UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE CIENCIAS ECONÓMICAS

PLANEACIÓN DE LA AUDITORÍA EN UN AMBIENTE DE SISTEMAS DE INFORMACIÓN POR COMPUTADORAS EN UNA DISTRIBUIDORA DE REPUESTOS

TESIS

Presentada a la Junta Directiva

de la

Facultad de Ciencias Económicas

por

MARIO RENÉ SAUCEDO MENDOZA

Previo a conferírsele el Título de

CONTADOR PÚBLICO Y AUDITOR

En el Grado Académico de

LICENCIADO

Guatemala, marzo del 2006

MIEMBROS DE LA JUNTA DIRECTIVA DE
LA FACULTAD DE CIENCIAS ECONÓMICAS

Decano	Lic. Eduardo Antonio Velásquez Carrera
Secretario	Lic. Oscar Rolando Zetina Guerra
Vocal 1o.	Lic. Canton Lee Villela
Vocal 2o.	Lic. Albaro Joel Girón Barahona
Vocal 3o.	Lic. Juan Antonio Gómez Monterroso
Vocal 4o.	P.C. Efrén Arturo Rosales Alvarez
Vocal 5o.	P.C. José Abraham González Lémus

PROFESIONALES QUE PRACTICARON EL EXAMEN
DE ÁREAS PRÁCTICAS BÁSICAS

Examinador Auditoria	Lic. Sergio Arturo Sosa Rivas
Examinador Contabilidad	Lic. Manuel Fernando Morales García
Examinador Matemático – Estadístico	Lic. Tiberio Amilcar Castillo Torres

PROFESIONALES QUE PRACTICARON EL EXAMEN PRIVADO DE TESIS

Presidente	Lic. Sergio Arturo Sosa Rivas
Examinador	Lic. Ruben Eduardo Del Aguila Rafael
Examinador	Lic. Julio Hernan Oliva Juárez

Guatemala 16 de abril de 2005

Licenciado
Eduardo Antonio Velásquez Carrera
Decano, Facultad de
Ciencias Económicas de la
Universidad de San Carlos de
Guatemala
Presente

Estimado Señor Decano:

En atención a la designación de que fuera objeto para asesorar el trabajo de Tesis del Señor **Mario René Saucedo Mendoza**, tengo el agrado de comunicar a usted que procedí a efectuar dicha asesoría, encontrándose el trabajo concluido a satisfacción.

El tema asignado **"PLANEACIÓN DE LA AUDITORÍA EN UN AMBIENTE DE SISTEMAS DE INFORMACIÓN POR COMPUTADORAS EN UNA DISTRIBUIDORA DE REPUESTOS"** fue desarrollado en forma completa y con conceptos totalmente actualizados, por lo que constituye un valioso aporte para la Profesión.

Por lo anterior, recomiendo que el mencionado trabajo sea aceptado para su discusión en el Examen Público previo a conferírsele el Título de Contador Público y Auditor en el grado de Licenciado.

Sin otro particular me suscribo de usted,

Atentamente,

Lic. Mibzar Castanón Orozco
Contador Público y Auditor
Colegiado No. 2088

CONTENIDO **Página**

PLANEACIÓN DE LA AUDITORÍA EN UN AMBIENTE DE SISTEMAS DE INFORMACIÓN POR COMPUTADORAS EN UNA EMPRESA DISTRIBUIDORA DE REPUESTOS

CAPÍTULO IV
PLANEACIÓN DE LA AUDITORÍA EN UN AMBIENTE DE SISTEMAS DE INFORMACIÓN POR COMPUTADORAS

CAPÍTULO V
CASO PRÁCTICO – PLANEACIÓN DE LA AUDITORÍA EN UN AMBIENTE DE SISTEMAS DE INFORMACIÓN POR COMPUTADORAS EN UNA DISTRIBUIDORA DE REPUESTOS

INTRODUCCIÓN

El propósito de éste documento de investigación es presentar como mínimo los lineamientos de planificación de auditoria financiera en una empresa distribuidora de repuestos. El enfoque de la auditoria de estados financieros debe considerar la evaluación de los sistemas de información por computadora (SIC), en la planeación y ejecución de una auditoria financiera. La auditoria financiera en una Distribuidora de Repuestos, consiste en un examen sistemático de los libros, documentos y demás registros contables, para formarse un criterio y obtener evidencia comprobatoria suficiente y competente para fundamentar objetiva y profesionalmente la opinión del Auditor sobre los estados financieros que prepara la administración de la entidad. Los procedimientos necesarios para la planeación de una auditoria, deberán ser determinados por el Auditor teniendo en cuenta las Normas de Auditoria, los requerimientos de Organismos Profesionales importantes, la legislación, los reglamentos y, también los términos del contrato de auditoria que incluye los requisitos para dictaminar.

El auditor deberá considerar cómo afecta a la auditoria un ambiente de Sistemas de Información Computarizada (SIC). El objetivo y alcance de auditoria no se ve modificado en un ambiente de Sistemas de Información Computarizada (SIC), pero, usar una computadora para hacer los registros contables, cambia el procesamiento, almacenamiento y comunicación de la información financiera, y puede afectar los sistemas contables y el control interno empleados por la entidad.

Al planear la auditoria que evaluará el ambiente SIC del cliente, el auditor debería obtener una comprensión de la importancia y complejidad de las actividades de SIC y la disponibilidad de datos para uso en la auditoria. El esquema del proceso de auditoria, que ejecutan

los auditores y los resultados de tales procedimientos se detallan a continuación.

Primero se trabaja la planeación de auditoria financiera, sin olvidar la participación del auditor de sistemas de información por computadora, para evaluar los sistemas contables, el control interno y el sistema informático del cliente, en forma simultánea. Las fases en la planeación de auditoria y evaluación del ambiente informático se detallan a continuación: Planear el trabajo e identificar las áreas significativas de auditoria, conocer el negocio del cliente, comprender y evaluar los sistemas contables, la estructura de control interno y estimar la participación del especialista en auditar los sistemas informáticos involucrados en el proceso contable y la elaboración de los estados financieros, con los datos adquiridos desarrollar el plan de enfoque de auditoria y la evaluación de los sistemas informáticos, luego ejecutar los procedimientos de auditoria que serán definidos en el memorando de planeación de Auditoria.

El Auditor financiero deberá reunirse con la dirección del cliente para discutir las novedades en el área financiera y los cambios en el área de sistemas de información por computadora, para evaluar el entorno de control haciendo un resumen de los cambios presentados, el cuál se registrará en el memorando de Planeación de Auditoria. Posteriormente se revisa y evalúa las aplicaciones contables significativas, documentando los controles internos, los controles generales del computador, controles de aplicación, y se documenta el Plan de Enfoque, posteriormente se aplican los procedimientos de auditoria definidos en el plan de enfoque y se recopilan los hallazgos para la Carta de Observaciones y Recomendaciones dirigida a la Gerencia.

Se ejecutan las pruebas de auditoria sobre los controles contables identificados, se prueban los controles generales del computador, los controles de aplicación en los ambientes informáticos y las pruebas sustantivas de auditoria con ayuda del computador (CAATs), para confirmar la confianza depositada en el control interno obtenida en la evaluación preliminar. Como último procedimiento se revisa los resultados relevantes de la auditoria y se establecen las conclusiones y hallazgos en el Memorando Resumen de Auditoria.

CAPITULO I
DISTRIBUIDORA DE REPUESTOS

1.1 Definición de Empresa

"La empresa está compuesta por un conjunto de elementos o factores humanos, técnicos y financieros, localizados en una o varias unidades físico - espaciales o centros de gestión, combinados y ordenados según determinados modelos de estructura organizativa" (2:78).

"También se puede decir que la empresa es un conjunto de elementos ordenados según las normas de cierta estructura y relacionados para el cumplimiento de ciertos objetivos en base a determinadas funciones características y cuyo logro se puede conocer a través del análisis de la sucesión de estados en que se pueda estudiar el sistema empresarial.

La empresa y su entorno, en el sentido más amplio, entorno es en el que se desenvuelve su actividad o sea todo lo que esta afuera de los límites de la empresa, sin embargo puede concretarse el entorno en dos partes: entorno social, que afecta a todas las empresas en una sociedad, y entorno específico, que afecta a cada empresa en concreto de una manera directa" (8:26).

1.2 Los Elementos de la Empresa

"De manera fácil podemos deducir que la problemática de la empresa es compleja y supera lo estrictamente económico. La empresa se inspira en la clásica formulación del concepto que la describe como *célula o unidad de producción dentro del sistema económico*. En definitiva, la empresa para cumplir sus objetivos y desarrollar el conjunto de sus actividades, ha de disponer de medios o factores, elementos que, en principio, se pueden considerar bajo dos grandes grupos: *las personas o factores activos y los bienes económicos o factores pasivos*" (8:75).

"Bajo una óptica general, la clasificación de los elementos constituyentes de la estructura de la empresa son:

- *El grupo humano o las personas;*
- *Los bienes económicos;*
- *La organización.*

Dentro del grupo humano se puede señalar la existencia de grupos diferenciados por sus intereses y relaciones con el resto:

- *Los propietarios del capital o socios;*
- *Los administradores o directivos;*
- *Los trabajadores o empleados.*

Evidentemente, entre los dos primeros grupos, y básicamente en el segundo, surge la figura del empresario tal y como hoy se le concibe.

Los bienes económicos se suelen clasificar en inversiones o duraderos y en corrientes o no duraderos, según su vinculación al ciclo productivo de la explotación" (8:139).

1.3 Que es una Distribuidora

"Se le conoce por distribución la acción de distribuir, la distribuidora por consiguiente es la entidad que se dedica a distribuir bienes de consumo, y el distribuir es dividir una cosa o bien entre varios designando lo que a cada uno le corresponde, dándole a cada uno de los bienes su oportuna colocación o el destino conveniente"(10:65).

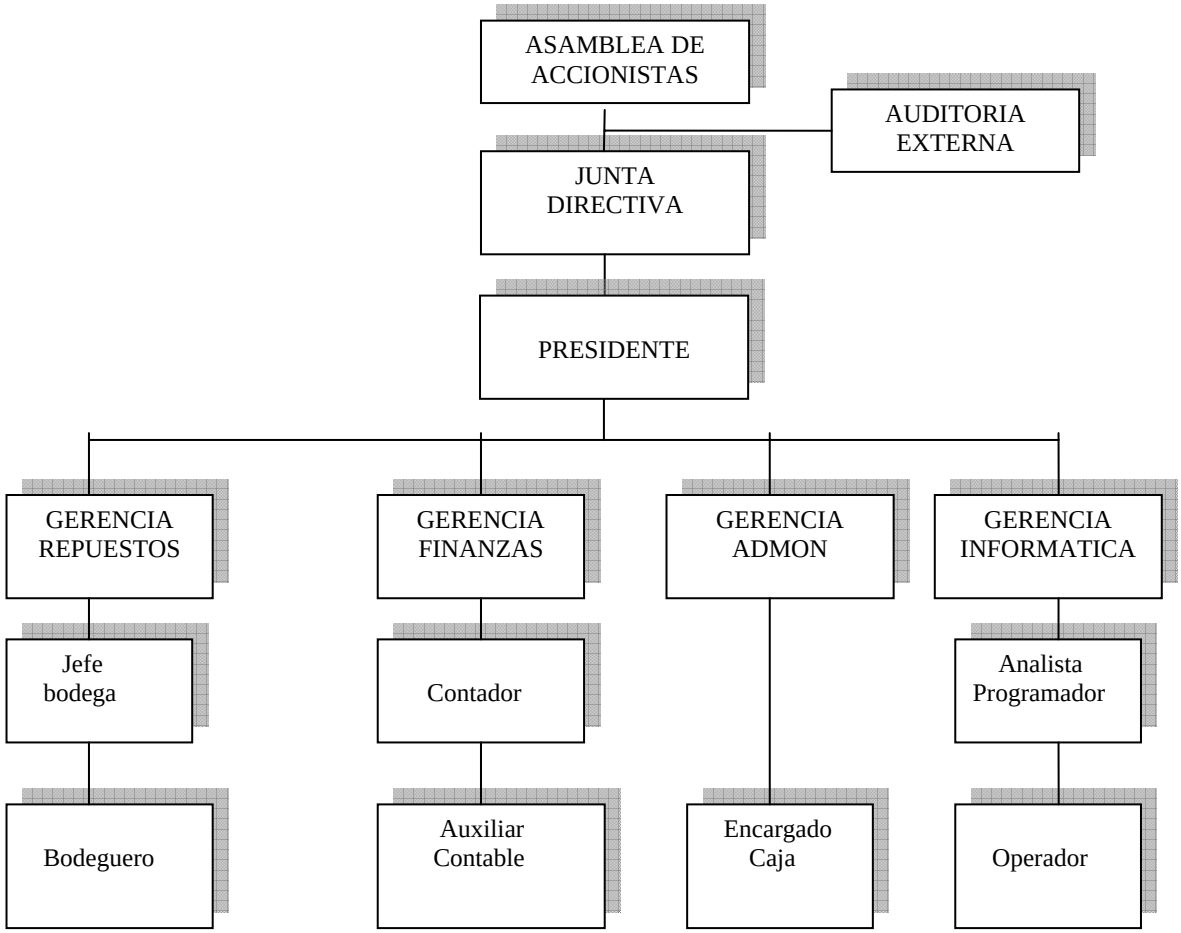
1.4 Distribuidora de Repuestos

El objetivo principal de la Distribuidora de Repuestos, es importar, exportar, distribuir, adquisición, compra y venta de bienes, repuestos, suministros, accesorios, y otros de cualquier índole directa o indirectamente relacionados a los anteriores. Son las personas individuales y jurídicas domiciliadas o no en Guatemala, que independientemente de su nacionalidad o residencia se dedique al mismo giro de actividades.

Políticas y Procedimientos: Las políticas son implementadas por la Junta Directiva de la Entidad. Los procedimientos son implementados y aplicados por cada unidad operativa de la Entidad. La Gerencia Financiera, se encarga de asegurar la aplicación de las Normas Internacionales de Contabilidad, que son regulaciones de alta calidad, que exigen seguir prácticas contables apropiadas. Este procedimiento también garantiza, mediante las consultas realizadas a Consultores, a los Organismos reguladores contables y a otros grupos e individuos interesados, que las Normas Internacionales de Contabilidad son aplicables para los usuarios y elaboradores de los estados financieros de la entidad.

A continuación la organización de la entidad se describe en el organigrama sugerido siguiente:

ORGANIGRAMA



CAPITULO II
CONTROL INTERNO

2.1 Definición de Control Interno

“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 razonabilidad y confiabilidad de su información financiera, promover la eficiencia operacional y provocar la adherencia a las políticas prescritas por la administración”(5:85).

En la auditoria de estados financieros, el auditor está interesado sólo en aquellas políticas y procedimientos dentro de los sistemas de contabilidad y de control interno que son relevantes y que afectan las aseveraciones de los estados financieros. La comprensión de los aspectos relevantes de los sistemas de contabilidad y de control interno, los ambientes informáticos, junto con las evaluaciones del riesgo inherente, el riesgo de control y otras consideraciones, harán posible para el auditor:

- Identificar los tipos de potenciales representaciones erróneas de importancia relativa que pudieran ocurrir en los estados financieros;

- Considerar factores que afectan el riesgo de representaciones erróneas sustanciales; y

- Diseñar procedimientos de auditoria apropiados.

Los controles internos relacionados con el sistema de contabilidad están dirigidos a lograr objetivos como:

- Las transacciones son ejecutadas de acuerdo con la autorización general o específica de la administración.
- Todas las transacciones y otros eventos son prontamente registrados en el monto correcto, en las cuentas apropiadas y en el periodo contable apropiado, a modo de permitir la preparación de los estados financieros de acuerdo con un marco de referencia para informes financieros identificado.
- El acceso a activos y registros es permitido sólo de acuerdo con la autorización de la administración.
- Los activos registrados son comparados con los activos existentes a intervalos razonables y se toma la acción apropiada respecto de cualquiera diferencia.

2.2 Estructura del Control Interno

"La estructura o ambiente de control, significa la actitud global, conciencia y acciones de directores y administración respecto del sistema de control interno y su importancia en la Distribuidora de Repuestos. La estructura o ambiente de control tiene un efecto sobre la efectividad de los procedimientos de control específicos. Una estructura o ambiente de control fuerte, por ejemplo, con controles presupuéstales estrictos y una función de auditoria interna efectiva, pueden complementar en forma muy importante los procedimientos específicos de control. Sin embargo, un ambiente fuerte no asegura, por sí mismo, la efectividad de la estructura del sistema de control interno.

Los factores reflejados en la estructura o ambiente de control incluyen:

- La función del consejo de directores y sus comités;
- La filosofía y estilo operativo de la administración;
- La estructura organizacional de la entidad y métodos de asignación de autoridad y responsabilidad;
- El sistema de control de la administración incluyendo la función de auditoria interna, políticas de personal, procedimientos y segregación de deberes" (5:90).

2.3 Objetivos Básicos del Control Interno

Los cuatro objetivos básicos del control interno son:

1) La protección de los activos de la empresa;
2) La obtención de información financiera veraz, confiable y oportuna;
3) La promoción de la eficiencia en la operación del negocio;
4) Lograr que en la ejecución de las operaciones se cumplan las políticas establecidas por los administradores de las empresas.

Se ha definido que los dos primeros objetivos abarcan el aspecto de controles internos contables y los dos últimos se refieren a controles internos administrativos" (5:116).

2.4 Objetivos Generales del Control Interno

Como se expuso en el numeral 2.1, el control interno contable comprende el plan de organización y los

procedimientos y registros que se refieren a la protección de los activos y a la confiabilidad de los registros financieros.

Cuando hablamos de los objetivos de los controles contables internos podemos identificar dos niveles:

- Objetivos generales de control interno aplicables a todos los sistemas; y
- Objetivos de control interno aplicables a ciclos de transacciones.

Los objetivos generales de control aplicables a todos los sistemas, se desarrollan a partir de los objetivos básicos de control interno enumerados anteriormente en el numeral 2.3, siendo más específicos para facilitar su aplicación.

Los objetivos de control de ciclos se desarrollan a partir de los objetivos generales de control de sistemas, para que se apliquen a las diferentes clases de transacciones agrupadas en un ciclo.

2.5 Control Interno en Ambientes de Microcomputadoras

"Generalmente, el ambiente de Sistemas de Información Computarizada – (SIC), en el que se usan microcomputadoras es menos estructurado que un ambiente de sistemas de información computarizada controlado en forma central.

Aunque al principio surgieron como máquinas de enorme tamaño, limitadas al terreno de la alta tecnología, las computadoras se introdujeron en los hogares y oficinas cuando aparecieron los computadores personales (PC). Con un equipo PC y un módem, un usuario puede conectarse a redes locales, nacionales e internacionales a través de las líneas telefónicas. A medida que se ha simplificado el uso de las computadoras y del

software, mucha gente las ha adoptado como elemento necesario, cuando no imprescindible, para su trabajo.

“Se han producido una serie de desarrollos importantes para el auge de los microcomputadores. Uno de ellos fue la introducción de un potente computador de 32 bits capaz de ejecutar sistemas operativos multiusuario avanzados a gran velocidad. Esta novedad redujo las diferencias entre micro y mini computadores, dotando a cualquier equipo de sobremesa (desktop) de una oficina con la suficiente potencia informática como para satisfacer las demandas de cualquier pequeña empresa y de la mayoría de las empresas medianas. Otra innovación fue la introducción de métodos más sencillos y amigables para el control de las operaciones de las microcomputadoras. Al sustituir el sistema operativo convencional por una interfaz gráfica de usuario, las computadoras permiten al usuario seleccionar iconos — símbolos gráficos que representan funciones de la computadora — en la pantalla, en lugar de requerir la introducción de los comandos escritos correspondientes”. (13:07)

Hoy ya existen nuevos sistemas controlados por la voz, pudiendo los usuarios operar sobre sus microcomputadores utilizando las palabras y la sintaxis del lenguaje hablado. El resultado de toda esta evolución es la existencia de computadores de gran potencia y con capacidades multimedia que se han convertido, no sólo en una herramienta de gran interés para la empresa, sino también en un elemento de ocio. El fenómeno Internet ha experimentado la explosión de los últimos tiempos debido, en gran medida, a la existencia de

computadores personales en muchos negocios de nuestro entorno.

En el ambiente de microcomputadoras, los programas de aplicación pueden desarrollarse relativamente rápido por usuarios que poseen sólo habilidades básicas de procesamiento de datos. En estos casos, los controles sobre el proceso de desarrollo de sistemas de información por computadora (por ejemplo, procedimientos de control de acceso), que son esenciales para el control efectivo de un ambiente mayor de computadoras, pueden no ser considerados por el que los desarrolla, el usuario o la administración, como importantes o como de costo efectivo en un ambiente de microcomputadoras.

