ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Instituto de Ciencias Matemáticas

"ANÁLISIS Y APROVECHAMIENTO DE LOS SISTEMAS DE INFORMACIÓN PARA UNA EFICIENTE AUDITORÍA Y CONTROL DE GESTIÓN"

TESIS DE GRADO

Previa a la obtención del Título de:

AUDITOR EN CONTROL DE GESTIÓN

Presentado por:

Jimmy Arturo Brito Domínguez

Guayaquil-Ecuador

AÑO

2004

AGRADECIMIENTO

A Jehová Dios el hacedor de mi vida por todas sus bendiciones, su ayuda, protección y dirección durante toda mi vida.

A mi mamá por darme y mí querida esposa por darme su apoyo, comprensión, amor y fortaleza en todo momento.

Al Ing. Galo Solís por su valiosa ayuda y dirección en la realización de esta Tesis.

CPA. Manuel Pérez, la Ing. Raquel de Vásquez y al CPA. Geovanny Regalado por sus enseñanzas y consejos en esta profesión tan exigente.

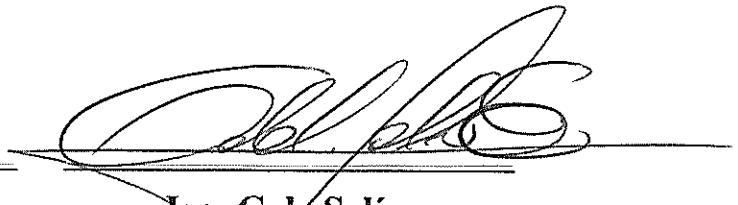
Y a mis grandes compañeros y amigos Jared, Flora, Ileana y Paola.

DEDICATORIA

A mi esposa y mi hermosa hija
quienes son mi razón de vivir.

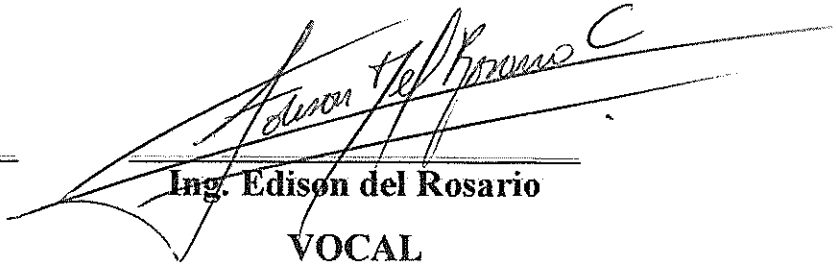
TRIBUNAL DE GRADUACIÓN

Mat. Jorge Medina
DIRECTOR DEL INSTITUTO DE CIENCIAS MATEMÁTICAS



Ing. Galo Solís
DIRECTOR DE TESIS

Ing. Ricardo Naranjo
VOCAL



Ing. Edison del Rosario
VOCAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITECNICA DEL LITORAL."

(Reglamento de Graduación de la ESPOL.)

Jimmy A. Brito Domínguez

RESUMEN

El grado de utilización que tienen los sistemas de información en el desarrollo de las actividades operativas y administrativas de las organizaciones de hoy, ha provocado una revolución en la manera de llevar a cabo los negocios, la forma en que se compite, los tipos de servicios que se brindan a los clientes, las estrategias de crecimiento y mercadotecnia, y la forma en que se realizan las alianzas estratégicas; en donde el manejo adecuado de la información es el principal factor para lograr el éxito o el fracaso en la denominada “Sociedad de la Información”.

Por ello, una de las mayores preocupaciones de los gerentes de hoy es cómo salvaguardar a este recurso tan preciado, la información, contra amenazas tales como la pérdida, la libre divulgación, el error y la manipulación. Es ahí donde aparecen dos factores clave para su protección: un adecuado Sistema de Control Interno Informático y la Auditoría de Sistemas, como elementos imprescindibles para la

prevención y detección de desviaciones significativas en la búsqueda de información íntegra, consistente y confiable.

Aspectos como estos, han transformado el enfoque de la auditoría tradicional y la han llevado a incorporar el uso de los sistemas de información dentro de cada una de sus fases, mejorándose enormemente la precisión, confiabilidad, eficiencia y administración del proceso de auditoría. Para ello, el auditor dispone de diversas técnicas y herramientas que le permiten maximizar el uso de los sistemas de información de forma efectiva y segura.

El auditor del nuevo milenio debe estar preparado para hacer frente a los cambios tecnológicos y debe desarrollar profundas habilidades para evaluar, con el uso eficiente de los sistemas de información, el entorno informático en las organizaciones de hoy, que permita realizar un examen integral de la gestión administrativa y la toma de decisiones correctivas, encaminadas hacia el logro de los objetivos establecidos y la transparencia en las actividades desempeñadas.

Índice General

Índice de Figuras

Índice de Tablas

ÍNDICE DE ABREVIATURAS

AICPA	Asociación de Contadores Públicos Certificados
CICA	Instituto Canadiense de Contadores Certificados
CISA	Certificación en Auditoría de Sistemas
COBIT	Objetivos de Control para Tecnología de Información y Tecnologías relacionadas
DBA	Administrador de Bases de Datos
DBMS	Sistema de Administración de Bases de Datos
GAO	Oficina de Contabilidad General de los Estados Unidos
IDEA	Análisis y Extracción Interactiva de Datos
ISACA	Asociación para el Control y Auditoría de Sistemas de Información
ISACF	Fundación para el Control y Auditoría de Sistemas de Información
ISO	Organización Internacional de Normalización
LAN	Red de Área Local
NSA	Agencia de Seguridad Nacional
SEI	Instituto de Ingeniería de Software
WAN	Red de Área Amplia
ITGI	Instituto para el Gobierno de Tecnología de Información
COSO	Sponsoring Organizations of the Treadway Commission
CAAT's	Técnicas de Auditoría Asistidas por Computador

INTRODUCCIÓN

Los Sistemas de Información han tenido un profundo desarrollo desde los años ’50 hasta la actualidad, convirtiéndose poco a poco a través de los años, en una valiosa herramienta dentro de las organizaciones, mejorando la eficiencia y aumentando la productividad; tanto así, que hoy en día casi no existe empresa pública o privada que no realice alguna de sus actividades mediante el uso del computador. Sin embargo, toda esta revolución tecnológica ha hecho surgir la necesidad de asegurar que dichos Sistemas de Información sean precisos y confiables, principalmente en el procesamiento de la información financiera, cayendo directamente esa responsabilidad sobre el auditor de Estados Financieros.

Es ahí donde nace uno de los principales desafíos de la auditoría moderna: evaluar y controlar de forma eficiente la gestión empresarial a través del uso de las herramientas informáticas; lo cual, hace surgir varias interrogantes como, ¿Cuáles son las técnicas y herramientas informáticas disponibles para los auditores modernos?, ¿De qué manera pueden ser aprovechadas dichas herramientas para la implementación y evaluación de un sistema de control informático?, y ¿Cuáles son y como se aplican los paquetes de auditoria más utilizados?. En el presente trabajo se analizan cada una de estas preguntas con la intención de ser un aporte en el enriquecimiento de una de las profesiones más fascinantes en los últimos años: la Auditoría de Sistemas de Información.

Capítulo 1

Objetivos y Alcance

1.1. Objetivos

1.1.1. Objetivo General

Analizar la forma en que pueden ser aprovechados los Sistemas de Información por parte de los auditores modernos, para una eficiente auditoría y Control de Gestión.

Para ello, es necesario explicar la forma en que los sistemas de información se han convertido en parte integrante de los procesos realizados por las organizaciones de todo tipo y tamaño.

Así mismo, se busca explicar cuáles son las técnicas y herramientas informáticas disponibles para los auditores tanto internos como externos; la manera en que pueden ser aprovechadas dichas herramientas para la implementación y

evaluación de un sistema de control informático, y cuáles son y como se aplican los paquetes de auditoria más utilizados.

1.1.2. Objetivos específicos

Los objetivos específicos son muy variados, basados en los objetivos generales mencionados anteriormente. Entre los objetivos específicos se encuentran los siguientes:

a) Establecer la importancia y el impacto que tienen los sistemas de información en el desarrollo de las actividades y toma de decisiones de las organizaciones modernas.
b) Explicar la evolución que ha tenido el Control Interno y la Auditoría través de los años, su importancia y la metodología para su implementación exitosa.
c) Explicar las diferentes metodologías para la ejecución de la auditoría informática en las diferentes áreas relacionadas con el procesamiento electrónico de datos.
d) Analizar los diferentes estándares mundiales sobre control y gestión de la tecnología de Información, y la forma en que estos contribuyen al mejoramiento del Control Interno Informático.

e) Analizar la importancia que tiene la Auditoría Informática para la detección de errores e ineficiencias dentro de la gestión de Tecnología de Información.

f) Analizar la forma en que los sistemas de información apoyan el proceso de auditoría, en el mejoramiento de las tareas administrativas, el proceso de análisis de la información y la elaboración de pruebas sustantivas.

g) Analizar algunos programas de auditoría disponibles en el mercado como IDEA, ACL, WORKING PAPERS, COBIT y la forma en que estos pueden ser aprovechados durante la ejecución de pruebas o actividades típicas de auditoría.

1.2. Alcance

El presente trabajo no busca analizar profundamente los diferentes tipos de sistemas de información, ni analizar aspectos relativos a su desarrollo e implementación; sino más bien, la forma en que estos apoyan a la gestión empresarial de las organizaciones modernas y el proceso de auditoría en ambientes de procesamiento electrónico de datos; y, la forma en que pueden ser aprovechadas las principales técnicas y herramientas informáticas utilizadas por los auditores en la práctica, así como los paquetes informáticos más utilizados en la actualidad.

CAPÍTULO 2

Los Sistemas de Información y la Gestión Empresarial

2.1. ¿Qué son los Sistemas de Información?

Existen muchos autores que definen de diversas formas a los sistemas de Información; sin embargo, todos ellos apuntan a que un Sistema de Información es un conjunto de elementos o componentes interdependientes entre sí en donde se puede ingresar, procesar, almacenar, controlar y presentar la información para la oportuna y eficiente toma de decisiones.

Bajo la definición anterior, está claro que al hablar de Sistemas de Información no necesariamente estamos hablando de computadores e informática, ya que existen Sistemas de Información manuales; es decir, donde la información es registrada y almacenada (archivada) en papel.

En cambio, los Sistemas de Información Computarizados son aquellos Sistemas de Información que se apoyan en la tecnología del hardware, software y comunicaciones. En esta Tesis al referirse a los Sistemas de Información, se hará referencia a los Sistemas de Información Computarizados.

Para muchos, los Sistemas de Información Computarizados abarcan solamente el software y hardware (programas y computadoras) utilizados en una organización. Sin embargo, estos por sí solos no se convierten en una solución para la organización, ya que necesitan estar diseñados de acuerdo a las necesidades y estructura operativa, administrativa y estratégica de la organización, para que realmente puedan ser llamados Sistemas de Información Computarizados.

Existen cuatro clases principales de Sistemas de Información, de acuerdo a los principales niveles jerárquicos de una organización. Estos son los sistemas de Nivel Operativo, Sistemas del Nivel de Conocimientos, Sistemas del Nivel Administrativo y Sistemas de Nivel Estratégico.

2.1.1. Sistemas de Nivel Operativo

Los cuales se encuentran directamente relacionados con los procesos operacionales y transaccionales de una organización. Dentro de este nivel se encuentran los Sistemas de procesamiento de transacciones. Ejemplos de estos, son los Sistemas de Facturación, Compras, Cuentas por Cobrar, Cuentas por Pagar, Inventarios, Control de ingreso de empleados, etc. Se caracterizan por ser de uso fácil, realizan procesos transaccionales sencillos, las consultas y reportes son limitados en su estructura y sus usuarios son los empleados y Jefes del nivel primario de la organización.

2.1.2. Sistemas del Nivel de Conocimientos

Estos se relacionan con el nivel secundario de la organización o también conocido como nivel de análisis de datos y conocimientos. El propósito de estos Sistemas consiste en ayudar a desarrollar, procesar, ordenar e interrelacionar el flujo de información y nuevos conocimientos de la organización. Dentro de este nivel se encuentran los *Sistemas de Automatización de Oficinas* tales como, procesadores de palabras, hojas de cálculo, agendas electrónicas, manejadores de bases de datos de escritorio, administradores de correo electrónico, etc.; y los *Sistemas de*

Trabajo de Conocimientos tales como, diseñadores gráficos, diseñadores arquitectónicos y mecánicos, diseñadores Web, etc.

2.1.3. Sistemas del Nivel Administrativo

Estos se enfocan hacia las actividades de monitoreo, dirección, control y toma de decisiones de los jefes o administradores de Nivel Medio. En esta categoría se encuentran los *Sistemas de Apoyo a Decisiones*, tales como, los Sistemas de análisis de Costos, análisis de Producción, análisis de Ventas y Rentabilidad, etc.; y los *Sistemas de Información Gerencial* como los Sistemas de Dirección de Ventas, Administración de Presupuestos e Inventarios, etc. Estos se caracterizan por presentar información periódica para análisis y por lo general relacionan variables de carácter interno y externo para producir resultados que ayuden a la gerencia a tomar decisiones eficaces y oportunas.

2.1.4. Sistemas de Nivel Estratégico

Estos apoyan en la toma de decisiones de nivel estratégico a largo plazo, tomando en consideración las políticas y metas propuestas interrelacionándolo con el ambiente externo de la organización, de tal forma que se puedan tomar decisiones que mejoren la competitividad. Dentro de esta clasificación se

encuentran los *Sistemas de Apoyo a Ejecutivos*, los cuales, son fáciles de usar, flexibles y no requieren que el usuario posea complejos conocimientos de informática para poder usarlos. Su característica principal es el análisis de datos provenientes de los otros Sistemas (Transaccionales y Administrativos) mediante el modelado de tablas o cubos de información, en el cual, se obtienen cuadros y resúmenes de información fáciles de armar e interpretar.

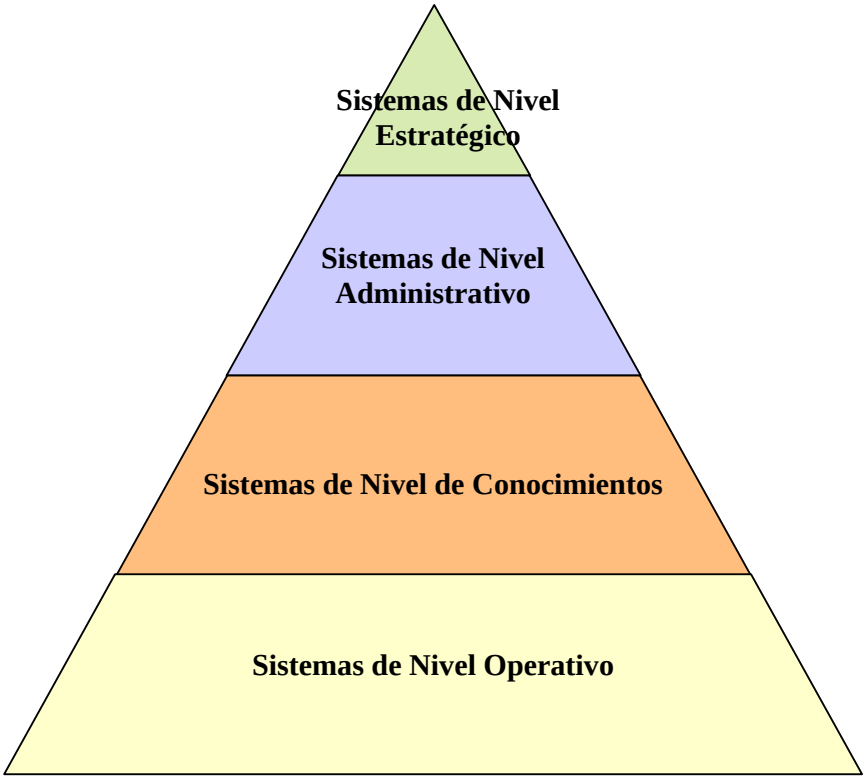


Figura 2.1. Ubicación de los SI en la pirámide organizacional

2.2. Importancia de los Sistemas de Información en los Negocios

2.2.1. La Era de la Información

Hoy en día nadie puede dudar de la importancia que tiene la información para el mundo empresarial, a tal punto de que se la considera como el activo más importante y diferenciador en las empresas al momento de ser competitivos; si a esto le sumamos la Tecnología de Información que día a día evoluciona de manera muy acelerada, tenemos como resultado potentes herramientas para la toma de decisiones para la gerencia moderna e innovadora.

Los gerentes modernos reconocen cómo el entorno de los negocios se ha visto claramente afectado debido a factores tales como la Globalización, el aumento de las empresas de servicio y el cambio en los modelos gerenciales; pero así mismo, han reconocido cómo la Tecnología de Información (**TI**) los ha ayudado a adaptarse a esos factores y ha mejorado considerablemente la eficiencia en las operaciones, la calidad en los productos y servicios, y la búsqueda de nuevos mercados.

El uso de los Sistemas de Información y las comunicaciones, dentro de la economía globalizada de hoy, permite a las empresas tener mayores y mejores oportunidades de negocios, al permitirles llegar a nuevos y distantes mercados poco explotados; mejorar la distribución de la información con los clientes y proveedores sin límites de horario; permite competir de manera abierta sin necesidad de poseer grandes infraestructuras corporativas y permite administrar de manera eficiente y descentralizada a la organización globalmente.

Las grandes superpotencias mundiales a su debido tiempo se dieron cuenta de cómo el conocimiento y la información son generadores de prosperidad y riqueza y es por ello, que han transformado sus economías pasando de ser países industrializados a ser países con economías de servicio basadas en el uso efectivo de la información. El manejo de la información y el conocimiento mediante el uso de los Sistemas de Información han mejorado la productividad, han dado lugar a la generación de nuevos productos y servicios y han cambiado la forma en que se mide la competitividad de las empresas y los Países.

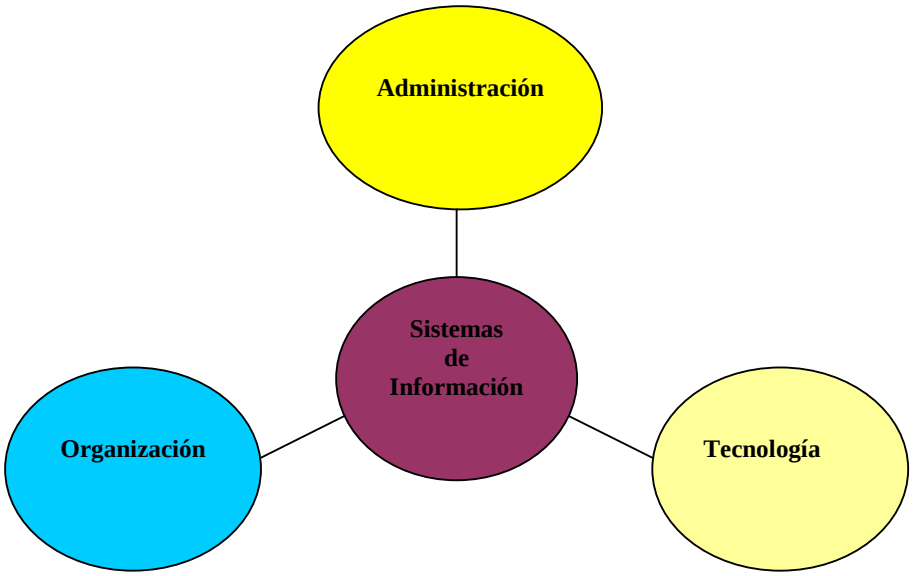


Figura 2.2. Integración de los SI en las organizaciones

Las empresas modernas se apoyan en el uso eficiente y eficaz de la información para la toma oportuna de decisiones que les permita flexibilidad para poder adaptarse y atender a los diferentes tipos de mercados. Bajo esta concepción, se deja a un lado las viejas estructuras jerárquicas complejas y verticales que disminuyen el tiempo de respuesta ante los cambios externos y que complican el flujo adecuado de la información en la organización, todo esto apoyado en potentes Sistemas de Información y a bajo costo.

2.2.2. Impacto de los Sistemas de Información en los Negocios

Como ya se mencionó anteriormente, los Sistemas de Información no solamente están compuestos por Hardware y Software, ya que estos dependen de otros componentes esenciales como son la Base Organizacional y la Dirección Gerencial. Es por ello, que se puede decir, que un Sistema de información, para ser tal, debe interrelacionarse con cada uno de los aspectos operativos, administrativos y de control con los que cuenta la organización y deben ser un reflejo de las estrategias, políticas y filosofías gerenciales de la administración.

Por otro lado, la organización depende de forma cada vez más creciente de los sistemas de Información, de tal forma que las estrategias y la planificación organizacional estarán dadas en función de la capacidad de crecimiento, flexibilidad y capacidad de sus Sistemas de Información. Por tal motivo, los gerentes modernos al momento de tomar decisiones importantes en cuanto a crecimiento, competitividad y calidad de sus productos y servicios deben considerar por el lado organizacional, las estrategias, políticas, procedimientos, recursos, capacidad organizacional; mientras que por el lado tecnológico debe

considerar Software, Hardware, Bases de Datos y Telecomunicaciones.

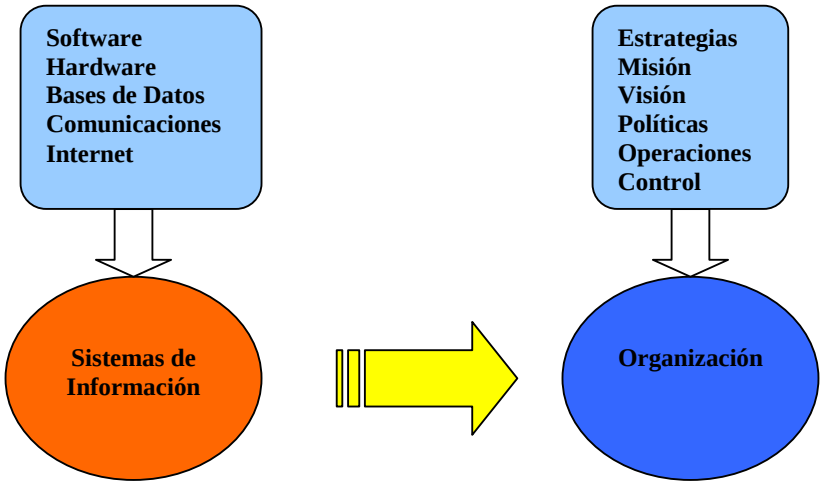


Figura 2.3. Impacto de los SI en las organizaciones

A todo esto debemos añadir el uso de la red de computadoras más grande de todo el mundo conocido como Internet; la cual, permite conectar a miles de redes en todo el mundo en más de 200 países brindando el acceso a cientos de millones de personas a un mundo infinito de información en las áreas de la ciencia, tecnología, economía, educación, gobierno, entre otros. Sin lugar a dudas, el Internet ha cambiado la forma de hacer negocios, ya que ahora es posible hablar de comercio y negocios electrónicos abriendo un sin número de oportunidades para la aparición de nuevos

productos y servicios, la eliminación de las distancias geográficas, formación de nuevas alianzas estratégicas basadas en la información, etc.

2.2.3. Ventajas competitivas que brindan los Sistemas de Información

La incorporación de la Tecnología de Información dentro de los procesos productivos de una organización puede convertirse en una ventaja competitiva, al permitirles ser más eficientes y darles la capacidad de desarrollar productos y servicios a menor costo y mejor calidad. La mayor parte de nuevos productos y servicios puede verse reflejado en el sector financiero, en donde se ofrecen servicios, tales como, banca en línea a través de Internet, consulta de movimientos y transacciones vía telefónica, Cajeros automáticos, etc. No obstante, cualquier sector dentro de la economía puede desarrollar Sistemas de Información estratégicos para mejorar su desempeño y competitividad.

Otra ventaja competitiva que ofrecen los Sistemas de Información, es la capacidad que estos ofrecen para realizar estudios de mercados que permitan establecer pronósticos de ventas, estrategias de marketing y publicidad, análisis financiero y

descubrimiento de nuevos nichos de mercado; todo esto a través de la extracción y análisis de grandes cantidades de datos que es procesado y analizado de forma rápida y sencilla.

La administración de los inventarios con el uso de los Sistemas de Información se convierte en un proceso muy sencillo y eficiente que representa un enorme ahorro de dinero, al reducirse los grandes Stock de productos y los gastos de alquiler y mantenimiento de los centros de almacenamiento. Esto se debe principalmente a que los Sistemas de Información modernos permiten tener un reabastecimiento de inventarios de forma continua mediante el envío de los pedidos de mercadería de forma automática a los proveedores tan pronto estos van siendo vendidos y, por otro lado, los proveedores vía Web pueden consultar los puntos de re-orden de sus clientes de tal forma que puedan atenderlos de forma rápida y específica.

Otro aspecto importante, es la posibilidad de poder formar alianzas de información, en las cuales las organizaciones pueden integrar sus Sistemas de Información con los de otras organizaciones, para intercambiar información estratégica que les permita tener acceso a nuevos mercados y clientes, poder ofrecer

productos sustitutos y lograr alianzas entre competidores en un ambiente de ayuda mutua para poder enfrentarse a nuevos competidores e incluso podrían formar alianzas a nivel de toda la industria para ser mas eficientes en los servicios que brindan a sus clientes, sin la necesidad de fusionar las compañías sino, estableciendo plataformas estandarizadas de comunicación e información en las que la información pueda fluir de forma adecuada.

Sin embargo, no debemos olvidar que la Dirección General de la organización tiene la responsabilidad de que a medida que se va integrando los Sistemas de Información a la estrategia general de la organización, también se debe establecer mecanismos adecuados para cambiar la estructura funcional, operativa y administrativa de la organización, de tal forma, que se maximice el uso y las ventajas competitivas que tiene el uso de la Tecnología de Información. Además, es importante que las organizaciones que lleguen a tener alianzas estratégicas de información, asuman una responsabilidad de cooperación mutua en el desarrollo de aplicaciones, inversión de tecnología y mantenimiento de sus Sistemas de Información interconectado para el éxito de los mismos; y, por último, es necesario que las

organizaciones eliminen las barreras ínter departamentales y funcionales mediante la cooperación mutua, la elaboración de políticas y procedimientos operativos estándar y el desempeño funcional eficiente, orientado hacia el logro de los objetivos institucionales.

2.3. Sistemas ERP's: sus Beneficios y Riesgos

Como ya se mencionó anteriormente, dentro de las organizaciones existen diferentes clases de sistemas de Información dependiendo del nivel jerárquico al cual estos estén enfocados, manejando diversas áreas del negocio. Puede ser que estos Sistemas estén integrados entre sí o puede que no, dependiendo de la capacidad tecnológica y los recursos con los que se cuente.

Sin embargo, cada vez es mayor el número de organizaciones que están optando por integrar cada uno de sus Sistemas independientes con el propósito de que la información fluya de forma eficiente entre cada departamento y llegue en forma oportuna a la alta gerencia para la correcta planificación de recursos y la toma de decisiones estratégicas. En el mundo empresarial, dicha ***Planificación de Recursos de la Empresa (ERP,*** *Enterprise Resourse Planning),* es un sistema de gestión estratégica de negocios que busca la integración coordinada de

la organización en las áreas de planificación, producción, ventas y finanzas, compartiendo la información entre sí.

Por tanto, un Sistema de Información de ERP integra la administración de recursos, los procesos, metodologías y Sistemas independientes en un solo Sistema de Información estratégico para la gestión empresarial. Mediante estos Sistemas, cada una de las transacciones generadas a diario dentro de la organización es registradas en una sola base de datos potente y robusta que mantiene en línea la información estratégicamente relevante para la administración de la organización.

2.3.1. Beneficios de los Sistemas ERP's

Son muchos los beneficios que una organización puede obtener al implementar un Sistema de ERP, entre los cuales podemos mencionar: integración de la información relativa a la planificación, producción, marketing, y ventas; mejor administración y control operativo y administrativo; mayor productividad en las operaciones; mejor calidad en los productos y servicios que se ofrecen a los clientes; minimización de los costos y gastos operativos y administrativos; análisis de información para la toma de decisiones y facilidades para incursionar en los negocios y comercio electrónico.

No obstante, muchas organizaciones no tienen éxito con sus Sistemas de ERP debido a que aspiran tener beneficios en muy corto tiempo, pensando que dichos sistemas van a resolver todos sus problemas y les van a dar ventajas competitivas de forma inmediata y duradera, sin antes haber hecho un profundo análisis de su realidad organizacional, su posición en el mercado y sus potenciales competidores.

2.3.2. Problemas y riesgos comunes en los Sistemas ERP's

En nuestro medio, uno de los principales problemas a los que se enfrentan las organizaciones dentro de la implementación de un Sistema de ERP es la *Integración*, debido a que muchas veces este es un proceso tecnológicamente complejo y muy costoso. Además, muchas de las ventajas competitivas que una organización pudiera obtener luego de la implementación de su Sistema de ERP, por lo general, no son muy duraderas ni aseguran una buena rentabilidad en el mediano y largo plazo, debido a que la *tecnología* está abierta para todos y en constante cambio, lo que significa que los competidores pudieran copiar o desarrollar Sistemas de ERP similares o superiores dejando atrás lo que antes era una ventaja competitiva.

Además, muchas veces los Sistemas de ERP no son suficientemente robustos y adaptables para realizar tareas relativas al control presupuestario, consolidación de la información financiera de subsidiarias, análisis estadístico multivariado, pronósticos de ventas entre otras actividades que los administradores esperan poder realizar con sus Sistemas de ERP.

Por otro lado, cuando una organización se embarca en el desarrollo e implementación de un Sistema ERP se enfrenta a proyectos muy complejos y costosos debido a que prácticamente, a pesar de poseer Sistemas ya en producción, prácticamente debe implementar un nuevo Sistema de Información integrado y estratégico, en paralelo con la reingeniería de los procesos organizacionales preestablecidos.

Por lo general, los proyectos de implementación de nuevos Sistemas representan un alto riesgo debido a su complejidad, costos operativos, inversión en tecnología y magnitud del tiempo que conllevan; aún mas, cuando no ha existido un correcto análisis de factibilidad y relación costo-beneficio. Por ello, es

importante que las organizaciones adopten metodologías estructuradas para el desarrollo o adquisición de sus Sistemas de ERP para reducir el riesgo que esto conlleva.

Por ello, para asegurar el éxito de los Sistemas de ERP, se deben elaborar planes de mantenimiento y mejoramiento continuo de dichos Sistemas; se debe mejorar el desempeño organizacional; optimizar el uso de los recursos de forma sostenible; incorporar controles preventivos, correctivos y posteriores en los Sistemas administrativos e informáticos, invertir periódicamente en tecnología, asegurar el cumplimiento de las políticas y procedimientos institucionales, realizar una correcta segregación de funciones; y, monitorear continuamente los cambios ocurridos dentro de la organización e incorporarlos al Sistema de ERP.

2.4. Economía digital: Una nueva forma de hacer negocios

2.4.1. El Internet

Como ya se mencionó anteriormente, el Internet es una red mundial de computadoras interconectadas entre sí a través de redes más pequeñas distribuidas a lo largo del planeta. La

capacidad que esta tiene para transmitir datos, gráficas y vídeos de forma interna y externa, la convierte en una potente herramienta para las empresas de hoy y dan lugar a la aparición de nuevos modelos de negocios conocidos como comercio electrónico y negocios electrónicos.

La interconexión es realizada a través de protocolos, que no son más que conjuntos de normas establecidas que rigen la forma en que las computadoras interactúan entre sí. Los protocolos utilizados en el Internet son el TCP (Transmission Control Protocol) y el IP (Internet Protocol) que combinados dan origen al TCP/IP. Este protocolo combinado, trabaja de tal forma que organiza la información en pequeños paquetes antes de enviarlos a la red, asignando a cada paquete una característica diferente como la dirección, tipo de información, procedencia y el contenido(cuerpo); luego, el ordenador que recibe los paquetes, a través de los exploradores Web, los reordena y puede presentar la información.

Entre las principales capacidades que tiene el Internet son el correo electrónico, Telnet, FTP(File Transfer Protocol),

WWW(World Wide Web), Chat, entre otros, las cuales dan lugar a una serie de procesos y actividades que se las resume a continuación:

Capacidad / Tecnología	**Proceso**	**Actividades**
E-mail	Comunicación	Uso del correo electrónico, la transmisión de archivos y las videoconferencias.
Chat	Comunicación	Acceso a salas de Chat y uso de los programas Messenger que permiten transmitir texto, voz y vídeo.
Telnet	Comunicación	Acceder a otras computadoras mediante un enlace remoto y poder trabajar en ella.
WWW(World Wide Web)	Acceso a Información	Utilización de los buscadores Web, las bibliotecas virtuales y las grandes bases de conocimientos.
XML (Extensible	Transacciones electrónicas	Posibilidad de realizar pagos de servicios, declaración de

Markup Language)		impuestos, consultas y transacciones bancarias, compra y venta de bienes y servicios, etc.
FTP (File Transfer Protocol)	Transmisión de datos	Envío y recepción de archivos entre servidores.

Tabla 1.1. Procesos y Actividades realizadas a través de Internet.

2.4.2. Las Intranets y Extranets

Una Intranet es una red privada que conecta entre si a las computadoras de una organización, en la que se pone a disposición de sus empleados información relevante para el desempeño de sus actividades. El medio para interconectar las computadoras es la red local de la organización y el protocolo es el mismo que se utiliza en Internet, el TCP/IP. La información es presentada a través de páginas Web utilizando exploradores Web.

La información que contiene una Intranet no está disponible para personas externas a la organización, a pesar que esta pueda permitir a los usuarios acceder a Internet. La Intranet mediante los firewall (cortafuegos) no permite el acceso no autorizado de los *hackers* para evitar daños a sus Sistemas o que extraigan información considerada estratégica para la organización.

Por otro lado, las Extranets son Intranets que permiten que personas externas a la organización puedan acceder a ella mediante el uso de un usuario y una contraseña; lo cual, permite que la organización pueda intercambiar determinada información estratégica con sus clientes, proveedores y aliados comerciales; como por ejemplo, precios de productos al por mayor, informes de ventas, puntos de re-orden del inventario de mercadería, etc. De igual forma, se hace necesario el uso de *firewalls* para la protección de la Extranet contra accesos no autorizados.

