dentro de la misma, para determinar y garantizar que las actividades se realicen de forma correcta y los recursos se utilicen de forma eficiente.

La Auditoría tubo sus inicios con la revisión y control que se realizaba sobre las operaciones contables de las empresas, hoy en día estas actividades de control y diagnostico abarcan algunas áreas específicas de la empresa así como también de sus actividades, es así que se puede realizar una auditoría a cualquier elemento de las empresas, por ejemplo tenemos auditoría de sistemas de cómputo, auditoría a la seguridad de la empresa, etc.

El auditor, tiene su origen del "latín ***uditor;*** que significa el que oye, del verbo ***audire,*** oír anteriormente oyente"[1]. El auditor es la persona encargada y capacitada para realizar cualquier tipo de auditoría en la empresa u otra institución y será la persona o grupo de personas que tendrán ciertas características especiales para desarrollar su trabajo.

Con el fin de tener una idea de la importancia de la auditoría a continuación veremos los conceptos y aspectos más importantes con el fin de conocer que es la auditoría, y como se desarrolla o lleva acabo una auditoría de sistemas informáticos. Los conocimientos que se estudiarán nos permitirán tener los conceptos necesarios para realizar de mejor manera este proyecto.

[1] Carlos Muñoz Razo. Auditoría de Sistemas Computacionales. Editorial Prentice Hall 2002 Pag. 11

1.2 Concepto de auditoría

1.2.1. Definición general de auditoría

En esta sección se presenta una definición de auditoría general, ya que se puede tener diferentes tipos de auditoría cada una tiene su definición para el área específica a la que se realiza, es por ello que planteamos la siguiente definición de auditoría:

"Auditoría es la revisión independiente que realiza el auditor, aplicando técnicas, métodos y procedimientos especializados, a fin de evaluar el cumplimiento de las funciones, actividades, tareas y procedimientos de una entidad administrativa así como dictaminar sobre el resultado de dicha evaluación..."[2].

De esta definición podemos extraer ciertas características que debe tener la auditoría, entre las que podemos citar:

"...Auditoría es la revisión independiente..."[2]; es primordial que se tenga una independencia tanto profesional como laboral, para realizarla de forma correcta.

"...aplicando técnicas, métodos y procedimientos especializados..."[2]; cualquier profesional puede realizar una auditoría pero sin los conocimientos necesarios difícilmente podría realizarla de una manera eficaz y efectiva, es por ello que se debe tener muy claro, conocer y aplicar estas técnicas y procedimientos para llevar una auditoría de forma adecuada.

"...a fin de evaluar el cumplimiento de las funciones, actividades, tareas y procedimientos de una entidad..."[2]; esta es la función principal de la auditoría, es decir la de hacer una evaluación de las actividades y recursos que se quiera auditar, para determinar un resultado de dicha evaluación

[2] Carlos Muñoz Razo. Auditoría de Sistemas Computacionales. Editorial Prentice Hall 2002 Pag. 34

que será un informe que con total profesionalismo y basado en las técnicas de auditoría dará a conocer los resultados de la evaluación.

1.2.2. Definición de auditoría informática

Antes de realizar esta definición debemos decir que la información, es el elemento primordial en cualquier sistema informático, además que la información no es más que el resultado del procesamiento de datos ya sea de forma manual o automática que permitirá tomar decisiones. Una vez definido lo que es la información, podemos decir lo siguiente.

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

1.3 Alcances de la auditoría informática

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

1.4 Tipos de auditoría

Para realizar una clasificación de los tipos de auditoría debemos tomar en cuenta y agruparlos por algunos factores como son:

1.4.1 Por su lugar de aplicación

Está determinado por el lugar de donde proviene el auditor por lo que puede ser de dos tipos:

Auditoría externa

Que es la ejecutada por personal ajeno a la organización o área objeto de estudio, cuyo objetivo fundamental es examinar y evaluar la situación real del área auditada; ésta cumple con los siguientes aspectos: independencia, metodología, experiencia, disponibilidad, credibilidad y validez técnica del sistema de control.

Auditoría interna

Es la que cumple una función de control al servicio de la alta dirección empresarial. El examen del sistema informático es efectuado únicamente por personas que trabajan en la organización, cuyo entorno de trabajo es financiero y operacional, es decir su campo de acción es toda la organización.

1.4.2 POR SU AREA DE APLICACIÓN

Denominada también por el objeto auditado, clasifica a la auditoría por el lugar en la empresa a la cual se va realizar la auditoría, así tenemos:

Auditoría Financiera

Llamada también contable, fue el primer tipo de auditoría que existió en el ámbito comercial. En este tipo de auditoría se somete al examen de un experto a la información contable, es decir información de los registros contables y operaciones financieras de la empresa.
Tiene como fin demostrar la veracidad de estados financieros, preparación de informes y evaluación de la eficiencia operacional, eficacia, economía de los métodos y procedimientos.

Auditoría Administrativa

En este tipo de auditoría se realiza una verificación sistemática de la actividad administrativa en una empresa, para determinar si el desempeño ha sido el adecuado, para lo cual se evalúa a la empresa en cuanto a su organización, relación entre el personal que lo integra, cumplimiento de procedimientos y funciones establecidas. También se encarga de evaluar las políticas y normas implantadas en la empresa que regulan el uso de los recursos.

Auditoría Operacional

El objeto a auditar son las operaciones, métodos, técnicas y procedimientos que se realizan en la empresa o área a auditar, para el desarrollo de sus actividades, con el único fin de verificar su existencia y su cumplimiento de forma correcta, eficaz y eficiente.

Auditoría de sistemas

Se preocupa de la función informática y sistemas computarizados, emite una opinión independiente sobre la validez técnica del sistema de control interno informático y la confiabilidad de la información.

1.5 OBJETIVOS DE AUDITORÍA INFORMATICA

Teniendo en cuenta que la evaluación de los sistemas informáticos, y todo los elementos que intervienen en un centro de cómputo, así como también los relacionados con el desarrollo, mantenimiento y los usuarios que manejan los sistemas computacionales, la auditoría informática tiene entre los más importantes los siguientes objetivos:

- Evaluar las operaciones del sistema y la gestión administrativa en el área de sistemas, utilizado personal capacitado, para emitir un informe sobre el mismo.

- Determinar si se están cumpliendo con los programas, planes, políticas, normas y estándares, que regulan el funcionamiento de todas las actividades, tanto de los sistemas de cómputo y equipos que se utilizan en la empresa o área a auditar como del personal y usuarios de los sistemas y equipos.

- Realizar evaluaciones sobre el uso de los recursos financieros que son utilizados dentro del centro de cómputo, ya sea para la adquisición o mantenimiento de equipos e instalaciones.

- Determinar si se está dando un uso adecuado a los equipos de cómputo, y sus periféricos (impresoras, escáner, etc.), y si las características son las adecuadas para el trabajo o utilidad para el que fueron adquiridos.

- Determinar que las instalaciones sean las adecuadas, de tal forma que se garantice la integridad de los equipos y del personal que labora dentro del centro de cómputo y de la empresa.

- Realizar un control y evaluación del software que se utiliza, ya sea para el procesamiento de la información, sistemas operativos, software de trabajo, y lenguajes de programación que son empleados para las actividades de la empresa o centro de cómputo y determinar si son los correctos y cumplen con su función.

- Realizar el control y evaluación de las actividades, áreas y funciones de una empresa, utilizando el apoyo sistemas computacionales, programas especiales para auditoría, y del software que nos permite desarrollar auditorías por medio del computador.

1.6 JUSTIFICATIVOS PARA EFECTUAR UNA AUDITORÍA DE SISTEMAS

Entre los principales motivos por los cuales se puede iniciar una auditoría de sistemas se pueden definir los siguientes:

- Realizar evaluaciones sobre el uso de los recursos financieros que son utilizados dentro del centro de cómputo, ya sea para la adquisición o mantenimiento de equipos e instalaciones.
- Aumento considerable e injustificado del presupuesto.
- Desconocimiento en el nivel directivo de la situación informática en la empresa.
- Falta total o parcial de seguridades lógicas y físicas que garanticen la integridad del personal, equipos e información.
- Descubrimiento de fraudes efectuados con el uso del computador.
- Falta de una planificación informática.
- Organización que funciona incorrectamente debido a falta de normas, estándares, autoridad y adecuada administración del recurso humano.
- Descontento general de los usuarios, incumplimiento de los plazos y mala calidad.
- Falta de documentación o inadecuada que dificulta dar mantenimiento.

1.7 Control interno informático

El control interno dentro de toda organización permite salvaguardar los bienes de la empresa, también es de gran utilidad al momento de desarrollar las actividades para que estas sean realizadas con eficiencia, eficacia y confiabilidad dentro de la empresa. Es por ello que profundizaremos un poco en lo que es el control interno informático, pero antes definiremos algunos conceptos esenciales para comprender el control interno informático de mejor manera.

1.7.1 Definición de control

"Se define al control como el conjunto de disposiciones metódicas, cuyo fin es vigilar las funciones y actitudes de las empresas, para ello permite verificar si todo se realiza conforme a los programas adoptados, órdenes impartidas y principios admitidos" [3]

La función de control nos permite determinar que se está llevando acabo cuantificándolo y evaluándolo, para luego establecer si es necesario aplicar medidas correctivas de manera que la ejecución se realice conforme a lo establecido.

1.7.2 Objetivos del control

El control es de vital importancia para las empresas y sus objetivos estarán en función del tipo de institución en el que se apliquen y más aún si es a un área específica. De forma general podemos decir que los objetivos del control son:

- Establecer políticas, estándares y procedimientos, medir su cumplimiento y evaluar el alcance real con los planes y programas.

- Salvaguardar los bienes y recursos de la empresa

- Permite llevar acabo de forma correcta el cumplimiento de las funciones, actividades y operaciones de la empresa.

- Nos permite establecer que se está llevando de forma incorrecta para tomar las medidas correctivas apropiadas.

[3] Wellington Ríos, Auditoría Informática, Editorial Corporación Edi-Ábaco 1994, Pág. 30.

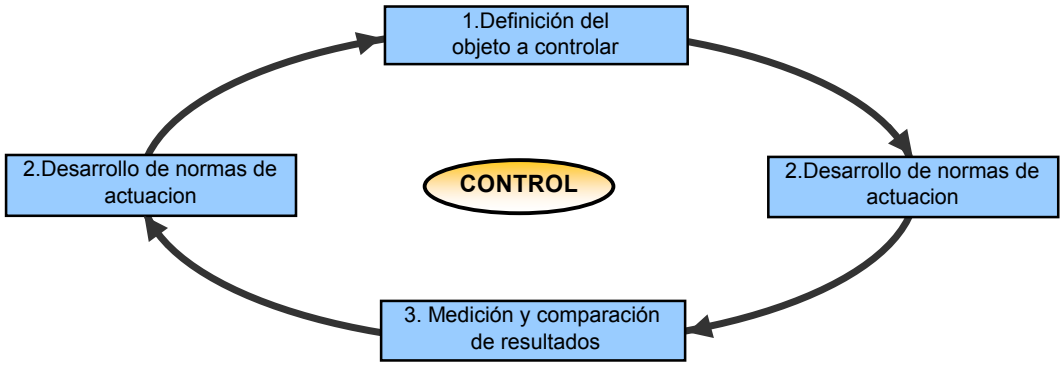
1.7.3 Estructura del control

Podemos decir que el control está definido por cuatro elementos básicos que son:

1. **Definición del objeto a controlar.-** que puede ser una característica cuantificable.
2. **Desarrollo de normas de actuación.**- que nos permitirán establecer el medio por el cual podamos medir las características o el objeto.
3. **Medición y comparación de resultados.**- aquí mediremos los resultados obtenidos con las normas establecidas para determinar las diferencias que pueden existir.
4. **Corrección de errores o inconsistencias.-** un medio para efectuar los cambios de tal forma que podamos acoplarlos a las necesidades o normas de actuación

Podremos establecer los elementos y estructura del control en la siguiente figura que nos permitirá ver de mejor manera lo que hemos expuesto:

Figura 1.1. Estructura del control



Fuente: Autores de la Tesis

1.7.4 Clasificación de los controles

Como se indicó antes el control es el elemento principal para proteger los recursos de una empresa y dentro de toda auditoría el objetivo principal es evaluar estos controles. A continuación presentamos la clasificación de los controles según varios puntos de vista:

a. Por su función

1. **Preventivos:** Controles o acciones que tienen como fin evitar que se lleven acabo las amenazas. Tienen como fin evitar que un hecho se produzca.

2. **Detectivos:** Como su nombre lo indica son los que van encontrar o detectar si existe alguna amenaza.

3. **Correctivos:** Son controles que se ejecutan cuando se ha realizado una amenaza, y evitar que continué. Es decir eliminar los riesgos cuando se ha producido una amenaza.

4. **Recuperativos:** Son las medidas encargadas de eliminar todas las consecuencias de los riesgos producidos.

b. Área de aplicación

1. **General:** Son los que se aplican a toda la empresa, o conjunto de sistemas operativos.

2. **Particular:** Son los que se aplican a un conjunto determinado de áreas, sistemas, recursos o elementos en la empresa, y que tienen algo en común.

3. **Individual:** Son los que se aplican a un determinado sistema, área, recurso o proceso dentro de la empresa

c. Por su estado

1. **Activo o implantado:** Son los controles o medidas que están en funcionamiento en la empresa y que fueron aceptadas por los administradores.

2. **Por Aplicar o implantar:** Controles o medidas a poner en práctica, por lo general se definen al dar los dictámenes o resultados de la auditoría y tienen como una característica el establecer una fecha máxima para su puesta en práctica o funcionamiento.

3. **Descartado o eliminado:** Son los controles o medidas que estuvieron implantados y que luego de su evaluación, se decide dejar de utilizar.

1.8 El control interno informático

Para entender mejor que es y como funciona el control interno informático, veremos a continuación algunas definiciones.

1.8.1 Definición de control interno

"El control interno es una función de la gerencia que tiene por objeto salvaguardar y preservar los bienes de la empresa, evitar desembolsos indebidos de fondos y ofrecer la seguridad de que no se contraen obligaciones sin autorización"[4]

Se entiende por sistema de control interno al conjunto de políticas, estándares y procedimientos de control establecidas por la empresa cuya función es proveer una seguridad razonable en el logro de una adecuada organización administrativa y eficiencia operativa, confiabilidad de los reportes que fluyen de sus sistemas de información, apropiada identificación y administración de los riesgos que enfrenta.

[4]Carlos Muñoz Razo. Auditoría de Sistemas Computacionales. Editorial Prentice Hall 2002 Pag. 106

1.8.2 Control interno informático

Una vez establecido la definición de control interno y establecido la importancia en la gestión administrativa de la empresa, ya sea tanto para el desarrollo correcto de las actividades y funciones, así como para preservar la integridad de sus bienes y recursos, es muy importante definir cuales son los objetivos más importantes que pretendemos alcanzar. Por lo que podemos decir que el control interno informático tiene como fin los siguientes objetivos[5]:

- Garantizar la confiabilidad, seguridad y protección de la información de los sistemas de información así como también de todos los recursos informáticos de la empresa.
- Establecer, ejecutar y controlar el cumplimiento de políticas, estándares y procedimientos necesarios para satisfacer los requerimientos de la empresa en cuanto al área informática, así como también, para el correcto y eficiente desarrollo de las funciones y actividades de la empresa.
- Establecer procedimientos y métodos que permitan el diseño e implementación adecuado de los sistemas de cómputo, para proporcionar información confiable y garantizar que todos los procesos se realicen de forma eficiente y eficaz.

Tomando en cuenta estos objetivos, a continuación plantemos los elementos fundamentales del control interno informático[6] más importantes que vamos a estudiar y estos son:

- Controles internos sobre la organización del área de informática.
- Controles internos sobre el análisis, desarrollo e implementación de sistemas.
- Controles internos sobre la seguridad del área informática.

[5] Carlos Muñoz Razo. Auditoría de Sistemas Computacionales. Editorial Prentice Hall 2002 Pag. 107
[6] Carlos Muñoz Razo. Auditoría de Sistemas Computacionales. Editorial Prentice Hall 2002 Pag. 135

1.8.3 Controles internos a la organización del área informática

Este elemento del control interno informático, tiene como fin determinar si la estructura y organización del área de sistemas es la adecuada para el correcto funcionamiento de las actividades y funciones en la empresa. Esto solo puede ser posible si existe un diseño adecuado de los siguientes elementos:

- La estructura de puestos
- Unidades de trabajo
- Líneas de autoridad
- Canales de comunicación
- Definición correcta de funciones y actividades
- Definición clara de los puestos de trabajo

Es por ello que a continuación se presentan los subelementos que conforman este elemento del control interno y estos son:

Dirección.

Es la función primordial dentro de la empresa que tiene por objetivo dirigir y coordinar las actividades en la misma o en un área específica, así como también la distribución equitativa de los recursos.

Para aprovechar de la mejor manera posible los recursos informáticos es importante establecer como elemento del control interno a la dirección, con lo cual se contribuye a la adecuada coordinación del uso y aprovechamiento de esos recursos. Para ello la dirección debe tener en cuenta los siguientes subelementos:

- **Coordinación de recursos**: Trata de distribuir y asignar de manera correcta los recursos informáticos disponibles, para que sean equitativos y productivos.

- **Supervisión de Actividades**: Esta a cargo de quien dirige el área de sistemas, y tiene que vigilar el que se realicen de forma correcta las actividades y funciones en el área de sistemas, evaluando el cumplimiento adecuado de los objetivos en esta área.
- **Delegación de autoridad y responsabilidad**: Su finalidad es obligar al personal del área a cumplir con las tareas y operaciones que tienen a su cargo.
- **La asignación de actividades**: Se la usa cuando se tiene una definición clara y concreta de todas las funciones y tareas de cada puesto, para cumplir con los objetivos del área de sistemas.
- **Distribución de recurso**: Consiste en distribuir equitativamente todas los recursos informáticos para que los empleados cumplan de eficientemente con las tareas que tengan encomendadas.

División del trabajo.

La división del trabajo incrementa la eficiencia y eficacia en las actividades de cualquier empresa, por esta razón es necesario dividir las actividades en áreas cada vez más especializadas con el fin de obtener tareas muy concretas y específicas.

A continuación se presentan las funciones básicas que cualquier centro de cómputo[7].

- Dirección general del área de informática: Es la entidad encargada de planear, organizar, dirigir y controlar los objetivos, actividades y presupuesto del área de informática.
- Área de análisis y diseño: Unidad encargada de estudiar las necesidades de procesamiento e información de la empresa.
- Área de programación: Unidad responsable de realizar todas las actividades que se requieren para codificar los programas.
- Área de sistemas de redes: Encargado de la administración, control, manejo y mantenimiento de la red informática de la empresa.

[7]Carlos Muñoz Razo. Auditoría de Sistemas Computacionales. Editorial Prentice Hall 2002 Pag. 106

- Área de operación: unidad encargada de la operación, procesamiento y uso de los sistemas computacionales.
- Área de telecomunicaciones: Unidad responsable de llevar a cabo todos los servicios de comunicación, ya sean internos o externos a la empresa (Internet, red a área local).

Asignación de responsabilidad y autoridad.

Este elemento tiene como función establecer las líneas de autoridad y limites de responsabilidad que tendrá cada puesto, incluyendo los canales formales de comunicación. Con esto garantizamos que el control interno del área de sistemas, y por ende el procesamiento de información de sistemas sea eficaz y eficiente.