“Sin embargo, a causa de que los datos están siendo procesados en una computadora, los usuarios de dichos datos pueden tender a depositar una confianza no justificada en la información financiera almacenada o generada por una microcomputadora, ya que las microcomputadoras están orientadas a usuarios finales individuales, el grado de exactitud internos fijados por la administración y adoptados por el usuario puede ser menor. Por ejemplo, cuando hay varios usuarios de una sola microcomputadora, sin controles apropiados, los programas y datos almacenados en medios de almacenamiento no removibles por un usuario pueden ser susceptibles al acceso, uso o alteración no autorizados, o también a robo, por otros usuarios”(3:271).

“En un ambiente típico de microcomputadoras, no puede ser claramente asegurada la distinción entre controles generales de sistemas de información por computadora y controles de

aplicación de sistemas de información por computadora" (9:46), pero el objetivo es definir los controles de aplicación, los que se describirán más adelante.

Existe un entorno de sistemas de información por computadora - (SIC) cuando está involucrada una computadora de cualquier tipo o tamaño en el procesamiento por parte de la entidad de la información financiera de importancia para el auditor, ya sea que la computadora sea operada por la entidad o por terceras partes.

Qué es una microcomputadora? Esta pregunta ayuda al Auditor a implementar la evaluación del riesgo y control interno, y las características y consideraciones del ambiente de sistemas de información que afectan los procesos y registros contables, y los riesgos colaterales al describir los sistemas de microcomputadoras usadas como estaciones de trabajo independientes". (3:271).

"Las microcomputadoras a menudo mencionadas como computadoras personales o "PCS," son computadoras integrales de uso general, económicas pero poderosas, las cuales se configuran típicamente con un procesador, memoria, monitor de video, unidad de almacenamiento de datos, teclado y conexiones para una impresora y comunicaciones. Los programas y los datos son almacenados en medios de almacenamiento removibles o no removibles" (3:272).
Las microcomputadoras pueden ser usadas para procesar transacciones contables y producir informes que son esenciales para la preparación de estados financieros.La microcomputadora puede constituir todo el sistema de contabilidad basado en computadora o solamente una parte del mismo. Generalmente,

los ambientes de sistemas de información por computadora - (SIC), en los que las microcomputadoras se usan son diferentes de otros ambientes de sistemas de información por computadora. Ciertos controles y medidas de seguridad que se usan para grandes sistemas de computación pueden no ser factibles para las microcomputadoras. Por otra parte, ciertos tipos de controles internos necesitan enfatizarse debido a las características de las microcomputadoras y a los ambientes en que se usan.

Las microcomputadoras pueden usarse en diversas estructuras para su operación. Estas incluyen:

- Una estación de trabajo independiente operada por un solo usuario o un número de usuarios en diferentes momentos;
- Una estación de trabajo que es parte de una red de microcomputadoras de un área local; y
- Una estación de trabajo conectada a una computadora central" (3:271).

La estación de trabajo independiente puede ser operada por un solo usuario o un número de usuarios en diferentes momentos teniendo acceso a los mismos o diferentes programas. Los programas y datos se almacenan en la microcomputadora o muy cerca de ella y, generalmente, los datos se alimentan manualmente por medio del teclado.

El usuario de la estación independiente que procesa aplicaciones contables puede ser conocedor de programación, y típicamente desempeña un variado número de funciones, (por ejemplo, alimentar datos, operar programas de aplicación y, en algunos

casos, escribir los programas de computadora en sí). Esta programación puede incluir el uso de paquetes de software comprados, para desarrollar hojas electrónicas de cálculo o aplicaciones de bases de datos.

Las microcomputadoras pueden establecerse en una red de área local (LAN – Local Área Network), ésta es una instalación donde dos o más microcomputadoras están enlazadas a través del uso de software especial y de líneas de comunicación. Típicamente, una de las microcomputadoras actuará como el dispensador de archivos (servidor) que maneja la red. Una red LAN permite compartir recursos como instalaciones de almacenaje e impresoras. Múltiples usuarios pueden tener acceso a la información, datos y programas almacenados en archivos compartidos. Una red de área local - LAN, puede conocerse como un sistema distribuido.

Las microcomputadoras pueden enlazarse a computadoras centrales (Mainframes) y usarse como parte de dichos sistemas, por ejemplo, como una estación inteligente en línea o como parte de un sistema de contabilidad distribuido. A un arreglo así puede llamársele un sistema en línea. Una microcomputadora puede actuar como una Terminal inteligente a causa de su lógica, transmisión, almacenaje y capacidades básicas de cómputo.

Ya que las consideraciones de control y las características del hardware y software son diferentes cuando una microcomputadora está enlazada a otras computadoras, tales ambientes de red, se deberán indagar y documentar como parte de la auditoria. Sin embargo, al grado de una microcomputadora que está enlazada a otra computadora pueda

también ser usada como una estación independiente, la información en esta declaración deberá considerarse por su importancia.

El software para un amplio rango de aplicaciones de la microcomputadora puede comprarse de proveedores distintos para su uso (por ejemplo, contabilidad de libro mayor, cuentas por pagar, control de producción y de inventario, planillas y personal, etc.). Estos paquetes de software son usados típicamente sin modificación de los programas. Los usuarios pueden también desarrollar otras aplicaciones con el uso de paquetes de software genérico, como hojas de cálculo electrónicas, o bases de datos, compradas a vendedores distintos.

El software de sistema operativo, los programas de aplicación y datos, pueden ser almacenados en, y recuperados de medios de almacenamiento removibles, incluyendo disquetes, cartuchos y discos compactos, discos duros removibles, unidades de memoria (USB) entre otros. Estos medios de almacenamiento, debido a su tamaño pequeño y a que son portátiles, están sujetos a borrarse accidentalmente, a daños físicos, a pérdidas o robo, particularmente por personas no familiarizadas con dichos medios o por algunos usuarios no autorizados.

Seguridad física del equipo – "A causa de sus características físicas, las microcomputadoras son susceptibles de robo, daño físico, acceso no autorizado, o mal uso. Esto puede resultar en la pérdida de información almacenada en la microcomputadora, por ejemplo, datos financieros vitales para el sistema de contabilidad". (3:509)

Un método de seguridad física es restringir el acceso a las

microcomputadoras cuando no están en uso, por medio de cerraduras en las puertas u otra protección de seguridad durante las horas no hábiles. La seguridad física adicional para las microcomputadoras puede establecerse, por ejemplo:

- Asegurando con llave la microcomputadora en un gabinete o estuche;
- Usando un sistema de alarma que se active cada vez que la microcomputadora sea desconectada o movida de su lugar;
- Fijando la microcomputadora a una mesa; o
- Instalando un mecanismo de cierre para controlar el acceso al botón de encendido/apagado. Esto puede no prevenir el robo de la microcomputadora, pero puede ser efectivo para controlar el uso no autorizado.

Seguridad física para medios removibles y no removibles – "Los programas y datos usados en una microcomputadora pueden ser almacenados en medios de almacenamiento removibles o no removibles. Los diskettes, discos compactos, unidades de memoria (USB) y cartuchos pueden ser removidos físicamente de la microcomputadora, mientras que los discos duros normalmente están sellados en la microcomputadora o en una unidad independiente anexa. Cuando se usa una microcomputadora por muchos individuos, los usuarios pueden desarrollar una actitud despreocupada sobre el almacenamiento de los discos compactos, diskettes o cartuchos de aplicación por los que son responsables. Como resultado, discos compactos, diskettes o cartuchos importantes pueden ser mal colocados, alterados sin autorización o destruidos." (3:514)

El control sobre los medios removibles puede establecerse poniendo la responsabilidad por dichos medios en personal

cuyas responsabilidades incluyen funciones de custodios de software o de bibliotecarios. El control puede reforzase más cuando se usa un sistema de verificación de entradas y salidas de archivos de programas y datos y se cierran con llave los lugares de almacenamiento. Dichos controles internos ayudan a asegurar que los medios de almacenamiento removibles no se pierdan, se desubiquen o se den a personal no autorizado. El control físico sobre medios de almacenamiento no removibles probablemente se establezca mejor mediante aditamentos de cerraduras de seguridad.

Dependiendo de la naturaleza de los archivos de programas y de datos, es apropiado conservar copias vigentes de discos compactos, diskettes, cartuchos y discos duros en un contenedor a prueba de fuego, ya sea en el local, fuera de él, o ambos. Esto aplica igualmente a software del sistema operativo y de utilería, y a copias de respaldo de discos duros.

Seguridad de programas y de datos – "Cuando las microcomputadoras están accesibles a muchos usuarios, hay un riesgo de que los programas y datos puedan ser alterados sin autorización." (3:515)

Ya que el software del sistema operativo de la microcomputadora puede no contener muchas características de control y seguridad, hay diversas técnicas de control interno que pueden integrarse a los programas de aplicación para ayudar a

asegurar que los datos son procesados y leídos según se autorice, y que se previene la destrucción accidental de datos. Estas técnicas, que limitan el acceso a programas y datos sólo a personal autorizado, incluyen:

- Separar datos en archivos organizados bajo directorios de archivos separados;
- Usar archivos ocultos y nombres secretos de archivos;
- Emplear palabras clave; y
- Usar criptografía.

El uso de un directorio de archivos permite al usuario segregar información en medios removibles y no removibles. Para información crítica y sensitiva, esta técnica puede suplementarse asignando nombres secretos de archivos y "ocultando" los archivos.

Cuando se usan las microcomputadoras por muchos usuarios, una técnica efectiva de control interno es el uso de palabras clave, que determinan el grado de acceso concedido a un usuario. La palabra clave se asigna y monitorea por un empleado que es independiente del sistema específico al que se aplica la palabra clave. El software para palabras clave puede ser desarrollado por la entidad, pero en la mayoría de los casos se compra. En cualquiera de los dos casos, los controles internos pueden reforzarse instalando software que tenga una baja probabilidad de ser sobrepasado por los usuarios.

La criptografía puede dar un control efectivo para proteger programas e información confidenciales o sensitivos del acceso

no autorizado y de modificación por parte de los usuarios. Generalmente es usada cuando se transmiten datos sensitivos por las líneas de comunicación, pero también puede usarse en información procesada por una microcomputadora. La criptografía es el proceso de transformar programas e información a una forma ininteligible. El cifrado y descifrado criptográfico de datos requiere el uso de programas especiales y una clave de código conocidos sólo a aquellos usuarios para quienes la información se restringe.

Los directorios y archivos ocultos, el software de autenticación de usuarios y la criptografía pueden ser usados para microcomputadoras que tienen medios de almacenamiento tanto removibles como no removibles. Para las microcomputadoras que tienen medios de almacenamiento removibles, un medio efectivo de seguridad para programas y datos es remover los discos compactos, los diskettes y cartuchos de la microcomputadora y colocarlos bajo custodia de los usuarios responsables por los datos o de los bibliotecarios de archivos.

Un control adicional de acceso para información confidencial o sensitiva almacenada en medios de almacenamiento no removibles es copiar la información a un disco compacto, diskette o cartucho y borrar los archivos en los medios de almacenamiento no removibles. El control sobre el disco compacto, diskette o cartucho puede establecerse entonces en la misma manera que para otros datos sensitivos o confidenciales almacenados de la misma forma. El usuario deberá tener presente que muchos programas en software incluyen una función de "borrar" o "suprimir", pero que dicha función quizá realmente no limpie los archivos borrados o suprimidos del disco duro. Dichas funciones pueden

simplemente limpiar el nombre del archivo del directorio del disco duro. Los programas y datos son quitados de hecho del disco duro sólo cuando se escriben nuevos datos sobre los viejos archivos o cuando programas especiales de utilería se usan para limpiar los archivos.

Integridad del software y de los datos – "Las microcomputadoras están orientadas a usuarios finales para el desarrollo de programas de aplicación, alimentación y procesamiento de datos y generación de informes. El grado de exactitud y confiabilidad de la información financiera producida dependerá de los controles internos instituidos por la administración y adoptados por los usuarios, así como de controles incluidos en los programas de aplicación. Los controles de integridad del software y de los datos puede asegurar que la información procesada esté libre de errores y que el software no sea susceptible de manipulación no autorizada (por ejemplo, que los datos autorizados sean procesados en la manera autorizada)." (3:519)

La integridad de los datos puede reforzarse incorporando procedimientos de control interno como un formato y verificaciones en línea y verificaciones cruzadas de los resultados. Una revisión del software comprado puede determinar si contiene recursos apropiados para verificación y detección de errores. Para software desarrollado para usuarios, incluyendo plantillas electrónicas de hojas de cálculo y aplicaciones de bases de datos, la administración puede especificar por escrito los procedimientos para desarrollar y poner a prueba los programas de aplicación. Para ciertas aplicaciones críticas, puede esperarse que la persona que procesa los datos, demuestre que se usaron datos apropiados y que los cálculos y otras operaciones de manejo de datos se

llevaron a cabo apropiadamente. El usuario final podría usar esta información para validar los resultados de la aplicación.

La documentación adecuada por escrito de las aplicaciones que son procesadas en la microcomputadora puede reforzar aún más los controles sobre la integridad del software y los datos. Dicha documentación puede incluir instrucciones paso a paso, una descripción de informes preparados, fuente de los datos procesados, una descripción de informes individuales, archivos y otras especificaciones, como cálculos. Si la misma aplicación contable se usa en varias localidades, la integridad y consistencia del software de aplicaciones puede mejorarse cuando los programas de aplicación se desarrollan y se mantienen en un lugar y no por cada usuario disperso por toda una entidad.

Respaldo del hardware, software y datos – "El respaldo se refiere a planes hechos por la entidad para obtener acceso a hardware, software, y datos comparables en caso de falla, pérdida o destrucción. En un ambiente de microcomputadoras, los usuarios normalmente son responsables por el procesamiento, incluyendo la identificación de programas y archivos de datos importantes que deben ser copiados periódicamente y almacenados en una localidad lejana de las microcomputadoras. Es particularmente importante establecer procedimientos de respaldo para que lleven a cabo los usuarios regularmente. Los paquetes de software comprados de proveedores distintos generalmente vienen con una copia de respaldo." (3:520)

Control interno en un sistema de computadoras en línea – "Ciertos controles generales del SIC son particularmente importantes para el procesamiento en línea." (3:523) Éstos incluyen:

- Acceso a los controles – Procedimientos diseñados para restringir e acceso a los programas y los datos, específicamente, seleccionar procedimientos que son diseñados para prevenir o detectar:
  - Acceso no autorizado a terminales de computadoras, programas y datos en línea:
  - Alimentación de transacciones no autorizadas;
  - Cambios no autorizados a archivos de datos;
  - Uso de programas operacionales de computadora por parte de personal no autorizado; y
  - Uso de programas de computadora que no han sido autorizados.
- Estos procedimientos de control de acceso incluyen - el uso de claves y de software especializado de control de acceso como monitores en línea que mantienen control sobre los menús, cuadros de autorización, claves, archivos y programas a los que se permite el acceso a los usuarios. Los procedimientos también incluyen controles físicos como el uso de cerraduras con clave en las terminales de computadoras.
- Controles sobre las claves - procedimientos para la asignación y mantenimiento de claves para restringir el acceso a los usuarios autorizados.
- Controles de desarrollo y mantenimiento de sistemas -

procedimientos adicionales para asegurar que se incluyen en el sistema durante su desarrollo y mantenimiento, los controles esenciales para aplicaciones en línea, como claves, controles de acceso, validación de datos y procedimientos de recuperación.

- Controles de programación - procedimientos diseñados para prevenir o detectar cambios no apropiados a los programas de computadora a los que se tiene acceso por las terminales de computadoras en línea. El acceso puede ser restringido por medio de controles como el uso de bibliotecas separadas de operaciones y de desarrollo de programas y el uso de software especializado de biblioteca de programas. Es importante que los cambios en línea a los programas estén adecuadamente documentados.
- Registros de transacciones - informes que se diseñan para crear un rastro de auditoria para cada transacción en línea, dichos informes a menudo documentan la fuente de una transacción (Terminal, hora, y usuario) así como los detalles de la transacción.

Ciertos controles de aplicación de SIC son particularmente importantes para el procesamiento en línea. Éstos incluyen:

- Autorización para pre – procesamiento – permiso: para iniciar una transacción, como el uso de una tarjeta bancaria junto con un número de identificación personal antes de hacer un retiro de efectivo por medio de un cajero automático.
- Pruebas de edición de las terminales de computadoras, de razonabilidad y otras pruebas de validación

- - rutinas programadas que verifican los datos de entrada y los resultados del procesamiento para su integridad, exactitud y razonabilidad. Estas rutinas pueden ser desempeñadas en una Terminal inteligente o en la computadora central.
- Procedimientos de corte - procedimientos que aseguran que las transacciones se procesan en el periodo contable apropiado. Son particularmente necesarios en sistemas que tienen un flujo continuo de transacciones. Por ejemplo, en los sistemas en línea donde las órdenes de venta y los embarques se registran mediante el uso de terminales en línea en diversas localidades, hay necesidad de coordinar el embarque real de las mercancías, la salida de inventario y el procesamiento de facturas.
- Controles de archivos - procedimientos que aseguran que se usan los archivos correctos de datos para el procesamiento en línea.
- Controles de archivo maestro - los cambios a los archivos maestros se controlan por procedimientos similares a los usados para controlar otros datos de entrada de transacciones. Sin embargo, ya que los datos del archivo maestro pueden tener un efecto profundo sobre los resultados del procesamiento, puede ser necesario un reforzamiento más estricto de estos procedimientos de control.
- Balances - el proceso de establecer totales de controles sobre los datos que se someten para procesamiento por medio de las terminales de computadoras en línea y de comparar los controles totales durante y después del procesamiento para asegurar que se transfieren datos completos y exactos a cada fase del procesamiento.

  Control interno en un ambiente de base de datos – “Generalmente, el control interno en un ambiente de base de

datos requiere controles efectivos sobre la base de datos, el Sistema Administrador de Bases de Datos (SABS) y las aplicaciones. La efectividad de los controles internos depende en un gran medida, de la naturaleza de las tareas de administración de la base de datos." (3:533)

Debido a los datos compartidos, a la independencia de los datos y a otras características del sistema de base de datos, los controles generales del SIC normalmente tienen una mayor influencia que los controles de aplicación del SIC sobre los sistemas de base de datos. Los controles generales del SIC sobre la base de datos, el SABS y las actividades de la función de administración de la base de datos tienen un efecto profundo sobre el procesamiento de las aplicaciones. Los controles generales del SIC de importancia particular en un ambiente de base de datos pueden clasificarse en los siguientes grupos:

- Enfoque estándar para desarrollo y mantenimiento de programas de aplicación;
- Propiedad de los datos;
- Acceso a la base de datos; y
- Segregación de funciones.

Enfoque estándar para desarrollo y mantenimiento de programas de aplicación: Ya que los datos son compartidos por muchos usuarios, el control puede ampliarse cuando se usa un

enfoque estándar para desarrollar cada nuevo programa de

aplicación y para modificación de programas de aplicación. Esto incluye seguir un enfoque formalizado, paso a paso que requiere la adhesión de todos los individuos que desarrollan o modifican un programa de aplicación. También incluye llevar a cabo un análisis del efecto de transacciones nuevas y existentes en la base de datos cada vez que se requiera una modificación. El análisis resultante indicaría los efectos de los cambios sobre la seguridad e integridad de la base de datos. Implementar un enfoque estándar para desarrollar y modificar programas de aplicación es una técnica que puede ayudar a mejorar la exactitud, integridad y que esté completa la base de datos.

Propiedad de los datos - En un ambiente de base de datos, donde muchos individuos pueden usar programas para alimentar y modificar datos, se requiere una asignación de responsabilidad clara y definida de parte del administrador de la base de datos por la exactitud e integridad de cada partida de datos. Deberá asignarse a un solo propietario de los datos la responsabilidad para definición de las reglas de acceso y seguridad, tales como quiénes pueden usar los datos (acceso) y qué funciones puede desempeñar (seguridad). Asignar responsabilidad específica por la propiedad de los datos ayuda a asegurar la integridad de la base de datos. Por ejemplo, el gerente de créditos puede ser designado el "propietario" del límite de crédito de un cliente y por lo tanto sería responsable de determinar los usuarios autorizados de esa información. Si varios individuos tienen capacidad de tomar decisiones que afecten la exactitud e integridad de los datos dados, aumenta la probabilidad de que los datos se contaminen o se usen en forma no apropiada.