2.4.3. Estrategias de negocios en el Internet

El uso adecuado del Internet dentro de las organizaciones da como resultado un mejor uso de sus recursos, reducción de sus costos, mejores productos y servicios, mayor alcance y

participación dentro del mercado, acceso a clientes potenciales, entre otros beneficios destacables. Las organizaciones que se han dado cuenta de esta realidad han desarrollado estrategias empresariales acorde con el entorno digital obteniendo muy buenos resultados. Entre las principales estrategias de negocios en Internet se encuentran:

- **Alianzas estratégicas,** a través del Internet las organizaciones pueden mantener alianzas de información con sus clientes, proveedores y aliados a bajo costo, sin límites geográficos y a nivel mundial.
- **Comunicación Online**, mediante el uso del correo electrónico y las Extranets, puede mantenerse en contacto a las sucursales a nivel mundial, se puede transferir documentos y archivos multimedia. Se puede tener acceso telefónico vía Internet a nivel internacional a bajo costo y contratar redes dedicadas de datos en el que se conecta, vía satelital mediante un proveedor de Servicios de Internet, dos puntos geográficos a gran distancia para el envío y recepción de información a gran velocidad.

- **Disminución de costos,** mediante el uso de documentos electrónicos, las organizaciones pueden ahorrar sustanciales cantidades de dinero al no utilizar papeles y dejar a un lado los grandes archivadores y centros de almacenamiento de documentos, se reduce los gastos de personal al realizarse muchas de las transacciones vía Internet y se mejora la eficiencia en las operaciones.
- **Satisfacción del cliente,** debido a que puede realizar muchas de sus transacciones desde su casa u oficina de forma rápida y económica, no teniendo que soportar trámites burocráticos lo cual garantiza la satisfacción del cliente y le abre las puertas a nuevos clientes que exigen estos tipos de servicios.
- **Acceso a información estratégica,** a través de la World Wide Web los administradores tienen acceso a información estratégica como estadísticas, información de sus competidores, información gubernamental, índices económicos a nivel mundial, información financiera de la industria, entre otros, lo cual garantiza que se cuente con información actualizada para tomar decisiones eficaces y oportunas.

2.4.4. Negocios Electrónicos

El uso del Internet permite que las organizaciones puedan tener nuevas oportunidades de negocio, al permitirles mantener sus servicios de forma ininterrumpida, mejorar la atención al cliente y mantenerse en contacto con ellos, dando lugar a la aparición de las tiendas en línea, en donde las organizaciones pueden ofrecer sus productos y servicios de manera online sin necesidad de tiendas físicas. Un ejemplo de esto es la tienda virtual Amazon.com

Otro modelo de negocios son las subastas electrónicas en el que una persona pone en subasta un artículo o bien sobre una base y los interesados presentan sus ofertas y se lo vende a quien haya ofrecido la mayor oferta. Otro tipo de subasta es en la cual varios proveedores presentan sus ofertas de bienes y servicios a un comprador el cual escoge al que presenta la oferta de menor costo.

Por otro lado, se facilitan las transacciones de compra y venta entre organizaciones mediante las Extranets automatizando a

través de sus portales electrónicos las tomas de pedidos de los clientes, el manejo de solicitudes de mercadería, la asignación de crédito, soporte técnico y otros servicios.

CAPÍTULO 3

El Control Interno y la Tecnología de Información

3.1. El Control Interno

3.1.1. Definición

A través de los años el concepto de Control Interno (conocido como “verificación interna” en los años ’30) y su enfoque ha ido cambiando al mismo ritmo que han evolucionado los procesos financieros y administrativos de las organizaciones. De tal forma que el órgano rector de los principios y normas de contabilidad a nivel mundial, el AICPA (American Institute of Certified Public Accountants), periódicamente ha cambiado el enfoque que tiene el Control Interno dentro de una organización, así pues, en el año 1936 definió el Control Interno de la siguiente manera:

“aquellas medidas y métodos adoptados en la misma organización para salvaguardar el efectivo y otros activos de la compañía así como verificar la exactitud aritmética del proceso de contabilización”.

Es importante notar que el enfoque dado al Control Interno en esa época estaba orientado hacia la protección del efectivo y en la determinación de fraudes en el manejo de los ingresos, dejando en un segundo plano a las cuentas por cobrar y los inventarios.

Luego, en 1949 el AICPA mediante un boletín especial denominado “Control Interno – Elementos de un Sistema coordinado y su importancia a la Gerencia y al Contador Público Independiente”, presentó la siguiente definición de Control Interno: “El control interno comprende el plan de organización, todos los métodos coordinados y las medidas adoptadas en el negocio, para proteger sus activos, verificar la exactitud y confiabilidad de sus datos contables, promover la eficiencia en la operaciones y estimular la adhesión a la prácticas ordenadas por la gerencia”.

Con esa nueva definición el concepto de Sistema de Control Interno va más allá de ser solamente medidas de salvaguarda del efectivo y aplicables solamente para los departamentos contables y financieros, y más bien, abarca a toda la organización desde el punto de vista financiero y administrativo.

Por ello, para reforzar esta idea el Comité de Procedimientos de Auditoría de la AICPA en octubre de 1958 expidió la siguiente declaración: "Los **controles contables** comprenden el plan de organización y todos los métodos y procedimientos que tienen que ver principalmente y están relacionados directamente con la protección de los activos y la contabilidad de los registros financieros; generalmente incluyen controles tales como los sistemas de autorización y aprobación, segregación de tareas relativas a la anotación de registros e informes contables de aquellas concernientes a las operaciones o custodia de los activos, los controles físicos sobre los activos y la Auditoría interna….Los **controles administrativos** comprenden el plan de organización y todos los métodos y procedimientos que están relacionados principalmente con la eficiencia de las operaciones, la adhesión a las políticas gerenciales y que, por lo común, sólo tienen que ver indirectamente con los registros financieros;

generalmente incluyen controles tales como los análisis estadísticos, estudios de tiempos y movimientos, informes de actuación, programas de adiestramiento del personal y controles de calidad".

Por lo tanto, podemos decir que el alcance del sistema de Control Interno abarca a cada uno de los departamentos y actividades de la empresa incluyendo aspectos como la función de Auditoría interna, los controles estadísticos de calidad, los subsistemas de recursos humanos, la planificación presupuestaria, planes de producción, etc. Ya se dejó atrás la idea de que el Control Interno solo debía abarcar los aspectos contables financieros y se lo ve a ahora como una cultura, idea y filosofía de toda la organización orientada hacia la eficiencia, eficacia, productividad y mejoramiento continuo de los procesos.

3.1.2. Importancia del Control Interno

Mantener un adecuado Sistema de Control Interno dentro de una organización es importante por las siguientes razones: mantener un eficiente control administrativo, cumplir con exigencias

gubernamentales y la responsabilidad de presentar información financiera confiable a terceros.

Tradicionalmente uno de los mecanismos preferidos por los dueños y gerentes de las empresas para llevar un control de la productividad y el manejo de sus recursos financieros y materiales, ha sido la observación directa “in situ” de las actividades realizadas por los empleados, con el fin de tener una certeza razonable de que se cumple cabalmente las directrices encomendadas.

Sin embargo, el crecimiento y evolución acelerada de las empresas, tanto en personal y operaciones, hace prácticamente imposible que el dueño o los administradores de una compañía puedan estar vigilando a cada uno de sus empleados o poner un capataz a cada uno para cerciorarse de que sean eficientes y productivos en el desempeño de sus actividades administrativas y operacionales. Por tanto, actualmente los administradores disponen de mecanismos de control como los informes financieros y análisis estadísticos para llevar a cabo el control de las operaciones y tomar decisiones. Dichos informes permiten a los gerentes conocer el cumplimiento de las políticas

institucionales, el apego a la planificación presupuestaria, la observación de los requerimientos de los organismos de control gubernamental, la situación financiera de la empresa respecto a liquidez y endeudamiento, entre otras cosas.

Es por ello, que poseer un eficiente Sistema de Control Interno garantiza a la administración disponer de medios de monitoreo que aseguren la razonabilidad de la información financiera y la eficiencia del desempeño administrativo y operacional de la organización.

Por otro lado, hoy en día luego de los escándalos financieros de multinacionales en todo el mundo, en muchos países y particularmente en el nuestro, se han intensificado los controles financieros estatales a fin de evitar desastres financieros en sus economías. Por ello, si una organización desea cumplir con las exigencias de control gubernamental, es necesario que implementen mecanismos de control eficientes y confiables. Por ejemplo, en el sector financiero es muy importante que las instituciones como bancos, financieras y cooperativas mantengan ciertos niveles de cumplimiento a las disposiciones de control emitidas por la Superintendencia de Bancos, relativo

al manejo de riesgos financieros, liquidez, información financiera, lavado de dinero, riesgo crediticio y sistemas de información. Además, es necesario que pongan a disposición del público sus Estados Financieros para que la ciudadanía pueda conocer su solidez y rentabilidad; y, de esa manera puedan saber si sus depósitos e inversiones se encuentran bien administrados, para lo cual, dicha información financiera deberá ser confiable y veraz.

Así mismo, las empresas que desean colocar sus acciones de capital en los mercados de valores necesitan presentar y dar una imagen de solidez y rentabilidad a sus accionistas; y, aquellas empresas que necesitan tener acceso a créditos de la banca necesitan dar confianza a sus acreedores en cuanto a su capacidad de pago; por lo que necesitan de una firma de Auditoría externa para que emita un dictamen sobre la razonabilidad de sus Estados Financieros y sobre la confianza de su Sistema de Control Interno.

Por ello, se han desarrollado un sin número de sistemas de información que permiten planificar, controlar y monitorear los riesgos inherentes y operativos de las organizaciones,

permitiendo que tanto gerentes, supervisores y auditores puedan, de acuerdo al enfoque de cada área, tomar los correctivos necesarios en caso de existir desviaciones significativas. Ejemplo de dichos sistemas son APOYO, DELPHOS, TEAMRISK, entre otros.

3.1.3. Objetivos del Control Interno

De acuerdo a la definición de Control Interno emitido por la AICPA, podemos distinguir de forma clara cuatro objetivos del Control Interno:

- La salvaguarda o protección de los activos de la empresa.
- La confiabilidad y razonabilidad de la información financiera.
- La eficiencia en las operaciones de la empresa.
- Cumplir con las políticas de la administración durante la ejecución de las operaciones.

No obstante, según las Normas Profesionales del AICPA, podemos clasificar los objetivos del Control Interno desde el punto de vista administrativo y desde el punto de vista contable,

aunque esto no significa que ambos sean mutuamente excluyentes, sino más bien, interdependientes.

Desde el punto de vista administrativo, el Control Interno busca:

- La elaboración de políticas y procedimientos contables, financieros y administrativos por parte de la administración.
- El cumplimiento a las políticas y procedimientos institucionales de todos los miembros de la organización.
- Que la administración establezca líneas de autorización para cada una de las transacciones u operaciones contables y administrativas.

Mientras que desde el punto de vista contable, un adecuado Sistema de Control Interno tiene como objetivos (relacionados con los objetivos administrativos):

- Que la ejecución de las transacciones u operaciones sean realizadas de acuerdo a políticas establecidas por la administración y cuenten con su respectiva autorización.
- La obtención de información financiera confiable y oportuna, a través, del registro de las transacciones y

eventos relacionados en las cuentas contables correspondientes para la emisión de estados financieros y control de los activos.

- Que el acceso a los activos de la empresa sea permitido únicamente con la autorización de la administración.
- La verificación de que los activos presentados en los registros contables sea igual a lo existente físicamente y que se tomen las debidas correcciones en el caso de existir diferencias.

3.1.4. Componentes de un Sistema de Control Interno

Un Sistema de Control Interno esta integrado por una serie de componentes interdependientes entre sí; lo que significa que la falta de cualquiera de ellos podría provocar cierta ineficiencia en el logro de los objetivos de control. A continuación se explica cada uno de estos componentes y su importancia:

- Ambiente de Control
- Plan de la organización.
- Procedimientos de autorización y registro.
- Función de Auditoría Interna.
- Personal idóneo.
- Confiabilidad.

El **Ambiente de control,** Comprende la modificación de la cultura organizacional hacia un objetivo claro de responsabilidad, ética y eficiencia por parte de todos quienes integran a la organización. Esto significa que desde el nivel operacional hasta la Alta Gerencia debe existir una mentalidad enfocada hacia el logro de los objetivos organizacionales, una idónea actitud profesional, lineamientos específicos de dirección, delegación correcta de funciones y responsabilidades y un adecuado sistema de gestión de los recursos humanos.

El **Plan de la Organización** comprende el conjunto de metas, objetivos, políticas y procedimientos de una organización, adaptado a sus necesidades generales y especificas de control. También se incluye la estructura organizacional conformada por organigramas a nivel general y departamental; así como, las líneas de autorización y las asignaciones de funciones y responsabilidades. Esto significa que dentro de una organización, ningún funcionario debería realizar todas las etapas de una operación desde su inicio hasta su culminación.

Además, es necesario dividir la organización en diferentes departamentos independientes, pero relacionados entre sí, cuyos gerentes son responsables de la realización adecuada de sus responsabilidades, de acuerdo a la autoridad que se les ha asignado, la misma que debería estar por escrito. Una correcta segregación departamental, mejora enormemente el control de una operación. Por ejemplo, si el departamento de bodega realiza una requisición de materia prima al departamento de compras y éste no realiza de forma inmediata el pedido a los proveedores; entonces, el departamento de bodega no podrá suministrar de materia prima al departamento de producción, lo que ocasionaría una reacción inmediata del gerente de producción quejándose a la gerencia general para que tome los correctivos necesarios.

Por lo tanto, un adecuado *Plan de la organización,* está enfocado hacia la independencia funcional y departamental; y, hacia una correcta asignación de responsabilidades y autorización, mejorando la eficiencia operativa y administrativa de toda la organización; y, alerta inmediatamente a la alta gerencia sobre posibles errores en el proceso de una operación para que tome los correctivos necesarios.

Los **procedimientos de autorización y registro** son aquellos que permiten tener un control sobre todo el ciclo de una transacción desde su autorización hasta su registro en los libros contables. Estos procedimientos también toman el nombre de "Manual de Contabilidad Interna" dentro de muchas organizaciones y en él se incluyen los mecanismos de comprobación de las autorizaciones efectuadas y de sus responsables, el catálogo de cuentas, la dinámica de registro de las transacciones, responsables de registro de las transacciones, procedimientos de ajustes y reclasificaciones, presentación y formatos de los estados Financieros y los métodos y políticas contables generalmente aceptadas que han sido adoptadas por la administración.

La **Auditabilidad,** está dado por la capacidad que tiene un Sistema de Control Interno de ofrecer información suficiente, íntegra y confiable respecto a las transacciones realizadas y sus responsables, con la finalidad de poder hacer un seguimiento a tales transacciones para revisión y control por parte de la administración y la función de Auditoría interna.

Contar con un **Personal Idóneo,** garantiza en gran manera el logro de los objetivos de un Sistema de Control Interno; para ello, la administración deberá seleccionar de manera muy minuciosa a las personas que ocuparán las áreas clave de la organización, de acuerdo a sus cualidades profesionales, conocimientos, experiencia, capacidad, responsabilidad y honradez. No obstante, el que una organización cuente con personal idóneo y un eficaz sistema de Control Interno no garantiza la eliminación por completo del riesgo de fraude o error; sino que lo minimiza.

La **Confiabilidad**, es muy importante dentro de un Sistema de Control Interno, ya que la administración debe estar segura de que cuenta con los mecanismos apropiados para poder prevenir, detectar y corregir el riesgo de fraude o error. Hay que resaltar el hecho de que la confiabilidad no es una característica indefinida del Sistema de Control Interno desde su implementación, ya que toda organización está en constante evolución y desarrollo; lo cual significa, que la administración general constantemente debe estar revisando y actualizando sus políticas y procedimientos al mismo ritmo de crecimiento de la organización.

3.1.5. Clasificación de los Controles

Los controles implementados dentro de una organización podrían clasificarse de acuerdo al momento en que se los ejecuta; por ello, se los ha clasificado como controles previos o preventivos, controles inmediatos o concurrentes y controles posteriores o detectivos. A continuación se explica en qué consiste cada uno de ellos:

Controles Preventivos.- Son aquellos enfocados hacia la prevención o disminución del riesgo de ocurrencia de errores o irregularidades. Para muchos, estos controles son los más importantes y económicos, ya que cuando son implementados de forma adecuada, representan un gran ahorro para la organización, puesto que se evitan pérdidas asociadas a la ineficiencia y el fraude. Ejemplos de estos controles son: las políticas y procedimientos institucionales, segregación de funciones, catálogos de cuentas, cifras de control, facturas prenumeradas, etc.

Controles Concurrentes.- Son aquellos que se ejecutan durante la realización de una operación o transacción. Es decir, que a

medida que se van completando cada una de las fases del ciclo transaccional, se revisa la conformidad del proceso con las políticas y procedimientos preestablecidos. Ejemplos de estos controles son: la verificación de firmas autorizadas, revisar que las facturas de los proveedores cumplan con los requisitos legales para su correspondiente pago, conciliación de las cifras de control, etc.

Controles Posteriores.- Son aquellos controles cuya finalidad es detectar los errores o irregularidades cometidos posteriormente a la realización del ciclo transaccional. A través de estos controles es posible conocer las debilidades o falencias de los controles preventivos y concurrentes. Muchas veces estos controles resultan ser costosos ya que requieren de un mayor análisis de la información y el volumen de transacciones examinadas es elevado. Ejemplos de estos controles son: la revisión de cuentas por cobrar vencidas, conciliaciones bancarias, revisión de transacciones eliminadas o modificadas, revisión de la razonabilidad de los saldos contables, etc.

3.2. Relación entre el Control Interno y la Tecnología de Información.

3.2.1. Debilidades y Amenazas en los Sistemas de Información

En capítulos anteriores se ha explicado la versatilidad y capacidad que tienen los sistemas de información para el procesamiento, almacenamiento, análisis y comunicación de la información de las empresas, poniendo a disposición de la alta gerencia herramientas estratégicamente diferenciadoras para la toma de decisiones y competitividad. No obstante, toda esta revolución ha conllevado a nuevos riesgos y amenazas tanto internas como externas relacionadas con el uso y acceso a la información institucional por parte de personas ajenas a la organización.

Por ello, el que una organización posea un Sistema de Información robusto y de última tecnología no garantiza que esté exento de sufrir problemas o inconvenientes en el manejo de la información, ya que muchos de los sistemas desarrollados y que están disponibles en el mercado padecen de ciertas vulnerabilidades asociados a aspectos tecnológicos, organizacionales y gerenciales. Entre las principales

vulnerabilidades que presentan los sistemas de información tenemos:

- Errores en el diseño lógico del sistema.
- Falta de incorporación de rutinas de control para el ingreso, procesamiento y salida de la información.
- Poca participación, a nivel de asesoría, del departamento de Auditoría interna en el diseño del sistema.
- Poca participación de los usuarios en la especificación de los requerimientos del sistema de información.
- Poca anticipación a posibles amenazas que pudieran afectar la seguridad del sistema de información en el futuro.

Asimismo, entre las amenazas más comunes a las que está expuesta la información se encuentran: incendio, fallas de hardware y software, robo, sabotaje, destrucción, divulgación, fraude, chantaje, virus informáticos, hackers, entre muchos otros. Los mismos que podrían significar enormes pérdidas tangibles e intangibles a las organizaciones, tanto públicas como privadas que sean víctimas de estas amenazas.

A todo esto, cabe mencionar los grandes fraudes corporativos que están a la orden del día en los periódicos y noticieros de

todo el mundo, los cuales, son realizados por los delincuentes de “cuello blanco” (presidentes ejecutivos y gerentes) a través de sus sistemas de información ocasionando grandes pérdidas financieras a terceros y dejando en la calle a miles de trabajadores.

Generalmente, las razones por la cual muchas personas cometen delitos informáticos se debe a: intereses particulares, competencia desleal, beneficiar a terceros, hobby, oportunidad, venganza, egolatría, problemas psicológicos, etc. Además, a todo ello hay que sumarle factores como: el incremento de profesionales y personas interesadas en el área informática, la disminución en el costo de la tecnología que ha permitido el acceso a las computadoras a millones de personas, la adopción de tecnología de información de casi todas las empresas en el mundo, la falta de adopción de políticas sustentables para la seguridad de la información y el uso de las telecomunicaciones; lo cual, origina nuevas amenazas de acceso indebido y manipulación de la información.

Es por ello, que se hace cada vez más importante desarrollar medidas de seguridad en los sistemas de información

implementando controles administrativos e informáticos, con la participación decidida de la gerencia general, la asesoría de la unidad de Auditoría Interna; y, la colaboración de cada uno de los Jefes Departamentales y Usuarios en general con la finalidad de lograr:

- La integridad, confidencialidad y disponibilidad de la información.
- Disponer de medidas y procedimientos para proteger los activos informáticos en caso de desastre o destrucción.
- Garantizar la continuidad operativa de la organización, a través de sus sistemas de información, en forma permanente.

3.2.2. El Control Interno Informático

El Control Interno informático es un subsistema dentro del Sistema de Control Interno de la organización y comprende todos los procesos administrativos y sistematizados dentro de una organización, cuyo objetivo es garantizar el control y seguridad de los recursos informáticos para una eficiente, efectiva y económica gestión operacional.

De lo mencionado anteriormente, se puede decir que el control interno informático abarca la salvaguarda, integridad y disponibilidad de la información, la protección de los equipos computacionales, mejorar la eficiencia y eficacia operativa, disminuir los riesgos de fraude y error; y, asegurar la continuidad operativa de la organización; los cuales, sin ninguna duda, son las principales preocupaciones de los administradores modernos, quienes hoy más que nunca se han dado cuenta de la importancia de la implementación de los controles informáticos, muchas veces sin importarles la inversión económica que esto signifique.

3.2.3. Objetivos del Control Interno Informático

Los objetivos del Control Interno Informático, podría dividirse en generales y específicos.

Entre los objetivos generales tenemos:

- El cumplimiento de las políticas y procedimientos establecidos por la alta gerencia y demás normativas legales relacionadas con el uso de tecnología.

- Establecer entre todos quienes integran la organización, un ambiente de responsabilidad y control en el manejo de los recursos informáticos.
- Servir como apoyo a la alta gerencia para el control de los recursos informáticos y como pistas de Auditoría para la función de Auditoría Interna o los auditores externos.
- Garantizar una adecuada gestión de la función de PED, la calidad del servicio informático y la satisfacción de los usuarios.

Mientras que entre los objetivos específicos tenemos:

- El cumplimiento de la planeación informática de la organización.
- Mantener el control de los cambios realizados a los Sistemas de Información.
- Asegurar el acceso a la información solo a personal autorizado.
- Asegurar la calidad del desarrollo y mantenimiento de los sistemas de Información.
- Proteger los Sistemas contra ataques informáticos provenientes desde el Internet (Hackers) y minimizar el riesgo de infección por virus.

- Mantener en orden las licencias y contratos por el uso de Sistemas y aplicativos.

3.2.4. Clasificación de los controles informáticos

Los controles informáticos son muy variados en cuanto a su aplicación, costo y beneficios; y, su implementación dentro de una organización, dependerá de las necesidades y el entorno estructural y operacional que esta tenga.

Los controles informáticos podrían clasificarse respecto al momento de **ejecución** y respecto a **objetivos de control**. Esto no significa que sean mutuamente excluyentes; ya que todos los controles tienen un objetivo de control; pero, son ejecutados en diversos momentos.

Respecto al momento en que se las ejecuta, tenemos:

Controles Preventivos.- Son aquellos que tienen como objetivo disminuir el riesgo de amenaza. Como por ejemplo: restringir la instalación de software ilegal, establecer perfiles de usuario, utilizar software de acceso al sistema, etc.

Controles Detectivos.- Son aquellos que buscan detectar los errores e irregularidades de forma inmediata, en caso de que hayan fallado los controles preventivos. Ejemplo de ello son: la validación de los datos de entrada, registro de errores o anomalías en el procesamiento de datos mediante LOG's del sistema, bloqueo de contraseñas luego de algunos intentos de ingreso fallidos, etc.

Controles Correctivos.- Son aquellos que buscan la corrección de ciertas anomalías sucedidas. Ejemplo: utilización de respaldos luego de un desastre, etc.

Respecto a los objetivos de control, podemos mencionar:

Controles Organizacionales.- Estos están orientados hacia la gestión del departamento de sistemas en cuanto al cumplimiento de las políticas y procedimientos informáticos, el manejo interno de los proyectos informáticos, la elaboración de documentación para revisión y control, etc. Dentro de esta categoría se encuentran los siguientes controles:

- Elaborar un Manual de políticas y procedimientos del Departamento o Unidad de Sistemas, incluyendo las funciones y responsabilidades del personal de informática.
- Elaborar los siguientes planes: Plan Estratégico de Sistemas de Información, Plan Maestro Anual, Plan o Manual de controles y seguridades, Plan de Contingencias y Continuidad del negocio.
- Establecer o adoptar estándares en cuanto a la adquisición, desarrollo y mantenimiento de Sistemas de Información.
- Establecer de manera formal el modo en que interactúa el departamento de Sistemas con los demás departamentos para la solicitud y entrega de nuevos sistemas o cambios a los existentes.
- Disponer de un nivel adecuado de independencia del personal de informática con el resto de funcionarios; lo cual, debe verse reflejado en el organigrama general de la empresa.
- Clasificar la información de acuerdo a su importancia y confiabilidad; y, establecer el personal autorizado a acceder a ella.
- Establecer de manera formal, la función de Oficial de seguridad Informática (OSI) y la de Auditoría Informática.

Controles de los recursos informáticos.- Estos buscan cuidar la seguridad de los recursos informáticos (hardware y software), el correcto funcionamiento de los equipos y el manejo adecuados de los programas por parte de los usuarios, para lograr el correcto desempeño de las actividades informáticas de la organización. En esta categoría están los siguientes controles:

- Establecer políticas y procedimientos relativos a la adquisición y utilización de los recursos informáticos.
- Mantener inventarios actualizados de los recursos informáticos, tanto del hardware como del software.
- Mantener respaldos de los principales archivos de los usuarios relativos al giro del negocio.
- Mantener contratos de mantenimiento de los equipos informáticos con una empresa especializada.
- Mantener una bitácora de mantenimiento de los equipos informáticos en el que se detalle el equipo afectado, el problema presentado, posibles causas, fecha, etc.
- Mantener conectados los equipos informáticos a los sistemas de energía ininterrumpida (UPS), para protegerlos en caso de variaciones en el voltaje y tener tiempo para cerrar el sistema operativo apropiadamente.

- Disponer de un plan de contingencias en caso de desastres como incendios, terremotos, sabotajes, robo, etc., que garantice la continuidad operativa del negocio.
- Establecer controles físicos a los recursos informáticos, restringiendo el acceso a ellos de personal no autorizado, mantenerlos en sitios seguros, etc.
- Mantener actualizada la lista del personal autorizado para acceder al sistema; así como sus perfiles y permisos de acceso. Se debe tener mucho cuidado con las Cuentas de Usuario del personal que ha sido dado de baja en la empresa para que sean eliminados inmediatamente, pues de no ser así existe el riesgo de que otros funcionarios las utilicen fraudulentamente.
- Establecer seguridades de protección contra virus informáticos que incluyan: la adquisición de software antivirus, restringir la instalación de software sin licencia, evitar la descarga de programas basura desde Internet, etc.

Controles de desarrollo, explotación y mantenimiento de los Sistemas.- Estos controles se orientan hacia el ciclo de vida de los sistemas de información; de tal forma que se establezca una relación costo/beneficio de los sistemas a implementarse, se

haga un correcto levantamiento de la información con la participación de los usuarios, se utilicen estándares de calidad en el desarrollo de los sistemas, se realice un adecuado mantenimiento a las aplicaciones, etc. Entre los principales controles en esta categoría se encuentran:

- Establecer una metodología formal para todo el ciclo de vida de los Sistemas de Información, su definición y documentación, diseño de entrada, procesamiento y salida, pruebas de validación y conformidad, pistas de Auditoría, etc.
- Establecer funciones y responsabilidades para los supervisores, analistas y programadores de los proyectos internos de desarrollo de Sistemas.
- Establecer de manera formal el proceso de solicitud de requerimientos de nuevos sistemas, su aprobación, análisis de factibilidad y tiempo estimado para su puesta en producción.
- Establecer procedimientos para la inversión en nueva tecnología, justificación, aprobación, presupuesto, contratos de garantía y licencias de ser necesario.
- Establecer procedimientos en cuanto al mantenimiento que se de a los Sistemas de Información, justificación,

costo-beneficio y pistas de control de los cambios efectuados y sus responsables.

- Incorporar dentro del presupuesto global de la empresa, el presupuesto de la Unidad de Sistemas. Este deberá incluir: inversiones en nuevas tecnologías, adquisición de programas y equipos, y modificaciones a los programas existentes.
- Establecer procedimientos sobre el uso adecuado de los equipos, carga de trabajo de los desarrolladores, distribución de proyectos, etc.
- Garantizar la seguridad física de los recursos informáticos a través de: restringir el acceso a la Unidad de Sistemas solo a personal autorizado; tomar medidas preventivas contra desastres, tales como: incendio, terremoto, robo, inundación, etc.; y, contar con un Plan de Contingencias que garantice la salvaguarda de los recursos informáticos y la continuidad operacional de la empresa.
- Disponer de seguridades lógicas, tales como: establecimiento de seguridades de acceso a la información, disponer de software de seguridad de redes de área local y firewalls contra ataques externos, poseer un plan de seguridad informática en el que se especifiquen

los pasos a seguir en caso de violaciones de la seguridad del Sistema, uso de claves de usuario y contraseñas, etc.

Controles del flujo de la información.- Estos controles tienen como objetivo asegurar que los sistemas de información funcionen correctamente durante todo el ciclo transaccional, durante la entrada, procesamiento y salida de la información. En esta categoría se encuentran los siguientes controles:

- *En la entrada de datos:*
  - Verificación por parte de los operadores de la razonabilidad de los campos críticos, de acuerdo al tipo de dato ingresado; ejemplos: precios, cantidad vendida, cantidad comprada, etc.
  - Ingreso doble de los campos críticos para garantizar su exactitud.
  - Uso de la Mesa o Tablero de Control, que consiste en la conformación de un equipo de operadores dentro de la Unidad de Sistemas, quienes son los encargados de recibir la información de los usuarios(por lo general de varias agencias o sucursales), verificar su

validez e integridad y llevar una bitácora de errores para su corrección y posterior revisión.

- Utilizar dígitos de verificación, los cuales, establecen la razonabilidad de ciertos campos, en base a algoritmos especiales.
- Establecer controles de acceso a los computadores de ingreso de datos considerados críticos, ya sean estos de proceso por lotes o en línea.
- Utilizar cifras de control, en donde se compare los totales manuales con los totales que presenta el Sistema.
- Incorporar dentro de los Sistemas, subrutinas de verificación de los datos ingresados antes de ser almacenados o alimentados en otros procesos y sistemas.

o *En el proceso de datos:*

- Utilizar códigos de transacción para cada operación; los mismos que no podrán ser repetidos e identificarán de forma única a cada operación; también, se los conoce como claves principales.

- La designación de un operador de control que verifique los listados de las transacciones ingresadas versus las transacciones procesadas para determinar su conformidad. Esto se utiliza mucho en las empresas internacionales de envío y recepción de remesas de dinero.
- El uso de Totales de Control en el que se verifica; por ejemplo, tomando el caso anterior, que el total de las transacciones de remesas recibidas de un País X, sea igual o menor al total de remesas pagadas de manera local, tanto en el número de transacciones como en el valor monetario que representa.
- Uso de códigos secuenciales, para asignar a cada uno de los registros procesados, un número secuencial único que permita identificar registros faltantes, ya sea esto, por eliminación o error del sistema durante el ingreso de transacciones.
- Elaborar de manera formal los manuales operativos de los programas; también conocidos como manuales de usuario, para el correcto manejo de los programas por parte de los operadores.

- Definir apropiadamente los roles de usuario para los operadores, de tal forma, que estos no puedan realizar funciones dentro del Sistema, más allá de lo estrictamente necesario.
- Incorporar rutinas automáticas de detección de transacciones incorrectas, ya sea por inconsistencia, datos inválidos u omisión de campos clave.
- Establecer rutinas automáticas de generación de respaldos de las Bases de Datos institucionales, para poder hacer frente a posibles siniestros o pérdidas de información.
- Restringir de manera adecuada el uso de utilitarios informáticos avanzados o programas potencialmente peligrosos, como los manejadores de archivos y bases de datos, que puedan tener acceso a la información institucional.

o *En el proceso de salida:*

- Comparar que los totales de entrada coincidan con los totales de salida, con el objeto de identificar errores de procesamiento o modificación de los registros almacenados.

- Comparar que el número de transacciones procesadas y que son presentadas en los reportes de salida sea igual al número de transacciones de entrada.
- Registrar en una bitácora las concordancias, errores y problemas sucedidos durante el procesamiento de datos en el centro de cómputo. Esta información debería ser mantenida para futuras revisiones de Auditoría.
- Establecer procedimientos respecto a las características que deben tener los informes de salida de los sistemas de información. Algunas de las principales características, tenemos: nombre del sistema, contenido o titulo, departamento, lapso que abarca, confidencialidad, nombre de usuario, hora, fecha, número de páginas, espacio para firma de revisión/autorización, etc.
- Establecer listas de control y rastreo de transacciones en el que se comparen el número de salidas con el número de entradas y de esa forma detectar transacciones no procesadas.

- Los usuarios deben realizar revisiones periódicas de las transacciones ingresadas por ellos y compararlos con las salidas o informes generados.
- Detectar y eliminar aquellos informes que no son necesarios para los usuarios.

Controles de Bases de Datos.- Estos tienen como objetivo garantizar la correcta administración de la base de datos, la protección de la información almacenada y garantizar su restauración en caso de desastre. En esta categoría tenemos los siguientes controles:

- Utilizar un Sistema de administración de bases de datos (DBMS), dependiendo de las necesidades de la empresa y el volumen de registros que maneje.
- Tener a un responsable de la administración de la información de la base de datos (**DBA**- Data Base Administrator), el cual deberá planificar, organizar y controlar la base de datos de la organización, con responsabilidad y dominio técnico sobre el tema.
- Establecer controles de supervisión de la base de datos mediante el manejo de LOG's sobre los accesos a la base de datos, registros modificados, identificador (ID) del

usuario, permanencia de los usuarios durante las sesiones, accesos indebidos, accesos negados, errores de procesamiento, errores de validación, etc. Dichos LOG's deben ser revisados frecuentemente para encontrar irregularidades y servirán como pistas de Auditoría.

