

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE CONTADURÍA PÚBLICA



“GUÍA PRACTICA PARA LA EVALUACIÓN DEL CONTROL
INTERNO EN LA AUDITORIA EN INFORMATICA

MARÍA ESTELA CISNEROS MANZANO
MARLENE ELIZABETH BELTRÁN GUTIÉRREZ
MARITZA ELIZABETH ARGUETA ARANO

PARA OPTAR AL GRADO DE:

LICENCIADO EN CONTADURÍA PÚBLICA

CIUDAD UNIVERSITARIA, SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA
JUNIO 2002

UNIVERSIDAD DE EL SALVADOR
AUTORIDADES UNIVERSITARIAS

Rectora : Dra. María Isabel Rodríguez

Secretaria General : Licda. Lidia Margarita Muñoz Vela

Decano de la Facultad de
Ciencias Económicas: : MSc Roberto Enrique Mena

Secretario de la Facultad
de Ciencias Económicas : Lic. José Wilfredo Zelaya Franco

Asesor : Licda. Glendy Ruth García de Araniva

Tribunal Examinador : Lic. Ricardo Alberto Jiménez
: Lic. Carlos Henríquez Ruano
: Licda. Glendy Ruth García de Araniva

Junio de 2002

San Salvador,

El Salvador,

Centro América

DEDICATORIA

A DIOS TODO PODEROSO: a quien sea toda la Gloria, el Poder y la Honra, ya que me dio la sabiduría, paciencia y perseverancia para terminar con éxito mi carrera

A MIS PADRES: que me brindaron y haber entregado incondicionalmente, todo su sacrificio hasta ver culminados sus sueños que son los míos propios;

A MIS HERMANOS: porque ellos han sido muy importantes en todo momento y siempre me invitaron a seguir adelante con mis esfuerzos de superación y me prepararon el camino;

COMPAÑEROS, Y AMIGOS: que siempre me apoyaron lo cual contribuyó a sentirme confiado y seguro de culminar lo que había comenzado;

FAMILIARES: que siempre confiaron en mí, que iba a lograr coronar mi carrera profesional.

María Estela

Marlene Elizabeth

Maritza Elizabeth

INDICE

RESUMEN

INTRODUCCIÓN

1. MARCO TEORICO CONCEPTUAL O DE REFERENCIA	1
1.1. UN POCO DE HISTORIA Y UN POCO DE ACTUALIDAD	1
1.2. AUDITORIA.	2
1.2.1 NATURALEZA Y PROPÓSITOS DE LA AUDITORÍA.	3
1.2.2 INFORMÁTICA	3
1.2.3 LA AUDITORIA DEL SISTEMA INFORMÁTICO	3
1.3. CONTROL INTERNO	5
1.3.1 CONTROL INTERNO ADMINISTRATIVO	8
1.3.2 CONTROL INTERNO FINANCIERO	8
1.3.3 CONTROL INTERNO EN AMBIENTE COMPUTARIZADO	8
1.3.4 LOS TRES ELEMENTOS DE LA ESTRUCTURA DE CONTROL	10
1.3.5 CARACTERÍSTICAS ESPECÍFICAS DE LOS SISTEMAS COMPUTARIZADOS	12
1.3.6 CONTROL INTERNO E INFORMÁTICA	14
1.4. EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO	18
1.4.1 EVALUACIÓN PRELIMINAR DEL RIESGO	19
1.4.2 EVALUACIÓN DEL RIESGO Y CONTROL INTERNO EN LA AUDITORÍA DE SISTEMAS COMPUTARIZADOS	20
1.5. RIESGOS DE AUDITARÍA	21
1.5.1 RIESGOS INHERENTES	22
1.5.2 RIESGO DE CONTROL	22
1.5.3 RIESGO DE DETECCIÓN	22
1.5.4 EVALUACIÓN DEL RIESGO INHERENTE Y DE CONTROL	22
1.5.5 RIESGO.	22

1.6.	CUESTIONARIOS DE CONTROL INTERNO COMO MÉTODO DE EVALUACIÓN	24
1.6.1	DEFINICIÓN	24
1.6.2	CUESTIONARIOS PARA AUDITORÍA EN INFORMÁTICA	25
1.6.3	VENTAJAS DE LOS CUESTIONARIOS	25
1.7.	AUDITORIA DE INFORMATICA Y SISTEMAS CON COMPUTADOR	25
1.7.1	ORGANIZACIÓN DEL DEPARTAMENTO PED.	26
1.7.2	PROCEDIMIENTOS DE DOCUMENTACIÓN DENTRO DEL DEPARTAMENTO DE PED.	29
1.7.3	DOCUMENTACIÓN DE SISTEMAS	29
1.7.4	DOCUMENTACIÓN DE PROGRAMAS	29
1.7.5	CONTROLES DE ACCESO Y OTRAS MEDIDAS DE SEGURIDAD	30
1.7.6	CONTROLES DE APLICACIÓN	31
1.7.7	CONTROLES DE ENTRADA	31
1.7.8	CONTROLES DE PROCESAMIENTO	32
1.7.9	CONTROLES DE SALIDA	32
1.7.10	PRUEBAS DE CUMPLIMIENTO	33
1.8.	TÉCNICAS DE AUDITORÍA EN SISTEMAS COMPUTARIZADOS	33
1.8.1	PROCEDIMIENTOS MANUALES	34
1.8.2	TÉCNICAS DE AUDITORÍA APOYADAS POR COMPUTADORAS	34
1.8.3	USO DE LA INFORMACIÓN DE PRUEBA	35
1.8.4	USO DE PROGRAMAS GENERALIZADOS DE AUDITARÍA	35
1.9.	AUDITORIA EN UN AMBIENTE DE SISTEMAS DE INFORMACIÓN POR COMPUTADORA. (NIAS)	36
1.9.1	INTRODUCCIÓN	36
1.9.2	HABILIDAD Y COMPETENCIA	38
1.9.2	PLANEACIÓN	37
1.9.3	EVALUACIÓN DEL RIESGO.	41
1.9.4	PROCEDIMIENTOS DE AUDITORIA	42
1.10.	AUDITORIA EN INFORMÁTICA	43
1.10.1	CAMPO DE ACCIÓN	43
1.10.2	EVALUACIÓN ADMINISTRATIVA DEL DEPARTAMENTO DE INFORMÁTICA	44
1.10.3	EVALUACIÓN DE LOS SISTEMAS, PROCEDIMIENTOS Y EFICIENCIA DE LA INFORMACIÓN	45
1.10.4	EVALUACIÓN DEL PROCESO DE DATOS Y DE LOS EQUIPOS DE CÓMPUTO.	45
1.10.5	LA IMPORTANCIA DE LA AUDITORÍA EN INFORMÁTICA.	45

1.10.6	ELEMENTOS DE AUDITORÍA EN INFORMÁTICA	53
1.10.7	PROCESO DE UNA AUDITORIA EN INFORMÁTICA	53
1.10.8	OBJETIVOS DE LOS PROCEDIMIENTOS DE LA AUDITORIA EN INFORMÁTICA	54
1.11.	PROCEDIMIENTOS DE EVALUACIÓN DE AUDITORIA EN INFORMÁTICA	55
1.11.1	PRIMERA FASE – ESTUDIO PRELIMINAR	55
1.11.2	SEGUNDA FASE – AMPLIACIÓN DEL ESTUDIO DEL CONTROL INTERNO.	55
1.11.3	TERCERA FASE - PRUEBAS A LOS CONTROLES PED	59
1.11.4	TERCERA FASE ALTERNA - PRUEBAS A LOS CONTROLES PED PARA INCREMENTAR LA EFICIENCIA EN LOS RESULTADOS DE AUDITORIA	60

CAPITULO II

2.	METODOLOGIA DE LA INVESTIGACIÓN	61
2.1	OBJETIVOS DE LA INVESTIGACIÓN	61
2.1.1.	GENERAL.	61
2.1.2.	ESPECÍFICOS.	61
2.2.	DEFINICIÓN DEL TIPO DE ESTUDIO	62
2.2.1.	UNIDADES DE ANÁLISIS	62
2.3.	POBLACIÓN Y MUESTRA	62
2.3.1.	POBLACIÓN	62
2.3.2.	MUESTRA	63
2.4.	MÉTODOS E INSTRUMENTOS PARA RECOLECCIÓN DE DATOS.	64
2.4.1.	INVESTIGACIÓN BIBLIOGRÁFICA	64
2.4.2.	INVESTIGACIÓN DE CAMPO	64
2.5.	TABULACION DE DATOS	65
2.5.1.	INTERPRETACIÓN DE LOS RESULTADOS	65
2.6.	RESULTADOS DE LA INVESTIGACION	65
2.6.1.	ANALISIS E INTERPRETACION DE LA INVESTIGACION DE CAMPO	65
2.7.	DIAGNÓSTICO	82

CAPITULO III

3.	GUÍA PRÁCTICA PARA LA EVALUACIÓN DEL CONTROL INTERNO EN LA AUDITORÍA EN INFORMÁTICA.	85
3.1	TERMINOS DE CONTRATACIÓN	85
3.2	EVALUACIÓN DEL CONTROL INTERNO	88

3.3	FASES DE UNA AUDITORIA EN INFORMÁTICA	89
3.4	OBJETIVOS Y PROCEDIMIENTOS POR FASE DE AUDITARÍA	90
3.4.1	PROCEDIMIENTOS RECOMENDADOS	91
3.4.2	SEGUNDA FASE AMPLIACIÓN DEL ESTUDIO DEL CONTROL INTERNO	92
3.5	SECUENCIA DE LA AUDITORÍA EN INFORMÁTICA	98
3.5.1	PLANEACIÓN DE LA EVALUACIÓN DEL CONTROL INTERNO EN INFORMÁTICA.	99
3.5.2	ENTREVISTA CON EL PERSONAL DE INFORMÁTICA	101
3.6	NARRATIVAS	101
3.6.1	ÁREA DE SEGURIDAD FÍSICA	102
3.6.2	ÁREA DE CONTROLES Y PROCEDIMIENTOS	103
3.6.3	ÁREA DE SISTEMA DE COMPUTO	105
3.6.4	ÁREA RESGUARDO Y RECUPERACIÓN	106
3.7	CUESTIONARIOS DE CONTROL INTERNO	107
3.7.1	CUESTIONARIOS DE EVALUACIÓN DE LA PLANIFICACIÓN	107
3.7.2	CUESTIONARIOS DE EVALUACIÓN DE LA ORGANIZACIÓN Y ADMINISTRACIÓN	111
3.7.3	CUESTIONARIOS DE EVALUACIÓN DEL ENTORNO OPERATIVO DE HARDWARE	116
3.7.4	CUESTIONARIOS DE EVALUACIÓN DE LA CONSTRUCCIÓN DE SISTEMAS	120
3.5.6	CUESTIONARIOS DE EVALUACIÓN DEL ENTORNO OPERATIVO DE SOFTWARE	123
3.5.7	EVALUACIÓN DEL RIESGO	126
3.6	EVALUACIÓN DE LOS PUNTOS DE CONTROL DE INFORMÁTICA	127
3.7	USO DE FLUJOGRAMAS	131
3.7.1	EVALUACIÓN DEL RIESGO DE LOS PUNTOS DE CONTROL DE INFORMÁTICA.	139
3.8	INFORME DE CONTROL INTERNO	140

CAPITULO IV

4.	CONCLUSIONES Y RECOMENDACIONES	144
4.1.	CONCLUSIONES	145

RESUMEN

El incremento permanente de las expectativas y necesidades relacionada con la informática, al igual que la actualización continua de los elementos que componen la tecnología de este campo, obliga a las entidades que la aplican a contar con controles, políticas y procedimientos que aseguren a la alta dirección que los recursos humanos, materiales y financieros involucrados, son protegidos adecuadamente y que se orienten a la rentabilidad y competitividad del negocio.

La tecnología de informática, traducida en hardware, software, sistemas de información, investigación tecnológica, redes locales, bases de datos, ingeniería de software, telecomunicaciones, servicios y organización de informática es una herramienta estratégica que brinda rentabilidad y ventaja competitiva a los negocios frente a sus similares en el mercado; pero puede originar costos y desventajas competitivas si no es bien administrada y dirigida por el personal encargado.

El desarrollo acelerado de la tecnología de computación y la significativa expansión del uso de computadoras para realizar tareas contables, han aumentado considerablemente la necesidad que tenemos de conocer con detalle los diversos sistemas de computación comúnmente en uso y los correspondientes procedimientos de control.

Lo que resulta innegable es que la informática se convierte cada día en una herramienta permanente de los procesos principales de los negocios, en una fuerza estratégica, un aliado confiable y oportuno. Todo lo anterior es posible tenerlo en la empresa si se implantan controles y esquemas de seguridad requeridos para su aprovechamiento óptimo.

Los contadores públicos en nuestro medio carecen de una guía práctica para la evaluación del control interno en informática que conlleve al desarrollo de la auditoría en forma eficiente, oportuna y profesional.

La respuesta siempre ha existido: mediante evaluaciones oportunas y completas de dicha función por personal calificado (o sea, consultores externos, auditores en informática), o evaluaciones periódicas por el mismo personal de informática entre otras estrategias.

El objetivo principal de la guía práctica para la evaluación del control interno en la auditoría en informática es el de brindar al auditor una idea de los aspectos de control que podrá encontrar en los diversos sistemas electrónicos de procesamiento de datos actualmente en uso.

El trabajo está orientado a proporcionar una metodología específica para que sirva de guía al profesional de la contaduría pública en el desarrollo y diseño de la evaluación del control interno para auditoría de informática, así como para la captación de información en forma lógica, ordenada y comprensible para facilitar su uso posterior al Recomendar políticas y procedimientos que aseguren la calidad y eficiencia en cada una de las funciones de informática, así como los productos y servicios de esta área.

INTRODUCCION

Habiendo efectuado una investigación previa con los contadores públicos y despachos de auditoría que prestan servicios de Auditoría en Informática, se detectó la inexistencia de una guía para realizar la evaluación del control interno de la Auditoría en Informática, además, deficiencias en los métodos de evaluación por el personal técnico del despacho o el contador público, por lo anterior surge la necesidad de crear un documento el cual conste de lineamientos para la evaluación del control interno en forma sistemática y técnica que cumpla con los requisitos normativos.

El presente trabajo está orientado a desarrollar una guía para la evaluación del control interno para auditoría en informática, la cual será una herramienta para el contador público. Este profesional se orienta a que se un punto de control y confianza para la alta dirección, además de que busque ser un facilitador de soluciones.

Se considera un trabajo novedoso por ser un área poco tratada en el ámbito nacional hasta la fecha: La evaluación del control interno en la auditoría en informática, es tan importante como determinar los puntos débiles en el sistema y, por tanto, se ha de tener en cuenta en el alcance y extensión de los procedimientos que se van a aplicar en la auditoría.

Debido a que la alta dirección debe contar siempre con la certidumbre respecto de la integridad y disponibilidad de la información y los recursos de informática, es necesario formalizar un proceso de auditoría en informática en la organización. La orientación de dicha función es clara: eliminar o al menos minimizar en lo posible los riesgos y circunstancias dañinos a los elementos mencionados:

Evaluación de la Seguridad Física: conocer si la empresa cuenta con la seguridad física necesaria para el resguardo del equipo de cómputo y su entorno; conocer los controles existentes sobre la seguridad física del hardware, transmisión de datos, accesos físicos y seguridad en casos de emergencia.

Evaluación de Controles y Procedimientos: conocer la efectividad y eficacia de los controles y procedimientos aplicados para el resguardo del software y hardware; Conocer los controles establecidos sobre el uso de programas y software, copia de respaldo, adquisición de paquetes y base de datos.

Evaluación de respaldo y recuperación: conocer si los tipos de respaldo de la información aplicados por la empresa son efectivos, permitiendo en un momento determinado la recuperación de la información.

Evaluación del sistema de cómputo: conocer si el sistema contable cuenta con las características necesarias requeridas por la empresa en el procesamiento de datos

Evaluación de Recursos Humanos: conocer la capacidad y eficiencia del personal del área, así como saber las necesidades existentes.

En el desarrollo del trabajo se describe como realizar una evaluación del control interno al departamento de informática utilizando los cuestionarios de control interno como método de evaluación; logrando la finalidad de obtener una base para formular sugerencias constructivas a las empresas con respecto al mejoramiento de su sistema de control interno.

Capítulo I El marco teórico contiene generalidades sobre la Auditoría en Informática que constituyen la base teórica del trabajo de investigación desarrollado y los conceptos concernientes al tema en estudio, los cuales serán aplicados en la ejecución y forman parte en el trabajo final; contiene la parte teórica referente a las bases para la Evaluación del Control Interno y su alcance; además, contiene la Evaluación del riesgo de auditoría en sus diferentes presentaciones y el uso de cuestionarios de evaluación de control interno y sus funciones; consecuentemente se incluyen conceptos que proporcionan las herramientas y lineamientos técnicos básicos para desarrollar la evaluación del control interno en informática; con la diversidad de conceptos incluidos en este capítulo el contador publico estará capacitado para abordar la parte operativa de informática, así

como la administración de la misma sin importar su complejidad y la diversificación de servicios que presta a la empresa.

Capítulo II Presenta un panorama detallado de la metodología utilizada durante la investigación. Se determinan los objetivos en donde se define el área de estudio y los resultados que se espera obtener, así como la puntualización de propósitos específicos considerados ejes problemáticos que en el desarrollo del trabajo tendrán la solución pertinente. La metodología de la investigación define las técnicas, métodos e instrumentos que se han de utilizar en la recolección de información necesaria para sustentar el trabajo.

En el capítulo III se presenta el desarrollo de un caso práctico que detalla los lineamientos técnicos básicos para desarrollar la Evaluación del Control Interno en Informática y la evaluación del riesgo de auditoría, incluyendo el uso de formatos específicos para este fin. Al terminar el trabajo se obtendrá la evaluación del control interno, desarrollada en todas sus fases, su Planeación y administración. En el plan estratégico se plasmará la información que se considere necesaria para el desarrollo de todas las fases de la Evaluación del control con enfoque de auditoría en informática y contable, lo que conlleva a la selección adecuada del personal que ejecutará la auditoría, los procedimientos y técnicas para la elaboración de los cuestionarios de control interno, así como el informe sobre control interno.

Capítulo IV se plantea las principales conclusiones y recomendaciones que, según criterio del grupo de trabajo, merecen destacarse y que su puesta en práctica posibilitaría a los contadores públicos y despachos de auditoría, superar en alguna medida las deficiencias y limitantes detectadas en la etapa de investigación.

CAPITULO I

1. MARCO TEORICO CONCEPTUAL O DE REFERENCIA

1.1. RESEÑA HISTÓRICA

En los años cuarenta empezaron a darse resultados relevantes en el campo de la computación, con sistemas de apoyo para estrategias militares; posteriormente se incrementó el uso de las computadoras y sus aplicaciones y se diversificó el apoyo a otros sectores de la sociedad: educación, salud, industria, política, banca, aeronáutica, comercio, etc.

En aquellos años la seguridad y control de ese medio se limitaba a dar custodia física a los equipos y a permitir el uso de los mismos a personal altamente calificado (no había gran número de usuarios, ya fueran técnicos o administrativos).

En el presente la informática se ha extendido a todas las ramas de la sociedad; es decir, resulta factible controlar un vuelo espacial por medio de una computadora así como seleccionar las compras del hogar en una micro computadora.

Esta rapidez en el crecimiento de la informática permite deducir que los beneficios se han incrementado con la misma velocidad, algunos con mediciones tangibles como reducción de costos e incremento porcentual de ventas y otros con aspectos intangibles como mejoría en la imagen o satisfacción del cliente, pero ambos con la misma importancia para seguir impulsando la investigación y actualización constante de la tecnología.

Con el paso de los años la informática y todos los elementos tecnológicos que la rodean han ido creando necesidades en cada sector social y se han vuelto un requerimiento permanente para el logro de soluciones.

A continuación se mencionan algunas consideraciones que corresponden a una necesidad real y no a una tendencia:

- Todas las actividades de la sociedad buscan apoyarse de alguna forma en la tecnología de informática.
- Tanto los equipos de cómputo de diferentes marcas y capacidades como las bases de datos y los sistemas de información deben ser una solución integrada.
- La capacitación tiene que ser permanente en el uso de la tecnología de informática debido a su constante crecimiento y actualización.
- Hardware, software, telecomunicaciones y otros medios electrónicos han de estar interrelacionados para explotar al máximo sus capacidades y dar soluciones a todos los sectores de la sociedad.
- Integrar a la comunidad de manera permanente al campo de la informática.
- La gran penetración de la informática en todos los niveles del sector educativo, así como en los sectores social y cultural.
- El control y seguridad sobre todos los recursos de informática es una necesidad.
- Se debe evaluar de manera formal y periódica la función de informática.
- El proceso de planeación de los negocios ha de integrar de manera permanente la función de informática.
- Otros

1.2 AUDITORIA.

Definición de auditoría

"El examen de las operaciones financieras, administrativas y de otro tipo de una entidad pública o de una empresa por especialistas ajenos a ella y con el objeto de evaluar la situación de las mismas."

"Un proceso sistemático para obtener y evaluar evidencia de una manera objetiva respecto de las afirmaciones concernientes a actos económicos y eventos para determinar el grado de correspondencia entre estas afirmaciones y criterios establecidos y comunicar los resultados a los usuarios interesados"¹

¹ KELL ZIEGLER, Auditoria Moderna, CECSA

1.2.1 NATURALEZA Y PROPÓSITOS DE LA AUDITORÍA.

La Auditoría en su más amplio sentido, puede concebirse como una investigación crítica para llegar a conclusiones ciertas sobre la contabilidad de los aspectos financieros y de operaciones de una organización económica.

- a. Una investigación crítica implica una acumulación ordenada de evidencias.
- b. Las conclusiones ciertas implican la interpretación de la evidencia acumulada por un auditor competente.
- c. Las conclusiones de auditoría deberán ser presentadas, para mejor uso, en un informe escrito.

1.2.2 INFORMÁTICA

El concepto de informática es más amplio que el simple uso de equipos de computo o bien de procesos electrónicos.

“No existe una sola concepción acerca de que es informática; etimológicamente, la palabra informática, deriva del francés INFORMATIQUE. Este neologismo proviene de la conjunción de information (información), y automatique (automática). Su creación fue estimulada por la intención de dar una alternativa menos tecnocrática y menos mecanicista al concepto de “*PROCESOS DE DATOS*”.

En 1966, la Academia Francesa reconoció este nuevo concepto y lo definió del modo siguiente:

“Ciencia del tratamiento sistemático y eficaz, realizado especialmente mediante máquinas automáticas, de la información contemplada como vehículo del saber humano y de la comunicación en los ámbitos técnico, económico y social”.

1.2.3 LA AUDITORIA DEL SISTEMA INFORMÁTICO

La informática influye o condiciona el trabajo de los auditores de dos formas o en dos niveles diferentes. En primer lugar, la informática es una poderosa tecnología para el

tratamiento de la información y que afecta, por lo tanto, de forma sustancial al quehacer de los auditores. Los auditores externos, o incluso la propia auditoría interna de la empresa, en los casos en que esta exista, no puede conformarse con auditar los “inputs” o los datos de entrada y los “outputs” o datos de salida del sistema. Necesitan verificar también, con el grado de profundidad que en cada caso se juzgue conveniente, los programas y procesos intermedios, así como el grado de seguridad o fiabilidad del sistema en su conjunto y de cada una de sus partes o elementos.

Cada día los auditores tienen mayores conocimientos en informática, y lo más deseable es que sean ellos mismos quienes efectúen las pruebas necesarias para evaluar el grado de seguridad o fiabilidad del sistema informático. En otro caso, y como ese trabajo suele ser previo a cualquier otra tarea de los auditores, éstos necesitan contar con la colaboración de expertos en informática, que por razones obvias no pueden ser los técnicos de la propia empresa, para que hagan el trabajo que ellos necesitan.

En segundo lugar, porque la inversión en informática en empresas de cierta importancia suele constituir una de las partidas más importantes del balance, teniendo también importantes efectos en la cuenta de pérdidas y ganancias. Como cualquier otro activo, la inversión en informática, y por ende, todo el sistema informático, ha de ser sometido a las pruebas y procedimientos de auditoría y los niveles de control convenientes. Concretamente, una auditoría del sistema informático ha de comprender la verificación o análisis de los siguiente extremos:

- a. ***Seguridad de los activos.*** Los activos de una instalación informática, bastante costosos y de obsolescencia rápida generalmente, se hallan integrados por una pluralidad de activos o elementos: Hardware, software, personal técnico, sistemas de documentos y suministros de diversa naturaleza. El hardware puede ser dañado maliciosamente; el software y los contenidos en los archivos pueden ser robados o usados para usos no autorizados. La seguridad de los diferentes activos del sistema informático debe ser protegida por el sistema de control interno de la empresa, en general, y del centro de proceso de datos, en particular.

- b. **Razonabilidad de los datos.** La razonabilidad de los datos significa que éstos son fidedignos, completos y coherentes. Si la empresa no dispone de una informática adecuada, nunca podrá disponer de una representación del mercado y de sí misma veraz, principal objetivo de toda actividad auditora.
- c. **Eficacia del sistema.** Un sistema informático es eficaz cuando permite dar respuesta a los objetivos perseguidos, esto es, cuando facilita información con el tratamiento adecuado para que sus usuarios puedan tomar decisiones.
- d. **Eficiencia del sistema.** Un sistema informático es eficiente cuando permite dar respuesta a las necesidades de información que se le requieren con un sacrificio de recursos o coste mínimo.

1.3 CONTROL INTERNO

Las definiciones relativas al control interno establecidas por el Instituto Americano de Contadores Públicos (AICPA) son de especial interés debido al trabajo de los auditores de estados financieros, que consiste en expresar una opinión sobre la razonabilidad de los estados financieros de su cliente. En los estándares del AICPA relativos a la práctica de Auditoría (320.09) se encuentra la siguiente definición, misma que es coincidente con la señalada en el boletín E-02 de la Comisión de Normas y Procedimientos de Auditoría del Instituto Mexicano de Contadores Públicos:

"El control interno comprende el plan de organización y todos los métodos y procedimientos que en forma coordinada se adoptan en un negocio para salvaguardar sus activos, verificar la exactitud y confiabilidad de su información financiera, promover eficiencia operacional y provocar adherencia a las políticas prescritas por la administración."

.28 *El control contable comprende el plan de organización y los procedimientos y registros relacionados con la salvaguarda de activos y la*

confiabilidad de los registros financieros y, consecuentemente, el diseño de éstos para proveer una razonable seguridad de:

- a. Que las transacciones son ejecutadas de acuerdo con autorizaciones generales o específicas por parte de la administración.
- b. Que las transacciones son registradas atendiendo la necesidad de permitir la preparación de estados financieros de conformidad con principios de contabilidad generalmente aceptados o cualquier otro criterio aplicable a tales estados y mantener la Contabilización de activos.
- c. Que el acceso a los activos sólo sea permitido de acuerdo con autorización general o específica de la administración.
- d. Que los registros contables de los activos sean comparados, por períodos razonables con los activos existentes y que se tomen acciones apropiadas con respecto a cualquier diferencia.

OBJETIVOS GENERALES

- a. Asegurar el cumplimiento de las normas legales y reglamentarias, de las disposiciones administrativas y otras regulaciones aplicables a sus operaciones;
- b. Proteger los recursos de las organizaciones contra irregularidades, pérdida, daños, abuso, desperdicio, fraude y errores;
- c. Obtener información operativa y financiera útil, confiable y oportuna;
- d. Promover la transparencia de las operaciones y lograr la obtención de las metas y objetivos, mediante el cumplimiento de sus planes, programas y presupuestos.

PRINCIPIOS

Los Principios de Control Interno son:

- a. Responsabilidades delimitadas.
- b. Separación de funciones de carácter incompatible.

- c. División en el procesamiento de cada transacción.
- d. Selección de servidores hábiles y capaces.
- e. Aplicación de pruebas continuas de exactitud.
- f. Rotación de deberes.
- g. Otorgamiento de fianzas.
- h. Instrucciones por escrito.
- i. Utilización de cuentas de control
- j. Uso de equipos con dispositivos de prueba automática.
- k. Depósito inmediato e intacto de los recursos financieros.

BENEFICIOS DEL CONTROL INTERNO.

Los beneficios del control interno en forma generalizada son los siguientes:

- Salvaguarda de sus activos.
- Seguridad laboral al trabajador.
- Incremento en el volumen de operaciones.
- Presentación de cifras financieras razonables, para la toma de decisiones por parte de la gerencia.
- Especialización en la calidad del recurso humano.
- Obtención de mejores resultados Financieros.

CARACTERÍSTICAS DE UN BUEN CONTROL

El control es un factor extremadamente crítico en el logro de los objetivos generales, dependiendo su efectividad, en ese sentido, de la información recibida. Los sistemas de control, para lograr un uso óptimo, deben poseer ciertas características, que son las siguientes:

- a. Deben ser oportunos.
- b. Seguir Una Estructura Orgánica.
- c. Ubicación Estratégica.

- d. Un Control Debe de Ser Económico.
- e. Revelar Tendencias y Situaciones.
- f. Resaltar la Excepción.

1.3.1. CONTROL INTERNO ADMINISTRATIVO

Está constituido por el plan de organización, los procedimientos y registros que conciernen a los procesos de decisión que conducen a la autorización de las transacciones por parte de los niveles jerárquicos superiores, de tal manera que fomenten la eficiencia en las operaciones, la observancia de las políticas y normas prescritas y el logro de las metas y objetivos programados.

La obtención de los resultados con eficiencia, efectividad y economía, la protección de los recursos y la revelación de errores o desviaciones son responsabilidad primordial e indelegable de los niveles jerárquicos superiores; por lo mismo es indispensable para ello mantener un sólido control interno administrativo.

1.3.2 CONTROL INTERNO FINANCIERO

Comprende el plan de organización, los procedimientos y registros concerniente a la custodia de los recursos financieros y materiales, y a la verificación de la exactitud, confiabilidad y oportunidad de los registros e informes financieros.

Es responsabilidad de cada entidad pública, principalmente de su titular o máxima autoridad, incluir dentro del trámite normal de las transacciones financieras los procedimientos que permitan lograr un eficiente control financiero, especialmente por medio de los procedimientos de control previo al compromiso y al desembolso.

1.3.3 CONTROL INTERNO EN AMBIENTE COMPUTARIZADO

CONCEPTO:

Plan de organización, métodos y procedimientos que se coordinan y adaptan en una entidad para salvaguardar sus activos, prevenir sabotajes, errores e irregularidades,

verificar la razonabilidad y confiabilidad de su información financiera, produciendo el cumplimiento de sus políticas.

OBJETIVOS DEL CONTROL INTERNO:

- a. Protección de los activos de la empresa.
- b. La obtención de información financiera veraz y oportuna.
- c. La promoción de eficiencia en la operación del negocio.
- d. Lograr que en la ejecución de las operaciones, se cumplan las políticas establecidas por los administradores de la empresa.
- e. Prevenir el robo, fraude o sabotaje que provoquen la pérdida total o parcial de la información y daños en los equipos.

EVALUACIÓN DEL CONTROL INTERNO EN SISTEMAS COMPUTARIZADOS

Como cualquier departamento de la empresa, el auditor tiene que evaluar el funcionamiento del Procesamiento Electrónico de Datos (PED). Debe evaluar el ambiente de control, para conocer la existencia de medidas de control interno y la habilidad de la gerencia para establecer mecanismos de autoevaluación y vigilancia, incluyendo es establecimiento de manuales y estándares, separación de funciones, supervisión y auditoría interna, y capacitación, apoyo a la investigación y adelantos técnicos.

OBJETIVOS DE LA EVALUACIÓN DEL CONTROL INTERNO

- a. Establecer la base para confiar en el sistema de control interno con el fin de determinar la naturaleza, extensión y oportunidad de las pruebas de auditoría que se deben aplicar en el examen.
- b. Obtener una base para formular sugerencias constructivas a las empresas con respecto al mejoramiento de su sistema de control interno.