Acceso a la base de datos - El acceso de usuarios a la base de datos puede ser restringido mediante el uso de claves. Estas restricciones aplican a individuos, aparatos terminales y

programas. Para que las claves sean efectivas, se requieren procedimientos adecuados para cambiar las claves, mantener el secreto de las mismas, y revisar e investigar los intentos de violación a la seguridad. Relacionar las claves a aparatos terminales, programas y datos definidos ayuda a asegurar que sólo usuarios y programas autorizados puedan tener acceso, o corregir o suprimir datos. Por ejemplo, el gerente de crédito puede dar autoridad a los vendedores para referirse al límite de crédito de un cliente, mientras que un dependiente del almacén puede no tener dicha autorización. El acceso de usuarios a los diversos elementos de la base de datos puede controlarse aún más mediante el uso de tablas de autorización. La implementación no apropiada de procedimientos de acceso puede dar como resultado el acceso no autorizado a los datos de la base de datos.

Segregación de funciones - Las responsabilidades para desempeñar las diversas actividades que se requieren para diseñar, implementar y operar una base de datos se dividen entre el personal técnico, de diseño, administrativo y de usuarios. Sus deberes incluyen diseño del sistema, diseño de la base de datos, administración y operación. Es necesario mantener la adecuada segregación de estas funciones para asegurar la integridad y exactitud, y que esté completa la base de datos. Por ejemplo, las personas responsables de modificar los programas de personal en la base de datos no deberían ser las mismas personas autorizadas para cambiar las tarifas de pago individuales en la base de datos.

Controles internos en un entorno SIC - Los controles internos sobre el procesamiento por computadora, que ayudan a lograr los objetivos globales del control interno, incluyen tanto procedimientos manuales como procedimientos integrados en programas de computadora. Dichos procedimientos de control combinados comprenden los controles globales que afectan al entorno de SIC (controles generales de SIC) y los controles específicos sobre las aplicaciones contables (controles de aplicación de SIC).

Controles generales de SIC - El propósito de los controles generales SIC es establecer un marco de referencia de control global sobre las actividades SIC y proporcionar un nivel razonable de certeza de que se logran los objetivos globales del control interno.

Los controles generales SIC pueden incluir:

a. Controles de organización y administración - diseñados para establecer un marco de referencia organizacional sobre las actividades SIC, incluyendo:

   - Políticas y procedimientos relativos a funciones de control.
   - Segregación apropiada de funciones incompatibles (por ejemplo, preparación de transacciones de entrada, programación y operaciones de computadora).

b. Desarrollo de sistemas de aplicación y controles de mantenimiento - diseñados para proporcionar certeza razonable de que los sistemas se desarrollan y mantienen de manera eficiente y autorizada. También están diseñados típicamente para establecer control sobre:

- Pruebas, conversión, implementación y documentación de sistemas nuevos o revisados;
- Cambios a sistemas de aplicación;
- Acceso a documentación de sistemas;
- Adquisición de sistemas de aplicación con terceros;

c. Controles de operación de computadoras - diseñados para controlar la operación de los sistemas y proporcionar certeza razonable de que:

- Los sistemas son usados para propósitos autorizados únicamente;
- El acceso a las operaciones de la computadora es restringido a personal autorizado;
- Sólo se usan programas autorizados;
- Los errores de procesamiento son detectados y corregidos;

d. Controles del software de sistemas - diseñados para proporcionar razonable certeza de que el software del sistema se adquiere o desarrolla de manera autorizada y eficiente, incluyendo:

- Autorización, aprobación, pruebas, implementación y documentación de software de sistemas nuevos y modificaciones del software de sistemas;
- Restricción de acceso a software y documentación de sistemas al personal autorizado;

e. Controles de entrada de datos y de programas - diseñados para proporcionar razonable certeza de que:

- Hay establecida una estructura de autorización sobre las transacciones que se alimentan al sistema;
- El acceso a datos y programas está restringido a personal autorizado;

Hay otras salvaguardas SIC que contribuyen a la continuidad del procesamiento. Estas pueden incluir:

- Respaldo de datos y programas de computadora en otro sitio;
- Procedimientos de recuperación para usarse en caso de robo, pérdida o destrucción intencional o accidental;
- Provisión para procesamiento externo en caso de desastre;

Controles de aplicación SIC - El propósito de los controles de aplicación SIC es establecer procedimientos específicos de control sobre las aplicaciones contables para proporcionar razonable certeza de que todas las transacciones están autorizadas y registradas, y son procesadas completamente, con exactitud y con oportunidad. Los controles de aplicación SIC incluyen:

A. Controles sobre datos de entrada - diseñados para proporcionar razonable certeza de que:

   - Las transacciones son autorizadas en forma apropiada antes de ser procesadas por la computadora; las transacciones son convertidas con exactitud a una forma legible por máquina y registradas en los archivos de datos de la computadora; las transacciones no están perdidas, añadidas, duplicadas o cambiadas en forma impropia; Las transacciones incorrectas son rechazadas, corregidas y, si es necesario, vueltas a someter a registro oportunamente.

B. Controles sobre el procesamiento y sobre archivos de datos de la computadora - diseñados para proporcionar razonable certeza de que:

- Las transacciones, incluyendo las transacciones generadas por el sistema, son procesadas en forma apropiada por la computadora; las transacciones no están perdidas, añadidas, duplicadas o cambiadas en forma no apropiada; los errores de procesamiento son identificados y corregidos oportunamente.

C. Controles sobre los datos de salida - diseñados para proporcionar razonable certeza de que:

- Los resultados del procesamiento son exactos; El acceso a los datos de salida está restringido a personal autorizado; los datos de salida se proporcionan al personal autorizado apropiado oportunamente.

CAPITULO III
AUDITORÍA

3.1 Definición de Auditoria

"La auditoria es el proceso sistemático de obtener y evaluar objetivamente la evidencia acerca de las afirmaciones relacionadas con actos y acontecimientos económicos, a fin de evaluar las declaraciones a la luz de los criterios establecidos y comunicar el resultado a las partes involucradas.

Su objetivo o fin es evaluar las declaraciones hechas. Estas declaraciones son afirmaciones realizadas por personas dentro de la entidad auditada. Generalmente estas afirmaciones deben ser cuantificables. Para poder evaluar las declaraciones se deben tener criterios establecidos. El Contador Público y Auditor debe formarse una opinión acerca de la medida en que las afirmaciones están de acuerdo con dichos criterios o normas establecidas al principio de la auditoria. Por último, de este examen surge un informe que reúne la opinión del auditor incluyendo las conclusiones, recomendaciones y sugerencias. Es decir, se reporta sobre el grado de correspondencia dentro de la información reunida y el criterio previamente establecido" (3:23).

El auditor debe determinar que ajustes, cambios o mejoras se necesitan para que la situación esté de acuerdo con el criterio establecido. La auditoria se puede aplicar a cualquier rama o ciencia.

"El objetivo de una auditoria de estados financieros es hacer posible al Auditor el expresar una opinión sobre si los estados financieros están preparados, respecto de todo lo sustancial, de acuerdo con Normas de Contabilidad Internacionales, un marco de referencia para reportes financieros identificado o a otros criterios"(3:36).

Aunque la opinión del Auditor aumenta la credibilidad de los estados financieros, el usuario no puede asumir que la opinión es una seguridad en cuanto a la futura viabilidad de la entidad ni a la eficiencia o efectividad con que la administración ha conducido los asuntos de la entidad.

El alcance de una auditoria - "se refiere a los procedimientos de auditoria considerados necesarios en las circunstancias para lograr el objetivo de la auditoria. Los procedimientos requeridos para conducir una auditoria de acuerdo a las normas de auditoria deberán ser determinados por el Contador Público y Auditor teniendo en cuenta los requisitos de las normas de auditoria, a los organismos profesionales importantes, la legislación, los reglamentos y, donde sea apropiado, los términos del contrato de auditoria y requisitos para dictámenes"(3:8).

3.2 Clasificación de la Auditoria

La auditoria tiene varias clasificaciones, el detalle a continuación:

3.2.1 Por la persona que la realiza

En Guatemala, es común encontrar la posición de la Auditoria reportando a la Asamblea de Accionistas,

Consejo de Administración, Administrador único y Junta Directiva, por lo cuál puede ser:

3.2.1.1 Auditoria Interna

"La Auditoria Interna, es una actividad de evaluación establecida dentro de una entidad como un servicio a la entidad. Sus funciones incluyen, entre otras cosas, examinar, evaluar y monitorear la adecuación y efectividad de los sistemas de control contables e internos" (3:217).

3.2.1.2 Auditoria Externa

"La auditoria externa es la que practica un Contador Público y Auditor o Firma de Auditoria, independiente de la administración de una empresa y tiene por objeto examinar los registros contables, financieros y no financieros con el propósito de dictaminar sobre la razonabilidad de los estados financieros proporcionados por la administración de la empresa"(3:9).

3.2.2 Por la fecha que son aplicados los procedimientos

A continuación se detalla los tipos de auditoria por la fecha de aplicación de los procedimientos:

3.2.2.1 Auditoria Preliminar

La Auditoria Preliminar, es la auditoria que se efectúa dentro del año normal de operaciones cada tres o cuatro meses, con el fin de adelantar el trabajo de la auditoria final. Esta auditoria permite examinar con más detenimiento las diferentes áreas que integran los estados financieros. Es útil, ya que algunas pruebas de auditoria como lo es la confirmación de saldos o circulación de las áreas de cuentas por cobrar, pasivos a corto plazo y a largo plazo, se pueden hacer oportunamente y sus resultados estarán disponibles para la auditoria final.

3.2.2.2 Auditoria Final

La Auditoria Final, es la auditoria en la que se conectan los saldos de la auditoria preliminar y los del cierre del ejercicio, verificando aquellas partidas que hayan tenido variaciones importantes durante el período.

3.2.3 Por el Objetivo que Persigue

A continuación se detalla por el objetivo que persiguen:

3.2.3.1 Auditoria Financiera

“La Auditoria Financiera, es el examen a los estados financieros de una entidad por un período determinado, con el objeto de emitir una opinión sobre la razonabilidad de los mismos, mediante la aplicación de las Normas de Auditoria Generalmente Aceptadas y si se han preparado

de acuerdo a Normas Internacionales de Contabilidad”(12:5).

3.2.3.2 Auditoria Administrativa

Es un enfoque sistemático orientado a evaluar la ejecución de la administración. La Auditoria Administrativa trabaja con gran cantidad de elementos cualitativos y proporciona una evaluación cuantitativa” (12:5). Es el examen comprensivo y constructivo de la estructura de una empresa en cuanto a sus planes y objetivos, sus métodos y controles, su forma de operación y sus facilidades humanas y físicas.

3.2.3.3 Auditoria Operacional

“Es examinar y evaluar sistemáticamente las operaciones de una entidad con el propósito de determinar si está operando en forma efectiva y eficiente, así como establecer el cumplimiento de las políticas, métodos y procedimientos de la entidad, efectuando recomendaciones para asegurar la observancia de dichas políticas.

3.2.3.4 Auditoria Fiscal

“Es la evaluación de la información financiera, declaraciones de impuestos y otras fuentes y documentos de información, de un período determinado con el objeto de establecer si se ha cumplido con las disposiciones

fiscales y si existen contingencias que puedan afectar las operaciones de la entidad”(12:5).

Auditoria Fiscal, es el examen que efectúa la superintendencia de administración tributaria, para comprobar que los contribuyentes están tributando correctamente.

3.2.4 Otras Clasificaciones

A continuación se describen otras clasificaciones de Auditoria:

3.2.4.1 Auditoria Recurrente

La Auditoria recurrente, es cuando la auditoria se efectúa año con año.

3.2.4.2 Auditoria Permanente

La Auditoria Permanente, es cuando dentro de la empresa siempre hay un auditor externo.

3.2.4.3 Auditoria Especial

La Auditoria Especial, está auditoria incluye exámenes de cuentas especiales, juzgadas independientemente de las otras que integran los estados financieros de un negocio, conocida también como auditoria de procedimientos convenidos.

Por ejemplo:

- Auditoria de caja
- Examen de costos de manufactura
- Razonabilidad de los saldos por cobrar, etc.

3.2.4.4 Auditoria Forense

La Auditoria Forense, es el examen efectuado por el Auditor independiente para determinar las causas jurídico-contables que provocan la extinción de una persona jurídica.

3.2.4.5 Auditoria de Ambientes de Sistemas de Información Computarizada

"La Auditoria de Ambientes de Sistemas de Información Computarizada – (SIC), se aplica cuando el Auditor ha considerado cómo afecta a la auditoria un ambiente de sistemas de información computarizada - (SIC). El objetivo y alcance globales de una auditoria no cambia 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 de sistemas de información computarizada – (SIC), puede afectar:

- Los procedimientos seguidos por el Auditor para obtener una comprensión suficiente de los sistemas contables y de control interno;

- La evaluación de los riesgos inherente y de control a través de la cual llega a la evaluación del riesgo global;
- El diseño y desarrollo de pruebas de control y procedimientos sustantivos apropiados para cumplir con el objetivo de la auditoria.
- Las habilidades y competencia para evaluar el ambiente de sistemas de información computarizada y para planear, dirigir, supervisar y revisar el trabajo desarrollado por los auxiliares. El auditor debería considerar si necesita de un profesional con habilidades especializadas en sistemas de información computarizada en una auditoria financiera con ambientes informáticos complejos. Estas habilidades pueden necesitarse para:

- Obtener una suficiente comprensión de los sistemas de contabilidad y de control interno afectados por el ambiente sistemas de información computarizada;
- Determinar el efecto del ambiente sistemas de información computarizada sobre la evaluación del riesgo global y del riesgo al nivel de saldo de cuenta y de clase de transacciones;
- Diseñar y desempeñar pruebas de control y procedimientos sustantivos apropiados.

Si se planea el uso de un profesional con habilidades especializadas en SIC, el auditor debería obtener suficiente evidencia apropiada de auditoria de que el trabajo es adecuado para los fines de la auditoria, de acuerdo con la norma de auditoria "uso del trabajo de un experto" (3:102).

A continuación se presenta cada una de las definiciones de auditorias especializadas, las cuales se aplican a las diferentes áreas y disciplinas del ambiente informático. Las definiciones propuestas para la auditoria de sistemas informáticos son las siguientes:

Auditoria Informática **–** "Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas informáticos, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipo periférico y demás componentes. Dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumo necesarios para el funcionamiento del centro informático. El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de sus resultados en la entidad, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionaros, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa."(14:05)

Auditoria con la computadora - "En este tipo de auditorias se puede distinguir como factor fundamental que la evaluación se realiza con el apoyo de los sistemas computacionales. Su definición es la siguiente: Es la auditoria que se realiza con el apoyo de los equipos de cómputo y sus programas para evaluar cualquier tipo de actividades y operaciones, no necesariamente computarizadas, pero si susceptibles de ser automatizadas; dicha auditoria se realiza también a las actividades del propio centro de sistemas y a sus componentes. La principal característica de este

tipo de auditoria es que, en un caso o en otro, o en ambos, se aprovechan las computadoras y sus programas para la evaluación de las actividades de auditoria a revisar, de acuerdo con las necesidades concretas del auditor, utilizando en cada caso las herramientas especiales del sistema y las tradicionales de la propia auditoria." (14:05)

Auditoria Sin Computadora - "En este tipo de auditoria se busca evaluar los sistemas desde una óptica tradicional, contado con el apoyo de las técnicas y procedimientos de evaluación acostumbrados y sin el uso de los sistemas informáticos, aunque éstos sean los que se evalúen. Por lo general esta auditoria se enfoca en los aspectos operativos, financieros, administrativos y del personal de los centros de sistemas informáticos. Por lo cual se define de la siguiente forma: Es la auditoria cuyos métodos, técnicas y procedimientos están orientados únicamente a la evaluación tradicional del comportamiento y validez de las transacciones económicas, administrativas y operacionales de un área de cómputo, y todos los aspectos que afectan a las actividades en las que se utilizan sistemas informáticos, pero dicha evaluación se realiza sin el uso de los sistemas informáticos. Es también la evaluación tanto a la estructura de la organización, funciones y actividades de funcionarios y personal de un centro de computo, así como a los perfiles de sus puestos, como de los reportes, informes y bitácoras de los sistemas, de la existencia y aplicación de planes, programas y presupuestos en dicho centro, así como del uso y aprovechamiento de los recursos informáticos para la realización de actividades, operaciones y tareas. Asimismo, es la evaluación de los sistemas de seguridad y prevención de contingencias, de la adquisición y uso del hardware, software y personal informático, y en sí de todo lo relacionado con el centro de

cómputo, pero sin el uso directo de los sistemas computacionales. ” (14:08)

Auditoria a la gestión informática – “Es la auditoria cuya aplicación se enfoca exclusivamente a la revisión de las funciones y actividades de tipo administrativo que se realizan dentro de un centro de cómputo, tales como:

- La planeación
- La organización
- La dirección
- El control de dicho centro

Esta Auditoria se realiza también con el fin de verificar el cumplimiento de las funciones y actividades asignadas a los funcionarios, empleados y usuarios de las áreas de sistematización, así como para revisar y evaluar las operaciones del sistema, el uso y protección de los sistemas de procesamiento, los programas y la información. Se aplica también para verificar el correcto desarrollo, instalación, mantenimiento y explotación de los sistemas de cómputo, así como sus equipos e instalaciones. Todo esto se lleva a cabo con el propósito de dictaminar sobre la adecuada gestión administrativa de los sistemas computacionales de una empresa y del propio centro informático. ” (14:11)

Auditoria al sistema de cómputo – “Es la técnica especializada que se enfoca únicamente a la evaluación del funcionamiento y uso correctos del equipo de computo, su hardware, y software y periféricos asociados. Esta auditoria también se realiza a la

composición y arquitectura de las partes físicas y demás componentes del hardware, incluyendo equipos asociados, instalaciones y comunicaciones internas o externas, así como al diseño, desarrollo y uso del software de operación, de apoyo y de aplicación, ya sean sistemas operativos, lenguajes de procesamiento y programas de desarrollo, o paquetería de aplicación institucional que se utiliza en la empresa donde se encuentra el equipo de computo que será evaluado; se incluye también la operación del sistema. ” (14:11)

Auditoria alrededor de la computadora – “Este tipo de auditoria se trata de evaluar todo lo que involucra la actividad de los sistemas computacionales, procurando, de ser posible, dejar a un lado todos los aspectos especializados, técnicos y específicos de los sistemas, a fin de evaluar únicamente las actividades vinculadas que se llevan alrededor de éstos. La definición propuesta es la siguiente: Revisión específica que se realiza a todo lo que está alrededor de un equipo de cómputo, como son sus sistemas, actividades y funcionamiento, haciendo una evaluación de sus métodos y procedimientos de acceso y procesamiento de datos, la emisión y almacenamiento de resultados, las actividades de planeación y presupuestación del propio centro de cómputo, los aspectos operacionales y financieros, la gestión administrativa de accesos al sistema, la atención a los usuarios y el desarrollo de nuevos sistemas, las comunicaciones internas y externas y, a todos aquellos aspectos que contribuyen al buen funcionamiento de un área de sistematización. ” (14:12)

Auditoria de la seguridad de los sistemas informáticos – “Revisión exhaustiva, técnica y especializada que se realiza a todo lo relacionado con la seguridad de un sistema de cómputo, sus áreas

y personal, así como a las actividades, funciones y acciones preventivas y correctivas que contribuyan a salvaguardar la seguridad de los equipos computacionales, las bases de datos, redes, instalaciones y usuarios del sistema. Es también la revisión de los planes de contingencias y medidas de protección para la información, los usuarios y los propios sistemas computacionales, y en si para todos aquellos aspectos que contribuyen a la protección y salvaguarda en el buen funcionamiento del área de sistematización, sistemas de redes o computadores personales, incluyendo la prevención y erradicación de los virus informáticos. " (14:13)

Auditoria de sistema de redes – "Es la revisión exhaustiva, específica y especializada que se realiza a los sistemas de redes de una empresa, considerando la evaluación los tipos de redes, arquitectura, topología, sus protocolos de comunicación, conexiones, accesos, privilegios, administración y demás aspectos que repercuten en su instalación, administración, funcionamiento y aprovechamiento. Es también la revisión del software institucional, de los recursos informáticos e información de las operaciones, actividades y funciones que permiten compartir las bases de datos, instalaciones, software y hardware de un sistema de red. " (14:13)