- Establecer una adecuada segregación de funciones en cuanto al acceso a la base de datos, para el administrador, programadores, analistas, auditores, operadores y usuarios.
- Limitar el acceso del administrador, para que este no tenga acceso a la base de datos de forma indebida y no pueda realizar transacciones o modificaciones a la base de datos sin autorización previa.
- Establecer un plan de contingencia para la recuperación de la información almacenada en la base de datos.
- Establecer seguridades para la protección de la base de datos que disminuyan el riesgo de ataques externos y sabotajes internos.
- Mantener por lo menos dos ambientes o conexiones para el acceso a la base de datos; el uno sería un ambiente de pruebas con datos ficticios para el acceso de programadores y analistas, y el otro de producción con los

datos reales del día a día al cual tienen acceso los usuarios a través de los sistemas.

- Elaborar manuales de diseño de la base de datos, en donde se especifiquen la estructura de las tablas, campos clave, relaciones, tipos de datos, formatos, etc.
- Elaborar manuales operativos de los sistemas de información para un correcto uso por parte de los usuarios.
- Mantener controles formales de la base de datos, en el que el administrador de la base de datos presente bitácoras e informes al departamento de Auditoría interna o a la gerencia general sobre los controles y seguridades implementados.
- Establecer mecanismos de supervisión para la instalación y uso de utilitarios, en las computadoras de los usuarios, ya que estos paquetes informáticos podrían permitir el acceso y modificación de la base de datos sin dejar huella. Esta es una de las principales responsabilidades del administrador de la base de datos. Un ejemplo de dichos paquetes es MS Access.
- Designar en forma específica la terminal que será utilizada por el **DBA** para la administración de la base de datos.

Dicha terminal deberá estar ubicada en el centro de cómputo bajo estrictos controles de acceso físico y lógico.

Controles en el Entorno de Red.- Buscan garantizar la seguridad en la transmisión de datos dentro de la red privada de la organización y que esta no pueda ser accedido por personas no autorizadas. Tenemos los siguientes controles:

- Definir políticas y procedimientos respecto a la administración y seguridad de la red de área local.
- El acceso a la red desde las terminales debe ser a través de un ID de usuario y una contraseña privada.
- Implementar herramientas de administración de la red que permitan una adecuada planificación, desempeño y control de la misma, que garantice la seguridad, integridad, confiabilidad y disponibilidad de la información.
- Establecer un personal específico para la administración y control de la red.
- Elaborar manuales completos sobre la arquitectura de la red, especificando el número de terminales, la distribución de los equipos en red, ubicación de los servidores y routeadores, conectividad con otras redes LAN o WAN,

sistemas operativos, utilitarios, lenguajes de programación, etc.

- Implementar y supervisar adecuados controles para el acceso a Internet a través de la red local, para que este no sea utilizado de forma indebida para fines ajenos a los de la organización. Para ello, se puede utilizar diversos paquetes informáticos disponibles en el mercado.
- Supervisar la velocidad de transferencia de archivos utilizando el Internet; y, la agilidad en el acceso a los sistemas de información a través de la red.

Controles de Comunicación de Datos.- Estos buscan mantener niveles de seguridad adecuados en la transmisión de datos hacia las redes externas como Internet y las conexiones remotas, de tal forma que no pueda ser interceptada por piratas informáticos tales como hackers y crackers quienes podrían hacer un mal uso de la información. En esta categoría tenemos los siguientes controles:

- Asignar a cada Terminal un código o dirección IP para que sea identificado durante su conexión al sistema de comunicación de datos.

- Definir una tabla de verificación en la que se almacene las direcciones IP autorizadas para acceder al sistema de comunicación de datos para evitar accesos no autorizados.
- Los archivos transferidos deben poseer una cabecera en el que se especifique la fecha, hora, destinatario y otro tipo de información que permita identificarlos de manera única.
- Utilizar técnicas y software de encriptación de los datos al transferir los archivos de manera remota, garantizando su confidencialidad e integridad en caso de ser interceptado por personas ajenas a la organización.
- Hacer uso de firewalls para garantizar que no existan accesos indebidos a la red interna por parte de hackers.
- Tener MODEMS y líneas telefónicas de respaldo que puedan ser utilizados en caso de suceder un siniestro o daño en los MODEMS y líneas principales.
- Establecer procedimientos predefinidos para la corrección de errores presentados en el sistema de comunicación de datos; así como también, la forma en que se llevarán bitácoras en las que se registren los errores presentados, posibles causas, fecha y hora, terminales afectadas, etc.

- Mantener contratos de mantenimiento de los equipos de comunicación de datos y de los equipos informáticos en general.
- Disponer de manuales completos sobre el uso de los sistemas de comunicación de datos, su instalación, configuración y demás aspectos técnicos para futuras Auditorías y revisiones de control.
- Establecer controles y seguridades físicas como mantener un plan de contingencias para el caso de daños en los equipos de comunicación de datos, poseer sistemas de energía ininterrumpida, etc.
- Mantener una Mesa de Control en el que se supervise y atienda las situaciones especiales que puedan presentarse durante la transmisión de datos.
- Mantener un Plan de Capacitación anual en el que los responsables del departamento de TI reciban capacitación periódica sobre la administración y seguridad de los sistemas de comunicación.

Controles de Sistemas Distribuidos.- Esos buscan garantizar la integridad y disponibilidad de la información en los sistemas distribuidos. Un sistema distribuido es una red de computadoras

localizadas en lugares remotos, cuyo procesamiento de datos se realiza en su respectiva localidad y se encuentran conectados a una computadora central. En esta categoría se encuentran los siguientes controles:

- Diseñar una adecuada arquitectura de red de los sistemas distribuidos, acompañado de políticas y procedimientos bien definidos sobre las terminales que van a estar en línea y las atribuciones de acceso que tendrán dentro de la base de datos cada uno de los usuarios.
- Establecer controles de autentificación de la base de datos matriz, de tal forma que solo determinadas terminales puedan ingresar o modificar transacciones dentro del sistema.
- Establecer controles de acceso físico a las terminales, así como identificadores de usuario y contraseñas; tanto a nivel del entorno de red, como de los sistemas de información distribuidos.
- Bloquear el acceso al sistema en caso de ser sometido a mantenimiento o durante horarios y días no hábiles.
- Emitir informes diarios sobre el desempeño del sistema durante los procesos de transmisión y recepción, procesamiento y salida de la información.

- Mantener pistas de Auditoría para la correcta detección de errores e irregularidades durante la transmisión y procesamiento de la información.
- Mantener un inventario de los equipos computacionales que integran la red distribuida tanto en la Matriz como en las sucursales remotas.
- Disponer de un plan de contingencias en el que se establezcan las medidas preventivas, inmediatas y posteriores ante posibles amenazas.
- Monitorear constantemente el estado de la red, accesos, carga de transmisión de datos, accesos indebidos o innecesarios, errores de transmisión, etc.

3.3. Metodología para Diseñar Controles en Sistemas Computarizados.

3.3.1. Desafíos en la implementación de los controles informáticos

Ya hemos visto los fundamentos conceptuales respecto al significado de Control Interno, su clasificación, sus componentes, relación con la tecnología de información e importancia para la organización. Asimismo, se ha hecho una descripción de los aspectos que involucra el control interno informático y los principales controles a tomar en cuenta en un

ambiente de procesamiento electrónico de datos. Sin embargo, la implementación de dichos controles, representan un verdadero desafío para muchas organizaciones, desde el punto de vista tecnológico, económico y organizacional. A continuación se explica las razones por las cuales la implementación de los controles informáticos es un verdadero desafío para muchas organizaciones.

Muchos administradores de empresas consideran que no es necesario invertir demasiado en tecnología y que basta con adquirir o desarrollar un sistema financiero-contable para la realización de sus actividades diarias; dejando a un lado aspectos como la seguridad de la información, y, las posibles amenazas y vulnerabilidades que pudieran tener en el futuro.

Además, el continuo cambio tecnológico origina nuevas amenazas y esto obliga a que continuamente se cambien los controles existentes, ya que sufren el riesgo de quedar obsoletos. Por otro lado, muchos de los controles para garantizar la seguridad informática son muy costosos y no todas las organizaciones están en la capacidad para invertir en controles y seguridades informáticas.

3.3.2. Elementos para la implementación de los controles informáticos

Al momento de implementar un sistema de control interno a nivel informático, es necesario considerar algunos elementos que ayudarán de sobremanera a la implementación exitosa de un Plan de Seguridad Informática. Los elementos son los siguientes:

- **Estructura de Control:** Es importante que dentro de la organización se establezca una estructura de control conformado por un comité de seguridad de la información, la función de Auditoría Interna y la función del Oficial de Seguridad Informático.
- **Equipo de Trabajo:** Es necesario conformar un equipo de trabajo con suficiente preparación académica, experiencia y dominio sobre el tema de las seguridades informáticas y que conozca la organización. Dicho equipo puede estar conformado por ejecutivos de la organización, auditores y consultores externos.
- **Normas:** La componen el conjunto de políticas, procedimientos, normas, estándares y marco legal sobre el cual se van a fundamentar los controles a implementarse.

- **Objetivos de Control:** Es lo que se busca controlar dentro de los procesos operacionales de la organización. Estos constituyen la "estructura ósea" de todo el sistema de control interno informático.
- **Procedimientos de Control:** Son las actividades a seguirse para lograr los objetivos de control de forma efectiva. Establecen la forma en que deben llevarse a cabo el control informático.
- **Herramientas de Control:** Son las que permiten llevar a cabo los procedimientos de control. Dichas herramientas la constituyen los paquetes informáticos, equipos y tecnología para llevar a cabo los controles, como por ejemplo: los sistemas de monitoreo de la red de área local, los programas de análisis de datos, etc.

Una vez establecido cada uno de estos elementos que serán utilizados para la creación del sistema de control interno informático, se debe establecer la metodología a seguirse para la implementación del sistema de control interno informático, realizando una armoniosa combinación entre cada uno de estos elementos.

3.3.3. Metodologías para la implementación del Control Interno Informático

A pesar de que existen una gran variedad de metodologías para la implementación de controles informáticos, basadas en diferentes estándares a nivel internacional, se las puede clasificar en dos grandes grupos: Cuantitativas y Cualitativas.

Metodologías Cuantitativas.- Se basan en el uso de modelos matemáticos para el análisis de riesgos, en el que se asigna a cada riesgo una probabilidad de ocurrencia. Luego utilizando simulaciones sofisticadas se puede establecer el grado de riesgo al que está expuesto la organización y los controles a implementarse para la disminución del riesgo.

Entre los beneficios de esta metodología están: el uso de técnicas y modelos matemáticos para el análisis de riesgo; se puede establecer, de acuerdo a las necesidades internas, el grado de significancia (confianza) para le elección de los controles; y, facilita la combinación de diversos tipos de debilidades y amenazas.

Sin embargo, esta metodología presenta algunas desventajas como son: la necesidad de profesionales altamente capacitados para el análisis de riesgos; la falta de información y estadísticas reales para la estimación de las probabilidades de ocurrencia de un riesgo; solo se pueden considerar aquellos impactos potenciales que sean cuantificables; y, generalmente solo las grandes firmas de auditoría y consultoría multinacionales ofrecen este tipo de asesoría.

Metodologías Cualitativas.- Se basan en la experiencia y capacidad del profesional a cargo de la implementación de los controles informáticos. Esta utiliza métodos estadísticos no sofisticados para identificar las posibles amenazas dentro de la organización para luego seleccionar los mecanismos de respuesta a tales amenazas.

Entre las principales ventajas de este tipo de metodologías, se encuentran: flexibilidad para el análisis de la organización y sus posibles amenazas, el enfoque de evaluación se extiende a toda la organización, facilidad para poder identificar posibles amenazas sin la necesidad de realizar análisis matemáticos

complejos y sus factores de influencia externa; y, puede considerar impactos potenciales de carácter cualitativo.

3.3.4. Clasificación de la Metodologías para la implementación de Controles Informáticos

Para la obtención del Sistema de Control Informático se pueden utilizar diferentes metodologías o la combinación de varias de ellas. Entre las principales tenemos: Análisis de Riesgos, Clasificación de la información y los Objetivos de Control. A continuación se explica cada una de ellas:

Análisis de Riesgos.- Se basan en el estudio de la probabilidad de que ciertos riesgos aparezcan o constituyan una amenaza para la organización. A esta metodología, en el sector financiero se la conoce como SCORING (puntajes), puesto que se pondera una calificación a cada riesgo.

Dentro de los procedimientos de esta metodología tenemos:

1. Establecer posibles amenazas.
2. Asignar una probabilidad de ocurrencia para cada amenaza.
3. Seleccionar las amenazas más significativas.

4. Identificar el impacto en la continuidad operativa-informática de la organización.
5. Estimar el impacto económico que representa la ocurrencia de cada amenaza (Scoring).
6. Seleccionar los servicios u operaciones críticas a recuperar de forma inmediata.
7. Identificar las alternativas de solución.
8. Seleccionar las alternativas más adecuadas y económicas.
9. Establecer procedimientos de control para la prevención de las amenazas.
10. Establecer procedimientos de control correctivos para corrección de los eventos negativos.

Clasificación de la Información.- Consiste en la diversificación de las medidas correctivas de acuerdo a la criticidad de la información. Esta metodología se basa en un análisis de la información, su segregación de acuerdo a la importancia que esta tiene y la incorporación de controles a la medida. Esta es una metodología muy interesante para empresas que buscan implementar un plan de Contingencias y continuidad del negocio. Grandes Bancos nacionales, hace aproximadamente

diez años atrás s dieron cuenta de la importancia de este tipo de planificación cuando cierto Banco grande en aquella época, sufrió un incendio que provocó la pérdida de gran parte de la información financiera y transaccional.

Dentro de esta metodología se pueden enumerar los siguientes procedimientos para su implementación:

1. Identificar lo que representa información significativa para la organización.
2. Elaborar un inventario de todos los activos de información de la organización. Los activos de información esta compuesto por los programas, bases de datos, archivos y demás estructuras de almacenamiento de datos.
3. Identificar o designar al propietario de la información. El propietario de la información es la persona responsable de la custodia y manejo de la información.
4. Establecer una clasificación de la información: pública, restringida, confidencial, secreta.
5. Establecer las medidas de control para cada clasificación de la información.

6. Correlacionar la información, de tal manera que se establezca para cada clasificación, sus respectivos objetivos de control, archivo maestro relacionado en el sistema, autorizaciones, validaciones, etc.
7. En base a lo anterior, elaborar el Plan de Controles y Seguridades.
8. Monitorear la efectividad del Plan y realizar los correctivos necesarios.

Objetivos de Control.- Consiste en la identificación de los aspectos informáticos que se desea controlar y los controles necesarios para el efecto. El estándar COBIT, que es estudiado más adelante, muestra los principales objetivos de control que deben considerarse en toda organización. Los procedimientos son los siguientes:

1 Análisis de la organización en cuanto a su estructura, políticas, procedimientos, funciones y responsabilidades.
2 Selección de estándares internacionales y generalmente aceptados para la seguridad de la tecnología de información, tales como: COBIT, SISAS, ISO, etc.
3 Definir los objetivos de control.

4 Definir los controles específicos para cada objetivo de control.

5 Definir las necesidades tecnológicas para la implementación de los controles.

6 Definir los procedimientos de control, que no son otra cosa más que establecer la forma en que se realizarán los controles.

7 Definir los recursos humanos necesarios para la implementación, lo que podría incluir reclutamiento y capacitación.

8 Implementación del sistema de control interno

9 Documentar el sistema a través del Plan de Controles y seguridades.

CAPÍTULO 4

Normativa y Legislación en Auditoría de Sistemas

4.1. Estándares mundiales en seguridad de la información

4.1.1. Introducción

Como hemos visto a lo largo de este trabajo, la tecnología de información ha ido evolucionando de forma permanente a través de los años, lo cual ha originado la aparición de estándares y normas en TI que se mantengan a la par de dicha evolución.

Un ejemplo, sobre la importancia de mantener altos estándares en la seguridad de la información, se presenta en las compañías internacionales especializadas en el manejo de información de

riesgo crediticio, también conocidas como “Buró de Riesgos Crediticios”, en el que los organismos de control financiero gubernamental (en nuestro País, la Superintendencia de Bancos y Seguros) les conceden a estas empresas el manejo de la información crediticia (Central de Riesgos) de sus Países; al cual mediante una suscripción, pueden acceder las instituciones financieras y comerciales a consultar la información crediticia de cualquier ciudadano que aspire a un crédito.

Para que estos Buró’s puedan calificar y dar sus servicios en algún País extranjero, se les pide un certificado que demuestre que se encuentran alineados con alguno de los estándares internacionales de seguridad informática; ¿la razón? Bueno, por lo general estas empresas mantienen sus Bases de Datos de forma centralizada en sus respectivos países de origen, de tal forma, que está en riesgo la información confidencial crediticia de todo el País, que en caso de caer en otras manos, podría ser utilizado para fines particulares o de forma maliciosa. En adelante, se explican de forma resumida algunos estándares y normas de TI y se profundiza de forma detallada en las dos normas más reconocidas y utilizadas por los auditores de TI: COBIT e ISO 17799.

4.1.2. Principales Estándares Internacionales

En la siguiente tabla, se mencionan los principales estándares a nivel internacional que son utilizadas por los profesionales de TI y de Auditoría informática para asegurar la seguridad de la información:

ESTÁNDAR	ORGANISMO EMISOR
COBIT (Objetivos de Control para tecnología de información y tecnología relacionada)	**ISACA** (Asociación de Auditoría y control de Sistemas de Información).
ISO 17799 (Estándares de Administración de Control y Seguridad de la Tecnología de Información)	**ISO** (Organización Internacional de Estándares)
"Administración del Control de Datos de la Tecnología de Información"	**CICA** (Instituto Canadiense de Contadores Certificados)
"Administración de la inversión de tecnología de Inversión: un marco para la evaluación y mejora del proceso de madurez"	**GAO** (Oficina de Contabilidad General de los Estados Unidos)
SYSTRUST (Principios y Criterios de Confiabilidad de Sistemas)	**AICPA** y **CICA** ("Asociación de Contadores Públicos" y el "Instituto Canadiense de Contadores Certificados")
CMM (Modelo de Evolución de Capacidades de software)	**SEI** (Instituto de Ingeniería de Software)
"Administración de Sistemas de Información: Una herramienta de evaluación práctica"	Directiva de Recursos de Tecnología de Información.

"Guía para el Cuerpo de Conocimientos de Administración de Proyectos"	Comité de Estándares del Instituto de Administración de Proyectos
SSE – CMM (Ingeniería de Seguridad de Sistemas – Modelo de Madurez de Capacidades)	NSA (Agencia de Seguridad Nacional con el apoyo de la Universidad de Carnegie Mellon)
"Administración de Seguridad de Información: Aprendiendo de Organizaciones Líderes"	GAO (Oficina de Contabilidad General de los Estados Unidos)

Tabla 4.1. Estándares Internacionales sobre Seguridad de TI

Objetivos de Control para Tecnología de Información y Tecnología Relacionada (COBIT)

Este es un estándar internacional de referencias de Auditoría informática, que abarca "las mejores prácticas" de Auditoría y control de sistemas de información. Estas ayudan a la alta dirección a comprender y administrar los riesgos relacionados con la tecnología de información, permiten establecer una interrelación entre los procesos de administración, tecnología, control interno y análisis de riesgos. Más adelante se analizará este estándar de forma más detallada.

Administración del Control de Datos de la Tecnología de Información

Es un modelo basado en el concepto de perfiles y roles. Esta establece responsabilidades relacionadas con los controles y seguridades de la tecnología de información. Esta norma clasifica los roles en los siguientes grupos:

- *A Nivel Interno:* Alta Dirección, Gerencia General, Gerencia de Sistemas, Jefes Departamentales, Supervisores y usuarios.
- *A nivel Externo:* Proveedores, Desarrolladores y Soporte Técnico.

Por otro lado, establece una diferenciación entre autoridad y responsabilidad respecto al control y riesgo de la tecnología de información. Esta norma se compone de objetivos de control y "prácticas generalmente aceptadas".

Administración de la inversión de tecnología de Inversión: un marco para la evaluación y mejora del proceso de madurez

Es un modelo basado en la identificación de los procesos críticos de la organización, analiza la importancia de las inversiones en tecnología de información y comunicación de datos.

ISO 17799

Pertenece a la familia de los ISO y presenta “las mejores prácticas” para la implementación de un Sistema de Control y Seguridad de Tecnología de la Información. Se estructura en 10 áreas de control. Este estándar es estudiado mas adelante.

Principios y criterios de confiabilidad de Sistemas

Este pretende incrementar la confianza de la alta gerencia, clientes y socios, con respecto a la confiabilidad en los sistemas por una empresa o actividad en particular. Este modelo incluye elementos como: infraestructura, software de cualquier naturaleza, personal especializado y usuarios, procesos manuales y automatizados, y datos. El modelo persigue determinar si un sistema de información es confiable, (i.e. si un sistema funciona

sin errores significativos, o fallas durante un periodo de tiempo determinado bajo un ambiente dado).

Modelo de Evolución de Capacidades de software (CMM)

Es un modelo enfocado hacia la evaluación de la capacidad o habilidad que tiene una organización para planificar, desarrollar y mantener Sistemas de Información. Se divide en 5 aspectos de análisis y 18 áreas de evaluación u objetivos de control, semejantes muchos de ellos a los que presenta COBIT.

Administración de sistemas de información: Una herramienta de evaluación práctica

Es modelo orientado hacia el *e-goberment*, que permite a las instituciones gubernamentales llegar a una profunda comprensión de la implementación estratégica de Tecnología de Información y negocios electrónicos que permita un desarrollo sustentable del sector público, un mejoramiento en la eficiencia y eficacia de los servicios públicos y la generación de nuevas oportunidades de servicios acorde con las metas estratégicas gubernamentales.

Guía para el cuerpo de conocimientos de administración de proyectos

Esta es una guía que se basa en “las mejores prácticas” sobre administración de proyectos de tecnología de información. Esta guía incluye los elementos necesarios para una adecuada gestión de proyectos, explicando las metodologías más utilizadas por los expertos para una exitosa implementación de proyectos de TI.

Ingeniería de Seguridad de sistemas

Este es un modelo que recoge las metodologías más utilizadas por las organizaciones en la elaboración de sus Sistemas de Seguridad informática, a través de una descripción de las características principales que debe tener la estructura de seguridad de TI y telecomunicaciones en las organizaciones.

Administración de seguridad de información: Aprendiendo de organizaciones líderes

Este es un modelo que presenta las 16 práctica esenciales para la implementación de un sistema de seguridad de TI, basado en el análisis de las metodologías empleadas por las ocho organizaciones privadas líderes en el mundo respecto a seguridad del área PED.

Como vemos, la mayoría de estos estándares y guías se basan en las “practicas aceptadas” de las organizaciones y expertos de tecnología de información; lo cual, significa que están desarrolladas de acuerdo a la realidad de las organizaciones y que ya han sido probadas con éxito en empresas exitosas a nivel mundial. Esto garantiza la disposición de herramientas eficaces para la implementación de los Sistemas de Control y Seguridad informática por parte de los profesionales y auditores de TI.

4.2. ISACA

4.2.1. ¿Qué es ISACA?

Es la Asociación en Control y Auditoría de Sistemas de Información que tiene como objetivo agrupar a los profesionales de diferentes áreas que están relacionados o participan en la práctica de Auditoría de sistemas. Esta asociación fue fundada en 1969, como EDP Auditors Association y actualmente cuenta con más de 26,000 miembros en más de 100 países.

Entre los miembros de ISACA se encuentran profesionales que son ingenieros en sistemas, economistas, contadores públicos, ingenieros comerciales, etc., lo cual es una prueba de que para

ser parte de esta reconocida asociación no se requiere necesariamente ser un profesional en el área de sistemas pero sí que tenga un desarrollo profesional o tenga interés en dicha área.

ISACA cuenta con alrededor de 200 capítulos en todo el mundo, entre los que se encuentra el capítulo Quito-Ecuador que fue aceptado el 6 de septiembre de 2002 y está conformado por 37 profesionales en diferentes áreas quienes se han asociado con el propósito de desarrollar y promover la Auditoría de Sistemas de Información en nuestro País de una manera dinámica y reconocida. Actualmente este capítulo se encuentra en fase inicial de consolidación mediante la realización de algunas actividades entre las que podemos mencionar:

- Incorporación de nuevos miembros buscando ampliar su cobertura y fortalecerse como organización.
- Difusión de actividades y eventos de capacitación.
- Facilitar e instruir a los participantes en la presentación del examen CISA.

4.2.2. Misión de ISACA

La misión de ISACA es “soportar los objetivos empresariales mediante el desarrollo, promoción y entrega de investigaciones, estándares, competencias y prácticas para un efectivo gobierno, control y evaluación de los sistemas de información y la tecnología relacionada”; y esto es muy cierto ya que esta organización se ha preocupado por mantener actualizado a los gerentes, auditores y profesionales de tecnología de información, en el manejo adecuado de los recursos informáticos, la seguridad de la información y la implementación de proyectos de TI, de acuerdo a las “mejores prácticas”.

4.2.3. Beneficios de ser socio ISACA

Entre los principales beneficios podemos mencionar:

- Suscripción gratuita a la revista bimensual **"IS Control Journal",** la cual es de gran interés para los auditores en Sistemas de Información.
- Descuentos en la librería de ISACA.
- Contactos locales e internacionales con profesionales que realizan la misma actividad.
- Participación en comités internacionales de desarrollo profesional.

- ❖ Acceso por medio de Internet a otros capítulos de ISACA en todo el mundo.
- ❖ Obtención del certificado CISA (Auditor Informático Certificado) con descuentos en los costos de examen.
- ❖ Conferencias regionales acerca de Auditorías de sistemas de Información, control y seguridades.
- ❖ Acceso completo a K-NET que es la red de conocimiento global de ISACA.

4.2.4. IT Governance: Un modelo de gobernabilidad y control para la tecnología de información

El IT Governance Institute (ITGI), fundado en 1998 por ISACA y su fundación afiliada, la ISACF, tiene como objetivo apoyar a la dirección en el liderazgo empresarial, para asegurar un éxito constante y duradero al ampliar la conciencia acerca de la necesidad y el beneficio de un manejo adecuado de la TI.

Este Instituto desarrolla y promueve la comprensión de lo importante que es el vínculo entre la TI y el manejó de una empresa, y ofrece una guía sobre las mejores prácticas aplicables al manejo de los riesgos relacionados con la TI, a través de lo que ellos llaman el IT Governance.

El IT Governance es una filosofía empresarial de gobierno de la Tecnología de Información en el que se busca una participación activa de la gerencia en los procesos de TI, su desarrollo y Control. Está enfocada hacia la alineación de la estrategia de TI con las operaciones de las organizaciones, la difusión de estrategias y metas a nivel de toda la organización, la estructuración de las organizaciones hacia el logro de las metas y objetivos, la adopción e implementación de una estructura de control de la TI y la medición del desempeño de TI.

Los resultados que se esperan al establecer esta filosofía del IT Governance, son los siguientes:

1. Que la TI esté alineada con la empresa y produzca los beneficios prometidos.
2. Que la TI habilite a la empresa al explotar oportunidades y generar los máximos beneficios.
3. Que los recursos de la TI se empleen responsablemente.
4. Que los riesgos relacionados con la TI se manejen adecuadamente.

Es por ello, que para cumplir con los objetivos antes mencionados, el IT Gobernante define cuatro áreas de acción que se deben considerar en el manejo de la tecnología de información.

Alineación estratégica de la Tecnología de Información.- Esto significa que los recursos planificados para la inversión en TI deben estar alineados a los objetivos estratégicos de la organización, aunque en la realidad esto no se cumpla por completo. Es decir, la estrategia de TI debe ser parte de la estrategia global de la organización y ser un soporte para las operaciones de la organización.

Valor derivado de Tecnología de Información.- La TI para una organización debe significar una ventaja competitiva, un mejoramiento a la eficiencia de sus operaciones, una mayor satisfacción del cliente, mayores rendimientos y utilidades, mejor manejo de la información y la toma de decisiones correctas y oportunas.

Medición del desempeño.- Se requiere definir una serie de parámetros sobre los cuales se debe desarrollar el manejo o

administración de la TI. Esto deberá servir para medir el desempeño de la TI dentro de las organizaciones y si es que se están cumpliendo las metas y objetivos institucionales. La mejor manera de efectuar este tipo de medición, es mediante alinear los parámetros de cumplimiento de TI con los de la organización, de tal forma que se pueda establecer una relación entre el desempeño, eficiencia y productividad de la organización con la gestión de TI.

Manejo de Riesgos.- La administración además de preocuparse por los riesgos operacionales y financieros a los que está expuesta la organización, debe poner especial interés en determinar, analizar y minimizar los riesgos relacionados con el manejo de la TI, debido principalmente a que un aumento del riesgo de amenazas para la TI de la organización, podría ocasionar simultáneamente un aumento del riesgo de las operaciones y gestión financiera de la organización.

4.2.5. La Certificación CISA

El programa CISA (Certified Information Systems Auditor), desde 1978 es patrocinado por ISACA y ha sido aceptado a nivel mundial como la norma entre los profesionales de

Auditoría, control y seguridad de TI. Poseer dicha designación, demuestra por parte de quien lo ostenta, conocimiento, dominio y experiencia profesional en la gestión y control de la Tecnología de la Información.

Una de las mayores ventajas de obtener la certificación CISA es la de ser reconocido a nivel internacional por la comunidad mundial de control y auditoría en Tecnología de la Información, como auditor experto de Sistemas de Información. Tanto así, que para muchos altos funcionarios públicos y privados, esta certificación se ha convertido en un requisito de contratación y ascensos dentro de muchas organizaciones, especialmente en los organismos de control estatales y las instituciones financieras.

Afortunadamente en nuestro País, desde el año 2003, ya se puede rendir el examen de certificación CISA, a través de nuestro capítulo Quito-Ecuador. La recepción de dicho examen se realiza en el mes de Junio de forma simultánea en todo el mundo.

4.3. Normas de Auditoría de Sistemas de Información de ISACA.

4.3.1. Emisión y Estructura de las Normas

ISACA a través de su *Comisión de Estándares* emite los estándares, guías y Procedimiento de Auditoría de TI; pero para ello, primero realiza una consulta a todos sus capítulos a nivel mundial sobre el tema a considerar, a la espera de sus comentarios, preguntas y sugerencias; los mismos que son revisados por los especialistas de la Comisión y otros participantes especiales, como los auditores CISA, de diferentes capítulos. Luego se procede a la emisión de los estándares.

ISACA mantiene un esquema de estándares estructurado en diversos niveles:

- **Estándares:** Establecen los lineamientos indispensables para la ejecución de las Auditorías de TI y la emisión de informes.
- **Guías:** Proveen las directrices para la aplicación de los estándares de TI y que los auditores deben considerar para la implementación de los estándares y la vigilancia de su cumplimiento.

- **Procedimientos:** Establece los pasos que un Auditor de TI puede utilizar durante la ejecución de una Auditoría o revisión especial. Estos procedimientos brindan al auditor información de cómo cumplir con los estándares pero no especifican requerimientos o herramientas, ya que eso queda a criterio del auditor.

Algo de particular importancia, es que ISACA ha emitido El *Código de Ética Profesional de ISACA* y que es exigido a todos sus miembros y los auditores CISA. Se puede decir que este es un estándar sobre comportamiento, habilidades y responsabilidades que deben tener los auditores de TI El incumplimiento a dicho Código de Ética podría ocasionar la expulsión de la asociación y en el caso de los CISA la pérdida de la certificación. Este Código de Ética es presentado mas adelante.

4.3.2. Objetivos de las Normas

ISACA, desde su creación en 1969 como EDP Auditors Asociation, ha formulado una serie de normas y declaraciones de Auditoría de TI que han servido de guía para los profesionales

que desean implementar controles y seguridades informáticas; y, para quienes desean evaluarlas: los auditores de TI.

Tales estándares de Auditoría buscan:

- Proveer información a los auditores informáticos sobre los lineamientos que deben seguir para cumplir con los estándares de la Auditoría de TI.
- Que los Auditores de TI estén lo suficientemente capacitados para cumplir con las responsabilidades profesionales establecidas en el código de ética profesional de ISACA para auditores de TI.
- Informar a los gerentes sobre la importancia y el proceso de implementación de los sistemas de seguridad de TI.

4.3.3. Normas Generales para la Auditoría de Sistemas de Información

Estas son un conjunto de normas de auditoria de sistemas de información, promulgadas por ISACA, con el fin de establecer los lineamientos que deben seguir los auditores y gerentes de TI para cumplir con su código de ética profesional y realizar su trabajo de forma adecuada enmarcada con los estándares internacionales.

Entre los aspectos que abarcan estas normas, están la independencia profesional, la ética, habilidad y capacidad, planeación, ejecución, evidencia, informes y actividades de seguimiento. Cada uno de estos aspectos son muy importantes para el auditor y la falta de alguna de ellas podría poner en riesgo el trabajo de auditoría, además del prestigio y confiabilidad del auditor, aspectos clave que el auditor en todo momento debe mantener intachable. En el Apéndice 1, se exponen las Normas Generales de auditoría de Sistemas de Información.

4.3.4. Código de Ética para los Auditores de TI

El código de Ética de los auditores de TI, ha sido emitido por ISACA, con el fin de establecer ciertos requisitos mínimos de conducta por parte de los auditores de TI, dentro de su desempeño profesional como personal; por ello, en dicho código se abarcan aspectos como: el cumplimiento de los estándares internacionales, la confidencialidad, independencia, competencia, responsabilidad, entre otros. En el Apéndice 2, se muestra el contenido de dicho código.

4.4. El estándar ISO 17799

4.4.1. En qué consiste la Norma

ISO 17799:2000 es una norma internacional basada en la norma BS 7799, la cual, en 1995 fue publicada por el Instituto Británico de Normas Técnicas; y, que luego fue actualizada en 1999.