1.3.4 LOS TRES ELEMENTOS DE LA ESTRUCTURA DE CONTROL

CONTROL DEL AMBIENTE

Los factores ambientales son influenciados por:

- a. La filosofía y estilo operacional gerencial
- b. La estructura organizacional de la entidad
- c. El funcionamiento de la Junta de Directores y Comités, especialmente el Comité de Auditoría
- d. Los métodos de asignar autoridad y responsabilidad
- e. Los métodos de control gerencial para supervisar y mantener el seguimiento sobre la ejecución, incluyendo la Auditoría Interna.

SISTEMA DE CONTABILIDAD

Un efectivo Sistema de Contabilidad establece métodos y formularios que:

- a. Identifiquen y registren todas las transacciones válidas.
- b. Describan oportunamente las transacciones, con un detalle suficiente para permitir una clasificación apropiada de las transacciones para Informes Financieros.
- c. Midan el valor de las transacciones para permitir contabilizar un valor monetario apropiado de los Estados Financieros.
- d. Determinen el período de tiempo en que las transacciones ocurren, para permitir contabilizar las transacciones en el período contable apropiado.
- e. Presenten apropiadamente las transacciones y revelaciones expuestas en los Estados Financieros.

LOS PROCEDIMIENTOS DE CONTROL

Estos procedimientos pueden categorizarse como pertenecientes a la:

- Autorización apropiada de transacciones y actividades.
- Segregación de deberes que reducen las oportunidades que permiten que cualquier persona, en una posición ejecute y oculte errores o irregularidades en el

curso normal de sus funciones; asignando a diferentes personas la responsabilidad de:

- Autorizar las transacciones,
 - Registrar las transacciones, y
 - Custodiar los activos.
-
- Utilización y diseño de documentos y libros adecuados que ayuden a asegurar la anotación apropiada de transacciones y hechos, tales como el seguimiento del uso correlativo de documentos de embarque prenumerados.
 - Custodia adecuada sobre el acceso al, y uso de, activos y de registros, tales como la seguridad de las instalaciones y la autorización para el acceso a los programas de computación y a los archivos de información.
 - Revisión independiente sobre la ejecutoria y la valuación apropiada de las cantidades anotadas, tales como:
 - Arqueos de activos tangibles,
 - Conciliaciones,
 - Comparación de activos con los libros contables.
 - Controles de los programas de computación,
 - Revisión gerencial de los Informes que resumen el detalle de las cuentas del balance (Ejemplo: Un estado de clientes por antigüedad de saldos).
 - Revisión por el usuario de los Informes generados por PED.

EL COSTO/BENEFICIO DE LA ESTRUCTURA DE CONTROL INTERNO

Es establecimiento y mantenimiento de una Estructura de Control Interno es responsabilidad gerencial.

Para asegurarse de que se logran sus objetivos, la Estructura de Control Interno debe MANTENERSE BAJO UNA CONTINUA SUPERVISION GERENCIAL para determinar que:

- a. Está operando como se efectivamente, y
- b. Se modifica acorde con los cambios en las condiciones que las operaciones exigen.

El concepto de seguridad razonable reconoce que EL COSTO DE la estructura de CONTROL INTERNO de una entidad NO DEBE EXCEDER LOS BENEFICIOS que se esperan de la misma. AUNQUE la relación de Costo/Beneficio es un criterio básico a considerar al diseñar la Estructura de Control Interno, SU MEDICION PRECISA usualmente NO ES POSIBLE.

Consecuentemente, la gerencia optará POR ESTIMADOS y CRITERIOS CUANTITATIVOS Y CUALITATIVOS para evaluar su Costo/Beneficio.

1.3.5 CARACTERÍSTICAS ESPECÍFICAS DE LOS SISTEMAS COMPUTARIZADOS²

- a. **Procesamiento Uniforme de las Transacciones.** El procesamiento computarizado somete uniformemente todas las transacciones similares a las mismas instrucciones de procesamiento, la posibilidad de errores al azar, un problema de control que se presenta en ambientes manuales, queda sustancialmente reducida. No obstante, aun cabe la posibilidad de que de que nos datos ingresados al computadora para su procesamiento puedan incluir errores o ser incompletos.
- b. **Posibilidad de Errores e Irregularidades no Detectadas.** La posibilidad de que ciertos individuos, incluyendo a aquellos que realizan procedimientos de control, accedan a los datos sin autorización, o los alteren sin dejar evidencias visibles, puede ser mayor en los sistemas computarizados que en los sistemas manuales. Ello se debe a que la información es almacenada en forma electrónica, con una menor participación del hombre en el procesamiento, reduciéndose, por consiguiente, la oportunidad de detectar manualmente los accesos no autorizados. Por los general, los recursos de información tienden a estar concentrados en los ambientes CIS (Sistemas de Información Computarizados).

- c. **Potencial para Una Mayor Supervisión Gerencial.** Los sistemas computarizados ofrecen a la gerencia una amplia variedad de herramientas analíticas que pueden ser utilizadas para revisar y supervisar las operaciones de la organización.
- d. **Rastro de las Transacciones.** El diseño CIS da como resultado que el rastro de las transacciones, que puede ser utilizado para propósitos de auditoría, sólo es conservado por poco tiempo o en forma electrónica.
- e. **Segregación de Funciones Incompatibles.** Ciertos controles, ejecutados por diferentes individuos en los sistemas manuales, pueden ser concentrados en los sistemas en los que se utiliza procesamiento computarizado. Esto puede resultar en una menor segregación de funciones incompatibles. Sin embargo, los sistemas computarizados pueden permitir que se implante una segregación de funciones más rigurosa ya que pueden existir controles basados en el software (tales como identificaciones del usuario y contraseñas).
- f. **Iniciación Automática o Ejecución Posterior de Transacciones Mediante el Computador.** La iniciación de ciertas transacciones, o ciertas funciones de procesamiento pueden ser efectuadas automáticamente por el computador. Pueden existir evidencias visibles de estos pasos de procesamiento.
- g. **Los Controles Manuales Dependen De La Contabilidad Del Procesamiento Computarizado.** El procesamiento computarizado puede producir información utilizable para realizar controles manuales. La efectividad de estos procedimientos de control manual puede depender de la efectividad de los controles sobre la integridad y exactitud del procesamiento computarizado.

² Evaluación y Prueba de Controles de PED, Serie de Guías de Auditoría, PRICE WATERHOUSE

1.3.6 CONTROL INTERNO E INFORMÁTICA

La informática o tratamiento electrónico de la información está condicionado o influenciado en la organización de las empresas, en sus formas de gestión y, en consecuencia, en la estructura de sus sistemas de control interno.³

SEPARACIÓN O SEGREGACIÓN DE FUNCIONES

Cuando en el departamento de informática se combinan funciones cuya agregación a efectos de su realización pudiera resultar poco convincente, hay que crear dentro del propio departamento *controles de compensación* que eviten posibles comportamientos fraudulentos de los técnicos o empleados que trabajan en el mismo.

Uno de esos controles es la propia segregación o separación de funciones dentro del departamento de informática; esto es, al frente del departamento de informática debe existir siempre un director o gerente, a quien corresponde dirigir y supervisar todo lo que allí se hace. El director del departamento de informática o centro de proceso de datos debe depender de algún vicepresidente de la compañía o del contralor.

A su vez, dependiendo del director o gerente y ya dentro del propio departamento de informática, deben estar separadas la funciones de *análisis de sistemas, programación, operaciones de computadora, biblioteca de programas y, archivo y control*.

Los analistas de sistemas son responsables del diseño del sistema de procesamiento de datos, guiados por las instrucciones que les proporcionan los analistas de sistemas; los programadores diseñan los flujogramas de la computadora requeridos por el sistema, traducen los programas al lenguaje de la computadora, los prueban y hacen las depuraciones necesarias.

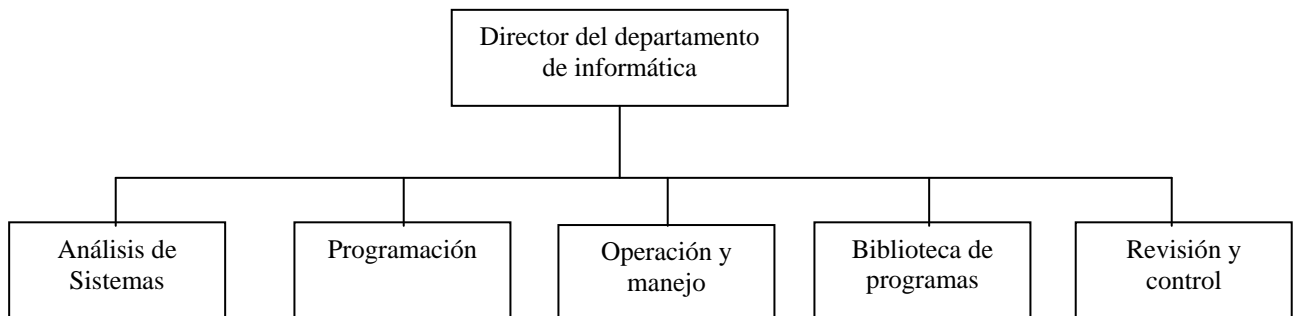
Los operadores manejan la computadora de acuerdo con las instrucciones de los programadores; las entradas en la computadora deben registrarse a través de otro medio antes de realizarlas, a fin de que quede constancia escrita e impresa de dichas entradas.

³ Guías de Auditoría, Sistemas de Información Computarizados, PRICEWATERHOUSE

Para evitar que se pierdan o se estropeen, los programas, el detalle de las transacciones, las cintas y demás documentos o elementos de software, que no estén siendo usados, deben guardarse en la biblioteca de programas o en el archivo.

Con independencia de la supervisión general del director o gerente, dentro del propio departamento de informática suele existir una división de control que revisa los trabajos de las divisiones encargadas de realizar las funciones a que se ha hecho referencia.

ORGANIGRAMA BÁSICO DE LA UNIDAD PED



Para evitar fraudes es muy importante la separación de funciones a que antes se hizo referencia. Las funciones de control de los “inputs” o datos de entrada a la computadora, programación y manejo de la computadora deben estar separadas y se realizadas por tres técnicos o grupos de técnicos en informática diferentes. Todo cambio en el programa de una computadora debe estar autorizado por la persona que corresponda.

Se denominan cuadros de flujo del sistema o flujogramas a las gráficas que describen de una manera lógica los diferentes pasos o fases del tratamiento de los diferentes datos, por ejemplo la recepción de un pedido de clientes o el aviso de reposición de stocks a proveedores, desde el momento mismo en el dato entra en el sistema; los auditores deben recoger estos flujogramas en sus papeles de trabajo, porque de su análisis se pueden deducir una serie de conclusiones sobre la bondad de los sistemas de control interno. Además de los cuadros de flujo del sistema, la documentación de in sistema

informático incluye también los cuadros de flujo de los programas, que muestra la lógica detallada de los diferentes programas de la computadora.

DOCUMENTOS Y REGISTROS ADECUADOS

En un sistema contable informatizado, la iniciación y registro de una transacción no siempre necesitan contar con soporte documental. Por ejemplo, una orden de pedido de un cliente formulada por teléfono puede entrar directamente en el sistema; una reposición del inventario de determinado producto puede formularse de un modo automático cuando dicho inventario alcanza un determinado nivel etc. Ello no obstante, en un sistema informático, cuando está bien diseñado, se guarda constancia de todo ello de forma más extensa incluso que en el sistema manual.

Es cierto que las computadoras son capaces de crear, modificar y borrar de sus registros con gran facilidad, de ahí que en los primeros tiempos del desarrollo de la informática existiera una cierta preocupación entre los auditores, en el sentido que el tratamiento electrónico de la información oscureciera o eliminaba las pruebas necesarias para el trabajo de los auditores.

Hoy día, todo sistema PED bien diseñado tiene que dejar pruebas, pistas o rastro suficiente para permitirle a la gerencia reconstruir el archivo en caso de errores en el tratamiento de la información o de fallos en la computadora, y satisfacer los requerimientos de los auditores y del sector tributario.

PERSONAL COMPETENTE Y DE CONFIANZA

Las tecnologías para el tratamiento electrónico de la información han venido siendo cada vez más complejas. Para manejar esas tecnologías se necesitan personas competentes y capacitadas para ello. Pero tan importante como la competencia y la capacitación es la confianza. Pues de poco valdría un sistema informático con un diseño técnico perfecto si las personas que lo manejan carecen de una apropiada deontología profesional.

SISTEMA DE AUTORIZACIONES

En una organización suele haber dos tipos de autorizaciones. Unas autorizaciones son de carácter general, por ejemplo: las contenidas en la lista de precios de los productos a vender que se le entregan al personal del departamento de ventas. Otras autorizaciones, en cambio, son específicas, por ejemplo los pagos o la autorización de gastos que superen unos límites previamente especificados, que en esos casos han de contar con la aprobación de algún superior jerárquico o miembro del consejo directivo.

En un sistema contable manual, los auditores pueden analizar la bondad del sistema de autorizaciones examinando el trabajo de los empleados de la empresa. En un sistema contable informatizado muchas de esas autorizaciones son parte del contenido del programa utilizado en el propio proceso de datos. Para evaluar el grado de idoneidad del sistema de autorizaciones, a los auditores no les basta con examinar el trabajo de los empleados. Tienen que verificar, además, el contenido o conjunto de instrucciones del programa.

CONTROL DE ACCESO A LOS REGISTROS

El control de acceso a los registros es fundamental, tanto en un sistema manual como en uno informatizado. Con este segundo sistema el problema es mucho mayor, por los datos y registros se hallan generalmente concentrados en un mismo lugar, dentro de las memorias y soportes magnéticos de la propia computadora, y no dispersos en lugares diferentes bajo la custodia de personas distintas, como ocurre generalmente con un sistema manual, en el que la comisión de un fraude presenta por ello mayores dificultades.

DELEGACIÓN DE AUTORIDAD Y RESPONSABILIDAD

Una clara línea de autoridad y responsabilidad es un control esencial en una organización. Cuando una empresa tiene informatizado el tratamiento de la información, esa demarcación clara de autoridad y responsabilidad de cada uno de los empleados no siempre resulta factible; por ejemplo, cuando el sistema informático se halla diseñado

par que pueda ser utilizado por múltiples usuarios no siempre resulta fácil determinar por adelantado quien es responsable si los datos o programas son distorsionados y quién tiene la obligación de identificar esos errores.

ADECUADA SUPERVISIÓN DIRECTIVA

En un sistema contable manual, la supervisión de los diferentes empleados por parte de sus jefes resulta generalmente fácil, por que todos ellos suelen trabajar en un mismo lugar o en dependencias muy próximas. En un sistema contable informatizado, en cambio las cosas son un poco diferentes. La informática hace posible hoy en día que los empleados puedan estar cerca de sus clientes y lejos de las oficinas centrales de la empresa, lo cual hace que la supervisión por parte de los directivos se dificulte.

SEGURIDAD Y CUSTODIA

Las instalaciones que acogen al centro de proceso de datos o núcleo principal del sistema informático deben reunir unas adecuadas condiciones de seguridad, a fin de prevenir un posible sabotaje, incendio o inundación. Al centro de proceso de datos sólo debe tener acceso el personal autorizado. El local en el que se guarda la unidad central de procesamiento no debe tener ventanas y pocas puertas, con cerraduras activables por fichas magnéticas, cuyas claves deben ser cambiadas con cierta frecuencia. El acceso a este local debe estar siempre cuidadosamente vigilado.

1.4 EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO

La segunda norma de auditoría relacionada con la ejecución del trabajo establece lo siguiente: “debe hacerse un apropiado estudio y evaluación del control interno existente, de manera que se pueda confiar en él como base para la determinación de la naturaleza, extensión y oportunidad de los procedimientos de auditoría”.

El estudio del Sistema de Control Interno utilizado por la organización o área que se va a auditar se incluye como un imperativo que se refleja en las normas de auditoría y tiene por objeto evaluar la eficiencia del control interno.

1.4.1 EVALUACIÓN PRELIMINAR DEL RIESGO

Estos momentos es la fase en que se identifican los sistemas “vivos y no vivos” más importantes que afectan las áreas más significativas del sistema PED. De estos sistemas, solo se dispone de una breve comprensión, pues no se ha entrado a un estudio detallado de su funcionamiento.

El siguiente paso es uno de los más importantes que se toma y consiste en tomarla decisión sobre estudiar detalladamente los sistemas identificados, una parte de ellos o ninguno. Esta decisión es una de las más importantes a tomar, pues de ella dependerá directamente el alcance y momento de realización de las pruebas; el cuadro siguiente muestra la relación entre estos conceptos:

CONCEPTO	SISTEMA ANALIZADO	SISTEMA ANALIZADO	SISTEMA NO ANALIZADO
Calidad de controles	Controles buenos	Controles malos	Controles no investigados
Riesgo de error	Pequeño	Medio alto	Desconocido
Alcance de las pruebas de auditoría	Menor	Mayor	mayor

SISTEMAS ANALIZADOS

Elegidos los sistemas que deseamos estudiar en profundidad, deberemos reunirnos con los distintos responsables de la empresa; quienes nos contarán como funcionan estos sistemas. Para plasmar en nuestros papeles de trabajo, podemos utilizar dos técnicas:

Flujogramas: Técnica que recoge la descripción de un sistema mediante gráfico, apoyados por una breve explicación narrativa.

Narrativas: Expresamos en un memorandum el funcionamiento del sistema

SISTEMAS NO ANALIZADOS

Otra posibilidad que tenemos, es decir, a priori, una vez identificado los sistemas significativos que afectan a las cuentas más importantes es la de no realizar estudio de los sistemas, o de alguno de ellos.

La evaluación del riesgo se puede decir que es la etapa en que el auditor efectúa un análisis general del riesgo implícito en el trabajo que va a realizar, con el objeto de considerarlo en el diseño de sus programas de trabajo de auditoría y para identificar gradualmente las actividades y a características específicas de la entidad.

1.4.2 EVALUACIÓN DEL RIESGO Y CONTROL INTERNO EN LA AUDITORÍA DE SISTEMAS COMPUTARIZADOS

Los riesgos inherentes y de control en un sistema de información por computadora pueden tener tantos efectos generales, como específicos debido a la probabilidad de presentaciones erróneas importantes. Estos pueden dar como resultado deficiencias en el desarrollo del sistema computarizado, en el desarrollo mantenimiento de programas, soporte al software de sistemas, control sobre acceso programas de utilería, controles de accesos al equipo, controles del fabricante entre otros.

Al realizar la auditoría se debe evaluar como la empresa sigue sus controles para el desarrollo de sus actividades y que tipo de riesgo se puede tener ya sea inherente, de control o de detección, ejemplo:

ACTIVIDADES A EVALUAR	% DE RIESGO	TIPO DE RIESGO	NIVEL
Hardware	30%	Riesgo de detección	Medio
Software	50%	Riesgo de control	Medio
Recurso humano	20%	Riesgo inherente	Bajo

ALCANCE DE LA AUDITORÍA

ÁREA	ACTIVIDAD
Hardware	Verificar que el equipo de computación este debidamente asegurado
Software	Evaluar el funcionamiento de los programas instalados en cualquier operación y verificar que tan confiable es esa información
Recurso Humano	Verificar si están cumpliendo con los objetivos que la empresa pretende alcanzar

1.5 RIESGOS DE AUDITORÍA

Se dice que una decisión esta sujeta a riesgo cuando existe alguna incertidumbre en cuanto a los resultados posibles a obtener; es el riesgo de que el auditor dé una opinión de auditoria inapropiada.

El riesgo de auditoría presenta la posibilidad de que el auditor pueda dar opinión sin salvedad, sobre los estados financieros que contengan errores y desviaciones de principios de contabilidad, en exceso a la importancia relativa. El riesgo de auditoría está integrado por el efecto combinado de los tres diferentes riesgos que se explican a continuación:

- a. Los riesgos inherentes y de control existen en forma independiente en la auditoría y su función. Ejemplo:

“El riesgo de que una declaración incorrecta importante que pudiera ocurrir en una afirmación no se evitará ni detectará oportunamente por medio de los procedimientos o políticas de la estructura de control interno de una entidad.”

- b. En el caso del riesgo de control, el auditor debe aplicar las pruebas de cumplimiento necesarios para probar los controles en que se basa su evaluación. Ejemplo:

“El riesgo de que el auditor no detectará una declaración incorrecta importante que existe en una afirmación.”

- c. El riesgo de detección lo establece el auditor al determinar la naturaleza, alcance y oportunidad de sus pruebas sustantivas.
- d. El riesgo de detección se debe establecer en la relación inversa a los riesgos inherentes y de control. A menor riesgo inherente, de control, mayor puede ser el riesgo de detección.

1.5.1 RIESGOS INHERENTES

Representa el riesgo de que ocurran errores importantes en un rubro específico, sin considerar el efecto de los procedimientos de control interno que pueden existir.

Ejemplo:

“Una medida de la evaluación que hace el auditor de la probabilidad que existan errores importantes en un segmento antes de considerar la eficacia de la estructura de control interno.”

1.5.2 RIESGO DE CONTROL

La evaluación preliminar del riesgo de control es el proceso de evaluar la efectividad de los sistemas de contabilidad de control interno de una entidad para prevenir, detectar y corregir representaciones erróneas de importancia relativa. Siempre habrá algún riesgo de control a causa de las limitaciones inherentes de cualquier sistema de contabilidad y de control interno.

Representa el riesgo de que los errores importantes que pudieran existir en un rubro específico de los Estados Financieros, sin embargo, el control nunca desaparece totalmente, aun cuando se alcancen todos los objetivos del sistema de control interno, debido a las limitaciones inherentes a cualquier sistema de este tipo. Normalmente no se examina la totalidad de las partidas que integran una cuenta o un rubro de los estados financieros.

1.5.3 RIESGO DE DETECCIÓN

Representa el riesgo de que los procedimientos aplicados por el auditor no detecten los posibles errores importantes que hayan escapado a los procedimientos de control interno.

1.5.4 EVALUACIÓN DEL RIESGO INHERENTE Y DE CONTROL

La evaluación del riesgo es una parte integrante del desarrollo de un plan de auditoría. Las características específicas de los sistemas computarizados crean riesgos que, por lo

general, son diferentes a los de un entorno de un proceso manual. Si bien los objetivos de la gerencia con respecto a los sistemas de información, contables y de control no se ven afectados por los medios utilizados para procesar datos y son aplicables tanto a entornos manuales como computarizados, la forma e implantación de los controles diseñados para reducir al mínimo los riesgos propios de los sistemas computarizados pueden ser diferentes.

1.5.5 RIESGO.

El riesgo se relaciona con el grado en el cual una partida es vulnerable a error. La cantidad de evidencia requerida en un caso determinado será proporcional al grado de riesgo asociado con la validez y corrección del saldo de una cuenta.

Para efectos de evaluar el riesgo, será de gran utilidad reconocer que el saldo de una cuenta podrá resultar de:

- a. Un proceso rutinario de transacciones tales como las ventas, compras y nóminas.
- b. Procesamiento no rutinario de transacciones, tales como las que se relacionan con compañías afiliadas, funcionarios y empleados.
- c. Criterios de los administradores, como en los casos relacionados con garantías de productos, cuentas incobrables e inventarios obsoletos.

El grado de riesgo asociado con saldos que surgen de procedimiento de rutina está inversamente relacionado con la eficiencia del sistema de control interno del cliente. Mayor cantidad de evidencia necesitará el auditor cuando los controles son débiles en contraste a cuando los controles son buenos.

Los procedimientos de control interno podrán no extenderse hasta el procesamiento de transacciones no rutinarias o respecto al criterio de los administradores. El riesgo relacionado con transacciones no rutinarias dependerá de la existencia y eficacia de controles específicos.

El grado de riesgo respecto a criterios de los administradores dependerá básicamente en la integridad de la administración y en cualquier control incorporado en el proceso de toma de decisiones del cliente.

1.6 CUESTIONARIOS DE CONTROL INTERNO COMO MÉTODO DE EVALUACIÓN

1.6.1 DEFINICIÓN

Un cuestionario de control interno consiste en la serie de instrucciones que deben seguir o responder al auditor. Cuando se finaliza una instrucción, deben escribirse las iniciales en el espacio al lado de la misma. Si se trata de una pregunta, la pregunta (que suele ser normalmente "si" "no" "no aplica") se anota al lado de la pregunta.

El auditor recopila la información por varios canales. El cuestionario podría entregarse en un principio al contralor o al jefe de contabilidad. Al finalizar la misma, el auditor comprueba si los procedimientos utilizados son los indicados y rellena el cuestionario personalmente, comprobando si los procedimientos empleados en la realidad se adaptan a las normas de control interno de la institución objeto de la auditoría.

El auditor es el responsable de obtener personalmente la información necesaria para evaluar el control interno de acuerdo con las preguntas que se les formulen.

Para el uso de los cuestionarios se deben tener en cuenta los siguientes pasos:

- ⇒ Entrevistas de los auditores con los empleados responsables de la entidad o del área por auditar.
- ⇒ Diligenciamiento del formulario en presencia de quien está respondiendo las preguntas.
- ⇒ Inclusión de preguntas adicionales, de ser necesario, durante el trabajo de campo.
- ⇒ Determinar durante el curso de las entrevistas si las preguntas son correctas; en caso negativo, hacer correcciones de forma inmediata.
- ⇒ Determinar la incidencia del estado del control interno en el alcance del examen y su relación con el programa de auditoría.

1.6.2 CUESTIONARIOS PARA AUDITORIA EN INFORMÁTICA

Los cuestionarios son una ayuda muy valiosa para el auditor en informática, ya que son materiales elaborados, revisados, adaptados y documentados de manera previa (incluso sirve de base para auditar diferentes negocios o empresas sin perder validez).

1.6.3 VENTAJAS DE LOS CUESTIONARIOS

- a. Objetivos y alcances predefinido
- b. Fáciles de aplicar, entender y contestar
- c. Orientados a que las respuestas sean fáciles de entender y analizar
- d. Preguntas adecuadas al perfil del personal que contestará
- e. Revisados y aprobados por el director de auditoría
- f. Apegados a políticas y procedimientos del negocio
- g. Relacionados con estándares recomendados para cada área
- h. Existen preguntas adaptadas a las características de cada área
- i. Con objetivos predefinido y una secuencia lógica en su aplicación

ÁREAS A EVALUAR

- a. Organización del área de informática
- b. Políticas y objetivos del área de informática
- c. Seguridad física
- d. Metodología del desarrollo y mantenimiento de sistemas
- e. Protección y confidencialidad de datos
- f. Sistemas contables

1.7 AUDITORIA DE INFORMÁTICA Y SISTEMAS CON COMPUTADOR

Los procedimientos de control interno relacionados con sistemas computarizados se pueden clasificar en controles generales y controles de aplicación. Los controles generales se aplican con amplitud en las aplicaciones del PED e incluyen elementos tales como:

- a. Organización del departamento PED
- b. Procedimientos de documentación dentro del departamento de PED
- c. Control del acceso y otras medidas de seguridad

Los controles de aplicación se relacionan con operaciones específicas de procesamiento de datos realizadas por el sistema. Algunas veces se les conoce como controles de información o controles de procedimientos, y comprenden los siguientes elementos:

- a. Controles de información
- b. Controles de procesamiento
- c. Controles de salidas de información

Al evaluar el control interno sobre el sistema PED el auditor debe revisar en primer lugar el sistema para llegar a entender el proceso y sus características de control. La segunda fase de evaluación debe consistir en pruebas de cumplimiento para asegurar el auditor que las características de control existentes estén funcionando de manera satisfactoria. Normalmente con la revisión del sistema se realiza utilizando un cuestionario especial de control interno diseñado para instalaciones PED.

Las siguientes secciones describen las características de los diversos elementos, tanto de los controles generales como de aplicación. Es necesario comprender estos elementos para evaluar con propiedad los controles de un sistema PED.

1.7.1 ORGANIZACIÓN DEL DEPARTAMENTO PED.

El estudio de las consideraciones de organización relacionadas con las instalaciones de computadoras puede comenzar con el examen de dónde debe estar ubicado el departamento PED en la organización general. Al revisar la estructura orgánica de varias compañías se puede encontrar que el director del departamento de PED depende directamente del presidente, contralor, del vicepresidente de administración o de algún otro ejecutivo.

La ubicación del departamento PED en la organización será importante desde el punto de vista del control interno. Esto se debe a que una ubicación inadecuada puede interferir con la necesaria separación de funciones dentro del negocio. Las funciones básicas que deben quedar separadas incluyen: 1) iniciación y autorización de las operaciones, 2) registro de las mismas, y 3) custodia de los activos. Por ejemplo: en aquellos casos en que el computador autoriza o inicia operaciones de acuerdos con criterios predeterminados puede presentarse la violación de la separación necesaria de funciones. No obstante, si se toman las precauciones adecuadas se obtendrá un control satisfactorio con un número de diferentes patrones de organización.

Una consideración relacionada que debe reconocer el auditor es la centralización de funciones provocadas por la instalación del PED. Esto se refiere a la concentración en departamento PED de muchas funciones que, antes de implantarse es sistema de computación, se llevarán a cabo en varios departamentos diferentes.

Aunque éste es el resultado natural de desarrollar una función separada de PED, es una situación que puede conducir a debilidades en el control interno. Para que exista un control interno adecuado deben separarse varias funciones dentro del departamento PED. Entre estas funciones se incluye:

- a. Análisis de sistemas y programación
- b. Operaciones del computador
- c. Función de la biblioteca de programas y archivos de transformación
- d. Unidad de control.

La separación de la función de análisis de sistemas y programación de las operaciones del computador es crítica desde el punto de vista del control interno. Esta división cumple con el fin de separar a aquellos que poseen el conocimiento necesario para introducir información no autorizada en el sistema (analistas y programadores) de aquellos que tienen acceso al equipo necesario para llevar a cabo esta acción (operadores de la máquina).

Se supone que los empleados que diseñan las aplicaciones de computación y escriben los programas tienen suficientes conocimientos de aplicación para poder elaborar métodos de introducción de cambios no autorizados en los programas o in formación no autorizada en las operaciones del computador.

Por este motivo las operaciones rutinarias de computación no deben ser realizadas por empleados de la división de sistemas y programación. Los operadores de la máquina no deben estar familiarizados con los detalles de los programas de operación si es que se desea que esta división tenga algún significado.

La función de la biblioteca de archivos de programas e información debe quedar separada de las demás divisiones del departamento a fin de que no haya libre acceso a los archivos de programas e información. Si no se mantiene el control de estos programas y registros se pueden introducir cambios fraudulentos con poca posibilidad de que sean detectados. Los procedimientos adecuados en esta área deben controlar el acceso a los materiales según se necesiten de acuerdo con el programa de operación diario o tal como quede autorizado.

La unidad de control en el departamento PED realiza la función de auditoría dentro de la instalación. Sólo este grupo debe tener acceso a la información de control asociada con los controles de aplicación para asegurar la exactitud de la información de salida. Y debe ser independiente de las demás divisiones departamentales y no llevar a cabo funciones rutinarias de operación.

Se observa que resulta necesaria la división apropiada de tareas dentro de la organización departamental de PED si se desea mantener un control interno adecuado. En algunas instalaciones muy pequeñas resulta difícil la división de las tareas debido a las limitaciones del personal, pero la conciencia de la separación funcional necesaria con frecuencia ayuda a desarrollar rutinas de trabajo que mejoran el control, incluso en el sistema más pequeño.

1.7.2 PROCEDIMIENTOS DE DOCUMENTACIÓN DENTRO DEL DEPARTAMENTO DE PED.

El control adecuado sobre el sistema de computación exige que se establezcan procedimientos apropiados de documentación. Estos documentos deben asegurar la creación y el mantenimiento de registros que describan los sistemas, programas, controles y otras operaciones del departamento. Estos procedimientos de documentación:

- a. Dan a la administración una clara comprensión del sistema de PED y aseguran que se cumplan sus políticas.
- b. Sirven de base para la revisión de los controles contables internos por los auditores internos y externos.
- c. Proporcionan una referencia conveniente para los analistas de sistemas y programadores que tienen bajo su responsabilidad el mantenimiento y la revisión de los sistemas y programas existentes.