Auditoria integral a los sistemas de computo – "Es la revisión exhaustiva, sistemática y global que se realiza por medio de un equipo multidisciplinario de auditores, de todas las actividades y operaciones de un centro de sistematización, a fin de evaluar, en forma integral, el uso adecuado de sus sistemas de cómputo, equipos periféricos y de apoyo para el procesamiento de información de la empresa, así como de la red de servicios de una empresa y el desarrollo correcto de las funciones de sus áreas, personal y usuarios. Es también la revisión de la administración del

sistema del manejo y control de los sistemas operativos, lenguajes, programas y paqueterías de aplicación, así como de la administración y control de proyectos, la adquisición del hardware y software institucionales, de la adecuada integración y uso de sus recursos informáticos y de la existencia y cumplimiento de las normas y políticas, estándares y procedimientos que regulan la actuación del sistema, del personal y usuarios del centro de cómputo. Todo esto hecho de manera global por medio de un equipo multidisciplinario de auditores. ” (14:18)

Auditoria ISO-9000 a los sistemas computacionales – “Las empresas en el mundo ha adoptado la calidad Iso–9000 como parte fundamental de sus actividades. Por esta razón los sistemas están relacionados también con este tipo de auditoria de certificación de calidad, las cuales son muy especializas y específicas en cuanto a los requerimientos establecidos en ellas. La definición es: la revisión exhaustiva, sistemática y especializada que realizan únicamente los auditores especializados y certificados en las normas y procedimientos ISO –9000, aplicando exclusivamente los lineamientos, procedimientos e instrumentos establecidos por esta asociación. El propósito fundamental de esta revisión es evaluar, dictaminar y certificar que la calidad de los sistemas computacionales de una empresa cumpla con los requerimientos del ISO-9000. ” (14:24)

Auditoria Outsouring – “Otra de las especialidades que ha adoptado en los sistemas computacionales, es la relacionada con la prestación de servicios de cómputo a la empresa, por otra entidad ajena, las cuales abarcan desde la maquinación de sus actividades

computacionales, hasta la asesoría y soporte computacional a sus propios sistemas; por esta razón se requiere de una especialización en la evaluación de estos servicios. Su definición: Auditoria Outsourcing, es la revisión exhaustiva, sistemática y especializada que se realiza para evaluar la calidad en el servicio de asesoría o procesamiento externo de información que proporciona una empresa a otra. Esto se realiza con el fin de revisar la confiabilidad, oportunidad, suficiencia y asesoría por parte de los prestadores de servicios de procesamiento de datos, así como el cumplimiento de las funciones y actividades que tienen encomendados los prestadores de servicios, usuarios y el personal en general. Dicha revisión se realiza también en los equipos y sistemas. ” (14:27)

Auditoria ergonómica de sistemas computacionales – “Uno de los aspectos menos analizados en el área de sistemas es el impacto negativo, que causan el mobiliario y los propios sistemas computacionales en los usuarios de computadoras; estos aspectos pueden llegar a influir en el bienestar, salud y rendimiento de los usuarios, razón por lo cual se deben considerar mediante una auditoria especializada. Se definen así: Es la revisión técnica, específica y especializada que se realiza para evaluar la calidad, eficiencia y utilidad del entorno hombre-máquina-medio ambiente que rodea el uso de sistemas informáticos en una empresa. Esta revisión se realiza también con el propósito de evaluar la correcta adquisición y uso del mobiliario y sistemas, a fin de proporcionar el bienestar, confort, y comodidad que requieren los usuarios de los sistemas de cómputo de la empresa, así como evaluar la detección de los posibles problemas y sus repercusiones, y la determinación

de las soluciones relacionadas con la salud física de los usuarios de los sistemas de la empresa. ” (14:27)

Definición de auditoria informática – “La auditoria informática, tanto externa como interna, debe ser una actividad exenta de cualquier contenido o matiz "político" ajeno a la propia estrategia y política general de la empresa. La función auditora puede actuar de oficio, por iniciativa del propio órgano, o a instancias de parte, esto es, por encargo de la dirección o cliente. Es el conjunto de técnicas y actividades destinadas a analizar, evaluar, verificar y recomendar sobre el control, planificación, la adecuación, eficacia y seguridad de la función computacional en la empresa. Es el examen discontinúo de un sistema computacional, o del servicio informático a petición de su dirección para mejorar la rentabilidad, la seguridad y la eficacia. ” (14:32) En la Auditoria Informática se verifican tres áreas del control, que son:

- Desarrollo y mantenimiento de aplicaciones
- Desarrollo de Sistemas
- Operaciones de instalación

Las aplicaciones incluyen todas las funciones de información del negocio, en cuyo procesamiento interviene un computador. Los sistemas de aplicación abarcan uno o más departamentos de la organización, así como la operación del computador y el desarrollo del sistema.

Objetivo - La Auditoria Informática tiene como principal objetivo, evaluar el grado de efectividad de las Tecnologías de Información, dado que evalúa en toda su dimensión, en que medida se garantiza la información a la organización de la entidad, su grado de eficacia, eficiencia, confiabilidad e integridad para la toma de decisiones, convirtiéndola en el método más eficaz para tales propósitos. Los

principales objetivos que constituyen a la Auditoria Informática son:

- El control de la función informática.
- El análisis de la eficiencia de los Sistemas Informáticos que comporta, la verificación del cumplimiento de la Normativa general de la empresa en este ámbito y la revisión de la gestión eficaz de los recursos materiales y humanos informáticos.

Alcance de la auditoria informática - El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoria informática, y se complementa con los objetivos de ésta. El alcance ha de figurar expresamente en el Informe Final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas.

CAPITULO IV
PLANEACIÓN DE LA AUDITORÍA EN UN AMBIENTE DE SISTEMAS DE INFORMACIÓN POR COMPUTADORA

4.1 Planeación de la Auditoria – Introducción

"La planeación abarca la definición de los objetivos o metas de la organización, el establecimiento de una estrategia global para alcanzar esas metas y el desarrollo de una amplia jerarquía de planes para integrar y coordinar las actividades. Se preocupa entonces por los fines (que debe hacer), también los medios (como se debe hacer).

La planeación se aplica para establecer un esfuerzo coordinado" (6:39).

"Planeación Financiera, las empresas distribuidoras, son organismos complejos, sujetos a la influencia de numerosos factores internos y externos por lo que, para tomar decisiones acertadas es esencial entender su funcionamiento y contar con herramientas metodológicas que ayuden a ordenar los razonamientos" (11:55).

"El llamado enfoque de sistemas consiste en analizar un organismo de cualquier tipo con una visión de computo incluyendo, tanto los elementos que lo integran como el entorno en que se ubica. Esta forma de ver las cosas permite analizar sistemas complejos de manera objetiva y sistemática, sin ideas

preconcebidas o normas generalmente aceptadas que muchas veces no son aplicables al caso que se estudia.

Para poder aplicarlo a la planeación es necesario:

- Analizar el funcionamiento de la empresa, los procesos que realiza y las restricciones a que está sujeta;
- Identificar los elementos que componen la empresa y observar la forma como éstos se relacionan entre sí y con el entorno;
- Identificar los factores que determinan el funcionamiento de la empresa y elegir indicadores que permitan evaluar su desempeño;
- Elaborar modelos que representen su operación para facilitar el análisis y la toma de decisiones.

Al observar la empresa con este enfoque, la definiremos como – Sistema Tecno – Económico - Social, esto es: un conjunto de elementos técnicos, económicos y humanos que actúan en forma coordinada para producir determinados bienes y servicios.

“Planeación de la Auditoria, el auditor deberá planear el trabajo de auditoria de modo que la auditoria sea desempeñada en una manera efectiva. Planeación significa desarrollar una estrategia general y un enfoque detallado para la naturaleza, oportunidad y alcance esperados de la auditoria. El Auditor planea desempeñar la auditoria en manera eficiente y oportuna” (5:98).

4.2 Conocimiento del Cliente

Al realizar el trabajo de auditoria de estados financieros, el Auditor debe obtener suficiente conocimiento del negocio para que le sea posible identificar y comprender los eventos, transacciones y prácticas que, a su juicio, puedan tener un efecto importante sobre los estados financieros o en el examen y dictamen de la auditoria. Dicho conocimiento es usado al evaluar los riesgos inherentes y de control y al determinar la naturaleza, oportunidad y alcance de los procedimientos de auditoria.

Antes de aceptar el trabajo, el Auditor deberá obtener conocimiento preliminar de la Industria, los dueños, la administración y operaciones de la entidad que auditará, y considerar si puede obtener un nivel de conocimiento del negocio adecuado para desempeñar la auditoria.

4.3 Evaluación de la Estructura de Control Interno

Se deberá obtener una comprensión de los sistemas de contabilidad y de control interno, para su evaluación y posteriormente para planear la auditoria y desarrollar el enfoque de auditoria efectivo y eficiente. El Auditor debería usar juicio profesional para evaluar el riesgo de auditoria y diseñar los procedimientos de auditoria para asegurar que el riesgo se reduce a un nivel aceptable. A fin de confirmar la comprensión de los sistemas contables importantes y los controles relevantes del cliente, se hacen recorridos de cada transacción importante a través de los procedimientos de procesamiento tanto manuales como computarizados y los controles relevantes.

Los recorridos se documentan en un memorando que describe las transacciones escogidas, como confirmación de la comprensión de los procedimientos de procesamiento manual y computarizado, los controles relevantes, y los resultados de los procedimientos. Cuando se han presentado cambios importantes en los sistemas manuales, informáticos o en el entorno de control, tales cambios y sus efectos sobre la planificación de auditoria, se documentan en el Memorando de Planeación de Auditoria. Generalmente se hacen los recorridos durante el evento de planeación para tener seguridad que los resultados se reflejan apropiada y oportunamente en el plan de la auditoria.

4.4 Conocer el Proceso Contable y los Ciclos de Negocios

Se debe obtener una comprensión suficiente del proceso contable y los ciclos de negocios (por ejemplo: cuentas por cobrar / ventas; inventarios / costos de ventas, etc.), para estar en condiciones de identificar riesgos específicos asociados con el proceso contable y para desarrollar un plan de auditoria apropiado.

Se debe distinguir entre clases importantes de transacciones que son procesadas sistemáticamente y aquellas que no lo son. También se debe clasificar el uso del computador del cliente como “importante” o “menor” para determinar la naturaleza, alcance y oportunidad requerida de la comprensión del uso de

computadoras y la necesidad de la ayuda de un especialista de seguridad del computador.

El proceso contable comprende el registro y procedimientos, incluyendo sistemas contables y controles, que el cliente utiliza para identificar, registrar, procesar, sumarizar e informar transacciones y mantener responsabilidad por los activos. El propósito de obtener una comprensión de alto nivel del proceso contable es adquirir una comprensión suficiente para:

- Identificar riesgos específicos;
- Desarrollar un plan de auditoria apropiado.

Esta comprensión provee condiciones para obtener una conclusión inicial acerca de la confiabilidad aparente del proceso contable que ayudará a evaluar si es probable que la estrategia de confiabilidad en los controles sea apropiada. Esta comprensión de alto nivel debe ser obtenida con independencia del hecho que se planee realizar pruebas o confiar en los controles.

El diseño de pruebas de control y pruebas sustantivas depende de la comprensión de la relación entre sistemas de aplicación, saldos de cuenta y tipo de transacciones. Por ejemplo: se obtiene mayor eficiencia si se tiene capacidad de utilizar la comprensión para diseñar procedimientos de auditoria que cubran varios saldos de cuenta y errores potenciales al mismo tiempo. Al preparar una revisión de alto nivel del proceso contable, se considera y concluye sobre la importancia y aparente confiabilidad de cada sistema de aplicación (ciclo de negocios) significativo. Estas conclusiones son la base para la clasificación general de la importancia de las computadoras para el negocio del cliente y del grado de uso. Además, mientras se

comprende el ambiente de la computadora, se obtiene información acerca de los programas y equipos del cliente. Esta información es útil para evaluar la complejidad del ambiente de la computadora, así como la medida en que las computadoras son utilizadas en el negocio.

La clasificación del uso de la computadora por parte del cliente ayuda en la determinación respecto a la inclusión de un especialista de Sistemas – (SIC). En circunstancias en las que no se haya estado en condiciones de realizar las actividades mencionadas arriba, considerar si la comprensión del negocio del cliente y los resultados de otras actividades de planeación preliminares indican el uso extensivo o complejo de los sistemas de la computadora. La inclusión de un Especialista de Sistemas de Información Computarizada – (SIC) ayudará a ampliar la comprensión de alto nivel del proceso contable, aún si el uso de la computadora no es importante.

Se puede identificar circunstancias internas significativas que podrían de otra manera ser pasadas por alto cuando personal profesional con experiencia y conocimientos menos apropiados realiza ese trabajo.

Consideraciones adicionales: El uso de las computadoras por parte del cliente puede ser muy diverso. Las circunstancias siguientes son relativamente comunes, y si alguna aplica, se puede considerar aspectos adicionales relevantes a la clasificación del uso de computadoras y se puede necesitar incluir un especialista de sistemas – (SIC) para determinar la clasificación:

- Clientes con unidades de negocios múltiples que usan:
  - Procesamiento central
  - Procesamiento distribuido
- Existencia de un sistema importante, complejo y significativo que impacta todas las áreas del negocio.
- Uso de una organización de servicios.
- Uso del cliente de paquetes de sistemas contables.

Preparar una revisión de alto nivel del proceso contable: Las actividades principales en la preparación de una revisión de alto nivel del proceso contable son las siguientes:

- Identificar y definir de los sistemas de aplicación significativos: Se puede identificar y comprender el sistema de aplicación principal (ambos basados en la computadora y manual) que alimentan y tienen efecto importante, sobre el mayor general, entonces se tendrá una comprensión de alto nivel del proceso contable. Se busca identificar las fuentes principales de ingresos del mayor general. Estas fuentes serán sistemas de aplicación significativos que se relacionan con el sistema del mayor general. Para una Distribuidora de Repuestos, que es una entidad comercial, estos sistemas de aplicación incluirán:
  - Procesamiento de órdenes y recepción de compras; Cuentas por pagar y procesamiento de los pagos; Contabilidad de los gastos;
  - Procesamiento de órdenes de ventas, envíos y facturación; Cuentas por cobrar y procesamiento de las cobranzas;

- Inventario y Contabilidad de los Costos;
- Contabilidad de activos fijos;
- Pagos de sueldos y procesamiento del personal.

Además de los sistemas de aplicación basados en la computadora, se busca identificar sistemas manuales que alimentan, o que se alimentan del mayor general. (Por ejemplo: sistemas de procesamiento del diario y el sistema para preparación de estados financieros desde el mayor).

Con la finalidad de comprender el efecto que los procedimientos de control tienen sobre los saldos de cuenta, se establece cuáles saldos de cuenta están relacionados con cuáles sistemas de aplicación. (Por ejemplo: ventas y cuentas por cobrar se relacionan con el sistema de Procesamiento de órdenes de ventas, envíos y facturación; Cuentas por cobrar y procesamiento de las cobranzas;).

También se necesita determinar si el sistema procesa o no transacciones en forma sistemática. En la ausencia de otros factores de riesgo, transacciones procesadas sistemáticamente tienen un bajo riesgo de error.

Identificar los sistemas de aplicación que tienen un efecto significativo sobre el proceso contable y de información financiera. Se puede obtener una comprensión de los sistemas no financieros del cliente en la extensión necesaria para comprender como los sistemas financieros utilizan la información procesada por los sistemas no financieros y para comprender como la gerencia controla

el negocio. (Por ejemplo: se puede obtener una comprensión del sistema de control de distribución porque tal sistema de aplicación puede ser fundamental al negocio y puede interrelacionarse en varios puntos con otros sistemas de aplicación).

Un sistema de aplicación significativo tiene un impacto particular sobre la información financiera y contable porque, entre otras características, procesa transacciones importantes. Identificar y definir los sistemas de aplicación significativos para un cliente en particular, son dependientes de hechos y circunstancias y son por lo tanto asuntos de juicio profesional.

Si un sistema de aplicación es muy grande o complejo, se puede dividir en subsistemas de acuerdo a las funciones principales y entonces considerar cada uno de esos subsistemas de aplicación, normalmente se obtiene una comprensión de alto nivel de aquellos sistemas que son probablemente relevantes e importantes para el Contador Público y Auditor.

Al establecer la importancia de cada sistema de aplicación, se consideran asuntos como:

- Importancia de las transacciones procesadas y los saldos de cuenta relacionados.
- Potencial de incremento del riesgo por error o apropiación.
- Si el sistema realiza solamente simple acumulación o funciones de suma o inicia y ejecuta transacciones. (por ejemplo: si el sistema prepara cheques o efectúa transferencias electrónicas

basadas en una compensación autorizada de órdenes de compra, recepción de informes y facturas de vendedores).

- La importancia relativa de los sistemas en las operaciones del negocio del cliente.

Los sistemas que no exhiben estas características son de menos importancia para alcanzar una conclusión sobre la confiabilidad de los sistemas de aplicación en su conjunto.

- Comprensión de la naturaleza y confiabilidad de los sistemas de aplicación significativa: La revisión de alto nivel de sistemas de aplicación significativos necesita contener una breve pero comprensiva descripción de cada sistema, incluyendo el flujo de transacciones.

  Aunque la identificación de controles no es el objetivo principal, probablemente se obtenga conocimiento acerca de los sistemas de control interno del cliente como un subproducto de la comprensión de los sistemas de aplicación. Esto incluirá una comprensión de alto nivel de las actividades de control y los procedimientos de control clave para cada sistema de aplicación.

  Diseñar el enfoque de “arriba hacia abajo” de las pruebas de control dirige a identificar y probar

controles gerenciales de alto nivel más que procedimientos de controles detallados de bajo nivel. Los controles que se identifican mientras se obtiene la comprensión de alto nivel es probable que sean los más eficientes para ser seleccionados para pruebas si se adopta una estrategia de confiar en los controles.

- Documentación de los sistemas de aplicación significativos: Al obtener la comprensión, se obtiene y documenta la información relevante. Por cada sistema de aplicación significativo, se deberá considerar y documentar lo siguiente:
  a) Descripción del sistema, que incluye lo siguiente:
     - Breve descripción del flujo de transacciones significativas procesadas por el sistema;
     - Propósito de negocios del sistema, incluyendo su importancia relativa para las operaciones de negocios;
     - Papel del sistema en la iniciación de transacciones y control del movimiento de activos;
     - Historia del procesamiento de errores por el sistema.
  b) Perfil del Sistema: Se obtiene información tal como el volumen aproximado de transacciones, si el software fue desarrollado internamente o adquirido externamente y la naturaleza del procesamiento (por lotes o en línea).

c) Revisión del procesamiento: Considerar las funciones de procesamientos claves y la frecuencia de su uso (diaria, semanal, mensual). Por ejemplo: las funciones clave de procesamiento del sistema de ventas y facturación pueden ser:

- Preparar facturas diariamente basados en la información relativa a cantidad y precio mantenidas en la computadora;
- Actualizar diariamente los archivos maestros de clientes;
- Actualizar las cuentas a cobrar y producir informes semanales para la gerencia.

Si el cliente tiene múltiples ambientes de procesamiento, se toma nota de los ambientes en los cuales el sistema opera. Esto puede incluir consideraciones de redes locales (LAN), mainframes y organizaciones de servicios.

d) Un flujo general de transacciones a través del sistema, incluyendo:

- Ingresos claves, ya sea de fuente documental o en pantalla. Por ejemplo: se considera si el cliente hace uso de fuente documental, o si se usa un intercambio de información electrónica.
- Salidas clave ya sea en pantalla, en forma electrónica o impresa y su utilización.
- Archivos maestros y tablas importantes y cómo se mantienen.

- Intercambio de información y otras relaciones entre los sistemas. Por ejemplo: la utilización de información de compra por el sistema de pagos. Comprender cómo la gerencia usa el sistema de salida tendrá importancia en la comprensión acerca del control del negocio por la gerencia.

e) Una historia cronológica del sistema: Incluyendo su instalación original y cualquier modificación significativa subsiguiente.

f) Enfoque general del control del sistema: Métodos empleados por la gerencia para determinar que el sistema es confiable:
   - Control de salida;
   - Conciliación de salida con información independiente;
   - Acceso restringido al sistema para ingresos o modificaciones (físico y lógico).

- Establecimiento de una conclusión preliminar acerca de la aparente confiabilidad de los sistemas de aplicación: Basados en toda la información recopilada, se establece una conclusión preliminar acerca de la confiabilidad aparente de cada sistema de aplicación. Considerando:
  - Calidad aparente del procesamiento, incluyendo la historia de errores;
  - Si el sistema es nuevo o ha sido cambiado significativamente;

- Experiencia y competencia del personal que opera el sistema;
- Grado de complejidad de las transacciones procesadas por el sistema;
- Papel del sistema en el control de movimiento de activos.

Ciertas condiciones pueden generar una conclusión preliminar en considerar no confiables los sistemas de aplicación. Esto incluye:

- Historia de errores en el procesamiento del sistema;
- Sistemas con conciliaciones que son indebidamente complejas o contienen numerosos ítems de conciliación;
- Evidencia de la falta de confianza del cliente en el sistema.