BS 7799 fue desarrollada con el objetivo de tratar aspectos de la seguridad informática en los negocios electrónicos. Sin embargo, fue muy poca la acogida que tuvo esta norma debido a que, para muchos profesionales de TI, esta Norma era poco práctica, muy general y era muy exigente para la realidad tecnológica de ese entonces. Es por ello, que se comenzó a trabajar en una segunda versión que abarque aspectos más amplios de seguridad y que sea flexible, para que cualquier organización esté en capacidad de implementar esta Norma. Es así como en 1999 se publicó la segunda versión mejorada de BS 7799.

A raíz de esta evolución en la Norma, el Comité Internacional de la ISO participó junto al Instituto Británico de Normas Técnicas para la emisión de la nueva ISO 17799; la cual, incluía la posibilidad para las organizaciones de obtener la Certificación

ISO 17799; y, para los auditores, obtener la acreditación internacional para poder ejercer la labor de implementación, capacitación y auditoría en esta Norma, que en la actualidad es de general aceptación a nivel internacional.

Sin lugar a dudas, este estándar se ha convertido en la actualidad en uno de los más utilizados por los profesionales de TI al momento de implementar un Sistema de Seguridad Informática.

Se fundamenta en la presentación de 10 áreas o dominios de control que deben ser cuidadosamente cubiertas por los responsables de TI de las organizaciones, sin importar el tamaño o estructura que estas tengan ya que esta norma recoge las “mejores prácticas” de seguridad sugeridas por los expertos.

Actualmente muchas organizaciones, por lo general multinacionales exitosas, están optando por obtener una certificación ISO 17799, púes la ven como una estrategia competitiva en este mundo globalizado en donde, además de la calidad, también es importante la seguridad de la información. Es por ello, que obtener una certificación ISO 17799 se convierte una característica diferenciadora en el mercado, especialmente para lograr clientes a quienes les interesa manejar de forma segura la información. Pero, además, le permitirá una

efectiva planeación y gestión de la seguridad informática, lograr alianzas estratégicas y comerciales más seguras, mayor confianza por parte de los clientes y, mejor control y auditoría informático.

4.4.2. Estructura de la Norma

El ISO 17799 esta organizado en 10 secciones principales, cada una cubre áreas o tópicos diferentes, las cuales son resumidas a continuación:

1. **Planeación de la Continuidad del Negocio**

   En esta área se busca que la organización identifique cuales son las principales amenazas que pondrían en riesgo la continuidad operativa del negocio, se busquen las posibles alternativas de solución a tales amenazas, se establezcan los recursos necesarios y se elabore un Plan de Contramedidas, que debería verse reflejado en un documento denominado Plan de Contingencias.

2. **Sistemas de Control de Acceso**

   En esta sección se busca hacer hincapié en los controles que deben implementarse para controlar el acceso a la información de la organización a través de los sistemas de

información, establece la importancia de tomar medidas preventivas contra accesos no autorizados en los sistemas de información, las redes, las terminales y las conexiones remotas.

3. Desarrollo y Mantenimiento de Sistemas

La norma establece los lineamientos respecto a la seguridad interna de los sistemas de información durante las etapas de diseño y desarrollo, bajo los principios de confidencialidad, autenticidad e integridad de la información; con la finalidad de prevenir ingresos, modificaciones o eliminación de la información. Así como también, la importancia de implementar controles de cumplimiento en los proyectos de tecnología de la información.

4. Seguridad Física y Ambiental

En esta sección se establece la importancia de prevenir el acceso no autorizado a las instalaciones con el objetivo de evitar daños a los bienes informáticos, robo, sabotaje y cualquier otro tipo de amenaza que ponga en riesgo la continuidad operativa de la organización.

5. Cumplimiento

La Norma establece los lineamientos respecto al cumplimiento de las leyes, reglamentos, normas y políticas referentes a la seguridad informática de cada región o País; y, la armonía que deberá existir entre dichas normas y las políticas internas de seguridad informática. Este aspecto involucra, además del sistema de control y seguridad informática, a la realización de revisiones o controles posteriores y las auditorías.

6. Seguridad del Personal

En esta área se establece la importancia de mantener informado y capacitado al personal respecto a seguridad y confidencialidad de la información, con el objetivo de reducir el riesgo de error, hurto, fraude y divulgación indebida de la información, los sistemas de información y los equipos informáticos.

Además, la Norma estipula que se deben establecer políticas específicas sobre el incumplimiento a estos requerimientos y las sanciones pertinentes, tomando muy en cuenta el registro de incidentes por medio de bitácoras internas.

Todo esto deberá verse reflejado en las políticas internas de controles y seguridades informáticos.

7. Seguridad de la Organización

En esta área se establece la importancia de establecer un Plan general de seguridad de la información dentro de la compañía, mantener la calidad de la seguridad en el área PED y los activos informáticos al cual tienen acceso los proveedores, clientes y aliados estratégicos y supervisar la integridad, confiabilidad y disponibilidades de la información cuando el procesamiento electrónico de datos está a cargo de empresas tercerizadoras de servicios informáticos.

8. Administración de las Operaciones y Equipo de Computo

Aquí se establecen lineamientos para la correcta operación de las instalaciones de procesamiento y la disminución de riesgos relativos a: el uso de los Sistemas de información, la seguridad del hardware software, la integridad y disponibilidad del procesamiento de la información y las comunicaciones, la protección de la información en red y su infraestructura, daños a los activos y procesos críticos de la

organización y la modificación, pérdida y mal uso de la información.

9. Clasificación y Control de Activos

Es de suma importancia mantener inventarios actualizados de los recursos informáticos para llevar a cabo una adecuada protección de dichos activos.

10. Políticas de Seguridad

La organización debe tener bien en claro cuáles son sus objetivos de control y la metodología que va emplear para establecer un subsistema de Control Interno Informático, el mismo que le ayudará a formalizar la seguridad de la información dentro de la organización.

4.5. El estándar COBIT

4.5.1. En qué consiste la Norma

En la presente sección explicaremos los fundamentos del estándar COBIT, el cual, es muy utilizado a nivel mundial por los auditores de sistemas de información y es considerado el estándar por excelencia para la implementación o evaluación de

la tecnología de información de las organizaciones. Esta Norma tiene como misión: Investigar, desarrollar, publicar y promover un conjunto internacional y actualizado de objetivos de control para tecnología de información que sea de uso cotidiano para gerentes y auditores.

COBIT fue presentada al mundo en el año1996 por ISACA, que como vimos anteriormente esta asociación se ha caracterizado por estar a la vanguardia en la emisión de normas, guías y procedimientos referentes a la auditoria y administración de Tecnología de la Información.

COBIT es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de TI, combinando exitosamente las prácticas de control y la Tecnología de Información, armonizando y combinando estándares de fuentes globales prominentes como el AICPA, firmas de auditoria internacionales y expertos en TI; de tal forma, que este estándar esté dirigido para gerentes ejecutivos, Administradores de TI y auditores informáticos.

Esta normativa puede ser implementada en cualquier organización que desee implementar un proyecto de TI sustentable y con altos estándares de control y seguridad de sus

sistemas de información; sin importar su tamaño o la tecnología con, la cual, desarrolle sus operaciones.

4.5.2. Características de COBIT

COBIT es una herramienta que está dirigida a los diferentes actores que conforman una organización que ha incorporado la Tecnología de la Información en sus actividades. A continuación se presenta una tabla en la que se explica como está enfocada la Norma.

DIRIGIDO A:	CON EL PROPÓSITO DE:
La Gerencia	Apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.
Los Responsables de TI	Identificar los controles que requieren en sus áreas.
Los Auditores	Soportar sus opiniones sobre los controles de los proyectos de TI, su impacto en la organización y

	determinar el control mínimo requerido.
Los Usuarios Finales	Obtener una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.

Tabla 4.2. Usuarios del estándar COBIT

Entre sus características tenemos:

- Orientado al negocio
- Alineado con estándares y regulaciones "de facto"
- Basado en una revisión crítica y analítica de las tareas y actividades en TI
- Alineado con estándares de control y Auditoría (COSO, IFAC, IIA, ISACA, AICPA)

4.5.3. Estructura de la Norma

ISACA a través de su sitio Web y las de sus capítulos por todo el mundo, ha difundido ampliamente la estructura fundamental de COBIT.

Esta Norma esta basada en tres principios fundamentales que son: Requerimientos de Información del Negocio, Recursos de TI y Procesos de TI.

Requerimientos de la información del negocio.- De acuerdo a la Norma, toda organización debe establecer de manera específica los requerimientos necesarios para un eficiente desarrollo de sus operaciones y debe hacerlo en base a tres aspectos:

- *Requerimientos de Calidad:* La organización debe establecer la calidad, costo y oportunidad de la información.

- *Requerimientos Financieros*: Deberá establecer respecto a su información, los mínimos niveles de efectividad y eficiencia operacional, la confiabilidad de los reportes financieros y los requerimientos de leyes y regulaciones.

- *Requerimientos de Seguridad*: Deberá establecer el grado de Confidencialidad, Integridad. y Disponibilidad de la información.

Recursos de TI.- Toda organización que haya implementado un proyecto de Tecnología de Información necesita de los siguientes recursos:

- *Datos:* Todos los objetos de información. Considera información interna y externa, estructurada no estructurada, gráficas, sonidos, etc.
- *Aplicaciones:* Entendido como los sistemas de información, que integran procedimientos manuales y sistematizados.
- *Tecnología:* Incluye hardware y software básico, sistemas operativos, sistemas de administración de bases de datos, de redes, telecomunicaciones, multimedia, etc.
- *Instalaciones:* Incluye los recursos necesarios para alojar y dar soporte a los sistemas de información.
- *Recurso Humano:* Por la habilidad, conciencia y productividad del personal para planear, adquirir, prestar servicios, dar soporte y monitorear los sistemas de Información.

Procesos de TI.- Asimismo para que una organización pueda lograr implementar de forma exitosa un gestionar de forma exitosa sus recursos, lo debe hacer mediante un conjunto de

procesos agrupados de forma natural para que proporcionen la información que la empresa necesita para alcanzar sus objetivos. Dichos Procesos están agrupados dentro de cuadro dominios centrales y a su vez cada proceso se divide en actividades o tareas.

- *Dominios:* Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional. Son cuatro dominios principales que a continuación se describen:
    - Planeación y Organización
    - Adquisición e implementación
    - Prestación de Servicios y Soporte
    - Seguimiento
- *Procesos:* Conjuntos o series de actividades unidas con delimitación o cortes de control. Estos son los objetivos de control de TI. COBIT presenta 34 Objetivos de Control repartidos en los cuatro dominios.
- *Actividades:* Acciones requeridas para lograr un resultado medible.

Planificación y organización.-Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos de negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas. A continuación se especifican los procesos que incluye:

- Definir un plan estratégico de TI
- Definir la arquitectura de información
- Determinar la dirección tecnológica
- Definir la organización y relaciones de TI
- Manejo de la inversión en TI
- Comunicación de la directrices Gerenciales
- Administración del Recurso Humano
- Asegurar el cumplir requerimientos externos
- Evaluación de Riesgos
- Administración de Proyectos

- Administración de Calidad

Adquisición e implementación.- Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a los sistemas existentes. Los procesos son los siguientes:

- Identificación de soluciones
- Adquisición y mantenimiento de SW aplicativo
- Adquisición y mantenimiento de arquitectura TI
- Desarrollo y mantenimiento de Procedimientos de TI
- Instalación y Acreditación de sistemas
- Administración de Cambios

Prestación y soporte.- En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte

necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación. Los procesos son los siguientes:

- Definición del nivel de servicio
- Administración del servicio de terceros
- Administración de la capacidad y el desempeño
- Asegurar el servicio continuo
- Garantizar la seguridad del sistema
- Identificación y asignación de costos
- Capacitación de usuarios
- Soporte a los clientes de TI
- Administración de la configuración
- Administración de problemas e incidentes
- Administración de datos
- Administración de Instalaciones
- Administración de Operaciones

Monitoreo.- Todos los procesos de una organización necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control, integridad y confidencialidad. Este es, precisamente, el ámbito de este dominio. Los procesos son los siguientes:

- Seguimiento de los procesos
- Evaluar lo adecuado del control Interno
- Obtener aseguramiento independiente
- Proveer una auditoría independiente

4.6. Legislación informática en el Ecuador

4.6.1. Introducción

Nuestro País no se ha caracterizado por mantener una legislación orientada hacia el control interno informático o la estandarización de los procesos de seguridad informática, que permita a gerentes y auditores tener una referencia, adaptada a nuestra realidad, de los aspectos que deben tomar en consideración para la gestión eficiente de la Tecnología de Información.

Sin embargo, se están haciendo esfuerzos en este sentido, más aún ahora, que se quieren implementar mecanismos que

permitan el uso de documentos electrónicos como facturas y declaración de impuestos, como ocurre en otros Países como Brasil, en donde el e-goverment está muy desarrollado; así lo demuestran las estadísticas y estudios realizados, que afirman una disminución significativa de miles de dólares al año al evitarse la emisión, control, almacenamiento y cuidado de los documentos en papel; y, por otro lado, el servicio que se le da a los ciudadanos es de calidad.

A continuación se explican algunas normativas vigentes en nuestro País y su aplicación.

4.6.2. Normas de Control Interno emitidas por la Contraloría

La Contraloría General del Estado, a través del **Acuerdo 017 CG**, ha emitido las Normas de Control Interno para el sector público, con el fin de establecer los lineamientos que se deben aplicar por parte de las entidades del Estado, para lograr un adecuado control de las operaciones en las áreas de Gerencia, Recursos Humanos, Proyectos, Deuda Pública, los Sistemas de Información Computarizados, entre otros...

Particularmente en el caso de los Sistemas de Información Computarizados, estas normas establecen ciertos lineamientos muy útiles respecto a cada una de las áreas críticas dentro del procesamiento electrónico de datos. Se hace referencia a las siguientes áreas:

- **Sistemas Nuevos o actualización de los existentes.-** Se establece que para cada año es necesario elaborar un Plan Integral de Sistemas, que indique los planes de adquisición, presupuesto y cronograma de actividades, en lo referente a la adquisición o mantenimiento de sistemas de información.

- **Producción, operación y mantenimiento.-** Aquí se explica, que es necesario que las entidades del sector público establezcan planes de mantenimiento de los equipos y los programas de forma periódica.

- **Acceso a los Sistemas.-** En esta sección se establece que deberán existir los suficientes controles físicos y lógicos para la protección de la información de la entidad.

- **Ingreso de datos para procesamiento.-** Aquí se indica la necesidad de establecer ciertos mecanismos de validación de los datos ingresados a los sistemas de información, con el fin de que se eviten errores o actos malintencionados.

- **Transacciones rechazadas.-** Esta norma indica que en caso de que existan transacciones con errores y que han sido rechazadas deben ser analizadas y corregidas de forma oportuna.

- **Procesamiento y entrega de datos.-** Aquí se establece que deben incorporarse controles para el procesamiento electrónico de los datos, con el fin de que la información presentada por el sistema al usuario final sea íntegra y consistente.

- **Segregación de funciones.-** Aquí se establecen lineamientos respecto a la asignación de autoridad y responsabilidades dentro del departamento de PED, puesto que una inadecuada segregación de funciones

podría ocasionar ineficiencia, riesgo de fraude, pérdida de datos, etc.

- **Cambios a los programas.**- Se establece que es necesario definir un proceso de trabajo o Workflow en el caso de que se requieran realizar cambios en el código fuente de los programas.

- **Seguridad general en el centro de procesamiento de datos.**- Aquí se especifica la necesidad de elaborar un plan de seguridad informática cuyo objeto sería la protección de los activos, la información y garantizar la continuidad del negocio.

Sin duda, estas normas cubren la mayor parte de las actividades y áreas más importantes dentro de un área PED, asimismo, ayudan a los responsables de TI a tomar medidas de precaución para garantizar la protección de los sistemas de información; y, aunque está dirigido al sector público, puede ser perfectamente aplicado por las empresas del sector privado, tal como ocurre actualmente. Para una revisión más exhaustiva de estas normas, remítase al **Apéndice 3 A**.

4.6.3. Ley de Propiedad Intelectual

Esta es una Ley emitida el 19 de mayo de 1998 que busca garantizar la propiedad intelectual de todas aquellas personas naturales y jurídicas que han creado alguna obra literaria, artística o técnica. En lo referente a los sistemas de información o "programas de ordenador", el Artículo 8 y la SECCIÓN 5 – "DISPOSICIONES ESPECIALES SOBRE CIERTAS OBRAS" – "PARÁGRAFO PRIMERO" – "DE LOS PROGRAMAS DE ORDENADOR", especifican que estos materiales están protegidos por la Ley de Propiedad Intelectual y son considerados dentro de la categoría de obras literarias. Por lo tanto, se considera como ilegal el mantener copias no autorizadas de cualquier programa informático y es castigado de acuerdo a la ley (Véase Apéndice 3 B).

Es por esa razón, que se hace necesario que las organizaciones cuenten con las respectivas licencias para cada uno de los programas instalados en sus computadores a nivel de servidores y terminales.

Los auditores de Sistemas de Información, dentro de sus programas de trabajo, deben incluir objetivos y procedimientos enfocados hacia revisar el cumplimiento de estos requisitos enmarcados en la Ley.

4.6.4. Ley de Comercio Electrónico

Esta es una Ley que luego de un largo proceso de discusión y análisis, entró en vigencia a partir del 17 de Abril del 2002 en el Registro Oficial Suplemento 557.

El objeto de esta Ley es normar, regular y controlar las actividades civiles y mercantiles realizadas a través del uso de Internet, para que estas sean accesibles y transparentes al efectuarse, especialmente en lo relacionado con el comercio electrónico.

En ella se analiza aspectos como los mensajes de datos; los requisitos de las firmas electrónicas y sus características; el uso de los certificados de firmas electrónicas; las obligaciones y requisitos que deben cumplir las entidades de certificación de la información; las infracciones informáticas; entre otras.

Un aspecto muy interesante, es lo relacionado con los delitos informáticos, puesto que en esta Ley se hacen reformas al Código Penal a partir de su artículo 202; y, se consideran penalizaciones y multas para la violación de claves de acceso, la eliminación o daños en la información almacenada en bases de datos privadas o públicas, la falsificación de documentos electrónicos, apropiación ilícita de información confidencial y cualquier otro tipo de delito informático. Cabe señalar que esta normativa es aplicable a delitos realizados por los funcionarios de las entidades afectadas o por terceros (hackers).

CAPÍTULO 5

Un enfoque de Auditoría considerando la Tecnología de Información

5.1. Implicaciones de las Tecnologías de la Información en la profesión del Auditor en Control de Gestión

5.1.1. Influencia de la informática en la Auditoría

A lo largo de este trabajo, se ha explicado la forma en que las organizaciones modernas han incorporado la tecnología de información dentro de sus procesos, mejorando enormemente su eficiencia, eficacia, rentabilidad y los mecanismos de control. Pero, asimismo se ha hecho más complejo el trabajo de Auditoría, tanto para los auditores internos como para los externos, ya que los auditores modernos, al realizar sus

Auditorías de Estados Financieros, deben evaluar diferentes tipos de sistemas administrativos-contables, bajo diversas plataformas tecnológicas y diseños específicos de acuerdo a cada organización.

Asimismo, la información en la gran mayoría de empresas, no reposa en papel; sino, en medios magnéticos como disquetes, cartuchos, CDs, DVDs, etc.; y, la mayoría de sus operaciones ya no se realizan manualmente sino de forma automatizada; por lo que, se hace necesario que el auditor domine por lo menos, los aspectos básicos de la informática, especialmente el manejo de bases de datos.

Los programas y procedimientos tradicionales de Auditoría, se ven alterados o reemplazados por nuevos procedimientos que incorporan la evaluación del Control Interno informático y el uso de nuevas herramientas de análisis de la información. Entre dichas herramientas de análisis se encuentran las pertenecientes a las Técnicas de Auditoría Asistida por Computador (CAATS), las mismas que son analizadas más adelante.

Por ello, es indispensable que el auditor, durante la ejecución de la Auditoría, utilice la computadora como una herramienta para mejorar la eficiencia en la revisión de la información y le permita: ampliar el alcance del examen, utilizar muestreo estadístico para la selección de transacciones y utilizar paquetes informáticos estandarizados para la administración de la Auditoría y el análisis de datos.

En la actualidad al referirnos a la Auditoría Financiera, es necesario hablar de auditoría asistida por computador y la Auditoría de Sistemas de Información; las cuales a pesar de ser parecidas son diferentes respecto al enfoque que tienen.

5.1.1.1. Auditoría Asistida por Computador

Al hablar de auditoría asistida por computador, nos estamos refiriendo a la utilización de las herramientas informáticas en la realización de un trabajo de auditoría.

A continuación se detalla de forma específica algunas de las actividades que puede realizar el auditor durante la ejecución de su trabajo:

- ✓ Evaluar la consistencia que presentan los sistemas de información; a través, de realizar simulaciones en paralelo de los procesamientos de información, desde el inicio hasta el final de una transacción de prueba.
- ✓ Selección de muestras de un conjunto indeterminado de transacciones de forma rápida y efectiva, en base a diferentes parámetros: estadísticos o contables.
- ✓ Análisis de datos de un universo de transacciones para verificar la integridad, consistencia y confiabilidad de la información presentada a través de los sistemas de información.
- ✓ Conciliación entre los datos presentados a través de consultas y reportes, con los datos almacenados en los sistemas de información para verificar la exactitud y confiabilidad del procesamiento de datos.
- ✓ Importación de datos desde las bases de datos hasta la computadora del auditor, para que este pueda realizar sus pruebas y análisis, sin importar

la plataforma en la que se encuentren los sistemas de información.

Pero así mismo, el auditor debe tener mucho cuidado con la información ingresada, almacenada y presentada a través de su computador, utilizando controles como por ejemplo: mantener todos sus documentos importantes con contraseñas; establecer contraseñas para el acceso al sistema operativo; mantener respaldos externos de la información y programas guardados en el computador; controlar mediante revisión permanente, el proceso de análisis de la información auditada; etc.

Por tanto, podemos decir, que los auditores deben desarrollar procedimientos en el que se considere las herramientas informáticas como apoyo para la ejecución de la Auditoría; y por otro lado, deben establecer como uno de sus objetivos de Auditoría, la evaluación de los sistemas de información y los controles internos informáticos establecidos por la

Gerencia de TI y la Dirección General de la organización.

5.1.1.2. Herramientas informáticas usadas en la Auditoría asistida por computador

Todas estas actividades antes mencionadas, pueden ser realizadas a través de las siguientes herramientas informáticas:

Herramientas Generales.- Son herramientas básicas para la creación y administración de documentos, uso de cálculos matemáticos y financieros, la creación de diagramas de procesos y organigramas, diseño y presentación de gráficos estadísticos, envío de correo electrónico, etc.. En esta categoría de herramientas informáticas generales se encuentran: los procesadores de palabras como MS Word y Lotus WordPro, las hojas de cálculo como MS Excel y Lotus 1-2-3, los diseñadores de gráficos como MS Visio, administradores de correo electrónico como MS Outlook, etc.

Herramientas Administrativas.- Son aquellas que permiten al auditor administrar todo el proceso de Auditoría desde la planeación hasta la generación de los informes. Permiten establecer presupuestos, administrar las horas y carga de trabajo del equipo de auditores, administrar y clasificar los papeles de trabajo, importar archivos contables para revisión y análisis, relacionar la información entre los diferentes papeles de trabajo, etc. En esta categoría se encuentran: Microsoft Project, Caseware Time, Caseware Working Papers, Auditor 2000, etc.

Herramientas de Análisis de Datos.- Estas herramientas le permiten al auditor acceder a diversos archivos de almacenamiento de datos para poder realizar sus análisis, utilizando muestreo o revisando el cien por ciento de los registros, entre los archivos que puede revisar, se encuentran: hojas de cálculo (*.xls), bases de datos (*.mdf, *.dat), archivos planos (*.txt, *.dbf), entre otros. En esta clasificación se encuentran programas como: IDEA, ACL, APOYO, etc.

Herramientas Especializadas.- Estos son herramientas basadas en los sistemas expertos, utilizando bases de conocimientos predefinidos para el análisis del control interno. Estas herramientas utilizan cuestionarios con preguntas cerradas y dividen las preguntas por categorías. A estos conjuntos de preguntas se las conoce como CheckList.

En la práctica estos tipos de herramientas son de gran ayuda para mejorar la evaluación de las áreas examinadas pues permiten realizar pruebas de cumplimiento y pruebas sustantivas, permiten el uso de herramientas y gráficos estadísticos, retroalimentan sus bases de conocimientos para futuras revisiones, presentan informes flexibles y dinámicos, entre otras cosas. En esta categoría se encuentran programas tales como el COBIT ADVISOR, para la evaluación del control interno informático.

5.1.2. La Auditoría Informática

La auditoría informática es un proceso sistemático de revisión y evaluación de los controles, sistemas, políticas y procedimientos

implementados en el ambiente de Procesamiento Electrónico de Datos (PED); la protección de los recursos informáticos; la seguridad, integridad y confidencialidad de la información; y, la eficiencia y eficacia en el uso de los recursos tecnológicos.

Un punto clave de mencionar es el hecho de que muchos auditores al referirse a la auditoría informática prefieren llamarla Auditoría de Sistemas de Información, ya que así la definición del párrafo anterior, involucra la información almacenada en medios escritos y electrónicos.

De la definición anterior podemos notar, que dentro del proceso de auditoria de los Sistemas de Información, es importante que el auditor se enfoque hacia los siguientes aspectos:

- La administración del área de Procesamiento electrónico de Datos.
- Los Controles, políticas y procedimientos que garanticen la eficiencia y eficacia en el uso de los recursos informáticos.
- Los controles implementados para la protección, confiabilidad e integridad de la información.

Esto significa que en los últimos años, ha existido un cambio en el enfoque de la auditoria informática; pues, durante mucho tiempo, la auditoria informática solo consistía en la participación de un profesional en informática para la extracción de información desde las Bases de datos de la empresa auditada, para que los auditores financieros pudieran efectuar sus revisiones y análisis de una forma eficiente.

En cambio, hoy en día, la auditoría informática se ha convertido en una función protagonista al interior de las organizaciones y las firmas de auditoria externa, que cuenta con sus propios objetivos, alcance, programas y procedimientos. De tal forma, que podríamos establecer una clasificación de los diferentes enfoques de una auditoría informática:

- Como soporte para la auditoría financiera en la obtención de información financiera, cuando ésta es voluminosa y difícil de acceder. Ya sea esta interna o externa.
- Como parte de una auditoria financiera en el que además de lo anterior, se evalúe los controles y seguridades implementados por el área PED para asegurar la integridad de la información.

- Como una función de apoyo dentro de la organización para la revisión del cumplimiento a los controles, políticas y procedimientos informáticos.
- Como una función externa de consultoría para la revisión del cumplimiento a los controles, políticas y procedimientos informáticos.

Lo cual, significa que la auditoría informática puede ser utilizada para evaluar diferentes aspectos de tecnología de Información dentro de una organización. Como podrían ser:

- **Gestión del área PED.-** Mediante la evaluación de: la planeación estratégica, políticas y procedimientos del área PED; la estructura funcional y segregación de funciones; los controles de desempeño; la eficiencia y eficacia del personal informático; inversiones en tecnología; etc.

- **Sistemas de Información.-** A través de la revisión de los siguientes aspectos: el análisis de factibilidad, diseño, desarrollo, pruebas y puesta en producción de los sistemas de información; el Control de los proyectos de

TI; la existencia de manuales de diseño y operación de los sistemas; las seguridades lógicas y físicas de los sistemas; monitoreo y corrección de fallos en los sistemas; el desempeño y utilización de los Sistemas; integridad, confiabilidad y disponibilidad de la información; licencias de usuario; etc.

- **Control de la Información.-** El auditor deberá revisar la existencia de los siguientes controles: de entrada, procesamiento y salida de la información; de generación de respaldos de las bases de datos, programas y archivos importantes; de carga de trabajo del personal del área PED; de acceso a la Red y Comunicaciones; etc.

- **Seguridad de los recursos de TI.-** Mediante la evaluación de los siguientes aspectos: seguridades físicas y lógicas; planes de contingencia para casos de desastre; contratación de seguros y servicio de soporte técnico; seguridades contra la instalación de software de dudosa procedencia; uso de antivirus; etc.

- **Disposiciones Legales.-** A través de la revisión del cumplimiento a disposiciones y regulaciones legales emitidas por los organismos de control gubernamental; la revisión de normas o estándares internacionales de seguridad informática adoptada por la organización; el cumplimiento a especificaciones técnicas y legales exigidas por los proveedores del hardware y software; etc.

5.2. Planeación de la Auditoría Informática

Tanto para la Auditoría informática como para cualquier otro tipo de Auditoría, la planeación es uno de los pasos más importantes dentro de todo el proceso de Auditoría. Durante esta etapa el auditor debe establecer:

- Cuáles son las metas y objetivos del examen a realizar.
- Las áreas de interés que deberán ser evaluadas.
- El enfoque de Auditoría que será utilizado.
- El marco legal que servirá de base para la evaluación.
- Los programas de trabajo de Auditoría, adaptados a la realidad tecnológica y estructural de la organización.

- Presupuesto de horas-hombre requeridas para el trabajo de Auditoría y otros costos adicionales.

Ciertamente, un aspecto muy importante es la definición de las metas y objetivos de la Auditoría informática, ya que en base a ello, el auditor podrá establecer el área de interés a evaluar, los cuales podrían ser:

- La gestión administrativa desempeñada por el personal de informática.
- Los procedimientos.
- Los equipos computacionales.
- El procesamiento de datos.
- Los Sistemas de Información.
- Bases de Datos.
- Redes y comunicaciones.
- Controles y Seguridades Informáticas.
- Cumplimiento a las disposiciones legales.

El proceso de planeación de la auditoría va a variar respecto al ámbito del examen ya que este puede ser externo o interno. La auditoría externa puede estar a cargo de una firma de auditores independientes o de un profesional experto en auditoría de TI. En cambio, la auditoria informática interna está a cargo de la Unidad de Auditoría Interna de la

organización y deberá contar con el soporte de un profesional auditor con conocimientos de TI. Los pasos a seguirse durante la planeación, desde el punto de vista de una auditoría externa, son los siguientes:

1. **Realizar una visita preliminar para conocer las instalaciones de la empresa.-** El auditor antes de comenzar su trabajo, debe visitar las instalaciones del cliente y mediante observación o conversación con personas clave, darse cuenta de cuál es el entorno de la organización, sus instalaciones, el giro o naturaleza del negocio, sus operaciones, distribución departamental, grado de sistematización de las operaciones administrativas y financieras, ubicación del área PED, sectores críticos o peligrosos dentro de la organización (bodegas, cafeterías, etc.), ubicación geográfica donde está ubicada la organización, posibles amenazas externas, etc.

   Es en este punto donde el auditor debe hacerse una idea de los posibles riesgos que pudieran afectar al manejo de la Tecnología de Información de la organización. También, podría ser de gran ayuda los papeles de trabajo que se mantienen en la firma, correspondiente al periodo anterior y los comentarios de otros auditores, anteriormente asignados a dicho cliente.

2. **Tener una entrevista preliminar con la Gerencia General y la Gerencia de Sistemas.-** Durante la visita preliminar que realiza el auditor a las instalaciones de la empresa, éste debe mantener una reunión con la Gerencia General para conocer sus expectativas respecto al manejo de la tecnología de información; la planeación estratégica adoptada, para la inversión e implementación de nuevas tecnologías; y, los requerimientos de control informáticos establecidos por la administración.

   Asimismo, el auditor debe reunirse con el responsable del manejo de TI de la organización, para establecer un adecuado vínculo de comunicación haciéndole notar que la auditoría informática no es una "cacería de brujas" en el que se busca la cabeza del Jefe de Sistemas (como algunos piensan), ni que se busca criticar y hacer notar los defectos del área PED, sino que mas bien, busca *recomendar* acciones dirigidas hacia el mejoramiento de la eficiencia y eficacia de la gestión informática, la incorporación de medidas de seguridad adecuadas y la protección de los recursos informáticos. En esta entrevista preliminar el auditor podría hacer algunas preguntas generales respecto a la tecnología disponible, Sistemas existentes, comunicaciones, personal disponible, grado de

formalidad en cuanto a controles y seguridades, posibles debilidades y amenazas, etc.

3. **Establecer las metas, objetivos y el alcance del examen.-** Una vez establecidas cuáles son las expectativas que tiene la administración respecto al manejo de los Sistemas y la importancia que se le da al desarrollo y control de la Tecnología de Información, es necesario que el auditor establezca junto al resto del equipo de auditoría, los objetivos y el alcance que va a tener el examen de TI. Esto quiere decir, que hay que establecer el enfoque a seguir (estos fueron presentados anteriormente), los sistemas a revisar, las áreas críticas de TI y los tipos de análisis de datos que se van a seguir.

   Por ejemplo, en una auditoría a una institución financiera, se podría establecer la necesidad de una revisión del módulo de créditos, realizar pruebas sustantivas de las seguridades para el ingreso y protección de la información crediticia y un análisis de datos con los registros de los créditos vencidos que tienen más de dos años de mora.

4. **Solicitar al departamento de sistemas, información interna referente al área que se desea evaluar.-** El auditor deberá solicitar de forma preliminar información relevante sobre el área que piensa revisar, para establecer el tipo de pruebas que va a utilizar. Por ejemplo el auditor podría solicitar la siguiente información:

   - **Documentos Generales:** Son los documentos referentes a la gestión y estructura de la organización y del área de Sistemas, entre los que se encuentran: Planeación Estratégica de la organización y de TI, Manuales de políticas y procedimientos del área de Sistemas; Manuales de Controles y Seguridades; Plan Maestro Anual y Presupuesto de TI; etc.

   - **Sobre los Recursos Informáticos:** Es la información referente a la situación tecnológica de la organización y los planes de crecimiento de TI. El auditor podría solicitar: información sobre los equipos informáticos disponibles, su distribución, características, etc.; contratos con terceros para el mantenimiento de los equipos informáticos; manuales técnicos sobre la instalación y configuración de los equipos; contratos con empresas aseguradoras; lineamientos sobre la utilización

de equipos considerados críticos, como Servidores, equipos de comunicaciones, etc.; y, planes de expansión tecnológica.

- **Sobre los Sistemas de Información:** Ésta se relaciona con los Sistemas de Información disponibles en la organización, su estructura, plataforma tecnológica, etc. El auditor podría solicitar: Un detalle de los sistemas en producción y en etapa de desarrollo; Manuales técnicos de los Sistemas de Información, como el Manual DERCAS, Manual de Diseño Lógico, Diagramas Entidad-Relación; Manuales de Diseño, etc.; Manuales de Control y Seguridades de la información; Planes de Contingencias; etc.