1.7.3 DOCUMENTACIÓN DE SISTEMAS

La documentación de cada sistema incluir materiales tales como:

- a. Declaración del problema que de una definición adecuada del propósito de la aplicación y cómo complementa otros sistemas de operación.
- b. Diagramas de flujos de los sistemas.
- c. Requisitos de información de entrada y de salida
- d. Métodos de procesamiento
- e. Requisitos de equipo.
- f. Copias de las autorizaciones para cambios en el sistema.
- g. Controles necesarios.

1.7.4 DOCUMENTACIÓN DE PROGRAMAS

Cada archivo de documentación del programa debe incluir:

- a. Declaración del problema que identifique la función de este programa en el sistema general.
- b. Diagrama de flujos del programa
- c. Relación de características de control.
- d. Registro de esquemas que especifiquen las características de la información y los campos en el archivo de la computadora.
- e. Instrucciones de operación.
- f. Relación del programa.
- g. Detalles y aprobación de cambios del programa.
- h. Descripción de los formatos de entradas y salidas.

1.75 CONTROLES DE ACCESO Y OTRAS MEDIDAS DE SEGURIDAD

Otro aspecto importante del control interno sobre los sistemas de computación es la consideración que se da a la seguridad del hardware y del software. Muchas compañías han llegado a comprender que la instalación de la computación representa en la práctica el sistema nervioso del negocio. Debido a esto un sistema completo de control interno debe incluir provisiones para la protección física del sistema PED y de la información almacenada en el mismo.

La protección adecuada del software incluye procedimientos para reconstrucción de archivos, almacenamiento de información en otro lugar fuera de las instalaciones y un estricto control de la biblioteca.

El plan de reconstrucción de archivos debe incorporar procedimientos que permitan mantener copias duplicadas de programas y de archivos de información, o que requieran que se conserven los archivos de información anteriores de modo que se pueda reconstruir toda la información actual si fuera necesario.

Para que los procedimientos de reconstrucción de archivos sean completamente efectivos se deben guardar los duplicados de todos los archivos maestros y programas importantes en un lugar a prueba de fuego o fuera de las instalaciones.

Los procedimientos de biblioteca deben limitar la entrega de materiales sólo a empleados autorizados sobre la base de “según los necesiten”. Normalmente sólo se deben entregar los programas y los archivos de información a los operadores, de acuerdo con el programa de operación que se esté realizando, y a los demás sólo bajo autorización específica.

1.7.6 CONTROLES DE APLICACIÓN

Los controles de aplicación específica son medidas tomadas en el diseño del sistema o en la fabricación el equipo de computación para dar seguridad de que la información se procese, se registre y se presente de modo apropiado. La mejor manera de estudiar estos controles es en el orden en que afectarían del procesamiento de datos a través del sistema, es decir, a través de controles de entrada, controles de procesamiento y controles de salida.

1.7.7 CONTROLES DE ENTRADA

Se deben desarrollar controles de entrada que den la seguridad de que se recibe la información, se traduce y entra si error al sistema. Algunas de las técnicas utilizadas para lograr esto incluyen:

- a. Registro de todos los números de los documentos de entrada prenumerados por la unidad de control.
- b. Establecimiento de cifras de control por lotes antes de entrar la información, y antes de su procesamiento comparar estas cifras con las de la información convertida.
- c. Uso de verificadoras para controlar errores de entrada de información.
- d. Mantenimiento de un procedimiento controlado de corrección de errores.
- e. Uso de conteo de mensajes o procedimientos de transmisión doble cuando se transmite la información entre distintas localidades geográficas.
- f. Conservación de documentos fuente durante períodos razonables, de modo de poder reconstruir la información si fuera necesario.

- g. Uso de dígitos de verificación para detectar errores cometidos por empleados, como pueden ser las transposiciones.

1.7.8 CONTROLES DE PROCESAMIENTO

Los controles de procesamiento de la información deben estar redactados en los programas de computación. Los ejemplos de controles de procesamiento programados comprenden:

- a. *Pruebas de límite.* Este tipo de prueba produce un mensaje de error si cualquier cálculo en una corrida de programas se encuentra fuera de un límite predeterminado.
- b. *Pruebas de lógica.* Esta prueba emitiría un mensaje de error si se produjeran resultados ilógicos en una corrida de programas (un cheque de nóminas negativo).
- c. *Comparaciones de validez.* Estas son pruebas que aseguran si ciertos datos son válidos – por ejemplo, el número de empleados.
- d. *Etiquetas de identificación.* Son códigos magnéticos de identificación apropiada de toda la información antes de su procesamiento.

1.7.9 CONTROLES DE SALIDA

El concepto básico de control de salida es que se deben comparar los totales de las entradas, e investigar y conciliar cualquier diferencia. Esta es una función importante de la unidad de control en el departamento de PED. En muchas compañías los departamentos usuarios llevarán a cabo una función de control similar como una verificación adicional. Para evitar entradas fraudulentas en este punto, todas las correcciones de errores se deben realizar y registrar de acuerdo con procedimientos autorizados. Los procedimientos para la entrega oportuna y apropiada de la información de salida a los usuarios representan un aspecto adicional del control de salidas.

1.7.10 PRUEBAS DE CUMPLIMIENTO

La revisión del auditor sobre el control interno del sistema PED debe estar diseñada de tal modo que se entienda cómo fluyen las operaciones a través del sistema y el grado de controles existentes sobre el proceso. El SAS Núm. 13 (AU 321.24) describe esta revisión como “un proceso de recopilación de información que depende de las preguntas dirigidas de manera inteligente al personal del cliente, la observación de la asignación disponible relacionada con el control contable”.

Para completa la revisión de control interno, el auditor debe llevar a cabo pruebas de cumplimiento para obtener la seguridad razonable que los procedimientos de control interno descrito han sido puestos en práctica. Al realizar estas pruebas el auditor puede observar relaciones de errores, examinar la documentación que muestre las aprobaciones, revisar las operaciones y observar la organización departamental. Se llevan a cabo otras pruebas de cumplimiento utilizando el equipo de PED para procesar información de prueba con el fin de revisar los controles programados en el sistema.

Una vez terminada la evaluación del control interno, el auditor debe determinar cuánta confianza puede depositar en el control interno contable dentro del departamento de PED del cliente. Si los controles dan una base para confiar, el auditor puede limitar la extensión de las pruebas sustantivas de operaciones a llevar a cabo sobre las aplicaciones de PED.

1.8 TÉCNICAS DE AUDITORÍA EN SISTEMAS COMPUTARIZADOS

Las técnicas y procedimientos utilizados por el auditor al realizar pruebas de cumplimiento del sistema y pruebas sustantivas de la información contable dependen en gran parte del diseño del sistema del PED del cliente. El diseño y la operación del sistema definen la naturaleza de las pistas de auditoría que tengan que emplear el auditor para obtener evidencia. Las cuales le permiten al auditor reconstruir y seguir las operaciones, se pueden definir tan bien en un sistema con computadora como en un sistema manual diseñado con propiedad. Por otra parte, en un sistema avanzado PED

con posibilidades de trabajar en línea y pocas copias escritas, podría suceder que las pistas de auditoría no existieran prácticamente.

No obstante, existen muchas razones válidas para que las empresas mantengan en un sistema de PED la posibilidad de reconstruir y seguir las operaciones. Estas incluyen el uso que haga la administración del detalle de la operación, requisitos de auditoría interna y externa, protecciones contra errores o interrupciones del sistema, y requisitos de las autoridades reguladoras y fiscales. De acuerdo con el diseño de la instalación del PED del cliente y la disponibilidad de pistas de auditoría viables, el auditor puede seleccionar procedimientos de auditoría manuales, técnicas de auditoría apoyadas por computadoras o una combinación de las dos.

1.8.1 PROCEDIMIENTOS MANUALES

En los sistemas PED donde existen pistas de auditoría satisfactorias y se dispone de documentos fuente adecuados, el auditor encontrará que los procedimientos manuales de auditoría resultan más efectivos desde el punto de vista de costos que las técnicas con apoyo de computadoras. Esto es parcialmente cierto cuando el volumen de información a examinar es más bien pequeño. En estas situaciones los procedimientos de auditoría utilizados serán del mismo tipo que los usados al auditar sistemas de contabilidad manuales.

1.8.2 TÉCNICAS DE AUDITORÍA APOYADAS POR COMPUTADORAS

En los sistemas de PED en línea que producen poca información escrita y no tienen referencias de auditoría utilizables, es lo más probable que resulten poco efectivas las técnicas manuales de auditoría. Por lo general se necesitan técnicas de auditoría apoyadas por computadoras que use el equipo o los programas del cliente, o ambos. Las técnicas apoyadas por las computadoras más usuales son:

- a. El uso de información de pruebas para verificar los controles programados para comprobar el cumplimiento,
- b. El uso de programas de auditoría generalizados para extraer información del

sistema y realizar otras funciones relacionadas con las pruebas sustantivas.

1.8.3 USO DE LA INFORMACIÓN DE PRUEBA

Al utilizar la información de prueba para obtener conclusiones respecto a la operación de un programa de computación, el auditor desarrolla información similar a la que procesa normalmente el programa. Después se procesa la información de prueba bajo condiciones controladas utilizando el programa del cliente. Cuando se obtiene la información procesada resultante, se compara con los resultados predeterminados manualmente para tener la seguridad de que se procesó de manera apropiada la información de prueba.

Al desarrollar información de prueba los auditores deben incluir operaciones que reflejen aquellas condiciones válidas y no válidas que se desean verificar. El enfoque de información de prueba da a los auditores la seguridad respecto a la operación del programa de su cliente en un momento en el tiempo. De la prueba el auditor puede llegar a la conclusión de que las operaciones válidas fueron procesadas con propiedad y que las operaciones no válidas con reconocidas por los controles programados y se producen los adecuados mensajes de aviso de error.

1.8.4 USO DE PROGRAMAS GENERALIZADOS DE AUDITORÍA

Existe una amplia variedad de paquetes de programas generalizados de auditoría que realizan muchos trabajos para apoyar al auditor en la realización de pruebas sustantivas y en otros aspectos de la auditoría. El uso de estas herramientas con frecuencia aumenta tanto la eficiencia como la efectividad de la auditoría de un cliente que usa sistemas de computadora.

Se diseña el programa de auditoría para correrlo en el sistema de computación del cliente, en el sistema propio del auditor o mediante un arreglo de tiempo compartido. Aunque los diversos paquetes de programas de que se dispone son un poco diferentes en sus posibilidades de auditoría, entre los trabajos que se llevan a cabo con más frecuencia se encuentran los siguientes:

- a. Selección e impresión de muestras de auditoría sobre bases estadísticas o no estadísticas.
- b. Verificación matemática de sumas, multiplicaciones y otros cálculos en los archivos de información del cliente.
- c. Realización de funciones de revisión analítica al establecer comparaciones, calcular razones, identificar fluctuaciones y llevar a cabo cálculos de regresión múltiple.
- d. Manipulación de la información al calcular subtotales, sumar y clasificar información, volver a ordenar en serie la información, etc.
- e. Preparación de balances de comprobación, estados financieros, solicitudes de confirmación, papeles de trabajo de auditoría.
- f. Examen de los registros de acuerdo con criterios especificados; por ejemplo, verificación de los límites de crédito excedidos, números de empleados válidos, cantidades negativas y operaciones en exceso de importes especificados.
- g. Varias funciones de comparación, tales como comparar las cantidades físicas de los inventarios con las cantidades de libros.

1.9 AUDITORIA EN UN AMBIENTE DE SISTEMAS DE INFORMACIÓN POR COMPUTADORA. (NIAS)

1.9.1 INTRODUCCIÓN

1. El propósito de esta Norma Internacional de Auditoría (NIA) es establecer normas y proporcionar lineamientos sobre los procedimientos que deben seguirse cuando se conduce una auditoría en un ambiente de Sistemas de Información Computarizada (SIC)⁴. Para fines de las NIAs, un ambiente SIC existe cuando está involucrada una computadora de cualquier tipo o tamaño en el procesamiento por la entidad de información financiera de importancia para la auditoría, ya sea que dicha computadora sea operada por la entidad o por una tercera parte.

⁴ Este término se utiliza en esta NIA en lugar de procesamiento electrónico de datos (PED) utilizado en la NIA anterior "Auditoría en un Entorno de PED"

2. El auditor deberá considerar como afecta a la auditoría en un ambiente SIC. Sin embargo, el uso de una computadora cambia el procesamiento, almacenamiento y comunicación de la información financiera y puede afectar los sistemas de contabilidad y de control interno empleados por la entidad. Por consiguiente, un ambiente SIC puede afectar:
- Los procedimientos seguidos por un auditor para obtener una comprensión suficiente de los sistemas de contabilidad y de control interno.
 - La consideración del riesgo inherente y del riesgo de control a través de la cual el auditor llega a la evaluación del riesgo.
 - El diseño y desarrollo por el auditor de pruebas de control y procedimientos sustantivos apropiados para cumplir con el objetivo de la auditoría.

1.9.2 HABILIDAD Y COMPETENCIA

4. El auditor debería tener suficiente conocimiento del SIC para planear, dirigir, supervisar y revisar el trabajo desarrollado. El auditor debería considerar si se necesitan habilidades especializadas en SIC en una auditoría. Estas pueden necesitarse para:
- Obtener una suficiente comprensión de los sistemas de contabilidad y de control interno afectados por el ambiente SIC.
 - Determinar el efecto del ambiente SIC sobre la evaluación del riesgo global y del riesgo al nivel de saldo de cuenta y de clase transacción.
 - Diseñar y desempeñar pruebas de control y procedimientos sustantivos apropiados.

Si se necesitan habilidades especializadas, el auditor buscaría la ayuda de un profesional con dichas habilidades, quien puede pertenecer al personal del auditor o ser un profesional externo. Si se plantea el uso de dicho profesional, el auditor debería obtener suficiente evidencia apropiada de auditoría que dicho trabajo es adecuado para los fines de la auditoría, de acuerdo con NIA “Uso del Trabajo de un Experto”.

1.9.3 PLANEACIÓN

5. De acuerdo con NIA “Evaluaciones del Riesgo y Control Interno” el auditor debería obtener una comprensión de los sistemas de contabilidad y de control interno, suficiente para planear la auditoría y desarrollar un enfoque de auditoría efectivo.
6. Al planear las porciones de la auditoría que pueden ser afectadas por el ambiente de SIC del cliente, el auditor debería obtener una comprensión de la importancia y complejidad de las actividades del SIC y la disponibilidad de datos para uso en la auditoría. Esta comprensión incluiría asuntos como:
 - La importancia y complejidad del procesamiento por computadora en cada operación importante de contabilidad. La importancia se refiere a la importancia relativa de las aseveraciones de los estados financieros afectadas por el procesamiento por computadora. Se puede considerar como compleja una aplicación cuando, por ejemplo:
 - El volumen de transacciones es tal que los usuarios encontrarían difícil identificar y corregir errores en el procesamiento.
 - La computadora automáticamente genera transacciones o entradas de importancia relativa directamente a otra aplicación.
 - La computadora desarrolla cálculos complicados de información financiera y/o automáticamente genera transacciones o entradas de importancia relativa que pueden ser (o no son) validadas independientemente.
 - Las transacciones son intercambiadas electrónicamente con otras organizaciones (como en los sistemas electrónicos de intercambio de datos – EDI) sin revisión manual para la propiedad o razonabilidad.
 - La estructura organizacional de las actividades SIC del cliente y el grado de concentración o distribución del procesamiento por computadora en toda la entidad, particularmente en cuanto pueden afectar la segregación de deberes.

- La disponibilidad de datos. Los documentos fuente, ciertos archivos de computadora, y otro material de evidencia que pueden ser requeridos por el auditor, pueden existir por un corto periodo de tiempo o sólo en forma legible por computadora. El SIC del cliente puede generar reportes internos que pueden ser útiles para llevar a cabo pruebas sustantivas (particularmente procedimientos analíticos). El potencial de uso de técnicas de auditoría con ayuda de computadora puede permitir una mayor eficiencia en el desempeño de los procedimientos de auditoría, o puede capacitar al auditor a aplicar en forma económica ciertos procedimientos a una población completa de cuentas o transacciones.
7. Cuando el SIC es significativo, el auditor deberá también obtener una comprensión del ambiente SIC y de si puede influir en la evaluación de los riesgos inherentes y de control. La naturaleza de los riesgos y las características del control interno en SIC incluyen lo siguiente:
- Falta de rastros de las transacciones. Algunos SIC son diseñados de modo que un rastro completo de una transacción, que podría ser útil para fines de auditoría podría existir por sólo un corto período de tiempo o sólo en forma legible por computadora. Donde un sistema complejo de aplicaciones desempeña un gran número de pasos de procesamiento, puede no haber un rastro completo. Por consiguiente, los errores incrustados en la lógica de un programa de aplicaciones pueden ser difíciles de detectar oportunamente por procedimientos (usuarios) manuales.
 - Procesamiento uniforme de transacciones. El procesamiento por computadora procesa uniformemente transacciones iguales con las mismas instrucciones de procesamiento. Así, los errores de oficina ordinariamente asociados con el procesamiento manual son virtualmente eliminados. Por el lado contrario, la programación de errores (u otros errores sistemáticos en el hardware o software)

ordinariamente dará como resultado que todas las transacciones sean procesadas incorrectamente.

- Falta de segregación de funciones. Muchos procedimientos de control que ordinariamente serían desempeñados por individuos por separado en los sistemas manuales, pueden ser concentrados en SIC. Así, un individuo que tiene acceso a los programas de computadora, al procesamiento o a los datos, puede estar en posición de desempeñar funciones incompatibles.
- Potencial para errores e irregularidades. El potencial para error humano en el desarrollo, mantenimiento y ejecución de SIC puede ser mayor que en los sistemas manuales, parcialmente a causa del nivel de detalle inherente a estas actividades. También, el potencial para que los individuos ganen acceso no autorizado a los datos o a la alteración de datos sin evidencia visible puede ser mayor en SIC que en los sistemas manuales.
- Además, la disminución de involucramiento humano en el manejo de transacciones procesadas por el SIC puede reducir el potencial para observar errores e irregularidades. Los errores o irregularidades que ocurren durante el diseño o modificación de programas de aplicación o del software de los sistemas pueden permanecer sin detectar por largos períodos de tiempo.
- Iniciación o ejecución de transacciones. El SIC puede incluirla capacidad de iniciar automáticamente. La autorización de estas transacciones o procedimientos puede no estar documentada en la misma forma que en el sistema manual, y la autorización de la administración de estas transacciones puede estar implícita en su aceptación del diseño SIC y modificación subsecuente.
- Dependencia de otros controles del procesamiento por computadora. El procesamiento por computadora puede producir reportes y otros datos de salida que son usados en el desempeño de procedimientos de control que son usados en

el desempeño de procedimientos de control manuales. La efectividad de estos procedimientos de control manuales puede depender de la efectividad de controles sobre la integralidad y precisión del procesamiento por computadora. A su vez, la efectividad y operación consistente de los controles del procesamiento de transacciones en las aplicaciones de computadora a menudo depende de la efectividad de los controles generales de SIC.

- Potencial para mayor supervisión de la administración. SIC puede ofrecer a la administración una variedad de herramientas analíticas que pueden ser usadas para revisar y supervisar las operaciones de la entidad. La disponibilidad de estos controles adicionales, si se usan, puede servir para mejorar toda la estructura de control interno.
- Potencial para el uso de técnicas de auditoría con ayuda de computadora. El caso del procesamiento y análisis de grandes cantidades de datos usando computadoras puede brindar al auditor oportunidades para aplicar técnicas y herramientas generales o especializadas de auditoría con computadora en la ejecución de pruebas de auditoría.

Tanto los riesgos como los controles introducidos como resultado de estas características d SIC tienen un impacto potencial sobre la evaluación del auditor del riesgo, y sobre la naturaleza, oportunidad y alcance de los procedimientos de auditoría.

1.9.4 EVALUACIÓN DEL RIESGO.

8. De acuerdo con NIA “Evaluación del riesgo y control interno”, el auditor debería hacer una evaluación de los riesgos inherente y de control para las aseveraciones importantes de los estados financieros.
9. Los riesgos inherentes y los riesgos de control en un ambiente SIC pueden tener tanto un efecto general como un efecto específico en la probabilidad de representaciones erróneas importantes, como sigue:

- Los riesgos pueden resultar de deficiencias en actividades generales de SIC como desarrollo y mantenimiento de programas, soporte al software de sistemas, operaciones, seguridad física de SIC, y control sobre el acceso a programas de utilería de privilegio especial. Estas deficiencias tenderían a tener un efecto penetrante en todos los sistemas de aplicación que se procesan en la computadora.
 - Los riesgos pueden incrementar el potencial de errores o actividades fraudulentas en aplicaciones específicas, en bases de datos específicas o en archivos maestros, o en actividades de procesamiento específicas. Por ejemplo, los errores no son poco comunes en los sistemas que desarrollan condiciones de excepción. Los sistemas que controlan desembolsos de efectivo u otros activos líquidos son susceptibles a acciones fraudulentas por los usuarios o por personal de SIC.
10. Al surgir nuevas tecnologías de SIC, frecuentemente son empleadas por los clientes para construir sistemas de computación cada vez más complejos que pueden incluir enlaces micro a redes, bases de datos distribuidas, procesamiento de usuario final, y sistemas de administración de negocios que alimentan información directamente a los sistemas de contabilidad. dichos sistemas aumentan la sofisticación total de SIC y las complejidad de las aplicaciones a las que afecta. Como resultado, pueden aumentar el riesgo y requerir una consideración adicional.

1.9.5 PROCEDIMIENTOS DE AUDITORIA

11. De acuerdo con NIA “Evaluaciones del riesgo y control interno” el auditor debería considerar el ambiente de SIC al diseñar los procedimientos de auditoria para reducir el riesgo de auditoria a un nivel aceptable bajo.
12. Los objetivos específicos de auditoria del auditor no cambian ya sea que los datos de contabilidad se procesen manualmente o por computadora. Sin embargo, los métodos de aplicación de procedimientos de auditoría para reunir evidencia pueden ser

influenciados por los métodos de procesamiento por computadora. El auditor puede usar procedimientos de auditoría manuales, técnicas de auditoría con ayuda de computadora, o una combinación de ambos para obtener suficiente material de evidencia. Sin embargo, en algunos sistemas de contabilidad que usan una computadora para procesar aplicaciones significativas, puede ser difícil o imposible para el auditor obtener ciertos datos para inspección, investigación, o confirmación sin la ayuda de la computadora.

1.10 AUDITORIA EN INFORMÁTICA

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

La auditoría en informática deberá comprender no sólo la evaluación de los equipos de cómputo o de un sistema o procedimiento específico, sino que, además, habrá de evaluar los sistemas de información en general, desde sus entradas, procedimientos controles, archivos, seguridad y obtención de la información. Ello debe incluir los equipos de cómputo como la herramienta que permite obtener la información adecuada y la organización específica (departamento de cómputo, departamento de informática, gerencia de procesos electrónicos) que hará posible el uso de los equipos de cómputo.

1.10.1 CAMPO DE ACCIÓN

Desde que la informática se enfocó hacia el apoyo de la sistematización en las áreas del negocio, se empezaron a implantar aplicaciones administrativas como contabilidad, nóminas, etc., lo cual originó lo que se conoce como auditoría a sistemas de información.

Posteriormente, el uso de la informática cubrió las áreas de negocio en todos los niveles con productos y servicios muy variados; proliferaron las minicomputadoras o equipos departamentales; después llegaron las microcomputadoras o computadoras personales y entraron de lleno las redes locales, la integración empresarial a través de las telecomunicaciones y un gran número de componentes de tecnología. Tal tecnificación del medio imposibilitó al responsable de informática y a los auditores de sistemas tradicionales seguir evaluando este campo con métodos y procedimientos anticuados.

Se hizo necesario un replanteamiento del fondo y forma de la auditoría en informática. Este trabajo busca, entre otras cosas, dar una dimensión más realista y adecuada a la auditoría en informática.

El ejercicio práctico y formal de la auditoría en informática brindará a sus ejecutantes y a los negocios un sentimiento de satisfacción justificado por el entendimiento y compromiso que implica asegurar el uso correcto de los recursos de informática para el logro de las estrategias.

Conviene recordar que en las empresas existen objetivos comunes a todas las áreas respecto de los recursos de informática; por ejemplo, el máximo uso y aprovechamiento de la tecnología mediante políticas, procedimientos y métodos apropiados. En este sentido, la función de la auditoría en informática es una de los medios más importantes y especializados para lograr dicho fin.

1.10.2 EVALUACIÓN ADMINISTRATIVA DEL DEPARTAMENTO DE INFORMÁTICA

- Los objetivos del departamento, dirección o gerencia
- Metas, planes, políticas y procedimientos de procesos electrónicos estándar
- Organización del área y su estructura orgánica.
- Funciones y niveles de autoridad y responsabilidad del área de procesos electrónicos
- Integración de los recursos materiales y técnicos
- Dirección

- Costos y controles presupuestales
- Controles Administrativos del área de procesos electrónicos

1.10.3 EVALUACIÓN DE LOS SISTEMAS, PROCEDIMIENTOS Y EFICIENCIA DE LA INFORMACIÓN

- Evaluación del análisis de los sistemas y sus diferentes etapas
- Evaluación del diseño lógico del sistema
- Evaluación del desarrollo físico del sistema
- Control de proyectos
- Control de sistemas de programación
- Instructivos y documentación
- Formas de implantación
- Seguridad física y lógica de los sistemas
- Confidencialidad de los sistemas
- Controles de mantenimiento y forma de mantenimiento de los sistemas
- Utilización de los sistemas.

1.10.4 EVALUACIÓN DEL PROCESO DE DATOS Y DE LOS EQUIPOS DE CÓMPUTO.

- Control de los datos fuente y manejo de cifras de control
- Control de operación
- Control de salida
- Control de asignación de trabajo
- Control de medios de almacenamiento masivo
- Seguridad física y lógica
- Confidencialidad
- Respaldos

1.10.5 LA IMPORTANCIA DE LA AUDITORÍA EN INFORMÁTICA.

La tecnología de informática, traducida en hardware, software, sistemas de información, investigación tecnológica, redes locales, bases de datos, ingeniería de software, telecomunicaciones, servicios y organización de informática es una herramienta

estratégica que brinda rentabilidad y ventaja competitiva a los negocios frente a sus similares en el mercado; pero puede originar costos y desventajas competitivas si no es bien administrada y dirigida por el personal encargado.

Dados los extremos señalados, surgen de inmediato un par de preguntas:

¿Cómo saber si estoy administrando y dirigiendo de manera correcta la función de informática?

La respuesta siempre ha existido: mediante evaluaciones oportunas y completas de dicha función por personal calificado (o sea, consultores externos, auditores en informática), o evaluaciones periódicas por el mismo personal de informática entre otras estrategias.

¿Es necesario auditar o evaluar la función de informática y quienes lo harían?

Aquí la respuesta depende de cada organización y de sus necesidades por conocer el estado real de su tecnología en informática.

Lo que resulta innegable es que la informática se convierte cada día en una herramienta permanente de los procesos principales de los negocios, en una fuerza estratégica, un aliado confiable y oportuno. Todo lo anterior es posible tenerlo en la empresa si se implantan controles y esquemas de seguridad requeridos para su aprovechamiento óptimo.

Una vez que la alta dirección tome conciencia de lo saludable y productivo que es contar con un área independiente que asegure y promueva el buen uso y aprovechamiento de la tecnología de informática, el siguiente paso es delegar la responsabilidad en personal altamente capacitado para ejercer la auditoría en informática dentro de la organización de manera formal y permanente.

RESUMEN

Siempre ha existido la filosofía de las organizaciones con respecto a llevar controles y procedimientos de todos los procesos, productos y datos considerados como activos

estratégicos. En el terreno de los sistemas de información y tecnología, un alto porcentaje de las empresas tiene problemas en el manejo y control tanto de los datos como de los elementos en que almacena, procesa y distribuye la información.

Esta situación genera tiempos de respuesta inadecuados en la recopilación, proceso y entrega de resultados; asimismo, origina incertidumbre acerca de la productividad de los recursos involucrados en la operación diaria de los datos y cuestiona de manera permanente la rentabilidad de la informática. Es una voz de alerta que se debe escuchar.

En forma adicional, cabe señalar que muchas compañías sólo creen que es necesario proteger la información que se maneja, por medio de recursos tecnológicos, mas no por ello están dispuestas a invertir dinero, tiempo y compromiso para minimizar o eliminar dicha problemática.

A lo anterior hay que agregar la presencia de dos grandes grupos de problemas:

- a. Falta de conocimiento del alcance de los sistemas de información, que en la práctica se traduce en meras actividades “apaga fuegos”, falta de estándares en software y hardware, así como usuarios valientes que desarrollan soluciones por su cuenta sin los requisitos metodológicos necesarios.
- b. Capacitación inadecuada a los usuarios y casi nula al personal de informática respecto del uso de metodología de planeación y desarrollo para la administración de sus funciones; insatisfacción de los usuarios clave del negocio por los resultados producidos por el departamento de informática, que termina calificada como “mala, vanidosa y cara”

Lo anterior se repite en gran número de compañías; por lo tanto, la pregunta inminente es: ¿por qué si se gasta tanto en informática y no da resultados no se deciden a desecharla o a usarla como debe ser?. Simplemente porque no saben que hacer con ella. Unos la desprecian por que no la entienden y otros, que le temen por su incapacidad para usarla y administrarla, le dan el beneficio de la duda.

Por ello, se concluye que el primer paso para detectar el grado de confianza, disponibilidad y rentabilidad de la información y de los recursos de informática es la aceptación de la dirección o accionistas de los beneficios que brinda dicha tecnología; el segundo es asegurar la custodia y protección de la misma.

Se requiere, además, la dimensión real del escenario tecnológico y del control existente a través de un estudio preliminar o diagnóstico de la situación actual. Después, todo recaerá en el compromiso que la alta dirección y los empleados asuman para dar solución oportuna a las debilidades o carencias que emanen de dicho análisis.

El incremento permanente de las expectativas y necesidades relacionada con la informática, al igual que la actualización continua de los elementos que componen la tecnología de este campo, obligan a las entidades que la aplican a contar con controles, políticas y procedimientos que aseguren a la alta dirección que los recursos humanos, materiales y financieros involucrados son protegidos adecuadamente y que se orienten a la rentabilidad y competitividad del negocio.

¿Por qué preocuparse de cuidar esa caja etiquetada con el nombre de informática?

Si la respuesta que brinde a cualquiera de las siguientes preguntas es negativa, le convendría reafirmar o considerar o considerar la necesidad de asumir la responsabilidad de controlar y brindar seguridad permanente a los recursos de informática:

- a. ¿Los usuarios y la alta dirección conocen la situación actual de función de informática en la empresa (organización, políticas, servicios, etc.)?
- b. ¿Se aprueba y formal y oportunamente el costo/beneficio de cada proyecto relacionado en forma directa con la informática?
- c. ¿La informática apoya las áreas críticas del negocio?
- d. ¿El responsable de la informática conoce los requerimientos actuales y futuros del negocio que necesitan apoyo de los servicios y productos de su área?

- e. ¿Todos los elementos del negocio conocen las políticas y procedimientos inherentes al control y seguridad de la tecnología de informática?
- f. ¿Existen dichas políticas y procedimientos de manera formal?
- g. ¿Hay un plan de seguridad en la informática?
- h. ¿Se ha calculado el alcance e impacto de la informática en la empresa?
- i. ¿Existen responsables que evalúen formal e imparcialmente la función de informática?
- j. ¿Se cuenta con un control formal de cada proyecto relativo al área?
- k. ¿Es importante para Ud. la informática?
- l. ¿Evalúa periódicamente y formalmente dicha función de la informática?
- m. ¿Auditan sólo sistemas de información y no otras áreas de la informática?