Si se concluye que la aplicación de un sistema en particular es aparentemente no confiable, se necesitará considerar si esto origina un riesgo de error del saldo de cuenta en el cual el sistema tiene influencia. Si se ha identificado un riesgo específico asociado con un saldo de cuenta en particular, se relaciona el riesgo de errores potenciales relacionados y se modifica el plan de acuerdo a ello.

- Consideración de la utilización de organizaciones de servicios (si es aplicable): El cliente puede utilizar el servicio de una organización o entidad (conocido en la

- actualidad como Outsourcing – entidad que presta servicios diversos al cliente), tal como una que ejecuta transacciones y procesa la información relativa (por ejemplo: una organización que presta servicios de sistemas de la computadora).

  Se necesita considerar como una organización de servicios afecta los sistemas de contabilidad y control interno del cliente para planear la auditoria y desarrollar un enfoque de auditoria efectivo. Algunas políticas, procedimientos y registros mantenidos por la organización de servicios pueden ser relevantes para la auditoria de los estados financieros.

  Una organización de servicios puede establecer políticas y procedimientos que afectan la organización contable del cliente y los sistemas de control interno. Estas políticas y procedimientos son físicamente y operacionalmente separados de la organización del cliente.

  Cuando la organización de servicios ejecuta las transacciones del cliente y mantiene la contabilidad, el cliente considera necesario confiar en políticas y procedimientos de la organización de servicios. Entonces se necesita determinar el significado de las actividades de la organización de servicios para el cliente y la relevancia para el trabajo de auditoria.

- Revisión de alto nivel del proceso contable: este procedimiento incluye:
  a) Una lista de sistemas de aplicación significativos y su relación con los saldos de cuenta;
  b) Un perfil de información concerniente con cada sistema de aplicación significativo (que puede incluir elementos del ambiente de la computadora y estructura de control de la computadora, si fuera aplicable).

- Comprender el ambiente de la computadora: Al obtener una comprensión del proceso contable, se busca comprender los elementos importantes del ambiente de la computadora dentro del cual opera el sistema contable basado en la computadora. Una comprensión del ambiente de computación puede ser importante para la evaluación del riesgo a nivel de saldo de cuenta y error potencial.

  Los elementos principales del ambiente de la computadora incluyen:
  - Tipos y ubicación de importantes mainframes y otras computadoras (incluyendo redes LAN de PCS, microcomputadoras y otras organizaciones de servicios);
  - Para cada ubicación de procesamiento:
    - Cuáles sistemas de aplicación son de interés para auditar;
    - Naturaleza general de la organización de la función de procesamiento. Por ejemplo: tamaño, estructura e informes de la organización;

- Tipos generales de actividad realizadas tales como operaciones de la computadora, desarrollo y mantenimiento de sistemas y funciones de seguridad y control.
- Manera general en la cual el ambiente de control se maneja y la extensión en las cuales las distintas ubicaciones de procesamiento tienen prácticas y políticas comunes;
- Como interactúan las microcomputadoras de la organización, locales o redes de área amplia y las organizaciones de servicios con los sistemas contables de interés para la auditoria. Por ejemplo: si las microcomputadoras están conectadas con mainframes y con microcomputadoras y tiene la posibilidad de entregar, procesar y/o recibir información contable importante, se necesitará comprender como opera el proceso y como se controla.

Esta información posibilita comprender el ambiente general de la computadora y sus principales componentes, el grado de control centralizado o descentralizado y las interrelaciones entre varias importantes ubicaciones de procesamiento.

Se podría considerar también los principales tipos de programas de la computadora usados en los sistemas contables de la entidad; por ejemplo:

- Programas para controlar el acceso o para seguridad;
- Programa para controlar la biblioteca y el cambio de programas;
- Lenguajes principales de programación;
- Lenguajes para recibir y reportar información;

- Manejo de bases de datos, sistemas de operación y comunicaciones.

Se puede relacionar información acerca del ambiente de la computadora entrevistando personal de la gerencia responsable por los sistemas contables. El personal entrevistado necesita tener un nivel apropiado de conocimiento del ambiente de la computadora. El propósito es obtener una comprensión de alto nivel del ambiente de la computadora, no desarrollar documentación detallada del equipo del sistema de información.

Se puede necesitar discutir con la gerencia y los usuarios de los sistemas sus opiniones acerca de la calidad del sistema contable de la organización y sus principales preocupaciones relativas al proceso de computación. Además, puede ser útil discutir las estrategias de la gerencia y los planes para los sistemas contables.

Se puede considerar factores que influencian las posibilidades de la gerencia para controlar el ambiente de la computadora, tales como la estructura organizacional y los métodos de asignación de autoridad y responsabilidad.

- Comprender la estructura del control de la computadora: Si el cliente es de computadora muy importante, se obtiene una comprensión de alto nivel de la estructura de

control de la computadora, incluyendo controles generales y otro tipo de controles de la computadora. Esta comprensión intenta proveer una indicación preliminar si es probable que existan controles que aseguren que los sistemas de aplicación procesan transacciones en forma confiable o si existen amplias deficiencias que se debe considerar al desarrollar el plan de auditoria.

Se necesita considerar si las deficiencias en los controles generales de la computadora resultan en un proceso no confiable de transacciones por los sistemas de aplicación soportados por esos controles. Si así fuera, se podría considerar esto como un riesgo específico. Se considera si este riesgo elimina la confiabilidad sobre procedimientos de control programados o en los controles de usuarios que son dependientes del procesamiento de la computadora.

También se obtiene información sobre la estructura de control de la computadora para decidir si es apropiado el tamaño y naturaleza de la entidad. Se toma en consideración que negocios diferentes tienen distintos requerimientos de control que dependen de la naturaleza y el tamaño de la entidad.

Basados en la comprensión de los sistemas, se está en condiciones de determinar el grado de dependencia de controles del usuario y otros sobre controles generales del computador.

Típicamente habrá una mayor dependencia sobre los controles generales de la computadora, cuando:

- El ambiente de la computadora resulta más complejo;
- El procesamiento de la computadora resulta más centralizado o interconectado;
- El grado de uso de la computadora tiende a ser más penetrante en la clasificación del uso de la computadora para el cliente.

Se busca obtener información acerca del enfoque general de la gerencia para controlar cada una de las áreas de controles generales de la computadora, la relativa importancia de cada área, los nombres de individuos responsables por funciones de control importantes y la manera en la cual la gerencia supervisa los procedimientos de control en esas áreas.

Las áreas de control general de la computadora y los elementos que se encuentran típicamente en cada área son:

- **Seguridad de la información**
  a) Seguridad de la información, programas y redes;
  b) Seguridad física;
  c) Políticas de seguridad, gerencia y administración;

- **Adquisición de sistemas, desarrollo y mantenimiento**
  a) Planeación, adquisición o programación, pruebas e implantación de nuevos sistemas de aplicación;

b) Cambios a los sistemas de aplicación existentes;
c) Seguridad de la calidad de los sistemas de aplicación;
d) Preparación de la documentación, mantenimiento y control;

- **Operaciones de la computadora**
  a) Programación, establecimiento y procedimientos de operación;
  b) Procedimientos para la administración de una biblioteca;
  c) Procedimientos de control de balances, procesos y salidas.

- **Soporte de los sistemas de información**
  a) Soporte a usuarios de microcomputadoras y lenguajes de extracción de datos;
  b) Soporte y operación de redes;
  c) Cambios en los programas para sistemas operativos y programas de administración de bases de datos;
  d) Administración y soporte de bases de datos.

No todas las áreas de controles generales de la computadora son aplicables a cada ambiente de procesamiento de la computadora, ni son todas ellas relevantes a la auditoria. Por ejemplo: algunas compañías pueden comprar programas de computadora y no mantener una función de desarrollo de sistemas. En otras situaciones, sistemas de aplicación pueden ser adecuadamente controlados por procedimientos de control y

actividades de supervisión que dependen de unos pocos o ningún control general de la computadora.

Generalmente se obtiene la información anterior, entrevistando gerentes responsables por las distintas áreas de control. Si fuera apropiado, se considera combinar las preguntas acerca de la estructura de control de la computadora y del ambiente de control en la misma reunión. En otras situaciones, se puede concluir las entrevistas cuando se haya obtenido una visión global de la estructura del control de la computadora y del control interno.

4.5 Evaluar el Riesgo en el Entorno de Control

Se deberá obtener una comprensión de los sistemas de contabilidad y de control interno suficiente para planear la auditoria y desarrollar un enfoque de auditoria efectivo. El auditor debería usar juicio profesional para evaluar el riesgo de auditoria y diseñar los procedimientos de auditoria para asegurar que el riesgo se reduce a un nivel aceptablemente bajo" (3:118).

"El término – Sistema de Control Interno, significa todas las políticas y procedimientos (controles internos) adoptados por la administración de una entidad para ayudar a lograr el objetivo de la administración de asegurar, tanto como sea factible, la conducción ordenada y eficiente de su negocio, incluyendo adhesión a las políticas de administración, la salvaguarda de activos, la prevención y detección de fraude y error, la precisión e integridad de los registros contables, y la oportuna preparación de información financiera confiable"(3:118).

“El riesgo de auditoria, significa el riesgo que el auditor dé una opinión de auditoria inapropiada cuando los estados financieros están elaborados en forma errónea de una manera importante. El riesgo de auditoria tiene tres componentes:

- Riesgo inherente;
- Riesgo de control y
- Riesgo de detección.

El riesgo inherente, es la susceptibilidad del saldo de una cuenta o clase de transacciones a una representación errónea que pudiera ser de importancia relativa, individualmente o cuando se agrega con representaciones erróneas en otras cuentas o clases, asumiendo que no hubo controles internos relacionados.

El riesgo de control, es el riesgo de que una representación errónea que pudiera ocurrir en el saldo de cuenta o clase de transacciones y que pudiera ser de importancia relativa individualmente o cuando se agrega con representaciones erróneas en otros saldos o clases, no sea prevenido o detectado y corregido con oportunidad por los sistemas de contabilidad y de control interno.

El riesgo de detección, es el riesgo de que los procedimientos sustantivos de un auditor no detecten una representación errónea que existe en un saldo de cuenta o clase de transacciones que podría ser de importancia relativa, individualmente o cuando se agrega con representaciones erróneas en otros saldos o clases” (3:118).

4.6 Sistemas Contables y Control Interno

Como se detallo en el inciso 4.3 Evaluación de la Estructura del Control Interno, se debe obtener una comprensión de los sistemas contables y de control interno y plasmarlo en un memorando de recorridos. A continuación se describe el sistema contable y el control interno:

El Sistema Contable o Sistema de Contabilidad, significa la serie de tareas y registros de una entidad por medio de las que se procesan las transacciones como un medio de mantener registros financieros. Dichos sistemas identifican, reúnen, analizan, calculan, clasifican, registran, resumen e informan transacciones y otros eventos.

En la auditoria de estados financieros, el auditor está interesado sólo en aquellas políticas y procedimientos dentro de los sistemas de contabilidad y de control interno que son relevantes para las aseveraciones de los estados financieros. La comprensión de los aspectos relevantes de los sistemas de contabilidad y de control interno, junto con las evaluaciones del riesgo inherente y de control y otras consideraciones, harán posible para el auditor:

- Identificar los tipos de potenciales representaciones erróneas de importancia relativa que pudieran ocurrir en los estados financieros;
- Considerar los factores que afectan el riesgo de representaciones erróneas sustanciales; y
- Diseñar procedimientos de auditoria apropiados.

El Control Interno o Sistema de Control Interno, significa todas las políticas y procedimientos (controles internos) adoptados por la administración de una entidad para ayudar a lograr el objetivo de la administración de asegurar, tanto como sea factible, la conducción ordenada y eficiente de su negocio, incluyendo adhesión a las políticas de administración, la salvaguarda de activos, la prevención y detección de fraude y error, la precisión e integridad de los registros contables y la oportuna preparación de información financiera contable. El sistema de control interno va más allá de aquellos asuntos que se relacionan directamente con las funciones del sistema de contabilidad y comprende:

a) El ambiente de control, que significa la actitud global, conciencia y acciones de directores y administración respecto del sistema de control interno y su importancia en la entidad. El ambiente de control tiene un efecto sobre la efectividad de los procedimientos de control específicos. Un ambiente de control fuerte, por ejemplo, uno con controles presupuéstales estrictos y una función de auditoria interna efectiva, pueden complementar en forma muy importante los procedimientos específicos de control. Sin embargo, un ambiente fuerte no asegura, por sí mismo, la efectividad del sistema de control interno. Los factores reflejados en el ambiente de control incluyen:

- La función del consejo de directores y sus comités;
- Filosofía y estilo operativo de la administración;
- Estructura organizacional de la entidad y métodos de asignación de autoridad y responsabilidad;

- Sistema de control de la administración incluyendo la función de auditoria interna, políticas de personal y procedimientos y segregación de funciones o deberes.

b) Procedimientos de control, significa aquellas políticas y procedimientos además del ambiente de control que la administración ha establecido para lograr los objetivos específicos de la entidad. Los procedimientos específicos de control incluyen:

- Reportar, revisar y aprobar conciliaciones;
- Verificar la exactitud aritmética de los registros;
- Controlar las aplicaciones y ambiente de los sistemas de información por computadora, por ejemplo, estableciendo controles sobre:
  - Cambios a programas de computadora;
  - Acceso a archivos de datos
- Mantener y revisar las cuentas de control y las balanzas de comprobación;
- Aprobar y controlar documentos;
- Comparar datos internos con fuentes externas de información;
- Comparar los resultados de cuentas del efectivo, valores e inventarios con los registros contables;
- Limitar el acceso físico directo a los activos y registros;
- Comparar y analizar los resultados financieros con las cantidades presupuestadas.

En la auditoria de estados financieros, el Auditor está interesado sólo en aquellas políticas y procedimientos dentro de los sistemas de contabilidad y de control interno que son relevantes

para las aseveraciones de los estados financieros. La comprensión de los aspectos relevantes de los sistemas de contabilidad y control interno, junto con las evaluaciones del riesgo inherente, de control y otras consideraciones, harán posible para el auditor:

- Identificar los tipos potenciales de representaciones erróneas de importancia relativa que pudieran ocurrir en los estados financieros;
- Considerar factores que afectan el riesgo de representaciones erróneas sustanciales; y
- Diseñar procedimientos de auditoria apropiados.

Al desarrollar el enfoque de auditoria, se considera la evaluación preliminar del riesgo de control (conjuntamente con la evaluación de riesgo inherente) para determinar el riesgo de detección apropiado por aceptar para las aseveraciones del estado financiero y para determinar la naturaleza, oportunidad y alcance de los procedimientos sustantivos para dichas aseveraciones.

4.7 Determinar la Materialidad

El objetivo de una auditoria de estados financieros es hacer posible al Auditor expresar una opinión sobre si los estados financieros están preparados, respecto de todo lo importante, de acuerdo con Normas Internacionales de Contabilidad ó de acuerdo con un marco de referencia para informes financieros identificado. La evaluación de qué es importante, es asunto de juicio profesional. “La Materialidad Preliminar es el juicio preliminar de materialidad hecho durante la planeación inicial.

Se utiliza para desarrollar el alcance general de los procedimientos de auditoria" (5:94).

Al diseñar el plan de auditoria, se establece un nivel aceptable de importancia relativa a modo de detectar en forma cuantitativa las representaciones erróneas de importancia relativa. Sin embargo se necesita considerar tanto el monto (cantidad) y la naturaleza (calidad) de las representaciones. Las representaciones erróneas cualitativas sería la descripción inadecuada e impropia de una política de contabilidad cuando es probable que un usuario de los estados financieros fuera guiado equivocadamente por la descripción y el dejar de revelar la infracción a requerimientos reguladores cuando es probable que al imponer restricciones regulatorias pueda hacer disminuir en forma importante la capacidad de operación del negocio.

Cuando se planea la auditoria, se debe considerar los asuntos que provocarán que los estados financieros pudieran estar representados erróneamente con una importancia relativa. La evaluación que se realice de la importancia relativa, relacionada con saldos de cuenta y clases de transacciones específicos, ayudarán a decidir qué partidas se examinarán y si se usará procedimientos de muestreo estadístico y procedimientos analíticos. Esto da la capacidad al Auditor para seleccionar procedimientos de auditoria que, en combinación, puede esperarse que reduzcan el riesgo de auditoria a un nivel aceptablemente bajo.

4.8 Preparar el Memorando de Planeación - Guía de Auditoria

Se debe desarrollar y documentar un plan de auditoria describiendo el alcance y conducción esperados de la auditoria. El plan de auditoria deberá estar suficientemente detallado para guiar el desarrollo del programa de auditoria, su forma y contenido precisos variarán de acuerdo al tamaño de la entidad, la complejidad de la auditoria, la metodología y tecnología específicas usadas por el Auditor.

Los asuntos que tendrá que considerarse al desarrollar el plan global de auditoria incluyen:

- **Conocimiento del Negocio del Cliente**
  1. Factores económicos generales y condiciones de la industria que afectan el negocio de la entidad;
  2. Características importantes de la entidad, su negocio, su desempeño financiero y sus requerimientos para informar incluyendo cambios desde la fecha de la anterior auditoria;
  3. El nivel general de competencia de la administración.

- **Comprensión de los sistemas de contabilidad y de control interno**
  1. Las políticas contables adoptadas por la entidad y los cambios en esas políticas;
  2. El efecto de pronunciamientos nuevos de contabilidad y auditoria;
  3. El conocimiento acumulable del Contador Público y Auditor sobre los sistemas de contabilidad y de control interno y

el relativo énfasis que se espera poner en las pruebas de control y otros procedimientos sustantivos.

- **Riesgo e importancia relativa**

1. Las evaluaciones esperadas de los riesgos inherentes y de control y la identificación de áreas de auditoria importantes;
2. El establecimiento de niveles de importancia relativa para propósitos de la auditoria;
3. La posibilidad de representaciones erróneas, incluyendo la experiencia de períodos pasados, de error o fraude;
4. La identificación de áreas de contabilidad complejas incluyendo las que implican estimaciones contables.

- **Naturaleza, tiempos y alcance de los procedimientos**

1. Posible cambio de énfasis sobre áreas específicas de auditoria;
2. El efecto de la tecnología de información sobre la auditoria;
3. El trabajo de auditoria interna y su esperado efecto sobre los procedimientos de auditoria externa.

- **Coordinación, dirección, supervisión y revisión**

1. La participación de otros auditores en la auditoria de componentes, por ejemplo: subsidiarias, sucursales y divisiones;
2. El involucramiento de expertos;
3. El número de localidades;
4. Requerimientos de personal.

- **Otros Asuntos**

1. La verificación del supuesto de negocio en marcha, el cuál pueda ser cuestionado;
2. Condiciones que requieren atención especial, como la existencia de partes relacionadas;
3. Los términos del trabajo y cualesquiera responsabilidades estatutarias o fiscales y tributarias;
4. La naturaleza y oportunidad de los informes u otra comunicación con la entidad que se esperan bajo términos del trabajo.

4.9 Desarrollar el Plan de Enfoque de Auditoria

Los integrantes del equipo de trabajo se reúnen nuevamente para discutir lo que han aprendido sobre el cliente, incluyendo los cambios importantes en sus negocios, modificaciones a la evaluación del entorno general de control, cambios en los sistemas y controles, resultados de la revisión analítica y áreas principales de auditoria que deben destacarse.

Como resultado de esta información, el equipo evalúa colectivamente los cambios importantes desde el año anterior a fin de actualizar el enfoque actual de auditoria. Además, se discuten las estrategias que se pueden implantar para mejorar la eficiencia general de la auditoria.

4.10 Programa de Procedimientos de Auditoria

Se debe desarrollar y documentar un programa de auditoria que describa la naturaleza, oportunidad y alcance de los procedimientos de auditoria planeados. El programa de auditoria sirve como un conjunto de instrucciones a los auxiliares involucrados en la auditoria y como un medio para el control y registro de la ejecución apropiada del trabajo. El programa de auditoria puede también contener los objetivos de la auditoria para cada área y un presupuesto de tiempos en el que son presupuestadas las horas para las diversas áreas o procedimientos de auditoria.

En la preparación del programa de auditoria, se debería considerar las evaluaciones específicas de los riesgos inherentes y de control y el nivel requerido de certeza que tendrán que proporcionar los procedimientos sustantivos. Se deberá también considerar los tiempos para pruebas de controles y de procedimientos sustantivos, la coordinación de cualquier ayuda esperada de la entidad, la disponibilidad de los auxiliares y el involucramiento de otros auditores o expertos, tal como el Auditor de Sistemas de Información por Computadora. Para hacer las pruebas de auditoria asistidas por el computador – CAATs (en Ingles – TAACs), es necesario hacer uso del software ACL.