5. **Determinar los recursos y herramientas que serán necesarios para la ejecución de la Auditoría.-** En base a la información recibida por el área de Sistemas y luego de haberlas analizado, el auditor deberá decidir las herramientas y técnicas informáticas necesarias para realizar su examen.

6. **Efectuar una revisión preliminar de las áreas a revisar.-** Consiste en la revisión general de las áreas informáticos considerados clave para el examen, mediante la observación

directa de las actividades desempeñadas por el personal informático, entrevistas con los diferentes responsables del área, encuestas al resto del personal de la organización sobre el desempeño del área PED. Todo este proceso deberá ser documentado y archivado en los papeles de trabajo como evidencia de la planificación.

7. **Establecer y redactar de forma detallada el programa de Auditoría informática.-** Una vez realizados los pasos anteriores, el auditor debe organizar y analizar toda la información recolectada con el propósito de definir el programa de auditoría informática; en el que se incluya los objetivos, procedimientos responsables, técnicas a utilizarse fechas para la realización del trabajo, referencias a papeles de trabajo, etc.

8. **Establecer la metodología de trabajo.-** Además de la elaboración del Programa de Auditoría, es necesario que el auditor junto al equipo de trabajo establezcan la metodología que será utilizada durante la ejecución del trabajo como por ejemplo: la utilización de cronogramas de trabajo, equipo de trabajo que será asignado, distribución de responsabilidades, líneas de comunicación que serán utilizadas, papeles de trabajo que serán utilizados durante la

ejecución del trabajo, etc. La mayoría de las Firmas de Auditoria Externa disponen de manuales completos respecto a la metodología que será utilizada, control de calidad e incluso “bases de conocimientos” para consulta de los auditores.

9. **Documentar la planeación y archivarlo en los papeles de trabajo.-** Todo el proceso de planificación de la Auditoría Informática deberá ser documentada para su futura revisión y consulta durante la etapa de ejecución y deberá ser organizada y archivada en el “FILE” de Papeles de Trabajo.

Los pasos antes mencionados dependerán mucho del profesional auditor que realice la Auditoría informática y de si se trata de una Auditoría Externa o Interna.

Dentro del proceso de planificación son de mucha utilidad los programas informáticos de Auditoría que están dentro de la categoría de herramientas administrativas, ya que estas le permiten al auditor documentar las áreas que se van a auditar, graficar las actividades a realizarse con su respectivo tiempo asignado (diagramas GANT), asignar cargas de trabajo al equipo de

Auditoría, establecer el presupuesto de la Auditoría, entre otras cosas.

5.3. Metodologías para la Ejecución de la Auditoría Informática

5.3.1. Metodología para auditar la Gestión Informática

Uno de los aspectos más importantes en el desarrollo de una auditoría informática es la evaluación de la gestión realizada por la dirección del área de Sistemas, ya que esta nos puede dar una idea más amplia sobre el grado de desarrollo y control de TI en la organización.

Para la revisión de la Gestión Informática el auditor deberá considerar los aspectos de Planificación, Organización, Dirección y Control desempeñada por la Dirección de Informática, pues estos aspectos son claves en toda administración.

5.3.1.1. Evaluación de la Planificación

Lo primero que debe revisar el auditor respecto a la planificación de TI es el Plan estratégico de TI, ya que

este es el marco básico de actuación de los Sistemas de Información en la empresa. Este deberá estar alineado con los mismos objetivos de la propia empresa.

No obstante en la práctica, en la mayoría de las organizaciones, la alta dirección no considera importante la planeación estratégica de la propia organización, peor aún, la de TI.

Muchos piensan que la planeación estratégica de TI debe ser independiente a la de la organización y que a pesar de no existir ésta última, los responsables de TI deberían realizar la planeación estratégica concerniente a la del área de TI. Sin embargo, son aspectos íntimamente relacionados ya que la tecnología es un apoyo al logro de los objetivos y metas de la organización, en el que deben participar el Comité de Informática y la Gerencia General.

Por otro lado, muchos auditores son exigentes respecto al alcance de la planeación estratégica ya que consideran obligatorio que esta sea definida para un

lapso de 3 a 5 años; Sin embargo, esta dependerá de la cultura organizacional, el giro del negocio, la competencia y los requerimientos gubernamentales.

El auditor al revisar la planeación estratégica de TI deberá evaluar el grado de alineación que tenga ésta con el de la organización y si en ésta se ha considerado aspectos como cambios organizacionales, marco legal informático, tecnología externa, recursos informáticos necesarios, etc.

Asimismo, el auditor deberá evaluar si se presta adecuada consideración a nuevas tecnologías informáticas, para los fines de la organización, si las tareas y actividades que esta presenta, posee una adecuada asignación de recursos para poder llevarlas a cabo, plazos estimados de culminación, etc.

Adicionalmente, una práctica muy sana es la revisión de las actas de sesiones del Comité de Informática dedicadas a la planificación estratégica, la identificación y lectura de los documentos relacionados

a la planificación estratégica, lectura y comprensión detallada del Plan Estratégico sobre los objetivos empresariales, cambios organizativos, evolución tecnológica, plazos y niveles de recursos, entrevistas al Gerente de Sistemas, miembros del Comité y usuarios con el objetivo de evaluar su grado de participación y conocimiento respecto al contenido del Plan.

Adicionalmente, el auditor deberá revisar otros planes muy importantes como son el Plan Maestro Anual y el Plan de Contingencias. El Plan Maestro Anual describe las actividades y proyectos a desarrollarse durante todo el año, cronogramas de trabajo, requerimientos tecnológicos, etc.; mientras que el Plan de Contingencias enmarca los riesgos y amenazas a la que está expuesta la organización y las actividades a tomar para minimizarlas y asegurar la continuidad operativa del negocio. El auditor deberá revisar que estos dos últimos planes estén elaborados y actualizados de acuerdo a las necesidades de la organización.

5.3.1.2. Evaluación de la Organización

Entre los principales aspectos para la revisión de la organización están:

- Realizar un seguimiento a las actividades realizadas por el Comité de Informática, mediante la revisión de la normativa interna, para conocer las funciones que debería cumplir el Comité de Informática, tener entrevistas con algunos de sus miembros para conocer la gestión que el Comité realiza y verificar que se cumple con las funciones encomendadas al Comité.
- Verificar el grado de independencia que mantiene el área de informática, con el resto de departamentos, al interior de la organización.
- Evaluar la segregación de funciones en el área de informática, mediante la revisión de su organigrama funcional, la revisión de las funciones y responsabilidades, la verificación de que el personal del área conozca sus funciones y responsabilidades, la observación “in situ” de las actividades desempeñadas por el personal y la comprobación de

la adecuada distribución de funciones y responsabilidades.

- Evaluar la gestión de recursos humanos, al revisar si existe un adecuado reclutamiento del personal de informática, verificar si se realizan evaluaciones periódicas del desempeño del personal, revisar los planes de capacitación y actualización en nuevas tecnologías, revisar las políticas laborales, etc.

5.3.1.3. Evaluación de la Dirección

En cuanto a la dirección el auditor deberá revisar los siguientes aspectos:

- Evaluar las líneas o nexos de comunicación que existe entre el gerente del área y el resto del personal, además, se deberá evaluar el grado de comunicación con otros departamentos, la gerencia general, etc.
- Revisar que exista un presupuesto financiero para el área de informática y que este cuente con la aprobación de la gerencia general y conste en el presupuesto global de la organización, revisar su cumplimiento y su razonabilidad.

- Evaluar las políticas para la adquisición de los recursos informáticos (hardware y software), autorizaciones, estándares para la adquisición de equipos, procesos de cotización y selección, razonabilidad de las inversiones y gastos en tecnología, etc.
- Revisar si existen contratos con empresas aseguradoras para la protección de los equipos informáticos y determinar su alcance, beneficios y limitaciones en las cláusulas de estos contratos.

5.3.1.4. Evaluación del Control

El auditor deberá evaluar la forma en que se llevan a cabo los controles encaminados hacia la seguridad de la información y se garantice su integridad, confiabilidad y disponibilidad. Para ello, el auditor deberá conocer las políticas y procedimientos para el control informático y verificar que sea realizado de manera efectiva; y, si dichos controles y la periodicidad con que se la realiza es la adecuada de acuerdo a las normas internacionales y ordenamientos emitidos por los organismos de control gubernamental.

5.3.2. Metodología para auditar los Controles Informáticos

5.3.2.1. Introducción

Otro de los aspectos sumamente importantes relativos a la gestión de TI, es la correcta implementación de los controles que garanticen una adecuada seguridad de la información; pues de lo contrario, se estaría expuesto a diversos riesgos (violación de accesos, errores, fraude, etc.) que podrían afectar de forma negativa al negocio; más aún, si reconocemos que la información es uno de los activos más importantes y estratégicos en las organizaciones.

Dentro de este proceso, el auditor debe determinar el grado de implementación de los controles informáticos en cada una de las diferentes áreas del procesamiento electrónico de datos, como por ejemplo, los controles físicos y lógicos, las seguridades a nivel de redes y aplicaciones, la planeación prevista ante posibles amenazas, etc. Asimismo, se debe definir el periodo a

ser examinado y las áreas claves para considerarse dentro de la auditoría.

En el caso de los auditores externos, es muy necesario que estos determinen cuáles van a ser las fuentes de información durante el examen; las cuales podrían ser: observación directa, revisión de documentación interna, entrevistas, encuestas, pruebas sustantivas, extracción y análisis de datos, etc.

Para la evaluación de las seguridades implementadas por la organización, el auditor puede valerse de diferentes herramientas informáticas, desde la planificación de las pruebas hasta la ejecución de las mismas.

5.3.2.2. Evaluación de las seguridades Físicas

Es importante que el auditor evalúe las seguridades implementadas en el área PED con respecto a hardware y software, datos, redes y del personal de informática. Se deberá revisar si existen precauciones contra diversas amenazas, las cuales podrían ser: inundaciones,

incendios, sabotaje, etc. Todas las contramedidas para afrontar dichas amenazas deberán ser perfectamente conocidas por el personal de informática y los usuarios, de acuerdo a las actividades asignadas; y, deberán con la documentación de soporte.

Dentro de esta revisión el auditor deberá evaluar:

- Los lugares en donde se encuentran ubicados el departamento PED y los distintos terminales que tienen acceso a la red de datos. A este respecto, es muy importante que el área PED no se encuentre ubicado junto a la cafetería o cocina de la empresa, frente a la calle o que éste tenga ventanales muy grandes sin las protecciones adecuadas.
- Los posibles riesgos a los que está expuesta la organización y las prevenciones establecidas por la dirección.
- Seguridades de acceso a las instalaciones, como guardias, puertas de hierro, cámaras de seguridad, porteros eléctricos, detectores de armas, etc.
- Controles de entrada y salida de equipos, especialmente los computacionales.

- Seguros vigentes para los equipos computacionales.

5.3.2.3. Evaluación de las Seguridades Lógicas

En este nivel será necesario evaluar si existen restricciones para el acceso a los sistemas de información, como la definición de perfiles y cuentas de usuario a nivel de las aplicaciones y el sistema operativo.

Se deberá verificar y recomendar, si no existen, el uso de las pistas de auditoría mediante el registro de LOG's de información clave como: la fecha y hora de ingreso, módulos accesados, usuario, dirección IP, tablas modificadas, registros modificados, etc.

Respecto al uso de contraseñas, es necesario evaluar que éstas sean cambiadas periódicamente (exigido por el propio sistema), que tengan un mínimo de seis caracteres, que sean alfanuméricas, que una vez cambiadas no puedan volverse a utilizar, etc.

Por otro lado, debe revisarse si controlan las entradas y salidas de personal, mediante la creación adecuada de las cuentas de usuario para nuevos empleados y el bloqueo inmediato de las cuentas de usuario de empleados que han salido de la organización o que no han sido accedidos durante un lapso determinado.

5.3.2.4. Evaluación de las Aplicaciones en Desarrollo

Este es tal vez, uno de los exámenes más elaborados, pues se requiere de manera adicional un conocimiento técnico sobre herramientas de desarrollo y bases de datos por parte del auditor de sistemas.

Entre algunos de los aspectos a evaluar está la forma en que se ha hecho la planificación del desarrollo de los sistemas, la participación de los usuarios en el establecimiento de las características funcionales, la asignación de recursos y elaboración de cronogramas de trabajo, estandarización de las rutinas elaboradas por los programadores y el cumplimiento del resto del ciclo de vida de los sistemas.

5.3.2.5. Aspectos de evaluación adicional

Otros de los aspectos que el auditor debe poner especial atención son las redes internas, las bases de datos y las comunicaciones; puesto que la mayoría de las organizaciones cuentan con sistemas en línea para sus operaciones; lo cual, en caso de ocurrir un daño en cualquiera de esos tres componentes, todo el servicio colapsaría, ocasionando molestias, retrasos y errores en el procesamiento electrónico de datos y el servicio brindado a clientes y usuarios.

Por otro lado, es necesario prestar atención a las seguridades para el uso de Internet y el correo electrónico, ya que estos podrían ser las puertas para el ingreso de virus y ataques cibernéticos.

Para finalizar, no podemos olvidarnos del Plan de Contingencias, la estrategia[*] más importante para la continuidad operativa del negocio, el cual debe cumplir con todas las características y requisitos establecidos en las normas internacionales y “las mejores prácticas”.

[*] El Plan de Contingencias no debe ser un documento archivado y olvidado.

5.4. Técnicas de Auditoría Asistidas por Computador (TAAC's)

5.4.1. TAAC's: ¿Qué son y cómo se aplican?

Las TAAC's son un conjunto de técnicas y herramientas utilizados en el desarrollo de las auditorias informáticas con el fin de mejorar la eficiencia, alcance y confiabilidad de los análisis efectuados por el auditor, a los sistemas y los datos de la entidad auditada.

Dichas técnicas incluyen métodos y procedimientos empleados por el auditor para efectuar su trabajo y que pueden ser administrativos, analíticos, informáticos, entre otros; y, los cuales, son de suma importancia para el auditor informático cuando este realiza una auditoría.

Dentro de las TAAC's se clasifican diferentes tipos de herramientas como el uso de los paquetes informáticos de auditoría estandarizado, los programas utilitarios y los programas de auditoría a la medida. Estos permiten la realización de pruebas y procedimientos analíticos, pruebas

sustantivas, pruebas de cumplimiento y evaluación de los controles informáticos implementados en los Sistemas de Información.

El uso de los TAAC's le permiten al auditor obtener suficiente evidencia confiable sobre el cual, sustentar sus observaciones y recomendaciones, lo que obliga al auditor a desarrollar destrezas especiales en el uso de estas técnicas, tales como: mayores conocimientos informáticos, discernimiento en el uso adecuado de las herramientas informáticas y analíticas, eficiencia en la realización de los análisis, etc.; sin dejar a un lado las técnicas tradicionales de auditoría como son la inspección, observación, confirmación, revisión, entre otros.

Dentro de la **SISAS Nº 9 – "Uso de Técnicas de Auditoría Asistidas por Computador",** se explica de manera más amplia la forma en que se deben aplicar dichas técnicas (Véase Apéndice 4).

5.4.2. Diseño de pruebas para la utilización de las TAAC's

Antes de utilizar las TAAC's el auditor debe diseñar de forma adecuada la forma en que se va a llevar a cabo el examen,

mediante el establecimiento oportuno de cuáles son los objetivos que busca el examen, establecer los sistemas de información críticos de la organización y la disponibilidad que se tiene para acceder a ellos [*], seleccionar los métodos y pruebas a realizarse durante la ejecución del examen, definir los reportes que se deberán generar como evidencias e informes de auditoria y otros procedimientos adicionales necesarios para la ejecución exitosa del examen.

Además, es necesario que el auditor tenga mucho cuidado respecto a la confidencialidad de los datos y sistemas a los cuales acceda durante su revisión. Para ello, el auditor debe realizar una adecuada planificación, selección y diseño de las técnicas y herramientas a utilizar, que le permita tener una seguridad razonable sobre la efectividad, confiabilidad y confidencialidad de los resultados que se vayan a obtener durante el examen.

5.4.3. Aplicación de TAAC's en la Auditoría Informática

[*] Muchas organizaciones no dan las facilidades a los auditores para que puedan acceder directamente a sus Sistemas de Información, pues lo consideran como una “intervención” o violación de su privacidad.

Una de las ventajas más notorias de las Técnicas de Auditoría Asistida por Computador es la versatilidad que estas presentan para la realización del trabajo de campo de la auditoría, ya que estas se pueden utilizar sin importar el tipo de organización, su tamaño, sus operaciones y sector del mercado. Pero, para ello el auditor deberá tener el suficiente discernimiento y experiencia profesional para establecer la técnica o herramienta a utilizar.

Sin embargo, el auditor dispone de una clasificación estandarizada respecto a las principales TAAC's aplicadas por auditores de todo el mundo; lo cual, facilita enormemente la selección de las técnicas y herramientas a utilizarse. Dicha clasificación se muestra a continuación:

- Técnicas Administrativas.
- Técnicas para evaluar los controles de Aplicaciones en Producción.
- Técnicas para análisis de Transacciones.
- Técnicas para análisis de Datos.
- Técnicas para análisis de Aplicaciones.

Dichas técnicas son analizadas más adelante en cuanto a sus principales características y formas de aplicación, aunque vale

mencionar que cada auditor es libre de aplicar de diversas formas dichas técnicas de acuerdo a la entidad auditada y la experiencia de quien realiza el examen.

Por otro lado, es importante reconocer el hecho de que existen muchos auditores de sistemas de información que desconocen a las TAAC's por sus nombres formales, lo cual significa que a pesar de que en la práctica muchos profesionales han desarrollado sus trabajos de acuerdo a las TAAC's, estos no lo sabían.

5.4.4. Técnicas Administrativas

Las Técnicas Administrativas son aquellas que permiten al auditor establecer el alcance de la revisión, definir las áreas de interés y la metodología a seguir para la ejecución del examen. Estas a su vez se dividen en dos grandes grupos:

a) **Técnicas para establecer el orden de prioridades en el proceso de auditoría.:** Entre las que se encuentran:

Selección de Áreas de Auditoría.- Mediante esta técnica, el auditor establece las aplicaciones críticas o módulos específicos dentro de dichas aplicaciones que necesitan ser

revisadas periódicamente, que permitan obtener información relevante respecto a las operaciones normales del negocio. Para ello, el auditor debe determinar las operaciones críticas del negocio, ordenar dichas operaciones o actividades de acuerdo a su importancia, identificar los aplicativos que son utilizados para dichas operaciones y establecer la información que deberá ser recolectada periódicamente para su posterior revisión y análisis.

Esta técnica es muy utilizada por los auditores internos de empresas corporativas grandes o medianas con un alto volumen de transacciones y exige que el departamento de auditoría interna construya sus propios aplicativos (con la ayuda del departamento de sistemas), para que puedan realizar su trabajo de forma eficiente.

Modelaje.- Esta técnica es muy similar a la técnica de *Selección de Áreas de Auditoria*, cuya diferencia radica en los objetivos y criterios de selección de las áreas de interés; ya que esta técnica tiene como objetivo medir la gestión financiera de la organización y todo lo que ello involucra.

La forma de llevar a cabo esta metodología, es a través de comparar los indicadores y razones financieras de la organización con los valores esperados al inicio del periodo o con los de la industria, luego se deben establecer las desviaciones significativas para cada uno de los rubros examinados y aquellas que lo ameriten deberán ser revisadas y analizadas por el auditor o la gerencia; pues dicho examen son de interés para ambas funciones.

Sistema de puntajes.- A través de esta técnica el auditor selecciona las aplicaciones críticas de la organización de acuerdo a un análisis de los riesgos asociados a dichas aplicaciones y que están directamente relacionadas con la naturaleza del negocio mediante asignarle a cada riesgo un puntaje de ocurrencia, de tal forma que sean examinadas detalladamente aquellas aplicaciones con mayor nivel de vulnerabilidad ante posibles riesgos.

Esta metodología requiere que el auditor identifique las principales aplicaciones en producción, los riesgos inherentes a tales aplicaciones y la metodología para la asignación de puntajes, para luego establecer las

aplicaciones que tendrán prioridad en ser examinadas de acuerdo al puntaje obtenido.

b) Técnicas para automatizar la Auditoría: En esta categoría tenemos las siguientes técnicas:

Software de Auditoría Multisitio.- Esta es una técnica que se basa sobre el mismo concepto de los sistemas distribuidos, en el que una organización con varias sucursales u oficinas remotas, dispone de un software de auditoria capaz de ser utilizado en dichas sucursales y a la vez, pueda actualizar y almacenar la información resultante en una base de datos principal, generalmente ubicada en la matriz de la organización.

Centros de competencia.- Esta técnica consiste en centralizar la información que va a ser examinada por el auditor, a través de la designación de un lugar específico que recibirá los datos provenientes de todas las sucursales remotas y que luego serán almacenadas, clasificadas y examinadas por el software de auditoria.

Obviamente, la diferencia de esta técnica con la anterior, radica en que mientras en la técnica de *software de auditoria de multisitio*, la revisión de los datos se la hace en las sucursales para luego enviar los resultados a la matriz; en el caso de la técnica de *centros de competencia*, los análisis de los datos son realizados en la casa matriz en línea y los resultados son enviados a las sucursales.

5.4.5. Técnicas para evaluar los controles de Aplicaciones en Producción

Estas técnicas se orientan básicamente a verificar cálculos en aplicaciones complejas, comprobar la exactitud del procesamiento en forma global y específica y verificar el cumplimiento de los controles preestablecidos. Entre las más importantes tenemos las siguientes:

Método de Datos de Prueba.- Esta es una técnica que consiste en la elaboración de un conjunto de registros que sean representativos de una o varias transacciones que son realizadas por la aplicación que va a ser examinada, y que luego serán ingresadas en dicha aplicación para la verificación del procesamiento exitoso de los datos.

Los datos de prueba, dependiendo del tiempo que disponga el auditor, deberán ser elaborados tomando en consideración todas las posibles entradas que podría utilizar el usuario.

Al utilizar estas técnicas, el auditor podrá encontrar inconsistencias en el procesamiento de los datos en el caso de que los resultados que arroje el sistema sean diferentes a los previamente esperados. Para ello el auditor debe realizar un profundo análisis de los controles incorporados a la aplicación y de la información que va a ser ingresada, sus características y número de registros.

Facilidad de Prueba Integrada (ITF).- Esta técnica es similar a la de *datos de prueba*, con la diferencia de que en esta se trabajan con datos reales y ficticios.

La metodología es muy simple y consiste en realizar pruebas del procesamiento de datos a las aplicaciones que se encuentran en producción, comparando los resultados obtenidos con los datos reales y los datos ficticios, teniendo mucho cuidado de no alterar la información real, mediante asignar a los registros de prueba un campo que los identifique como tales.

Simulación paralela.- Esta es una técnica en la que el auditor elabora, a través de lenguajes de programación o programas utilitarios avanzados, una aplicación similar a la que va a ser auditada, con el objetivo de ingresar simultáneamente la misma información en ambas aplicaciones para verificar la exactitud del procesamiento de datos de la aplicación en producción.

El auditor para llevar a cabo esta técnica deberá poseer un amplio conocimiento sobre la aplicación auditada respecto a su diseño lógico y las funciones que este realiza.

5.4.6. Técnicas para Análisis de Transacciones

Estas técnicas tienen como objetivo la selección y análisis de transacciones significativas de forma permanente, utilizando procedimientos analíticos y técnicas de muestreo. Las principales técnicas pertenecientes a esta categoría son las siguientes:

Archivo de revisión de auditoría como control del sistema (SCARF).- Esta es una técnica muy utilizada por los departamentos de auditoría interna de muchas organizaciones y consiste en el diseño de ciertas medidas de control para el

procesamiento electrónico de los datos, para luego incorporarlos dentro de los aplicativos en producción (como rutinas huéspedes), con el objetivo de garantizar un control permanente de las transacciones realizadas.

Para poder llevar a cabo esta técnica, el auditor debe establecer de forma clara los objetivos de control necesarios y presentarlos de forma entendible al personal de sistemas, para que estos hagan las incorporaciones requeridas. El resultado final será la generación de un archivo de datos que almacenará una réplica de los registros que hayan presentado anomalías para el posterior análisis del auditor.

Archivo de revisión de auditoría por muestreo (SARF).- Esta es una técnica muy utilizada por los auditores externos y consiste en la definición de ciertos parámetros de selección de registros utilizando muestreo, para luego analizarlos detalladamente.

La metodología para llevar a cabo esta técnica consiste en la presentación de los requerimientos de selección al personal de sistemas, seleccionar los registros que cumplan con los requerimientos (utilizando SQL), utilizar muestreo estadístico

para seleccionar los registros que serán examinados, analizar dichos registros y finalmente, emitir un informe.

Esta técnica, como vemos, no requiere la incorporación de rutinas de programación dentro de los aplicativos, aunque de ser necesario, se lo podría hacer en caso de que se realicen auditorias recurrentes.

Registros Extendidos.- Esta es una técnica muy particular y útil para los auditores que han desarrollado ciertas destrezas en el análisis de datos; y, consiste en la conservación histórica de todos los cambios que haya sufrido una transacción en particular, convirtiéndose en un LOG de auditoría.

Esta técnica requiere de la incorporación de rutinas especiales en las aplicaciones en producción por parte del personal de sistemas, que permitan almacenar en un archivo todos los cambios efectuados a las transacciones almacenadas en la Base de Datos.

5.4.7. Técnicas para el Análisis de Datos

Las técnicas para el examen de archivos son aquellas que están orientadas hacia el uso de programas informáticos especializados

que le permiten al auditor, de forma eficiente y flexible, examinar la información que ha sido procesada electrónicamente a través de los sistemas de información, aplicativos o programas utilitarios. Entre las principales técnicas para el examen de archivos, tenemos las siguientes:

Programas generalizados de auditoría.- Esta es una de las técnicas de mayor desarrollo y aplicación en los últimos años, tal es así, que se encuentran disponibles en el mercado, numerosos paquetes de auditoría con muy buen desempeño y flexibilidad en los tipos de archivos que pueden examinar. Los más conocidos y difundidos en nuestro medio son IDEA y ACL, aunque también existen programas como AUDAP, AUDITOR 2000, entre otros.

Las ventajas de utilizar estas herramientas, radica en la facilidad para el diseño de las pruebas de auditoría, la flexibilidad en cuanto a los formatos de archivo que pueden ser examinados y la adaptabilidad que estos tienen para manejar y presentar la información de acuerdo a las necesidades del auditor.

En el siguiente capítulo, se presenta de forma más detallada la forma en que son utilizados en la práctica los programas generalizados de auditoría.

Programas de auditoría a la medida.- Consisten en programas desarrollados especialmente para el análisis de datos de un sistema de información en particular, cubriendo todas las funciones y características que este posea, de acuerdo a los objetivos del auditor.

Estos programas de auditoría a la medida pueden ser desarrollados directamente por el auditor con la ayuda del personal de informática de la organización o viceversa, de acuerdo al grado de complejidad que tenga el sistema de auditoría a ser desarrollado.

Los programas de auditoría a la medida pueden ser utilizados aparte del personal de auditoría, por la alta gerencia y por el responsable del área PED.

Programas Utilitarios.- Son programas estandarizados para la ejecución de actividades muy diversas para el manejo de la

información, la gestión de documentos, la realización de cálculos matemáticos y estadísticos, el almacenamiento de datos y control de proyectos, etc.; los cuales, son muy utilizados por los auditores durante la ejecución de todo el proceso de auditoría.

Además, algunos de ellos le permiten al auditor la extracción, almacenamiento y análisis de datos de forma muy eficaz, mejorándose de esa forma la calidad del trabajo de auditoría tanto en la disminución de errores, como en el manejo y presentación de la información.

Por otro lado, éstas también permiten realizar pruebas muy variadas para verificar la exactitud y razonabilidad de los datos. No obstante, se debe tener mucho cuidado durante la utilización de estos programas, pues estos podrían alterar de forma permanente e irreparable los datos examinados.

5.4.8. Técnicas para el Análisis de Aplicaciones

Estas técnicas a diferencia de las técnicas anteriormente mencionadas, posee un grado mayor de complejidad respecto a su aplicación y grado de conocimiento técnico que debe poseer el auditor, pues se orientan hacia la evaluación del funcionamiento

interno de las aplicaciones en producción y la forma en que estos procesan la información. Entre las principales técnicas para análisis de aplicaciones tenemos las siguientes:

Técnica de Imagen instantánea.- Consiste en obtener una imagen instantánea del procesamiento electrónico de datos en un momento determinado, a través de la identificación única de ciertas transacciones de interés para el auditor y que, mediante rutinas especiales, son seleccionadas para revisar el flujo que esta ha seguido dentro del sistema.

En algunos casos, esta técnica requiere un grado de conocimiento amplio por parte del auditor en el diseño de sistemas, ya que este debe comprender el diseño lógico y estructural del sistema para identificar donde debe ser implementada la rutina SNAPSHOT.

Técnica de Mapeo.- Esta es una técnica que es muy utilizada por desarrolladores de sistemas de información para medir la eficiencia de ejecución de las rutinas que integran el sistema, a través de la utilización de programas especializados para dicho fin que mediante reportes presentan las veces en que se ejecutan las

rutinas implementadas y el tiempo que le ha tomado al procesador ejecutarlas.

Adicionalmente, mediante esta técnica se puede determinar las rutinas que no han sido utilizadas y aquellas que posiblemente han sido incorporadas con fines fraudulentos. Por lo tanto, esta técnica es muy útil al auditor para identificar rutinas innecesarias o riesgosas, medir la eficiencia en el procesamiento de la información y detectar posibles fraudes por parte del personal de sistemas.

Técnica de Rastreo.- Esta técnica es muy parecida a la técnica de Mapeo, con la diferencia de que mediante la técnica de Rastreo, se establece el orden en que han sido ejecutadas las rutinas durante una determinada transacción. Esto permite que el auditor pueda evaluar si el orden secuencial en que se va ejecutando cada una de las etapas del procesamiento electrónico de datos coincide con los procesos institucionales preestablecidos.

Análisis Lógico de las Aplicaciones.- Esta técnica consiste en la revisión del programa de acuerdo a las especificaciones técnicas y operativas presentadas en los Manuales de Diseño y Usuario, que

permita identificar errores o inconsistencias en el procesamiento electrónico de datos.

Por otro lado, el auditor debe poseer un alto grado de comprensión sobre la lógica del programa y de los manuales que lo acompañan; pero para ello, el auditor debe estar plenamente convencido de que los manuales del programa están adecuadamente elaborados y libres de errores significativos.

5.5. Retos de la Auditoría hacia el futuro

5.5.1. Una visión de la Auditoría del Futuro

A través de estos últimos años, la auditoría financiera ha evolucionado de forma muy acelerada y ha ido incorporando en el camino, el uso de distintas herramientas: financieras, estadísticas y especialmente informáticas; lo que la convierte una profesión muy dinámica y exigente, que obliga a quienes la ejercen, a desarrollar nuevas prácticas, enfoques y pruebas para lograr los objetivos previstos.

Hoy no es raro hablar de auditoría asistida por computador, ya que casi todas las actividades que realiza el auditor lo hace mediante los ordenadores. Sin embargo, todavía existen profesionales de la auditoría, con muchos años de experiencia y

prestigio, que son resistentes al cambio y se les hace difícil dejar de utilizar sus “viejos papeles de trabajo” (las hojas de 7 y 14 columnas) para utilizar los papeles de trabajo electrónicos; pero, poco a poco van incorporando a sus trabajos el uso del computador.

Asimismo, la auditoría de Sistemas de Información se va convirtiendo poco a poco, en uno de los requisitos clave dentro de los contratos de auditoría financiera, puesto que es un factor necesario para garantizar la seguridad y eficiencia en los ambientes de Procesamiento Electrónico de Datos.

En el futuro inmediato, la Auditoría de Sistemas de Información será cada vez más requerida por las organizaciones privadas y públicas; y será tan importante como la Auditoría Financiera; es más, los servicios de Auditoría de Sistemas de Información, serán contratados de forma independiente de si se realiza o no junto con una Auditoría Financiera.

Por otro lado, el uso que se le dará a la auditoría será no solo como una forma de detectar errores o fraudes; sino que se convertirá en una herramienta utilizada para el mejoramiento de

la calidad de vida de las personas, utilizada en la construcción de sociedades cuyas políticas y economías sean transparentes y mejores.

5.5.2. El Auditor de Sistemas de Información

El Auditor de Sistemas de Información debe ser un profesional con profundos valores éticos en el desempeño de su trabajo, procurando brindar un servicio de calidad cuando sea requerida su participación en la ejecución de una auditoría. El prestigio es muy importante en esta dura profesión, ya que ganarlo es muy difícil, pero perderlo es muy fácil.

Por ello, el auditor debe cuidarse en disponer de las herramientas necesarias para la ejecución óptima de su trabajo; mantenerse al día con los cambios tecnológicos que le permita trabajar en el cada vez más fluctuante entorno de las tecnologías de la información dentro de las organizaciones; que les permitan ser expertos en las diferentes ramas de la tecnología informática: comunicaciones, redes, ofimática, comercio electrónico, seguridad, gestión de bases de datos, etc.

El Auditor de Sistemas de Información dejará de ser un profesional procedente de otra área*, para pasar a ser un profesional formado y titulado en auditoría informática que tendrá a su alcance diferentes medios de formación, externa fundamentalmente, y que tendrá que formar una red de conocimientos compartidos con otros profesionales, tanto en su organización como con profesionales de otras organizaciones.

* Existen auditores de sistemas de información que son contadores o economistas.

CAPÍTULO 6

Uso de los Sistemas de Información para Auditoría y Control de Gestión

6.1. Software para Auditoría y Análisis de Datos

6.1.1. IDEA

6.1.1.1. Introducción

IDEA (por sus siglas en inglés), significa Interactive Data Extraction and Analysis (Análisis y Extracción Interactiva de Datos) y es una versátil y útil herramienta que permite el análisis de datos de forma eficiente y segura, adaptable para casi todas las plataformas tecnológicas de manejo de bases de datos.

Este producto es desarrollado por CASEWARE Corp., una prestigiosa compañía canadiense de desarrollo de software de auditoría que desde hace varios años ha ido introduciendo en el mercado, muchas soluciones tecnológicas para la ejecución eficiente de la auditoría.