Establecimiento de estándares y procedimientos.

Es importante la estandarización de todas las actividades y funciones del área de sistemas, para lograr que estas se realicen conforme a las necesidades concretas de las unidades informáticas que componen la empresa. A fin de que estas actividades se realicen de forma uniforme y homogénea.

Estos estándares y procedimiento deben estar encaminados concretamente a las siguientes operaciones y actividades que se realizan en el área de sistemas:

- Al diseño, instalación y adquisición del Software y Hardware.
- Al uso de los equipos, componentes y periféricos.
- En lo referente a los sistemas de redes se deben establecer estándares y procedimientos al diseño, instalación, configuración y aprovechamiento de los sistemas instalados en la empresa, así como a todos los recursos de red.
- En lo referente al software, al mantenimiento, modificación parcial o total de los sistemas informáticos de la empresa.

- Estándares a los sistemas de seguridad y protección del personal y usuarios, así como también a los equipos y sistema de cómputo en general.

Perfiles de puestos.

Esta función del control interno, nos permitirá identificar y definir los requisitos, habilidades, experiencia, nivel de estudio y conocimientos específicos que deberá tener el personal para ocupar un puesto específico de trabajo en el área de sistemas.

La definición de los perfiles de puesto de trabajo, permitirán a los auditores, determinar si la selección de personal que ocupa los puestos es la adecuada. Por lo cual la información básica que se debe contemplar en el perfil de puesto es la siguiente[8]:

Figura 1.2. Contenido básico de un perfil de puesto

Nombre genérico del puesto
Objetivo del puesto
Líneas de autoridad:
    Dependencia de …
    Responsabilidad sobre …

Funciones del puesto:
    Sustantivas, básicas o fundamentales
    Específicas, concretas o cotidianas

Requisitos del puesto:
    Conocimientos
        En sistemas
        En áreas similares
    Otros conocimientos del puesto

Experiencia
    En el puesto
    En el área

Características de personalidad
Otros requerimientos
Otros conocimientos

Fuente: Auditoría en Sistemas Computacionales

[8] Carlos Muñoz Razo. Auditoría de Sistemas Computacionales. Editorial Prentice Hall 2002 Pag. 145

1.8.4 Controles internos para el análisis, desarrollo e implementación de sistemas

Como ya sabemos las actividades que se realizan para el análisis, diseño e implementación de sistemas de cualquier empresa son únicas y por tanto, no tienen parecido alguno con otras actividades. Para entender este elemento del control interno, presentaremos las principales fases del análisis y diseño de sistemas. Por lo cual proponemos una metodología general para el desarrollo de sistemas la misma que consta de los siguientes puntos:

- Análisis del sistema actual.
- Diseño conceptual.
- Diseño detallado.
- Programación.
- Prueba de correcciones.
- Documentación del sistema.
- Capacitación de usuarios.
- Implementación del sistema.
- Liberación del sistema.
- Mantenimiento.

El uso de esta metodología requiere de un seguimiento paso a paso, para de esta forma garantizar el correcto análisis, desarrollo e implementación de cualquier sistema.

A continuación se indican los subelementos necesarios para el cumplimiento de este elemento de control interno:

- Estandarización de metodologías para el desarrollo de proyectos.
- Asegurar que el beneficio del sistema sea óptimo.
- Elaborar estudios de factibilidad del sistema.
- Garantizar la eficiencia y eficacia en el análisis y diseño del sistema.
- Vigilar la efectividad y eficacia en la implementación y mantenimiento del sistema.
- Lograr un uso eficiente del sistema por medio de su documentación.

Estandarización de metodologías para el desarrollo de proyectos

Como sabemos existen múltiples metodologías de aplicación general para el desarrollo de sistemas, por lo cual es importante que la empresa adopte alguna en especial que sea acorde al desarrollo de sus proyectos.
La utilización de esta metodología garantizará la uniformidad en la aplicación de cualquier sistema y ayudará a obtener la máxima eficiencia en el uso de los recursos informáticos, por esta razón, es de suma importancia estandarizar el desarrollo de los proyectos en una empresa.
Para esto debemos uniformar los métodos y procedimientos establecidos en la unidad de sistematización, a fin de estandarizar el desarrollo de sistemas, de tal manera que los nuevos proyectos que se realicen en empresa siempre se lo hagan de la misma manera.

Asegurar que el beneficio del sistema sea óptimo.

Consiste en hacer un más eficiente y eficaz el desarrollo de las actividades que normalmente se llevan a cabo en la empresa o en cualquiera de sus áreas.
La optimización del sistema no se refiere exclusivamente a las aplicaciones informáticas, sino también a la optimización del equipo con el cual se desarrolla su función; por ejemplo, periféricos, bases de datos, etc.
El objetivo final que se espera en las empresas que implementan un sistema informático nuevo, se lo puede ajustar a dos aspectos concretos:

- Beneficios Tangibles**:** Es poder medir las mejoras que presentan las personas que utilizan el sistema, como por ejemplo una mayor emisión de facturas en la empresa, más y mejores registros contables por jornada, etc. Todos estos resultados son tangibles, debido a que se pueden cuantificar para determinar si se cumple o no con los objetivos esperados del sistema.

- Beneficios Intangibles**:** son los beneficios que se esperan obtener de los sistemas de cómputo intangibles, es decir los resultados no lo podemos

contar; sin embargo, existen formas de hacer su cuantificación, ya que la mayoría de los sistemas tienen ciertos valores cualitativos, por ejemplo, la oportunidad en la toma de decisiones con la ayuda de los sistemas computacionales, la confiabilidad de los resultados, etc.

Elaborar estudios de factibilidad del sistema.

Dentro de un plano más concreto, en cuanto al análisis y diseño de sistemas, todo proyecto informático tiene que ser evaluado desde los puntos de vista de la viabilidad[9] y la factibilidad[10]. Se debe contemplar en estos factores los puntos de vista operativo, económico, técnico y administrativo para poder valorar la optimización del nuevo sistema.
El resultado final de estas valoraciones será la certificación de que el proyecto será aplicable a las necesidades de la empresa, para así satisfacer los requerimientos de control interno informático.

Garantizar la eficacia y eficiencia en el análisis y diseño del sistema.

Debemos entender que un nuevo proyecto se justifica si con él podemos satisfacer la eficiencia y eficacia de las actividades de la empresa, lo cual se logra con la adopción de una metodología estándar para el desarrollo de sistemas.
Para garantizar la eficiencia y eficacia en la implementación de un nuevo sistema es necesario contar con varias herramientas, técnicas, métodos y elementos que permitan uniformar los procedimientos, estándares, normas, y lineamientos requeridos para desarrollo de estas actividades.

Vigilar la efectividad y eficiencia en la implementación y mantenimiento del sistema.

Es importante vigilar la efectividad en la implementación del sistema, y una vez liberado, también se debe procurar su eficiencia a través del mantenimiento.

[9] Viable: "Del francés **viable**, de vie: existencia. Que pueda realizarse".
[10] Factible: "Del latín **factibilis,** de facere: hacer. Que es posible de realizar".

No basta con sólo elaborarlo si no tiene que ser implementado completamente, tiene que ser liberado por el usuario y se tiene que dar mantenimiento permanente para garantizar su efectividad.
La vida estimada de un proyecto informático es de seis a ocho años, por ésta razón es de suma importancia no sólo desarrollar eficientemente el análisis y diseño del nuevo sistema, sino también implementarlo de manera adecuada y darle constante mantenimiento ya sea de carácter preventivo o correctivo.

Lograr un uso eficiente del sistema por medio de su documentación.

Una vez terminado de desarrollar un sistema, es indispensable elaborar los documentos que contengan las características de operación, técnicas operativas, administrativas y económicas que lo fundamentaron, con los manuales de apoyo al usuario y con todos los demás manuales que sirvan de apoyo al propio desarrollador del sistema. Con esto garantizaremos el buen funcionamiento del sistema y aseguraremos una mejor operación y utilización del mismo.

Existen muchos tipos de documentos útiles para el usuario y desarrollador del sistema, entre más importantes tenemos:

- Manuales e instructivo del usuario: son documentos que sirven de guía para el usuario, encontraremos las instrucciones básicas del sistema, guía de operación, términos más usados, etc.

- Manual e instructivo de operación del sistema: en este documento encontraremos los pasos a seguir para la operación normal de sistema, incluyendo el detalle del manejo de los equipos.

- Manual técnico del sistema: es un documento especializado en el que se indican todos los aspectos técnicos que se deben considerar para el adecuado manejo del sistema, estos suelen indicar las características especiales sobre funcionamiento técnico de los sistemas.

- Manual para el seguimiento del desarrollo del proyecto: en este documento el desarrollador plantea todas las acciones y tareas que se realizan en el análisis, desarrollo, programación e implementación del sistema.

- Manual e instructivo del mantenimiento del sistema: es un complemento al documento anterior, aquí se presentan las actualizaciones, preventivas o correctivas, que van surgiendo durante la vida activa del proyecto.

- Otros manuales e instructivos del sistema: estos son de apoyo, y sirven para conocer el funcionamiento del nuevo sistema, contemplando todos los aspectos que ayudan al desarrollador y al usuario a conocer todas sus características, comportamiento, componentes y todos los aspectos esenciales que ayudan a su buen funcionamiento.

1.8.5 Controles internos sobre la seguridad del área de sistemas

Un aspecto esencial dentro del área de sistemas y sobre todo del control interno, es la seguridad, la cual está encaminada a la protección de los recursos informáticos y personal que labora en el área informática.
Para lograr esto se debe implementar medidas tanto preventivas como correctivas, además es muy importante el establecimiento y ejecución de planes de contingencia.

Dependiendo del elemento y su función dentro de la empresa, continuación definimos los diferentes tipos de seguridad que podemos tener dentro de la empresa:

- Seguridad física: Son todas las medidas necesarias para salvaguardar los elementos o bienes físicos de la empresa y sobre todo del área de cómputo como son periféricos y equipos, mobiliario de oficina, etc.

- Seguridad lógica: Son todas las medidas necesarias para salvaguardar, proteger y acceder a la información, programas y archivos de la empresa. Es decir a la protección de todos los elementos intangibles de la empresa. Dentro de esta se contempla todo lo referente a respaldos de información sobre todo de base de datos y el control de acceso a la misma, con el fin de evitar pérdida o alteración de la misma.

- Seguridad de operación: Se refiere a las seguridades a tomar en cuenta al momento en el que se utilizan los programas por parte del personal, así como también de los usuarios que acceden a la información y bases de datos. Aquí también se contemplan las seguridades al momento de utilizar los equipos, mobiliario, etc.

- Seguridad del personal de informática: Se refiere a las seguridades que brindan las instalaciones para el personal que labora en el centro de cómputo, así como también del personal que esta en contacto con el sistema.

- Seguridad de las telecomunicaciones y redes: Tiene que ver con las seguridades y protección de los niveles de acceso, privilegios, recepción y envío de información, así como también garantizar, la comunicación y transmisión de la información dentro y fuera de la empresa, por medio de equipos, protocolos o software disponible.

- Prevención de riesgos y planes de contingencia: Se refiere con todas las acciones para prevenir y controlar los riesgos posibles, y determinar planes en caso de que estos riesgos se produzcan en la empresa. Estas acciones y planes están encaminadas a la prevención de accidentes de los equipos, perdida o daño de información, planes para prevención en caso de incendio, uso de extintores, etc. También la realización de planes preventivos y simulacros para determinar si son correctos y verificar que todo el

personal que labora en la empresa tenga conocimiento de las mismas.

A continuación estableceremos los elementos del control interno informático que nos permitan garantizar la seguridad de los sistemas de información, entre los que podemos citar tenemos:

Controles para prevenir y evitar amenazas, riesgos y contingencias en a las áreas de sistematización.

Este elemento es de gran utilidad para identificar y establecer los controles que ayuden a prevenir los riesgos y amenazas dentro del ambiente del área de sistemas. Para prevenirlos antes de que ocurran, controlarlos cuando estén ocurriendo o corregirlos después de que suceden. Para esto es necesario identificar primero cuales son los elementos que pueden infringir seguridades en las instalaciones, información, equipos y del personal que labora, para identificar estas eventualidades.

A continuación se presentan algunos tipos de controles que se pueden aplicar a las áreas de sistematización para evitar riesgos y amenazas a los sistemas y recursos informáticos de la empresa.

- Control de accesos físicos del personal al área de cómputo
- Control de accesos al sistema, base de datos, programas e información.
- Niveles de privilegios para acceso, nombres de usuario y claves.
- Identificación de riesgos y amenazas para el sistema.
- Simulacros, planes de contingencia y bitácoras

Controles para la seguridad física del área de sistemas

Al aplicar este tipo de controles se busca proteger los activos tangibles de la empresa, desde el punto de vista informático, todo lo referente a equipos,

periféricos, suministros y mobiliario de cómputo, así como también proteger la integridad del personal y usuario que labora en el centro de cómputo.

Entre algunos controles de este tipo presentamos los más importantes, cabe recalcar que cada empresa es responsable de aplicar los controles de acuerdo a sus necesidades:

- Inventario del hardware, mobiliario y equipos.
- Bitácoras de mantenimiento de los equipos.
- Asignación de equipos y documentación del mismo.
- Controles de acceso para el personal.
- Contratos de actualización y mantenimiento de hardware.
- Control a las conexiones eléctricas del departamento de cómputo.

Controles para la seguridad lógica de los sistemas

Son los procedimientos, medidas preventivas y correctivas a adoptar para salvaguardar los bienes lógicos de la empresa, es decir la información, programas, sistemas operativos, etc.

Entre algunos controles podemos citar los siguientes:

- Controles de acceso al sistema y al a información.
- Dígitos verificadores y cifras de control.
- Palabras clave de accesos
- Seguimiento de secuencias y rutinas lógicas del sistema.

Controles para la seguridad de las bases de datos

No esta demás decir que el activo más importante para toda empresa es su información, de ahí que es de vital importancia definir los controles preventivos, correctivos y de recuperación de información que nos permitan proteger la información de posibles alteraciones, perdidas, robo o uso

inadecuado de la misma. Estos controles pueden permitir a la administración monitorear quien accede al sistema y que información utiliza para proteger la información. Eventualmente se pueden producir percances que pueden dañar la información como son los desastres naturales de ahí que se deba proteger la información por medio de respaldos periódicos de la base de datos y procesos de recuperación de la misma. Entre los controles que podemos citar tenemos los siguientes:

- Respaldos periódicos de información.
- Planes y programas para la recuperación de la información.
- Control de acceso a las bases de datos.
- Rutinas de monitoreo y evaluación de operaciones relacionadas con la base de datos

Controles para la seguridad en la operación de los sistemas computacionales

Estos controles nos permiten establecer las medidas preventivas para evitar accidentes, actos dolosos o fraudulentos que pueden producirse al momento de realizar las actividades en la empresa. Entre los controles que podemos citar tenemos los siguientes:

- Controles para procedimientos de operación.
- Controles para el procesamiento de información.
- Controles para la emisión de resultados.
- Controles para almacenamiento de información.
- Controles para seguridad del personal de informática.

Controles para la seguridad del personal informático

Dentro del centro de cómputo el personal informático y los usuarios son el recurso más importante, ya que son quienes diseñan, implementan y usan los programas, procesan la información y la almacenan, es por ello que se deben establecer controles que permitan salvaguardarlos, con ello se logra un mejor desempeño de sus actividades.

Entre los controles más importantes tenemos:

- Planes y programas de capacitación
- Controles administrativos de personal
- Seguros de vida y fianzas para el personal

Controles para la seguridad en la telecomunicación de datos y sistemas de redes

El establecimiento de los controles para este elemento, dependerá mucho de los protocolos, medios de comunicación y equipos utilizados, y sobre todo al modo de transmisión utilizado. En el caso de las redes dependerá del tipo de red a utilizar que puede ser desde una red de área local (LANs) hasta una red de área mundial (WANs) para lo cual se deberá tomar en cuenta como está instalada, al número de terminales y tipos de conexión. Para lo cual el auditor deberá establecer los controles adecuados en base a las características antes mencionadas utilizadas en la telecomunicación de datos.

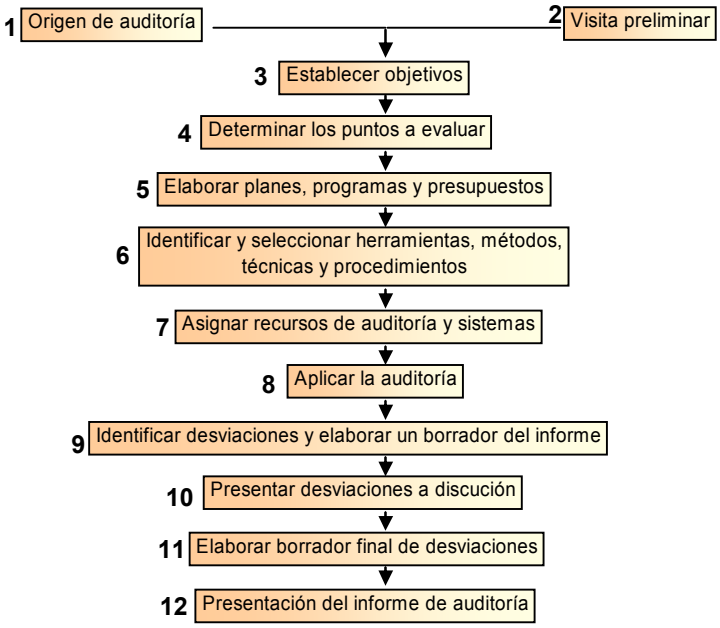
1.9 Metodología para realizar auditorías de sistemas

Para realizar una auditoría ya sea de sistemas o una auditoría de cualquier área es necesario, seguir una serie de pasos, procesos o acciones específicas, los cuales deberán ser llevados de una manera secuencial, ordenada y cronológica.

En caso de realizar cualquier tipo de auditoría de sistemas, los métodos o procedimientos a ejecutar, dependerá de las necesidades y técnicas de evaluación del área a auditar. A continuación se presentan los pasos a seguir para realizar una auditoría[11]:

[11] Carlos Muñoz Razo. Auditoría de Sistemas Computacionales. Editorial Prentice Hall 2002 Pag. 181

Figura 1.3. Pasos para realizar una auditoría



Fuente: Auditoría de sistemas computacionales

Estos pasos a seguir de forma general, para realizar una auditoría nos permitirán definir una metodología específica para realizar auditorías de sistemas o a cualquier área de informática.

1.9.1 Definición de la metodología

La metodología tiene 3 etapas y estas son:

1. **Etapa:** Planeación de la auditoría de sistemas computacionales
2. **Etapa:** Ejecución de la auditoría de sistemas computacionales
3. **Etapa:** Dictamen de la auditoría de sistemas computacionales

Estas etapas o pasos son la base de la metodología que nos permitirá realizar cualquier tipo auditorías de sistemas, a continuación se realizará una definición de cada etapa y de la forma de realizar cada una de ellas.