Uso del software ACL para hacer pruebas TAACs: ACL (en inglés – ACL - Audit Consult Language) es una herramienta genérica desarrollada por ACL Services Ltd., esta entidad es especializada en desarrollo, ubicada en Vancouver – Canadá. La herramienta ACL es especialmente desarrollada para realizar pruebas de auditoria con ayuda del computador, TAACs o CAATs - (Técnicas de Auditoria Asistidas por Computador o

Computing Auditing Assisted Techniques). Esta es una herramienta importante que permite utilizar información almacenada en los archivos de la computadora del cliente. Para interrogar los archivos, la ayuda de un auditor de sistemas de información, puede ser apropiada cuando se usa programas de interrogación de archivos. El ACL, es una herramienta analítica poderosa, porque puede manejar grandes volúmenes de información eficientemente.

Uso del Computador en la Auditoria El software usado por los auditores en la ejecución de auditorias generalmente clasifica dentro de una de las siguientes tres categorías. El primer tipo son herramientas de auditoria basadas en el micro que son desarrollados y diseñados para planear, ejecutar y evaluar los procedimientos de auditoria, independientemente de si los clientes están automatizados o no.

El segundo tipo de software se usa para interrogar y examinar los archivos de datos del cliente. Estos procedimientos son generalmente denominados técnicas de auditoria asistidas por el computador (CAATs). Este software, denominado ACL, requería históricamente un computador grande para su ejecución. Sin embargo, el software ACL de hoy día puede ser ejecutado tanto en equipo grande como en el microcomputador.

“Cuando un computador es usado para mantener o procesar información contable, el software ACL puede ser usado para ejecutar procedimientos tales como cálculos (sumas, extensiones, procedimientos de revisión analítica, antigüedad de la cuenta), pruebas lógicas (clasificación, sumarización, comparación de montos del año corriente con el año anterior, consumo hasta la fecha con el saldo actual), selección e impresión de partidas claves y de muestras representativas.

El uso de ACL hace la auditoria (1) más completa, ya que cada partida en un archivo puede ser examinada y sujeta a una variedad de pruebas, y (2) más eficiente porque el computador puede manejar grandes volúmenes de datos, reduciendo así las dispendiosas tareas de los auxiliares. El uso del software ACL para automatizar las pruebas CAATs, permite que el auditor se concentre en la especificación de los criterios de prueba y en evaluar e interpretar los resultados de las pruebas, en lugar de desarrollar los procedimientos detallados de auditoria" (5:183).

El tercer tipo de software de auditoria, denominado como otro software, no está generalmente diseñado para fines de auditoria específicos. Sin embargo, el otro software es usado para ayudar al auditor en la auditoria.

El otro software son programas diseñados y desarrollados para ser corridos en microcomputadores, algunos son:

- Hojas electrónicas de cálculo
- Procesadores de palabras
- Balances de prueba / informes financieros
- Correo electrónico
- Flujogramación
- Manejo de bases de datos
- Gráficas

Software CAATs Al planear los procedimientos de auditoria, se considera una combinación apropiada de técnicas manuales de auditoria y los CAATs. Al determinar si se van a usar los CAATs, considerar sí:

1. La ausencia de documentos de entrada o falta de una ruta visible de auditoria puede requerir el uso de CAATs para probar controles y ejecutar procedimientos sustantivos, por ejemplo:

   a. Los documentos de entrada pueden ser inexistentes cuando las órdenes de venta son incorporadas en línea. Además, las transacciones contables, como los descuentos y cálculos de intereses, pueden ser generadas por programas de computador sin autorización visible de transacciones individuales.

   b. El sistema puede no producir una ruta de auditoria visible de transacciones procesadas a través del computador. Las notas de entrega y las facturas de proveedores pueden ser cruzadas por un programa de computador. Además, los procedimientos de controles programados, como la verificación de los límites de los clientes, pueden aportar evidencia visible sólo excepcionalmente. En dichos casos, puede no haber evidencia visible de que todas las transacciones han sido por excepción.

   c. Los informes de resultados pueden no ser producidos por el sistema. Además, un informe impreso puede sólo contener información sumaria mientras que los detalles de soporte que pueden ser útiles para fines de auditoria son retenidos en los archivos del computador.

2. La eficacia y eficiencia de los procedimientos de auditoria pueden ser mejorados mediante el uso de los CAATs, por ejemplo:

a. Algunas transacciones pueden ser probadas más eficazmente respecto a un nivel similar de costo utilizando el computador para examinar todas o un mayor número de transacciones al que de otro modo podrían seleccionarse.
b. Al aplicar los procedimientos de revisión analítica, pueden revisarse los detalles de las transacciones o del saldo e imprimirse los informes sobre partidas inusuales más eficientemente usando el computador que mediante métodos manuales.
c. El uso de CAATs para probar los controles programados puede ser más eficiente que ejecutar procedimientos sustantivos extensos.

Una consideración importante al decidir usar CAATs es la naturaleza y el alcance de los procedimientos que se requieren satisfacer, que los registros usados (manuales o computarizados) contengan toda la información necesaria, y que la información sea confiable. Como es el caso con cualquier procedimiento de auditoria, la naturaleza y el alcance de los procedimientos ejecutados con un CAAT dependerán ampliamente de la evaluación de la eficacia del entorno de control del cliente y los controles de aplicación tanto programados como manuales.

Un solo CAAT puede ser diseñado para ejecutar varias pruebas al mismo tiempo, aumentando así la eficiencia de la auditoria. Sin embargo, antes de desarrollar cualquier CAAT, se da

consideración al costo del CAAT en relación con el costo de otros métodos para lograr los objetivos de la auditoria.

Planeación Se identifican las posibles aplicaciones CAAT durante el proceso de planeación. Una vez se ha identificado un CAAT potencial, el equipo de auditoria y, cuando sea apropiado el auditor de sistemas de información evalúan la factibilidad de desarrollar e implantarlo. Un auditor de sistemas de información puede ser particularmente valioso al hacer esta evaluación debido al entrenamiento especializado que ha recibido. Los pasos para evaluar la factibilidad son determinar el alcance y los objetivos del procedimiento, los informes resultantes necesarios, los archivos disponibles del cliente y el procedimiento requerido. También son considerados el equipo del computador a ser usado, el software requerido, el personal necesario y la oportunidad en la cual se debe completar el CAAT.

Cuando sea apropiado, se desarrollan costos estimativos para los costos no recurrentes de desarrollar el CAAT y los costos recurrentes de procesarlo. Estos estimativos son comparados con los costos de las técnicas alternativas que podrían ser usadas.

Equipo de Cómputo Los CAATs son procesados en computadores del cliente, del auditor y de terceros (centros de servicio – cuando se trabaja Outsourcing en el cliente). La selección del equipo más apropiado para una aplicación CAAT particular dependerá de una serie de criterios, incluyendo:

a. Requisitos del software CAAT
b. El tamaño de los archivos de datos del cliente relativos a la capacidad y desempeño del equipo disponible.

Con frecuencia los clientes ponen sus computadores a la disposición del auditor. La ventaja de usar los computadores del cliente son que hay poco costo de procesamiento, si lo hubiere, a facturar al cliente, hay personal disponible que entiende los procesos y los archivos, y los archivos de datos que contienen información patentada permanecen en las instalaciones del cliente. Cuando se usa el equipo del cliente, considerar la necesidad de ejecutar procedimientos de control adicionales.

Generalmente, el alcance del equipo computarizado usado por los clientes es diverso y los CAATs no siempre pueden ser corridos en todos los sistemas del cliente. Por lo tanto, con frecuencia será más eficiente obtener una copia de la información del cliente y procesarla en otro computador cuando haya disponibilidad de software apropiado como ACL.

Software Si la información del cliente es cargada en un microcomputador, se tiene la flexibilidad de usar una amplia gama de software de microcomputador, por ejemplo, hojas electrónicas de cálculo, gráficas y análisis estadísticos, además del software CAAT desarrollado en ACL, tales como muestreo estadístico, histogramas y rutinas de cruce.

Cuando el software CAAT no es mantenido bajo el control permanente del auditor (es decir, programas suministrados por el proveedor para el cliente), necesita considerar:

a. Los cambios efectuados para adaptar el paquete a las necesidades del cliente.
b. La versión del paquete que el cliente está usando.

Cualquiera de estos factores puede afectar la capacidad del software CAAT de lograr los objetivos de auditoria. Finalmente, la capacidad de usar paquetes de software que no están bajo el

control del auditor dependerá del alcance a que los resultados de la aplicación estén sujetos a otros procedimientos de verificación (por ejemplo, conciliación de conteos de registros o pruebas de resultados de procesamiento).

Personal Los CAATs son revisados, y generalmente, ejecutados por un auditor de sistemas de información u otra persona con capacidad y experiencia apropiadas. Los auditores de sistemas de información son capacitados en el uso del software, en redactar y probar los CAATs, y en controlar su procesamiento.

Ocasionalmente los auditores internos con capacitación en computadores o el personal de procesamiento de datos del cliente pueden ayudar a desarrollar programas de auditoria computarizados de propósito específico. En estos casos, necesitamos lograr un claro entendimiento con el cliente respecto a la prioridad que se le debe dar a desarrollar los programas, las fechas de terminación programadas, y la necesidad del auditor de dirigir al personal del cliente en esta actividad. Un auditor de sistemas de información u otra persona con apropiada capacitación y experiencia supervisa el desarrollo de los programas, participa en su prueba (para asegurarse que los programas sean desarrollados según lo especificado) y controla los archivos de entrada de datos del cliente antes y durante el procesamiento.

Sin embargo, cuando intentamos confiar en el trabajo de los auditores internos, evaluamos su competencia y objetividad y

revisamos su trabajo en la misma forma en que revisamos el trabajo de nuestro propio personal.

Desarrollo y Prueba Inicialmente, el equipo de auditoria y, cuando sea apropiado el auditor de sistemas de información revisa el CAAT planeado, define el trabajo para desarrollar e implantarlo, establece el presupuesto de tiempo, y estipula la supervisión del trabajo.

Las especificaciones detalladas de la aplicación incluyen ordinariamente dentro del programa de auditoria de sistemas de información por computadora:

- Flujograma de procesamiento del sistema y narrativa;
- Esquemas de archivos de datos de entrada y salida;
- Esquema de Informes;
- Narrativas de programas o cuadros lógicos;
- Instrucciones de operaciones;
- Procedimientos de verificación de control de totales;
- Plan de prueba, datos de prueba y resultados predeterminados.

Después de que las especificaciones detalladas de la aplicación han sido preparadas y aprobadas por el equipo de auditoria, el programa es redactado y probado para determinar que funcionará apropiadamente y producirá resultados confiables. Cuando sea apropiado el auditor de sistemas de información supervisa o participa en el desarrollo y la prueba.

Control del Procedimiento Normalmente se controla o supervisa lo siguiente:

- Los programas a ser usados para el procesamiento;
- La documentación del programa;
- El control del trabajo;
- Archivos de datos significativos de entrada y salida;
- Procedimientos operacionales durante el procesamiento;
- Informes de resultados.

"Es importante controlar el procesamiento de las aplicaciones CAATs, especialmente cuando se usa el computador del cliente y el programa es corrido por él. Mantener el control sobre los programas a ser usados ayuda a asegurar la confiabilidad de los resultados. El auditor se satisface que la versión probada del programa es la que se usa realmente en el procesamiento, guardando una copia en sus papeles de trabajo; esta copia controlada del programa es usada más adelante en el procesamiento del CAAT. (Cuando se usa el programa del cliente en un CAAT, se analiza y se hacen pruebas antes del procesamiento real)" (5:185).

El control de los archivos de datos de entrada requiere la seguridad que los archivos usados son auténticos. Los procedimientos usados incluyen la verificación de totales de control, del archivo de datos conciliando con los registros contables del cliente. Por ejemplo, cuando se usa un CAAT para seleccionar una muestra antes de ejecutar cualquier procedimiento adicional, se verifican los totales del control (producidos por el CAAT mientras se selecciona la muestra) con los registros del cliente.

"No se necesita operar personalmente el computador durante el procesamiento del CAAT, pero el auditor es conocedor de las operaciones que se están ejecutando para poder supervisar y controlar el CAAT. Se verifica los archivos de datos de entrada y salida que se están usando para asegurarse que son los archivos apropiados, y se revisan los mensajes del sistema. Normalmente, los CAATs son diseñados para proporcionar totales de control de procesamiento de corrida a corrida que pueden ser cruzados hacia delante y hacia atrás con otros registros para fines de verificación" (5:185).

Documentación Los papeles de trabajo de auditoria documentan el diseño, la codificación, la prueba y el procesamiento de los CAATs.

La documentación de diseño describe el procesamiento general, incluyendo:

a. La identificación de los archivos de datos de entrada (por ejemplo, inventario físico de fin de año)
b. La descripción de los pasos importantes del CAAT y las principales funciones de procesamiento (por ejemplo, calcular las extensiones de valores y sumar los archivos);
c. La identificación del resultado, incluyendo la forma física, el uso y los requisitos de retención (por ejemplo, el informe de elementos de inventario potencialmente obsoletos que serán solicitados para evaluar la reserva de obsolescencia y retenidos en los papeles de trabajo como evidencia de la evaluación).

CAPITULO V
CASO PRÁCTICO – PLANEACIÓN DE LA AUDITORÍA EN UN AMBIENTE DE SISTEMAS DE INFORMACIÓN POR COMPUTADORAS EN UNA DISTRIBUIDORA DE REPUESTOS

5.1 Planeación de la Auditoria – Introducción

En el estudio del caso práctico se analiza la Distribuidora de Repuestos, S. A., siendo necesario definir cada una de las actividades relacionadas con el enfoque de auditoria, con el propósito de ayudar en la organización y ejecución de actividades relacionadas con la auditoria financiera y evaluación de los sistemas de información por computadora que afectan las aplicaciones que son utilizadas para registrar las transacciones contables y que afectan las aseveraciones en los estados financieros.

A continuación se presentan los lineamientos de cómo efectuar una adecuada planeación de la auditoria, y específicamente los lineamientos para la evaluación de los sistemas de información, cuando los ambientes de procesamiento sistematizados son complejos y afectan las transacciones contables.

El esquema del proceso de planeación de la auditoria financiera y la evaluación de los ambientes de sistemas de información por computadora, que ejecutan los auditores y los resultados de tales procedimientos se detallan a continuación.

En primer plano se tienen el conocimiento del negocio del cliente, evaluación de la estructura del control interno, conocimiento de los procesos contables y los ciclos de negocios, a través de recorridos;

después evaluar el riesgo en el entorno de control, definir el entendimiento de los sistemas contables y de control interno; también determinar la materialidad preliminar del compromiso.

Con la acumulación de información de los pasos anteriormente descritos se prepara el memorando de planeación de auditoria (guía de auditoria), el desarrollo del plan de enfoque de auditoria y los programas de procedimientos de auditoria financiera y la evaluación de los sistemas de información por computadora, que afectarán las aseveraciones presentadas en los estados financieros y por último se elabora el memorando resumen de auditoria.

Derivado de los procedimientos anteriormente descritos, se desarrolla y ejecuta el enfoque de auditoria, haciendo las pruebas de auditoria sobre controles contables, la evaluación de controles generales y de aplicación de los sistemas de información por computadora, pruebas sustantivas de auditoria con ayuda del computador (CAATs) y por último se revisa los resultados relevantes del trabajo realizado, junto con los hallazgos y recomendaciones de auditoria.

EVENTO DE PLANEACIÓN

Distribuidora de Repuestos, S. A.
Al 31 de diciembre de 200x

Lunes 09/01/200x 10 a.m.	
Orientar al equipo de trabajo	Equipo de Auditoria
Lunes 09/01/200x 14 p.m.	
Reunión con el cliente	Equipo de Auditoria y Cliente
Lunes 09/01/200x 17 p.m.– Martes 10/08/200x 9 a.m.	
Reuniones adicionales	Auditor responsable – Ejecutivos del cliente
	Auditor, Auditores SIC - Gerente de Procesamiento de Datos – del cliente
Lunes 09/01/200x 17 p.m.– Miércoles 11/01/200x 12 a.m.	
Recorridos	Auditor, asistentes, según sea apropiado (con ayuda de otros auditores)
Completar “otros asuntos”	Según sea apropiado
Miércoles 11/01/200x 14 p.m.	
Actualizar enfoque de auditoria y Programa de auditoria	Equipo de Auditoria
Preparar memorando de Planeación de auditoria	Equipo de Auditoria
Preparar carta de servicios al cliente	Equipo de Auditoria

(Nota: El auditor responsable estará presente todo el día lunes y el miércoles en la tarde)

AGENDA PARA LA REUNIÓN DE PLANEACIÓN DE AUDITORÍA - EQUIPO DE AUDITORÍA

Distribuidora de Repuestos, S. A.
Al 31 de diciembre del 200x

I. Participación de la información sobre el cliente, obtenida por el equipo desde la auditoria del año anterior (si aplicaré).

II. Cómo afectan el proceso de auditoria los acontecimientos comerciales del cliente, incluyendo las tendencias industrial y económica.

III. Revisión de los resultados financieros intermedios y previstos del cliente.

IV. Problemas observados en las auditorias anteriores (si aplicare).

V. Asuntos de auditoria y contabilidad del año actual y el enfoque para abordarlos.

VI. Evaluación del entorno de control.

VII. Recorridos para confirmar nuestra comprensión de los sistemas y controles del cliente.

VIII. Recorridos para confirmar nuestra comprensión de los controles informáticos y los sistemas de aplicación.

IX. Evaluación del riesgo y de las estrategias dentro del plan de auditoria.

X. Establecimiento de la materialidad preliminar, margen de error tolerable y alcances.

XI. Identificar las estrategias dentro del plan para mejorar la eficiencia en auditoria. Establecimiento de metas de mejoría y cómo medirlas.

XII. Tareas y responsabilidades de los integrantes del equipo de trabajo.

XIII. Cómo responderá el auditor a las expectativas del cliente.

XIV. Factores considerados en la revisión anual de continuación o aceptación de clientes.

AGENDA PARA LA REUNIÓN DE ESTRATEGIAS DE AUDITORÍA - CLIENTE

Distribuidora de Repuestos, S. A.
Al 31 de diciembre del 200x

I. Acontecimientos comerciales recientes:

- A. Cambios en la industria y las operaciones del cliente (pe., adquisiciones, nuevos sistemas importantes).
- B. Cambios en las condiciones económicas.
- C. Resultados financieros intermedios y previstos.
- D. Estrategias comerciales.

II. Cambios en los sistemas y/o estructura de control interno del cliente:

III. Alcance de la auditoria:

- A. Responsabilidad de la presentación razonable de los estados financieros.
- B. Participación de los auditores internos.
- C. Asuntos sobre localidades múltiples.

IV. Asuntos de contabilidad y auditoria:

- A. Áreas importantes de juicio.
- B. Nuevos requisitos contables.

V. Expectativas del cliente:

- A. Áreas a las cuales la gerencia desea que el Auditor enfoque su mayor atención.
- B. Duración esperada del trabajo.
- C. Áreas donde el auditor puede brindar valor agregado al cliente.
- D. Productos del proceso de auditoria.

VI. Asuntos administrativos:

- A. Ayuda del cliente.
- B. Dotación de personal de auditoria.
- C. Calendario.

ASUNTOS A CONSIDERAR DURANTE LAS REUNIONES CON EL CLIENTE

Asuntos a discutir en reuniones con gerentes clave de operaciones y finanzas (Por ejemplo, producción, mercadeo, desarrollo de nuevos productos, personal). Enfoque del entorno comercial y económico que afectan al cliente, las estrategias de negocios y los cambios en estas áreas:

- Objetivos a mediano y largo plazos:
  - Oportunidades; riesgos; factores críticos de éxito
- Productos competitivos y sustitutos, incluyendo la tecnología relevante
  - Condiciones económicas/políticas/legales/reglamentarias en la industria/mercados del cliente
- Objetivos comerciales para el año y éxitos hasta la fecha
- Cambios en productos/segmentos del mercado/áreas geográficas
- Cambios en las estrategias de mercadeo
- Cambios importantes en la base de consumidores/proveedores
- Adquisiciones/enajenaciones de entidades, actuales o anticipadas
- Cambios en la gerencia
- Cambios en los tenedores de los negocios
- Satisfacción con la información gerencial
- Establecimiento de información clave utilizada por el director ejecutivo para manejar y supervisar el negocio

Otros asuntos para discutir en reuniones con el director financiero y otro personal contable clave

- Revisión del presupuesto para el año y resultados reales hasta la fecha
- Informes de los reguladores
- Relaciones con los proveedores clave de financiación y los analistas financieros
- Convenios de deuda, riesgos de incumplimiento y otras inquietudes de liquidez
- Cambios en los términos de crédito para los consumidores
- Cambios en los sistemas de información y uso de tecnología de información
- Controles a los cuales la gerencia otorga confianza y cualesquier cambios en los mismos desde el año anterior
- Cambios en sistemas contables importantes
- Cambios en políticas/procedimientos/personal contables
- Efectos de cambios recientes a las normas contables
- Efectos de regulaciones recientes o pendientes
- Existencia de litigios/contingencias importantes

CARTA DE SERVICIOS AL CLIENTE

23 de Septiembre de 200X

Sr. Bruno Díaz
Director Ejecutivo
Distribuidora de Repuestos, S. A.