Cada una de estas preguntas encierra una importancia específica para el buen funcionamiento informático en cualquier negocio; todas están interrelacionadas y la negación de alguna es una pequeña fuga de gas que – con el tiempo y un pequeño chispazo – puede ocasionar graves daños a los negocios, sean estos traducidos en fraudes, proyectos cancelados con alto porcentaje de costos no recuperables, rechazo de los servicios de informática por los usuarios clave del negocio, improductividad y la baja calidad de los recursos de informática, planes de informática no orientados a las metas y estrategias de negocio, piratería de software, fuga de información a la competencia o proveedores, entre otros daños.

La improductividad, el mal servicio y la carencia de soluciones totales de la función de informática fueron, son y pueden seguir siendo mal de muchas organizaciones.

El problema real radica en que todos los proyectos prioritarios hacen gala de sentirse apoyados por la informática; entonces, ¿por qué no cuidarla?

En seminarios, pláticas de comedor o pasillo en empresas (así como en instituciones de gobierno y escuelas universitarias) y aun en las mismas áreas o departamentos de informática se relatan los problemas más comunes de los usuarios y del personal.

Sin embargo, parece ser que un gran porcentaje de tales interlocutores no se percata o no desea reconocer que esta problemática se ha venido planteando desde hace muchos años por las mismas causas y con los mismos efectos negativos para la organización. La diferencia puede ser que ahora los individuos que cometen estas fallas o debilidades funcionales están dispersos por toda la organización utilizando tecnología supuestamente más eficiente y, por supuesto, más cara. Algunos problemas de esta índole son:

- Debilidades en la planeación del negocio al no involucrar la informática.
- Resultados negativos (improductividad, duplicidad de funciones, etc.) en el desarrollo, operación y mantenimiento de sistemas de información.
- Falta de actualización del personal de informática y técnico donde se encuentran instalados los sistemas y las soluciones del negocio.
- Mínimo o nulo involucramiento de los usuarios en el desarrollo e implantación de soluciones de informática.
- Capacitación deficiente en el uso de los sistemas de información, el software y el hardware.
- Administración débil o informal de proyectos.
- Carencia de un proceso de análisis Costo/beneficio formal previo al arranque de cada proyecto de informática
- Metodología de planeación y desarrollo de sistemas informales no estandarizadas y en muchos casos inexistentes.
- Uso y entendimiento mínimo o inexistente de técnicas formales para el desempeño de funciones en las áreas de informática:
 - Análisis
 - Entrevistas
 - Cuestionarios
 - Modelación de datos
 - Costo/beneficio, etc.

- Falta un proceso formal de planeación de informática.
- Involucramiento mínimo o informal de la alta dirección en los proyectos de informática.
- Proyectos de auditoría o evaluación de informática esporádicos e informales.

1.10.6 ELEMENTOS DE AUDITORÍA EN INFORMÁTICA

Definición de Auditoría en Informática
<p>Es la revisión , evaluación de <i>controles, sistemas, procedimientos de informática de los equipos de cómputo, su utilización, eficiencia y seguridad de la organización</i> que participan en el procesamiento de la información a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones. Evaluando no solamente los equipos de cómputo o de un sistema específico, sino también, los sistemas de información en general</p>



Elementos de la definición	
Elemento	Información Generada
<p>a. Controles para los procesos electrónicos.</p>	<p>a. Proporciona los objetivos, dirección, gerencia, metas, planes y procedimientos, de los procesos electrónicos estándar, la organización funciones y autoridad, así como la responsabilidad que existe en los procesos electrónicos, los recursos que interrelacionan y los costos en que incurra.</p>



<p>b. Sistemas y procedimientos de informática.</p>	<p>b. Proporciona el análisis de los sistemas, sus etapas, el diseño, la evaluación del desarrollo físico, su programación e implementación, la seguridad física y lógica, la confidencialidad, la forma de respaldo que proporciona, así como el mantenimiento y utilización de los sistemas en su conjunto.</p>
---	---



c. Equipos de cómputo.	c. Se refiere a todos los equipos o software, su interrelación, el ordenamiento, la seguridad física, la confidencialidad en la generación de la información.
------------------------	---



d. Eficiencia y seguridad en la organización para la generación de la información	d. Proporciona los medios para lograr la eficiencia y seguridad en la generación de información en cuanto a control de la fuente y manejo de las cifras. Control de las operaciones entradas y salidas de la información, medios de almacenamiento, seguridad y confidencialidad de la información generada.
---	--



Elementos	Como se Auditan
a. Controles para los procesos electrónicos. b. Sistemas y procedimientos de informática. c. Equipos de cómputo. d. Eficiencia y seguridad en la organización para la generación de la información	<p>TÉCNICAS</p> <ul style="list-style-type: none"> ▪ Análisis ▪ Inspección física ▪ Investigación ▪ Observación ▪ Cuestionarios y narrativas <p>PROCEDIMIENTOS</p> <ul style="list-style-type: none"> ▪ Se diseña el cuestionario de acuerdo a las áreas, procesos de control en informática. ▪ Se entrega al departamento de informática para que sea contestado. ▪ Se tabula y analizan las respuestas ▪ Se determinan las áreas críticas y sus debilidades para darle seguimiento mediante pruebas. <p>NORMATIVA</p> <ul style="list-style-type: none"> ▪ Párrafo 401 de las Normas Internacionales de Auditoría ▪ SAS ▪ Normas Internacionales de Auditoría ▪ NAGAS, en la referente a cualquier proceso de auditoría. ▪ Normas de Contabilidad Financiera, en lo referente al cumplimiento a principios a principios de contabilidad.

1.10.7 PROCESO DE UNA AUDITORIA EN INFORMÁTICA

PRIMERA FASE. Estudio preliminar, obligatorio y necesario efectuar en todas las empresas que usen en alguna forma el PED para la obtención de su información financiera.

SEGUNDA FASE. Ampliación del estudio del Control Interno. De aplicación obligatoria cuando en el estudio preliminar se ha determinado que se tiene aplicaciones de importancia para la obtención de la información financiera, que existen transformaciones importantes en la información y de que el auditor tiene que confiar en una medida importante en el control interno que existe sobre dichas aplicaciones.

TERCERA. Pruebas de los controles PED. De aplicación obligatoria cuando la importancia de los sistemas sujetos a proceso sea tal en cuanto a las transformaciones y al grado de confianza que el auditor depositará en el control interno, que el no efectuar pruebas de cumplimiento a los controles PED limita el alcance del trabajo del auditor al no obtener evidencia suficiente y competente. Habrá casos que el auditor, tenga necesariamente que confiar en el control interno del PED y, por lo tanto, tenga que evaluarlo y después probarlo en forma completa e integral a través de pruebas de cumplimiento. También habrá casos, que por el resultado esperado de sus pruebas sustantivas, de importancia relativa y de riesgo probable, el auditor obtendrá la necesaria evidencia suficiente y competente que le permita solamente evaluar ciertos controles internos importantes y reducir sustancialmente sus pruebas de cumplimiento, limitándolas estas a probar controles internos importantes de entrada y salida, y por lo tanto solamente cumplir con la primera fase y, según las circunstancias, cubrir parcialmente la segunda y omitir la tercera.

Es importante señalar que desde la primera fase se requiere de experiencia en auditoría en PED por parte del auditor y conforme se vayan pasando a las siguientes fases se requerirá de mayor capacitación.

1.10.8 OBJETIVOS DE LOS PROCEDIMIENTOS DE LA AUDITORIA EN INFORMÁTICA

Los objetivos en la primera fase, estudio preliminar, son los siguientes:

- a. Determinar las principales aplicaciones y su efecto en la información financiera.
- b. Conocer las características del equipo PED.
- c. Concluir sobre el efecto del PED en la información financiera y, en su caso, pasar a la segunda fase.

Los objetivos en la segunda fase, ampliación del estudio del control interno, son los siguientes:

- a. Evaluar la organización del centro de cómputo y los controles generales establecidos.
- b. Conocer las características de las aplicaciones y evaluar los controles de aplicación o específicos inherentes a las mismas, considerando el grado de transformación de la información y el volumen de operaciones que dependen del PED, a efecto de poder juzgar si se deben efectuar pruebas de cumplimiento de los controles PED.
- c. Formarse un juicio sobre la eficacia del control interno existente en PED que permita determinar la naturaleza, el alcance y oportunidad de los procedimientos de auditoría, tanto de cumplimiento, como sustantivos.
- d. Concluir sobre los resultados obtenidos y, en su caso, pasar a la tercera fase, considerando que el no probar los controles PED resultaría en una limitación importante en el trabajo del auditor, pues no se obtendrá la necesaria evidencia suficiente y competente.

El objetivo de la tercera fase, pruebas de los controles PED, es probar los controles específicos de las aplicaciones mediante pruebas de cumplimiento.

1.11 PROCEDIMIENTOS DE EVALUACIÓN DE AUDITORIA EN INFORMATICA

1.11.1 PRIMERA FASE – ESTUDIO PRELIMINAR

El estudio preliminar está enfocado a determinar la importancia que el PED tiene en la información financiera y al conocimiento general del equipo.

DESCRIPCIÓN DE LAS APLICACIONES

Consiste en conocer y documentar en papeles de trabajo las principales aplicaciones, volúmenes de operación, objetivos del sistema y de sus aplicaciones, identificando la entrada, proceso y salida de la información por cada aplicación, teleprocesos, etc. Pudiendo con ello determinar la información que se obtiene y procesa a través del PED y su repercusión en los estados financieros.

ESTUDIO GENERAL DEL EQUIPO DE COMPUTO

Descripción de la unidad central de proceso y de las unidades periféricas, incluyendo datos tales como capacidad de memoria, sistema operativo, base de datos, comunicaciones, capacidad en pantalla remotas, modelo, antigüedad, etc.

CONCLUSIÓN

Documentar ésta, de tal forma que respalde la decisión del auditor de continuar o no a la segunda fase.

1.11.2 SEGUNDA FASE – AMPLIACIÓN DEL ESTUDIO DEL CONTROL INTERNO.

La ampliación del estudio del control interno está enfocada a conocer con más detalle las características de los sistemas y de formarse un juicio sobre la eficiencia de los controles internos.

REVISIÓN DE LOS ESTUDIOS DE VIABILIDAD

De esta forma se conocerá si la selección del equipo fue hecha en forma cuidadosa y si responde a las necesidades particulares de la empresa.

ANÁLISIS DE LA ORGANIZACIÓN DEL CENTRO DE CÓMPUTO

Cerciórese de que no exista incompatibilidad de funciones, que se tenga un buen soporte técnico, que existan líneas de autoridad definidas, que haya una planeación a corto y largo plazo y, en general, se cuenten con políticas definidas y acordes a la importancia del departamento. También se debe revisar que existan procedimientos, autorización de cambios a los sistemas y fijar los estándares para el desarrollo de los sistemas. En sistemas pequeños donde no es posible la existencia de todos los controles, deberá determinarse la existencia de controles compensatorios que cubran dicha deficiencia.

ANÁLISIS DE LOS SISTEMAS

Verificar que el análisis, diseño, programación, prueba de datos y mantenimiento de los sistemas esté documentado y de acuerdo a los estándares establecidos, juzgando a su vez lo apropiado de dichos estándares y del flujo de la información.

EXISTENCIA DE MANUALES OPERATIVOS

Comprobar que existan manuales actualizados de operación del equipo y de los sistemas en operación y de que exista una historia de los cambios en los manuales, y sus causas, etc.

CONTROLES SOBRE BITÁCORA

Verificar que exista una bitácora del centro de cómputo donde se registren los tiempos de proceso, cambios de programas, descomposturas, mantenimiento, operadores, etc. Y que exista supervisión adecuada y oportuna de esta bitácora.

CONTINGENCIAS

Cerciorarse de que existe un plan de contingencias que asegure una continuidad razonable de la información.

EXISTENCIA DE PLANES CONTRA FALLAS

Investigar si en caso de fallas se cuenta con un equipo de soporte y procedimientos de reinicio.

CONTROLES SOBRE PROCESO

Verificar que la información procesada está sujeta a controles que aseguren que dicha información es válida y completa y que no se procesa información errónea y duplicada. Determinar el grado de transformación de la información y asegurar que existan huellas o pistas que permitan la reconstrucción o seguimiento de la información procesada y de su transformación. En caso de información rechazada, que ésta sea analizada, corregida y evitada para el futuro y, en su caso, vuelva a ser oportunamente procesada. Asimismo, debe verificarse que toda la información procesada este previamente autorizada.

DOCUMENTACIÓN DE LOS PROGRAMAS

Comprobar que la documentación que soporta los programas está de acuerdo con los estándares establecidos, que se encuentra completa y que exista evidencia y autorización de los cambios efectuados.

EXISTENCIA DE MANUALES CON LOS USUARIOS

Verificar la existencia de manuales actualizados para los usuarios.

PROTECCION DE SISTEMAS

Verificar que copias actualizadas de la documentación de los sistemas estén debidamente protegidos.

PROTECCIÓN DE LOS ARCHIVOS

Cerciorarse de que existen copias actualizadas de los archivos maestros y de las transacciones, conservándose por un tiempo razonable en un lugar seguro, tanto en un edificio distinto al del centro de cómputo, como una copia en el mismo centro.

ELEMENTOS DE SEGURIDAD FÍSICA

Comprobar la seguridad física del centro de cómputo y determinar si el equipo está en un lugar que asegure la separación de funciones entre el personal y el acceso restringido al área. Que se cuente con extintores, detectores de humo y medidas razonables contra posibles sabotajes y cobertura adecuada de seguros mediante una evaluación profesional de los riesgos a que está sujeto tanto el equipo como la información.

AUDITORIA INTERNA

Evaluar el trabajo de auditoría interna y revisar sus reportes.

CONTROLES PARA CENTRO DE CÓMPUTO EXTERNO

Cuando el PED se realice en un centro de cómputo externo, los procedimientos aplicables son los siguientes:

- i. Revisión del contrato para comprobar que es adecuado a las circunstancias de la empresa y que se está cumpliendo con las condiciones estipuladas, así como si existe una revisión periódica del mismo para adecuarlo a las necesidades de la empresa.
- ii. Recabar informes sobre el soporte técnico y la solvencia del centro de cómputo, con el objeto de evaluar la confiabilidad.
- iii. Investigar sobre las alternativas que se ofrecen en caso de que el centro no pueda procesar la información.
- iv. Verificar el flujo de la información del y al centro de cómputo y de los informes obtenidos, así como la actualización de los archivos maestros y de transacciones y de la seguridad de los mismos.

- v. Verificar los procedimientos que ha seguido la empresa para asegurarse de la validez de la información.
- vi. Cuando las aplicaciones son de importancia, debe evaluarse la necesidad de efectuar una revisión directa del auditor en centro de cómputo.

1.11.3 TERCERA FASE - PRUEBAS A LOS CONTROLES PED

Las pruebas a los controles PED están entonces enfocadas a que el auditor obtenga evidencia de que los sistemas PED funcionan como los determinó en la fase II. Es importante mencionar que a partir de esta fase es imprescindible que el auditor tenga la debida especialización y conocimiento de cómputo electrónico que le permita juzgar sobre los controles establecidos y efectuar pruebas al computadora.

En caso de apoyarse en otras personas, el auditor deberá tener suficientes conocimientos PED para dirigir, supervisar y revisar el trabajo de sus asistentes o para obtener la certeza razonable de que el trabajo hecho por expertos externos con conocimientos de PED, es adecuado en las circunstancias. Mas aun, cuando el PED es parte integrante del sistema contable y del control interno relativo, el auditor no debe delegar en un experto en PED su responsabilidad sobre las conclusiones importantes de su trabajo.

ANÁLISIS DE LOS SISTEMAS

Los procedimientos de auditoria deben enfocarse al conocimiento detallado de los sistemas que se hayan seleccionado para prueba. Este conocimiento se logró en la fase II mediante el estudio y evaluación de los sistemas a través de los diagramas de flujo de datos y que describen los controles existentes en la entrada, proceso y salida de la información, así como a través de entrevistas con los analistas y personal del centro de cómputo y de sus usuarios.

ANÁLISIS DE LOS CONTROLES DE APLICACIÓN ESPECÍFICOS

Sobre los sistemas seleccionados se verificará que los controles establecidos sean adecuados a través de pruebas de seguimiento o de reestructuración para verificar que

funcionan satisfactoriamente. Estos controles se mencionan en la selección de controles de aplicación o específicos.

DETERMINACIÓN Y DESARROLLO DE LAS PRUEBAS DE AUDITORIA

El auditor debe seleccionar las pruebas de cumplimiento a efectuar al sistema y, en algunos casos excepcionales, puede lograrse a través de pruebas tradicionales; sin embargo, debido a que la mayoría de los controles internos importantes están dentro de los sistemas, y éstos solamente podrán probarse utilizando ciertas técnicas que se aplican usan el mismo computadora.

ANÁLISIS Y EVALUACIÓN DE LAS PRUEBAS DE CUMPLIMIENTO

Los resultados de las pruebas de cumplimiento deben ser analizados a fin de evaluar si estos dieron los resultados esperados y que, por lo tanto, confirman que los controles funcionan como el auditor los conoció en las fases anteriores. En caso de que existan deficiencias o desviaciones no esperadas, éstas deberán ser evaluadas para definir como su efecto trascendió a la información financiera y, en su caso necesariamente ampliar los procedimientos sustantivos de auditoria hasta llegar a una conclusión, cabe mencionar que el auditor también puede probar el contenido y corrección de los archivos que mantienen los análisis de saldos.

1.11.4 TERCERA FASE ALTERNA - PRUEBAS A LOS CONTROLES PED PARA INCREMENTAR LA EFICIENCIA EN LOS RESULTADOS DE AUDITORIA

Puede darse el caso de que el auditor, aun cuando tuviera la certeza de obtener evidencia suficiente y competente por otros medios, pudiera decidir llevar a cabo pruebas de cumplimiento y sustantivas usando el computadora para lograr pruebas de auditoría más efectivas, extensas, precisas y con un menor esfuerzo de tiempo en el trabajo.

CAPITULO II

2. METODOLOGIA DE LA INVESTIGACION

2.1 OBJETIVOS DE LA INVESTIGACIÓN

2.1.1. GENERAL.

Formular, analizar, evaluar y proponer una guía practica que sirva para la Evaluación del Control Interno en la Auditoria en Informática, como servicio profesional a los niveles más altos de la empresa privada, para responder con una visión innovadora a las demandas de servicios que plantean las empresas en la actualidad y que el profesional de la contaduría pública debe ofertar. Así como conocer y diagnosticar mediante la investigación de campo sobre el funcionamiento del PED, evaluando el ambiente de control, para conocer la existencia de medida de control interno y la habilidad de la gerencia para establecer mecanismo de autoevaluación y vigilancia.

2.1.2. ESPECÍFICOS.

- a. Evaluación de la Seguridad Física: conocer si la empresa cuenta con la seguridad física necesaria para el resguardo del equipo de cómputo y su entorno; conocer los controles existentes sobre la seguridad física del hardware, transmisión de datos, accesos físicos y seguridad en casos de emergencia.
- b. Evaluación de Controles y Procedimientos: conocer la efectividad y eficacia de los controles y procedimientos aplicados para el resguardo del software y hardware; Conocer los controles establecidos sobre el uso de programas y software, copias de respaldo, adquisición de paquetes y base de datos.
- c. Evaluación de respaldo y recuperación: conocer si los tipos de respaldo de la información aplicados por la empresa son efectivos, permitiendo en un momento determinado la recuperación de la información.

- d. Evaluación del sistema de cómputo: conocer si el sistema contable cuenta con las características necesarias requeridas por la empresa en el procesamiento de datos
- e. Evaluación de Recursos Humanos: conocer la capacidad y eficiencia del personal del área, así como saber las necesidades existentes.

2.2. DEFINICIÓN DEL TIPO DE ESTUDIO

La metodología utilizada fue la del paradigma Hipotético Deductivo, Positivista o Cuantitativo que permitió obtener respuesta a determinados fenómenos relacionados con este campo de estudio y es de los paradigmas más conocidos y utilizado en la comunidad científica.

Este permitió realizar la técnica de investigación de manera cuantitativa a partir de datos estadísticos obtenidos de herramientas de apoyo principalmente de cuestionarios y entrevistas. El tipo de estudio se realizó combinando el descriptivo y el analítico, mediante el cual se conoció el problema, se caracterizó y se efectuó el análisis de sus principales aspectos.

2.2.1. UNIDADES DE ANÁLISIS

Las unidades de análisis tomadas en cuenta para desarrollar la investigación, están conformadas por los pequeños y medianos despachos de auditoría y consultoría constituidos legalmente como sociedades, de acuerdo a información obtenida en el Consejo de Vigilancia de la Contaduría Pública y Auditoría de El Salvador

2.3. POBLACIÓN Y MUESTRA

2.3.1. POBLACIÓN

Según datos proporcionados por el Consejo de Vigilancia de la Contaduría Pública y Auditoría de El Salvador, el total de despachos de auditoría constituidos legalmente como sociedades ascendían a 97, estratificados de la manera siguiente:

Compañías	35
Y Asociados	39
Sociedades Anónimas	1
Sociedad Colectiva Mercantil	<u>22</u>
	<u>97</u>

Del total de despachos se estima que 10 de ellos se clasifican como grandes y 87 entre pequeños y medianos.

2.3.2. MUESTRA

La muestra poblacional examinada fue de 29 despachos de Auditoría y Consultoría, obtenida por medio de la fórmula siguiente:

$$M = \frac{Z^2 \cdot P \cdot Q \cdot N}{(N-1)E^2 + Z^2 \cdot P \cdot Q}$$

En la cual:

M = Muestra a obtenerse al sustituir valores y efectuar las operaciones respectivas

Z = Valor crítico que corresponde a un coeficiente de confianza del 90%, donde Z es 1.64, de acuerdo al área bajo la curva normal

P = Proporción Poblacional que ofrece servicios de Auditoria en Informática (20%)

Q = Proporción Poblacional que no ofrece Servicios de Auditoria en Informática (80 %)

N = Total de pequeños y medianos despachos de auditoría 87

E = Error muestral (10%)

Sustituyendo Valores en fórmula:

$$M = \frac{(1.64)^2 (0.20) (0.80) (87)}{(87-1)(0.10)^2+(1.64)^2(0.20)(0.80)}$$

Desarrollando el resultado, se obtiene:

$$M = 29$$

De los enfoques básicos de muestreo estadístico, se utilizó el de muestreo por atributos debido a la caracterización del fenómeno estudiado. Además, la técnica de selección de muestras condujo a utilizar el de muestreo aleatorio que permitió seleccionar cada uno de los despachos encuestados.

2.4. MÉTODOS E INSTRUMENTOS PARA RECOLECCIÓN DE DATOS.

2.4.1. INVESTIGACIÓN BIBLIOGRÁFICA

La técnica documental: sirvió para conocer los aspectos generales y específicos del tema, basados en los conocimientos y experiencias relacionadas a la Auditoría en Informática; los datos recolectados a través de esta técnica son el punto inicial de la investigación y es determinante para completar el trabajo de campo.

Lectura o investigación documental de libros, revistas, tesis, síntesis de seminarios, diccionarios y literatura que tenga relación con los diferentes tipos de Herramientas relacionadas con la Evaluación del Control Interno, especialmente aquellos que se refieran a la evaluación del riesgo y control en la Auditoría en informática y sistemas de información.

Sobre la base de esta fuente de información se pudo ampliar los conocimientos, conceptos y otros aspectos que tienen relación con el tema a desarrollar, a fin de concretizar resultados positivos.

2.4.2. INVESTIGACIÓN DE CAMPO

La investigación bibliográfica se complementó con la investigación de campo, para determinar la aplicación de la Auditoría en Informática en la empresa privada, la investigación se efectuó por medio de un cuestionario para los gerentes de servicio de los despachos de auditoría y consultoría sujetas de estudio. Se utilizó el método de investigación participativa con el objeto de que se complementen las relaciones entre investigadores e investigados proporcionándose un apoyo mutuo.

Para lograr el objetivo que se ha trazado fue necesario obtener información a través de consultas, encuestas y entrevistas estructuradas, dirigidas a personal de dirección y de asesoría, a efecto de visualizar mejor la realidad en el Proceso de la Auditoría en Informática, especialmente en la etapa de evaluación del control interno, sus componentes y el riesgo de auditoría.

2.5. TABULACION DE DATOS

La información obtenida de cada cuestionario, se tabuló agrupando la cantidad de respuestas por cada pregunta tanto en el caso de las respuestas cerradas como de las abiertas, obteniendo de esa manera las frecuencias en términos absolutos y luego convirtiéndolas en términos relativos (porcentajes), posteriormente se elaboró un cuadro para cada una de ellas.

2.5.1. INTERPRETACIÓN DE LOS RESULTADOS

Una vez tabuladas las respuestas en sus cuadros correspondientes, se desarrolla la interpretación de las frecuencias absolutas y relativas establecidas por cada pregunta, considerando adicionalmente los comentarios expresados por los socios o representantes de los despachos de auditoría y consultoría, sobre los cuales se llevó a cabo la investigación.

2.6. RESULTADOS DE LA INVESTIGACION

2.6.1. ANALISIS E INTERPRETACION DE LA INVESTIGACION DE CAMPO

De una población total de 87 pequeños y medianos despachos que funcionan como sociedades legalizadas, la muestra poblacional estimada fue de 29 unidades ($M=29$); Considerando que la cantidad de preguntas incluidas en el cuestionario no era extensa, la clasificación y la tabulación de datos se efectuó en forma manual.

A continuación se presenta cada uno de los cuadros con sus preguntas, análisis e interpretación respectivos:

PREGUNTA N° 1

- Objetivo de la pregunta:

Conocer el grado de experiencia que por antigüedad, podrían tener los despachos

¿Cuántos años tiene de operar su despacho?

*Período de funcionamiento de los pequeños y medianos
despachos de auditoría en El Salvador*

CATEGORÍA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) De 0 A 3 años	4	14 %
b) De 3 A 5 años	7	24 %
c) De 5 A más años	18	62 %
TOTAL	29	100 %

- Análisis de los resultados:

Como puede observarse, los resultados obtenidos demuestran que del total de pequeños y medianos despachos encuestados, 18 de ellos equivalentes al 62% del total poseen experiencia considerable en la prestación de servicios ya que tienen 5 ó más años de permanecer en el mercado de la profesión, aunque ello no signifique que hayan alcanzado un desarrollo sustantivo. En porcentaje menor, 4 unidades equivalentes al 14% contestaron tener entre 0 a 5 años de permanecer en el mercado.

PREGUNTA N° 2

- Objetivo de la pregunta:

Estratificar y Dimensionar el tamaño de los despachos de auditoría y consultoría existentes.

Según su criterio ¿Cómo considera el tamaño de su despacho?

Tamaño del despacho de auditoría

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Pequeño	22	76 %
b) Mediano	7	24 %
c) Grande	0	0 %
TOTAL	29	100 %

- Análisis de los resultados:

Según el cuadro anterior, los resultados obtenidos indican que del total de 29 despachos de auditoría y Consultoría encuestados 22 de ellos equivalentes al 76 %, se definieron como pequeños y 7 de ellos equivalentes al 24 %, como medianos.

Lo anterior evidencia la importancia de apoyar con investigación académica de esta naturaleza, ya que herramientas técnicas para la Evaluación del Control Interno en la Auditoría en Informática les daría la posibilidad de mejorar la calidad y prestación de sus servicios logrando el crecimiento y desarrollo de sus unidades.

PREGUNTA N° 3

- Objetivo de la pregunta:

Estratificar y dimensionar el tamaño de los despachos de auditoría y Consultoría a través del número de empleados.

¿A cuánto asciende el total de empleados de su despacho?

Número de empleados que conforman el despacho

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Entre 2 Y 10 Empleados	21	72 %
b) Entre 11 Y 20 Empleados	8	28 %
c) Mas de 20 Empleados	0	0 %
TOTAL	29	100 %

- Análisis de los resultados:

En cuanto al número de los empleados de los pequeños y medianos despachos de auditoría, el cuadro demuestra que el 72 % de las unidades encuestadas(21 de 29) poseen, un máximo de 10 empleados, el 28 % (8 de 29), entre 11 y 20 empleados.

Lo anterior evidencia la necesidad de que este tipo de unidades optimicen el uso del personal a través de la eficiencia y eficacia para cumplir con programas de trabajo

establecidos y satisfacer las demanda de servicios específicos solicitados por sus clientes.

PREGUNTA N° 4

- Objetivo de la pregunta:

Conocer la composición y el tamaño de la cartera de clientes de los despachos de auditoría y consultoría.

En términos porcentuales, ¿Cómo está estratificada su cartera de clientes?

Estratificación de la cartera de clientes

CATEGORIA	FRECUENCIA	
	RELATIVA	ABSOLUTA
a) Clientes pequeños	16	55 %
b) Clientes medianos	9	31 %
c) Clientes grandes	4	14 %
TOTAL	29	100 %

- Análisis de los resultados:

En cuanto a la conformación de la cartera de clientes para los pequeños y medianos despachos se determinó calculando un porcentaje promedio de cada una de las categorías, indicando que del total de los despachos un promedio de 16 mantiene el 55 % de clientes pequeños, asimismo 9 despachos en promedio mantienen el 31% de clientes medianos, la muestra se completa con 4 despachos en promedio que mantienen el 14 % de clientes grandes.

En sondeos para profundizar sobre estos resultados, se obtuvo que en la captación del 14% de clientes grandes, hay una tendencia a distribuirse equitativamente este porcentaje entre pequeños y medianos; es decir, la captación de clientes grandes no esta únicamente en función del tamaño del despacho sino en la calidad del trabajo y la habilidad para incursionar en el sector de la gran empresa.

PREGUNTA N° 5

- Objetivo de la pregunta:

Estratificar la cartera de clientes de acuerdo al sector económico a que pertenecen

De acuerdo con la actividad económica, en términos porcentuales, ¿Cómo clasifica su cartera de clientes?

Estratificación de cartera de clientes según actividad económica

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Banca	0	0 %
b) Comercio	13	45 %
c) Industria	6	21 %
d) Agropecuaria	2	7 %
e) Otros	8	27 %
TOTAL	29	100 %

- Análisis de los resultados:

Con relación a la clasificación de la cartera de clientes según su actividad económica, se observa que existen tres sectores principales que demandan servicio de pequeños y medianos despachos de auditoría y consultoría, siendo el primero el sector comercio que representa en promedio el 45% lo cual indica que la experiencia que se posee sobre este sector es muy significativa; el segundo lugar lo ocupa la categoría de otros que incluye servicios, a ONG'S entre otros, que alcanza un promedio del 27 %, los clientes del sector industria ocupan el tercer lugar con un promedio del 21%.

Además, los datos reflejan que la relación con actividades como la banca y agropecuarias es mínima; por lo que se hace importante brindar el apoyo adecuado a las unidades en estudio para mejorar su incidencia en estas ramas del mercado de la profesión. Proporcionarles instrumentos de apoyo técnico (como el presente), contribuirá con ese propósito.

PREGUNTA N° 6

- Objetivo de la pregunta:

Conocer la diversificación de servicios y localizar cuales son los principalmente demandados.

Dentro de los servicios que oferta su despacho ¿Cuáles poseen mayor demanda?*Principales servicios demandados*

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Auditoría Financiera	12	41 %
b) Auditoria Tributaria	7	24 %
c) Servicios de Contabilidad	8	28 %
d) Auditoria en Informática	2	7 %
TOTAL	29	100 %

- Análisis de los resultados:

En lo que se refiere a los principales servicios que los clientes demandan de los pequeños y medianos despachos de auditoría y consultoría, se obtuvo que los más significativos son Auditoría Financiera con 41% en promedio, servicios contables con 28% en promedio y el área de impuestos con 24% en promedio, constituyéndose estos tres servicios en los más importantes, ya que suman el 93% del total y significan los ejes principales del quehacer de estas unidades de servicios. Muy distantes de los servicios anteriores se coloca la Auditoria en Informática con el 7% en promedio del total.

Los resultados son normales respecto a los servicios tradicionales que brindan los pequeños y medianos despachos de auditoría, sin embargo, es necesario incorporar otros servicios que estén acordes a las exigencias de la época entre los que destaca la Auditoria en Informática.

PREGUNTA N° 7

- **Objetivo de la pregunta:**

Conocer las alternativas existentes que los despachos consideran ante los cambios en la demanda de servicios, especialmente cuando se refiere a la Auditoría en informática.