1.9.1.1 Primera etapa: Planeación de la auditoría de sistemas

Es el paso inicial para realizar cualquier auditoría de sistemas computacionales, y consiste en realizar un plan de las actividades necesarias para la ejecución. Lo que pretendemos alcanzar en esta etapa es lo siguiente: [12]

- Identificar las razones para realizar la auditoría.
- Determinación del objetivo de la auditoría.
- Identificación y diseño de los métodos, procedimientos y técnicas para llevar a cabo la auditoría.
- Determinación y preparación de documentos que servirán de apoyo a la auditoría.
- Elaboración del plan, programa y presupuesto para la auditoría.

El responsable de la auditoría debe determinar para que se realiza la misma, también si se deberá realizar una visita previa y por último los objetivos que se pretende alcanzar con la auditoría.

Para esta etapa debemos tener en cuenta los siguientes puntos:

P.1 Identificar el origen de la auditoría

Es el primer paso a realizar en toda auditoría en el área de sistema, y consiste en determinar porque necesidad o causa se realiza la auditoría, para lo cual debemos cuestionarnos para que y por que se requiere hacer una auditoría de sistemas en la empresa o área de la misma. Con ello el auditor tendrá claro hacia donde encaminar la planeación de la auditoría y de que manera realizar la revisión.
Entre las posibles causas por la cual se puede realizar una auditoría de sistemas tenemos las siguientes:

[12] Carlos Muñoz Razo. Auditoría de Sistemas Computacionales. Editorial Prentice Hall 2002 Pag. 187

- Por solicitud expresa de procedencia interna; es decir por solicitud de alguien que pertenece a la empresa por ejemplo gerente, socios, jefe de un área de la empresa, etc.
- Por solicitud expresa de procedencia externa; cuando se realiza la petición de una auditoría por parte de alguien ajeno a la empresa, tiene el carácter de obligatorio cuando es realizado por alguna autoridad.
- Consecuencia de emergencias y situaciones especiales
- Por riesgos y contingencias informáticas que puedan afectar al personal y/o a los recursos informáticos.
- Como resultado de los planes de contingencia para determinar su efectividad.
- Por resultados de otras auditorías.
- Por que se requiere en los programas integrales de auditoría que puede tener la empresa.

P.2 Realizar una visita preliminar al área a evaluar

Este es el segundo paso dentro de esta primera etapa de planeación de la auditoría, que es de gran importancia para el auditor y se debe realizar antes de iniciar formalmente la auditoría. Esta visita preliminar tiene como finalidad inicial el contacto con el personal que labora en el área a auditar y conocimiento de las funciones y cargo que ocupan, conocer las instalaciones en la cual se va a llevar a cabo la auditoría, determinar como se encuentra distribuido los sistemas, local y equipos dentro del área a auditar. A demás permitirá observar las medidas de seguridad visibles que existen y establecer a simple vista la problemática que se va a evaluar.

P.3 Establecer los objetivos de la auditoría

El tercer paso es determinar los posibles objetivos que se pretenden alcanzar con la auditoría. Para ello es muy importante realizar los dos pasos anteriores, para determinar claramente lo que se pretende lograr.

Los objetivos se pueden establecer de la siguiente manera:

Objetivo general
Es el fin global o total que se busca obtener con la auditoría.

Objetivos particulares
Son los fines individuales que se pretende alcanzar con la auditoría, ya sea de un área específica o función particular. Están de acuerdo con las necesidades concretas de la evaluación.

Objetivos específicos
Es la determinación en forma más detallada de lo que se busca alcanzar con la auditoría de sistemas, para ello se deberá indicar concretamente los áreas, sistemas, elementos o componentes concretos a ser evaluados y la forma de cómo se va ha realizar.

P.4 Determinar los puntos que serán evaluados en la auditoría

Para realizar este punto dentro de la etapa de planeación es necesario haber establecido ya los objetivos de la auditoría para en base a ellos determinar lo que se quiere evaluar. Es muy importante este paso ya que al definir los elementos a ser evaluados podremos determinar luego las herramientas y la manera en la que realizaremos la auditoría.

Cabe recalcar que este paso dentro de la planeación es de suma importancia para el auditor, ya que este es resultado de un análisis previo al realizar la visita preliminar y establecer los objetivos, ya que aquí se definirá

como se pretende satisfacer estos objetivos y a su vez como realizar la auditoría.

Al establecer los puntos que serán evaluados se deberá tomar en cuenta varios factores, que influirán de forma directa en la selección de dichos puntos entre los principales tenemos, las necesidades de la empresa y el equipo de auditoría, características y conocimientos del auditor, métodos y procedimientos a utilizar en la auditoría, sistemas operativo y equipos, etc.

Los puntos a ser evaluados pueden ser agrupados en los siguientes grupos:

- Evaluación de funciones, actividades, áreas y unidades administrativas del centro de cómputo.
- Evaluación de la seguridad de los sistemas de información.
- Evaluación de los sistemas, equipos, instalaciones y componentes.
- Evaluación de los recursos humanos del área de sistemas.
- Evaluación del hardware y/o software.
- Evaluación de la información y base de datos
- Personal del área que será evaluada.
- Apoyo de los sistemas y equipos técnicos e informáticos
- Recursos económicos

P.5 Elaborar planes, programas y presupuestos para realizar la auditoría

Una vez defino lo que vamos a evaluar, ahora realizaremos la planeación formal de la auditoría para ello deberemos establecer:

- Los documentos que contemplen los planes para el desarrollo de la auditoría.
- Los programas donde se definan las etapas, actividades, acciones, tiempos y responsables para cumplir con los objetivos propuestos.

- Los presupuestos de la auditoría que serán documentos que nos permitan determinar los costos y el tiempo de los recursos que serán utilizados dentro de la auditoría.

Para realizar este paso dentro de la etapa de planeación debemos seguir los siguientes pasos:

a. Elaborar el documento formal de los planes de trabajo para la auditoría.

Aquí se elabora de forma específica y precisa los planes de trabajo a ejecutar para realizar la auditoría de sistemas computacionales. Estos planes se presentarán dentro de un documento llamado "*Plan de auditoría de sistemas*"[13] que contendrá toda la información sobre la ejecución de la auditoría a realizar, como son las actividades, tiempos, responsables y recursos, información sobre los auditores que van a participar, especificaciones del programa de auditoría.
Este documento deberá tener los siguientes elementos:

1. Carátula de identificación, que tendrá el siguiente formato:

Figura 1.4. Carátula de identificación

Fuente: Auditoría de Sistemas Computacionales

[13] Carlos Muñoz Razo. Auditoría de Sistemas Computacionales. Editorial Prentice Hall 2002 Pag. 214

2. Índice de contenido, para una revisión rápida con nombre del contenido y página.
3. Definición de objetivos
4. Delimitación de estrategias para el desarrollo de la auditoría
5. Plan de auditoría
6. Definición de políticas, normas y estándares para el desarrollo de la auditoría.

b. Contenido de los planes para realizar la auditoría.

Aquí se detallan las tareas a realizar y que estarán plasmados dentro del documento "Plan de auditoría de sistemas" para lo cual se considerarán los siguientes aspectos:

1. Definir los objetos finales de la auditoría.
2. Establecer las estrategias para realizar la auditoría.
3. Diseñar las etapas, eventos y tareas.
4. Calcular la duración de estas etapas y tareas
5. Distribuir los recursos entre las etapas, tareas y eventos

c. Elaborar el documento formal de los programas de auditoría.

Por lo general es de forma gráfica, y se definen las actividades, responsable y tiempo que tendrán durante la auditoría tal como se muestra en el siguiente ejemplo:

Figura 1.5. Ejemplo de un programa de auditoría

AUDITORIA DE SISTEMAS COMPUTACIONALES

Vigencia	DD | MM | AA
del	28 | 03 | 05
al	31 | 04 | 05

Empresa: Universidad del Azuay
Auditor: Ing. Jorge Espinoza
Periodo: 01 al 16 de marzo de 2005
Area auditarda: Centro de cómputo

PLAN DE AUDITORIA DE SISTEMAS

ACTIVIDAD			SEMANAS						
Nº	NOMBRE	RESPONSABLE	1	2	3	4	5	6	7
1	Elaborar plan de auditoría	Dpto. Asignado							
2	Preparación de instrumentos de evaluación	Resp. Auditoria							
3	Iniciar auditoría	Aud. Asignados							
4	Auditar la seguridad del centro de computo	Aud. Senior 1							
5	Auditar sistemas de cómputo	Aud. Senior 2							
6	Auditar al personal informático	Aud. Senior 3							
7	Auditar el software de los equipos	Aud. Senior 4							
8	Auditar el hardware	Aud. Senior 5							
9	Presentar borrador de informe	Resp. Auditoria							

Fuente: Auditoría de Sistemas Computacionales

d. Elaborar los programas de actividades para realizar la auditoría.

Este punto se establecerá por escrito, y se elabora con lo anterior ya que es una parte integral del documento de planeación, y contendrá los siguientes puntos:

1. Definir de manera precisa las etapas de la auditoría
2. Identificar de forma concreta y detallada todos los eventos que se llevarán a cabo en cada etapa de la auditoría
3. Delimitar lo más claramente posible las actividades, tareas y acciones para cada etapa
4. Distribuir los recursos para las diferentes etapas y para los eventos y actividades que hay en las mismas.
5. Calcular el tiempo o duración de las etapas, actividades y tareas planeadas para la auditoría

e. Elaborar los presupuestos para la auditoría.

Esta tarea se contempla con lo anterior y se define los recursos a utilizar en el plan con información referente al costo y tiempo de utilización.

P.6 Establecer los métodos, procedimientos y herramientas a utilizar

En esta paso de determinarán los documentos y medios por los cuales se llevará acabo la revisión de los puntos a ser evaluados, por medio del diseño de los métodos, procedimientos y herramientas necesarios, establecidos en los planes y programas definidos para la auditoría.

P.7 Asignar los recursos para la auditoría

En este paso distribuimos y asignamos los recursos tanto humanos, tecnológicos y materiales a las distintas etapas definidas en el plan de auditoría.

1.9.1.2 Segunda etapa: Ejecución de la auditoría de sistemas computacionales

Esta etapa como su nombre lo indica es la de ejecución de todo lo planeado en la etapa anterior. Para lo cual se tendrá que llevar a cabo los siguientes pasos para cumplir con esta etapa:

E.1 Realizar las acciones programadas para la auditoría

Los auditores deberán realizar las actividades que están en el programa de auditoría, conforme fueron diseñadas, en el tiempo establecido y utilizando los recursos correspondientes para la misma con el fin de cumplir los objetivos.

E.2 Aplicar los instrumentos y herramientas de evaluación

Consiste en ejecutar los instrumentos y herramientas elegidos para realizar la evaluación (entrevistas, encuestas, etc.), para realizar la recopilación de información que luego será analizada.

E.3 Identificar y elaborar los documentos de desviaciones encontradas

Luego de recopilar la información el auditor deberá analizar y detectar las posibles anomalías encontradas y elaborar un informe, con las pruebas necesarias.

E.4 Elaborar el dictamen preliminar o borrador

Una vez encontradas anomalías el auditor debe elaborar un documento en el que se especifique las desviaciones detectas, y junto a este informe un comentario de las personas que tienen relación con estas desviaciones, establecer las causas y posibles soluciones para cada una de estas causas. Si desea el auditor puede definir responsables para solucionarlas e incluso plazos para hacerlo.

El auditor también deberá integrar a este documento el conjunto de papeles de trabajo utilizados para realizar la auditoría, así como todos los documentos utilizados, a fin de que pueda demostrar las observaciones encontradas.

1.9.1.3 Tercera etapa: Dictamen de la auditoría de sistemas computacionales

El último paso o etapa a cumplir por parte del auditor es el de elaborar o emitir un dictamen final sobre el resultado de la auditoría de sistemas realizada, para lo cual debe seguir o realizar los siguiente pasos:

D.1 Analizar la información y elaborar un informe de desviaciones detectadas

Esta es una tarea paralela que se realiza con la detección de desviaciones, al momento de realizar el borrador como se indico en el paso E.4 del postulado anterior.

Luego de comentarlas y realizar las modificaciones pertinentes, deberá elaborar el informe definitivo a presentar, con las situaciones encontradas.

Las actividades a realizar son:

1. Analizar los papeles de trabajo
2. Señalar las situaciones o desviaciones encontradas de forma específica.
3. Comentar las situaciones encontradas con el personal del área afectada.
4. Realizar las modificaciones necesarias
5. Elaborar un documento de situaciones relevantes

D.2 Elaborar el dictamen final

Una vez que se realizó el informe de auditoría de sistemas, el auditor debe agregar a este el dictamen final o la opinión del auditor.

D.3 presentar el informe de auditoría

El último paso consiste en presentar el informe y dictamen de auditoría a la alta directiva de la empresa, para dar a conocer los resultados obtenidos. Cabe recalcar que esta presentación debe ser de carácter formal y deberá contener los siguientes elementos:

1. La carta de presentación
2. El dictamen final de auditoría
3. El informe de situaciones relevantes, que contendrá la información de todas las desviaciones detectadas
4. anexos y cuadro adicionales, aquí se incorpora todos los papeles de trabajo utilizados en la auditoría

1.10 Los papeles de trabajo para auditoría

Una de las características fundamentales de la auditoría de sistemas informáticos, es el registro eficiente de la información que el auditor va recolectando durante su evaluación.

Para ello tiene que recopilar los datos obtenidos durante la auditoría y registrarlos formalmente en documentos conocidos como papeles de trabajo, los cuales pueden ser: documentos, gráficas, disquetes, o cualquier otro medio escrito o magnético, en los cuales se van anotando los hechos, pruebas, interpretaciones, así como análisis de los datos obtenidos durante la revisión. Con todo lo anterior, el auditor tendrá un apoyo para confirmar los hechos y validar la información que utilizará como base para elaborar el informe de auditoría.

Es necesario reiterar que el auditor elabore estos documentos o registros electromagnéticos para asentar todo lo que encuentre durante su revisión.

Existen múltiples formas de elaborar y utilizar los papeles de trabajo de una auditoría de sistemas informáticos, las cuales estarán determinadas por la

experiencia, conocimientos y habilidades del auditor, así como por su necesidad de usar estos documentos.

Para que los papeles de trabajo o medios de captura se puedan admitir como soporte documental de una auditoría de sistemas, y para que se utilicen para fundamentar los resultados y opiniones que presenta el auditor, es necesario que, tanto en su diseño como en su uso, reúnan ciertos requisitos y formalidades, los mismos que serán determinados previamente por la empresa encargada de realizar la auditoría, o auditor responsable de llevarla a cabo.

1.10.1 Contenido de los de papeles de trabajo

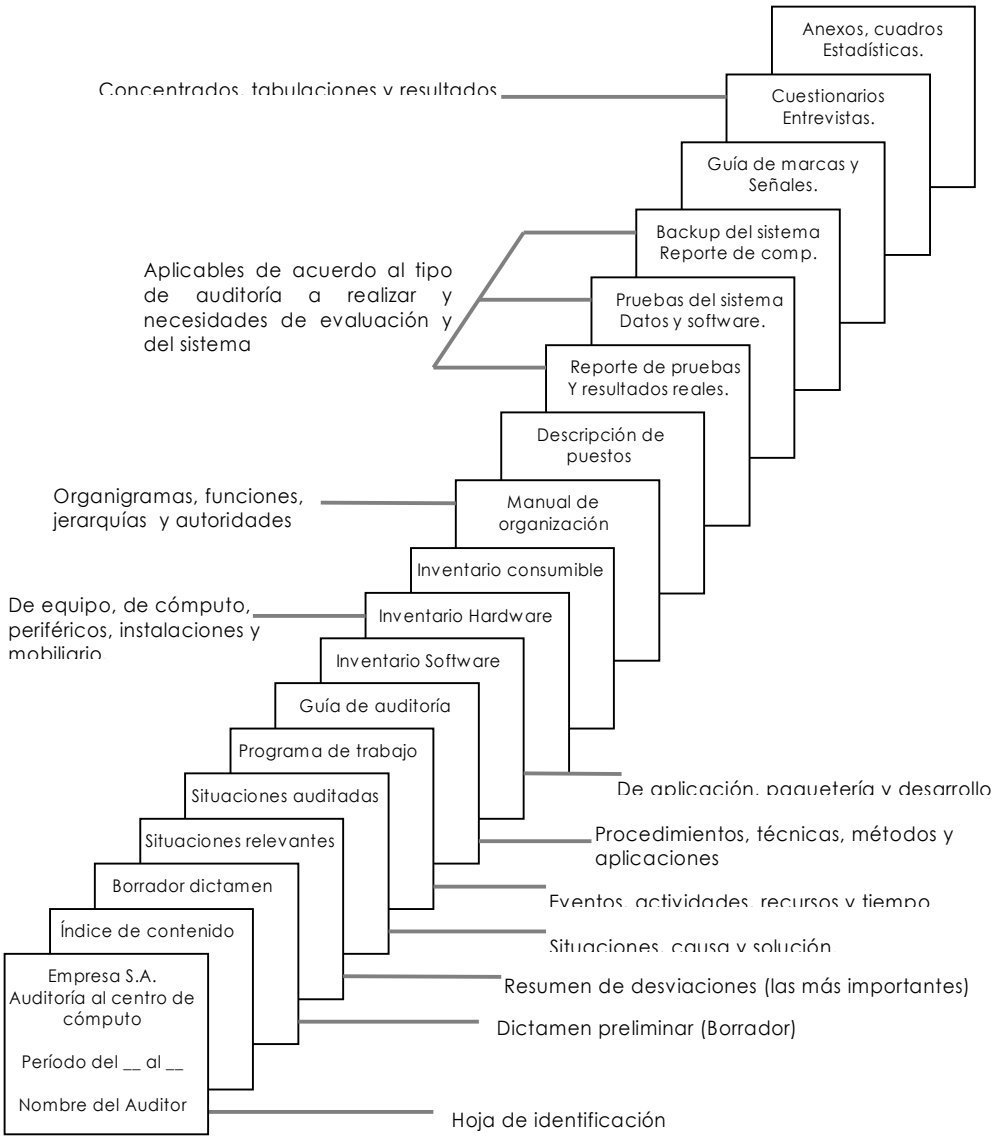
A continuación intentaremos dar una idea precisa de la cantidad mínima de documentos con la que se podrán integrar los papeles de trabajo del auditor de sistemas; también proyectamos señalar como sugerencia un criterio de orden y conservación para los papeles de trabajo de la auditoría de sistemas.

El conjunto de papeles de trabajo, por su naturaleza y contenido, es el aspecto fundamental para elaborar el dictamen de la auditoría, y su uso es confidencial y exclusivo del auditor de sistemas, debido a que éste va integrando en estos papeles, los documentos reservados y de uso exclusivo de la empresa, mismos que recopila durante su revisión y los complementa con los registros, en papel o en medios electromagnéticos, que obtiene como evidencias formales de alguna desviación en el área de sistemas que es auditada.

El contenido de los papeles de trabajo puede variar de un auditor a otro y de un tipo de auditoría a otra, ya que en cada trabajo existen procedimientos, técnicas y métodos de, evaluación especiales que hacen diferente la recolección de los documentos.

A continuación presentaremos un ejemplo del contenido de estos documentos, los cuales varían de acuerdo con las necesidades de información del auditor:

Figura 1.6. Papeles de trabajo



Fuente: Auditoría de Sistemas Computacionales

- Hoja de identificación.

  Ésta es la parte frontal y el primer documento formal que se identifica del conjunto de papeles de trabajo de la auditoría de sistemas informáticos, esta hoja puede ser una carátula formal rigurosamente empastada o

una simple portada de cartón o de papel común y corriente, se anotan los datos elementales que sirven para identificar la documentación contenida en el legajo.