Estimado Bruno:

Gracias por haber participado en nuestras actividades de planeación de la auditoria en fecha reciente. Su estímulo hacia los asuntos críticos que afectan a Distribuidora de Repuestos, S. A., las inquietudes expresadas sobre algunas de sus operaciones y las expectativas establecidas por usted sobre la auditoria, nos han ayudado mucho en el desarrollo de nuestro plan de auditoria. Como indiqué durante nuestra reunión, nos comprometemos a entregar una auditoria eficiente y de alta calidad, así como otros servicios que puedan brindar valor agregado a Distribuidora de Repuestos, S. A. El objeto de esta carta es confirmar cómo pretendemos lograr tal compromiso.

Sus asuntos críticos e inquietudes:

He estado pensando en algunos de los asuntos mencionados por usted durante nuestra reunión.

Usted indicó su preocupación sobre el problema que está enfrentando la compañía con los efectos de la aplicación de inventarios. Ustedes consideran que, aunque aprecian nuestra ayuda para la evaluación de los ambientes de sistemas de información y las diferentes aplicaciones financieras y contables, la cuantía actual de tales costos de modificación es claramente mucho más crítica. Con tal objeto, Luís Mirón y yo nos reuniremos el próximo martes con Juan Pérez de su departamento de beneficios. Luís es un auditor con experiencia considerable en la reestructuración de planes de evaluación de ambientes de sistemas de información. Reconocemos la importancia de este asunto, particularmente si tenemos en cuenta que su tiempo vence a finales de este año.

Otra área a la cual enfocaremos nuestra atención es el nuevo programa de garantías descrito por usted y la administración de sus costos. Además de revisar y someter a prueba sus procedimientos para determinar las expectativas de cambios, realizaremos una revisión a alto nivel de su proceso de operación para evaluar las capacidades de su control interno para detectar situaciones de riesgo. El propósito de una revisión a alto nivel es buscar "alertas rojas" que puedan indicar que una revisión más detallada podría descubrir oportunidades para reducir fallas de operación.

Discutimos su reciente decisión de descontinuar el desarrollo de la nueva aplicación “Windows - Access”. Al revisar la razonabilidad de los planes registrados para contingencias dedicaremos especial atención a este aspecto.

Finalmente, usted expresó inquietud sobre el tiempo requerido para verificar el funcionamiento de su super-dispositivo Y2K. Nuestro análisis ha indicado que, al modificar el tiempo en un 10% (apenas por encima del promedio en la industria), la compañía podría ahorrar aproximadamente Q1.5 millones. Obviamente, si una mejoría de 10% puede resultar en un ahorro de Q1.5 millones, una reingeniería para reducir dramáticamente el tiempo tendría mayor efecto. Durante nuestra excursión por la sección de procesamiento de datos, la semana pasada se me ocurrieron algunas ideas que deseo discutir con usted. La semana entrante me comunicaré con usted sobre esto.

Oportunidad de nuestros servicios:

Usted manifestó que le gustaría tener nuestro informe sobre los estados financieros no más tarde del 22 de febrero de 200y, para facilitar la refinanciación planeada de la deuda a principios 200x. Hemos diseñado nuestro calendario, como se indica en la documentación adjunta, teniendo en cuenta nuestro compromiso de cumplir con tal fecha límite. Además, en la misma fecha esperamos entregar:

- Recomendaciones para mejorar las políticas y procedimientos operativos y/o sistemas contables y controles internos que podamos identificar en el curso de nuestra auditoria.

- Resúmenes sobre asuntos de contabilidad y auditoria, y diferencias de auditoria no ajustadas que encontremos durante la auditoria

- Borradores de las declaraciones de impuestos para el 200x

- Carta sobre el cumplimiento con las cláusulas específicas de su convenio de préstamo.

Esperamos poder entregarle todos los documentos antes mencionados el 22 de febrero del 200y. En caso de surgir circunstancias inesperadas que nos impidan hacerlo, le comunicaremos oportunamente. Naturalmente, nuestra capacidad para cumplir con el calendario establecido depende de la ayuda que recibamos de su organización como lo indicamos anteriormente.

Una vez más deseo agradecer a usted por el tiempo dedicado a nuestro proceso de planeación. Su participación contribuirá para asegurar que la auditoria logre nuestro mutuo objetivo de agregar valor para Distribuidora de Repuestos, S. A.

Atentamente,

Mario Saucedo
Auditor

* * * * *

5.2 Conocimiento del Cliente

Al realizar el trabajo de auditoria de estados financieros, se debe obtener suficiente conocimiento del negocio para que le sea posible identificar y comprender los eventos, transacciones y prácticas que, a su juicio, puedan tener un efecto importante sobre los estados financieros o en el examen y dictamen de la auditoria. Dicho conocimiento es usado para evaluar los riesgos inherentes y de control y al determinar la naturaleza, oportunidad y alcance de los procedimientos de auditoria.

Se deberá obtener conocimiento preliminar de la Industria, los dueños, la administración y operaciones de la entidad que auditará, y considerar si puede obtener un nivel de conocimiento del negocio adecuado para desempeñar la auditoria, para tal propósito deberá considerarse los requerimientos de información del inciso 5.1 Planeación de la Auditoria – Introducción; y plasmarlos en memorandos que se adjuntan a los papeles de trabajo de auditoria.

5.3 Evaluación de la Estructura de Control Interno

EVALUACIÓN DEL AMBIENTE DE CONTROL:

El ambiente de control de la ***Distribuidora de Repuestos, S. A., al 31 de diciembre del 200x***; refleja tres elementos distintos: La conciencia de control de la gerencia y su estilo operativo; los mecanismos de control de la gerencia, y otras influencias sobre la gerencia. La gerencia manifiesta su conciencia de control en parte, estableciendo ciertos mecanismos de control generales y ejercitando la disciplina necesaria que produzca que los mecanismos funcionen en forma efectiva. Una respuesta NO a cualquiera de las siguientes preguntas no indica necesariamente una deficiencia en el ambiente de control. Sin embargo, las respuestas NO son consideradas cuando evaluamos el impacto, si lo hubiere, en nuestra evaluación de riesgo. Este formulario provee elementos para determinar la evaluación de riesgo en grupos de cuentas en el formulario Evaluación del riesgo en cuentas y grupos de cuentas.

No.	**Pregunta sobre control**	***SI***	***NO***
1.	¿Muestra el dueño o gerente una evidente conciencia de control?	***X***	
2.	¿Están el dueño o gerente activa y efectivamente involucrados en las operaciones del negocio?	***X***	
3.	¿Le dan consideración apropiada a los riesgos del negocio? (asuntos operacionales, financieros, ambientales, etc.)	***X***	
4.	La filosofía de la dirección sobre información financiera puede describirse mejor como (indique los que aplican): . Maximizar ganancias . Crecimiento uniforme de los ingresos . Logro de presupuestos/metas . Minimizar la renta gravable . Ningún sesgo en particular . Otro:_____	***X***	
5.	¿La dirección ha establecido un ambiente de control que puede afectar los estimados contables u otras decisiones?		***X***
6.	¿Están segregadas las cuentas personales y transacciones del dueño o gerente de aquellas del negocio?	***X***	
7.	¿Las políticas y acciones gerenciales estimulan a los empleados a mantener éticas personales y adhesión a los controles en el logro de metas financieras y operacionales? (¿ofertas y énfasis de incentivos financieros son apropiados, la presión que se ejerce o se percibe para que se violen preceptos de ética son evitados?)	***X***	
8.	¿Hay una junta directiva que vigila activamente el proceso de información financiera y los controles internos de la compañía?	***X***	
9.	¿Le ha dado la gerencia consideración adecuada a nuestras anteriores recomendaciones en asuntos concernientes a controles y asuntos importantes de contabilidad?	***X***	
10.	¿Ha habido influencias externas (autoridades regulatorias, oficiales de crédito bancario, etc.) que puedan traer como resultado que el cliente cambie o modifique su contabilidad normal y sus políticas de informes?		***X***
11.	¿La estructura de informática es relativamente sencilla (el cliente no usa		

	mainframes, redes complejas o mini computadoras sofisticadas tales como IBM/400 o HP/3000)?	***X***
	Identifique la marca y modelo del computador usado: (incluya anexo)	***AS400***
	Si no, considere si procedimientos adicionales son necesarios para obtener un entendimiento apropiado del Impacto del procesamiento de data en el ambiente de control.	***X***
12.	Las aplicaciones de software son primariamente:	
	• Enlatados de distribución general. Identifique el software usado:	
	• Enlatado de distribución general modificado para alcanzar las necesidades del cliente.	***X ORACLE***
	• Software hecho a la medida desarrollado por un programador bajo contrato.	
	• Programas desarrollados internamente y/o templates (disquetes de programas) usados con software de hojas de cálculo estándares.	
	• Variantes por aplicaciones (explique brevemente en anexo).	
13.	¿El dueño o gerente ha pensado y desarrollado sistemas de información contingentes adecuados para asegurarse de la continuación de las operaciones en caso de un desastre?	***X***
14.	¿La dirección ha establecido procedimientos de back-up y recuperación para programas y archivos?	***X***
15.	¿El dueño o gerente ha considerado y desarrollado medios apropiados para autorizar transacciones, incluyendo sistemas para prevenir cambios no autorizados a los archivos y programas?	***X***
16.	La segregación de funciones es suficiente, dado el tamaño y complejidad de la organización y el involucramiento del dueño o gerente, para impedir funciones incompatibles con:	
	• ¿La función de contabilidad?	***X***
	• ¿Las funciones de las operaciones de computadora y programación?	***X***
17.	¿Se preparan estados financieros a intervalos frecuentes?	***X***
18.	¿El dueño o gerente maneja estados financieros internos rutinariamente (estados financieros mensuales)?	***X***
19.	¿El dueño o gerente o alguien independiente de las funciones contables analizan y reconcilia cuentas significativas de forma oportuna?	***X***
20.	Si la compañía es una subsidiaria, división o sucursal, la casa matriz ejerce control efectivo (requisitos de información financiera estándares, revisión de resultados reportados, visitas de auditores internos)	***X***
21.	¿Cuando se emplea personal clave, se revisan sus antecedentes, y los resultados de estas investigaciones son considerados adecuadamente por el dueño o gerente?	***X***
22.	¿Los antecedentes y experiencia del personal del cliente aparentan ser las suficientes para el nivel de responsabilidad asignado?	***X***

Comentarios sobre elementos significativos y conclusiones sobre la efectividad del ambiente de control general:

En general evaluamos el control interno de la compañía como efectivo.

RESUMEN DE SISTEMAS DE INFORMACIÓN

Distribuidora de Repuestos, S. A.
Al 31 de diciembre del 200x

A continuación se acompaña una relación de preguntas que deben ser consideradas por el Auditor SIC, para lograr los objetivos establecidos, al hacer las indagaciones con el responsable individual del Cliente para Evaluación del Ambiente de Sistemas de Información Computarizada. Este cuestionario, puede entregarse al Cliente con anticipación a la reunión para discutir los asuntos en mención. El entregar el cuestionario por anticipado al cliente le permite prepararse apropiadamente para la reunión y que el cuestionario contestado se use como esbozo de la discusión. Solicitarle al Cliente que proporcione respuestas por escrito a estas preguntas.

Resumen de Sistemas de Información

1- Favor de proporcionar la información correspondiente a cada una de las aplicaciones contables importantes que se listen en el cuadro.

Descripción del Hardware (fabricante y Modelo) señalando con una marca las aplicaciones en que se utiliza.

Nombre de las aplicaciones:	**IBM AS/400 B60**	**Señalar número de localidades en que se efectúa el proceso:**	**Si se procesan transacciones de acceso remoto, indicar: D-Dial up R-RJE**	**Describir la configuración de micros, si procede: S-"Stand-alone" N-"Network con micros" L-"Linked o conectada con Mainframe o Mini".**
Inventarios / Costo de ventas	***X***	***1***	***N/a***	***Ninguna***
Compras / Cuentas por Pagar	***X***	***1***	***N/a***	***Ninguna***
Ventas / Cuentas por Cobrar	***X***	***1***	***N/a***	***Ninguna***
Mayor General	***X***	***1***	***N/a***	***Ninguna***
Entradas a Caja	***X***	***1***	***N/a***	***Ninguna***
Nóminas	***X***	***1***	***N/a***	***Ninguna***
Sistemas de Responsabilidades Departamentales	***X***	***1***	***N/a***	***Ninguna***
Orden de compra por Lote Económico	***X***	***1***	***N/a***	***Ninguna***

Nombre de las aplicaciones:	**Software que se utiliza en cada aplicación:**	**Nombre y versión de software comprado (cuando aplique)**	**Fecha de último cambio mayor (*)**	**En su caso, fecha de cambios mayores futuros, en su caso.**

1. **Desarrollado.**
2. **Comprado, no modificado.**
3. **Comprado, adaptado.**
4. **Centro de servicio**

Inventarios / Costo de ventas	***3***	***MAPICS V1.0***	***8/200w***	***Ninguna***
Compras / Cuentas por Pagar	***1***		***8/200w***	***Ninguna***
Ventas / Cuentas por Cobrar	***1***		***8/200w***	***Ninguna***
Mayor General	***3***	***MAPICS V1.0***	***8/200w***	***Ninguna***
Entradas a Caja	***2***	***MAS 90***	***1/200w (3)***	***Ninguna***
Nóminas	***1***		***8/200w***	***Ninguna***
Sistemas de Responsabilidades Departamentales	***3***	***SUN TECH V4.0***	***9/200v ((2)***	***Ninguna***
Orden de compra por Lote Económico	***2***	***MAPICS V1.0***	***1/200w (1)***	***Ninguna***

2. Indicar los nombres de los programas operativos de sistemas que utilizan en cada equipo:

Indicar el tipo de hardware (fabricante modelo) de la pregunta 1.

	AS /400 B60	**WINDOWS NT**
Sistema Operativo	OS/400 R.21	Windows NT 4.0
Control de Accesos	OS/400	Windows NT 4.0
Compiladores	RPG III, COBOL/400	Windows NT 4.0
Sistema Administrador de Programas	OS/400	Windows NT 4.0
Sistema Administrador de Bases de Datos	OS/400	Windows NT 4.0
Soporte para Comunicaciones de Datos	OS/400	Windows NT 4.0
Sistema Interactivo de Programación	SEU	Windows NT 4.0
Otros: Utilería	DFU, QUERY 400	
	Apoyo a PCS	Windows NT 4.0

(1) En enero de 200W se instaló un sistema de pedidos por Lote económico (EOQ).

(2) En septiembre de 200V se compró paquete de sistema de Responsabilidades Departamentales que es una aplicación de presupuestos que utiliza la dirección para analizar los resultados presupuestados con los reales.

(3) En diciembre de 200V se instaló una red local Windows NT para manejar las entradas de Efectivo y la facturación de Distribuidora de Repuestos, S.A. esta red se puso en operación hasta el 1 de enero de 200W.

Las respuestas a las preguntas siguientes se considerarán aplicables a todas las aplicaciones listadas en la Pregunta 1. Si las respuestas varían para algunas aplicaciones dentro de una misma aplicación, favor de llenar otro juego con las preguntas 3 a 15, o describir brevemente las diferencias en el espacio de la Pregunta 16.

Conciencia de Control de la Dirección y Estilo de Operación

		Si	No
3.	¿Está en vigor un plan de contingencias?	**X**	
	¿En caso afirmativo, cuando se actualizo? __30/08/200w		
	¿Se probó?	**X**	
4.	¿Se obtienen copias de respaldo regularmente de los programas de las aplicaciones y los archivos de datos?	**X**	

Mecanismos de Control de la Dirección

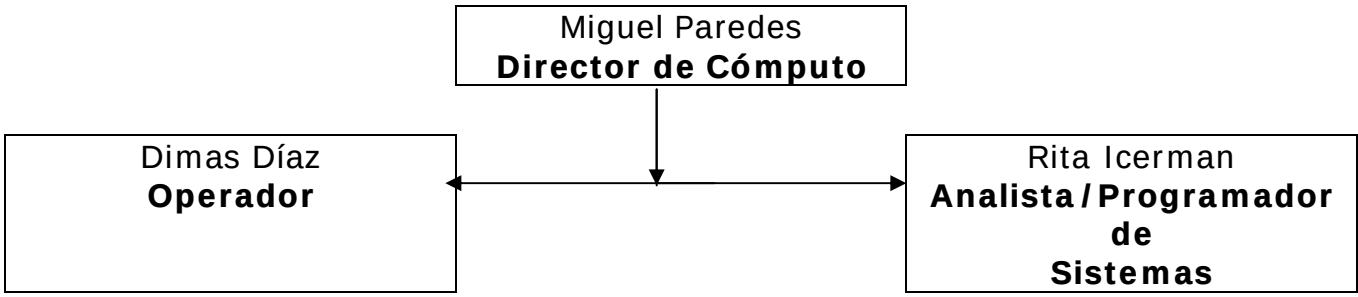
5. Adjuntar un organigrama del departamento de Sistemas de Información:

Describir brevemente los aspectos de segregación de labores relativos a sistemas de información que puedan impactar nuestra evaluación general del entorno de control o nuestra comprensión posterior de las fuentes de información. Estos aspectos pueden referirse a las relaciones y funciones existentes dentro del departamento de sistemas de información (Por ejemplo: programación, revisión y supervisión, operación de sistemas, entradas a aplicaciones, ejecución de programas).

El departamento de cómputo consiste del Director de cómputo, un operador y un programador/analista. Ocasionalmente, para proyectos específicos, se contratan programadores o consultores externos. Tanto el Programador/analista como el Operador reportan al Director de Computo, quien a su vez, reporta al Director General. Nuestra experiencia con el cliente indica que cómputo y los usuarios han establecido líneas de comunicación bien definidas y que los usuarios asumen la responsabilidad por sus aplicaciones.

Distribuidora de Repuestos, S. A.,
al 31 de diciembre del 200x

Organigrama – Departamento de Sistemas de Información



		Si	No
6.	¿Se respetan en el departamento de sistemas de información las normas y procedimientos predefinidos sobre recursos humanos (Por ejemplo: contratación, adiestramiento, evaluación, promoción)?	X	
7.	¿Se asegura la dirección financiera y vigila la participación de los usuarios en el desarrollo de programas, incluyendo el diseño de controles y pruebas de control interno?	X	
8.	En cuanto a la implementación y modificación de programas de computación, tanto comprados como desarrollados internamente, se cuenta con responsabilidades claramente definidas (para usuarios y personal de sistemas de información) sobre:	X	
	• ¿Pruebas de programas?	X	
	• ¿Documentación de programas?	X	
	• ¿Aprobación de programas?		
9.	¿Existe una estructura formal para asignar la propiedad de la información, incluyendo autorización para iniciar y/o modificar transacciones?	X	
10.	Se utilizan programas de seguridad, de sistemas de operación, y/o de aplicaciones para controlar el acceso, tanto centralizado como descentralizado a:		
	• Información	X	
	• ¿Funciones de los programas (Por ejemplo: ejecutar, actualizar, modificar parámetros, leer únicamente)?	X	
11.	¿Existe la función correspondiente al oficial de seguridad (auditor interno) para vigilar las actividades de procesamiento de sistemas de información?		X
12.	¿Teniendo presente la naturaleza del negocio del cliente, es razonable la seguridad física que existe en el área de computación, en las terminales (en el departamento de sistemas de información y usuarios) sobre las cintas, disco,	X	

etc.?

13. Existen políticas y procedimientos que aseguren que los programas importantes:

    - ¿Utilizan la versión apropiada de archivo de información y programas? **X**

    - ¿En el orden cronológico apropiado? **X**

14. ¿Cuando hay desviaciones importantes en el procesamiento, se determinan e investigan? **X**

Otras influencias sobre la Dirección

15. ¿Participa el consejo de directores, el comité de auditoria, etc., en el seguimiento de los proyectos de sistemas de información y en la asignación de prioridades de inversión? **X**

Descripción de las diferencias

16. Respecto de las preguntas 3 a 15, explíquense a continuación las diferencias importantes entre las aplicaciones, o dentro de las aplicaciones listadas en la pregunta 1.