¿Ante los cambios en la demanda de servicios de la época, ¿Cuál es la alternativa de competitividad que su Despacho considera más viable para diversificar sus servicios?

Alternativas de competitividad para despachos de auditoría y consultoría

CATEGORIAS	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Efectuar alianzas estratégicas con otros despachos	6	21 %
b) Contratación de especialistas	4	14 %
c) Apalancamiento financiero	0	0 %
d) Capacitación permanente al personal técnico	19	65 %
e) otros	0	0 %
TOTALES	29	100 %

- **Análisis de los resultados:**

Respecto a la alternativa que los pequeños y medianos despachos encuestados, consideran más viable para ser competitivos en la diversificación de los servicios, 19 unidades equivalentes al 65% del total respondieron que la alternativa es la capacitación permanente al personal técnico, pues contarían con un recurso humano cualificado que respondería a las necesidades de las respectivas unidades. En cuanto a otras opciones, 6 unidades equivalentes al 21% del total consideran que el desarrollo de alianzas estratégicas les permitirá ser competitivos, especialmente frente a los grandes despachos de auditoría; En tercer lugar 4 unidades equivalentes al 14% consideran que la alternativa más viable sería la contratación de especialistas.

En síntesis, la mayoría de los despachos encuestados (86% del total), consideran que con la capacitación permanente y las alianzas estratégicas sus unidades de servicio se

fortalecerían y se evitaría drenar recursos a través de la subcontratación de otros servicios a través de especialistas.

PREGUNTA N° 8

- Objetivo de la pregunta:

Conocer la cuantía de los despachos y en que medida desarrollan este tipo de auditoria.

¿ Ha Trabajado su despacho en el área de Auditoria en Informática?

Desarrollo de Auditoria en Informática

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Sí	6	21 %
b) No	23	79 %
TOTALES	29	100 %

- Análisis de los resultados:

En cuanto al desarrollo de la Auditoria en Informática, por parte de los pequeños y medianos despachos un total de 23 unidades equivalente al 79% del total respondió que no la desarrollan y únicamente 6 unidades equivalentes al 21% del total contestaron afirmativamente. En preguntas exploratorias con quienes desarrollan este tipo de Auditoria, acerca de como han adquirido esos conocimientos, afirmaron haberlos obtenido al involucrarse en los distintos eventos nacionales y regionales de la profesión que se desarrollan y que les ha permitido mantener una actualización de conocimientos para ofertar este tipo de servicios, además de estar incorporados a Asociaciones Profesionales de Contadores Públicos.

PREGUNTA N° 9

- Objetivo de la pregunta:

Indagar sobre las razones por la que no es desarrollada la Auditoria en Informática por algunos despachos, así como indagar el grado de conocimientos de la misma.

Si su respuesta a la pregunta anterior es “No”, ¿Porqué no la desarrolla?

Causas para no desarrollar la Auditoría en Informática

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Conocimientos insuficientes sobre Auditoría en Informática.	12	52 %
b) No posee los recursos necesarios	9	39 %
c) Otros	2	9 %
TOTALES	23	100 %

▪ Análisis de los resultados:

Según el cuadro, del total de encuestados, 23 contestaron que no desarrollan la Auditoría en Informática, al profundizar sobre tal situación, el cuadro anterior demuestra las causas por qué no desarrollan este tipo de Auditoría; 12 unidades equivalentes al 52% del total afirmaron no desarrollarla debido a la falta de solidez sobre los conocimientos sobre la Auditoría en Informática, 9 unidades equivalentes al 39% respondieron no poseer los recursos necesarios para su desarrollo y 2 unidades equivalentes al 9% contestaron que no la desarrollaban por otros motivos.

De los resultados obtenidos, se evidencia la necesidad de dar a conocer las ventajas que los pequeños y medianos despachos pueden obtener al desarrollar la Auditoría en Informática, asociado a poseer el conocimiento en la materia y el recurso humano necesarios para su implementación.

PREGUNTA N° 10

▪ Objetivo de la pregunta:

Conocer si la estructura organizativa de los despachos, considera la unidad de Auditoría en Informática.

¿ En su firma de consultoría, existe una unidad especializada en materia de Auditoría en Informática?

Unidad de Auditoria en Informática

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Si	2	7 %
b) No	27	93 %
TOTAL	29	100 %

▪ Análisis de los resultados:

Un 93% de los despachos que prestan el servicio de Auditoria en Informática no contempla en su estructura organizativa el servicio en el área de Informática. Es evidente la necesidad de contar con la unidad de Informática y la integración de personal especializado.

PREGUNTA N° 11

▪ Objetivo de la pregunta:

Conocer el tipo de metodología que se desarrolla en los despachos de auditoria respecto a la Auditoria en Informática.

¿ En el proceso de la Auditoria en Informática, ¿ A cual de las siguientes etapas se les da más importancia: Planificación de la Auditoria, Evaluación del Control Interno, Diagnóstico, y presentación del Informe Final sobre los resultados de los estudios que desarrolla su firma sobre Asesoría y Auditoria?

Enfoque del proceso del desarrollo de la Auditoria en Informática

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Planificación de la Auditoria	3	11 %
b) Evaluación Técnica del Control Interno	10	34 %
c) Diagnostico	1	3 %
d) Informe Final	15	52 %
TOTALES	29	100 %

▪ Análisis de los resultados:

De los 29 despachos encuestados, 15 respondieron que el elemento de mayor importancia es el informe final sobre el estudio realizado, conformando un 52%; en

segundo lugar con el 34%, la etapa más importante del desarrollo de la Auditoría en Informática es la Evaluación del Control Interno con un total de 10 despachos; a la etapa de planificación casi no se le da importancia ya que el 3% la menciona como la más importante; el diagnóstico se puede decir que según lo manifestado por los despachos entrevistados no forma parte de la metodología utilizada en la Auditoría en Informática.

PREGUNTA N° 12

- Objetivo de la pregunta:

Conocer el enfoque de la Evaluación del Control Interno en la Auditoría en Informática.

De acuerdo con las respuestas obtenidas en el cuadro anterior ¿En el desarrollo de la Auditoría en Informática ¿Cómo desarrolla la Evaluación del Control Interno en la Auditoría en Informática?

Enfoque metodológico para la Evaluación del Control Interno

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Evaluación de la Dirección de Informática	3	10 %
b) Evaluación de los Sistemas	5	17 %
c) Evaluación de los Equipos	12	42 %
d) Evaluación del Software	9	31 %
TOTALES	29	100 %

- Análisis de los resultados:

Al analizar el cuadro, demuestra que del total de despachos encuestados, 12 pequeños y medianos despachos contestaron que desarrollan la evaluación del Control Interno a través de los equipos de computo, 9 unidades que conforman el 31% contestaron que lo hacen a través del Software; es poca la importancia que se da a los Sistemas, para la evaluación del control interno, por otra parte, poco se evalúa la dirección del departamento de informática.

PREGUNTA N° 13

- Objetivo de la pregunta:

Evaluar las fases de importancia en la ejecución de la Auditoría en Informática.

¿En la ejecución de la auditoría en informática se desarrollan las siguientes fases?

Ejecución de la Auditoría en Informática

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Estudio preliminar de las operaciones PED, para la obtención de información financiera.	3	10 %
b) Estudio del Control Interno.	7	24 %
c) Estudio de las transformaciones importantes en la información.	4	14 %
d) Evaluación del riesgo	5	17 %
e) Prueba de controles PED	10	35 %
TOTALES	29	100 %

- Análisis de los resultados:

Es notorio que la ejecución de la Auditoría en Informática los despachos la basan en las pruebas de controles al procesamiento electrónico de datos y el estudio del control interno, ya que un total de 35% y 24% respectivamente contestaron dar mayor énfasis a estas etapas; en segundo lugar la evaluación del riesgo y el estudio de las transformaciones importantes en la información conformando un total de un 31%; únicamente el 10% realiza un estudio preliminar de las operaciones PED para la obtención de información financiera.

PREGUNTA N° 14

- Objetivo de la pregunta:

Obtener información de cómo se evalúa la dirección de informática

¿La evaluación de la dirección de informática consta de los elementos siguientes: organización, estructura, recurso humano, normas y políticas, capacitación, planes de trabajo, controles y estándares?

Evaluación de la dirección de Informática

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Organización	1	3 %
b) Estructura	4	14 %
c) Recurso Humano	0	0 %
d) Normas y políticas	8	28 %
e) Capacitación	3	10 %
f) Planes de Trabajo	1	3 %
g) Controles	10	35 %
h) Estándares	2	7 %
TOTALES	29	100 %

▪ Análisis de los resultados:

La evaluación de la dirección en la Auditoría en Informática los despachos la basan en la evaluación de los controles, tomando en consideración las normas y políticas de la institución; en segundo lugar la capacitación del personal y la estructura del departamento de informática; es de poca importancia la evaluación de así como la organización y la evaluación de los estándares operacionales.

PREGUNTA N° 15

▪ Objetivo de la pregunta:

Obtener información de cómo se evalúan los Sistemas

¿La evaluación de los Sistemas consta de los elementos siguientes: ?

Evaluación del Los Sistemas

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Opinión de los Usuarios	5	17 %
b) Evaluación de Avance de los Sistemas en Desarrollo y Congruencia con el Diseño General	3	10 %
c) Evaluación de prioridades y recursos asignados	9	31 %
d) Seguridad Física y Lógica de los Sistemas, su Confidencialidad y Respaldo	12	42 %
TOTALES	29	100 %

▪ Análisis de los resultados:

La evaluación de los sistemas se efectúa básicamente a la seguridad física y lógica de los sistemas, su confiabilidad y respaldo; en segundo lugar se evalúan las prioridades y recursos asignados, cuenta poco la opinión de los usuarios y la evaluación del avance de los sistemas en desarrollo es casi nula.

PREGUNTA N° 16

- Objetivo de la pregunta:

Obtener información de cómo se evalúan los Equipos

¿La evaluación de los Equipos consta de los elementos siguientes?

Evaluación del Los Equipos

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Capacidades	6	21 %
b) Utilización	11	38 %
c) Nuevos Proyectos	0	0 %
d) Seguridad Física y Lógica	2	7 %
e) Respaldo de equipos	7	24%
f) Seguros	3	10 %
g) Contratos	0	0 %
TOTALES	29	100 %

- Análisis de los resultados:

Principalmente para evaluar los equipos, el elemento más importante es la Utilización de los Equipos y el Respaldo que estos tienen; en segundo lugar se evalúa las Capacidades y la Seguridad Física y Lógica; los Nuevos Proyectos y los Contratos no son evaluados.

PREGUNTA N° 17

- Objetivo de la pregunta:

Indagar sobre el sistema de comunicación de los resultados

¿Se elaboran informes que contengan conclusiones y recomendaciones por cada uno de los estudios y evaluaciones realizados?

Comunicación de Resultados

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Diagnóstico	0	0 %
b) Informes Intermedios e Informe Final	5	17 %
c) Solamente Informe Final	9	31 %
d) Las tres formas de comunicación	15	52 %
TOTALES	29	100 %

▪ Análisis de los resultados:

De los despachos encuestados el 52%, presentan informe inicial, informes intermedios e informe final; un 31% presenta únicamente informe final, en el trabajo de auditoría en informática no se formula un diagnóstico previo a los informes.

PREGUNTA N° 18

▪ Objetivo de la pregunta:

Indagar sobre las bases técnicas utilizadas por los despachos para soportar la planificación de la consultoría de Inversión.

1. ¿Cuál es el soporte técnico en que basa la planificación de la Consultoría de Inversión?

Base Técnica para la evaluación del Control Interno

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Entrevistas con el Personal Involucrado	10	35 %
b) Cuestionarios de Control Interno	16	55 %
c) Narrativas de Procedimientos	2	7 %
d) Flujogramación de los procedimientos operativos	0	0 %
e) Gráficos	1	3 %
TOTALES	29	100 %

▪ Análisis de los resultados:

Un 55% de los despachos utiliza como base técnica la formulación de cuestionarios de control interno para recopilar y evaluar la información, esto se hace a través de entrevistas con el personal involucrado; algunas veces es utilizada la técnica de narrativas y gráficos, no se utiliza la técnica de flujogramación como base técnica de la evaluación del control interno.

PREGUNTA N° 19

- Objetivo de la pregunta:

Conocer la existencia de políticas de capacitación el personal

¿ En que áreas capacita a su personal técnico?

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Área de Seguridad Física de los Sistemas Informáticos, Respaldo y Recuperación	10	35 %
b) Desempeño del Recurso Humano del área de Sistemas de Información	3	10 %
c) Sistemas de Computo, Producción y Confidencialidad de los Datos	14	48 %
d) Área Organizacional del Servicio Informático	2	7 %
TOTAL	29	100 %

- Análisis de los resultados:

Las áreas de mayor capacitación la constituyen los sistemas de computo, producción y la confidencialidad de los datos; la seguridad física de los sistemas informáticos, respaldo y recuperación. El área organizacional y el desempeño del recurso humano de informática no es objeto de una capacitación integral.

PREGUNTA N° 20

- Objetivo de la pregunta:

Conocer el grado de aplicación de procedimientos específicos para el desarrollo de la Consultoría.

¿Ud. como Auditor en Informática ha aplicado alguna vez alguna clase de procedimientos técnicos que respalden la Evaluación del Control Interno del auditor?

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Procedimientos Técnicas de Evaluación	9	31 %
b) Procedimientos Empíricos de Evaluación	7	24 %
c) Procedimientos Generales de Auditoria	13	45 %
TOTAL	29	100 %

▪ Análisis de los resultados:

De los despachos de auditoria entrevistados un 45% contestó que los procedimientos utilizados para la evaluación de control interno son los tradicionales o generales, un 31% utiliza técnicas específicas para evaluación del control interno de auditoría en informática; existe un 24% de los despachos que la evaluación del control interno la realiza empíricamente, es decir, de acuerdo con al experiencia adquirida en el desarrollo de su trabajo.

PREGUNTA N° 21

▪ Objetivo de la pregunta:

¿Considera usted que la elaboración de una guía para la Evaluación de la Estructura del Control Interno para Auditoria en Informática, sería de mucho beneficio para los despachos de auditoria y asesoría interesados en prestar este servicio?

Importancia de un documento para Evaluar el Control Interno en Informática

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Sí	27	93 %
b) No	2	7 %
TOTAL	29	100 %

▪ Análisis de los resultados:

En cuanto a la utilidad del trabajo que se desarrolla dando a conocer lineamientos sobre la Evaluación del Control Interno en la Auditoria en Informática; del total de

encuestados, 27 unidades equivalentes al 93% del total contestó que sí les sería de utilidad a su despacho un documento de esta naturaleza, ya que contarían con una herramienta valiosa para la evaluación del control interno para este tipo de auditoría, reduciendo sus costos. Por otra parte, 2 unidades equivalentes al 7% del total respondieron que no sería de gran utilidad.

Con lo anterior se destaca la importancia del trabajo para los pequeños y medianos despachos de auditoría, en la búsqueda de opciones de competitividad.

2.7. DIAGNÓSTICO

Basándose en los resultados obtenidos de las preguntas relacionadas, se ha establecido que la mayoría de los despachos encuestados tienen más de cinco años de estar en el medio, lo cual indica que poseen cierta experiencia para seguir operando en el mercado de la profesión contable, asimismo se visualiza que del total de los despachos, prevalecen los pequeños, que poseen de dos a diez empleados; ante esto es importante que los pequeños y medianos despachos deben aplicar medidas, en lo técnico y en sus estructuras organizativas para mejorar sus servicios al cliente que normalmente son servicios tradicionales como auditoría, contabilidad e impuestos y también deben considerar el ofertar nuevos servicios como la Auditoría Integral.

2.7.1. Aplicación de políticas de capacitación para el personal técnico

Se observa, que la mayoría de los despachos encuestados respondió que sí poseen como política la capacitación y promoción para su personal técnico, pues consideran que es una opción positiva que les permite satisfacer las demandas del cliente y actualizar sus conocimientos. En cuanto a las áreas en que se capacita al personal, la frecuencia con mayor respuesta fue el área del Impuestos, pero con la aclaración de que las áreas de auditoría y contabilidad, también ocupa un lugar privilegiado, evidenciándose la falta de capacitación en áreas innovadoras como la Consultoría de Inversiones; sin embargo, con ello, los pequeños y medianos despachos de auditoría pretenden satisfacer adecuadamente a su cartera de clientes y mantenerse en el mercado de la profesión.

2.7.2. Aplicación de Consultoría de Inversiones.

Los pequeños y medianos despachos de Auditoría y Consultoría encuestados, consideran que la consultoría de inversiones les generarían mejores beneficios económicos en la demanda de sus servicios. En síntesis hay una evidente mayoría que considera que el servicio de Consultoría de inversión sería muy provechosa para su despacho, y los que respondieron negativamente basaron su respuestas en el desconocimiento de este tipo de Consultoría.

La mayoría de los despachos encuestados contestaron que no desarrollan la Consultoría de Inversión, el resto afirmó que no la aplica por desconocimiento de este tipo de Servicio. Lo anterior demuestra, que a pesar de que el mayor porcentaje de pequeños y medianos despachos encuestados no desarrollan la Consultoría de Inversión, sí consideran que aplicarla sería favorable a sus respectivas despachos.

2.7.3. Enfoque de la Planificación de la Consultoría de Inversión y Soporte Técnico Aplicado por los Pequeños y Medianos Despachos.

Este tipo de Consultoría se desarrolla realizando visitas de campo exploratorias y con esa información elaboran los programas para cada área específica que constituye la Consultoría.

En síntesis, los pequeños y medianos despachos que desarrollan la Consultoría de Inversión la realizan, con alcance a las áreas estratégicas de las empresas como Finanzas, Administración, y otros aspectos considerados importantes; el soporte técnico son las normativas internacionales generalmente aceptadas debido a que la Consultoría de Inversión no posee, a la fecha actual, su propio marco normativo de general aceptación, únicamente se limita a enumerar Normas de Auditoría Generalmente Aceptadas basadas en principios éticos¹.

¹ IV CONVENCION NACIONAL DE CONTADORES, Código de Etica Profesional, (Propuesta), El Salvador, 1996, pág. 6.

2.7.4. Beneficios a obtener al ofertar servicios de Consultoría de Inversión

El resultado obtenido evidencia que los pequeños y medianos despachos de auditoría urgen de herramientas que les permitan alcanzar niveles de crecimiento y desarrollarse en un ambiente cada vez más competitivo.

Los despachos encuestados, consideran que con la aplicación de la Consultoría de Inversiones; obtendrían mejores resultados tanto económico como incremento en su cartera de clientes, argumentando que la limitante que percibe es que el cliente lo ve en función del costo en honorarios y no por los beneficios que obtendría su ente para el mediano y largo plazo, ven positivamente que un documento conteniendo lineamientos sobre el desarrollo de proceso de la Consultoría, les sería útil a los pequeños y medianos despachos de auditoría para afrontar los cambios de la época.

Este tipo de despachos, si realizan los ajustes necesarios a través de una capacitación permanente a su personal técnico, pueden permitirles afrontar de mejor manera el proceso de globalización y ser competitivos.

2.8. Diagnóstico sobre el desarrollo de la Consultoría de Inversión por los pequeños y medianos despachos de auditoría y consultoría.

2.8.1. Ventajas

El porcentaje mayor de las unidades encuestadas poseen experiencia en el campo de la profesión contable, especialmente dedicados a áreas tradicionales como Impuestos, Auditoría y Contabilidad.

Las empresas a quienes proporcionan sus servicios son variadas, tanto en tamaño como en actividad económica;

En las unidades encuestadas, hay un consenso generalizado en cuanto a cualificar permanentemente al recurso humano que poseen, a través de capacitarlo y promocionarlo adecuadamente; esto es importante debido a que los pequeños y medianos despachos tienen que optimizar el uso del recurso humano limitado que

poseen, debido a que es uno de los elementos básicos con que cuentan estas unidades de servicio en la búsqueda de competitividad.

2.8.2. Limitaciones

Los pequeños y medianos despachos de auditoría, debido a su dispersión, no poseen la estructura organizativa adecuada para afrontar a los grandes despachos de auditoría que en alianzas con firmas internacionales, acaparan los mayores segmentos del mercado de la profesión.

La experiencia acumulada en el medio (5 años o más), no ha bastado para alcanzar niveles de crecimiento significativo, manteniendo igual el tamaño de sus despachos, en la mayoría de los casos se mantienen como pequeños.

El mayor número de unidades no posee los conocimientos actualizados que les permita la aplicación de la Consultoría de Inversión; que representa opción real para la generación de mayor valor agregado e inserción al proceso de cambios que viven las economías.

Urge el desarrollo de herramientas de apoyo para el sector de pequeños y medianos despachos de auditoría y consultoría, debido a que es un sector vulnerable de ser afectado por los cambios que se dan en el ámbito internacional y que repercuten en el ámbito nacional.

La oferta de servicios de consultoría de inversión para los pequeños y medianos despachos, que comprende el presente trabajo, se constituye en parte fundamental de las opciones que estas unidades de servicio necesitan para lograr un mayor desarrollo y competitividad.

CAPITULO III

3. GUÍA PRÁCTICA PARA LA EVALUACIÓN DEL CONTROL INTERNO EN LA AUDITORÍA EN INFORMÁTICA.

El desarrollo tecnológico que ha experimentado la sociedad salvadoreña en los últimos años en las operaciones empresariales con la implementación de nuevos sistemas de información a través del procesamiento electrónico de datos, obligan al Contador Público Académico a analizar la importancia de Estados financieros y su relación con la Auditoria de Sistemas.

La auditoria de sistemas, comprende evaluación y resultados de control interno de los sistemas de información de las áreas críticas, controles detectivos, controles preventivos, riesgos y técnicas para la evaluación de las diferentes áreas de aplicación en que se dividen los sistemas de información en los centros de cómputo.

3.1 TERMINOS DE CONTRATACIÓN

Hemos sido contratados por la Junta General de Accionistas para llevar a cabo la auditoría en informática de la empresa DRUPY S.A. de C.V. Para verificar la lógica del sistema, así como también la efectividad del funcionamiento del mismo:

Contenido de los informes:

A continuación se detallan los requerimientos de mayor relevancia:

- a. Informar a la Junta General de Accionistas sobre la contabilidad y la seguridad del sistema a auditar el cual deberá estar de acuerdo a Normas de Auditoria Generalmente Aceptadas y Normas de Internacionales de Auditoria de Sistemas Informáticos.

- b. Emitir Carta a la Gerencia de las Observaciones y Recomendaciones: se presentará de los resultados obtenidos durante la evaluación del control interno, en el cual se informará acerca de los hallazgos encontrados en dicha evaluación, el cual contendrá
- ▶ Descripción del hallazgo encontrado
 - ▶ Efectos que produce dicho hallazgo
 - ▶ Conclusiones y recomendaciones

ANTECEDENTES Y GENERALIDADES DE LA EMPRESA

VISIÓN

Una industria de textiles en el mercado con bajos precios, buen servicio y sobre todo buena calidad.

MISION

Una empresa que fabrica textil para satisfacer las necesidades de sus clientes a los cuales brindan calidad.

HISTORIA

La sociedad comienza sus operaciones en la República de El Salvador y su plazo inicial para operar fue de diez años, siendo inscrita su constitución el 27 de noviembre de 1995, según escritura pública celebrada el 01 de octubre de 1995 ante los oficios del Dr. Luis Martínez Castro.

NATURALEZA JURIDICA

La industria DRUPY S.A. de C.V. está constituida de acuerdo a las leyes mercantiles de la República de El Salvador, organizada como una sociedad anónima de capital variable. La responsabilidad de los accionistas está reconocida como limitada a la cuantía del Capital Social con relación a terceros.

FINALIDAD

La finalidad de la sociedad es la realización de actividades industriales con especialidad en textiles basándose en fibras artificiales y sintéticas, incluyendo la confección, la compra de materia prima y demás bienes y servicios que las necesidades requieran; así como la distribución y la venta de los productos producidos.

CAPITAL SOCIAL

El Capital Social de la sociedad está formado por 1700 acciones de valor nominal de ¢ 100.00 c/u, siendo su composición la siguiente:

ACCIONISTA	NUMERO DE ACCIONES	CAPITAL SOCIAL
Marina Castaneda	800	¢ 80.000.00
Idalia Huevo	350	¢ 35.000.00
Carlos Orellana	150	¢ 15.000.00
Jaqueline Guardado	400	¢ 40.000.00
TOTAL	1700	¢ 170.000.00

SISTEMA DE CONTABILIDAD

Nombre: Núcleo Administrativo Financiero

Proveedor: Consultoría y Desarrollo, S.A.

Módulos que lo constituyen

1. Cuentas por Cobrar
2. Cuentas por Pagar
3. Activo Fijo
4. Cheques
5. Facturación
6. Importaciones
7. Inventario

8. Recursos Humanos
9. Planillas
10. IVA
11. Planta de Producción
12. Contabilidad

Reportes que genera

1. Balance Detallado
2. Balance Resumido
3. Balance General
4. Estado de Resultados
5. Diario General Anual
6. Diario Mes en Proceso
7. Caja Diario Mayor

EXISTENCIA DE EQUIPO

DESCRIPCIÓN DEL EQUIPO	CANTIDAD EXISTENTE
Servidor Compaq	1
Servidor Dell	1
Maquinaria Compaq	32
Maquinas clones	7
Maquinas Dell	1
Impresor matricial	5
Impresor de tinta	2

3.2 EVALUACIÓN DEL CONTROL INTERNO

Como cualquier departamento de la empresa el auditor tiene que evaluar el funcionamiento del PED. Debe evaluar el ambiente de control, para conocer la

existencia de medidas de control interno y la habilidad de la gerencia para establecer mecanismos de auto evaluación y vigilancia, incluyendo el establecimiento de manuales estándares, segregación de funciones, supervisión y auditoría interna, entrenamiento y capacitación, apoyo a la investigación y adelantos técnicos.

Evaluación de riesgo y control interno en la auditoria de sistemas computarizados

Los riesgos inherentes y de control en un sistema de información por computadora pueden tener tanto efectos generales como específicos debido a la probabilidad de presentaciones erróneas importantes. Estos pueden dar como resultado deficiencias en el desarrollo del sistema computarizado, en el desarrollo y mantenimiento de programas, soporte al software de sistemas, control sobre acceso a programas de utilería, controles de acceso al equipo, controles del fabricante entre otros.

Tipos de controles aplicables a un sistema computarizado

- a. Controles de entrada de información.
- b. Controles de ingreso y validación de datos
 - i. Controles de procesamiento
 - ii. Controles de salida de información

3.3 FASES DE UNA AUDITORIA EN INFORMÁTICA

PRIMERA FASE

Estudio preliminar obligatorio y necesario efectuar en todas las empresas que usen en alguna forma el PED para la obtención de su información financiera

SEGUNDA FASE

Ampliación del estudio del control interno. De aplicación obligatoria cuando en el estudio preliminar se ha determinado que se tiene aplicaciones de importancia para la obtención de la información financiera, que existen transformaciones importantes en la

información y de que el auditor tiene que confiar en una medida importante en el control interno que existe sobre dichas aplicaciones.

TERCERA FASE

Pruebas a los controles PED. De aplicación obligatoria cuando la importancia de los sistemas sujetos sea tal en cuanto a las transformaciones y al grado de confianza que el auditor depositará en el control interno, que el no efectuar pruebas de cumplimiento a los controles PED limita el alcance del trabajo del auditor al no tener evidencia suficiente y competente.

Existen casos en que el auditor, tenga necesariamente que confiar en el control interno del PED y, por lo tanto, tenga que evaluarlo y después probarlo en forma completa e integral a través de pruebas de cumplimiento. También habrá casos que por el resultado esperado de sus pruebas sustantivas, de importancia relativa y de riesgo probable, el auditor obtendrá la necesaria evidencia suficiente y competente que le permita solamente evaluar ciertos controles internos importantes de entrada y salida, y por lo tanto solamente cumplir con la primera fase, según las circunstancias, cubrir parcialmente la segunda y omitir la tercera.

Es importante señalar que desde la primera fase se requiere de experiencia en auditoría PED por parte del auditor y conforme se vayan pasando a las siguientes fases se requerirá de mayor capacitación.

3.4 OBJETIVOS Y PROCEDIMIENTOS POR FASE DE AUDITORÍA

a. ESTUDIO PRELIMINAR

- ▶ Determinar las principales aplicaciones y su efecto en la información financiera
- ▶ Conocer las características del equipo PED.
- ▶ Concluir sobre el efecto del PED en la información financiera y en su caso, pasar a la segunda fase

- ▶ Documentar ésta, de tal forma que respalde la decisión del auditor de continuar o no a la segunda fase.

b. AMPLIACIÓN DEL ESTUDIO DEL CONTROL INTERNO

- ▶ Evaluar la organización del centro de computo y los controles generales establecidos.
- ▶ Conocer las características de las aplicaciones y evaluar los controles de aplicación o específicos inherentes a las mismas, considerando el grado de transformación de la información y el volumen de operaciones que dependen del PED, a efecto de poder juzgar si se deben efectuar pruebas de cumplimiento a los controles PED.
- ▶ Formarse un juicio sobre la eficacia del control interno existente en PED que permita determinar la naturaleza, el alcance y oportunidad de los procedimientos de auditoría, tanto en cumplimiento como sustantivos.
- ▶ Concluir sobre los resultados obtenidos y en su caso, pasar a la tercera fase, considerando que el no probar los controles PED resultaría en una limitación importante en el trabajo de auditor, pues no se obtendrá la necesaria evidencia suficiente y competente.

c. PRUEBA DE CONTROLES

- ▶ Probar los controles específicos de las aplicaciones mediante pruebas de cumplimiento

3.4.1 PROCEDIMIENTOS RECOMENDADOS

El estudio preliminar está enfocado a determinar la importancia que el PED tiene en la información financiera y al conocimiento general del equipo

a. Descripción de las Aplicaciones

Consiste en conocer y documentar en papeles de trabajo las principales aplicaciones, volúmenes de operación, objetivos del sistema y de sus aplicaciones, identificando la entrada, proceso y salida de la información por cada aplicación, teleprocesos, etc. Pudiendo con ello determinar la información que se obtiene y procesa a través del PED y su repercusión en los estados financieros.

b. Estudio General del Equipo de Cómputo

Descripción de la unidad central de proceso y de las unidades periféricas, incluyendo datos tales como capacidad de memoria, sistema operativo, base de datos, comunicaciones, capacidad en pantalla remotas, modelo, antigüedad, etc.

c. Conclusión

3.4.2 SEGUNDA FASE AMPLIACIÓN DEL ESTUDIO DEL CONTROL INTERNO

La ampliación del estudio de control interno está enfocada a conocer con más detalle las características de los sistemas y de formarse un juicio sobre la eficiencia de los controles internos.

a. Revisión de los Estudios de Viabilidad

De esta forma se conocerá si la selección del equipo fue hecha en forma cuidadosa y si responde a las necesidades particulares de la empresa.

b. Análisis de la Organización del Centro de Computo.

Cerciórese de que no exista incompatibilidad de funciones, que tenga un buen soporte técnico, que existan líneas de autoridad definidas, que haya una planeación a corto y largo plazo; en general, se cuenten con políticas bien definidas y acorde a la importancia del departamento. También se debe revisar que existan procedimientos, autorizar cambios a los sistemas y fijar los estándares para el desarrollo de los sistemas. En sistemas pequeños donde no es posible la existencia de todos los controles, deberá determinarse la existencia de controles compensatorios que cubran dicha deficiencia.

c. Análisis de los Sistemas.