Tal ha sido el éxito de este producto, que en la actualidad existen miles de usuarios alrededor del mundo, entre los que se cuentan auditores, gerentes de TI, consultores, funcionarios gubernamentales y altos ejecutivos.

El uso de este tipo de herramientas, facilita el acceso a los datos de los archivos y bases de datos sujetas a auditoría, sin depender del personal de sistemas; lo cual, facilita mantener un nivel de independencia aceptable por parte del auditor. Además, que su aplicación no requiere de avanzados conocimientos en el diseño de sistemas de información o el procesamiento electrónico de datos.

Por otro lado, la capacidad que tiene este producto para acceder a un gran volumen de datos, es casi infinito. Por ejemplo, el número de campos por cada tabla abierta es de

máximo 32,167; el número de registros que pueden ser leídos por cada tabla es de 2.1 x 10^{12} y el tamaño del archivo que puede ser abierto es de hasta 1.8 x 10^{18}; lo cual, demuestra la gran capacidad que tiene este software para acceder a la información de grandes corporaciones que manejan inimaginables Bases de Datos.

6.1.1.2. Componentes

Este software posee cuatro componentes principales que permiten realizar diferentes tareas, como la importación de datos, el análisis de datos, definición de estructuras de archivos y programación de rutinas especificas. A continuación se explican tales componentes:

IDEA.- Este es el módulo principal del software y es el que permite realizar las tareas de auditoría y análisis de datos, con una gran flexibilidad para acceder a archivos procedentes de archivos planos (.txt), hojas de cálculo (.xls), manejadores de bases de datos (.mdb), accesos remotos ODBC (conectividad de bases de datos), los DBMS (Sistemas de Administración de Bases de Datos), entre otros.

RDE.- Es el diseñador de estructuras para datos complejos importados; la cual, permite el uso de herramientas avanzadas para definir registros estándar y su posterior análisis.

DATAIMPORT.- Es una herramienta para la importación de reportes impresos en archivos planos.

IDEASCRIPT.- Es la herramienta más compleja del software, que permite a los auditores con sólidos conocimientos de programación, crear sus propias rutinas y funciones para el análisis de datos y diseño de pruebas de auditoría complejas o estandarizadas; mediante el uso de Visual Basic para aplicaciones (VBA).

6.1.1.3. Ventanas de IDEA

Existen dos ventanas principales de IDEA que permiten visualizar las diferentes herramientas, funciones y archivos para el análisis de datos, estas son: la ventana Base de Datos y la ventana Macros.

La Ventana Base de Datos es la que se presenta al iniciarse la aplicación. A continuación se presenta dicha ventana:

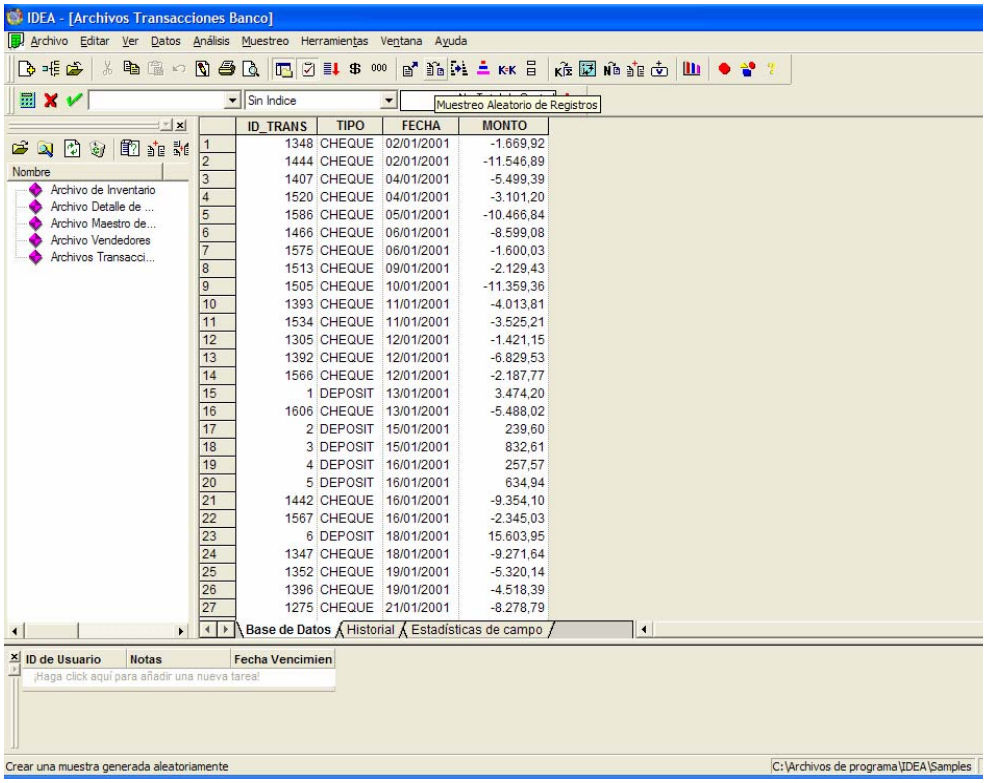


Figura 6.1. Ventana Base de Datos de IDEA

En cambio la Ventana Macros debe ser accedida a través de la opción ***Herramientas/Macros/Nueva Macro***. Esta ventana permite a los usuarios avanzados de IDEA crear rutinas especiales de auditoría, mediante el uso del lenguaje de programación VBA. A continuación se muestra dicha Ventana:

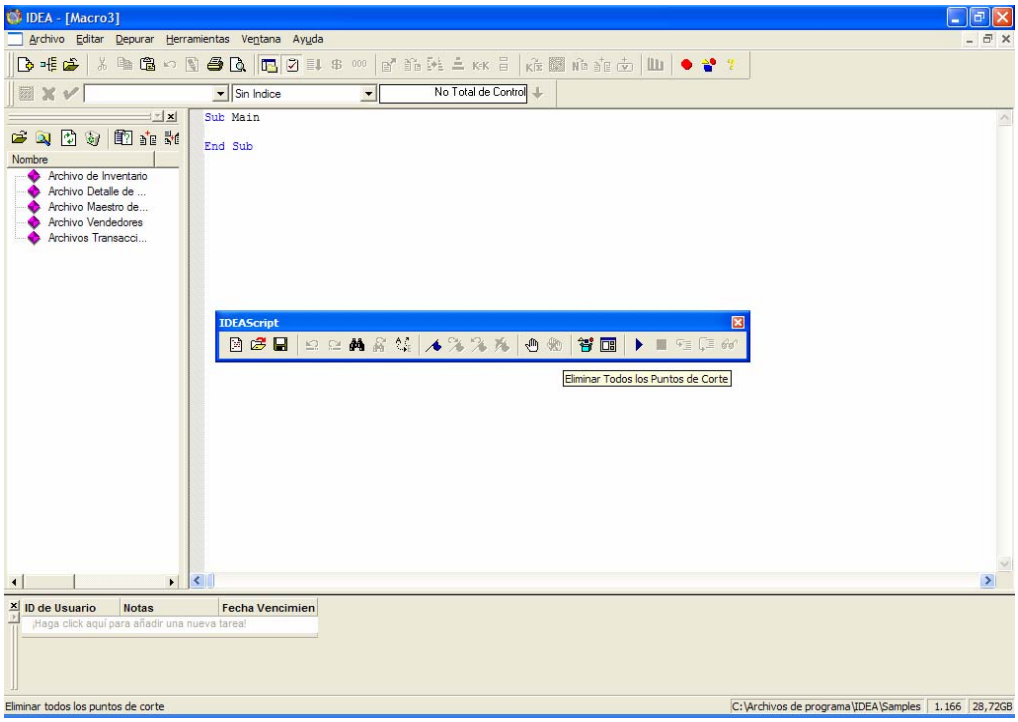


Figura 6.2. Ventana Macro de IDEA

6.1.1.4. Ventana Base de Datos

Mediante esta ventana, el usuario está en capacidad de observar las tablas abiertas y los campos que las conforman, de una manera fácil y amigable. Adicionalmente, existen tres vistas dentro de la Ventana Base de Datos, que se encuentran en la parte inferior de la ventana. Estas son: Vista Base de Datos, Vista Historial y Vista Estadísticas de Campo.

Cuando se accede a la **Vista Base de Datos**, se puede apreciar los datos como si estuvieran en una hoja de cálculo en el que los nombres de los campos se encuentran en la parte superior en forma de columnas y los registros almacenados se presentan en forma de filas (Ver figura 6.1).

En el caso de la **Vista Historial**, el auditor puede ver todas las acciones realizadas en los archivos de datos abiertos en la Ventana Base de Datos; lo cual, permite tener un control sobre las actividades realizadas por parte de los Asistentes y Senior’s de auditoría, que hayan realizado diversas tareas de revisión a los archivos, tales como abrirlos, importarlos, sumarlos, ordenarlos, agregarles campos, estratificarlos, etc. Sin duda, este LOG es de mucha ayuda como soporte para los papeles de auditoría y sirve como herramienta de control del proceso de análisis de los archivos de datos examinados. En la Figura 6.3 se presenta dicha Vista.

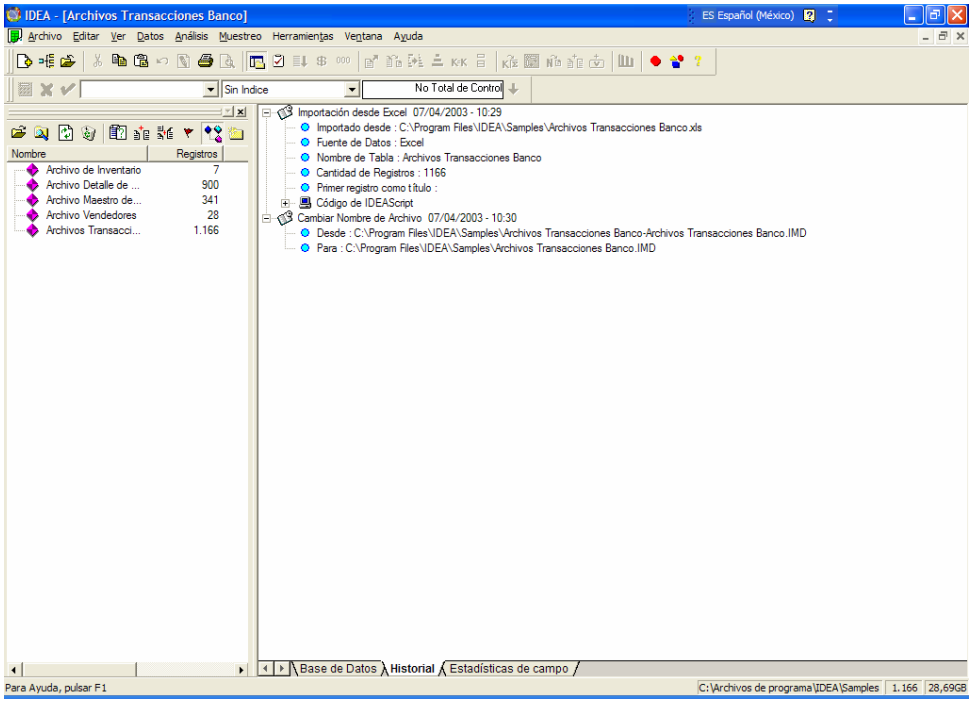


Figura 6.3. Vista Historial en la Ventana Base de Datos

Por otro lado, la **Vista Estadísticas de Campo**, le permiten al auditor conocer algunas características de interés sobre los campos que componen a las tablas examinadas. En el caso de los campos tipo fecha, se presentan las siguientes estadísticas: el número de registros, los registros en blanco, valores correctos, la fecha más temprana, la fecha más tardía, numero de registros más tempranos, más tardíos, el día más común y el número de registros por cada mes del año, lo cual, le permite al auditor conocer si los registros

almacenados corresponden a fechas razonables y si el comportamiento transaccional es de acuerdo a lo esperado.

En cambio, para los campos numéricos se presentan las siguientes estadísticas: Valor Neto (Sumatoria entre positivos y negativos), Valor Absoluto (Sumatoria sin importar positivos y negativos), número de registros, número de elementos cero, Valor positivo (Sumatoria de los valores positivos), Valor negativo (Sumatoria de los valores negativos), número de registros positivos, número de registros negativos, número de datos erróneos, número de datos correctos, Valores mínimo, máximo y medio; entre otros. Estas estadísticas le permiten al auditor, conocer el comportamiento de los datos y detectar irregularidades o errores.

Un aspecto interesante, es el hecho de que el auditor, con un clic, puede visualizar y guardar los datos correspondientes a cada estadística. En la **Figura 6.4** se muestran la Vista Estadísticas de Campo.

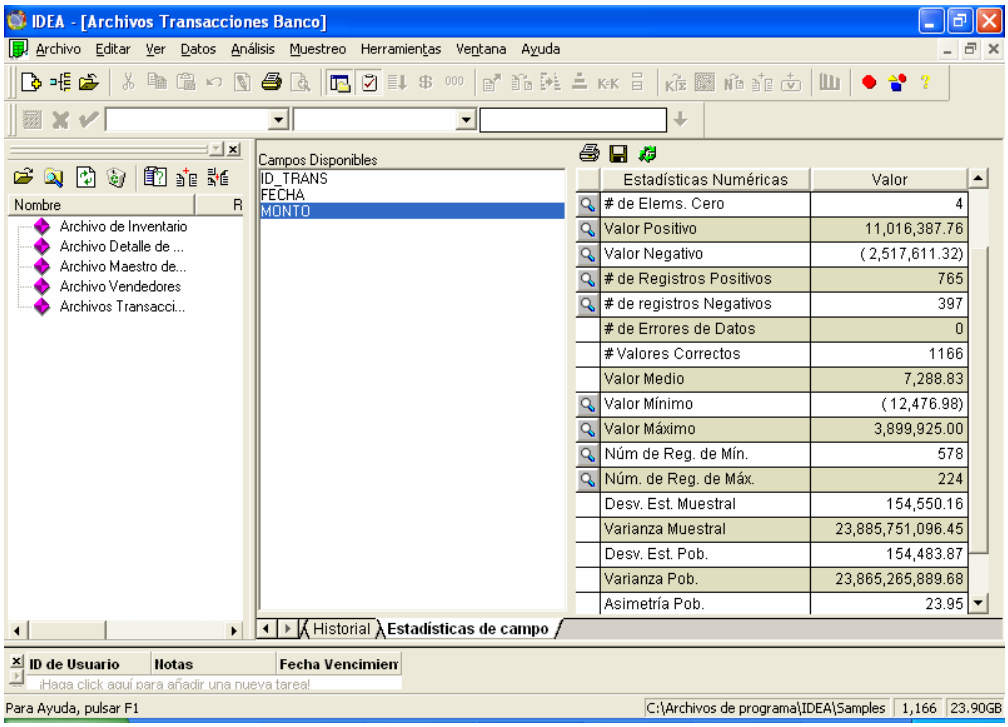


Figura 6.4. Vista Estadísticas de Campo

6.1.1.5. Caso de aplicación de IDEA

A continuación se expone un caso práctico de aplicación de este software, aplicado a una institución financiera.

1. Creación de la Carpeta de Trabajo

El primer paso para iniciar el trabajo, es la creación de la carpeta de trabajo del cliente, a través de la opción: **Archivo / Establecer carpeta de trabajo**

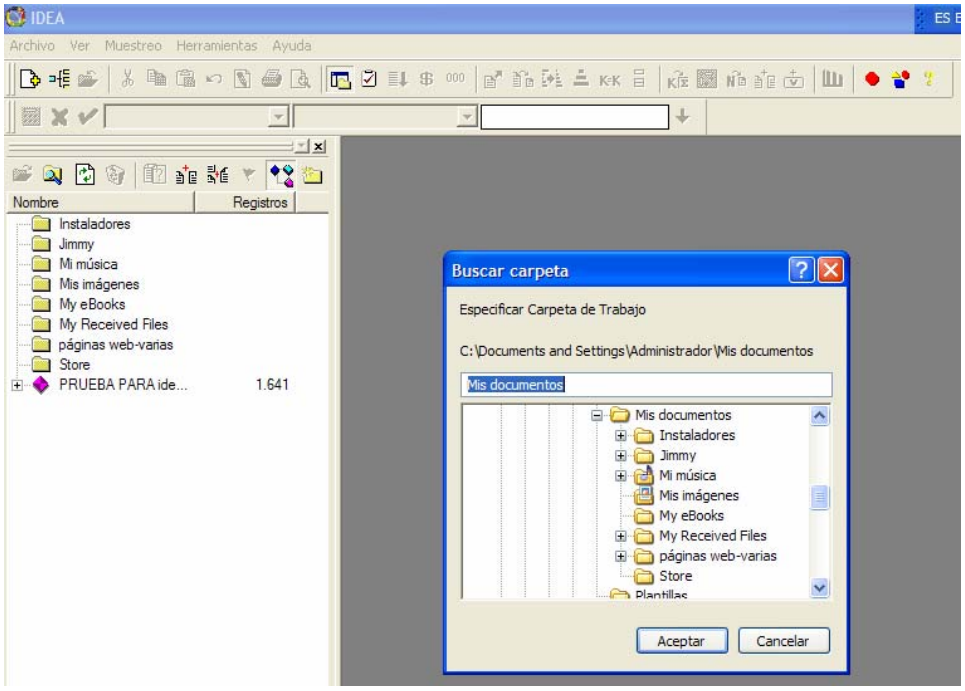


Figura 6.5. Ventana para guardar carpeta de trabajo

Una vez establecida la carpeta de trabajo, el programa automáticamente guardará todos los archivos resultantes del proceso de análisis en dicha carpeta. Se debe crear una carpeta diferente para cada cliente, con el fin de evitar errores.

2. **Importar los archivos de datos**

Ahora el auditor debe seleccionar la fuente de los datos para su análisis, mediante importar el archivo o base de datos donde se encuentra almacenada la información. Algo importante es la flexibilidad que muestra este software, puesto que el auditor puede seleccionar la información en línea o a través de un archivo de datos. Para realizar la importación, el auditor debe escoger la opción: **Archivo / Asistente de Importación.**

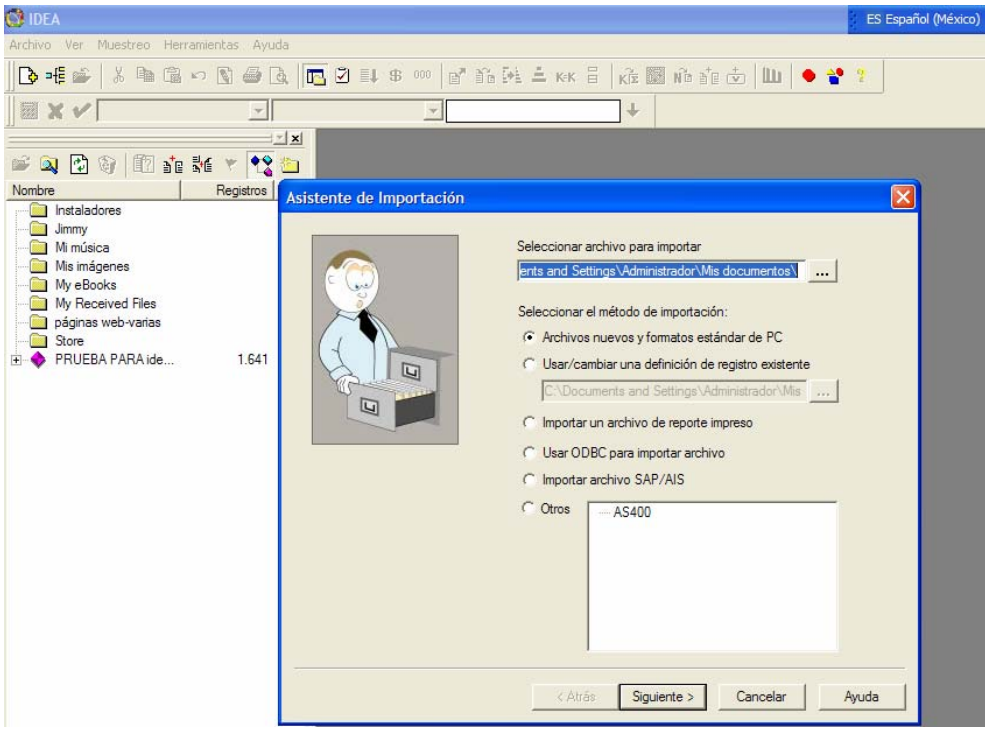


Figura 6.6. Asistente para la importación de datos

A través de este asistente, el auditor puede seleccionar la fuente de datos y el tipo de archivo; de forma muy sencilla y dinámica. Luego de ello, se puede dar formato a las columnas y ver las estadísticas de campo para efectos de constatar que se ha importado correctamente los datos o encontrar de forma preliminar alguna inconsistencia en los registros.

3. Análisis de los datos

- **Selección por muestreo**

El auditor puede seleccionar un conjunto de registros para ser examinados, a través de utilizar muestreo, mediante el Menú **Muestreo / Aleatorio…**

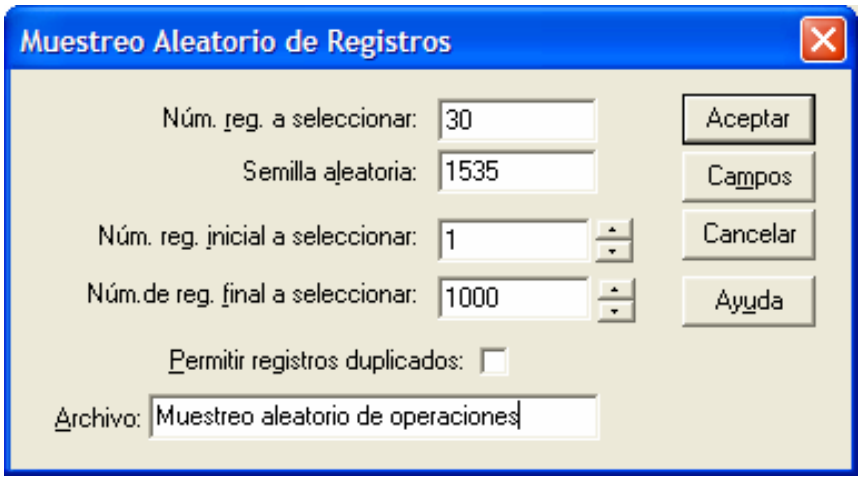
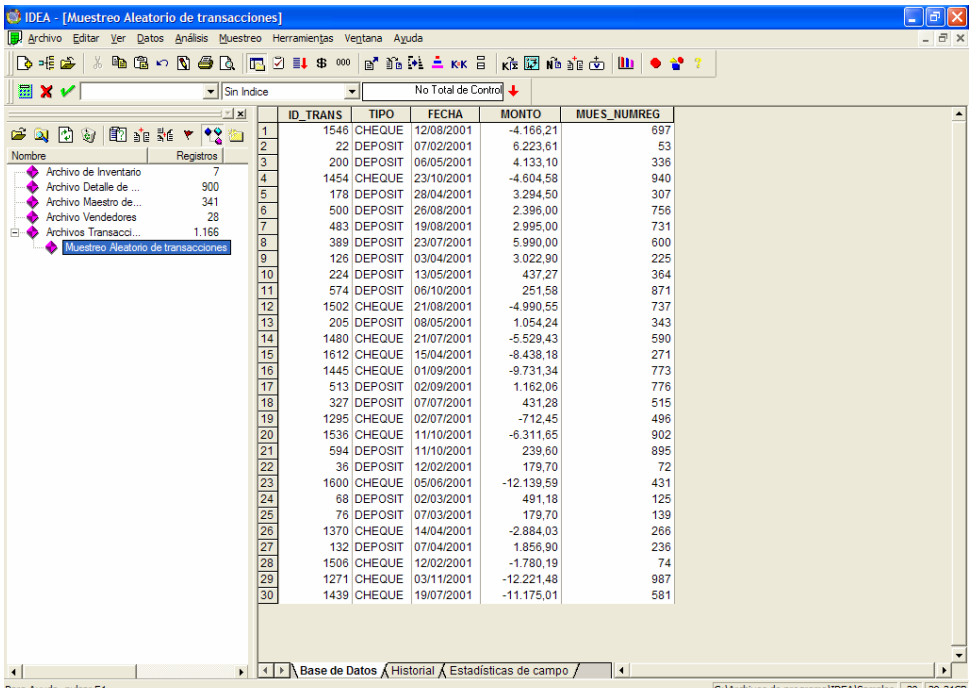


Figura 6.7. Ventana de Muestreo Aleatorio de registros

El auditor a través de esta Ventana, especifica el número de registros a seleccionar, que en nuestro caso corresponde a 30 registros; el registro inicial a seleccionar y el registro final, los cuales se recomienda que sean el primero y el final del archivo respectivamente; y, el nombre del archivo de resultados. Luego de presionar **Aceptar** se presenta la siguiente pantalla:



	ID_TRANS	TIPO	FECHA	MONTO	MUES_NUMREG
1	1546	CHEQUE	12/08/2001	-4.166,21	697
2	22	DEPOSIT	07/02/2001	6.223,61	53
3	200	DEPOSIT	06/05/2001	4.133,10	336
4	1454	CHEQUE	23/10/2001	-4.604,58	940
5	178	DEPOSIT	28/04/2001	3.294,50	307
6	500	DEPOSIT	26/08/2001	2.396,00	756
7	483	DEPOSIT	19/08/2001	2.995,00	731
8	389	DEPOSIT	23/07/2001	5.990,00	600
9	126	DEPOSIT	03/04/2001	3.022,90	225
10	224	DEPOSIT	13/05/2001	437,27	364
11	574	DEPOSIT	06/10/2001	251,58	871
12	1502	CHEQUE	21/08/2001	-4.990,55	737
13	205	DEPOSIT	08/05/2001	1.054,24	343
14	1480	CHEQUE	21/07/2001	-5.529,43	590
15	1612	CHEQUE	15/04/2001	-8.438,18	271
16	1445	CHEQUE	01/09/2001	-9.731,34	773
17	513	DEPOSIT	02/09/2001	1.162,06	776
18	327	DEPOSIT	07/07/2001	431,28	515
19	1295	CHEQUE	02/07/2001	-712,45	496
20	1536	CHEQUE	11/10/2001	-6.311,65	902
21	594	DEPOSIT	11/10/2001	239,60	895
22	36	DEPOSIT	12/02/2001	179,70	72
23	1600	CHEQUE	05/06/2001	-12.139,59	431
24	68	DEPOSIT	02/03/2001	491,18	125
25	76	DEPOSIT	07/03/2001	179,70	139
26	1370	CHEQUE	14/04/2001	-2.884,03	266
27	132	DEPOSIT	07/04/2001	1.856,90	236
28	1506	CHEQUE	12/02/2001	-1.780,19	74
29	1271	CHEQUE	03/11/2001	-12.221,48	987
30	1439	CHEQUE	19/07/2001	-11.175,01	581

Figura 6.8. Resultados del Muestreo Aleatorio

Además del muestreo aleatorio, se pueden realizar muestreo sistemático, muestreo estratificado, por unidad monetaria y

utilizar técnicas estadísticas más complejas como la evaluación de atributos y la generación de números aleatorios. Una vez realizada la selección aleatoria de registros, el auditor puede proceder a la revisión de la documentación de soporte de dichas transacciones, para encontrar alguna inconsistencia o error.

- **Extracción de registros**

  El auditor puede realizar extracciones de aquellos registros que cumplan con ciertas condiciones de selección, de acuerdo a las necesidades que este tenga. Tal como se muestra en el siguiente ejemplo, que se necesita extraer los depósitos mayores a 2,000 dólares para efectos de notificación al CONSEP. Para ello, se deberá seleccionar el Menú **Datos / Extracción Indexada**

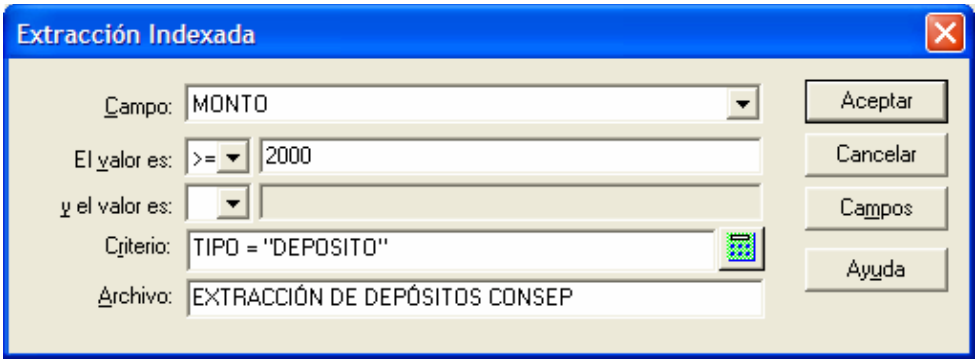


Figura 6.9. Extracción de registros

Nótese que en este caso se establece un criterio de selección que indica que solo se considere las operaciones de Depósito mayores a 2,000 dólares. El resultado se muestra a continuación en la siguiente figura:

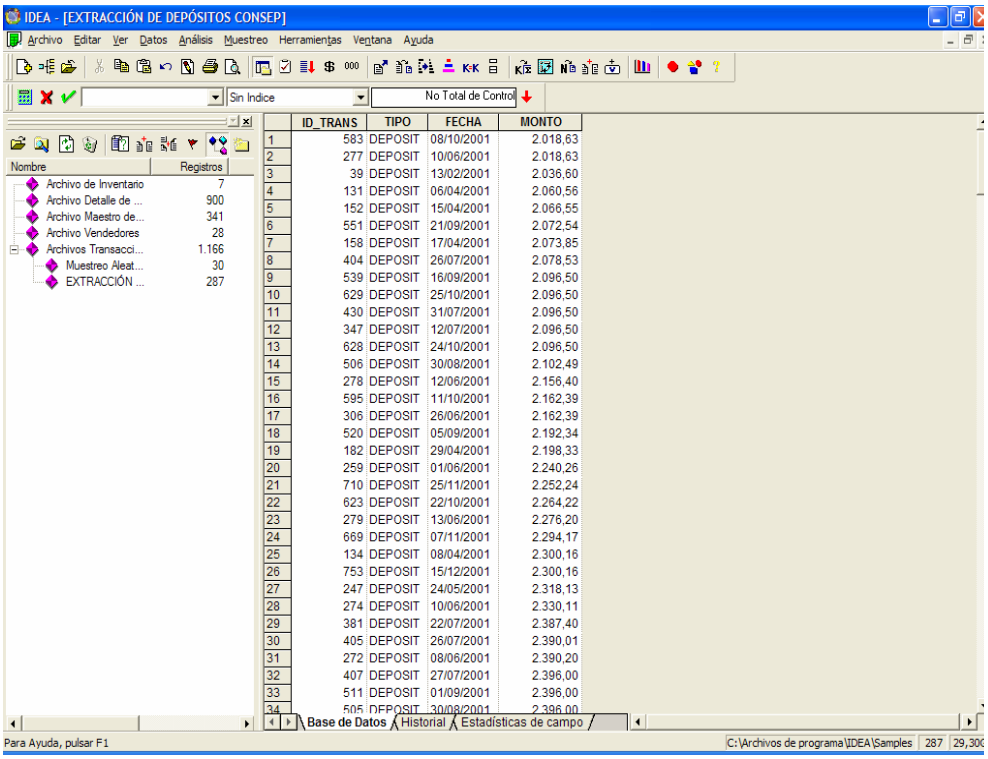


Figura 6.10. Resultado de la extracción de registros

Como se puede notar, solo se muestran los depósitos mayores a 2,000 dólares. Adicionalmente, se puede consultar

las estadísticas de campo para dicha selección, para ver el número de registros, el valor máximo, el valor mínimo, el total de depósitos, etc. En base a estos registros seleccionados, se procede a la revisión de la información de soporte, como el Formulario de Licitud de Fondos que es exigido por el CONSEP, cuando algún cliente supera un ingreso en su cuenta bancaria superior a los 2,000 dólares.

- **Detección de Duplicados**

  A través de la opción **Datos / Clave Duplicada / Detección,** podemos encontrar aquellos registros cuya clave principal han sido duplicados. Esto tiene especial aplicación en los números de cédula, número de factura o como en nuestro caso, el numero de transacción.

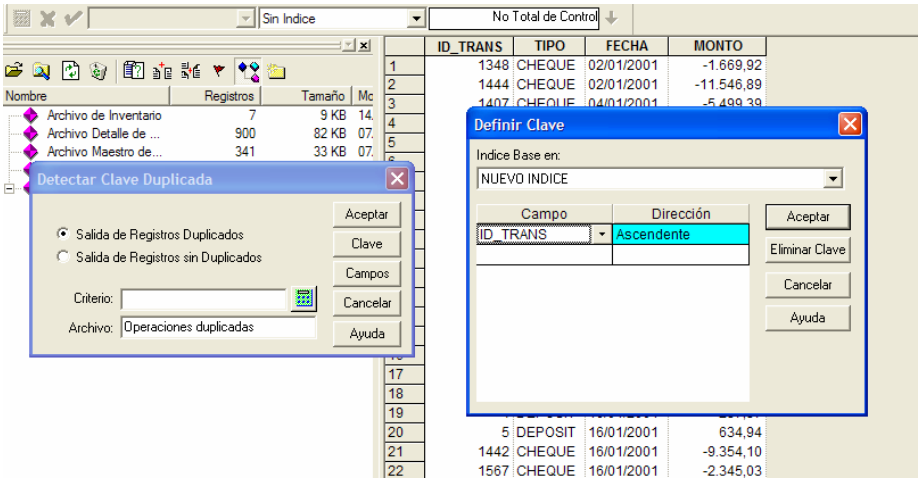
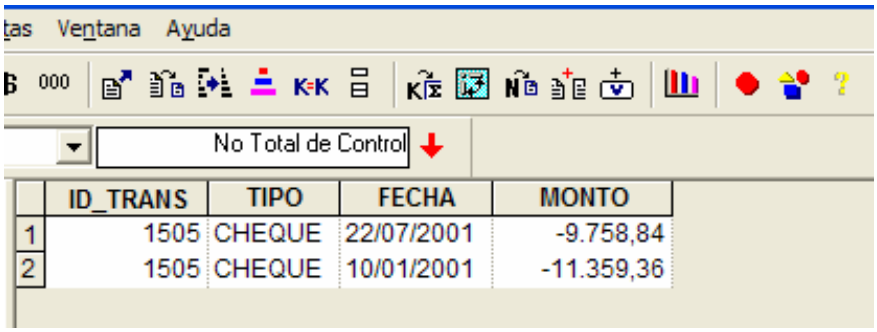


Figura 6.11. Parámetros para la Detección de campos duplicados

Para este análisis es necesario que el auditor especifique el campo que desea analizar, el mismo que deberá ser una clave principal de la tabla analizada. A continuación se muestra el resultado:



	ID_TRANS	TIPO	FECHA	MONTO
1	1505	CHEQUE	22/07/2001	-9.758,84
2	1505	CHEQUE	10/01/2001	-11.359,36

Figura 6.12. Resultado de la detección de campos duplicados

Como se aprecia, existen dos transacciones cuyos códigos son iguales y cuyas fechas y montos son diferentes, lo que significa que no es un registro que ha sido ingresado dos veces, sino que, corresponde a dos transacciones totalmente diferentes cuya clave de transacción ha sido ha ingresado dos veces.