Esta portada debe contener como mínimo los siguientes datos:

- *Nombre de la empresa responsable de llevar a cabo la auditoría de sistemas.*- Donde se anotan el nombre y logotipo de la empresa.
- *Identificación del conjunto de papeles de trabajo.*- Aquí va el nombre genérico que se le da al documento y sirve para identificar que se trata de la concentración de los documentos que avalan la realización de la auditoría de sistemas.
- *Nombre de la empresa o área de sistemas auditada.*- Aquí se coloca el nombre completo de la empresa y el área de sistemas en la cual se practica la auditoría.
- *Periodo en que se realizó la auditoría.*- En este lugar se anota la fecha de inicio de la auditoría y su terminación.
- *Puesto y cargo del responsable de realizar la auditoría.*- Aquí se anota el nombre completo del responsable de llevar a cabo la auditoría.
- *Fecha de emisión de] dictamen final.*- Es la fecha en la que se, presenta por escrito el dictamen final de auditoría.

- Índice de contenido de los papeles de trabajo.

En esta parte se hace la descripción detallada y se enumera el contenido total de los papeles de trabajo, con el propósito de identificar rápidamente la página en donde se encuentra cada una de las partes que integran este conjunto de papeles.

No existe ninguna forma especial de presentarlo, la única condición es que sea una presentación ordenada y que se identifiquen claramente las páginas y su contenido.

Como sugerencia de debería numerar con siglas cada capítulo de la auditoría, seguidas de un número consecutivo que vuelva a iniciar en cada parte; por ejemplo: SI-001 (Seguridad Informática - hoja 001).

También sugerimos utilizar los siguientes apartados para los documentos de trabajo:

HW: Para la documentación relacionada con el equipo físico, periféricos y demás equipos de sistemas.

SW: Para la documentación relacionada con el software y paqueterías.

SG: Para la documentación relacionada con la seguridad informática.

BD: Para la documentación relacionada con las bases de datos, información y demás archivos de datos.

DS: Para la documentación relacionada con el análisis, diseño y desarrollo de sistemas.

IS: Para la documentación relacionada con las instalaciones del área de sistemas.

CC: Para documentación relacionada con el centro de cómputo.

CA: Para la documentación relacionada con la gestión administrativa del centro de cómputo.

CM: Para la documentación relacionada con los consumibles del área.

- Dictamen preliminar (borrador).

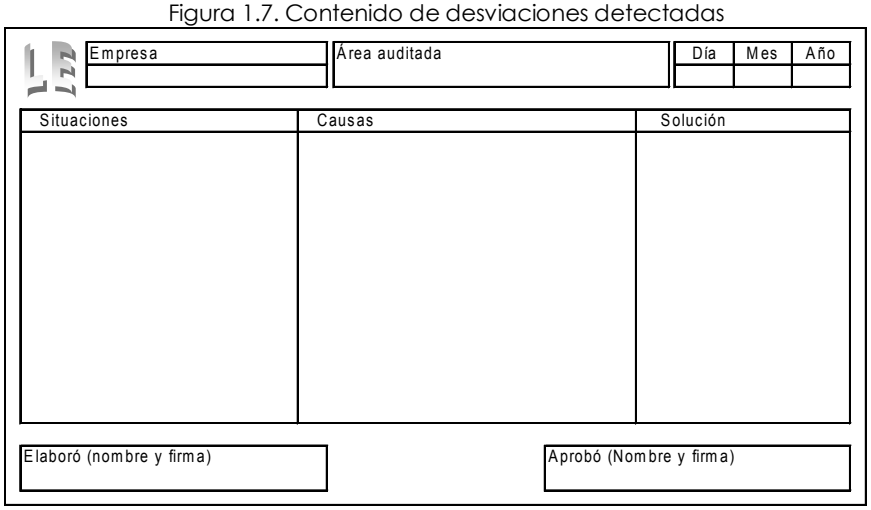
El auditor utiliza esta sección para conservar, como papeles de trabajo, un resultado preparatorio de la evaluación del área evaluada, a fin de hacer el análisis y consulta posteriores de todos los aspectos que presentó en forma de borrador, además de utilizarlo como soporte en aclaraciones posteriores y preparar el informe final.

- Resumen de desviaciones detectadas (las mas importantes).

Otro de los documentos importantes que debe conservar en la auditoría es la copia de los documentos originales, y en algunos casos el borrador manuscrito, de las desviaciones que considera como las más importantes encontradas durante la revisión, así como sus causas y

posibles soluciones. Este documento se lo presenta en el formato que se indica a continuación.

Figura 1.7. Contenido de desviaciones detectadas

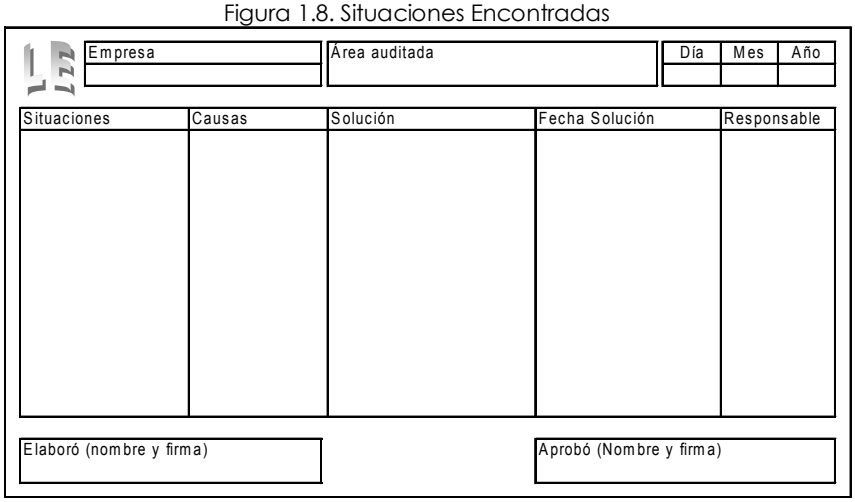


Fuente: Auditoría de Sistemas Computacionales

- Situaciones encontradas (situaciones, causas o soluciones).

Aquí se presentan los manuscritos, y en ocasiones los borradores mecanografiados, de todas las situaciones detectadas durante la auditoría, separando en situaciones encontradas, las causas que las originan y las posibles soluciones; también se anota al responsable de solucionarlas y las fecha de solución para cada causa o situación reportada, conforme se describe en el formato que presentarnos a continuación.

Figura 1.8. Situaciones Encontradas



Fuente: Auditoría de Sistemas Computacionales

- Programa de trabajo de auditoría.

  Es un documento escrito en el que constan los planes, programas y presupuestos hechos para el control y desarrollo de la auditora; este documento se elabora en un formato especial o en una gráfica en la cual se anotan las etapas y actividades para la evaluación, así como los tiempos para llevarla a cabo; también se anotan los recursos disponibles para realizar todas esas actividades. Estos aspectos se deben señalar en forma cronológica, secuencial y correctamente, coordinada.

- Guía de auditoría.

  Este documento, es primordial para el buen desarrollo de una auditoría, por esta razón, debe tener una descripción detallada de todos y cada uno de los puntos importantes que se deben auditar, según las necesidades de evaluación y características específicas del área de sistemas de la empresa. A continuación mostramos un ejemplo:

Figura 1.9. Contenido básico de un perfil de puesto

Referencia	Actividad o Función a evaluar	Técnica de evaluación	Ponderación	Calificación	Observaciones
G-01	Evaluar, la organización del area de sistemas de la empresa, sus puestos, funciones	Revisión documental de manual de organización. Entrevistas con empleados	0.05%		

Fuente: Auditoría de Sistemas Computacionales

- Inventario de software.

  Es un documento esencial dentro de los papeles de trabajo, aquí constará el inventario de los programas, lenguajes, paqueterías, sistemas operativos y cualquier otro software que se utilice en la institución para el procesamiento de la información y la operación de los sistemas.

En el documento que, se muestra a continuación se debe anotar la versión del software, las licencias para su uso y o general todas sus características, así como a los responsables de su resguardo:

Figura 1.10. Contenido básico de un perfil de puesto

					Fecha		
					DD MM AA		**Hoja**
					20 Nov 05		12 de 20
	Empresa: LE importaciones.						
	Período: 01-nov-05 al 30 nov-05						
	Responsable: Juan Perez.						
REF	**Software**	**Versión**	**No. Inventario**	**Licensias**	**Presentación**	**Asignado a**	**Localización**
W01	Win 2003	Server	09 234-1	2	Cd-Rom	C.Cómputo	Servidor
W02	Office	2003	09 234-2	1	Cd-Rom	C.Cómputo	Finanzas
W02	Office	2003	09 234-3	1	Cd-Rom	C.Cómputo	Contabilidad

Fuente: Auditoría de Sistemas Computacionales

- Inventario de hardware.
- Inventario de consumibles.
- Manual de organización.
- Descripción de puestos.
- Reportes de pruebas y resultados.
- Respaldos de datos, disquetes y programas de aplicación.

Los sistemas computacionales tienen características específicas en cuanto a la forma de captura, almacenamiento y emisión de información; por esta razón, encontramos que el respaldo de documentos es muy importante en una auditoría de sistemas computacionales. Estos documentos de trabajo, que contienen información importante, se pueden archivar en disquetes, cintas, Cd-Roms, DVDs o en algún otro medio electrónico.

Estos papeles de trabajo son importantes debido a la forma en que se, archiva la información en ellos, sin embargo, no solo es por la forma de

almacenar la información, sino también la cantidad, periodicidad y utilidad de la información que va a ser documentada.

- Respaldos de las bases de datos y de los sistemas.

  Es el respaldo periódico de información que se hace a través de disquetes (o cualquier otro medio), en los cuales se almacenan los datos de algún ejercicio, operación, o cualquier otra serie de datos que es importante conservar. El auditor de sistemas debe decidir cómo conservar esta información como parte de su evaluación.

  El auditor debe también verificar que existan respaldos (periódicos o únicos) de los sistemas operativos, programas, paqueterías o sistemas realizados en la empresa, con en el objeto de evaluar que, dichos respaldos sean los adecuados en caso de ocurrir problemas en el sistema.

- Cuadros y estadísticas de información.

  Este punto se refiere a todo lo relacionado con los cuadros estadísticos que utiliza el auditor para recabar y evaluar la información obtenida en la evaluación; en estos cuadros se incluyen las gráficas, datos, censos, muestras, formulas estadísticas, etc. Es de suma importancia para el auditor archivar estos cuadros en el conjunto de papeles de trabajo, ya que serán de gran ayuda para acreditar sus opiniones.

- Anexos de recopilación de información.

  Además de la información estadística, el auditor puede obtener otro tipo de información que lo es útil para realizar la evaluación de los sistemas computacionales, misma que puede ser muy variada y que debe guardar como anexos de información. A continuación presentamos algunos ejemplos de estos anexos:

- Resultados del procesamiento de datos.
- Descripción de puestos, funciones y actividades
- Copias de formatos y licencias de, programas y paqueterías.
- Mapas de distribución de redes, instalaciones, equipos, muebles y sistemas de información.
- Bitácoras *de* reportes y servicios de mantenimiento preventivo y correctivo.

- Testimoniales, actos y documentos legales de comprobación y confirmación.

  En algunos casos, estos documentos pueden ser de los más importantes en una auditoría de sistemas, debido a que son el testimonio de empleados, usuarios, responsables o de las personas que por algún motivo declararon algo relacionado con los sistemas auditados o con alguna situación especifica.

1.10.2 Claves del auditor par marcar papeles de trabajo

Son las marcas de carácter informal que utiliza exclusivamente el auditor o el grupo de auditores que realizan la auditoría, con el fin de facilitar la uniformidad de los papeles de trabajo y para identificarlos mejor.

Así, cuando alguien del grupo de auditores encuentra algún documento con estas marcas, sabe que éste ya ha sido revisado o que tiene una característica especial en la cual se tiene que advertir alguna observación, de acuerdo con el significado de los símbolos.

También ayudan al auditor a realizar un resumen de observaciones para identificar de manera rápida y sencilla las posibles desviaciones. Además le permite estandarizar su trabajo, siempre y cuando sean las mismas para toda la revisión.

Con el uso de, estas marcas se hace más sencilla la revisión de documentos impresos en papel, de disquetes, bases de datos y de todo lo relacionado con los sistemas evaluados.

No existe algún convenio formal respecto al tipo de marcas utilizadas entre un auditor y otro, sin embargo, por sentido común se unifican las marcas o símbolos que se utilizan en los papeles de trabajo. Entre estas marcas destacan las siguientes:

Figura 1.11. Marcas para papeles de trabajo.

Símbolo	Significado	Símbolo	Significado
	Verificado una vez		Archivo verificado
	Verificación dos veces		Archivo conerrores
	Dato correcto		Verificacion den pantalla
	Dato con error		Transmición interrumpida
	Pendiente de revisar	*com*	Comentario especial
	Revisado	**OBS**	Observación
¿ ?	Confirmar Preguntas	*EE*	Entrevista empleado
!!	Observaciones importantes	*EF*	Entrevista funcionario
ERR	No Coinciden Datos	*EU*	Entrevista usuario
VIR	Virus Datos contaminados	*EP*	Emtrevista personal
ENT	Entrevista	*CUES*	Cuentionario

Fuente: Auditoría de Sistemas Computacionales

Es importante recalcar que los símbolos, anteriormente presentados únicamente sirven como referencia y ejemplo a seguir, y que son producto de la experiencia en la aplicación de auditorías de sistemas.

1.10.3 Cuadros, estadísticas y documentos concentradores de información.

En esta parte se presentan todos los documentos del conjunto de papeles de trabajo que son complemento de alguna revisión y sirven para identificar y comprobar desviaciones y situaciones.

Dichos documentos pueden ser estadísticas, gráficas o cuadros en los cuales se concentran y se comparan datos tales como listados de

resultados de un proceso, operaciones y tareas que se realizan con un sistema computacional, así como información estadística, las bitácoras de seguimiento y reportes, etc.

A continuación indicaremos algunos de los documentos que deben ser considerados en este tema:

- *Cuadros estadísticos.*

  Es un cuadro en donde se anotan datos útiles tales como operaciones aritméticas, matemáticas y/o estadísticas que le darán algún significado a la evaluación.
  A continuación se muestra un ejemplo que consta de un cuadro en el que se anota el consumo de horas de impresión semanales de las impresoras de las diferentes áreas de una empresa. Con el análisis de estos datos se podrían optimizar las impresoras mediante una red con impresoras compartidas, etc.

Figura 1.12. Ejemplo de cuadro estadístico.

Consumo de horas de impresión por semana					
Tipo de impresora	**Departamento de contabilidad**	**Departamento de finanzas**	**Departamento de Ventas**	**Departamento de Diseño**	**Totales**
Epson LX-300	5	6	8	1	20
Epson FX-810	19	10	4	1	34
Láser Xerox	2	4	4	25	35
Láser HP	2	4	2	20	28
Totales	28	24	18	47	117

Fuente: Autores de la Tesis

- *Cuadro de comparación de información.*

  Es un cuadro, en el que se comparan los resultados contra parámetros normales previamente definidos. Esta comparación nos dará un criterio de evaluación para esos rangos.

A continuación presentaremos un ejemplo de una tabla en la que se hace la comparación de tiempo programado de impresión contra el tiempo real.

Figura 1.13. Ejemplo de cuadro de comparación de información

Tiempo Consumo vs Tiempo Programado							
Tipo de impresora	**Departamento de contabilidad**	**Departamento de finanzas**	**Departamento de Ventas**	**Departamento de Diseño**	**Totale Área**	**Tiempo Programado**	**Direrencia**
Epson LX-300	5	6	8	1	20	40	-20
Epson FX-810	19	10	4	1	34	40	-6
Láser Xerox	2	4	4	25	35	45	-10
Láser HP	2	4	2	20	28	150	-122
Totales	26	20	16	27	89	125	-36
Tiempo Asignado	30	30	30	70	160		
Diferencia	-4	-10	-14	-43	-71		

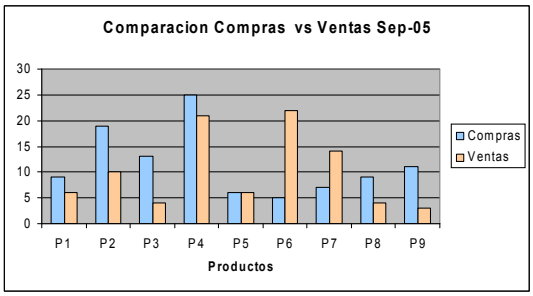
Fuente: Autores de la Tesis

- *Gráficas.*

Es la representación gráfica de la información que proporciona un valor significativo a los datos. Tiene como propósito representar los datos en forma visual.

En el ejemplo que mostraremos a continuación se representa los ingresos contra consumos, a fin de señalar la llamada oferta y demanda.

Figura 1.14. Ejemplo de gráficas.



Fuente: Autores de la Tesis

1.10.4 Diagramas de Sistemas

Es la representación gráfica del procedimiento que se sigue para realizar una serie de operaciones y actividades debidamente coordinadas entre sí.

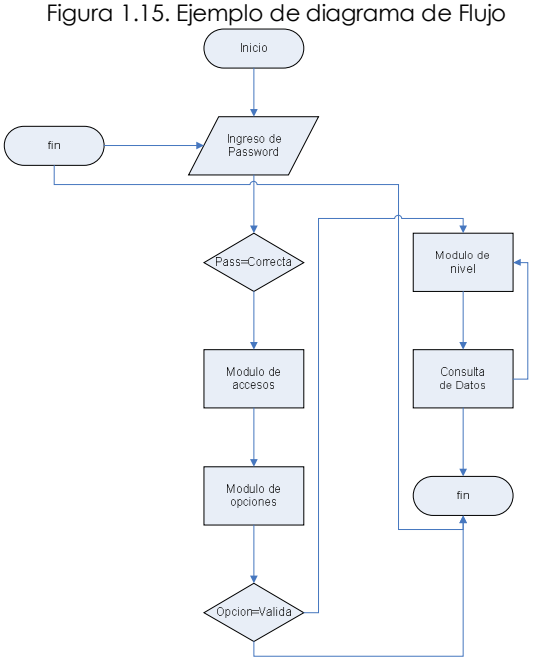
En el ambiente de sistemas, este diagrama es la representación gráfica de un procedimiento el cual está representado por líneas de flujo y símbolos que representan algún tipo de actividad, documento o de una decisión.

- *Diagramas de Flujo.*

  En este tipo de diagramas se señalan los procedimientos; por medio de símbolos los mismos que indican el flujo que siguen los datos.

  El uso de los diagramas de flujo es una de las principales herramientas que utiliza un auditor para la evaluación de programas, bases de datos, programación de sistemas de la empresa, debido a que permito seguir perfectamente los datos.

Figura 1.15. Ejemplo de diagrama de Flujo



Fuente: Autores de la Tesis

- *Diccionario de Datos*.

  Éste es otro de los documentos importantes para el auditor, ya que le ayuda a identificar el contenido y composición de las bases de datos, su forma, el tamaño de los archivos, el número de dígitos por cada registro que ingresa a la computadora y demás características que componen una base de datos.