Verificar que el análisis, diseño, programación prueba de datos y mantenimiento de los sistemas esté documentado y de acuerdo a los estándares establecidos, juzgando a su vez lo apropiado de dichos estándares y del flujo de información.

d. Existencia de Manuales Operativos

Comprobar que existan manuales actualizados de operación del equipo y de los sistemas de operación y de que exista una historia de los cambios en los manuales y sus causas, etc.

e. Existencia de Copias de los Manuales Operativos

Verificar que se cuente con copias de manuales operativos debidamente protegidas fuera de la sala de cómputo.

f. Controles sobre Bitácoras

Verificar que existe una bitácora del centro de cómputo donde se registren los tiempos de proceso, cambios de programas, descomposturas, mantenimiento, operadores, etc.; y que exista supervisión adecuada y oportuna de esta bitácora.

g. Contingencias

Cerciorarse de que existe un plan de contingencia que asegure una continuidad razonable de la información.

h. Existencia de Planes contra Fallas

Investigar si en caso de fallas se cuenta con un equipo de soporte y procedimientos de reinicio.

i. Controles sobre Proceso

Verificar que la información procesada está sujeta a controle que aseguren que dicha información es válida y completa y que no se procesa información errónea y duplicada.

Determinar el grado de transformación de la información y asegurar que existan huellas o pistas que permitan la reconstrucción o seguimiento de la información procesada y de su transformación. En caso de información rechazada, que ésta sea analizada, corregida y evitada para el futuro y, en su caso, vuelva a ser oportunamente procesada. Asimismo, debe verificarse que toda la información procesada esté previamente autorizada.

j. Documentación de los Programas

Comprobar que la documentación que soporta los programas está de acuerdo con los estándares establecidos, que se encuentra completa y que exista evidencia y autorización de los cambios efectuados.

k. Existencia de Manuales con los Usuarios

Verificar la existencia de manuales actualizados para los usuarios.

l. Protección de Sistemas

Verificar que copias actualizadas de la documentación de los sistemas estén debidamente protegidos.

m. Protección de los Archivos

Cerciorarse de que existen copias actualizadas de los archivos maestros y de las transacciones, conservándose por un tiempo razonable en un lugar seguro, tanto en un edificio distinto al del centro de cómputo, como una copia en el mismo centro.

n. Elementos de Seguridad Física

Comprobar la seguridad física del centro de cómputo y determinar si el equipo está en un lugar que asegure la separación de funciones entre el personal y el acceso restringido al área. Que se cuente con extintores, detectores de humo y medidas razonables contra posibles sabotajes y cobertura adecuada de seguros mediante una evaluación profesional de los riesgos a que está sujeto tanto el equipo como la información.

o. **Auditoría Interna**

Evaluar el trabajo de auditoría interna y revisar sus reportes.

p. **Controles cuando Existe un Centro de Computo Externo**

Cuando el PED se realice en un centro de computo externo, los procedimientos aplicables son los siguientes:

- ▶ Revisión del contrato para comprobar que es adecuado a las circunstancias de la empresa y que se está cumpliendo con las condiciones estipuladas, así como si existe una revisión periódica del mismo para adecuarlo a las necesidades de la empresa.
- ▶ Recabar informes sobre el soporte técnico y la solvencia del centro de computo, con el objeto de evaluar la confidencialidad.
- ▶ Investigar sobre las alternativas que se ofrecen en caso de que el centro no pueda procesar la información.
- ▶ Verificar el flujo de la información del y al centro de computo y de los informes obtenidos, así como la actualización de los archivos maestros y de transacciones y de la seguridad de los mismos.
- ▶ Verificar los procedimientos que ha seguido la empresa para asegurarse de la validez de la información.
- ▶ Cuando las aplicaciones son de importancia, debe evaluarse la necesidad de efectuar una revisión directa del auditor en el centro de computo.

Tercera Fase “Pruebas a los controles PED”

Las pruebas a los controles PED están enfocadas a que el auditor obtenga evidencia de que los sistemas PED funcionan como los determinó en la fase II. Es importante mencionar que a partir de esta fase es imprescindible que el auditor tenga la debida

especialización y conocimiento de computo electrónico que le permita juzgar sobre los controles establecidos y efectuar pruebas en la computadora.

En caso de apoyarse en otras personas, el auditor deberá tener suficientes conocimientos de PED para dirigir, supervisar y revisar el trabajo de sus asistentes o para obtener la certeza razonable de que el trabajo hecho por expertos externos con conocimientos de PED, es adecuado en las circunstancias. Más aun, cuando el PED es parte integrante del sistema contable y del control interno relativo, el auditor no debe delegar en un experto en PED su responsabilidad sobre las conclusiones importantes de su trabajo.

a. Análisis de los Sistemas

Los procedimientos de auditoria deben enfocarse al conocimiento detallado de los sistemas que se hayan seleccionado para prueba. Este conocimiento se logró en la Fase II mediante el estudio y evaluación de los sistemas a través de los diagramas de flujos de datos y que se describen los controles existentes en la entrada, proceso y salida de la información, así como a través de entrevistas con los analistas y personal del centro de computo y de sus usuarios.

b. Análisis de los controles de aplicación específicos.

Sobre los sistemas seleccionados se verificará que los controles establecidos sean los adecuados a través de pruebas de seguimiento o de reestructuración para verificar que funcionan satisfactoriamente. Estos controles se mencionan en la selección de controles de aplicación o específicos.

c. Determinación y Desarrollo de la Pruebas de Auditoria

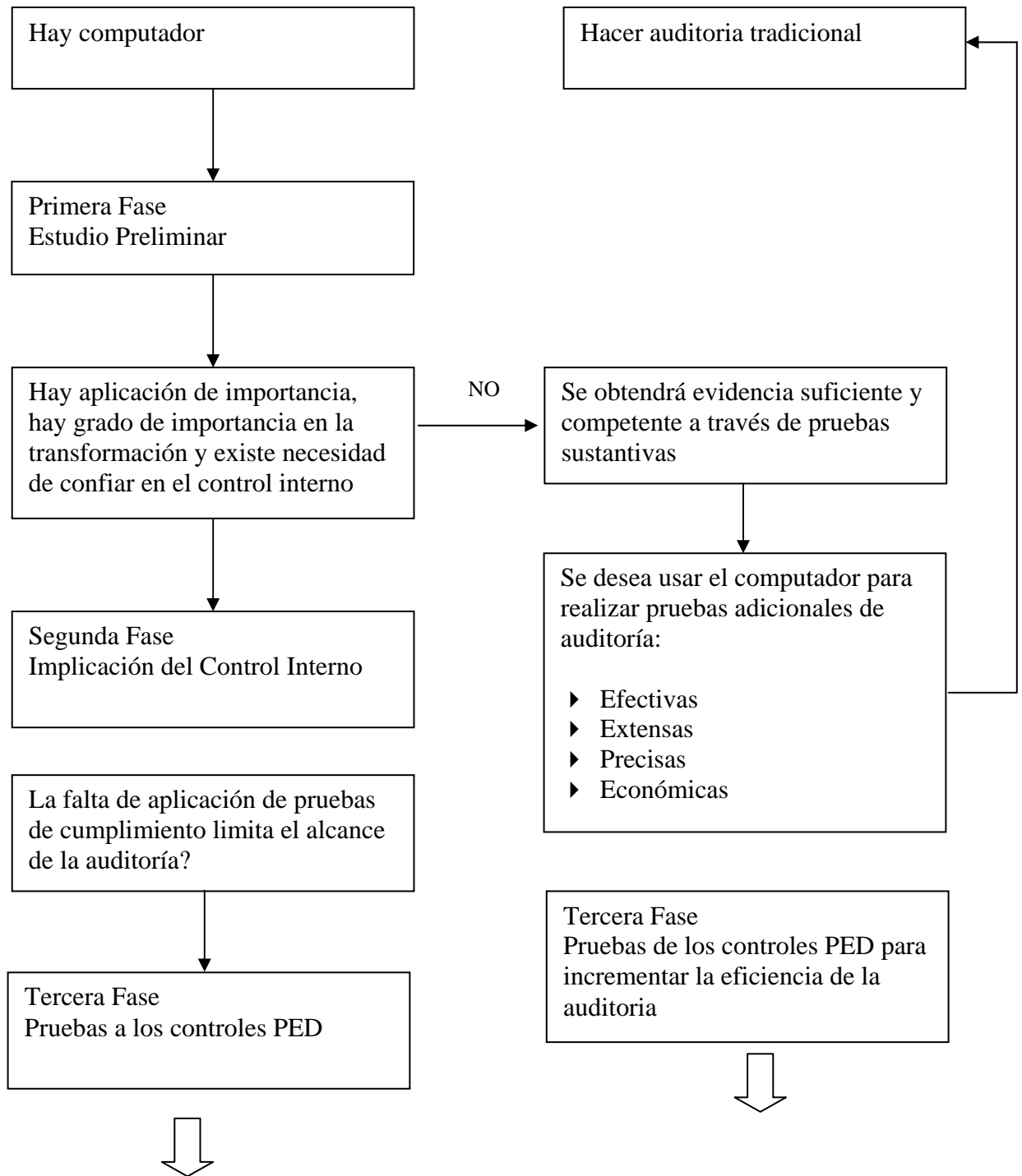
El auditor debe seleccionar las pruebas de cumplimiento a efectuar al sistema y, en algunos casos excepcionales, puede lograrse a través de pruebas tradicionales; sin embargo, debido a que la mayoría de los controles internos importantes están dentro de los sistemas, y éstos solamente podrán probarse utilizando ciertas técnicas que se aplican usando el mismo computador.

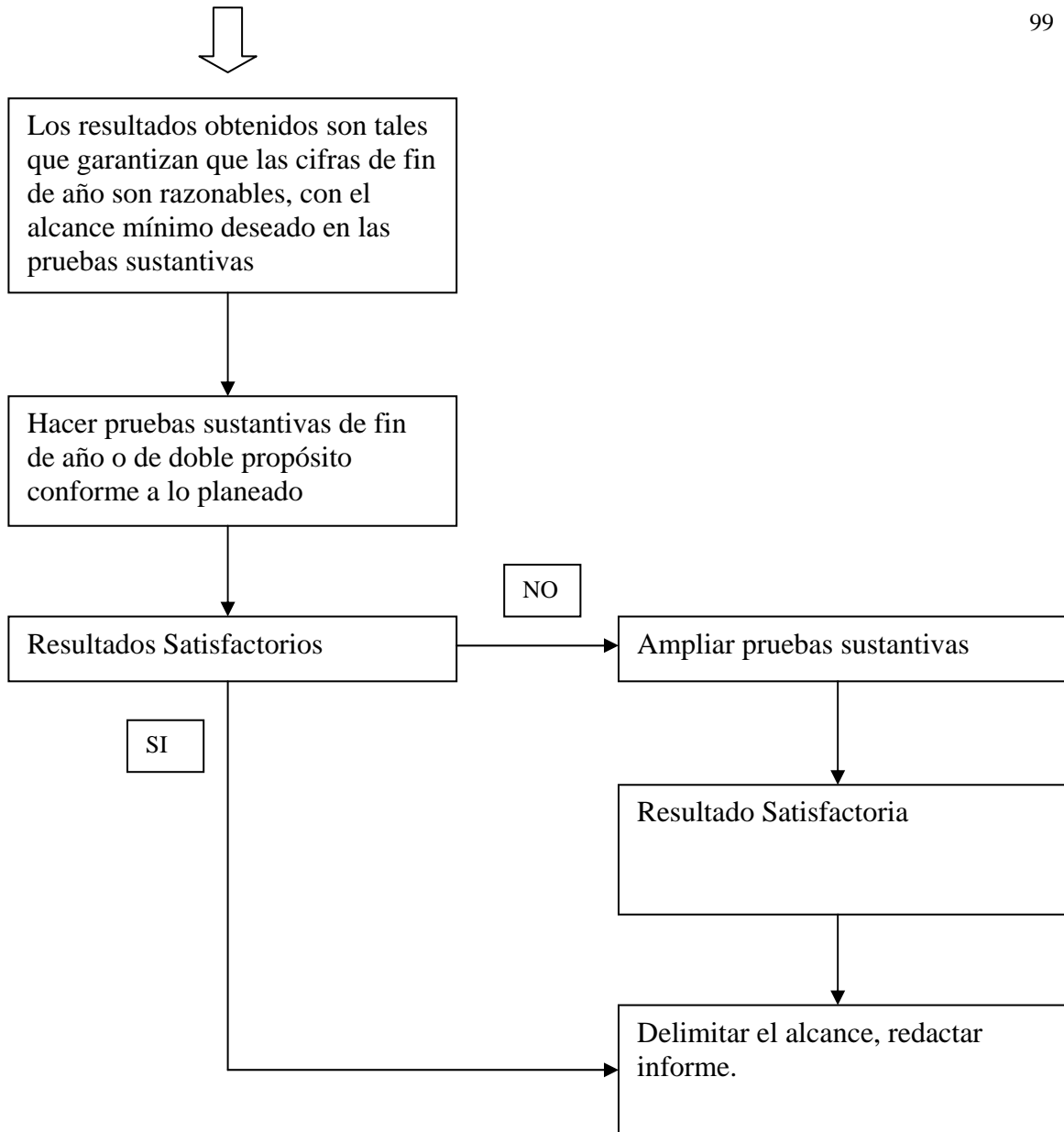
d. Análisis y Evaluación de las Pruebas de Cumplimiento

Los resultados de las pruebas de cumplimiento deben ser analizados a fin de evaluar si estos dieron resultados esperados y que, por lo tanto, confirmar que los controles funcionan como el auditor los conoció en las fases anteriores. En caso de que existan deficiencias o desviaciones no esperadas, éstas deberán ser evaluadas para definir como su efecto trascendió a la información financiera y, en su caso, necesariamente ampliar los procedimientos sustantivos de auditoría hasta llegar a una conclusión, cabe mencionar que el auditor también puede probar el contenido y corrección de los archivos que mantienen los análisis de saldos.

Puede darse el caso de que el auditor, aun cuando tuviera la certeza de obtener evidencia suficiente y competente por otros medios, pudiera decidir llevar a cabo pruebas de cumplimiento y sustantivas usando el computadora para lograr pruebas de auditoría más efectivas, extensas, precisas y con un menor esfuerzo de tiempo en el trabajo.

3.5 SECUENCIA DE LA AUDITORÍA EN INFORMÁTICA





3.5.1 Planeación de la Evaluación del Control Interno en Informática.

Los sistemas de computadora generalmente tienen áreas comunes de control y procedimientos relacionados a las áreas de aplicación, los tipos de control tienen por objeto proporcionar asesoría para planear y llevar a cabo las pruebas de controles de la computadora. Para la evaluación del control interno se elaborarán cuestionarios que consideren las áreas principales.

Dentro de las principales áreas de control interno a evaluar se consideran:

a. Planificación

- Sistemas de Información
- Recursos Humanos
- Generales
- Desarrollo

b. Organización y Administración

- Estructura
- Organización y Planificación
- Formación
- Estándares y Metodología
- Documentación
- Informes
- Segregación de Funciones

c. Entorno Operativo Hardware

- Seguridad Física
- Accesos Lógicos
- Accesos Físicos

d. Construcción de Sistemas

- Desarrollo
- Pruebas
- Implantación

e. Entorno Operativo Software

- Utilidades de Software
- Protección de Ficheros Producción

- ☒ Copias de Respaldo (Backup)
- ☒ Adquisición de Paquetes

3.5.2 Entrevista con el personal de informática

Se deben efectuar entrevistas con el personal de procesamiento de datos, para lo cual pueden entrevistar a un grupo de personas elegidas quienes podrán exteriorizar sus opiniones lo servirá para determinar:

- a. Grado de cumplimiento de la estructura organizacional administrativa
- b. Grado de cumplimiento de las políticas y procedimientos administrativos
- c. Satisfacción o insatisfacción
- d. Capacitación
- e. Observaciones generales

Guía de entrevista:

- a. Nombre del puesto
- b. Puesto del jefe inmediato
- c. Puesto a que reporta
- d. Puesto de las personas que reportan al entrevistado
- e. Actividades periódicas
- f. Actividades eventuales
- g. Señalar vacíos que considera existen en la organización

3.6 NARRATIVAS

A continuación se presentan las narrativas formuladas con base a la inspección realizada a las instalaciones de la unidad de informática y a las entrevistas sostenidas con personal ejecutivo y de operación, esta es la recopilación de información previa a la evaluación del control interno.

3.6.1 ÁREA DE SEGURIDAD FÍSICA






<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA NARRATIVAS ÁREA DE SEGURIDAD FÍSICA	REFERENCIA <hr/>
DESCRIPCIÓN	OBSERVACIONES Y COMENTARIOS	
<p>☞ El Departamento de cómputo se encuentra en un lugar separado del área operativa de la empresa, en una habitación de sistema mixto, con ventana de vidrio y cortinas de plástico. Dentro de esta habitación se mantienen extintores, que se renuevan cada seis meses.</p> <p>☞ El señor gerente administrativo – financiero de la empresa no ha accedido sobre adquirir un seguro contra incendio, robo y líneas aleadas; se puede observar que el lugar se encuentra seguro contra inundaciones, pero no así el techo, lo cual presenta pequeñas grietas, por lo que se filtra agua en época lluviosa, ocasionando inconvenientes en el trabajo que ahí se desarrolla.</p> <p>☞ Es de hacer notar que existe alarma contra robo, el cual se activa al momento de tratar de desplazar alguna máquina de su ubicación.</p> <p>☞ Al empleado nuevo, según lo informa el jefe de informática, se le da una inducción de 15 días para el cuidado y uso de la computadora, ya que no existe manual de procedimientos. Además del personal del personal de informática únicamente tiene acceso el personal de servicios generales con autorización del gerente administrativo, siendo éstos los únicos que tienen las llaves del centro de computo.</p>		

3.6.2 ÁREA DE CONTROLES Y PROCEDIMIENTOS





<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA NARRATIVAS ÁREA DE CONTROLES Y PROCEDIMIENTOS	REFERENCIA _____
DESCRIPCIÓN	OBSERVACIONES Y COMENTARIOS	
<ul style="list-style-type: none"> ☞ El programa no cuenta con un manual de procedimientos para el usuario, lo cual complica el procesamiento de la información cuando se cambia de personal, ya que se vuelve indispensable que la persona que se encarga de los procesos de la información se encuentre presente para explicar o describir el procedimiento a seguir. ☞ El programa adquirido no cuenta con una póliza de servicio de mantenimiento, ni de adiestramiento a los usuarios por parte del proveedor. El mantenimiento al hardware lo realiza una empresa diferente a la empresa a quienes se les compro el programa. ☞ El mantenimiento preventivo que se le da al programa es vigilado por el jefe del departamento de informática, quien supervisa que el equipo no sea maltratado. ☞ Las modificaciones al sistema son autorizados por el contador, a la fecha no se han hecho modificaciones desde su instalación. ☞ Para acceder al sistema el usuario debe digitar un password o contraseña, compuesto por ocho caracteres. ☞ El gerente administrativo y el jefe del departamento de computo son las únicas personas que poseen el listado de los password de los usuarios. ☞ Aunque el programa carece de manual de procedimientos para el usuario, el programa cuenta con pasos comprensibles para su ejecución, al ingresar a la carpeta del programa, éste muestra el menú de sistemas y otras opciones, para las cuales el programa requiere la clave de acceso 		

<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA NARRATIVAS ÁREA DE CONTROLES Y PROCEDIMIENTOS	REFERENCIA _____
DESCRIPCIÓN	OBSERVACIONES Y COMENTARIOS	
<ul style="list-style-type: none"> ☞ El programa cuenta con un menú principal, en el cual se detallan todas las opciones de todas las operaciones que éste realiza, ejemplo: formula preguntas de si o no desea continuar. ☞ Para evitar duplicidad al procesar la información a todo documento que se ingreso al programa se le estampa el sello de “PROCESADO” ☞ El gerente administrativo y jefe de informática supervisa y autoriza el ingreso de personas al departamento de computo. ☞ Cada terminal cuenta con password de acceso para el usuario diferente a la del programa. ☞ El proceso de actualización, es una rutina que únicamente la realiza el jefe de informática. ☞ Las opciones de modificar, agregar y borrar información que posee el sistema SISCONTA solo son ejecutadas por el jefe de informática. ☞ Se realiza un bloqueo al sistema para evitar el ingreso de información por personas no autorizadas. ☞ Si se procesa un documento y al ingresarlo no queda balanceado el programa muestra un mensaje indicando que el documento está descuadrado. Este mensaje consiste en que al final del registro, aparece solamente la cantidad por la que no se cuadra el registro. 		

3.6.3 ÁREA DE SISTEMA DE COMPUTO

<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA NARRATIVAS ÁREA DE SISTEMA DE COMPUTO	REFERENCIA <hr/>
DESCRIPCIÓN	OBSERVACIONES Y COMENTARIOS	
<p>  El programa SISCONTA no cuenta con un manual de aplicaciones y procedimientos ya que fue diseñado por un ingeniero y no por un proveedor de sistemas. El conocimiento del programa fue basándose en asesoría personalizada por parte del ingeniero en informática. </p> <p>  Para ingresar al programa se ha asignado un password que es utilizado únicamente por el personal del departamento, esta clave puede rectificarse periódicamente para evitar que personas no autorizadas ingresen al sistema. </p> <p>  El menú principal del programa es el siguiente: <ul style="list-style-type: none"> Selección de la empresa Movimiento en archivos Listado de cuentas Utilería del sistema Salirse de Foxbase Menú de proyectos Finalizar trabajo </p> <p>  El catálogo de cuentas, así como los movimientos contables cuentan con la opción de “Eliminar o modificar opciones” que no tienen ninguna restricción para evitar la susceptibilidad de la información a cambios no autorizados. </p> <p>  Los reportes con que cuenta son: El libro diario, libro de caja, diario mayor movimiento por cuentas, balance de comprobación, anexos al balance de comprobación, balance general y estados de resultados. </p>		

3.6.4 ÁREA DE RESGUARDO Y RECUPERACIÓN

<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA NARRATIVAS ÁREA RESGUARDO Y RECUPERACIÓN	REFERENCIA <hr/>
DESCRIPCIÓN	OBSERVACIONES Y COMENTARIOS	
<p>  La información procesada se guarda en disquetes de 3.5" de alta densidad, se utiliza siete juegos de disquetes para almacenar el movimiento diario (Backup externo) rotulados uno para cada día de la semana (lunes a sábado), detallando mes y año a que corresponde la información. Se realizan dos backup diarios, uno a mediodía y otro al finalizar las labores diarias. Los backup son realizados por el contador de la empresa. </p> <p>  Si por algún motivo se daña la base de datos, o se pierde información, se envía el último backup actualizado al proveedor del programa para su revisión. </p> <p>  Se posee un backup externo del catálogo de cuentas. Ante de efectuar un cierre de mes, se realiza un backup general. </p> <p>  En el disco duro se mantienen los archivos de la información contable de los últimos tres años, y el año actual; los años anteriores son almacenados en disquetes, a efecto de liberar espacio y cuando se desean consultar son restaurados al disco duro. </p>		

3.7 CUESTIONARIOS DE CONTROL INTERNO

3.7.1 Cuestionarios de Evaluación de la Planificación

<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO ÁREA DE PLANIFICACIÓN		REFERENCIA A
PREGUNTAS	Respuestas		OBSERVACIONES Y COMENTARIOS
	Si	No	
SISTEMAS DE INFORMACION			
1. ¿La dirección general y ejecutiva ha considerado la importancia que tiene el estudio del sistema de información?			
2. ¿Se establecen los requerimientos de información a largo plazo?			
3. ¿Se ha realizado una planeación estratégica del sistema de información para la empresa?			
4. ¿Existe una metodología para llevar a cabo tal planificación?			
5. ¿Se ha establecido requerimientos de información por departamentos usuarios?			
6. ¿Está definida la función del director del departamento PED?			
7. ¿Existe un plan estratégico del departamento del sistema de información?			
8. ¿Hay algún estudio sobre alternativas de soporte del sistema de información?			
9. ¿Existe la función de arquitectura de sistemas			
	NOMBRE		FIRMA
ELABORADO POR:			FECHA
REVISADO POR:			

<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO ÁREA DE PLANIFICACIÓN		REFERENCIA A
PREGUNTAS	Respuestas		OBSERVACIONES Y COMENTARIOS
	Si	No	
RECURSOS HUMANOS 1. ¿Es suficiente el número de personal para el desarrollo de las funciones del área de informática? 2. ¿Se deja de realizar alguna actividad por falta de personal? 3. ¿Está capacitado el personal para realizar con eficiencia sus funciones? 4. ¿Se estudia la evolución del mercado de computadores y la adaptación del personal a esa evolución? 5. ¿El personal de informática recibe noticias del momento tecnológico por revistas, notas técnicas, etc.? 6. ¿Se recibe información y se planifica ésta mediante asistencia a cursos seminarios etc.? 7. ¿Se planifica los recursos humanos y técnicos para cumplir los requerimientos del usuario? 8. ¿Es idóneo el personal que tiene acceso al hardware y software de la empresa? 9. ¿El responsable del área de informática conoce la clave de acceso de los usuarios? 10. ¿Se efectúan con cierta periodicidad la rotación del personal del área de informática? 11. ¿La empresa capacita periódicamente al personal de informática? 12. ¿Existen políticas de motivación para el área de informática? 13. ¿Cuándo hay nuevos empleados éstos son objetos de una atención especial, en cuanto a capacitación?			
	NOMBRE		FIRMA
ELABORADO POR:			FECHA
REVISADO POR:			

<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034		AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO ÁREA DE PLANIFICACIÓN		REFERENCIA A
PREGUNTAS		Respuestas		OBSERVACIONES Y COMENTARIOS
		Si	No	
GENERALES				
1. ¿Se ha elaborado un presupuesto del área de informática?				
2. ¿Se justifican sistemáticamente el incremento en los costos del área de informática?				
3. ¿Los involucrados tienen conocimiento de los objetivos incluidos en los planes?				
1. ¿Los planes sobre procesos de datos están integrados en los planes estratégicos para toda la empresa?				
2. ¿Los cambios en los sistemas informáticos son consecuencia de la planificación más que de la presión por necesidades operativas?				
3. ¿Están planificados los servicios externos tanto de hardware como de software?				
4. ¿Se solicitan demostraciones sobre nuevos artículos a los proveedores?				
5. ¿Existen estudios de disponibilidad comercial de paquetes de aplicación adecuados en cada momento?				
6. ¿Se consideran en las estimaciones de costos, los recursos adicionales que pueden ser necesarios para la evolución del sistema?				
7. ¿El equipo de informática es utilizado para generar información ajena a la actividad normal de la empresa?				
	NOMBRE	FIRMA		FECHA
ELABORADO POR:				
REVISADO POR:				

<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO ÁREA DE PLANIFICACIÓN		REFERENCIA A
PREGUNTAS	Respuestas		OBSERVACIONES Y COMENTARIOS
	Si	No	
DESARROLLO 1. ¿Se sabe si existe un adecuado paquete de software que pueda adquirirse como una alternativa conveniente y oportuna al desarrollo interno de un nuevo sistema? 2. ¿Se ha desarrollado un plan de aplicaciones que cubra las necesidades de información durante el periodo táctico? 3. ¿Se ha desarrollado un plan de proyectos que cubra las necesidades de los planes tácticos de datos y aplicaciones? 4. ¿Participan los usuarios, que corresponda en cada caso en la definición de la cartera de aplicaciones? 5. ¿Cómo parte de la aceptación del proyecto, el gerente de PED da su aprobación, haciendo constar que la documentación está completa y actualizada?			
	NOMBRE		FIRMA
ELABORADO POR:			FECHA
REVISADO POR:			

3.7.2 Cuestionarios de Evaluación de la Organización y Administración

<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO ORGANIZACIÓN Y ADMINISTRACIÓN		REFERENCIA B
PREGUNTAS	Respuestas		OBSERVACIONES Y COMENTARIOS
	Si	No	
ESTRUCTURA 1. ¿Existe una persona encargada del área de informática? 2. ¿Una vez fijada la posición del departamento informático dentro del organigrama general de la empresa? 3. ¿Se ha diseñado un plan de trabajo del área de informática? 4. ¿Se ha detectado las unidades funcionales más afectadas por la existencia del PED? 5. ¿Las aplicaciones planificadas o en desarrollo son susceptibles de introducir algún cambio en la organización? 6. ¿Existe una buena opinión generalizada del PED? 7. ¿Están definidas las dependencias funcionales en un organigrama del departamento? 8. ¿Existen manuales de funciones para cada una de las personas del departamento? 9. ¿La gerencia del PED administra realmente el departamento usando técnicas apropiadas para planear, programar y supervisar el trabajo? 10. ¿Es personal de desarrollo tiene prohibido el operar la Unidad Central de Proceso? 11. ¿Hay seguimiento a la calidad del servicio informático? 12. ¿Se efectúan regularmente misiones de auditoria de la actividad de informática?			
	NOMBRE		FIRMA
ELABORADO POR:			FECHA
REVISADO POR:			

<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO ORGANIZACIÓN Y ADMINISTRACIÓN		REFERENCIA B
PREGUNTAS	Respuestas		OBSERVACIONES Y COMENTARIOS
	Si	No	
ORGANIZACIÓN Y PLANIFICACIÓN 1. ¿Están equilibrados los recursos con los objetivos a cubrir? 2. ¿Se asignan prioridades en desarrollo de proyectos? 3. Si es así, ¿en función de que se hace? Por la relación costo – beneficio Por estudios de viabilidad Por imposición de departamentos usuarios 4. ¿Son adecuados los procedimientos? 5. ¿Se utilizan correctos procedimientos presupuestarios para la imputación de costos en el departamento? 6. ¿Existe una clara definición de objetivos? 7. ¿Hay algún servicio informático no previsto en la organización del departamento? 8. ¿Se ejecutan con regularidad los controles de calidad de los software?			
	NOMBRE		FIRMA
ELABORADO POR:			FECHA
REVISADO POR:			

<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO ORGANIZACIÓN Y ADMINISTRACIÓN		REFERENCIA B
PREGUNTAS	Respuestas		OBSERVACIONES Y COMENTARIOS
	Si	No	
FORMACIÓN 1. ¿El desarrollo de aplicaciones tiene en cuenta el nivel de adecuación y formación de personal? 2. ¿Existen proyectos planificados o en desarrollo que requieran el uso de categorías por encima del nivel del personal? 3. ¿Se ha evaluado el grado de conocimiento del personal en las siguientes áreas? Sistemas operativos Nuevos equipos Sistema general de base de datos Comunicaciones Metodología de análisis y programación 4. ¿Existe un importante número de personal condicionado por sus limitaciones técnicas? 5. ¿Hay presupuestos de tiempo y dinero para el departamento de informática			
	NOMBRE		FIRMA
ELABORADO POR:			FECHA
REVISADO POR:			

<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034		AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO ORGANIZACIÓN Y ADMINISTRACIÓN		REFERENCIA B
PREGUNTAS		Respuestas		OBSERVACIONES Y COMENTARIOS
		Si	No	
DOCUMENTACIÓN				
1. ¿Hay normas que definen el modo de documentar aplicaciones?				
2. ¿Se están formulando manuales de usuario con el suficiente nivel de comprensión?				
3. ¿Se documentan todas y cada una de las fases del desarrollo de una aplicación?				
4. ¿Se utilizan herramientas de ayuda o soporte a la documentación?				
5. ¿Los cambios en los programas quedan reflejados en la documentación?				
6. ¿Hay copia de toda la documentación?				
	NOMBRE	FIRMA		FECHA
ELABORADO POR:				
REVISADO POR:				

<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034		AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO ORGANIZACIÓN Y ADMINISTRACIÓN		REFERENCIA B
PREGUNTAS		Respuestas		OBSERVACIONES Y COMENTARIOS
		Si	No	
INFORMES				
1. ¿Son efectivos los informes, que se elevan a la jefatura informática y a las altas instancias de la dirección?				
2. ¿Estos informes incorporan suficientes elementos como para que la dirección emprenda medidas correctivas, si es el caso?				
3. ¿Son adecuados los informes utilizados para controlar la actividad de análisis?				
4. ¿Son destruidas las impresiones no utilizadas?				
	NOMBRE	FIRMA		FECHA
ELABORADO POR:				
REVISADO POR:				