- **Sumarizar Campos**

  En el caso de que el auditor desee totalizar ciertos campos numéricos de forma directa y de acuerdo a cada campo clave

diferente, puede valerse de la opción **Análisis / Sumarización de campo / Campo Clave,** tal como se muestra a continuación:

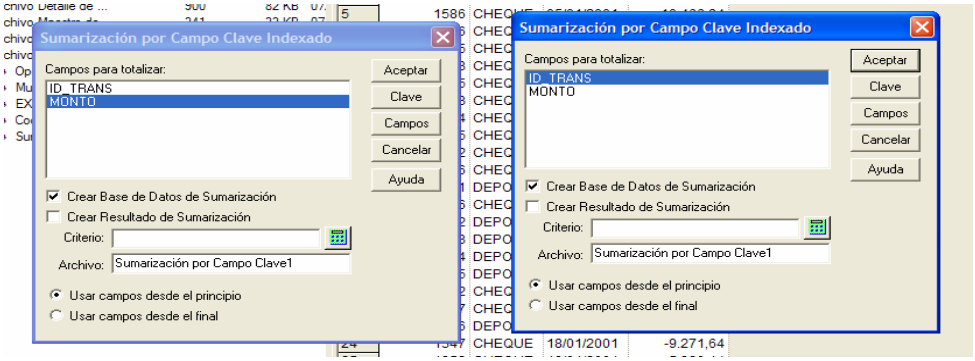


Figura 6.13. Sumarización por Campo Clave

Tal como se ve en la figura, el auditor debe especificar el campo que va a totalizar y el campo clave que servirá de referencia. A continuación se presenta los resultados:

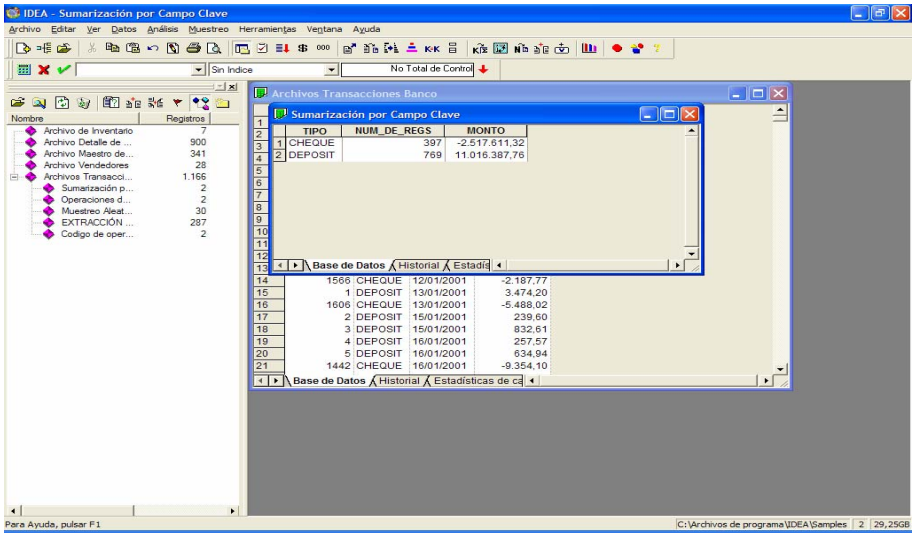


Figura 6.14. Resultado de la Sumarización por Campo Clave

Como se puede notar, se presenta el total de cheques pagados ($ 2.517.611,32) y el total de depósitos recibidos ($11.016.387,76).

- **Tabla Pívot**

  Esta herramienta se basa en el concepto de los cubos n-dimensionales en el que se pueden obtener resúmenes de ciertos campos de una tabla, muy parecido a las tablas dinámicas de Excel. Se puede acceder a él a través de la opción Análisis / Tabla Pívot. A continuación se la muestra:

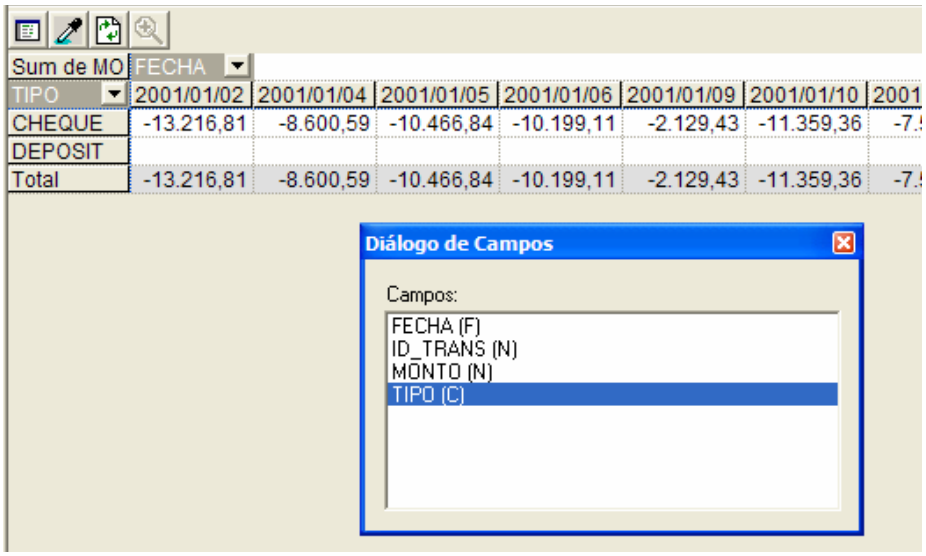


Figura 6.15. Tabla Pívot de IDEA

En nuestro caso, se ha querido realizar un resumen de los totales de cheques pagados y depósitos recibidos por cada día. El auditor tiene toda la libertad para formar los cubos que requiera, con tan solo arrastrar los campos desde la ventana **Dialogo de Campos** hasta las filas y columnas de la Tabla Pívot.

Estas son algunas de las muchas utilidades que tiene esta aplicación para la extracción y análisis de datos, que le permiten al auditor, realizar un trabajo muy completo orientado hacia la detección de errores y fraudes.

6.1.2. ACL

ACL es otro paquete de extracción y análisis de datos, muy similar a IDEA, tanto en las funciones incorporadas como en las características de visualización de los datos. Ya lleva quince años en el mercado y se ha convertido, al igual que IDEA, en uno de los más utilizados por los auditores externos e internos en todo el mundo.

Actualmente existe disponible la Versión 8; la cual, ha mejorado sustancialmente su desempeño y facilidad de uso en comparación con su predecesora la versión 7.

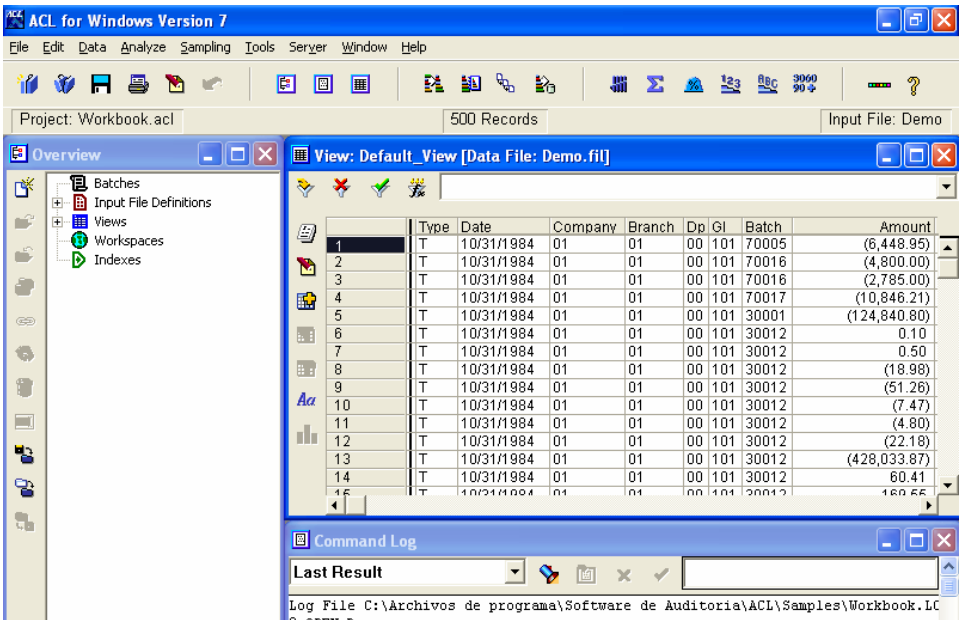


Figura 6.16. Ventana principal de ACL versión 7

Como se puede notar en la figura 6.16, la ventana principal de ACL es muy similar a la de IDEA 2002, con la diferencia de que en la parte izquierda se muestra una estructura de árbol en el que se muestra la estructura del proyecto, mostrándose las tablas, las vistas, los Scripts y los índices; a diferencia de

IDEA que muestra, en esa área, las tablas importadas y los resultados obtenidos por cada análisis realizado.

ACL es muy similar a IDEA en cuanto a las pruebas y análisis, por lo que no sería necesario realizar las mismas pruebas que se hicieron con IDEA en secciones anteriores. Sin embargo, es importante indicar que trabajar con IDEA es mucho más sencillo que con ACL; las funciones son más claras de comprender, asimismo las ventanas de Input son más especificas sobre los datos necesarios para el análisis; y, lo mas interesante de IDEA 2002 frente a ACL 7, es la posibilidad de acceder a los “datos objetivo” presentados en las estadísticas de campo y los gráficos, con tan solo un clic.

6.2. Software para administrar el proceso de Auditoría y los papeles de trabajo

6.2.1. CASEWARE WORKING PAPERS

Este es un software especializado en la administración y generación de papeles de trabajo de auditoría, con un ilimitado número de funciones y comandos, que permite mejorar el desempeño de los auditores, especialmente los Asistentes y

Senior's de Auditoría, en la ejecución de pruebas y documentación de evidencias.

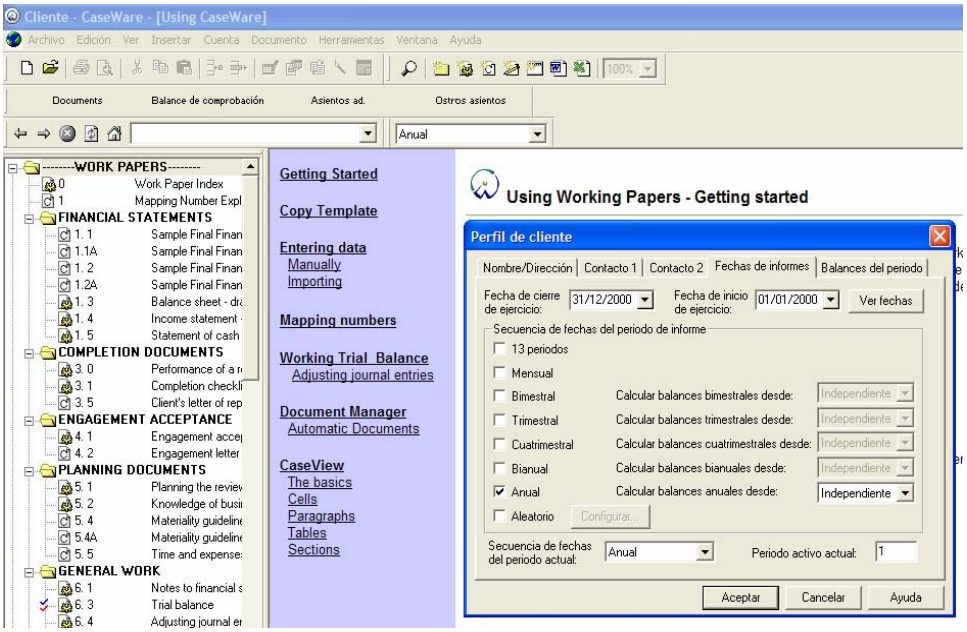


Figura 6.17. Ventana de inicio de Caseware Working Papers

La ventana presentada en la Figura 6.17, nos muestra la ventana de inicio de esta aplicación, luego de haber especificado una ubicación en el disco duro para el almacenamiento de todos los papeles de trabajo generados. El siguiente paso, es ingresar en la ventana “Perfil del Cliente”, toda la información básica del cliente auditado, como la dirección teléfono, contacto, periodo de revisión, fechas de presentación de informes, etc.

Al lado izquierdo de la ventana principal podemos apreciar en forma de árbol, cada uno de los papeles de trabajo y las subcarpetas donde se encuentran almacenadas; la carpeta principal, con el nombre del cliente, contiene al resto de subcarpetas y archivos.

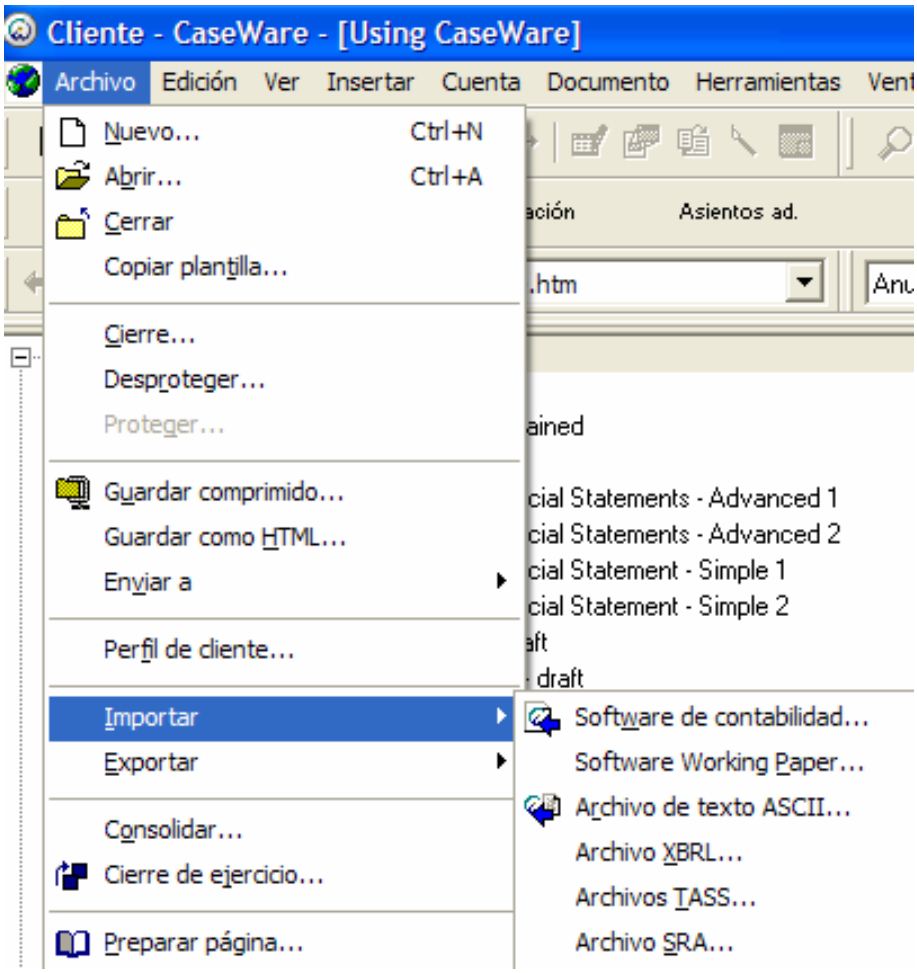


Figura 6.18. Menú de Importación de Caseware Working Papers

Ahora el auditor está en capacidad de poder importar o abrir cualquier archivo con la información contable o financiera para efectuar sus análisis y archivar las evidencias de auditoría. Como vemos en la Figura 6.18, el auditor tiene a su disposición la posibilidad de importar diversos tipos de archivos, como los archivos de salida de una gran variedad de software contable, archivos planos .txt, archivos de trabajo Working Papers e incluso los archivos de resultados generados por IDEA.

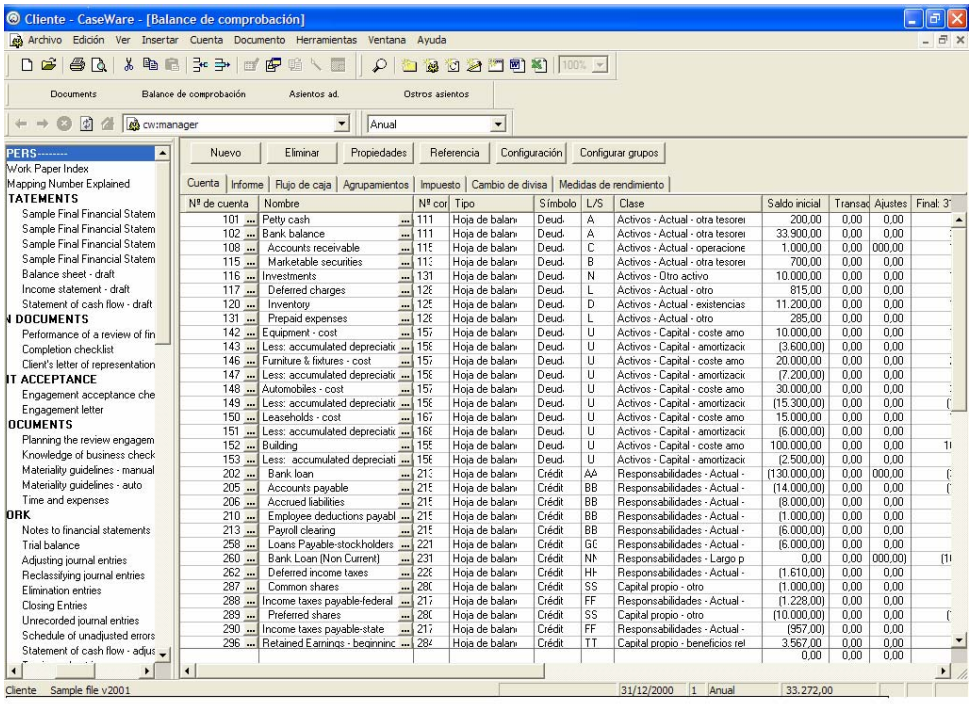


Figura 6.19. Ventana del Balance de Comprobación Contable

Una vez importada la información contable del cliente, a través del botón “Balance de Comprobación”, se puede visualizar la información contable que ha sido importada, en donde se muestra los códigos y saldos de cada cuenta a una fecha de corte determinada, tal como se puede apreciar en la Ventana 6.19.

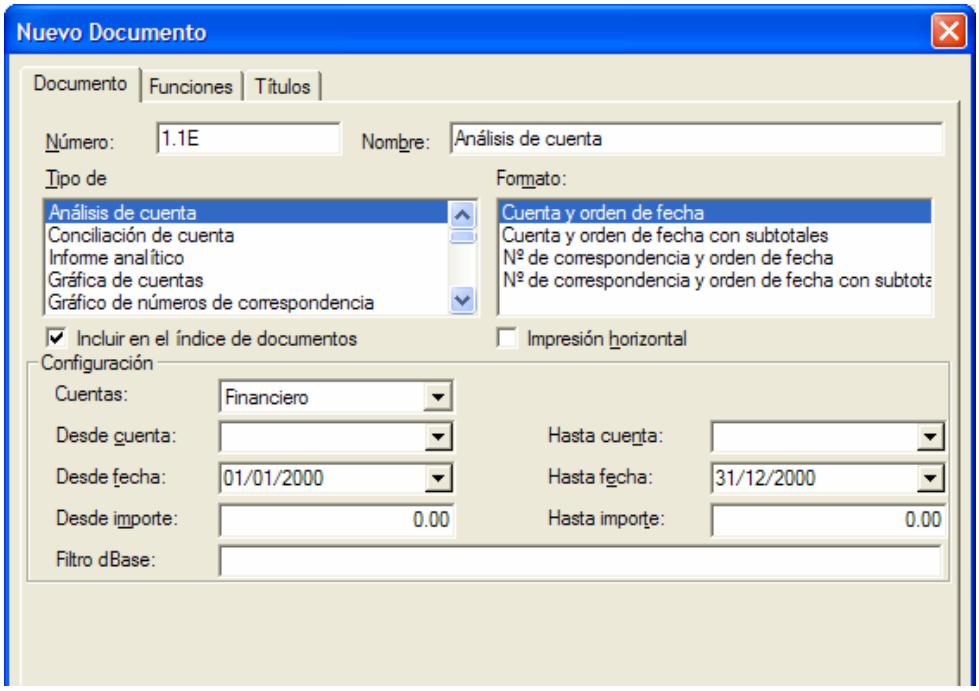


Figura 6.20. Ventana de generación de papeles de trabajo automáticos

Entre las muchas funciones que tiene este software, está la generación automática de ciertos papeles de trabajo estandarizados, como las cédulas sumarias y analíticas, cuyas

marcas de referencia incluyen el código, el responsable y la fecha de elaboración y revisión del documento. En la Figura 6.20, se presenta la ventana de generación de papeles de trabajo automáticos, para acceder a ella se debe presionar el botón "Nuevo documento Caseview" en la barra de herramientas.

Sin embargo, si el auditor desea generar los papeles de trabajo de forma manual para luego almacenarlos como plantillas, lo puede hacer de forma muy simple, dándole un clic en el botón "Nuevo documento Manual" de la barra de herramientas. Asimismo en el caso de que el auditor desee generar sus papeles de trabajo a través de MS Word o Excel, lo puede realizar a través del menú **Documento/Nuevo.**

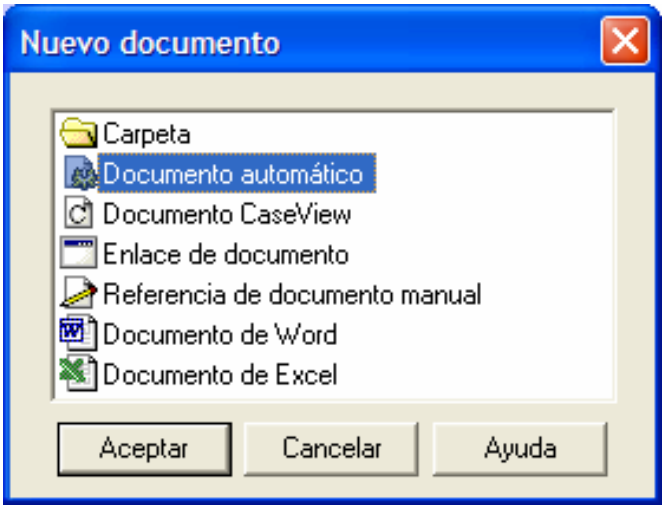


Figura 6.21. Ventana Nuevo documento Working Papers

Luego de seleccionar el tipo de documento, Word o Excel, debe especificar un código o número que identifique de manera única al documento, una descripción sobre su contenido y el nombre del archivo, el cual se almacenará por DEFAULT en la carpeta del cliente. Adicionalmente, en la pestaña Funciones, se debería especificar el auditor quien lo elaboró y quién lo revisó.

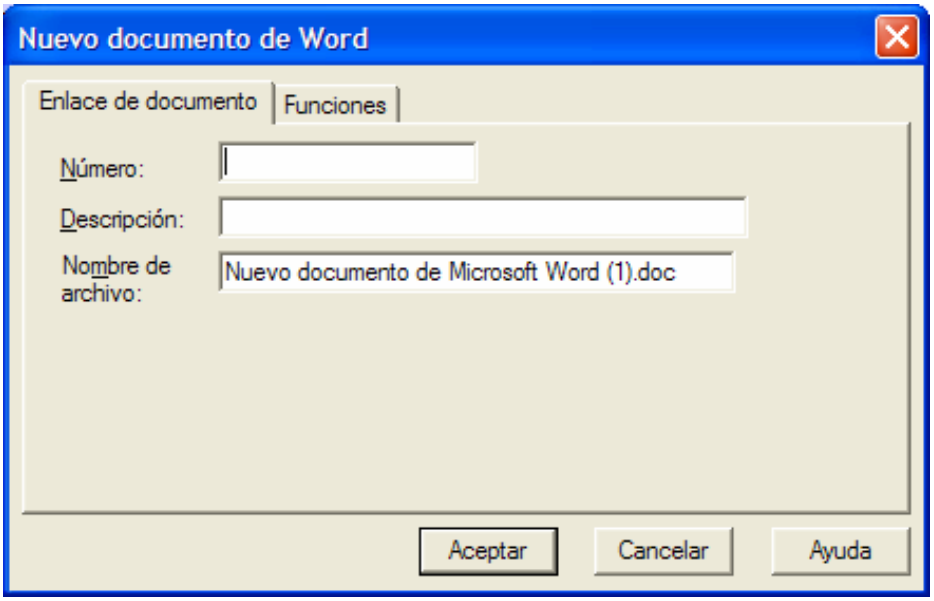


Figura 6.22. Ventana Nuevo documento de Word.

De manera adicional, en caso de que los papeles de trabajo ya existan, solo es necesario copiarlo en la carpeta del Cliente y

luego crear un vínculo hacia dicho archivo, mediante el botón "Nuevo Enlace de documento", cuya ventana es la siguiente:

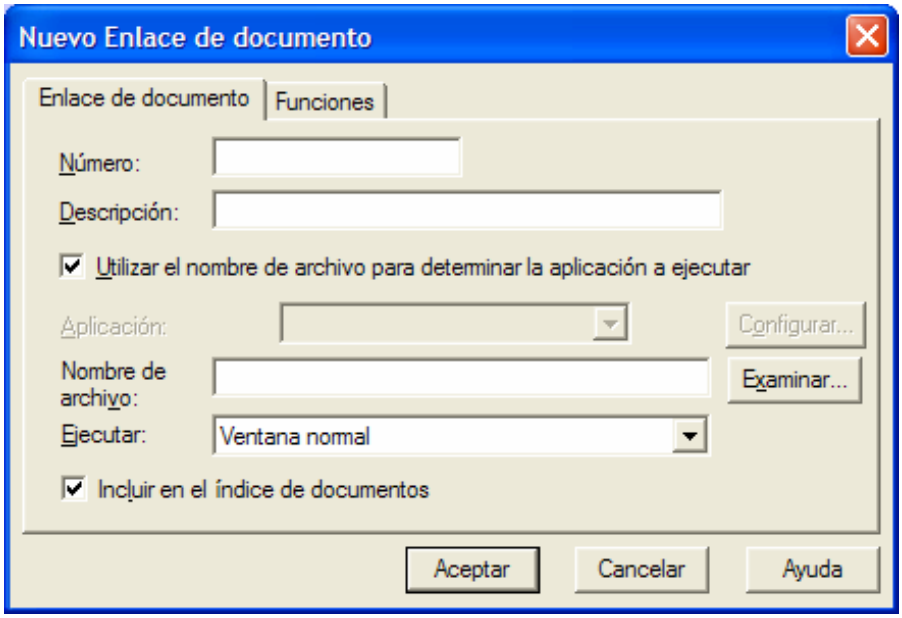


Figura 6.23. Ventana Nuevo Enlace de documento

En esta ventana, como en la anterior, es necesario ingresar un número de identificación única y una descripción, con la diferencia de que en esta ventana se especifica la ubicación del archivo.

Estas funciones le dan mucha flexibilidad al auditor para que pueda realizar de forma eficiente su trabajo. A continuación se

presenta un ejemplo de la creación de carpetas y archivos relacionados en Caseware Working Papers:

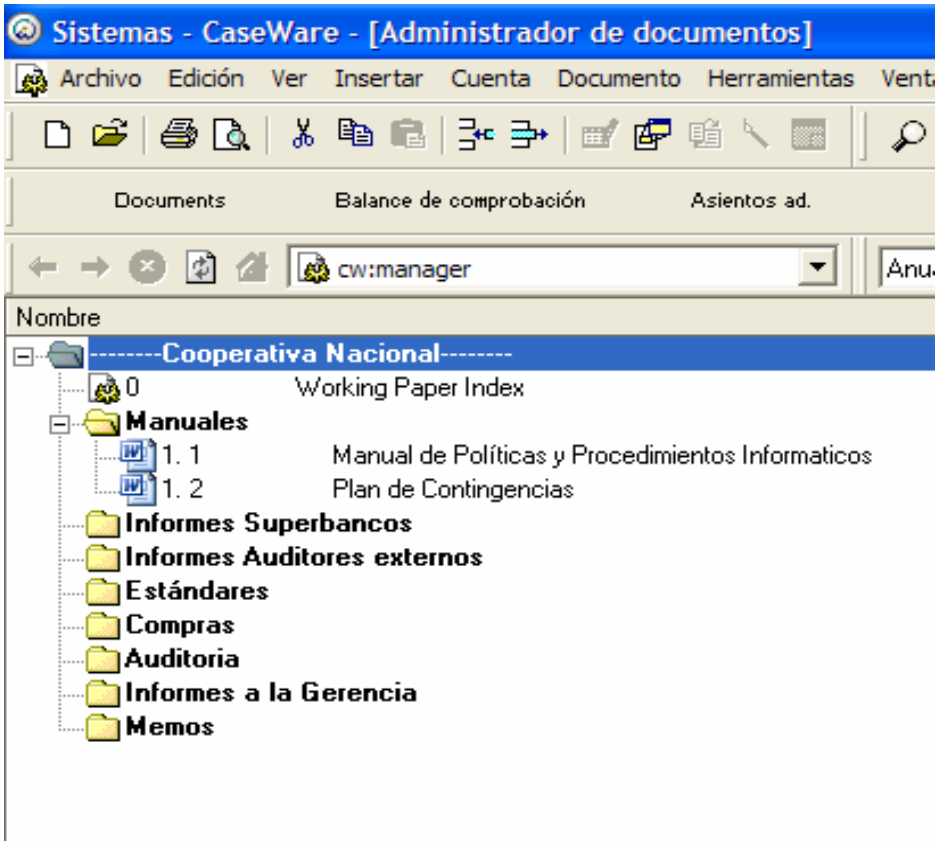


Figura 6.24. Ventana Documentos

Otra característica muy importante de este software es la variedad de reportes y visualizaciones en pantalla de los papeles de trabajo, lo que permite manejar eficientemente la entrega de informes preliminares y finales con absoluta rapidez y seguridad.

CAPÍTULO 7

Conclusiones y Recomendaciones

7.1. Conclusiones

- La tecnología de la información se ha convertido en uno de los recursos más indispensables para las organizaciones en su camino hacia la competitividad y el servicio de calidad. Esto ha originado nuevos riesgos y amenazas que en caso de no ser atendidos de manera oportuna podría dar lugar a cuantiosas pérdidas económicas.

- El Control Interno Informático en muchas organizaciones no es considerado como un aspecto crítico dentro de la gestión empresarial y pasa a ser un aspecto secundario dentro de los procesos y actividades operacionales y administrativas.

- El desarrollo de los Sistemas de Información brindan al auditor informático nuevas técnicas y herramientas que mejoran el proceso

de ejecución de la auditoría; pero que lastimosamente no ha sido aprovechado al máximo.

- El auditor moderno se enfrenta a nuevos desafíos asociados al manejo de la tecnología de información, ya que requiere que adquiera nuevos conocimientos y desarrolle nuevas habilidades respecto al manejo de las herramientas informáticas, bases de datos y software de auditoría.

- Existen en el mercado diferentes tipos de software de auditoría que mejoran considerablemente el proceso de ejecución de la auditoría, el análisis de datos y la evaluación del control interno informático y que deben ser aprovechados de forma adecuada en los trabajos de auditoría.

7.2. Recomendaciones

- Las organizaciones requieren incorporar mecanismos de control, tanto administrativos como informáticos que garanticen establecer un nivel adecuado de seguridad de la información y que garantice la salvaguarda de los recursos informáticos.

- Hoy más que nunca, el Control Interno Informático merece profunda atención por parte de gerentes, auditores y usuarios dentro de las organizaciones, ya que esta debe abarcar aspectos relacionados a la tecnología de información con el objetivo de garantizar la integridad, confiabilidad y disponibilidad de la información.

- Los Gerentes del primer nivel Jerárquico de las organizaciones, deben tomar la seria responsabilidad de establecer los lineamientos y estrategias que permitan una adecuada gestión de la Tecnología de Información que apoyen de forma significativa el logro de los objetivos de la organización y minimice los riesgos operativos a los que esté expuesta.

- Es necesario que los auditores financieros tradicionales conozcan que el enfoque de la auditoría moderna ha cambiado e incorpora

la tecnología de información dentro de sus objetivos y procedimientos, por lo que es indispensable que el auditor aproveche el uso de los sistemas de información para asegurar la eficiencia, calidad y confiabilidad de la auditoría.

- Los auditores en Control de Gestión deben desarrollar nuevas habilidades y adquirir constante entrenamiento en el uso de las Técnicas y Herramientas Informáticas, que le permitan realizar una evaluación integral de la organización a nivel operativo, financiero, administrativo e informático.

APÉNDICES

APÉNDICE 1

NORMAS GENERALES DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN

A continuación se exponen las Normas Generales de Auditoría de Sistemas de Información emitidas por ISACA y que se encuentran disponibles en su sitio Web, www.isaca.org.

Introducción

La Asociación de Auditoría y Control de Sistemas de Información ha determinado que la naturaleza especializada de la auditoría de los sistemas de información y las habilidades necesarias para llevar a cabo este tipo de auditorías, requieren el desarrollo y la promulgación de Normas Generales para la Auditoría de los Sistemas de Información. La auditoría de los sistemas de información se define como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes. Las normas promulgadas por la Asociación de Auditoría y Control de Sistemas de Información son aplicables al trabajo de auditoría realizado por miembros de la Asociación de Auditoría y Control de Sistemas de Información y por las personas que han recibido la designación de Auditor Certificado de Sistemas de Información.