  A continuación se muestra un ejemplo en el que se observa un diccionario de datos que contiene la identificación del campo, su descripción, el tipo de datos que admite y el tamaño de los datos que ingresan.

Figura 1.16. Ejemplo de diccionario de datos

CAMPO	TIPO	TAMAÑO	DESCRIPCIÓN
Cmater	Carácter	5	Clave del material.*
Cusuario	Carácter	5	Clave del usuario.*
Fprestam	Numérico	6	Fecha del préstamo.*
Flímite	Numérico	6	Fecha limite de entrega.*
Fentrega	Numérico	6	Fecha de devolución del préstamo.
Xedopres	Caráctar	9	Estado de préstamo: prestado, perdido
Crespons	Carácter	3	Iniciales de la persona que modificó el registro por última vez.*

Fuente: Autores de la Tesis

- *Modelos.*

  Estos documentos son muy importantes en la evaluación de los sistemas computacionales, ya que ayudan al auditor a representar la realidad de lo que va a evaluar. Estos modelos no son más que la abstracción gráfica de la realidad que el analista o programador conceptualiza y plasmas en un documento.

  En la figura que mostramos a continuación se muestra las principales características de cualquier modelo utilizado en la programación orientada a objetos, incluyendo la descripción de los procedimientos presentados.

Figura 1.17. Ejemplo de modelo de evaluación de sistemas

Análisis	Procesos	De flujo de datos
	Gráficas de Transformación	
	Datos	Entidad-Relaciónn Modelado de datos Estructura de datos Estructura lógica
	Estado-Evento	Estado de Transición Historia de vida de la entidad
Diseno	Diseño	Gráficas de estructura
Las demás no son soportadas		

Fuente: Auditoría de Sistemas Computacionales

1.11 Conclusiones del capítulo

En este capítulo se revisaron varios conceptos importantes sobre la auditoría y que serán de gran ayuda para la mejor comprensión y desarrollo del presente proyecto. Se pudo establecer la definición de auditoría de sistemas y una pequeña relación con la auditoría general. Definimos los objetivos y justificativos para el desarrollo de una auditoría de sistemas.

Establecimos los conceptos básicos del Control y se realizó un análisis sobre el control interno informático así como su importancia y una breve metodología de cómo llevar a cabo este tipo de control para ello se estableció los principales tipos de controles internos para el área de informática.

También se reviso y definió una metodología para el desarrollo de auditorías de sistemas, que permitirán un mejor desarrollo del control y evaluación de cualquier elemento del área de sistemas.

Por último se definieron los principales papeles de trabajo, así como también pudimos establecer un modelo a seguir para la presentación y elaboración de estos papeles de trabajo.

El estudio y desarrollo de este capítulo es gran importancia, en especial el contenido del control interno, ya que es uno de los objetivos a los que esta encaminado este proyecto.

CAPÍTULO 2:

CONOCIMIENTO DE LAS HERRAMIENTAS A UTILIZAR

CONTENIDO

2.1 Introducción al capítulo

En este capítulo se pretende realizar el estudio de las herramientas que se utilizarán para el desarrollo del software a implementar, para obtener los conocimientos necesarios, con el fin de desarrollar el proyecto de la mejor manera posible.

A continuación presentaremos las ventajas y características principales por las cuales hemos escogido a Microsoft SQL Server 2000 como base de datos y a Visual Basic .Net como lenguaje de programación.

Indicaremos cual es el proceso de instalación de dichas herramientas, y realizaremos un estudio de la forma de integrarlas.

2.2 Microsoft SQL Server 2000

Actualmente la manipulación de bases de datos es esencial dentro del manejo de información en las grandes y pequeñas empresas, ya que estas confían su información, en grandes bancos de datos. Este proceso suele ser complicado y toma un tiempo valioso no solo en almacenaje sino además en las consultas.

Microsoft SQL Server 2000 esta diseñado para que los procesos de almacenamiento y consulta de información sean breves y en tiempo real. Cabe destacar que SQL Server 2000 es uno de los mejores manejadores de base de datos a nivel mundial.

2.2.1 Definición

Microsoft SQL Server 2000 "*es un sistema de gestión de base de datos relacionales, que permite como su propio nombre lo indica la gestión de un entorno de base de datos relacional, que abarca, tanto el área de diseño,*

como la administración, proporcionando una interfaz bastante amigable para el usuario " [14]

SQL Server utiliza una extensión al SQL estándar, el cual se denomina Transact SQL lo cual significa que soporta el SQL de ANSI, pero además a adquirido funciones adicionales que no están contempladas en el estándar pero que son exclusivas de SQL Server 2000.

2.2.2 Características

Como se sabe SQL Server ha venido evolucionando rápidamente en los últimos años sobre todo en el entorno remoto y distribuido de base de datos, por lo que podemos mencionar entre sus principales ventajas las siguientes:

Soporte para XML

Xml (Extensible *markup language*), es un meta lenguaje, es decir es un lenguaje utilizado para definir lenguajes, usado sobre todo en el intercambio de datos.

La sintaxis de XML es muy similar a la HTML, es decir que maneja etiquetas que definen la estructura de los datos por ejemplo:

```
<Cliente>
        <Nombre>Juan</Nombre>
        <Apellido>Guerra</Apellido>
        <Dirección>Av. Del ejército</ Dirección >
</Cliente>
```

Microsoft SQL Server es capaz de devolver un conjunto de resultados utilizado este tipo de formato con lo cual facilita el intercambio de datos

[14] Aburto Correa, Pantigoso Silva, Base de datos con SQL Server 2000, Editorial Megabyte, 2001, Pág. 6 -1

Funciones de usuario

Una nueva característica incluida en esta versión, es la de permitir al usuario definir sus propias funciones, con lo cual se podrá ocultar parte de la complejidad que pueda contener una consulta, para la posterior reutilización de la misma, teniendo en cuenta la abstracción para otros usuarios que puedan requerir su uso

Nuevos triggers

Un *trigger* es un procedimiento especial que se ejecuta cuando se cumple una condición dada, por ejemplo al modificar o eliminar datos. SQL Server 2000 soporta dos nuevos tipos de *Triggers*, el INSTEAD OF que sustituye el comportamiento de comandos como i*nsert, update* o *delete*, y AFTER el cual se ejecuta una vez concluida la acción de lo a disparado.

Soporte para consultas distribuidas

SQL Server 2000 posee un optimizador de consultas que ofrece la funcionalidad de ubicar datos en servidores distribuidos dependiendo de valores como el tráfico de red, el nivel de carga de datos, etc., permitiendo que las consultas puedan acceder a distintos servidores para obtener el resultado final.

Seguridad y cifrado de datos

SQL Server 2000 utiliza Kerberos como servidor de autentificación para acreditar el acceso al servidor que se realiza desde el cliente, así como diversas técnicas de seguridad

2.2.3 Instalación

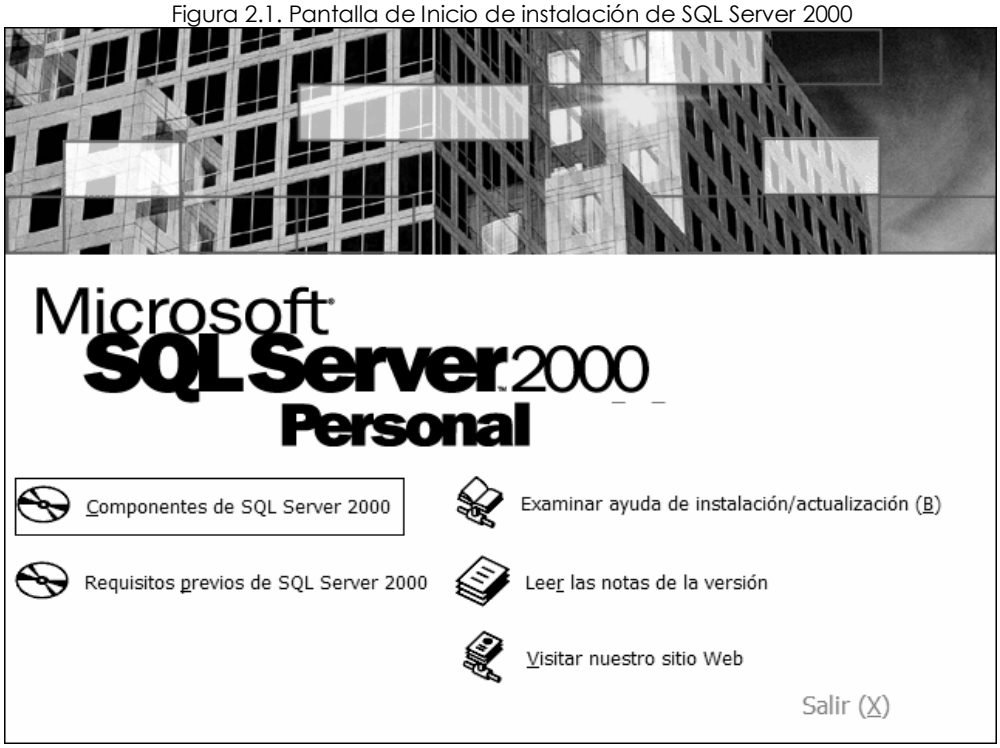
A continuación veremos como se realiza el proceso de instalación de Microsoft SQL Server 2000 Edición Personal y las diferentes opciones que plantea durante el este proceso.

Para empezar introducimos el CD – ROM del programa.
Tenemos dos opciones:

- La estándar, que realiza una instalación completa
- La personal, que muy útil cuando no se dispone de un servidor.

La figura siguiente muestra la pantalla que aparece al introducir el Cd–Rom.

Figura 2.1. Pantalla de Inicio de instalación de SQL Server 2000



Fuente: Autores de la Tesis

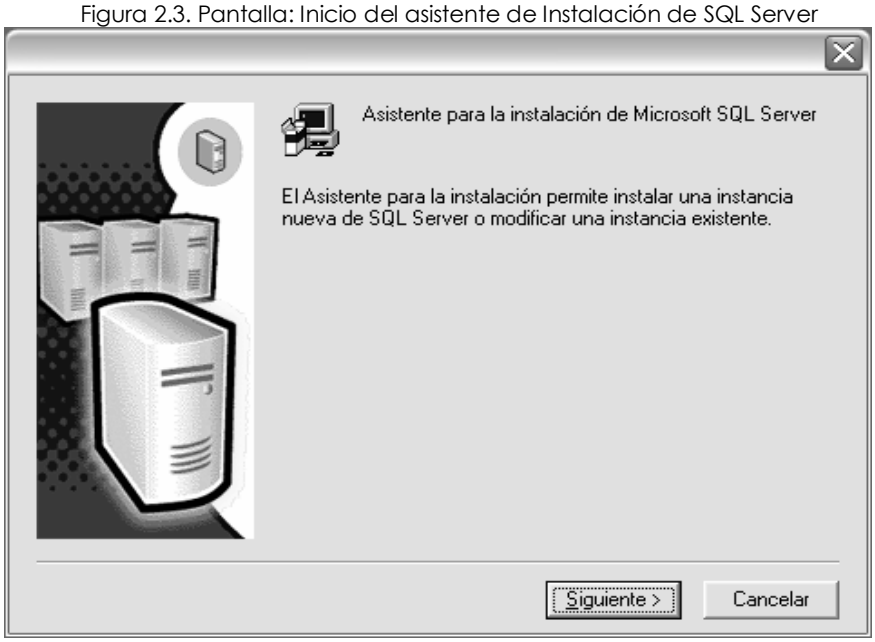
En nuestro caso instalaremos la opción estándar, pulsamos sobre la opción *Componentes de SQL Server 2000*, con lo cual aparece la pantalla siguiente.

Figura 2.2. Pantalla: Instalación de componentes

Fuente: Autores de la Tesis

Al escoger la primera opción se comprobará si disponemos de un servidor, no si no se diera ese caso nos reportará un mensaje en el cual se indica que solo están disponibles los componentes de cliente, pero como la versión que estamos instalando no requiere que se tenga de un sistema operativo servidor, nos mostrara lo que se tiene en la figura 2.3

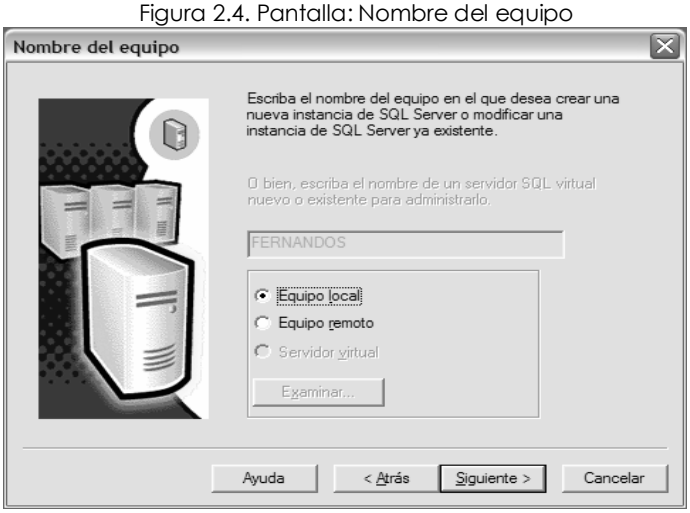
Figura 2.3. Pantalla: Inicio del asistente de Instalación de SQL Server



Fuente: Autores de la Tesis

Nos indica que vamos a iniciar la instalación de una nueva instancia de SQL Server por lo que pulsamos sobre el botón siguiente visualizándose la pantalla que se muestra en la figura 2.4

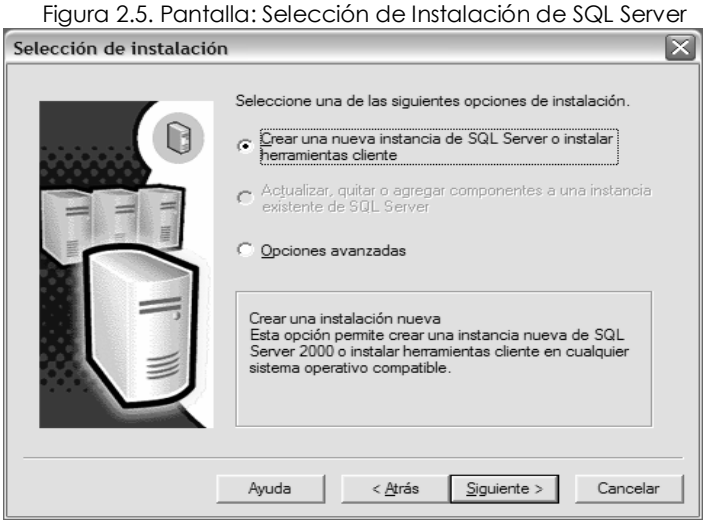
Figura 2.4. Pantalla: Nombre del equipo



Fuente: Autores de la Tesis

Pide el nombre del equipo y la forma de instalación, si es local o remota, si es remota informamos desde que equipo vamos a instalar. Para nuestro caso escogemos la opción *Equipo Local,* y pulsamos el botón siguiente con lo que nos aparecerá la pantalla que se muestra en la figura 2.5.

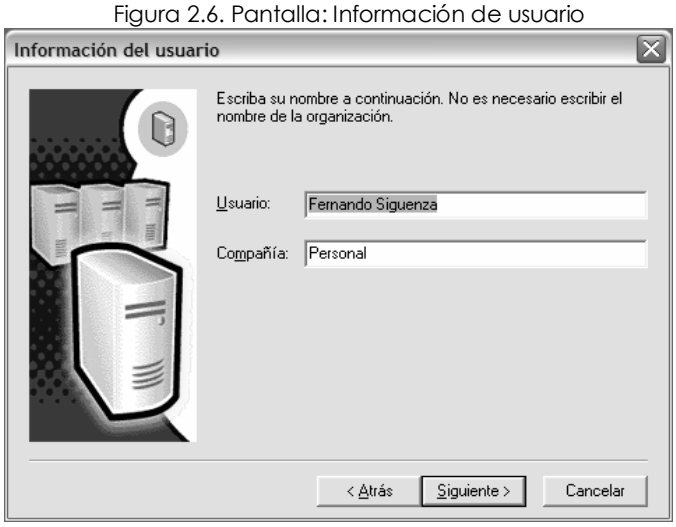
Figura 2.5. Pantalla: Selección de Instalación de SQL Server



Fuente: Autores de la Tesis

Seleccionar una opción de instalación, *instalar una nueva instancia del SQL Server*, instalar las partes clientes u opciones avanzadas donde podremos crear instalaciones desatendidas o reconstruir el registro del SQL Server si estuviera dañado. La opción central solo estará activa si ya tenemos un SQL Server instalado y queremos modificar su instalación, luego al pulsar sobre el botón siguiente se muestra lo que tenemos en la figura 2.6.

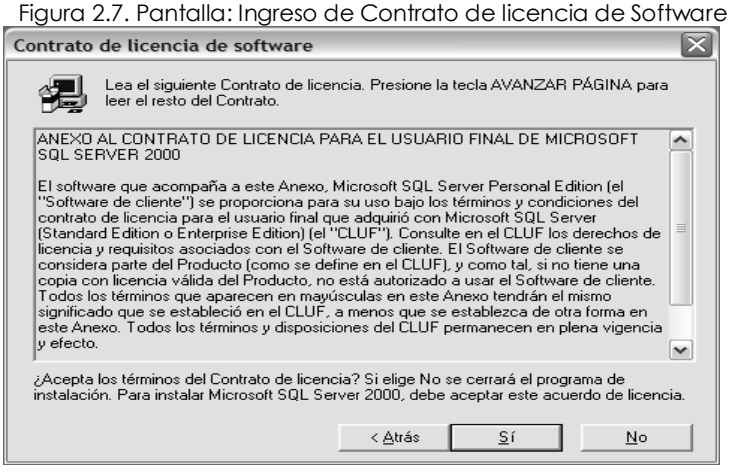
Figura 2.6. Pantalla: Información de usuario



Fuente: Autores de la Tesis

En esta ventana se tiene que ingresar la información del usuario, los campos que se solicitan son el nombre y la compañía. Una vez ingresado la información necesaria pulsamos nuevamente sobre el botón siguiente y nos aparece la siguiente ventana

Figura 2.7. Pantalla: Ingreso de Contrato de licencia de Software

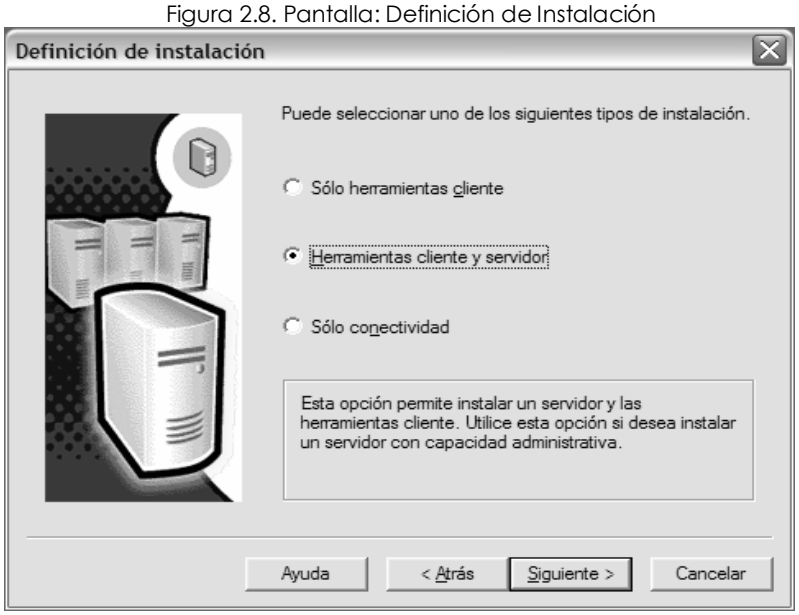


Fuente: Autores de la Tesis

Aquí nos muestra el contrato de licencia, en donde se indican los métodos de uso bajo los términos y condiciones que propone el creador del programa.