<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO ORGANIZACIÓN Y ADMINISTRACIÓN		REFERENCIA B
PREGUNTAS	Respuestas		OBSERVACIONES Y COMENTARIOS
	Si	No	
SEGREGACIÓN DE FUNCIONES 1. ¿Son apropiados los grupos de trabajo definidos? 2. ¿Se utilizan sin ningún método estos grupos de trabajo? 3. ¿La utilización se hace en función de la naturaleza del trabajo a realizar? 4. ¿Están bien distribuidas las responsabilidades dentro del departamento? 5. ¿Esta distribución está documentada?			
	NOMBRE		FIRMA
ELABORADO POR:			FECHA
REVISADO POR:			

3.7.3 Cuestionarios de Evaluación del Entorno Operativo de Hardware

<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO ENTORNO OPERATIVO HARDWARE		REFERENCIA C
PREGUNTAS	Respuestas		OBSERVACIONES Y COMENTARIOS
	Si	No	
SEGURIDAD FÍSICA			
1. ¿Se han dispuesto dispositivos de protección de la unidad central de proceso y de la memoria central?			
2. ¿Se han detectado una especial concentración de riesgos naturales que puedan afectar al local PED?			
3. ¿La sala dispone de las medidas necesarias de acondicionamiento de aire, suelo falso, ventilación, etc.?			
4. ¿Hay dispositivos para minimizar el efecto de una inundación en la sala?			
5. ¿El equipo de informática está protegido con baterías y reguladores de voltaje por fallas eléctricas inesperadas?			
6. ¿Está polarizado el sistema eléctrico, al cual están conectadas las computadores?			
7. ¿El almacenamiento de cintas, discos, disquetes, etc. Ofrece los suficientes elementos de seguridad?			
8. ¿El equipo está asegurado contra cualquier eventualidad?			
9. ¿Existe un seguro específico para cubrir el equipo de la unidad central de proceso?			
10. ¿Existe personal de seguridad en la empresa?			
11. ¿Se protege el equipo de informática con cubiertas especiales?			
12. ¿El área de informática y toda la empresa está protegida contra incendios?			
13. Existe contrato de mantenimiento preventivo y correctivo para el equipo			
14. ¿Existe una política de depreciación del equipo de computo?			
15. ¿Existe una política de que hace con el equipo de computo dañado y obsoleto?			
16. ¿Existe un procedimiento para la adquisición del nuevo equipo de computo?			
	NOMBRE		FIRMA
ELABORADO POR:			
REVISADO POR:			FECHA

<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO ENTORNO OPERATIVO HARDWARE		REFERENCIA C
PREGUNTAS	Respuestas		OBSERVACIONES Y COMENTARIOS
	Si	No	
COMUNICACIONES			
1. ¿Cómo se efectúa la transmisión de datos? Telefónicamente Microondas Satélite			
2. ¿Los errores son detectados automáticamente?			
3. ¿Se obtiene reportes históricos de los mensajes recibidos?			
4. Se emplea código y procedimientos de transmisión especiales			
	NOMBRE	FIRMA	FECHA
ELABORADO POR:			
REVISADO POR:			

<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO ENTORNO OPERATIVO HARDWARE		REFERENCIA C
PREGUNTAS	Respuestas		OBSERVACIONES Y COMENTARIOS
	Si	No	
<p>ACCESOS LOGICOS</p> <p>1. ¿Posee contraseña para acceder a su máquina?</p> <p>2. ¿Posee contraseña para acceder a cada uno de los programas que utiliza?</p> <p>3. ¿Se actualizan regularmente?</p> <p>4. ¿Se conoce en forma precisa una lista auténtica de usuarios autorizados con sus derechos y asignaciones a cada función del programa?</p> <p>5. ¿Se da seguimiento a los intentos de violación a los intentos de violación de accesos a terminales?</p> <p>6. ¿Se ha detectado una adecuada sensibilización de los usuarios, en lo que respecta a la confidencialidad de los perfiles?</p> <p>7. Si el mantenimiento de los perfiles está centralizado en los responsables de la seguridad: ¿Puede modificar la tabla alguna persona distinta de este responsable? ¿Se mantiene un "log", de los cambios habidos en las tablas de perfiles?</p> <p>8. ¿Se conoce de forma precisa la auténtica lista de usuarios autorizados con sus derechos y asignaciones, a cada función de programas y ficheros (perfiles de usuario)?</p> <p>9. ¿Se realizan seguimientos mediante un log de las diferentes violaciones de acceso en terminales?</p> <p>10. ¿El fichero de perfiles está encriptado o goza de una protección adicional?</p> <p>11. ¿Existen restricciones de las funciones a realizar según la localización de cada terminal?</p> <p>12. ¿Se han establecido controles para impedir para que procesos lanzados en batch (lotes), puedan obtener accesos mayores que los que correspondían a una ejecución online (interactiva)?</p>			
	NOMBRE		FIRMA
ELABORADO POR:			
REVISADO POR:			FECHA

<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO ENTORNO OPERATIVO HARDWARE		REFERENCIA C
PREGUNTAS	Respuestas		OBSERVACIONES Y COMENTARIOS
	Si	No	
ACCESOS FÍSICOS 1. ¿Existe una localización y señalización conveniente de las áreas sensibles? 2. ¿Hay procedimientos de cobertura de las visitas al área de PED? 3. ¿Están restringidos los derechos de acceso a la sala del computador? 4. ¿Se han implantado mecanismos de identificación del personal? 5. ¿La ubicación del departamento PED es independiente del resto de los departamentos?			
	NOMBRE		FIRMA
ELABORADO POR:			
REVISADO POR:			

3.7.4 Cuestionarios de Evaluación de la Construcción de Sistemas

<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO CONSTRUCCIÓN DE SISTEMAS		REFERENCIA D
PREGUNTAS	Respuestas		OBSERVACIONES Y COMENTARIOS
	Si	No	
DESARROLLO 1. ¿Existen procedimientos adecuados para el desarrollo y prueba de sistemas? 2. ¿Los desarrollos están basados en un conjunto formal de requerimientos? 3. ¿Los datos generados por los programas sirven para la toma de decisiones de la gerencia? 4. El proceso de desarrollo incluye la necesidad de aprobación por parte del usuario, antes de proseguir, en puntos clave tales como: Estudio de la factibilidad Propuestas del diseño del sistema Especificaciones del estudio Determinación de los controles de usuario Realización de paralelos o de pruebas de aceptación del sistema Modificaciones al sistema anteriores a su implantación 5. El planeamiento de proyectos y los métodos de control son empleados tanto como para indicar: Que los proyectos están adecuadamente planeados Que el progreso es supervisado en forma tal que asegura que las áreas de problemas son rápidamente descubiertos			
	NOMBRE		FIRMA
ELABORADO POR:			FECHA
REVISADO POR:			

<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO CONSTRUCCIÓN DE SISTEMAS		REFERENCIA D
PREGUNTAS	Respuestas		OBSERVACIONES Y COMENTARIOS
	Si	No	
PRUEBAS 1. ¿Los procedimientos para pruebas del sistema están incluidos en los estándares de la instalación? 2. ¿Las pruebas utilizan datos inteligibles? 3. ¿Se están utilizando en las pruebas ficheros productivos? 4. ¿Se han definido librerías para pruebas? 5. ¿Se realizan pruebas del sistema completo para verificar las interacciones entre programas? 6. ¿Antes de implantar un sistema se realizan paralelos adecuados? 7. ¿Se guardan los ficheros de pruebas para su posterior uso en el mantenimiento del sistema? 8. ¿Se están comprometiendo a los usuarios en la revisión de las pruebas del sistema? 9. ¿Se ejecutan con regularidad los controles de calidad a los software? 10. ¿Es satisfactoria la calidad del software?			
	NOMBRE		FIRMA
ELABORADO POR:			FECHA
REVISADO POR:			

<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO CONSTRUCCIÓN DE SISTEMAS		REFERENCIA D
PREGUNTAS	Respuestas		OBSERVACIONES Y COMENTARIOS
	Si	No	
IMPLANTACIÓN 1. ¿Queda constancia de las autorizaciones para transferir los programas a las librerías productivas? 2. ¿Verifican los usuarios que los posibles cambios han sido desarrollados correctamente? 3. ¿Se efectúan los oportunos entrenamientos a los futuros usuarios?			
	NOMBRE		FIRMA
ELABORADO POR:			
REVISADO POR:			

3.5.6 Cuestionarios de Evaluación del Entorno Operativo de Software

<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO ENTORNO OPERATIVO SOFTWARE		REFERENCIA E
PREGUNTAS	Respuestas		OBSERVACIONES Y COMENTARIOS
	Si	No	
UTILIDADES Y SOFTWARE			
1. ¿Poseen licencia para utilizar el software?			
2. ¿Se tiene un programa de asistencia técnica sobre el uso y actualización del software?			
3. ¿El software posee bitácora?			
4. ¿En caso de falla del programa existe un responsable?			
5. Existen controles sobre el uso de utilitarios: ¿Limitaciones en el numero de usuarios? ¿Autorización de uso? ¿Queda registrado su uso? ¿Se almacena fuera del almacenamiento principal? ¿Se verifican los medios magnéticos antes de usarse en la computadora con respecto a copias fraudulentas o infectados con virus			
6. ¿Está separado el departamento de sistemas del resto de las funciones del procedo de datos?			
7. ¿Se controlan las modificaciones del software del sistema?			
8. ¿Están documentadas estas modificaciones?			
9. ¿Se pueden detectar modificaciones?			
10. ¿Las modificaciones y procedimientos del sistema son aprobados por la autoridad competente?			
11. ¿La solicitud de modificaciones a los programas se hacen por escrito?			
12. ¿Existe un procedimiento formal que se debe seguir antes de que un sistema o programa sea aceptado y puesto en marcha?			
	NOMBRE	FIRMA	FECHA
ELABORADO POR:			
REVISADO POR:			

<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034		AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO ENTORNO OPERATIVO SOFTWARE		REFERENCIA E
PREGUNTAS		Respuestas		OBSERVACIONES Y COMENTARIOS
		Si	No	
PROTECCION DE FICHEROS				
1. ¿Está prohibido el acceso a las librerías productivas?				
2. ¿En programación es obligatoria la norma de establecer controles y validaciones a los datos de entrada?				
3. ¿Se establecen también controles de salida?				
4. ¿Se revisa periódicamente el contenido de los ficheros?				
5. ¿Se revisan regularmente las versiones de los programas productivos?				
6. ¿Se recopilan los programas cuando pasan a la librería de explotación?				
7. ¿Existe un programa actualizado de antivirus?				
	NOMBRE	FIRMA		FECHA
ELABORADO POR:				
REVISADO POR:				

<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034		AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO ENTORNO OPERATIVO SOFTWARE		REFERENCIA E
PREGUNTAS		Respuestas		OBSERVACIONES Y COMENTARIOS
		Si	No	
COPIAS DE RESPALDO (BACKUP)				
1. ¿Existen normas debidamente documentadas respecto de la obtención de copias de seguridad?				
2. ¿Se guardan periódicamente los archivos generados y copias de respaldo?				
3. ¿Existe y se mantiene actualizado un backup exterior?				
4. ¿Se utilizan paquetes de ayuda en la gestión y obtención del backup?				
5. ¿Se realizan con cierta regularidad análisis del contenido de los discos de seguridad para suprimir archivos no utilizados?				
6. ¿En caso de accidente, están definidas las modalidades de recuperación de datos?				
	NOMBRE	FIRMA		FECHA
ELABORADO POR:				
REVISADO POR:				

<i>Consultores Cisneros Beltrán y Asociados</i> Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO ENTORNO OPERATIVO SOFTWARE		REFERENCIA E	
PREGUNTAS	Respuestas		OBSERVACIONES Y COMENTARIOS	
	Si	No		
<p>BASE DE DATOS</p> <ol style="list-style-type: none"> 1. ¿Se obtienen regularmente copias de la base de datos? 2. ¿Se chequean regularmente la base de datos para garantizar su integridad? 3. ¿Se efectúan reorganizaciones periódicas de los ficheros de la base de datos? 4. ¿Se obtiene un registro de las terminaciones anormales de los procesos que acceden a la base de datos? 5. ¿Existe y se revisa un log de las transacciones a la base de datos? 6. ¿Se realiza un chequeo regular de las claves y punteros para la consistencia interna? 7. ¿Existe documentación y prueba periódica de los procedimientos de restauración de la base de datos? 8. ¿Se han previsto técnicas para evitar el bloqueo de procesos en demanda de datos? 9. ¿Se facilita la adecuada formación técnica al staff de proceso de datos? 10. ¿Se han definido los procedimientos de seguridad para el acceso a entidades de datos? 11. ¿Es necesaria autorización para el uso de utilidades del sistema de gestión de la base de datos para actualizarla? 12. ¿Se han definido inequívocamente las funciones del administrador de la base de datos? 13. ¿Se implica a los usuarios a la propiedad de los datos? 				
	NOMBRE		FIRMA	FECHA
ELABORADO POR:				
REVISADO POR:				


3.5.7 Evaluación del riesgo

ÁREA	TIPO DE RIESGO	NIVEL		
		ALTO	MEDIO	BAJO
PLANIFICACIÓN	Riesgo de detección		X	
Sistemas de información				
Recursos humanos				
Generales				
Desarrollo				
ORGANIZACIÓN Y ADMINISTRACIÓN	Riesgo de control		X	
Estructura				
Organización y Planificación				
Formación				
Documentación				
Informes				
ENTORNO OPERATIVO HARDWARE	Riesgo de control	X		
Seguridad Física				
Accesos Lógicos				
Accesos Físicos				
CONSTRUCCIÓN DE SISTEMAS				X
Desarrollo				
Pruebas				
Implantación				
ENTORNO OPERATIVO SOFTWARE	Riesgo inherente		X	
Utilidades y Software				
Protección de Ficheros Productivos				
Copias de Respaldo (Backup)				
Base de datos				
	NOMBRE	FIRMA	FECHA	
ELABORADO POR:				
REVISADO POR:				

3.6 EVALUACIÓN DE LOS PUNTOS DE CONTROL DE INFORMATICA

Consultores Cisneros Beltrán y Asociados Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO EVALUACIÓN DE CONTROLES		REFERENCIA F
	PREGUNTAS		
	Respuestas		OBSERVACIONES Y COMENTARIOS
Si	No		
<input type="checkbox"/> CONTROLES DE LA APLICACIÓN POR LOS USUARIOS Controles sobre los Datos de Entrada <ul style="list-style-type: none"> ▶ ¿Existen controles del usuario sobre la preparación y aprobación de transacciones? ▶ ¿El usuario controla la entrada de datos? 			
Controles sobre los Datos Fijos <ul style="list-style-type: none"> ▶ ¿Existen controles del usuario sobre las modificaciones de los datos fijos que se realicen en los archivos maestros y tablas del sistema? ▶ ¿Existen controles del usuario sobre la permanente integridad y exactitud de los datos fijos correspondientes a archivos maestros y tablas? ▶ 			
Controles sobre Ítems Rechazados y en Suspense <ul style="list-style-type: none"> ▶ ¿Existen controles del usuario sobre las transacciones rechazadas? ▶ ¿Son los ítems en suspenso controlados por los usuarios? 			
Controles sobre Datos de Salida <ul style="list-style-type: none"> ▶ ¿Existen controles del usuario sobre los datos de salida? 			
<input type="checkbox"/> CONTROL DE APLICACIONES POR EL GRUPO DE CONTROL DE DATOS Controles sobre los Datos de Entrada <ul style="list-style-type: none"> ▶ ¿Los datos de entrada son controlados por el grupo de control de datos? 			
Controles sobre los Datos de Salida <ul style="list-style-type: none"> ▶ ¿Existen dentro del grupo de control de datos procedimientos de control con relación al examen y distribución de los datos de salida? 			

Consultores Cisneros Beltrán y Asociados Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO EVALUACIÓN DE CONTROLES		REFERENCIA F		
				PREGUNTAS	
		Si	No		
<input checked="" type="checkbox"/> CONTROL DE APLICACIONES POR EL PROCESAMIENTO DE DATOS Controles sobre los Datos de Entrada <ul style="list-style-type: none"> ▶ ¿Existen controles sobre la digitación de datos? ▶ ¿Existe consistencia y validación de los datos de entrada? 					
Controles sobre los Ítems en Suspenseo <ul style="list-style-type: none"> ▶ ¿Existen controles del procesamiento de datos sobre los ítems en suspenseo? 					
Controles sobre el Procesamiento <ul style="list-style-type: none"> ▶ ¿Existen controles de procesamiento para balancear los archivos de transacciones y maestros? ▶ ¿Existe una adecuada evidencia de auditoría? 					
<input checked="" type="checkbox"/> CONTROLES GENERALES Separación de Tareas y Seguridad <ul style="list-style-type: none"> ▶ ¿Existe una adecuada separación de tareas dentro del área de procesamiento de datos? ▶ ¿Existen controles para restringir el acceso físico no autorizado a la sala de la computadora, terminales, archivos en discos o cintas magnéticas y documentación de sistemas y programas? 					
Controles sobre el Software de Sistema <ul style="list-style-type: none"> ▶ ¿Existen controles sobre modificaciones al software de sistemas? 					
Controles sobre las operaciones <ul style="list-style-type: none"> ▶ ¿Existen procedimientos para minimizar el riesgo de que se procesen trabajos y programas no autorizados? ▶ ¿Existen controles para garantizar que se utilizan los archivos correctos? ▶ ¿El personal de operación de la computadora está, en todos los turnos, adecuadamente supervisado? 					

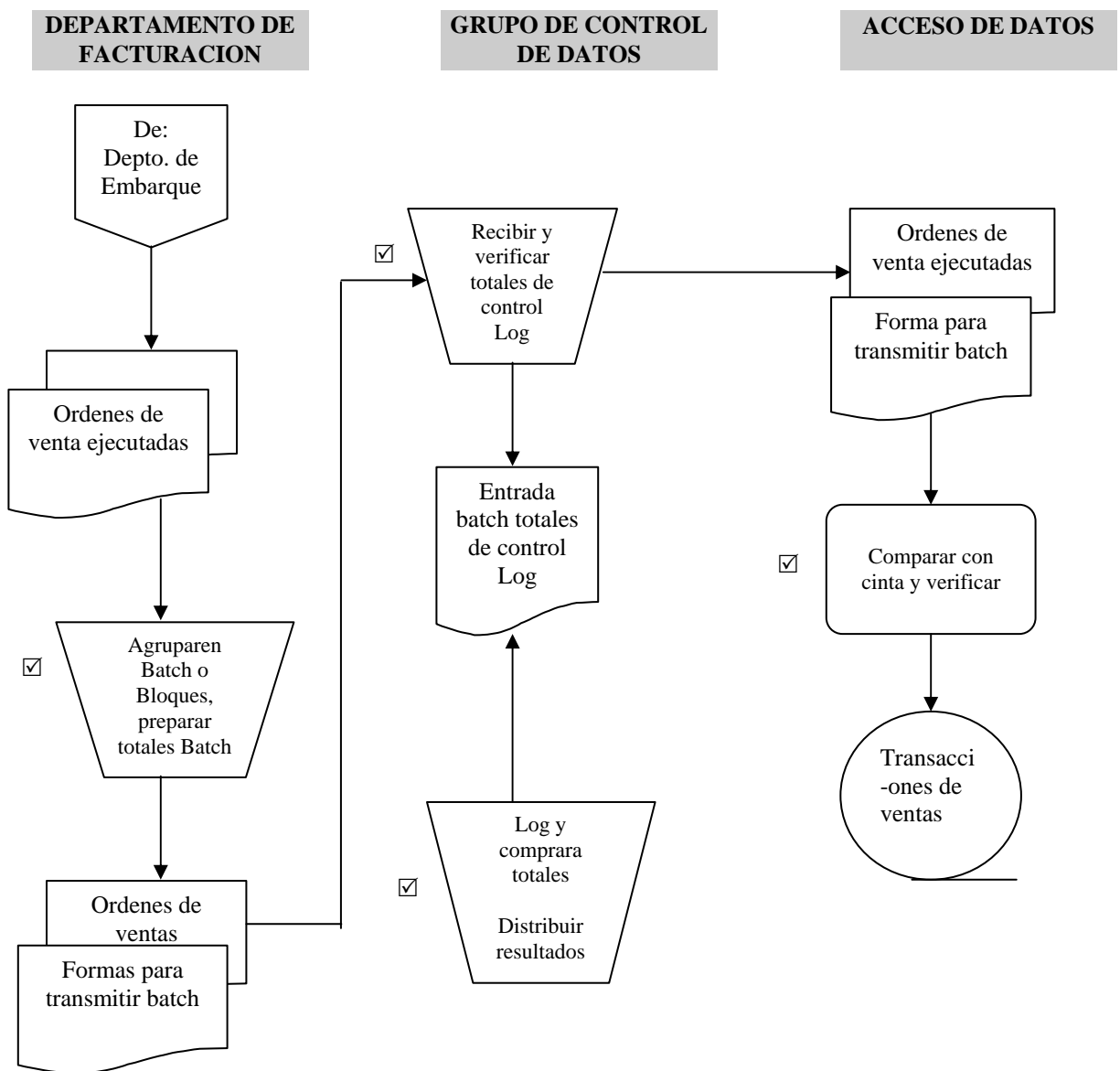
Consultores Cisneros Beltrán y Asociados Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO EVALUACIÓN DE CONTROLES		REFERENCIA F		
				PREGUNTAS	
		Si	No		
Controles sobre la Continuidad del Procesamiento <ul style="list-style-type: none"> ▶ ¿Existen procedimientos para evitar que un accidente que afecte la función PED pueda interrumpir totalmente el flujo de la información o resulte en la pérdida del control contable? ▶ ¿La documentación PED es lo suficientemente adecuada como para garantizar que el cliente podrá continuar operando aun en el caso de que miembros importantes del equipo PED hagan abandono de sus cargos? 					
Controles Sobre el Desarrollo de Sistemas <ul style="list-style-type: none"> ▶ ¿Participa el usuario en el desarrollo de nuevos sistemas y en las modificaciones a los ya existentes? ▶ ¿Existen procedimientos para la prueba de sistemas nuevos y modificaciones a los ya existentes? ▶ ¿Existen procedimientos para la implantación de nuevos sistemas y de modificaciones a los ya existentes? 					
 CONTROLES ADICIONALES PARA SISTEMAS AVANZADOS Controles sobre la Entrada de Datos en Línea <p>¿Existen controles para que el uso de las terminales en línea quede restringido únicamente a las personas autorizadas?</p> <p>¿Se balancean los totales de control de los datos entrados en línea?</p> <p>¿Existe adecuada evidencia de auditoría para cada uno de los ítems ingresados para procesamiento mediante la utilización de terminales en línea?</p>					
Procesamientos para Recuperación y Reenganche en Sistemas en Línea <p>¿Existen procedimientos de recuperación y reenganche para el caso de una interrupción de la transmisión o del procesamiento?</p>					
Controles sobre la Modificación de Programas en Línea <p>¿Existen controles sobre la modificación de programas en línea?</p>					

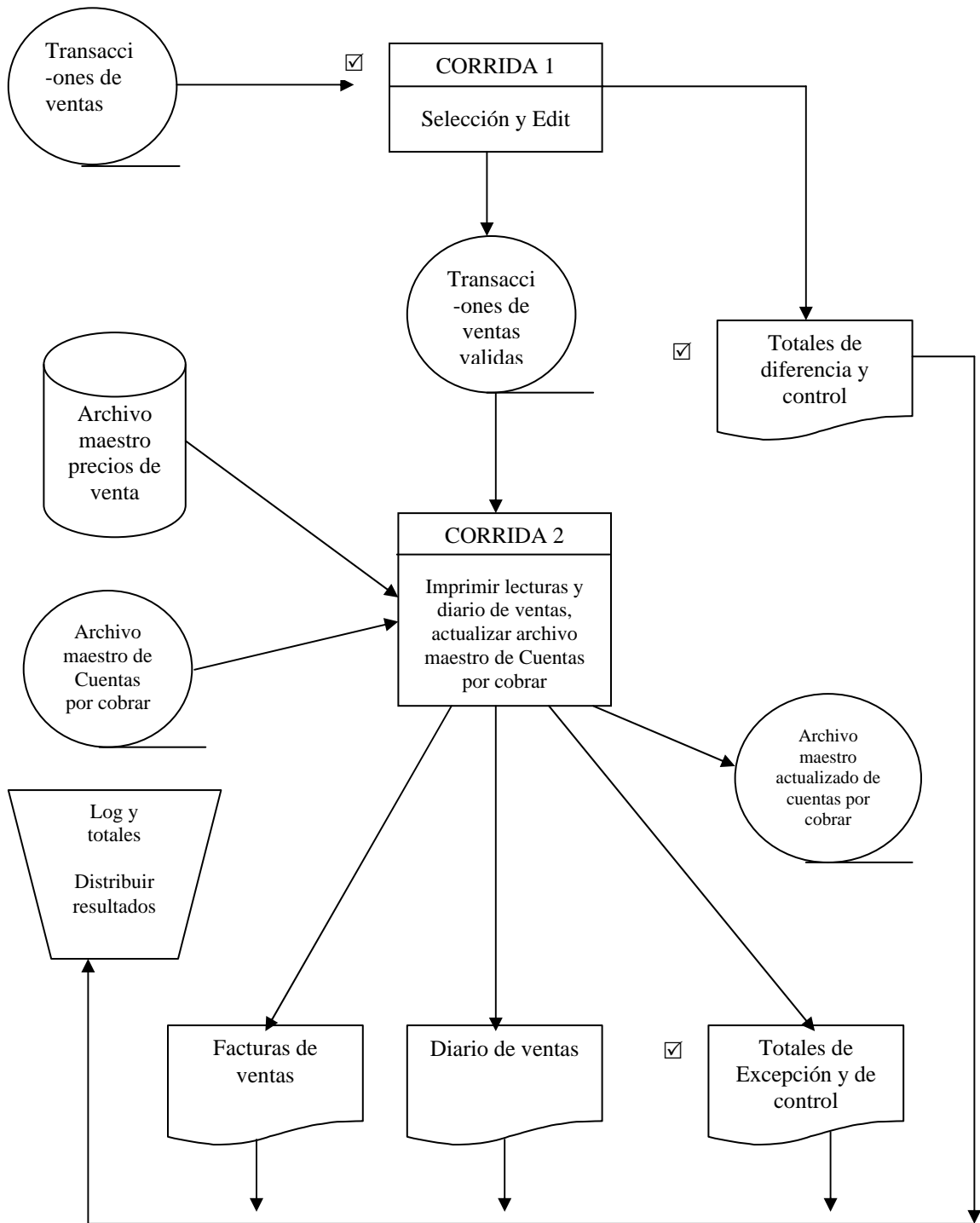
Consultores Cisneros Beltrán y Asociados Colonia Flor Blanca 51 Av. Sur # 430 San Salvador. Telefax 298-4034	AUDITORIA INFORMÁTICA CUESTIONARIO DE CONTROL INTERNO EVALUACIÓN DE CONTROLES		REFERENCIA F <hr/>
Controles sobre el Procesamiento Distribuido ¿Existen controles sobre el procesamiento distribuido?			
Controles de Sistemas Integrados ¿Existen procedimientos para controlar la transferencia de datos entre sistemas contables integrados?			
Controles sobre la base de datos ¿Existen controles sobre el sistema de manejo de la base de datos? ¿Existe la función de administración de la base de datos, o el diccionario / guía de datos, un registro de la estructura de la base de datos?			
	NOMBRE	FIRMA	FECHA
ELABORADO POR:			
REVISADO POR:			

3.7 USO DE FLUJOGRAMAS

Se utilizan para describir movimientos de documentos, tratamientos de información, pasadas o corridas de ordenador, descripciones de la lógica de los programas y sus especificaciones detalladas.