Objetivos

Los objetivos de estas normas son los de informar a los auditores del nivel mínimo de rendimiento aceptable para satisfacer las responsabilidades profesionales establecidas en el Código de Ética Profesional y de informar a la gerencia y a otras partes interesadas de las expectativas de la profesión con respecto al trabajo de aquellos que la ejercen.

010 Título de Auditoría

010.010 Responsabilidad, autoridad y rendimiento de cuentas

La responsabilidad, la autoridad y el rendimiento de cuentas abarcados por la función de Auditoría de los sistemas de información se documentarán de la manera apropiada en un título de Auditoría o carta de contratación.

020 Independencia

020.010 Independencia profesional

En todas las cuestiones relacionadas con la Auditoría, el Auditor Informático deberá ser independiente de la organización auditada tanto en actitud como en apariencia.

020.020 Relación organizativa

La función de Auditoría de los sistemas de información deberá ser lo suficientemente independiente del área que se está auditando para permitir completar de manera objetiva la Auditoría.

030 Ética y normas profesionales

030.010 Código de Ética Profesional

El Auditor Informático deberá acatar el Código de Ética Profesional de la Asociación de Auditoría y Control de Sistemas de Información.

030.020 Atención profesional correspondiente

En todos los aspectos del trabajo del Auditor Informático, se deberá ejercer la atención profesional correspondiente y el cumplimiento de las normas aplicables de Auditoría profesional.

040 Idoneidad

040.010 Habilidades y conocimientos

El Auditor Informático debe ser técnicamente idóneo, y tener las habilidades y los conocimientos necesarios para realizar el trabajo como auditor.

040.020 Educación profesional contínua

El Auditor Informático deberá mantener la idoneidad técnica por medio de la educación profesional continua correspondiente.

050 Planificación

050.010 Planificación de la Auditoría

El Auditor Informático deberá planificar el trabajo de auditoría de los sistemas de información para satisfacer los objetivos de la auditoría y para cumplir con las normas aplicables de auditoría profesional.

060 Ejecución del trabajo de auditoría

060.010 Supervisión

El personal de auditoría de los sistemas de información debe recibir la supervisión apropiada para proporcionar la garantía de que se cumpla con los objetivos de la auditoría y que se satisfagan las normas aplicables de auditoría profesional.

060.020 Evidencia

Durante el transcurso de una auditoría, el Auditor Informático deberá obtener evidencia suficiente, confiable, relevante y útil para lograr de manera eficaz los objetivos de la auditoría. Los hallazgos y conclusiones de la auditoría se deberán apoyar por medio de un análisis e interpretación apropiados de dicha evidencia.

070 Informes

070.010 Contenido y formato de los informes

En el momento de completar el trabajo de auditoría, el Auditor Informático deberá proporcionar un informe, de formato apropiado, a los destinatarios en cuestión. El informe de auditoría deberá enunciar el alcance, los objetivos, el período de cobertura y la naturaleza y amplitud del trabajo de auditoría

realizado. El informe deberá identificar la organización, los destinatarios en cuestión y cualquier restricción con respecto a su circulación. El informe deberá enunciar los hallazgos, las conclusiones y las recomendaciones, y cualquier reserva o consideración que tuviera el auditor con respecto a la auditoría.

080 Actividades de seguimiento

080.010 Seguimiento

El Auditor Informático deberá solicitar y evaluar la información apropiada con respecto a hallazgos, conclusiones y recomendaciones relevantes anteriores para determinar si se han implementado las acciones apropiadas de manera oportuna.

APÉNDICE 2

CÓDIGO DE ÉTICA DE ISACA

Según el Código de Ética de ISACA los Auditores de Sistemas deberán:

a) Apoyar el establecimiento y cumplimiento apropiado de estándares, procedimientos y controles en los sistemas de información.

b) Cumplir con los Estándares de Auditoría de Sistemas de Información adoptados por la Asociación de Auditoría y Control de Sistemas de Información.

c) Dar servicio a sus empleadores, accionistas, clientes y público en general en forma diligente, leal y honesta y no formar parte de actividades impropias o ilegales.

d) Mantener la confidencialidad de la información obtenida en el curso de sus tareas. Dicha información no debe ser usada en beneficio propio ni ser entregada a terceros.

e) Realizar sus tareas en forma objetiva e independiente, y rechazar la realización de actividades que amenacen o parezcan amenazar su independencia.

f) Mantener competencia en los campos relacionados a la auditoría de sistemas de información a través de la participación en actividades de desarrollo profesional.

g) Obtener suficiente material y documentación de sus observaciones que le permita respaldar sus recomendaciones y conclusiones.

h) Informar a las partes que correspondieren los resultados del trabajo de auditoría realizado.

i) Dar apoyo a la educación y el conocimiento de clientes, gerentes y público en general sobre la auditoría de sistemas de información.

j) Mantener altos estándares de conducta y personalidad tanto en las actividades profesionales como personales.

APÉNDICE 3

NORMATIVA INFORMÁTICA EN EL ECUADOR

A. NORMAS DE CONTROL INTERNO

CÓDIGO: 133-01

MATERIA: SISTEMAS DE INFORMACIÓN COMPUTARIZADOS

TÍTULO: SISTEMAS NUEVOS O ACTUALIZACIÓN DE LOS EXISTENTES

Los sistemas de información computarizados, incluyendo equipos (hardware), programas (software) y personal, se generarán a partir de los requerimientos formalmente establecidos por los usuarios. Su ejecución partirá de un Plan Integral de Sistemas aprobado por el ejecutivo máximo y se sujetará a las disposiciones de la Dirección Nacional de Informática de la Contraloría General del Estado y de otros organismos competentes.

El Plan Integral de Sistemas contendrá como mínimo:

1. La definición de los sistemas de información automatizados que necesita la institución.

2. La priorización de los mismos

3. La base tecnológica requerida para su implementación (equipos, programas y personal)

4. El presupuesto financiero

5. El cronograma de las actividades principales a desarrollar para la ejecución del plan.

Para la incorporación de nuevos sistemas y para la actualización o crecimiento de los existentes, se utilizará tecnología probada y actual, tanto en los equipos como en los programas de soporte computacional (software de base).

El proceso de desarrollo de sistema seguirá una metodología que comprenda al menos:

1. Un análisis de factibilidad

2. Una propuesta de desarrollo

3. Un diseño conceptual y físico

4. Una prueba de aceptación luego de una etapa de trabajo en paralelo

5. Un plan de implantación que considere:

5.1 Capacitación

5. 2 Adecuación a los nuevos sistemas

5.3 Mantenimiento.

Esta metodología incorporará en todas sus fases, la participación de todos los usuarios y de la Unidad de Auditoria Interna, donde esta exista, así como instancias de aprobación y aceptación escritas por parte de los usuarios directamente involucrados y la entrega obligatoria de la documentación detallada de cada fase, del sistema en general y de su operación o del usuario.

En caso de adquisición de programas computacionales (paquetes) se preverán tanto en el proceso como en los contratos respectivos, mecanismos que aseguren el cumplimiento satisfactorio de los requerimientos del usuario, la obtención de la licencia de uso legalizada, la recepción de los programas, diseños, documentación en general y la garantía ofrecida por el proveedor.

CÓDIGO: 133-02

MATERIA: SISTEMAS DE INFORMACIÓN COMPUTARIZADOS

TÍTULO: PRODUCCIÓN, OPERACIÓN Y MANTENIMIENTO

Para los sistemas incorporados a su gestión, en cada entidad se elaborarán procedimientos formales y detallados del funcionamiento y operación, tanto a nivel de usuarios como de la unidad de sistemas de información computarizados.

Los sistemas en producción se someterán a constantes pruebas y evaluaciones para identificar inconsistencias o inconformidades respecto a su funcionamiento. Para solucionar estas deficiencias se aplicarán los procedimientos de mantenimiento de los sistemas, los mismos que serán definidos por la entidad.

El mantenimiento comprenderá tanto a los equipos como a los programas, especialmente cuando se trate de programas comerciales de constante actualización.

CÓDIGO: 133-03

MATERIA: SISTEMAS DE INFORMACIÓN COMPUTARIZADOS

TÍTULO: ACCESO A LOS SISTEMAS Y MODIFICACIÓN DE LA INFORMACIÓN

El ejecutivo máximo de cada entidad pública o por su delegación los directivos y jefes de unidades administrativas, establecerán las medidas que permitan acceder y modificar los datos e información contenidos en los sistemas computarizados sólo a personal autorizado. Estas se concretarán en controles de acceso físico y lógico.

Entre los controles de acceso físico a los puntos terminales del sistema de información computarizado se tendrán a los siguientes:

1. Mantener los puntos terminales bajo llave

2. Mantener los puntos terminales bajo supervisión directa

3. Utilizar llaves para operar los puntos terminales.

Entre los controles de acceso lógico a los sistemas y la información contenida en el computador, se utilizará:

1. Claves de acceso (palabras secretas)

2. Rangos limitados de actividades (menús restringidos)

3. Perfiles de acceso, de acuerdo a las funciones y jerarquías de los usuarios

4. Una bitácora de operación de los sistemas llevada en forma manual o computarizada, la misma que consistirá en al menos:

4.1 Un registro de utilización de cada uno de los sistemas por cada uno de los usuarios

4.2 Registro de los intentos de acceso no autorizados

4.3 Implantación de circuitos especiales que identifican al dispositivo terminal como autorizado para acceder a los sistemas.

Se entenderá por "puntos terminales" a los terminales de computación, los microcomputadores independientes y los conectados a otros equipos, ya sea en la modalidad de red o multiusuario, y todos aquellos dispositivos que permitan la intercomunicación directa del usuario con el computador.

CÓDIGO: 133-04

MATERIA: SISTEMAS DE INFORMACIÓN COMPUTARIZADOS

TÍTULO: INGRESO DE DATOS PARA PROCESAMIENTO

El ejecutivo máximo de cada entidad pública o por su delegación los directivos y jefes de las unidades administrativas serán responsables de asegurar que los sistemas tengan controles manuales o automáticos de validación de los datos a ser ingresados para procesamiento.

Una parte esencial de la validación serán los procedimientos para verificar que la información registrada en los documentos fuente sea pertinente y para identificar errores de formato, campos faltantes y el ajuste de valores dentro de límites de razonabilidad para ese proceso.

Otro aspecto importante constituirán los procedimientos que garanticen el ingreso al computador solo de datos válidos en el contexto del procesamiento al que van a ser sometidos; es decir, que sean consistentes con los archivos maestros, estén balanceados, sean íntegros, exactos, completos e ingresen una sola vez.

CÓDIGO: 133-05

MATERIA SISTEMAS DE INFORMACIÓN COMPUTARIZADOS

TÍTULO TRANSACCIONES RECHAZADAS

En sistemas computarizados que procesen transacciones, aquellas que no cumplan con las características establecidas para su ingreso al computador serán devueltas al usuario o incluidas en un archivo de transacciones en suspenso para su posterior corrección. Una vez corregidas serán sometidas a los mismos mecanismos de control establecidas para las transacciones originales.

El proceso de corrección de estas transacciones será definido de manera que se cumpla oportunamente y con eficiencia.

De acuerdo a las necesidades de información y al menos al fin de cada mes, el responsable final de la información revisará las transacciones rechazadas que se mantengan pendientes y tomará las acciones para su corrección.

Se mantendrá un registro u otro tipo d e control sobre las transacciones rechazadas y el estado en que se encuentra cada una.

Así mismo se realizarán periódicamente análisis estadísticos y de excepción de las transacciones rechazadas para detectar errores repetitivos y adoptar medidas que eviten su recurrencia.

CÓDIGO: 133-06

MATERIA: SISTEMAS DE INFORMACIÓN COMPUTARIZADOS

TÍTULO: PROCESAMIENTO Y ENTREGA DE DATOS

El ejecutivo máximo de cada entidad pública o por su delegación los ejecutivos y jefes de las unidades administrativas establecerán para los sistemas de carácter administrativo, financiero y técnico controles para asegurar que los datos procesados y la información obtenida sean consistentes, completos y correspondan al período correcto. Estos controles podrán ser manuales o automáticos y según el tipo de información procesada podrán consistir en:

1.- Totalización de valores críticos, antes y después del procesamiento.

2.- Verificación de compatibilidad de fechas y números de transacciones.

3.- Conciliación del número de movimientos y modificaciones de los datos.

4.- Balanceo de saldos o totales de conciliación.

5.- Utilización correcta de archivos para procesamiento.

6.- Verificación de que los datos trasmitidos hayan sido completos e íntegros.

7.- Consistencia en la recuperación de las transacciones, luego de una interrupción del procesamiento.

8.- Validez de los datos generados automáticamente.

9.- Generar rastros o pistas de auditoria.

La información procesada será entregada de forma oportuna y completa, a los usuarios autorizados, dejando constancia escrita de esta entrega.

CÓDIGO: 133-07

MATERIA SISTEMAS DE INFORMACIÓN COMPUTARIZADOS

TÍTULO SEGREGACIÓN DE FUNCIONES

El ejecutivo máximo de cada entidad pública definirá y aprobará la estructura organizativa y funcional de la unidad de Sistemas de Información Computarizados (SIC), separando las responsabilidades individuales de los usuarios internos y de los servidores de dicha unidad, de manera que se evite la concentración de funciones que creen riesgos de cometimiento de errores o irregularidades.

Así mismo definirá la estructura jerárquica necesaria para el adecuado funcionamiento de los sistemas de información computarizados, en lo que respecta a la dirección, supervisión y operación en la parte técnica y al enlace entre las unidades de sistemas de información computarizados y sus usuarios.

Para el adecuado funcionamiento de los sistemas de información computarizados, los usuarios generalmente asumirán la responsabilidad sobre la iniciación y aprobación de transacciones, así como sobre la idoneidad, consistencia y seguridad de los datos ingresados para procesamiento. Los servidores de la unidad de Sistemas de Información Computarizados serán responsables del procesamiento y

distribución de la información obtenida como resultado, así como de la seguridad e integridad de los datos informados.

En los casos de los sistemas que funcionen independientemente de la unidad de Sistemas de Información Computarizados, se debe compensar la falta de segregación de funciones incorporando controles por parte del usuario que podrán consistir en:

1.- Mantener registros por tipo de transacción.

2.- Obtener totales de control de datos permanentes.

3.- Conciliar los datos ingresados con la información de salida.

4.- Revisar todos los datos de entrada y salida considerados significativos.

5.- Supervisar directamente la utilización de los sistemas.

Para garantizar la confiabilidad de la operación de la unidad de Sistemas de Información Computarizados, esta mantendrá una división funcional que permita segregar la administración de la unidad, el desarrollo de sistemas, el mantenimiento del software de base, la operación del computador (incluyendo biblioteca y archivos), el control y la seguridad de los datos.

Por unidad de Sistemas de Información Computarizados se entenderá al área responsable de desarrollar, actualizar y operar los sistemas computarizados, a nivel de toda la institución o de una parte de ella.

CÓDIGO: 133-08

MATERIA: SISTEMAS DE INFORMACIÓN COMPUTARIZADOS

TÍTULO: CAMBIOS A LOS PROGRAMAS

Las modificaciones a los programas de un sistema de información computarizado que no signifiquen desarrollo de nuevos sistemas o subsistemas, pero que impliquen cambios en los resultados generados por el computador, seguirán un procedimiento que se inicie con la petición formal de los usuarios y especifique las autorizaciones internas a obtener antes de su aplicación. Dichas modificaciones quedarán adecuada y completamente documentadas.

CÓDIGO: 133-09

MATERIA: SISTEMAS DE INFORMACIÓN COMPUTARIZADOS

TÍTULO: SEGURIDAD GENERAL EN LOS CENTROS DE PROCESAMIENTO DE DATOS

Los centro de procesamientos de datos de la institución establecerán mecanismos que protejan y salvaguarden, contra pérdidas y fugas, los medios físicos (equipos y programas) y la información. Con este fin aplicarán por lo menos las siguientes medidas:

1.- Procedimientos de acceso físico restringido al centro de procesamiento de datos, biblioteca magnética, documentos, datos y documentación de los programas.

2.- Obtención periódica de respaldos y ubicación física de los más importantes en lugares resguardados, fuera de los centros de procesamiento de datos.

3.- Seguridades e instalaciones físicas adecuadas.

4.- Un plan de contingencia que prevea las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas con los equipos, con los programas o con el personal.

5.- Procedimiento de seguridad a observarse por parte del personal que trabaja en turnos por la noche o en fin de semana.

Se entenderá por centro de procesamiento de datos al área física donde se ubiquen el o los computadores que almacenan la información.

CÓDIGO: 133-10

MATERIA: SISTEMAS DE INFORMACIÓN COMPUTARIZADOS

TÍTULO: UTILIZACIÓN DE LOS EQUIPOS, PROGRAMAS E INFORMACIÓN INSTITUCIONAL

El ejecutivo máximo de cada entidad pública o por su delegación los directivos y jefes de las unidades administrativas, establecerán procedimientos para asegurar el uso eficiente, efectivo y económico de los equipos, programas de computación e información computarizada, a través de:

1.- El registro y seguimiento de la operación de los mismos.

2.- La capacitación de los funcionarios en la utilización de los equipos y programas.

3.- La evaluación periódica de los objetivos cumplidos mediante la computarización.

Los equipos y programas serán utilizados exclusivamente en las actividades propias de la institución.

La información obtenida del proceso computarizado será de uso e intercambio entre las instituciones del sector público, con excepción de aquella considerada expresamente reservada o de uso restringido. En el caso de fijarse un precio para la información a proporcionar a estas entidades, el mismo considerará únicamente los

costos de su obtención, procesamiento y transmisión que será materia del Reglamento pertinente.

CÓDIGO: 133-11

MATERIA: SISTEMAS DE INFORMACIÓN COMPUTARIZADOS

TÍTULO: APROVECHAMIENTO DE LOS RECURSOS COMPUTARIZADOS DEL SECTOR PÚBLICO

El ejecutivo máximo de la entidad pública establecerá mecanismos que aseguren eficiencia, efectividad y economía en el aprovechamiento de los recursos computarizados (equipos, programas e información) del sector público.

Estos mecanismos promoverán y viabilizarán el intercambio de información interinstitucional así como de programas de aplicación desarrollados al interior de las instituciones.

Complementariamente, la Dirección Nacional de Informática autorizará la adquisición de bienes y servicios para sistemas computarizados, tomando en cuenta la compatibilidad tanto en equipos como en programas que permita la interconexión de los sistemas y mantendrá un registro del Parque Informático del Sector Público. Esta última información será difundida periódicamente a las instituciones interesadas, a nivel nacional.

Cada entidad pública deberá mantener un registro de los equipos y programas que posee, para que puedan ser considerados en el Parque Informático del Sector Público.

El Parque Informático del Sector Público estará conformado por la suma de los equipos, programas e información computarizados (software y hardware) que posean las entidades gubernamentales.

B. LEY DE PROPIEDAD INTELECTUAL

SECCION II

OBJETO DEL DERECHO DE AUTOR

Art. 8.- La protección del derecho de autor recae sobre todas las obras del ingenio, en el ámbito literario o artístico, cualquiera que sea su género, forma de expresión, mérito o finalidad. Los derechos reconocidos por el presente Título son independientes de la propiedad del objeto material en el cual está incorporada la obra y su goce o ejercicio no están supeditados al requisito del registro o al cumplimiento de cualquier otra formalidad.

Las obras protegidas comprenden, entre otras, las siguientes:

…

k) Programas de ordenador; y,

…

SECCION V

DISPOSICIONES ESPECIALES SOBRE CIERTAS OBRAS

PARAGRAFO PRIMERO

DE LOS PROGRAMAS DE ORDENADOR

Art. 28.- Los programas de ordenador se consideran obras literarias y se protegen como tales. Dicha protección se otorga independientemente de que hayan sido incorporados en un ordenador y cualquiera sea la forma en que estén expresados, ya sea en forma legible por el hombre (código fuente) o en forma legible por máquina (código objeto), ya sean programas operativos y programas aplicativos,

incluyendo diagramas de flujo, planos, manuales de uso, y en general, aquellos elementos que conformen la estructura, secuencia y organización del programa.

Art. 29.- Es titular de un programa de ordenador, el productor, esto es la persona natural o jurídica que toma la iniciativa y responsabilidad de la realización de la obra. Se considerará titular, salvo prueba en contrario, a la persona cuyo nombre conste en la obra o sus copias de la forma usual.

Dicho titular está además legitimado para ejercer en nombre propio los derechos morales sobre la obra, incluyendo la facultad para decidir sobre su divulgación.

El productor tendrá el derecho exclusivo de realizar, autorizar o prohibir la realización de modificaciones o versiones sucesivas del programa, y de programas derivados del mismo.

Las disposiciones del presente artículo podrán ser modificadas mediante acuerdo entre los autores y el productor.

Art. 30.- La adquisición de un ejemplar de un programa de ordenador que haya circulado lícitamente, autoriza a su propietario a realizar exclusivamente:

a) Una copia de la versión del programa legible por máquina (código objeto) con fines de seguridad o resguardo;
b) Fijar el programa en la memoria interna del aparato, ya sea que dicha fijación desaparezca o no al apagarlo, con el único fin y en la medida necesaria para utilizar el programa; y,
c) Salvo prohibición expresa, adaptar el programa para su exclusivo uso personal, siempre que se limite al uso normal previsto en la licencia. El adquirente no podrá transferir a ningún título el soporte que contenga el programa así adaptado, ni podrá

utilizarlo de ninguna otra forma sin autorización expresa, según las reglas generales.

Se requerirá de autorización del titular de los derechos para cualquier otra utilización, inclusive la reproducción para fines de uso personal o el aprovechamiento del programa por varias personas, a través de redes u otros sistemas análogos, conocidos o por conocerse.

Art. 31.- No se considerará que existe arrendamiento de un programa de ordenador cuando éste no sea el objeto esencial de dicho contrato. Se considerará que el programa es el objeto esencial cuando la funcionalidad del objeto materia del contrato, dependa directamente del programa de ordenador suministrado con dicho objeto; como cuando se arrienda un ordenador con programas de ordenador instalados previamente.

Art. 32.- Las excepciones al derecho de autor establecidas en los artículos 30 y 31 son las únicas aplicaciones respecto a los programas de ordenador.

Las normas contenidas en el presente Párrafo se interpretarán de manera que su aplicación no perjudique la normal explotación de la obra o los intereses legítimos del titular de los derechos.

APÉNDICE 4

SISAS Nº 9

USO DE TÉCNICAS DE AUDITORÍA ASISTIDAS POR COMPUTADOR (CAAT's)

1.1. Relación con los Estándares

La norma 060.020 (evidencia) establece que “durante el curso de una auditoría, el auditor de sistemas de información debe obtener evidencia suficiente, confiable, relevante y útil para lograr los objetivos de la auditoría efectivamente. Los resultados y conclusiones de la auditoría deben estar apoyados por un apropiado análisis e interpretación de esta evidencia”.

La norma 050.010 (planificación de auditoría) establece que el auditor de sistemas de información debe proponer los sistemas de información para el trabajo de auditoría para dirigir los objetivos de ésta y cumplir con las normas profesionales de auditoría.

La norma 030.020 (Cuidado profesional adecuado) establece que “El cuidado profesional adecuado y la observación de las normas de auditorías deben ser utilizadas en todos los aspectos de los trabajos del auditor de sistemas de información.

1.2. Necesidad de esta Guía

Las técnicas de auditoría asistidas por computador son de suma importancia para el auditor SI cuando realiza una auditoría. CAAT´s incluyen distintos tipos de herramientas y de técnicas, las que más se utilizan son los software de auditoría generalizado, software utilitario, los datos de prueba y sistemas expertos de auditoría. CAAT´s se pueden utilizar para realizar varios procedimientos de auditoría incluyendo: Prueba de los detalles de operaciones y saldos Procedimientos de revisión analíticos, Pruebas de cumplimiento de los controles generales de sistemas de información, Pruebas de cumplimiento de los controles de aplicación. CAAT´s pueden generar una gran parte de la evidencia de la auditoría que provienen de las auditorías de sistemas de información y como consecuencia el auditor de sistemas de información debe planificar cuidadosamente y mostrar el cuidado profesional debido cuando se utiliza los CAAT. Esta guía muestra como el auditor de sistemas de información debe cumplir con las normas mencionadas. El ajustarse a esta guía no es obligatorio, pero el auditor de sistema de información debe esta preparado para justificar cualquier incumplimiento a ésta.

2. Planificación

2.1. Los factores a tomar en cuenta cuando se toma la decisión de utilizar CAAT

Cuando se planifica la auditoría, el auditor de sistemas de información debe considerar una combinación apropiada de las técnicas manuales y las técnicas de auditoría asistidas por computador. Cuando se determina utilizar CAAT los factores a considerar son los siguientes:

- Conocimientos computacionales, pericia y experiencia del auditor de sistemas de información. Disponibilidad de los CAAT y de los sistemas de información.
- Eficiencia y efectividad de utilizar los CAAT en lugar de las técnicas manuales.
- Restricciones de tiempo.
- Pasos para la planificación de los CAAT.

Los pasos más importantes que el auditor de sistemas de información debe considerar cuando prepara la aplicación de los CAAT's seleccionados son los siguientes: Establecer los objetivos de auditoría de los CAAT Determinar accesibilidad y disponibilidad de los sistemas de información, los programas/sistemas y datos de la organización. Definir los procedimientos a seguir (por ejemplo: una muestra estadística, recálculo,

confirmación, etc.). Definir los requerimientos de output. Determinar los requerimientos de recursos Documentar los costos y los beneficios esperados Obtener acceso a las facilidades de los sistemas de información de la organización, sus programas/sistemas y sus datos. Documentar los CAAT's a utilizar incluyendo los objetivos, flujogramas de alto nivel y las instrucciones a ejecutar. Acuerdo con el cliente (auditado) Los archivos de datos, tanto como los archivos de operación detallados (transaccionales, por ejemplo), a menudo son guardados sólo por un período corto, por lo tanto, el auditor de sistemas de información debe arreglar que estos archivos sean guardados por el marco de tiempo de la auditoría. Organizar el acceso a los sistemas de información de la organización, programas/sistemas y datos con anticipación para minimizar el efecto en el ambiente productivo de la organización.

El auditor de sistemas de información debe evaluar el efecto que los cambios a los programas/sistemas de producción puedan tener en el uso de los CAAT. Cuando el auditor de sistemas de información lo hace, debe considerar el efecto de estos cambios en la integridad y utilidad de los CAAT's, tanto como la integridad de los programas/sistemas y los datos utilizados por el auditor de sistemas de información. Probando los CAAT's El auditor de sistemas de información debe obtener una garantía razonable de la integridad, confiabilidad, utilidad y seguridad de los CAAT's por

medio de una planificación, diseño, prueba, procesamiento y revisión adecuados de la documentación. Esto debe ser hecho antes de depender de los CAAT's. La naturaleza, el tiempo y extensión de las pruebas depende de la disponibilidad y la estabilidad de los CAAT's.

La seguridad de los datos y de los CAAT's Los CAAT's pueden ser utilizados para extraer información de programas/sistemas y datos de producción confidenciales. El auditor de sistemas de información debe salvaguardar la información de los programas/sistemas y los datos de producción con un nivel apropiado de confidencialidad y seguridad. Al hacerlo el auditor debe considerar el nivel de confidencialidad y seguridad que exige la organización a la cual pertenecen los datos. El auditor de sistemas de información debe utilizar y documentar los resultados de los procedimientos aplicados para asegurar la integridad, confiabilidad, utilidad y seguridad permanentes de los CAAT's. Por ejemplo, debe incluir una revisión del mantenimiento de los programas y controles de los cambios de programa de auditoría para determinar que sólo se hacen los cambios autorizados al CAAT.

Cuando los CAAT están en un ambiente que no está bajo el control del auditor de sistemas de información. Un nivel de control apropiado debe ser implementado para identificar los cambios a los CAAT. Cuando se hacen

cambios a los CAAT el auditor de sistemas de información debe asegurarse de su integridad, confiabilidad, utilidad y seguridad por medio de una planificación, diseño, prueba, procesamiento y revisión apropiados de la documentación, antes de confiar en ellos.

3. Realización de la auditoría

3.1. Recolectar evidencia de la auditoría

El uso de los CAAT debe ser controlado por el auditor de sistemas de información para asegurar razonablemente que se cumple con los objetivos de la auditoría y las especificaciones detalladas de los CAAT's. El auditor debe: Realizar una conciliación de los totales de control; Realizar una revisión independiente de la lógica de los CAAT Realizar una revisión de los controles generales de los sistemas de información de la organización que puedan contribuir a la integridad de los CAAT (por ejemplo: controles de los cambios en los programas y el acceso a los archivos de sistema, programa y/o datos).

3.2. El software de auditoría generalizado

Cuando el auditor de sistema de información utiliza el software de auditoría generalizado para acceder a los datos de producción, se debe tomar las medidas apropiadas para proteger la integridad de los datos de la

organización. Además, el auditor de sistemas de información tendrá que estar involucrado en el diseño del sistema y las técnicas que se utilizaron para el desarrollo y mantenimiento de los programas/sistemas de aplicación de la organización.

3.3. Software utilitario

Cuando el auditor de sistemas de información utiliza el software utilitario debe confirmar que no tuvieron lugar ninguna intervención no planificada durante el procesamiento y que éste software ha sido obtenido desde la biblioteca de sistema apropiado, mediante una revisión del Log de la consola del sistema o de la información de contabilidad del sistema. El auditor de sistemas de información también debe tomar las medidas apropiadas para proteger la integridad del sistema y programas de la organización, puesto que estos utilitarios podrían fácilmente dañar el sistema y sus archivos.

3.4. Datos de prueba

Cuando el auditor de sistemas de información utiliza los datos de prueba debe estar consiente de que pueden existir ciertos puntos potenciales de errores en el procesamiento; dado que ésta técnica no evalúa los datos de producción en su ambiente real. El auditor de sistemas de información también debe estar consiente de que el análisis de los datos de prueba

pueden resultar extremadamente complejos y extensos, dependiendo de el número de operaciones procesadas, el número de programas sujetos a pruebas y la complejidad de los programas/sistemas.

3.5. Localización y maping del software de aplicación

Cuando el auditor de sistemas de información utiliza el software de aplicación para sus pruebas CAT, debe confirmar que el programa fuente que está evaluando es lo mismo que se utiliza actualmente en producción. El auditor de sistemas de información debe estar consiente de que el software de aplicación sólo indica el potencial de un proceso erróneo, no evalúa los datos de producción en su ambiente real. Los sistemas de auditoría especializados Cuando el auditor de sistemas de información utiliza los sistemas de auditoría especializados debe conocer profundamente las operaciones del sistema par confirmar que las sendas de decisión seguidas son apropiadas para el ambiente/situación de auditoría.

4. La documentación de los CAAT’s Papeles de trabajo

Una descripción del trabajo realizado, seguimiento y las conclusiones acerca de los resultados de los CAAT’s deben estar registrados en los papeles de trabajo de la auditoría. Las conclusiones acerca del funcionamiento del sistema de información y de la confiabilidad de los

datos deben estar registradas en los papeles de trabajo de la auditoría. El proceso paso a paso de los CAAT debe estar documentado adecuadamente para permitir que el proceso se mantenga y se repita por otro auditor de sistemas de información. Específicamente los papeles de trabajo deben contener la documentación suficiente para describir la aplicación de los CAAT incluyendo los detalles que se mencionan en los párrafos siguientes.

Planificación La documentación debe incluir lo siguiente:

- Los objetivos de los CAAT Los CAAT a utilizar
- Los controles a implementar
- El personal involucrado, el tiempo que tomará y los costos.

Ejecución. La documentación debe incluir:

- Los procedimientos de la preparación y la prueba de los CAAT y los controles relacionados.
- Los detalles de las pruebas realizadas por los CAAT.
- Los detalles de los input (ejemplo: los datos utilizados, esquema de archivos), el procesamiento (ejemplo: los flujogramas de alto nivel de los CAAT, la lógica) y los outputs (ejemplo: archivos Log, reportes).

Evidencia de auditoría. La documentación debe incluir lo siguiente:

- El output producido.

- Una descripción del trabajo de análisis de auditoría que se realizó para el output.

Resultado de la auditoría, Conclusiones de la auditoría y Otros. La documentación debe incluir lo siguiente: Las recomendaciones de la auditoría

5. Informe/Reporte Descripción de los CAAT

La sección del informe donde se tratan los objetivos, la extensión y metodología debe incluir una clara descripción de los CAAT utilizados. Esta descripción no debe ser muy detallada, pero debe proporcionar una buena visión general al lector. La descripción de los CAAT utilizados también debe ser incluida en el informe donde se discute el hallazgo específico relacionado con el uso de los CAAT. Si se puede aplicar la descripción de los CAAT a varios hallazgos o si es demasiado detallado debe ser descrito brevemente en la sección del informe donde se tratan los objetivos, extensión y metodología y una referencia anexa para el lector, con una descripción más detallada.

6. Fecha efectiva

6.1. Esta pauta es efectiva para todos los auditores de los sistemas de información que comiencen durante o después (de la fecha de emisión).

BIBLIOGRAFÍA

1. Sistemas de Información Gerencial – Autores: Kenneth C. Laudon Jane P. Laudon, Editorial: Prentice Hall, Sexta Edición, 2002
2. Auditoria Informática – Autor: José Antonio Echenique, Editorial: McGraw-Hill, 2nd edición Octubre 2001
3. Auditoria Informática: Un enfoque práctico – Autor: Mario Piattini, Editorial: Alfa Omega , Agosto 2001
4. COBIT 2da Edición – ISACA, 2002
5. Enciclopedia de la Auditoria – Grupo Océano, Febrero 1999
6. Normas Ecuatorianas de Auditoría (NEA) – Federación Nacional de Contadores Públicos, Editorial: PUDELECO Editores S.A., Primera Edición, 2000.
7. Principios de Auditoría – Walter B. Meigs, Editorial Diana, Primera Edición, Mayo de 1977.
8. Auditoría Informática, Aplicaciones en Producción – José Dagoberto Pinilla, ECOE Ediciones, Primera Edición, 1997.
9. Declaraciones sobre Normas de Auditoría – AICPA, Quinta reimpresión 1978.
10. Piratas Cibernéticos, Cyberwars, Seguridad Informática e Internet – Jesús de Marcel Rodao, Editorial: Alfa Omega, 2002.