Una vez aceptado el contrato nos aparecerá la pantalla que se muestra en la figura 2.8

Figura 2.8. Pantalla: Definición de Instalación

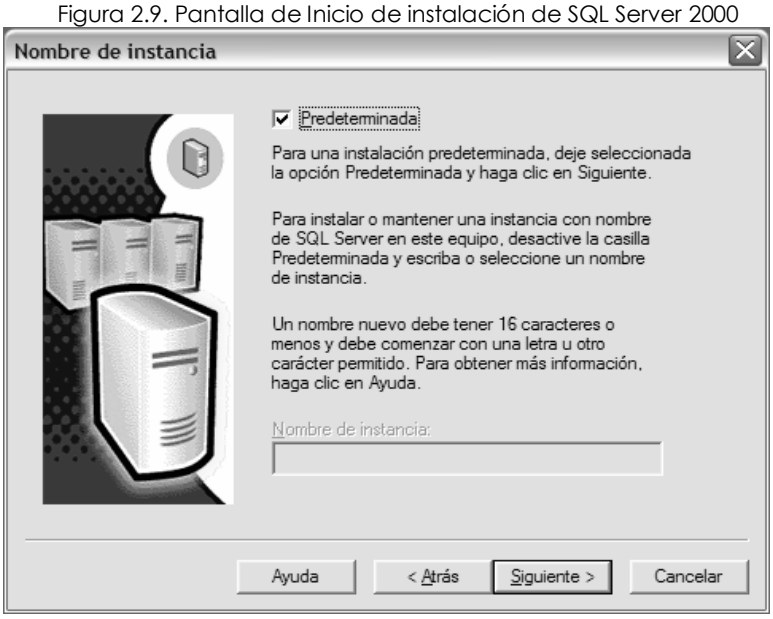


Fuente: Autores de la Tesis

Aquí se nos presenta tres opciones, de las herramientas que instalaremos, es decir, si instalamos solo las *herramientas de cliente* tendremos acceso a un servidor remoto, si escogemos *herramientas de cliente y servidor*, nos instala un servidor como gestor de bases de datos y además todas las herramientas de cliente, y si escogemos *solo conectividad* nos instala únicamente el MDAC [15]. En nuestro caso escogemos la segunda opción, y pulsamos sobre el botón siguiente.

[15] Microsoft Data Access Componente, son las tecnologías para activar Acceso universal a datos entre los cuales tenemos Microsoft ActiveX data Objects (ADO), Open Database connectivity (ODBC) y OLEDB.

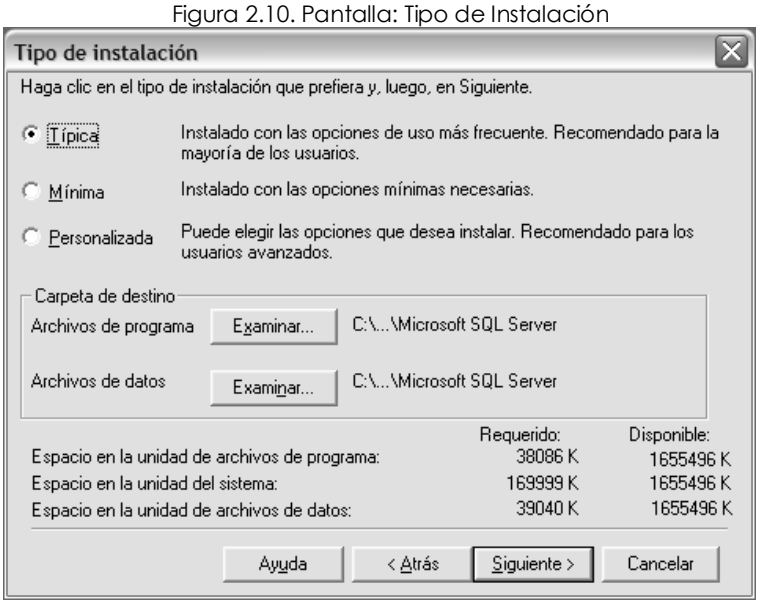
Figura 2.9. Pantalla de Inicio de instalación de SQL Server 2000



Fuente: Autores de la Tesis

Aquí podremos ingresar el nombre de la instancia que vamos a crear, si es nueva instancia (no hay ningún SQL Server instalado) por defecto coge el nombre de la máquina aunque podemos cambiarlo, si es una segunda instalación debemos darle un nuevo nombre.

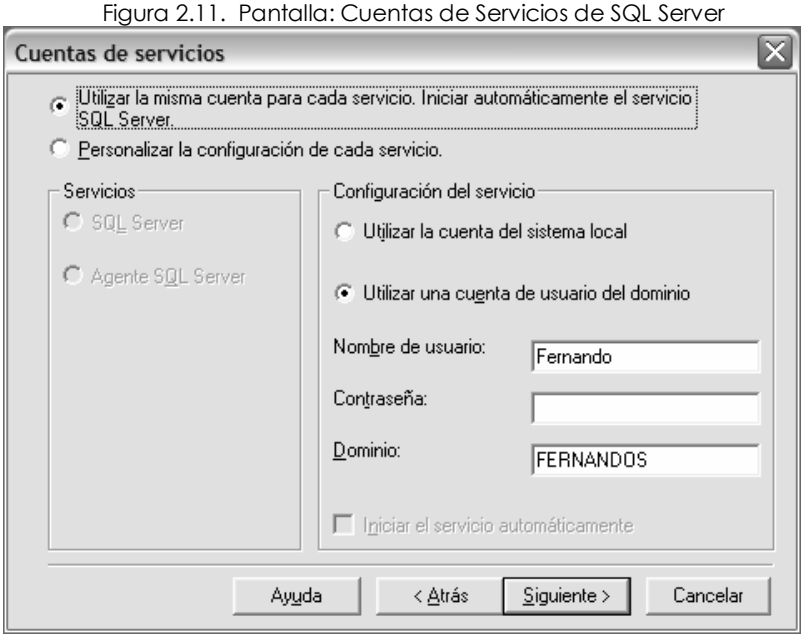
Figura 2.10. Pantalla: Tipo de Instalación



Fuente: Autores de la Tesis

Ahora tenemos que escoger el tipo de instalación, se nos da a escoger tres opciones, *Típica* que instala todas las opciones de uso mas frecuente, *Mínima* que instala las opciones mínimas necesarias para que se ejecute el programa, y por ultimo tenemos la opción, *Personalizada,* la misma que nos permite elegir las opciones que deseamos instalar como por ejemplo el elegir la ruta de los datos a una unidad con suficiente espacio en disco. Nosotros escogemos la opción típica y pulsamos sobre el botón siguiente.

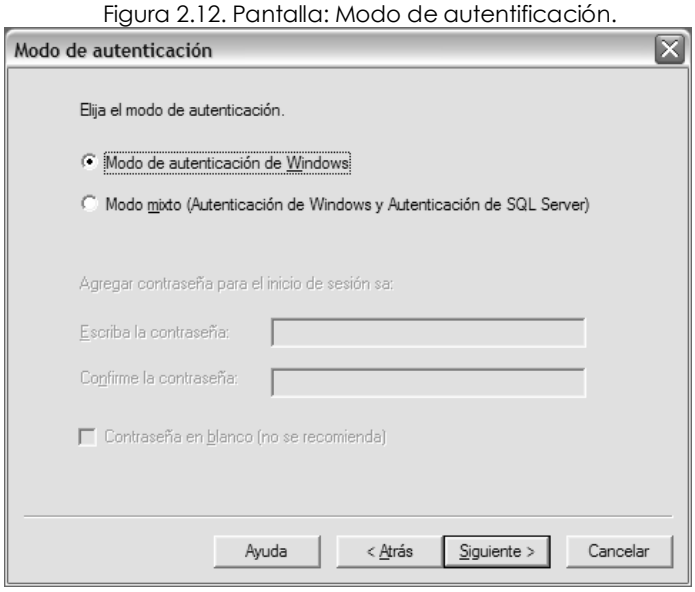
Figura 2.11. Pantalla: Cuentas de Servicios de SQL Server



Fuente: Autores de la Tesis

Ahora tenemos que indicar el Usuario que ejecutará los servicios del SQL Server y de SQL Agent, por defecto lo ejecuta el usuario administrador. Pero podemos cambiarlo. Para lo cual tenemos que indicar el nombre de usuario, la contraseña y el dominio. Una vez indicado que usuario será el que utilice los servicios, pulsamos sobre el botón siguiente y se nos mostrara lo que tenemos en la figura 2.12.

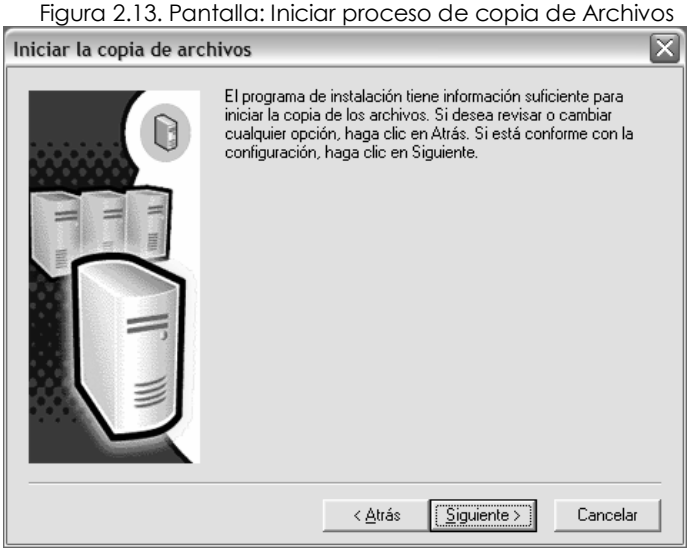
Figura 2.12. Pantalla: Modo de autentificación.



Fuente: Autores de la Tesis

Nos toca escoger el Modo de autentificación a SQL Server, se puede elegir entre autentificación Windows (la autentificación se realiza por medio de usuarios pertenecientes al dominio) o modo mixto que la autentificación se realiza por medio de usuarios dados de alta en el SQL Server, si se elige esta segunda opción, no es recomendable dejar el password en blanco. Nosotros escogemos la primera opción, y pulsamos sobre le botón siguiente.

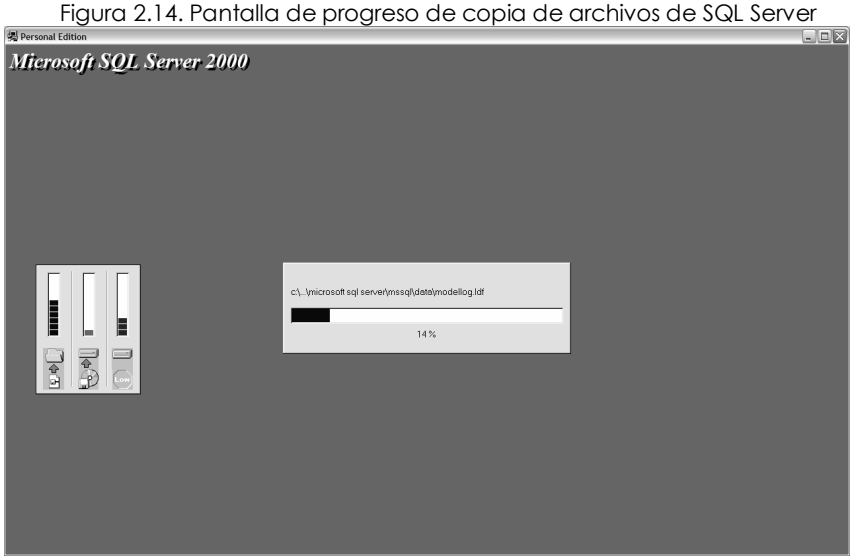
Figura 2.13. Pantalla: Iniciar proceso de copia de Archivos



Fuente: Autores de la Tesis

En esta paso nos indica que ya hemos introducido la información necesaria para iniciar el proceso de instalación, pulsamos sobre siguiente y empezara dicho proceso tal y como se muestra en la figura 2.14.

Figura 2.14. Pantalla de progreso de copia de archivos de SQL Server



Fuente: Autores de la Tesis

A partir de este punto SQL Server instalará las opciones que seleccionaos anteriormente y cuando la barra de estado llegue al 100%, la instalación habrá finalizado con lo que tendremos un SQL Server listo para trabajar.

2.3 Visual Basic .NET

Actualmente el paradigma de programación se ha enfocado a nuevas necesidades de modernos y globales sistemas de información basados en redes y aún más en la red mundial de Internet, actualmente es más importante poder concebir y construir sistemas de información con estas nuevas tecnologías de programación.

2.3.1 Definición

Visual Basic .Net es un leguaje de programación desarrollado por Microsoft, muy apropiado para construir sistemas de información basados en red e Internet.

.Net es la nueva tecnología que permite hacer más fácil la construcción y desarrollo de programas y aplicaciones para Internet.

Visual Basic .Net esta basado en .Net Framework, utilizando una jerarquía de clases que están incluidas en el mismo.

.Net Framework es un entorno para construir, instalar y ejecutar servicios Web y otras aplicaciones. Se compone de tres partes principales: El Common Language Runtime, las clases Framework y el ASP .Net.

2.3.2 Características

Visual Basic .NET es hoy en día una de las herramientas más utilizadas y productivas para la realizar aplicaciones utilizadas en ambiente Windows.
Una de las principales características o ventajas es que se puede seguir utilizando los conocimientos para crear la próxima generación de servicios y aplicaciones Web.

Entre las principales características que posee este paquete tenemos las siguientes:

Aplicaciones eficaces para Windows.

El trabajo de los programadores se simplifica enormemente ya que con la herencia de los objetos de Windows, se puede centralizar la interfaz de usuario y la lógica común de toda su solución en formularios primarios. A demás permite crear formularios redimensionables sin tener aplicar código, a demás permite crear menús mas fácil y rápidamente.

Aplicaciones para Web

Visual Basic .Net permite crear aplicaciones Web de manera fácil e interactiva arrastrando y pegando elementos, por medio de su diseñador

de Web Forms y de XML. Los programadores pueden utilizar la tecnología Microsoft IntelliSense, o el editor WYSIWYG.

Aplicaciones móviles

Mobile Internet de Visual Studio .Net nos permite crear aplicaciones para dispositivos compatibles con Internet. Con esta característica se puede desarrollar aplicaciones para teléfonos móviles WAP, HTML compacto para teléfonos i-mode o para Pocket PC y similares.

Plantillas y asistentes que permiten ahorrar tiempo.

La plantilla de servicios Web XML crea e implementa automáticamente los diversos componentes de un servicio Web. El Asistente para la instalación permite distribuir las aplicaciones .NET de forma sencilla.

El lenguaje más sencillo y popular.

Visual Basic .Net es el lenguaje de programación más fácil de leer y escribir que existe en la actualidad, a demás que su compilación de segundo plano permite obtener información al instante y señala los errores que se puede cometer en la programación.

Funciones de programación ampliadas

La implementación lado a lado acaba con los conflictos entre versiones y la herencia permite reutilizar el código de cualquier lenguaje basado en .NET. El Control de excepciones estructurado proporciona un código de control de errores fácil de mantener.

2.3.3 Instalación

Visual Basic .Net es una parte de todo el paquete denominado Visual Studio .Net, en el que no solo se encuentra este lenguaje sino también otros lenguajes, tales como Visual C# .NET o Visual C++ .NET, además de la documentación de Visual Studio.NET.

A continuación se detalla los pasos necesarios para la instalación de Visual Studio .Net, cabe indicar que en la versión profesional de Visual Studio.NET se incluye en cinco discos compactos.

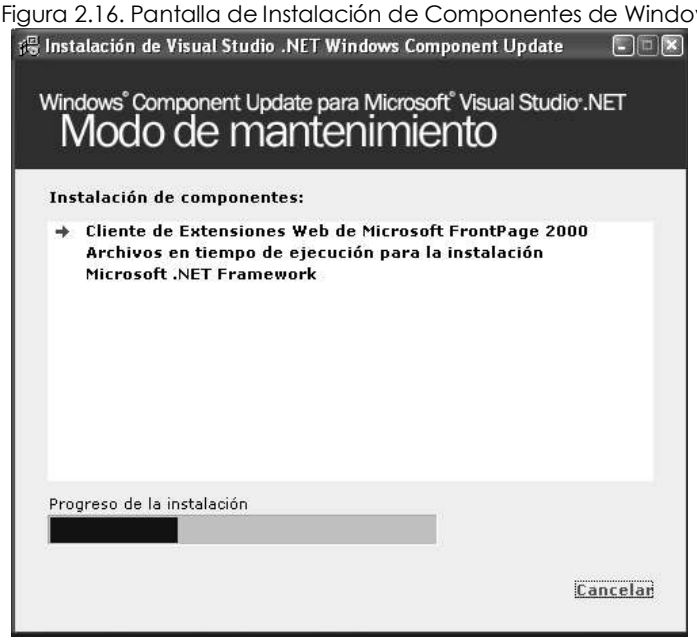
Para la instalación debemos insertar el primer disco, y aparecerá la siguiente pantalla (figura 2.15):

Figura 2.15. Pantalla de Inicio de instalación de Visual Studio .NET

Fuente: Autores de la Tesis

Luego pulsamos la opción 1 Windows Component Update que comprobará que se tenga instalado una serie de componentes para el correcto funcionamiento de Visual Studio.NET, si no se tiene dichos componentes se inicia la instalación de los mismos y aparecerá la pantalla que se muestra en la figura 2.16:

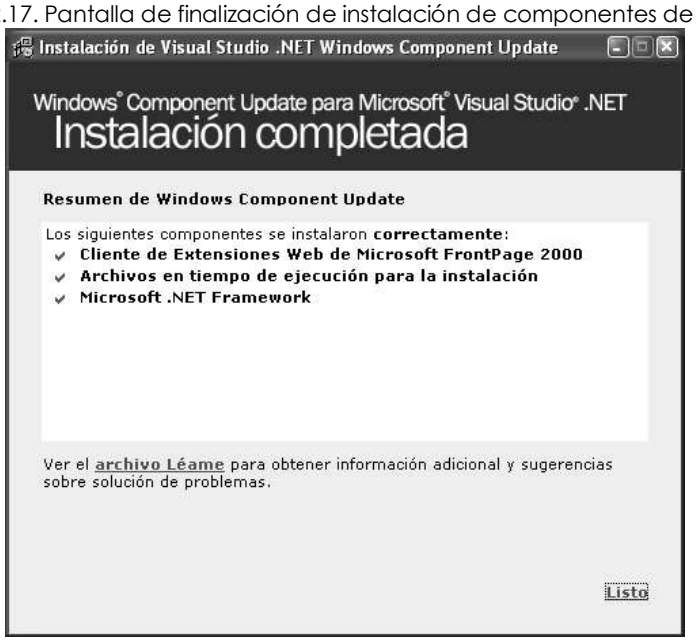
Figura 2.16. Pantalla de Instalación de Componentes de Windows



Fuente: Autores de la Tesis

Una vez finalizado el proceso de actualización de componentes de Windows se mostrará en pantalla un mensaje de finalización, figura 2.17

Figura 2.17. Pantalla de finalización de instalación de componentes de Windows



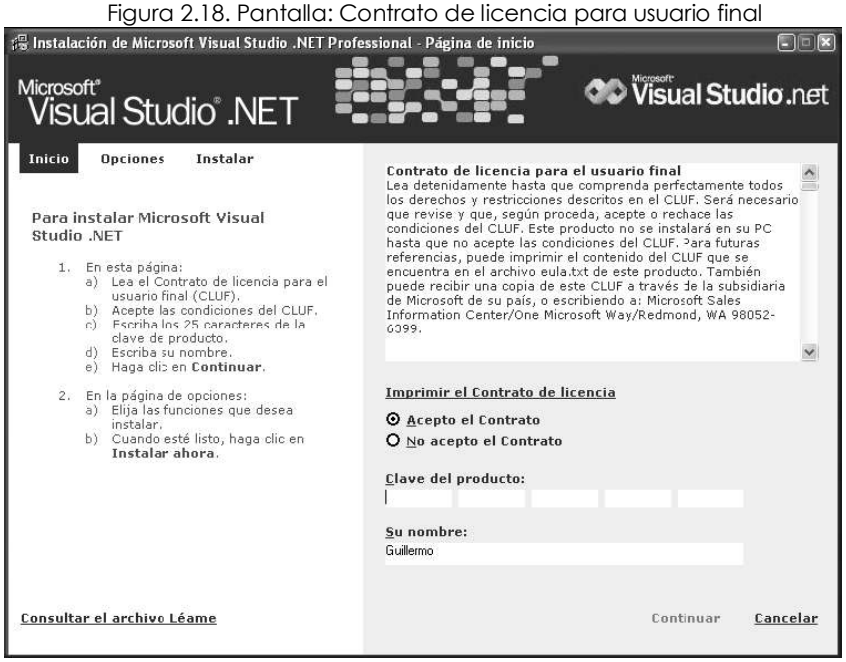
Fuente: Autores de la Tesis

Figura A.3 Información sobre el resultado de la actualización de componentes

Después de actualizar Windows con los componentes necesarios para que Visual Studio.NET funcione se mostrará nuevamente la pantalla de instalación que se mostró en la figura 2.15, solo que tendrá desactivado el paso 1.