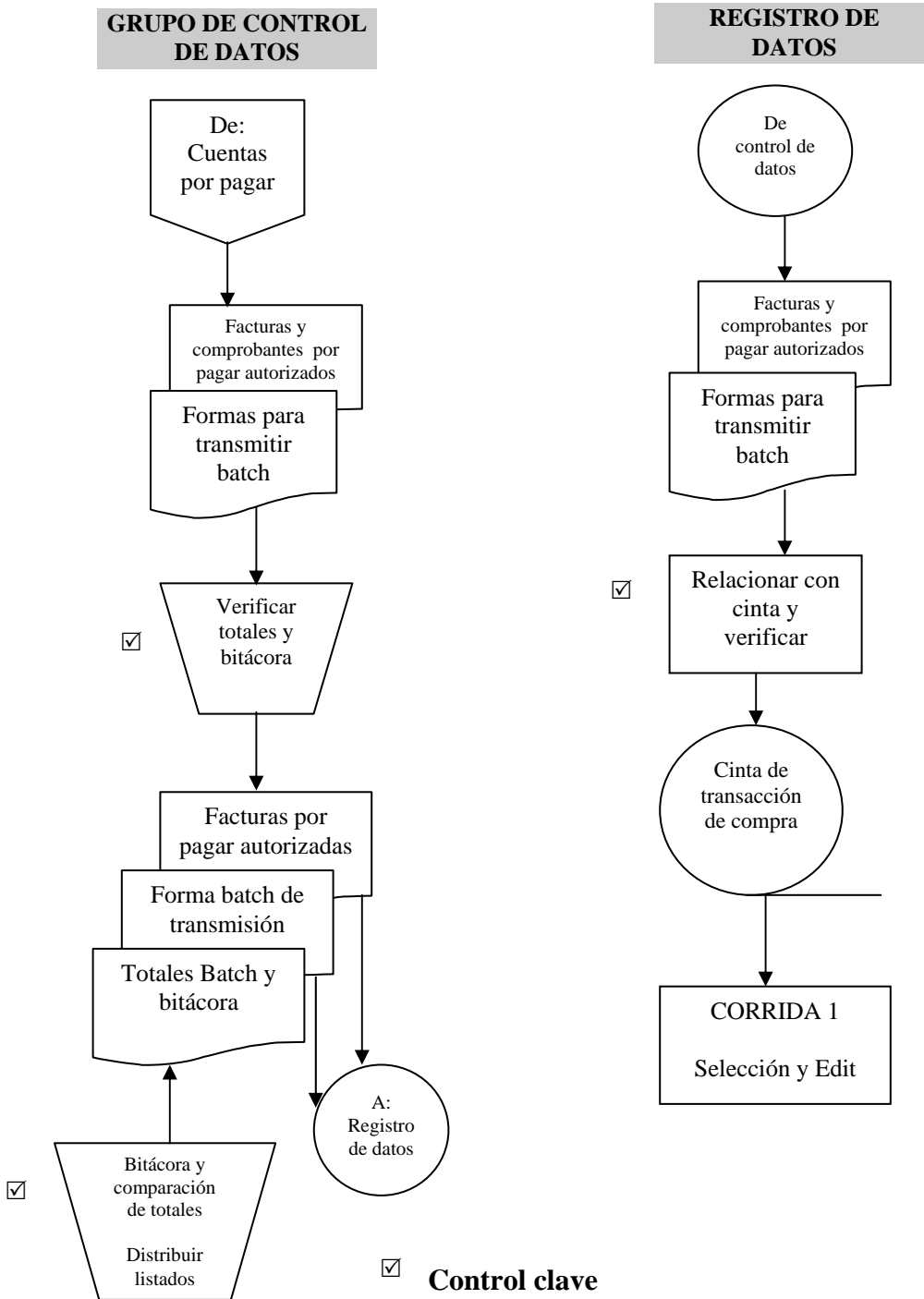
FLUJOGRAMA SISTEMA PED PARA TRANSACCIONES DE VENTAS

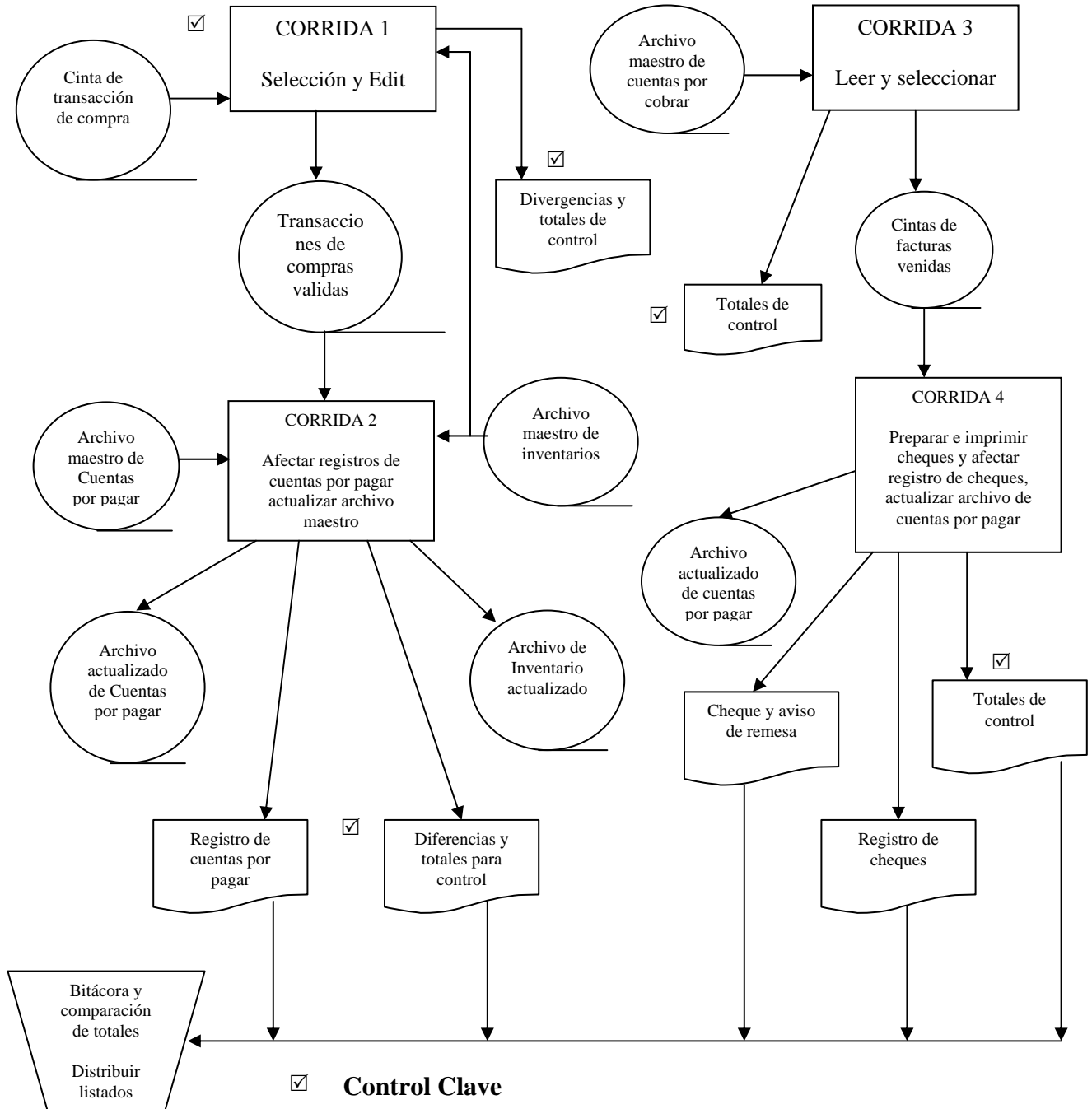




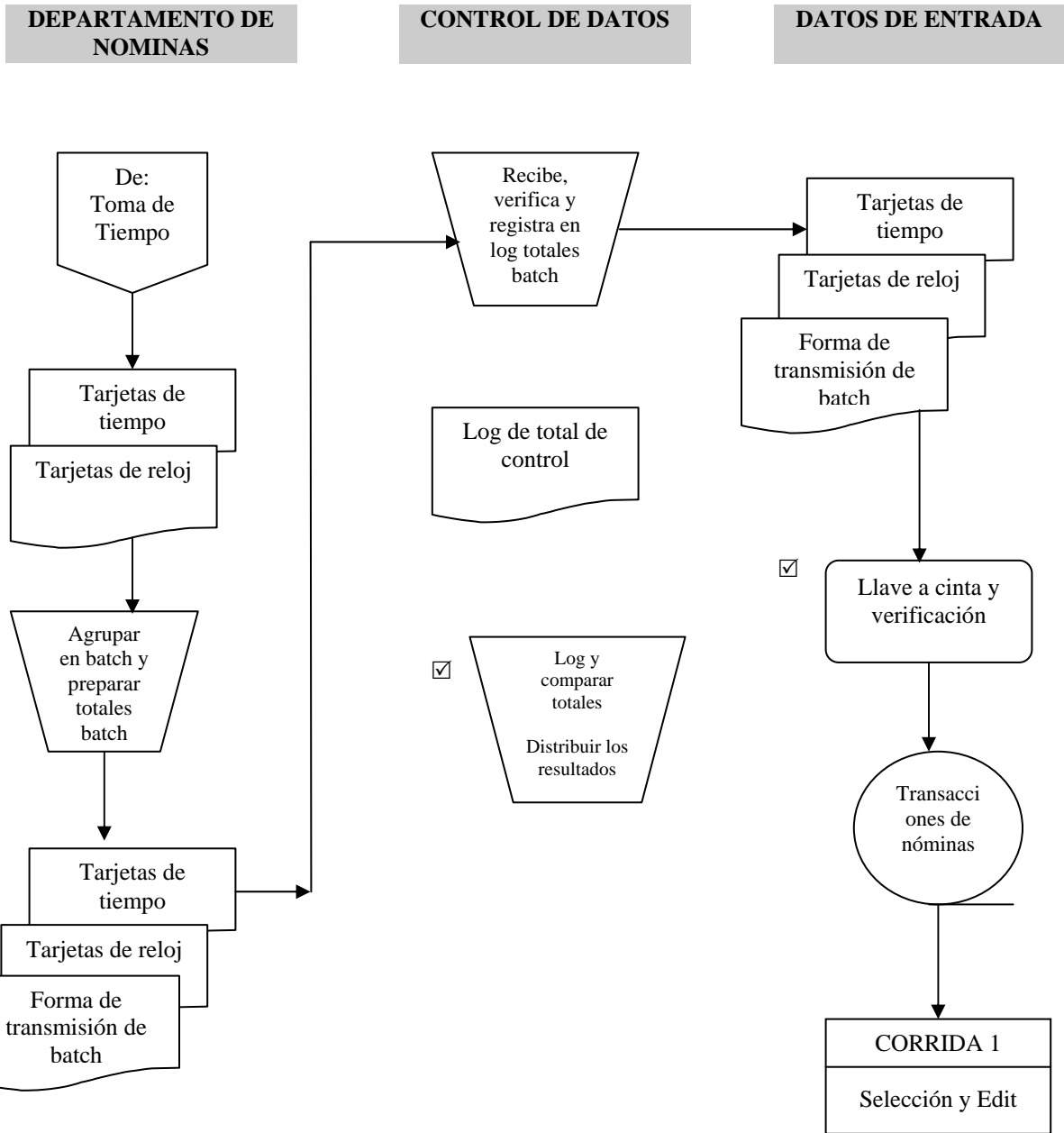
Control clave

FLUJOGRAMA SISTEMA PED PARA TRANSACCIONES DE COMPRAS Y DESEMBOLSOS EN EFECTIVO

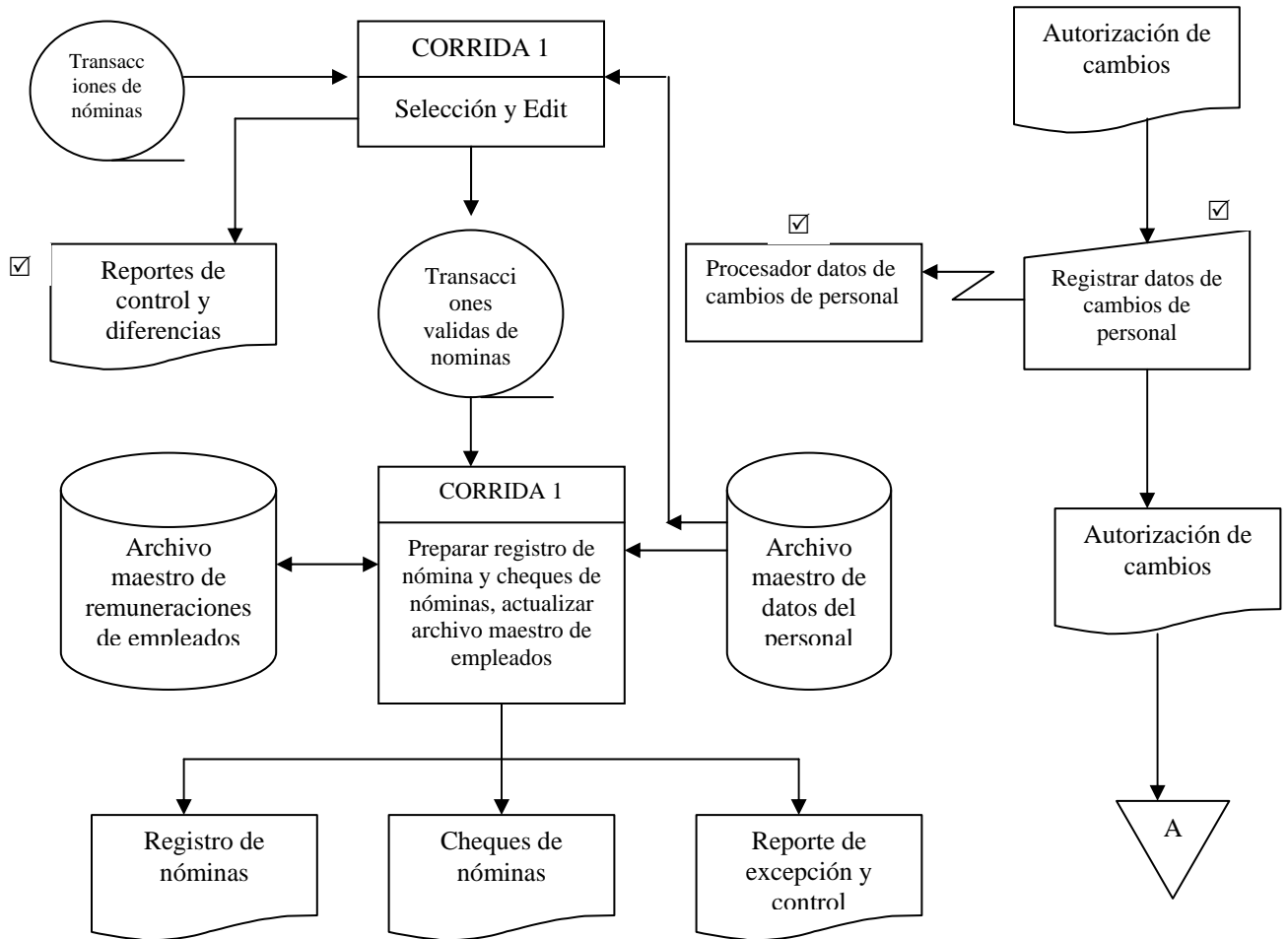




FLUJOGRAMA SISTEMA PED PARA TRANSACCIONES DEL PAGO DE NOMINA

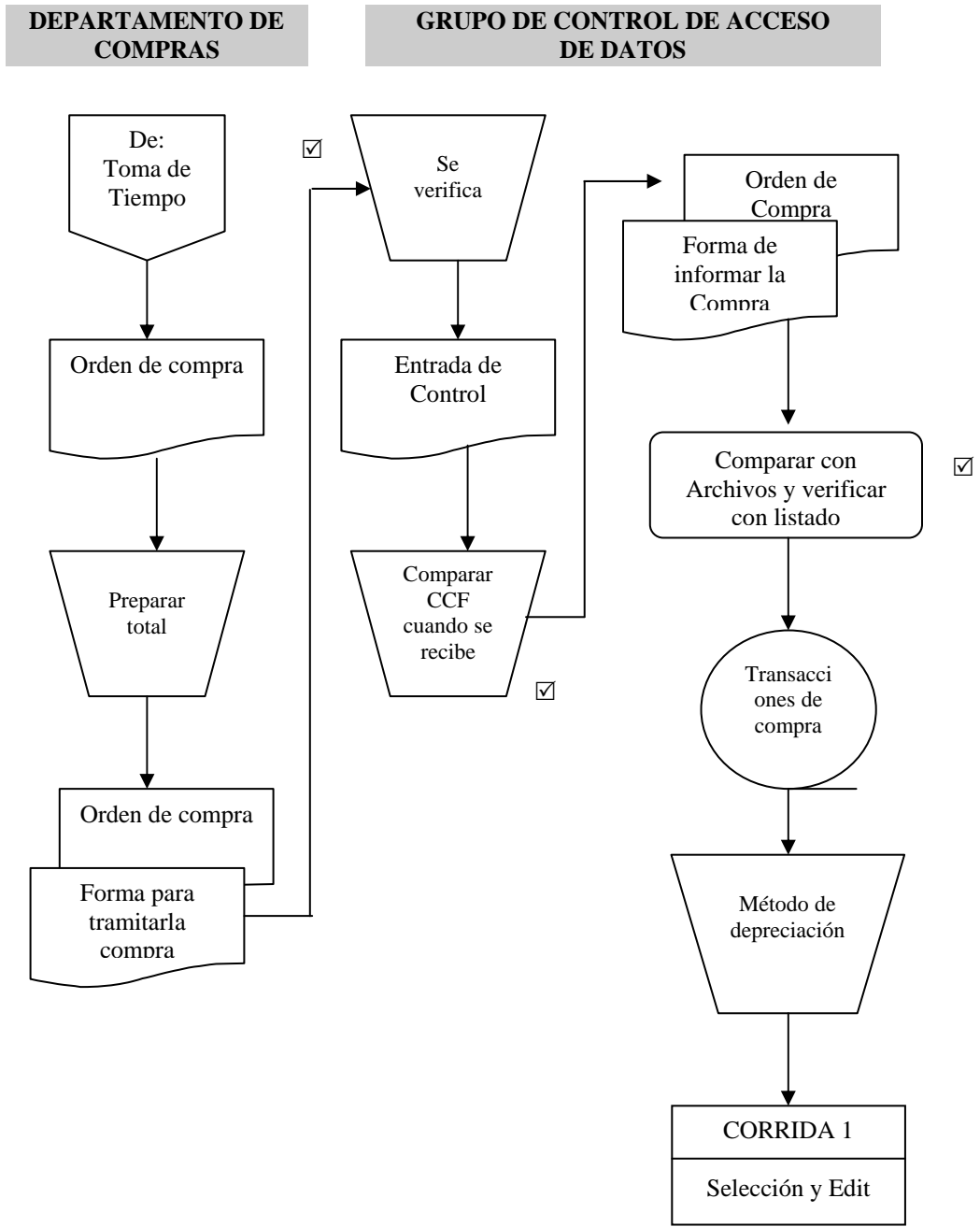


PROCEDIMIENTOS POR COMPUTADORA Y LISTADOS EMITIDOS

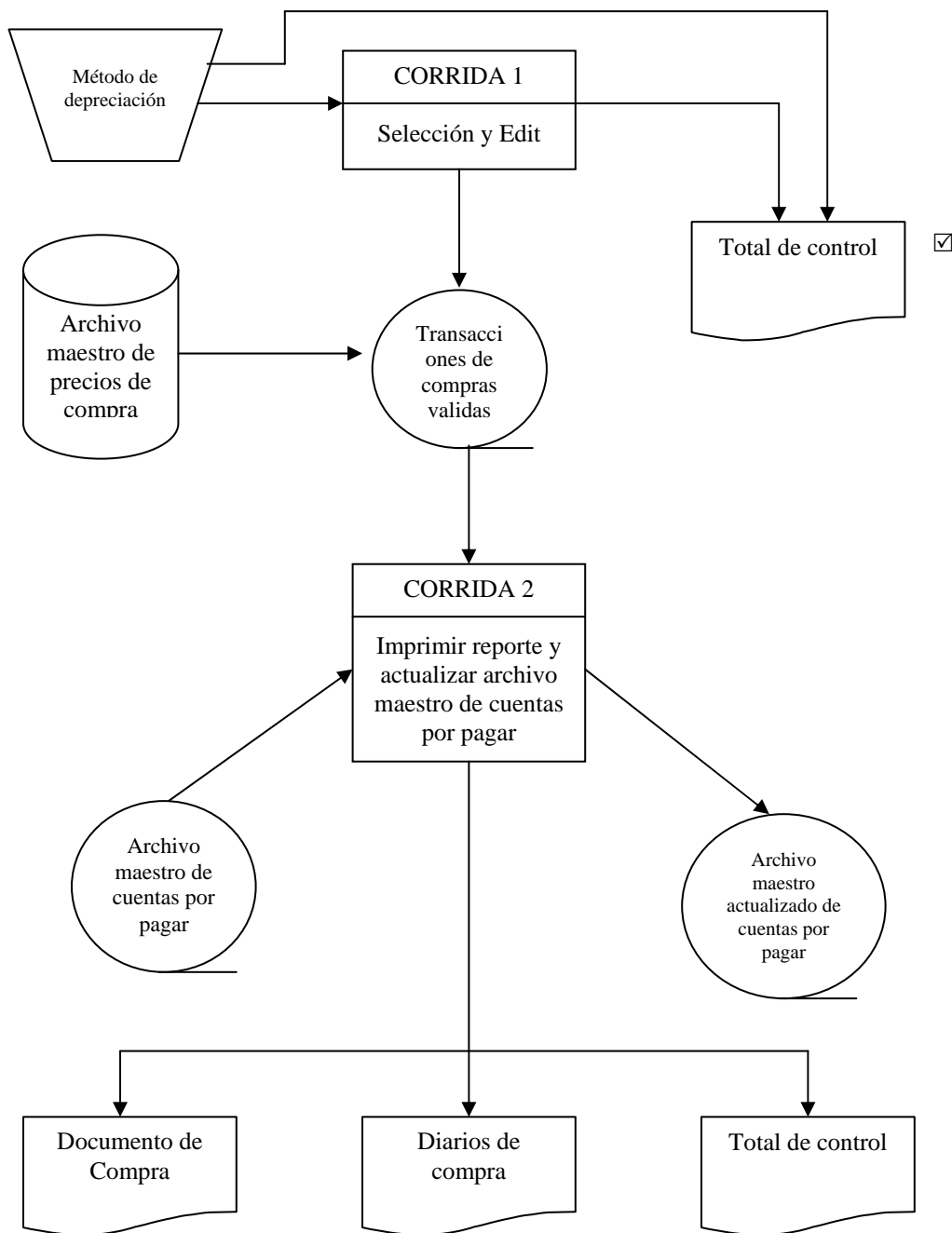


☑ **Control clave**

Sistema PED para Transacciones de Activo Fijo



PROCESAMIENTO DE COMPUTADORA Y RESULTADOS EMITIDOS



☑ **Control clave**

3.7.1 Evaluación del riesgo de los puntos de control de informática.

TIPO DE CONTROL	TIPO DE RIESGO	NIVEL		
		ALTO	MEDIO	BAJO
CONTROLES DE APLICACIÓN POR LOS USUARIOS	Riesgo de Deteccion		X	
Controles sobre datos de entrada				
Controles sobre los datos fijos				
Controles sobre ítems rechazados y en suspenso				
Controles sobre los datos de salida				
CONTROL DE APLICACIONES POR EL GRUPO DE CONTROL DE DATOS	Riesgo de Control			X
Controles sobre los datos de entrada				
Controles sobre los datos de salida				
CONTROLES DE APLICACIONES POR EL PROCESAMIENTO DE DATOS				
Controles sobre los datos de entrada				
Controles sobre los ítems en suspenso				
Controles sobre el procesamiento				
CONTROLES GENERALES	Riesgo inherente	X		
Separación de tareas y seguridad				
Controles sobre el software de sistemas				
Controles sobre las operaciones				
Controles sobre la continuidad del procesamiento				
Controles Sobre el desarrollo de sistemas				
CONTROLES ADICIONALES PARA SISTEMAS AVANZADOS	Riesgo de Deteccion			X
Controles sobre la entrada de datos en línea				
Procedimientos para recuperación y reenganche en sistemas en línea				
Controles sobre la modificación de programas en línea				
Controles sobre el procesamiento distribuido				
Controles de sistemas integrados				
Controles sobre la base de datos				
	NOMBRE	FIRMA	FECHA	
ELABORADO POR:				
REVISADO POR:				

3.8 INFORME DE CONTROL INTERNO

(CARTA DE GERENCIA)

San salvador, 23 de marzo de 2002.

Señores

Junta Directiva

DRUPY S.A. de C.V.

Presente

Estimados señores:

Hacemos de su conocimiento que este despacho de Auditoria y Consultoría ha realizado la evaluación del control interno, mediante cuestionarios con el objeto de establecer los alcances para examen del área de informática para el año 2002. De dicha evaluación se determinaron observaciones y recomendaciones en los puntos que se presentan a continuación:

OBSERVACIONES Y RECOMENDACIONES

1. Existe poca seguridad contra riesgos inesperados.

Se recomienda suscribir las pólizas de seguro de fidelidad y otras pertinentes para garantizar la seguridad tanto del equipo como del software instalado.

2. El sistema eléctrico de las computadoras no esta polarizado.

Por lo delicado del caso se vuelve necesario efectuar un estudio técnico a fin de superar esta deficiencia para la seguridad física del equipo y de los empleados que laboran en la unidad.

3. El equipo no es protegido con cubiertas especiales, siendo esta actividad necesaria para la vida útil del equipo de computo.

Es recomendable mandar a confeccionar cubiertas para la protección del equipo, para evitar el deterioro del mismo y reducir gastos en mantenimiento.

4. No existe restricción de acceso al lugar donde se guardan las copias de respaldo. *Debe ser restringido el acceso físico para evitar cualquier extravío o fuga de información, esto a través de un estudio del personal que ponga de manifiesto, cual es el personal con afinidad para el acceso a la unidad*

5. No existe contrato de mantenimiento preventivo y correctivo para el equipo informático

Es necesario los contratos de servicios pertinentes para evitar fallas en el equipo y prolongar la vida de los mismos.

6. No existe rotación del personal del área de informática.

Esto dificultar el desarrollo de las actividades de la empresa si en un determinado momento faltare un miembro del personal, probablemente no se encuentre un sustituto. Por lo que se recomienda diseñar un plan de rotación de personal.

7. El personal de informática no es capacitado periódicamente, lo cual llama la atención, puesto que por lo dinámico del área de informática, es necesario capacitar al personal de tal manera que este desarrolle su trabajo de manera eficiente.

8. No existen políticas de motivación para el área de informática

La motivación no es para toda el personal, lo cual podría ocasionar conflictos y descontentos en el personal. Se recomienda que todas las políticas de motivación sean equitativas para el personal de acuerdo al puesto desempeñado

9. La inducción de nuevos empleados es deficiente y algunas veces nula

Esto podría generar problemas de pérdida de archivos, daños en equipo y revelación inadecuada de la información; por lo tanto se recomienda elaborar un instructivo de bienvenida el cual contenga la inducción necesario al personal de nuevo ingreso.

10. No se posee contraseña para acceder a cada uno de los programas que se utilizan
Es necesario que todo el personal involucrado posea claves de acceso a todos los programas que utiliza en el área de producción.
11. No están definidas las modalidades de recuperación de datos en caso de accidente
Se considera necesario implantar este tipo de modalidad dentro de esta área, a fin de evitar la pérdida de información que se vuelva irrecuperable
12. Las impresiones no utilizadas, no son destruidas
Se recomienda girar instrucciones e incorporar al manual de procedimientos, el hecho de destruir todos los reportes generados y no utilizados, incluyendo cualquier impresión que comprometa a la unidad de informática y consecuentemente a la empresa.
13. La unidad de informática no posee actualizado el manual escrito de procedimientos.
Lo que se hace necesario para el buen funcionamiento de dicha unidad. Se recomienda actualizar todos los manuales diseñados para la unidad de informática por lo menos una vez cada seis meses debido a la dinámica de la unidad
14. No se ha diseñado un plan de trabajo en el área de informática
Se recomienda formular anualmente un plan de trabajo a fin de evaluar y controlar el avance y el cumplimiento de metas.
15. No se efectúan misiones de auditoría a la unidad de informática.
Esto recomendable realizar auditorías, para mejorar esta área porque el personal de esta unidad sabe que son supervisadas sus actividades.
16. No se ha elaborado un presupuesto en esta área
Se recomienda la elaboración anual del presupuesto a fin de conocer si los gastos incurridos son razonables a las actividades basándose en los objetivos y metas de la unidad.

17. No se ejecutan con regularidad los controles de calidad a los software

Se recomienda revisar lo controle de calidad por lo menos cada seis meses a fin de reformular el diseño de los mismos para su efectividad

18. No se analiza el contenido de los discos de seguridad para suprimir archivos no utilizados.

Debe revisarse periódicamente cada tres meses los archivos; los que son de utilidad para los usuarios y aquellos que contienen información que algún momento dado pueden ser de utilidad a fin de eliminar el volumen de archivos en desuso.

19. No existen copias de seguridad de los archivos informáticos fuera de la empresa

Se estima conveniente que por prevención a cualquier eventualidad se mantenga copia de archivos fuera del centro de computo de preferencia fuera de la empresa.

En espera de nuestras observaciones y recomendaciones sean de utilidad a su empresa, atentamente,

Maritza Elizabeth Argueta Arano

Jefe de Auditoria de sistemas
CISNEROS BELTÁN Y ASOCIADOS

CAPITULO IV

4. CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES

4.2.1. Los despachos que prestan el servicio de Auditoria en Informática no contemplan en su estructura organizativa el servicio en el área de Informática.

4.2.2. En el desarrollo de la auditoria en informática, no se da la debida importancia a la Evaluación del Control Interno.

4.2.3. Es poca la importancia que se da a la evaluación de la dirección del departamento de informática.

4.2.4. No se realiza un estudio preliminar de las operaciones PED para la obtención de información financiera.

4.2.5. Es de poca importancia la evaluación de así como la organización y la evaluación de los estándares operacionales.

4.2.6. La opinión de los usuarios y la evaluación del avance de los sistemas en desarrollo es casi nula.

4.2.7. No se utiliza la técnica de flujogramación como base técnica de la evaluación del control interno.

4.2.8. La evaluación del control interno la realiza empíricamente, es decir, de acuerdo con al experiencia adquirida en el desarrollo de su trabajo.

4.2 RECOMENDACIONES

- 4.2.1. Los despachos que prestan el servicio de Auditoría en Informática deben considerar dentro su organización la sección de auditoría en informática a fin de no quedar fuera de este mercado y lograr una especialización en esta rama.
- 4.2.2. Los despachos deben considerar la Evaluación del Control Interno, ya que esta es la base para la ejecución de toda auditoría, y la auditoría en informática no es la excepción.
- 4.2.3. La dirección de la unidad de informática es uno de los componentes de mayor importancia en la evolución y manejo del sistema PED, por lo tanto, es necesario que los despachos consideren este factor.
- 4.2.4. Siempre debe realizarse el estudio preliminar de las operaciones PED para la obtención de información financiera, ya que con este procedimiento se mide la efectividad de la unidad de informática.
- 4.2.5. Los estándares en las unidades de informática son base, ya que esto refleja el estilo y la efectividad del trabajo que ahí se desarrolla.
- 4.2.6. Se recomienda a los despachos tomar en cuenta la opinión de los usuarios ya que ellos proporcionan de manera formal o informal la realidad de los sistemas, que a veces son difíciles de detectar.
- 4.2.7. Dentro de la cambiante dinámica de la auditoría los despachos deben utilizar la flujogramación par efectos de la evaluación del control interno, ya que este queda reflejado en forma gráfica mostrando las debilidades o puntos de control efectivos.

4.2.8. Es recomendable que los despachos adopten una guía de procedimientos para la evaluación del control interno, para obtener resultados de una forma profesional que respalde sus informes.

BIBLIOGRAFIA

📁 **ENRIQUE HERNÁNDEZ HERNÁNDEZ**

AUDITARÍA EN INFORMÁTICA

Un Enfoque Metodológico y Práctico

COMPañÍA EDITORIAL CONTINENTAL,

Primera Impresión 1998

📁 **RICARDO MÉNDEZ**

DICCIONARIO DEL LENGUAJE DE LAS COMPUTADORAS

IMPRESORA MÉNDEZ

San Salvador, El Salvador, C.A. 1997

📁 **ROBERT J. THIERAUF**

AUDITORÍA ADMINISTRATIVA

Evaluación del Sistema de Información

EDITORIAL LIMUSA, 1986

📁 **HABRAHAM PERDOMO MORENO**

FUNDAMENTOS DE CONTROL INTERNO

Segunda edición

México D.F

ECASA, Segunda reimpresión 1987

📁 **GUSTAVO CEPEDA ALONSO**

AUDITORÍA Y CONTROL INTERNO

McGraw-Hill, 1998

📁 **WALTER G. KELL – WILLIAN C. BOYNTON**

AUDITORÍA MODERNA

CECASA, Segunda impresión

Mexico, 1997.

📁 **CASTELLANOS, J. L. Y OTROS,**

Texto de Auditoría de Sistemas

Universidad Centroamericana

San Salvador, El Salvador. 1996

📁 **DELGADO, A. F. Y ARRIAZA, R.A**

Técnicas y Herramientas de la Auditoria de Sistemas

Universidad de El Salvador 1997

San Salvador, El Salvador

📁 **GONZALEZ MANZANO, ALVARO BALMORE**

Evaluación de Puntos Críticos

Trabajo de Graduación

Universidad de El Salvador 1996

San Salvador, El Salvador

📁 **GOMEZ GIRON, JOSÉ ALFREDO Y OTROS**

**Diseño de un Modelo de Evaluación de los Niveles de Riesgo en la Auditoría de
Sistemas de Procesamiento Electrónico de datos**

Trabajo de Graduación 1995

Universidad de El Salvador

San Salvador, El Salvador

Consultores Cisneros Beltrán y Asociados

Colonia Flor Blanca 49 Av. Sur # 614
San Salvador. Telefax 245-0414

Contrato de Auditoria en Informática

Contrato de prestación de servicios profesionales de auditoria en informática que celebran por una parte “DRUPY S.A. de C.V.”, representado por César Rodríguez en su carácter de Representante Legal y en lo sucesivo se denominará cliente, por otra parte Despacho de Auditoría Cisneros Beltrán y Asociados, representado por Maritza Elizabeth Argueta Arano a quien se le denominará auditor, de conformidad con las declaraciones y cláusulas siguientes:

DECLARACIONES

I. El Cliente declara:

- a) Que es una empresa comercial
- b) Que está representado para acto por César Rodríguez y tiene como su domicilio la ciudad de San Salvador.
- c) Que requiere tener servicios en informática, por lo que ha decidido contratar los servicios del auditor.

II. Declara el Auditor:

- a) Que es una Sociedad Anonima, constituida y existente de acuerdo con las leyes y que dentro de sus objetivos primordiales está el de prestar auditoría en informática Despacho de Auditoria Cisneros Beltrán y Asociados.
- b) Que está constituida legalmente según escritura 18472 de fecha 14 de julio de 1986, ante notario público N° 256-4, Lic. Rolando Larín.

- c) Que señala como su domicilio la ciudad de San Salvador.

III. Declaran ambas partes:

- a) Que habiendo llegado a un acuerdo sobre lo antes mencionado, lo formalizan otorgando el presente contrato que contiene lo siguiente:

CLAUSULAS

PRIMERA. OBJETO

El auditor se obliga a prestar al cliente los servicios de auditoria informática para llevar a cabo la evaluación de la dirección de informática del cliente, que se detallan en la propuesta de servicio anexa, firmada por las partes, forma parte integral del contrato.

SEGUNDA. ALCANCE DEL TRABAJO

El alcance de los trabajos que llevará a cabo el auditor dentro de este contrato son:

- a) Evaluación de la dirección de informática en lo que corresponde a:
- ▶ Su organización
 - ▶ Su estructura
 - ▶ Recurso Humano
 - ▶ Normas y Políticas
 - ▶ Capacitación
 - ▶ Planes de Trabajo
 - ▶ Controles Estándares

b) Evaluación de los sistemas:

- ▶ Opinión de los usuarios de los diferentes sistemas
- ▶ Evaluación de los usuarios de los diferentes sistemas