En esta pantalla pulsaremos en la segunda opción Visual Studio .NET, pedirá el ingreso del disco 1, e iniciará el proceso de instalación con el ingreso de datos como clave del producto y datos personales como se muestra en la figura 2.18

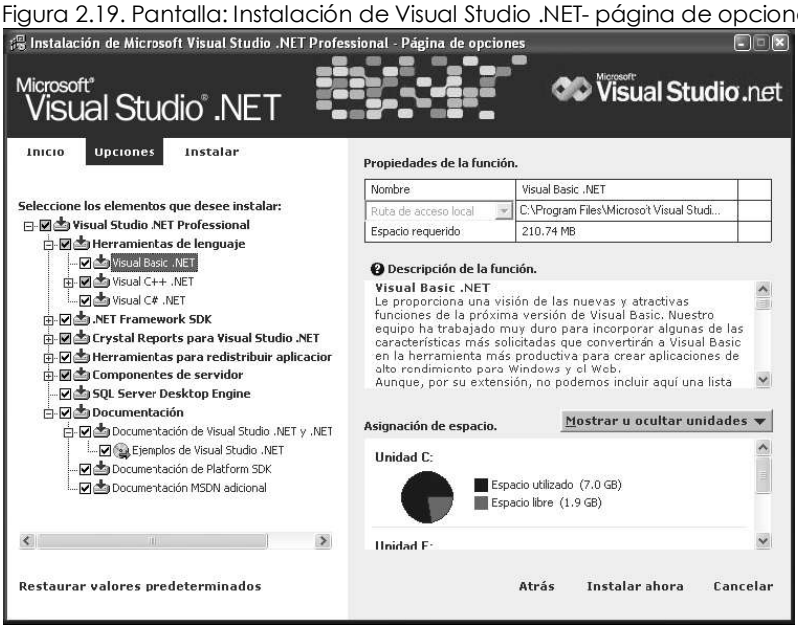
Figura 2.18. Pantalla: Contrato de licencia para usuario final



Fuente: Autores de la Tesis

Una vez ingresados los datos necesarios pulsamos el botón de continuar y nos aparecerá la siguiente pantalla en la que escogeremos los productos a instalar así como el directorio de destino, tal como se muestra en la figura 2.19:

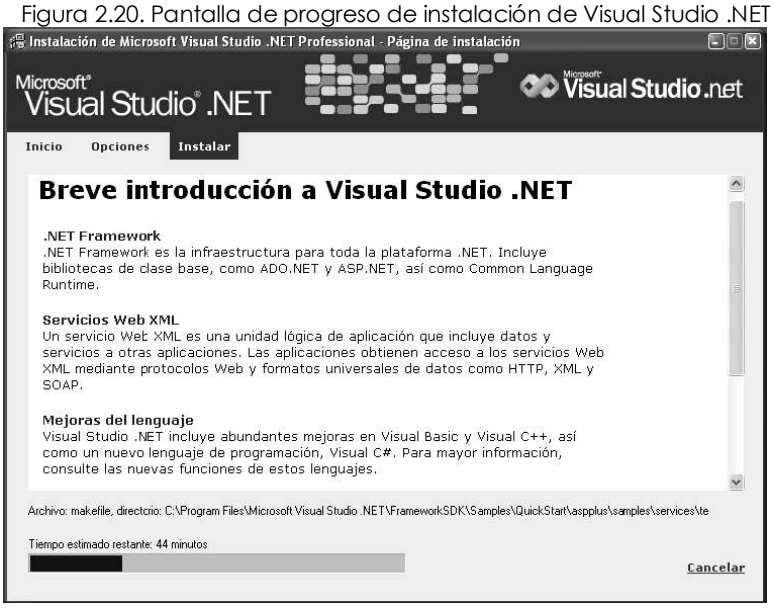
Figura 2.19. Pantalla: Instalación de Visual Studio .NET- página de opciones



Fuente: Autores de la Tesis

Pulsamos la opción de instalar ahora y empezará el proceso de instalación de Visual Studio.NET. Para ello se mostrara una pantalla en la cual se indica el estado del proceso de instalación en porcentaje y tiempo restante tal como se muestra en la figura 2.20:

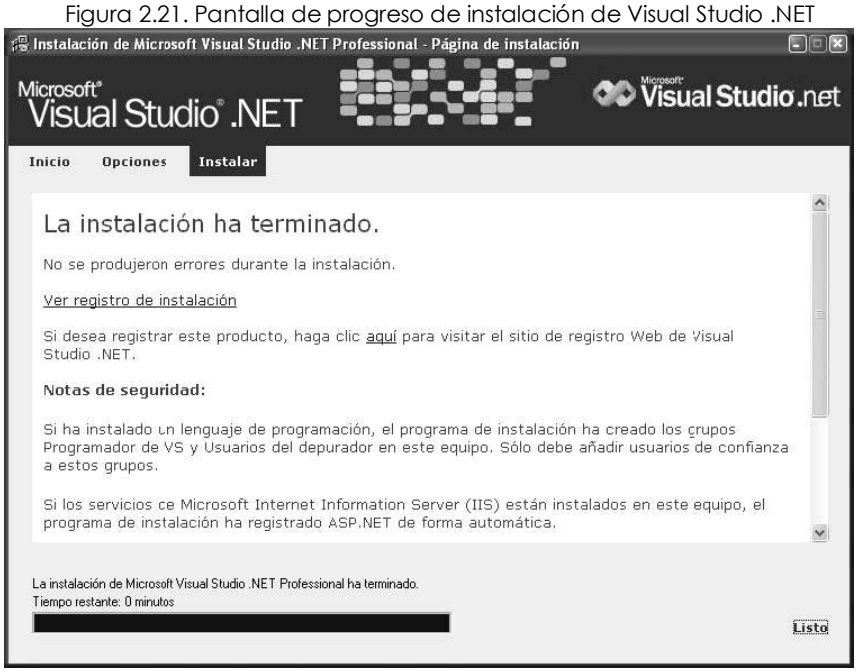
Figura 2.20. Pantalla de progreso de instalación de Visual Studio .NET



Fuente: Autores de la Tesis

Según avance el proceso de instalación se deberá insertar los discos que el proceso nos pida para completar la instalación. Una vez finalizado nos muestra un mensaje tal como se muestra en la figura 2.21 que se muestra a continuación:

Figura 2.21. Pantalla de progreso de instalación de Visual Studio .NET



Fuente: Autores de la Tesis

Una vez finalizado el proceso de instalación, podemos iniciar Visual Studio.NET utilizando el acceso directo creado en el menú de programas.

Durante el proceso de carga, se mostrará una pantalla en la que se mostrarán los productos que hemos instalado, tal como podemos ver en la figura 2.22:

Figura 2.22. Pantalla de finalización de instalación de Visual Studio .Net

Fuente: Autores de la Tesis

2.4 Integración de Visual Basic .net y SQL Server 2000

Visual Basic .Net utiliza varios métodos de acceso a datos, entre los que podemos mencionar OLE DB, XML, y ADO.NET. Nuestro estudio estará centrado en el uso de ADO.Net para el acceso a datos, debido a que nos proporciona acceso coherente a orígenes de datos como Microsoft SQL Server. Las aplicaciones para usuarios que comparten datos pueden utilizar ADO.NET para conectar a estos orígenes de datos y recuperar, manipular y actualizar los datos.

2.4.1 Ado .NET

"Objeto de acceso a datos. (ActiveX Data Objects), es un conjunto de clases que exponen servicios de acceso a datos al programador de .NET. ADO.NET proporciona un conjunto variado de componentes para crear aplicaciones distribuidas de uso compartido de datos. Forma parte integral de .NET Framework, y proporciona acceso a datos relacionales, datos XML y datos de aplicaciones. ADO.NET es compatible con diversas necesidades de programación, incluida la creación de clientes de bases de datos

clientes y objetos empresariales de nivel medio utilizados por aplicaciones, herramientas, lenguajes o exploradores de Internet " [16].

ADO.NET separa de una forma transparente el acceso a datos de la manipulación de datos y crea componentes discretos que se pueden usar por separado o conjuntamente. Los resultados de los accesos a datos se procesan directamente o se colocan en un objeto DataSet de ADO.NET con el fin de exponerlos al usuario para un propósito específico, junto con datos de varios orígenes, o de utilizarlos de forma remota entre niveles.

DataSet.

El DataSet de ADO.NET es el componente central de la arquitectura sin conexión de ADO.NET. El DataSet está expresamente diseñado para el acceso a datos independientemente del origen de datos. Como resultado, se puede utilizar con múltiples y distintos orígenes de datos, con datos XML o para administrar datos locales de la aplicación. El DataSet contiene una colección de uno o más objetos DataTable formados por filas y columnas de datos, así como información sobre claves principales, claves externas, restricciones y relaciones a los datos incluidos en los objetos DataTable [17].

2.4.2 Proceso de integración

A continuación se indicara el proceso de integración entre Visual Basic .Net y SQL Server 2000, mediante un ejemplo, en el que realizaremos una pequeña aplicación para establecer la forma de acceso a información de una Base de Datos de SQL. Server 2000, con la ayuda de ADO.NET

Primero iniciamos el Visual Studio .NET, por defecto te mostrará la "página de inicio" desde la cual pueden crearse nuevos proyectos o bien abrir alguno

[16] ttp://msdn.microsoft.com/library/spa/default.asp?url=/library/SPA/cpgui de/html/cpconaccessingdatawithado net.asp
[17] Representa una tabla de datos en memoria.

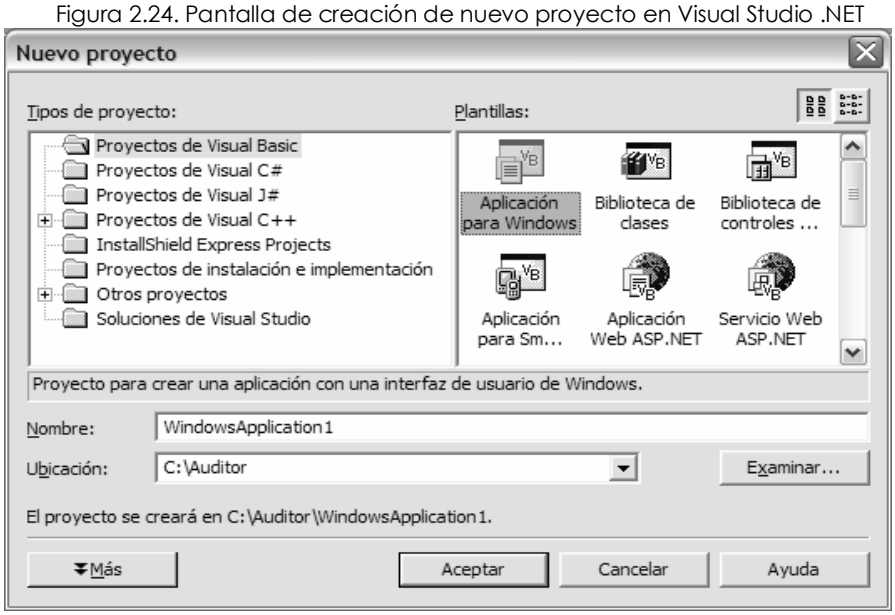
de los más recientemente abiertos. Pulsa en Nuevo proyecto. Tal y como se muestra en la figura 2.23.

Figura 2.23. Pantalla inicial de Visual Studio .NET

Fuente: Autores de la Tesis

Ahora se mostrará los diferentes tipos de proyectos que se pueden crear, en el panel izquierdo seleccionamos Proyectos de Visual Basic y de los que muestra en el panel de la derecha, seleccionamos aplicación de Windows:

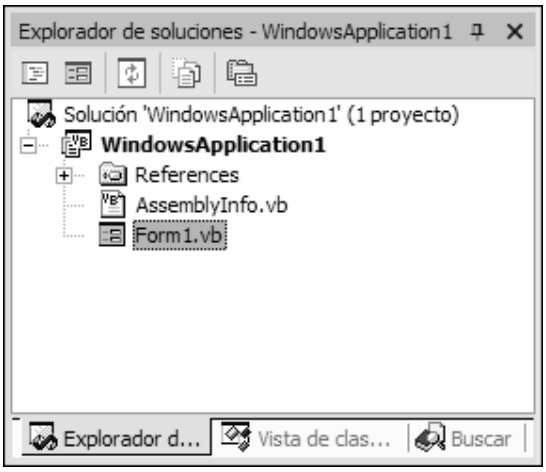
Figura 2.24. Pantalla de creación de nuevo proyecto en Visual Studio .NET



Fuente: Autores de la Tesis

En el proyecto, se habrá creado un formulario, el cual seguramente se lo podrá ver de forma automática. Si no se mostrara nada, en el lado derecho de la pantalla, hay un "panel" o ventana en la que se indica el proyecto actual y se muestran los ficheros que lo componen. Ese panel es el Explorador de Soluciones.

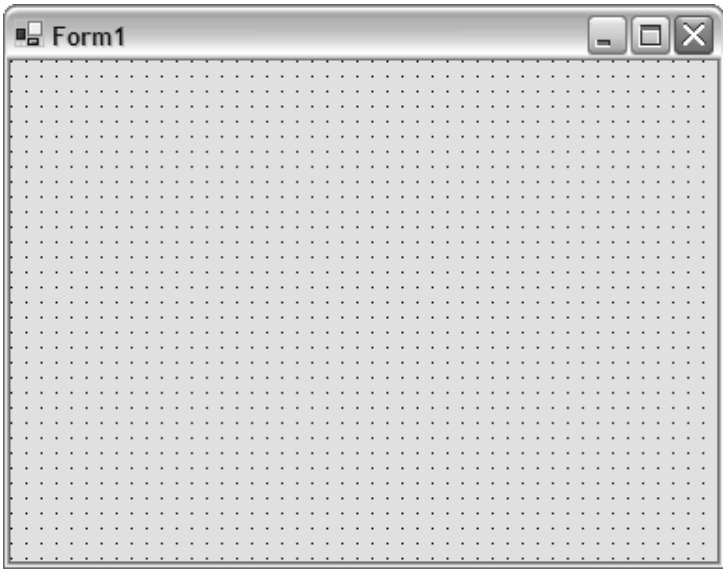
Figura 2.25. Pantalla: Explorador de soluciones



Fuente: Autores de la Tesis

Para que se muestre el formulario (Form1), se da doble clic en dicho "elemento" del explorador de soluciones. Tal como se indica en la figura 2.26

Figura 2.26. Pantalla: Ejemplo de formulario de Visual Basic .NET



Fuente: Autores de la Tesis

Para añadir controles al formulario, hay que usar la barra de herramientas que está situada en la parte izquierda del IDE de Visual Studio .NET, por ejemplo para añadir una etiqueta (Label) y una caja de texto (TextBox), simplemente hacemos doble-click sobre esos elementos de la barra de herramientas y se añadirán automáticamente al formulario. Para poder ubicarlos en el sitio que más nos agrade, simplemente pulsamos sobre ellos y manteniendo el botón del ratón pulsado, lo colocamos donde más nos guste.

Para nuestro ejemplo añadiremos un botón (Button) y una grilla (DataGrid). Para cambiarle el texto que muestra el botón, hay que usar la ventana de propiedades, y la propiedad que nos interesa es *Text*, escribe CargarDatos y cuando pulsemos Enter, observaremos que el texto del botón también ha cambiado.

Ahora vamos a escribir código que se ejecutara cada vez que se haga click en el botón que hemos añadido. Para esto, seleccionamos el botón CardarDatos y damos doble click sobre él, con lo que se nos mostrará una nueva ventana, en este caso la ventana de código asociada con el formulario que tenemos en nuestro proyecto.

Lo que se mostrara es lo siguiente:

```
Private Sub Button1_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles Button1.Click
End Sub
```

Ahora escribimos el código que se ejecutará cuando se haga click en ese botón, lo cual producirá el evento Click asociado con dicho botón. Este evento se producirá si se hace un click propiamente dicho, o se pulsa el botón Enter.

Primero definimos las variables que se usaran en el procedimiento, estas son:

```
Dim SqlConStr As String = "Provider=SQLOLEDB;Persist Security
Info=False;User Id=sa;password=sa;Initial Catalog=pubs;Data
source=fernandos;"
Dim oConexion As OleDbConnection
Dim dsConsulta As DataSet
Dim SqlComando As OleDbDataAdapter
Dim SqlSentencia As String
```

SqlConStr.- Esta es una variable de tipo string, que almacena la cadena de conexión, en la cual indicamos el origen de los datos, es decir, le tenemos que poner a que Base de Datos nos vamos a conectar (en nuestro ejemplo nos conectaremos a la base de datos pubs, que se crea al instalar SQL Server 2000), la ubicación de las misa (localhost indica que la base de datos se encuentra en la maquina local), el nombre del usuario que tiene acceso a esta base de datos y su clave.

oConexion.- es de tipo OleDbConnection y almacena o representa una conexión abierta a un origen de datos, En el caso de un sistema de bases de datos de cliente y servidor, equivale a una conexión de red al servidor, como en nuestro ejemplo, por lo que oConexion será nuestra variable para la conexión

dsConsulta.- es de tipo DataSet y será la variable donde se guarde la consulta o resultado de la consulta a la base de datos que vamos a utilizar en el ejemplo, como ya se explicó antes en el concepto de DataSet.

SqlComando.- es de tipo OleDbDataAdapter y nos va a permitir ejecutar los comandos para acceder a los datos en una conexión y actualizar también información de un origen de datos. Es decir que con este objeto podremos obtener los datos para ser colocados en un DataSet en nuestro caso dsConsulta, contendrá los datos al ejecutar el un comando para consultar la base de datos "employee" de nuestro ejemplo.

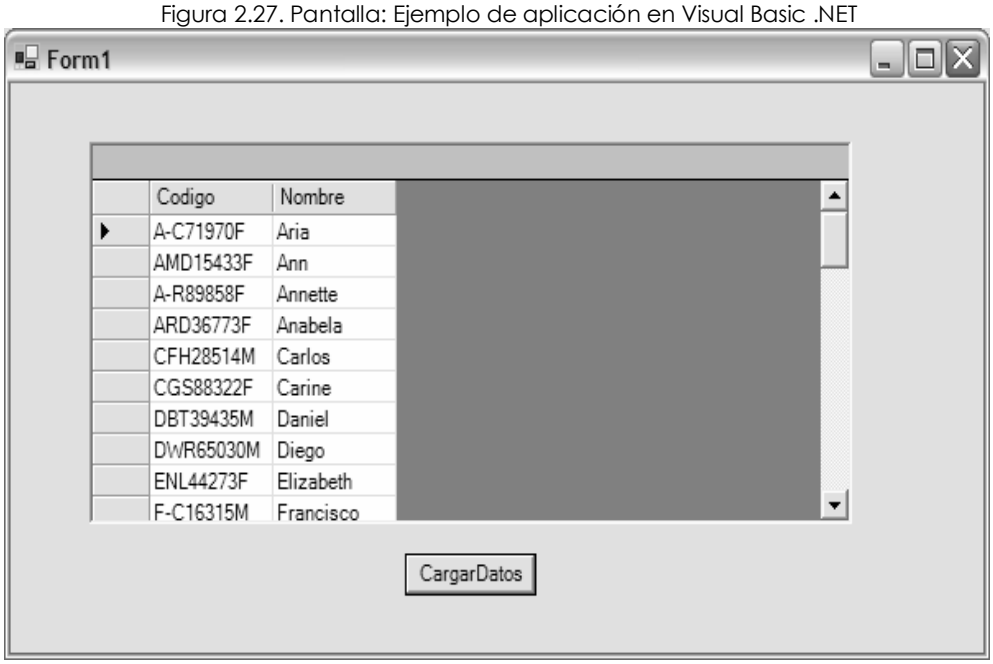
SalSentencia.- Variable de tipo String, contendrá la sentencia Sql para realizar una consulta a la base de datos, en este caso un select.

Una vez definidas nuestras variables escribimos el siguiente código que nos permitirá realizar una consulta a la tabla "Employee" que pertenece a una Base de datos pública de SQL Server.

```
SqlSentencia = "Select emp_id Codigo,fname Nombre from employee"
oConexion = New OleDbConnection(SqlConStr)
SqlComando = New OleDbDataAdapter(SqlSentencia, oConexion)
dsConsulta = New DataSet
SqlComando.Fill(dsConsulta, "Tabla")
DataGrid1.DataSource = dsConsulta
DataGrid1.DataMember = "Tabla"
oConexion.Close()
```

Primero establecemos nuestra sentencia SQL, en este caso una consulta, luego establecemos la una nueva conexión con el origen de datos esto en la segunda línea del código anterior, en la tercera línea ejecutamos el comando el cual nos va permitir acceder a la Base de datos.
Luego definimos un nuevo DataSet para guardar los datos obtenidos de la consulta, con el objeto SqlComando.Fill(...) obtenemos los datos de la consulta y los colocamos en el Dataset, por último agregamos estos datos al DataSource del objeto DataGrid y listo. Se mostrará en pantalla todos los datos de la tabla employee tal como se muestra en la figura 2.27.

Figura 2.27. Pantalla: Ejemplo de aplicación en Visual Basic .NET



Fuente: Autores de la Tesis

2.5 CONCLUSIONES DEL CAPÍTULO

En este capítulo estudiamos las herramientas a utilizar, tanto Visual Basic .Net como Microsoft SQL Server 2000, pudimos determinar las características principales que nos llevaron a escoger estas herramientas de desarrollo, y además determinamos la utilidad y alcances que nos permitirán tener en el desarrollo del software de auditoría.

Realizamos el proceso de instalación de las herramientas, y aprendimos la forma adecuada para su integración, por medio de la utilización de ADO .NET que nos facilita el acceso a la información de cualquier base de datos, en el caso del proyecto para SQL Server 2000.

CAPÍTULO 3:

METODOLOGIA PARA CONTROL, EVALUACION Y AUDITORÍA DE SISTEMAS DE INFORMACION

CONTENIDO

3.1 Introducción al capítulo

En este capítulo desarrollaremos la metodología para llevar un adecuado control, evaluación y auditoría de cualquier sistema, para ello realizaremos una descripción detallada de la metodología y las fases a seguir.

Este capítulo será de suma importancia para el desarrollo del software, ya que aquí se establecerá de forma teórica, los pasos en el control, evaluación y auditoría de sistemas.

A demás plantearemos los conceptos necesarios, para el desarrollo de esta metodología.

3.2 Marco teórico

Antes de realizar el desarrollo de la metodología creemos necesario tener claro algunos conceptos y términos que serán utilizados. A continuación presentamos un pequeño análisis sobre la empresa.

3.2.1 La empresa como sistema

Puede definirse como sistema a *"un conjunto de elementos íntimamente relacionados que actúan e interactúan entre sí, hacia la consecución de un fin determinado"*[18].

De ahí podemos concebir a una empresa como un sistema, ya que la empresa tiene elementos que están relacionados e interactúan entre sí, y a demás toda empresa esta encaminada a alcanzar un objetivo.

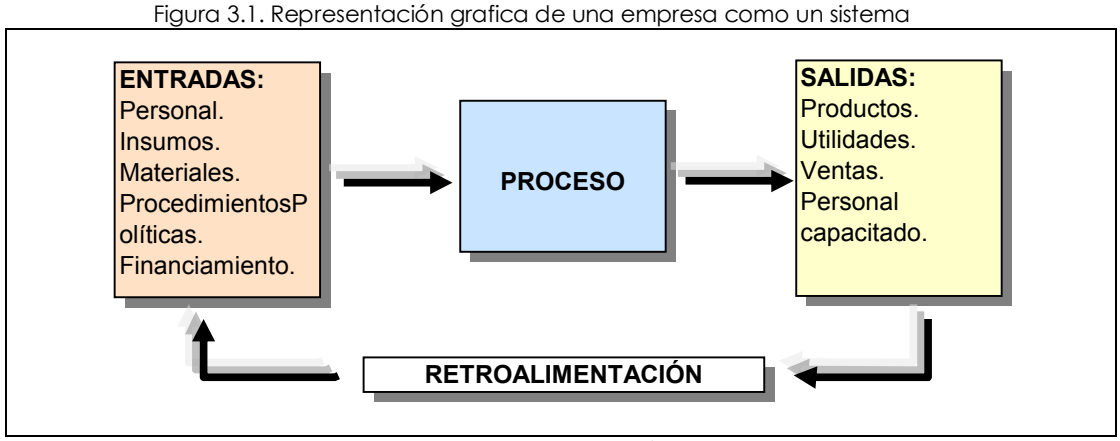
En cualquier sistema se puede encontrar cuatro elementos básicos para su funcionamiento; desde el punto de vista de un sistema:

[18] http://www.aulafacil.com/administracionempresas/Temario.htm, AULA FACIL, lección 27

1. Entradas o insumos: abastecen al sistema de lo necesario para cumplir su misión.
2. Procesamiento: es la transformación de los insumos.
3. Salidas o producto: es el resultado del proceso.
4. Retroalimentación: es la respuesta de los sistemas que han recibido como insumo el producto de un sistema previo o la respuesta del medio ambiente.

Gráficamente, una empresa vista como sistema se representa de la siguiente manera:

Figura 3.1. Representación grafica de una empresa como un sistema



Fuente: Autores de la Tesis

Podemos indicar que en cualquier empresa podemos encontrar los siguientes elementos:

- Operaciones
- Transacciones que están conformados de procesos o procedimientos
- Recursos que pueden ser:
  - Humanos
  - Materiales
  - Financieros
  - Datos e información
- Controles

Operaciones: Las operaciones son acciones de tipo económico o administrativos que se realizan en la empresa para alcanzar los objetivos propuestos para la misma.

Transacciones: son los eventos lógicos que se dan a lugar durante la vida o ciclo de una operación. Las transacciones están compuestas de procesos o procedimientos los cuales a su vez pueden estar formados de subprocesos.

Procesos o procedimientos: Son un conjunto de pasos, acciones o fases sucesivas, es decir que tienen un orden establecido. Los procesos buscan satisfacer o cumplir un objetivo.

Recursos: son los elementos humanos, materiales, financieros e informáticos que son utilizados o participan en un proceso que es parte de una transacción.

Controles: Son las medidas orientadas a disuadir, prevenir o detectar la materialización de una amenaza.

Amenazas: Son los peligros a los cuales pueden estar expuestos los recursos.

Riesgos: Son los eventos o hechos que resultan de la realización de una amenaza, es decir de cuando ocurren los peligros a los que pueden estar sujetos los recursos.

3.2.2 Matrices de control

Las matrices de control llamadas también Matrices de Relación, son una herramienta muy importante para el proceso de evaluación de la suficiencia de los controles identificados para proteger los recursos de una transacción o la transacción misma de las amenazas a los que pueden estar expuestos.

Su función principal es que permite visualizar de manera gráfica la relación existente entre los recursos o transacciones con los riegos identificados en un sistema y los controles definidos para su protección. Los más utilizados son la matriz Transacciones/Riesgos y la matriz Recursos/Riesgos.

La matriz se estructura de la siguiente manera, los riesgos del sistema se ubican en las filas y las Transacciones o Recursos ocupan las columnas de la matriz. Las celdas que resultan del cruce de filas y columnas sirven para colocar los códigos asignados a los controles relacionados con un listado de Transacciones/Riesgo o Recurso/Riesgo que se verán más adelante en el apartado 3.3.

A continuación se presenta un ejemplo para la matriz Transacción/Riesgo:

Figura 3.2. Matriz Transacción Riesgo

MATRIZ DE CONTROL
TRANSACCIONES - RIESGOS

PESOS		RIESGOS				
		01 Fraude / Desfalco 4	2 Perdida / Extravio 3	3 Robo / Hurto 3	4 Daño / Destrucci 5	5 Multas / Sanciones 1
TRANSACCIONES	Transacción 100 5	20		15	25	
	Transacción 101 4		12			4
	Transacción 102 5	20			25	
	Transacción 103 3	12				3
	Transacción 104 4		12		20	
	Transacción 105 2	8				2

3.3 Estructura de la metodología para el control, evaluación y auditoría de sistemas de información.

La metodología que presentaremos a continuación, nos permitirá conocer las tareas y actividades que deberán llevarse acabo para el control, evaluación y auditoría de sistemas de información.

Esta metodología nos permitirá realizar la evaluación de las transacciones, procesos y recursos que son parte del sistema, con el fin de identificar las amenazas y riesgos a los cuales pueden estar expuestos, a demás que nos

ayudará a determinar si los controles implantados para la protección de dichos recursos son los adecuados y funcionan eficientemente.

La estructura de la metodología para el control, evaluación y auditoría de sistemas será la siguiente:

Fase 1: Planeación.

a) Selección del sistema ha auditar.
b) Definición del alcance del proyecto.
c) Elaboración del plan de actividades.
d) Organización de papeles de trabajo.
e) Conocimiento del sistema.

Fase 2: Análisis de transacciones y recursos.

a) Definición de las transacciones.
b) Análisis de las transacciones.
c) Identificación de los recursos
d) Relación entre transacciones y recursos.

Fase 3: Análisis de amenazas y riesgos.

a) Identificación de riesgos y amenazas.
b) Relación entre recursos/amenazas/riesgos.

Fase 4: Análisis de control.

a) Identificación de controles.
b) Relación entre recursos/amenazas/riesgos y controles.
c) Análisis de cobertura de controles.

Fase 5: Evaluación de los controles

a) Pruebas de controles
b) Análisis de resultados

Fase 6: Informe y recomendaciones.

3.3.1. Planeación.

Selección del sistema ha auditar.

Generalmente la participación de Auditoría en la evaluación de controles en sistemas, se da cuando la empresa cuenta con varios de ellos en funcionamiento. Por esta razón es necesario llevar a cabo un proceso de selección mediante la aplicación de criterios que reflejan su importancia para la empresa.

A continuación enumeramos algunos de estoy criterios:

- Propósito general de la auditoría.
- Satisfacción del usuario.
- Estados de funcionamiento.
- Forma de operación.
- Impacto por fallas en el sistema.
- Evidencia de fallos en los sistemas
- Resultados de auditoría anteriores

Definición del alcance del proyecto.

La definición de alcances permitirá establecer los elementos del sistema seleccionado sobre los cuales deberá concentrarse la atención de los recursos. Para esto hay que tomar en cuenta los resultados obtenidos en el proceso de selección del sistema a auditar.

Aquí se definirá en algunos casos, el tiempo que llevará realizar la evaluación, lo cual será un condicionante para el desarrollo de los controles, evaluaciones y/o auditorías.

Se deberá tener en cuenta los recursos disponibles para la ejecución del proyecto.

Los alcances del proyecto pueden ser modificados por el auditor durante el desarrollo de la evaluación siempre y cuando exista una situación que lo amerite.

Elaboración del plan de actividades.

Tiene como fin los siguientes puntos:

- Definir las actividades para cada una de las fases de la auditoría.
- Asignar los recursos responsables para la ejecución de las actividades.
- Estimar el tiempo y los costos del proyecto.
- Generar el plan o cronograma detallado del proyecto.

El resultado de lo anterior es el cronograma detallado de actividades a realizar en el proyecto, que nos permitirá conocer cual es el avance en el proyecto así como también conocer que recursos materiales y humanos necesitamos para cumplir con lo propuesto.

Una vez culminados los pasos anteriores y elaborado el plan de actividades, la documentación pertinente deberá ser presentada al jefe del área de auditoría, a su vez este debe presentar el plan de trabajo a las áreas comprometidas en la auditoría.

Organización de papeles de trabajo.

Como en cualquier proyecto de auditoría, la evaluación de controles en un sistema deberá ser documentada siguiendo los principios básicos para la organización y compilación de los papeles de trabajo, según como se indico en el capítulo 1. [19]

Conocimiento del sistema.

El propósito de esta fase es reunir toda la información referente a las políticas, normas y procedimientos del sistema ha auditar, así como también información referente a la administración del mismo. Esto permitirá conocer al auditor como está estructurado el sistema y será una base de referencia para la evaluación de los controles detectados en el mismo.
Toda esta documentación, si el auditor considera necesario, deberá ser adjuntada como una copia a los papeles de trabajo.

El Auditor deberá obtener la siguiente información:

- Organigrama del área a auditar y si es posible de toda la empresa.
- Manuales de funciones y procedimientos si existen para conocer como se administra y como funciona la empresa.
- Documentación de auditorías anteriores si las hubo.

3.3.2. Análisis de transacciones.

Definición de las transacciones.

Las transacciones se definen a partir de las características y forma de operación del sistema a ser auditado. Dependiendo de la cobertura de la transacción esta puede ser dividida en procesos y estos a su vez en subprocesos.

[19] Capítulo 1, Sección 10: Los papeles de trabajo para auditoría.

La división de las transacciones en procesos y estos a su vez en subprocesos facilitan su análisis y la identificación de los recursos que intervienen en cada una de ellas.

Para una buena definición de las transacciones debemos contar con el apoyo de los administradores del sistema a ser auditado, una vez realizado esto se deberá asignarles un peso que no es más que la importancia que tiene la transacción dentro del sistema.

El auditor deberá realizar un listado especificando cada transacción con sus procesos y subprocesos, así como también el peso o importancia relativa dentro del sistema de cada una de ellas

Análisis de las transacciones.

Para cada transacción definida se realiza el análisis de auditoría que tiene como propósito lo siguiente:

- Establecer los responsables de los procesos, subprocesos y transacciones.
- Identificar las relaciones existentes entre los procesos y subprocesos que conforman la transacción.
- Identificar los recursos que participan en los procesos y subprocesos.
- Establecer el flujo de documentos y su punto de almacenamiento.

El método que proponemos es el análisis grafico por medio de diagramas de flujo de procesos, y nos permite mostrar de manera integrada los procesos facilitando la identificación y análisis de los recursos.

Identificación de los recursos

Es muy importante la identificación de los recursos que se utilizan en el sistema a ser auditado para poder analizar las amenazas a los que están expuestos, para de esta forma definir los controles necesarios para eliminar o reducir los riesgos.

El análisis de los recursos inicia durante la preparación de los diagramas de flujo de procesos, y al igual que en las transacciones, procesos y subprocesos se deberá asignar un peso de acuerdo a la importancia que tengan dentro del sistema. Hay que tener en cuenta que un recurso puede participar en diferentes transacciones o procesos.

Relación entre transacciones y recursos.

Con la ayuda de los diagramas de flujo, se deberá determinar las relaciones existentes entre los recursos y las transacciones identificadas. El Auditor deberá realizar un registro de los recursos que participan en cada transacción.

El auditor deberá tener en cuenta que un recurso puede participar en más de una transacción o proceso, y que además una transacción puede tener varios recursos diferentes asignados.

En el caso de una transacción con procesos y subprocesos se recomienda señalar los recursos en el proceso o subproceso en el cual participa de forma específica.

3.3.3. Análisis de amenazas y riesgos.

Identificación de riesgos y amenazas.

Como se menciono anteriormente amenaza y riesgo son dos conceptos diferentes por lo cual su identificación debe hacerse de forma separada.

Lo primero que se debe realizar es identificar los riesgos que pueden ocurrir al materializarse las amenazas.

Como la cobertura de auditoría a la totalidad de las áreas del sistema resulta casi imposible, es importante que los auditores utilicen un enfoque que les permita concentrar sus esfuerzos en aquellas áreas que de acuerdo con la administración se consideren mas criticas.

Entre los riesgos de mayor importancia podemos citar los siguientes:

- Daño físico o destrucción de los recursos.
- Pérdida de lo documentos.
- Perdida económica por fraude interno.
- Robo de dispositivos.
- La integridad de la información.

Al igual que en las transacciones es de vital importancia asignarles un peso relativo que dependerá de la criticidad de los riesgos; mientras mayor daño cause el riesgo mayor será su peso.

Luego de identificar los riesgos procedemos a identificar las amenazas. Las amenazas están directamente relacionadas con lo recursos que participan en los sistemas, por lo cual hay que considerar que un recurso puede estar expuesto a diferentes amenazas que pueden originar uno o varios riesgos.