Pregunta 8.- *por la naturaleza crítica del sistema administrador de inventarios, las modificaciones a los programas de este sistema se prueban formalmente y se documentan por el Departamento de Cómputo y el usuario.*
En 200w se ha formalizado el proceso de probar y documentar los cambios, conjuntamente por Cómputo y el usuario.
Pregunta 9.- *La dirección autoriza las transacciones para todas las aplicaciones pero no hay un método formal para asignar la propiedad de la información.*

5.4 Conocer el Proceso Contable y los Ciclos de Negocios

FORMULARIO DE ANALISIS DE CONTROL DE LAS APLICACIONES

Se adjunta el formulario de análisis de control sobre las aplicaciones más importantes de Distribuidora de Repuestos, S.A. Se refleja la información incluida en el Formulario de Documentación de Sistemas de Información Sistematizada, que incluye nuestra evaluación preliminar de controles para cada error potencial. Esta información se utilizará para desarrollar el Plan de Enfoque de Auditoria sobre las diferentes aplicaciones seleccionadas.

Análisis de Control:
Distribuidora de Repuestos, S.A.
Período cubierto por la evaluación: al *31 de diciembre del 200x*
Cuentas que afecta la aplicación: Inventarios / Costo de ventas

Errores potenciales / Que puede fallar	Procedimientos de control del cliente	Quien los aplica	Comentarios Evaluación preliminar
Todas las transacciones que deben contabilizarse se contabilizan (Integridad)			
a) el archivo de existencias no se actualiza en cuanto a las cantidades recibidas.	*Cuando los empleados del almacén actualizan las recepciones de mercancías, verifican que estén completas las existencias.*	*Valida el computador*	*Confiable*
b) no se procesan los recibos de existencias en cuanto a volúmenes realmente recibidos.	*Antes que el personal del almacén registren el ingreso, verifican que concilie con lo recibido físicamente.*	*Computador*	*Confiable*
c) el archivo diario de órdenes de compra no incluye todas las requisiciones según el archivo de existencias recibidas.	*El computador compara el correlativo de orden de compra y coteja con la recepción del almacén los recibos de existencias en base a codificación de producto.*	*Computador*	*Confiable*
2. Todas las transacciones contabilizadas son reales. (Validez)			
a) se procesan	*Para registrar y actualizar*	*Encargado*	*Confiable*

las órdenes de compra y se actualiza el archivo de diario de existencias por volúmenes de mercancías no recibidas.	*el archivo de existencias, el encargado del almacén debe revisar que se ha recibido todo el producto y coteja la factura del proveedor con la existencia recibida.*	*del almacén*	
b) pueden hacerse recepciones a proveedores inválidos.	*Previo a actualizar el archivo de existencias, se verifica el código de proveedor en las órdenes de compra.*	*Computador*	*Confiable*

3. Todas las transacciones contabilizadas se registran correctamente. (Registro)

a) se registran incorrectamente las transacciones diarias de recepción de existencias.	*Toda la valuación la realiza el computador, con base en el archivo maestro de existencias.*	*Computador*	*Confiable*
b) las sumas del archivo de recepción de compra diaria se vacían incorrectamente al mayor general.	*Los datos del archivo de recepción de compras, se validan antes de trasladar al registro contable en el mayor general.*	*Computador*	*Confiable*

4. Todas las transacciones se contabilizan en periodo contable a que corresponden. (Corte)

a) las compras se registran en un período posterior al de recibo.	*Al recibir la mercancía en el almacén, el computador requiere la fecha de recepción y valida con el sistema.*	*Computador*	*Confiable*
b) las existencias se registran antes de que las mercancías se reciban.	*Antes que el personal del almacén cargue la mercancía recibida el computador verifica la orden de compra.*	*Computador*	*Confiable*

5. Todas las transacciones contabilizadas están valuadas apropiadamente. (Valuación)

a) el procesa-miento de ingresos diario de existencias no realiza valuación (por ejemplo: volumen x precio) correctamente.	*Toda la valuación la realiza el computador automáticamente con base en el archivo maestro de existencias.*	*Computador*	*Confiable*
b) el archivo maestro de existencias está incorrecto.	*Mensualmente se compara el "informe de modificaciones en archivo maestro de existencias" generado por el computador con los formularios "modificaciones de aplicación", se investigan las discrepancias.*	*Ayudante del encargado de almacén*	*Confiable*
c) los volúmenes que anota el empleado en la boleta de recepción de mercancías o la cantidad que se introduce al archivo de existencias es incorrecta.	*Antes de que el personal del almacén registre las mercancías recibidas o entregadas, se emite una boleta de recepción o requisición, la cual se valida a través del computador.*	*Computador*	*Confiable*

6. Todas las transacciones contabilizadas están clasificadas apropiadamente. (Presentación)

a) las existencias se cargan al código de cuenta incorrecto.	*Previo a entregar o recibir mercancías, se registran los datos en el computador, el cual valida, para generar la boleta correspondiente.*	*Computador*	*Confiable*
b) las requisiciones se registran en	*Previo a entregar o recibir mercancías, se registran los datos en el computador, el*	*Computador*	*Confiable*

clasificaciones incorrectas del mayor general (por ejemplo: materia se registra en producto terminado?).	*cual valida, para generar la boleta correspondiente.*

Análisis de Control:
Distribuidora de Repuestos, S.A.
Período cubierto por la evaluación: al *31 de diciembre del 200w*
Cuentas que afecta la aplicación: Ventas / Cuentas por cobrar

Errores potenciales / Que puede fallar	**Procedimientos de control del cliente**	**Quien los aplica**	**Comentarios Evaluación preliminar**
1. Todas las transacciones que deben contabilizarse se contabilizan. (Integridad)			
a) el archivo de pedidos no se actualiza en cuanto a las cantidades embarcadas.	*Cuando el encargado de almacén actualiza la salida/pedido, automáticamente se modifica el estatus que guarda el pedido en el computador*	*Computador*	*Confiable*
b) no se procesan los embarques en cuanto a volúmenes realmente embarcados.	*Antes de que el encargado de almacén cargue la mercancía para embarque, se revisa y aprueba los documentos de embarque.*	*Supervisor de Almacén*	*Confiable*
c) el archivo diario de facturación no incluye todos los pedidos que se embarcaron según el archivo de pedidos.	*El computador compara volumen embarcado en relación al archivo de pedidos y las cantidades facturadas, las diferencias se investigan a través del informe diario de ventas.*	*Computador /* Contabilidad	*Confiable*
2. Todas las transacciones contabilizadas son reales. (validez)			
a) se procesan las notas de embarque y se actualiza el archivo de diario de facturas por volúmenes de mercancías no embarcadas.	*Se generan estados de cuenta mensuales que se envían a los clientes para confirmar el monto de la deuda.*	*Computador*	*Confiable*
b) pueden hacerse ventas a compradores inválidos.	*Antes de incorporar nuevo comprador, se aplica política de verificación de crédito.*	*Créditos*	*Confiable*
3. Todas las transacciones contabilizadas se registran correctamente. (Registro)			
a) se registran	*El encargado de cuentas por*	*Cartera*	*Confiable*

incorrectamente las transacciones diarias de facturación.	*cobrar concilia mensualmente el análisis de antigüedad de cuentas a cobrar con los saldos del mayor, diferencias se investigan.*		
b) las sumas del archivo de facturación diaria se vacían incorrectamente al mayor general.	*El computador verifica la conciliación de los datos de facturación antes de postear al mayor general. Cualquier inconsistencia se investiga*	*Computador /* Contabilidad	*Confiable*

4. Todas las transacciones se contabilizan en periodo contable a que corresponden. (Corte)

a) las ventas se registran en un período posterior al embarque.	*La fecha del computador se utiliza para asegurar el adecuado registro en el período al que corresponde.*	*Computador*	*Confiable*
b) las ventas se registran antes de que las mercancías se embarquen.	*Antes que se registre la entrega de mercancías en el almacén, se verifica la fecha de despacho en la boleta de embarque.*	*Computador*	*Confiable*

5. Todas las transacciones contabilizadas están valuadas apropiadamente. (Valuación)

a) el procesamiento de facturación diaria no realiza valuación (por ejemplo: volumen x precio) correctamente.	*En el programa del computador, se valúa las ventas y la facturación realizada. Verificando cantidades, precios y totales.*	*Computador*	*Confiable*
b) el archivo maestro de ventas está incorrecto.	*Automáticamente el programa verifica el "informe de modificaciones al archivo maestro de ventas", contra la "bitácora de cambios a programas", cualquier cambio se reporta e investiga.*	*Computador*	*Confiable*
c) los volúmenes que anota el empleado en la boleta de embarque o la cantidad que se introduce al archivo de pedidos es incorrecta.	*Antes que se cargue la mercancía en el almacén, se emite boleta de embarque y se aprueba por supervisor.*	*Computador /* Supervisor	*Confiable*

6. Todas las transacciones contabilizadas están clasificadas apropiadamente. (Presentación)

a) las ventas se cargan a la cuenta de un comprador incorrecto.	*A medida que se introduce la información del pedido, el programa verifica automáticamente los datos.*	*Computador*	*Confiable*
b) las ventas se registran en clasificaciones incorrectas del mayor (por ejemplo: IVA, cuentas por cobrar a relacionadas, ventas brutas, cuentas a cobrar, división, tipo de producto.	*Las clasificaciones de mayor general están definidas en los parámetros de archivo maestro de ventas y se registran automáticamente, cualquier diferencia se valida y emite reporte de inconsistencias.*	*Computador*	*Confiable*

*** * * * ***

DOCUMENTACIÓN DE CONTROLES DE SISTEMAS DE INFORMACIÓN

Distribuidora de Repuestos, S.A.
Al 31 de diciembre de 200x

Políticas y Procedimientos sobre modificaciones a Programas

1. Describir las principales políticas y procedimientos sobre el desarrollo, compra y mantenimiento de programas. Cubrir la prueba, aprobación, implantación y documentación.
   Los factores que pueden ser relevantes incluyen:

   - Normas escritas actualizadas; planeación estratégica de la entidad/departamento; comité orientador de sistemas de información, etc.
   - Estructura general de la metodología para desarrollo de sistemas; cómo varían los procedimientos para adaptación, prueba e implantación de programas comprados; modificaciones mayores versus menores.
   - Uso de herramientas de desarrollo tales como prototipos, CASE, lenguajes de cuarta generación, etc.
   - Diseño de controles apropiados tales como controles computarizados y/o conciliaciones manuales, etc.
   - Personas, distintas a los programadores responsables que realizan las pruebas; naturaleza de las pruebas típicas (por ejemplo: paralelas, uso de archivos de prueba, recómputos manuales); retención de los resultados de las pruebas; cómo se asegura la dirección de que los archivos “vivos” no se corrompen por programas de prueba; etc.
   - Existencia y documentación de la aprobación formal e informal de modificaciones por parte de los usuarios, de la dirección de sistemas de información, y de otros (por ejemplo: auditoria interna, control de calidad).
   - Alcance típico de la documentación de sistemas.

Un formulario de solicitud (ver anexo 1), **que también se utiliza como formulario de seguimiento al proyecto**, se utiliza para iniciar todos los proyectos de desarrollo y mantenimiento de aplicaciones. El departamento usuario llena el formulario de solicitud y el jefe del departamento usuario lo aprueba. Los formularios de solicitud se entregan al Director de Cómputo quién asigna un número de proyecto a las solicitudes que han sido aceptadas con una estimación de menos de 100 horas de programador. Todas las solicitudes que requieren más de 100 horas de programador se envían al Comité de Sistemas de Computación para su aprobación. Si el Comité aprueba la solicitud, la firma y le asigna un número de proyecto. El Director de Cómputo indica en su registro si la solicitud fue aceptada o rechazada. El Director de Cómputo prepara un informe bimestral para el Comité de Sistemas de Información sobre el estado de los proyectos en proceso. Adicionalmente, el Director de Cómputo prepara un análisis mensual de las horas por proyecto.

El Director de Cómputo verifica el cumplimiento con los procedimientos de prueba, documentación, revisión y aprobación que se documentan mediante firma en el formulario de solicitud.

Para cada proyecto mayor, se asigna un representante del usuario con la responsabilidad de contactos diarios con el programador/analista o el Director de Cómputo. El representante del usuario reporta con regularidad al jefe de su departamento sobre el estado de avance del proyecto y los resultados obtenidos en las pruebas. Al terminarse los procedimientos de prueba, el jefe del departamento usuario firma el formulario de solicitud, que también se utiliza como una hoja de seguimiento al proyecto.

Si bien no existen procedimientos escritos para asegurar que las nuevas aplicaciones y las modificaciones a programas incluyen controles contables, durante la fase de análisis y diseño de nuevas aplicaciones o modificaciones a programas existentes hay una intervención cercana del departamento usuario. El representante del usuario se asegura de que se incorporan los controles necesarios en los nuevos sistemas y que se establecen los controles manuales necesarios para asegurar la integridad de los programas y los datos. También el programador / analista revisa el efecto de las modificaciones sobre las aplicaciones existentes.

El programador/analista es el responsable de los procedimientos de prueba y de datos de prueba. El diseño de la fase de prueba y sus resultados son objeto de revisión por el Director de Cómputo. **El Director de Cómputo documenta su aprobación en el formulario de solicitud**.

No hay normas establecidas para las pruebas sobre modificaciones a programas. No se requiere que los usuarios se involucren en la fase de prueba. La naturaleza y alcance de las pruebas (Por ejemplo: paralela, pruebas contra copias de datos vivos, recómputos manuales) varían según el tipo de modificación.

Normalmente no se guardan los datos de prueba y los resultados de las pruebas. Los programas nunca se someten a prueba con archivos vivos. Hay seguridad de esto por el acceso restringido a la biblioteca de producción y porque todas las pruebas se realizan en la biblioteca de pruebas.

Cuando el programa modificado está listo para prueba, el Director de Cómputo lo traslada de la biblioteca de desarrollo de pruebas del programador a la biblioteca de pruebas (TESTLIB). **Se requiere que el departamento usuario apruebe las pruebas si la modificación afecta a los listados de salida. Si se trata de mantenimiento menor en los programas, se notifica a los usuarios sobre la modificación para que, si lo consideran necesario, pasen revista a las pruebas. El formulario de solicitud debe ser aprobado por el departamento usuario. Si el departamento usuario decide no pasar revista a los resultados de la prueba para cambios menores a programas, de todas maneras se requiere su firma en el formulario de solicitud indicando que no pasaron revista a los resultados de las pruebas.**

El Director de Cómputo revisa el formulario de solicitud aprobado por los usuarios que indica que el jefe del departamento usuario considera que el programa está listo para su implantación. El Director de Cómputo confía en la revisión del departamento usuario y en los controles contables.

La utilería de programación que se utiliza en línea es SEU (Source Entry Utility). La SEU permite al programador/analista introducir y mantener las instrucciones fuente para las aplicaciones. El programador/analista no tiene acceso a las bibliotecas de programas de producción. Cuando se debe modificar un programa de producción, el Director de Cómputo copia el programa de la biblioteca de producción a la biblioteca de desarrollo del programador/analista (ELLELIB).

Los manuales de los usuarios incluyen especificaciones de la información de entrada e instrucciones a los usuarios. También incluyen procedimientos para corrección de errores tales como procedimientos para reintroducción de datos a los departamentos apropiados, procedimientos de conciliación, requerimientos de aprobaciones, distribución de los listados de salida y requerimientos para su retención, requerimientos para respaldos y descripción de los listados de salida.

Toda la documentación del programa está bajo la custodia del Director de Cómputo. El Director de Cómputo mantiene esta documentación en una bóveda a prueba de incendios en su oficina, excepto la que ha entregado al programador/analista para actualización.

El formulario de solicitud contiene espacios para firmas indicando las actualizaciones de la documentación apropiada. El programador/analista es responsable de preparar o actualizar la documentación El Director de Cómputo revisa la documentación antes de implementar ningún programa nuevo o modificado para asegurar que la documentación es adecuada.

En la medida que los procedimientos sean aplicables, los procedimientos de desarrollo son virtualmente los mismos para los programas desarrollados en casa, adaptación de programas comprados, e implantación de paquetes sin adaptación. No hay funciones otorgadas a auditoria interna, administración de bases de datos o de control/seguridad de calidad.

2. Describir cómo se envían los programas a producción.
   Los factores que pueden ser relevantes incluyen:

   - Que personas tienen el o los niveles de acceso necesarios para actualizar programas de producción.
   - Antes de entrar a producción, se revisan para constatar su aprobación apropiada.
   - Hay procedimientos para conciliaciones periódicas entre las modificaciones aprobadas y las modificaciones realizadas y su seguimiento.
   - La programación se realiza en etapas (Por ejemplo: hay bibliotecas o subdivisiones separadas para desarrollo, pruebas independientes y producción).
   - Hay procedimientos y controles sobre el código fuente en relación al código de ejecución.
   - Hay procedimientos para realizar las modificaciones a programas en un entorno de procesamiento descentralizado.

Las nuevas aplicaciones y las modificaciones importantes a aplicaciones existentes se someten a un período de prueba en que se corren en paralelo los sistemas antiguo y nuevo.

Los departamentos usuarios pueden involucrarse durante esta fase de prueba. Antes de iniciar la conversión, se diseña un plan de conversión. El plan de conversión incluye el adiestramiento y debe ser aprobado por el departamento usuario, por la Dirección de Cómputo, y por el Comité de Sistemas de Información.

El departamento usuario revisa las cifras de control de los campos clave y los recuentos de registros para asegurarse que el archivo de datos ha sido convertido completamente y correctamente. El Director del departamento usuario está obligado a firmar el formulario de solicitud para indicar su aprobación y aceptar el proyecto antes de la implantación de la aplicación modificada. El formulario de solicitud se entrega a continuación al Director de Cómputo.

En cuanto a mantenimiento de programas, los jefes de los departamentos usuarios **están obligados a firmar el formulario de solicitud para indicar su aceptación y para** revisar y someter a prueba los resultados que consideran necesarios según la naturaleza de la modificación del programa.

Al recibir el formulario, el Director de Cómputo revisa **y aprueba (inicialando el formulario de solicitud)**, todo el desarrollo y mantenimiento de programas antes de su implantación. **Esta revisión incluye lo siguiente:**

- **El código nuevo o modificado es adecuado;**
- **Las pruebas resultaron correctas;**
- **La documentación del programa está completa y actualizada;**
- **El departamento usuario hizo constar su aprobación en el formulario de solicitud.**

Si no descubre problemas, el Director de Cómputo traslada el programa fuente sea éste nuevo o modificado de la biblioteca de pruebas (TESTLIB) a producción y compila y edita el programa para enlace. En su expediente de perfil de usuarios traslada la propiedad, tanto del programa fuente como del programa objeto, y cambia la autorización de *USE del programador/analista.

Después de la instalación del programa nuevo o modificado, el Director de Cómputo **firma** el formulario de solicitud para indicar **su aprobación** y que el programa ha quedado implantado. Anota en el registro la fecha de traslado a producción. No se realiza ninguna conciliación formal entre el registro del Director de Cómputo y los programas en producción. El director de Cómputo está tranquilo en el sentido de que la revisión de su registro detectaría cualquier actividad inusual. La implantación de los programas que requieren más de 100 horas de programador se reportan en informes bimestrales al Comité de Sistemas de Información.

3. Describir los procedimientos y políticas sobre modificación a programas de producción en casos de emergencia.
   Los factores relevantes incluyen:

   - Alcance de los cambios de emergencia en aplicaciones significativas.
   - Cómo difieren los procedimientos de control sobre modificaciones a programas en comparación con los normales.
   - Requisitos de las aprobaciones verbales
   - Anotación en registro de las modificaciones de emergencia
   - Procedimientos para prueba y aprobación subsiguientes de las modificaciones.

Puesto que el cliente solamente trabaja un turno, cinco días a la semana, las modificaciones de emergencia son mínimas. Si debe hacerse una modificación de emergencia en ausencia del

Director de Cómputo, el operador debe obtener del Director General la contraseña del Director de Cómputo, antes de que el programa modificado pueda entrar a producción (el Director General mantiene en su caja fuerte, en un sobre cerrado, la copia en papel de la contraseña del Director de Cómputo, (QSECOFR).

Al regreso del Director de Cómputo, revisa la modificación al programa para asegurarse de que se probó y aprobó adecuadamente por el departamento usuario, y de que toda la documentación se actualizó.

La contraseña del QSECOFR se modifica tan pronto regresa el Director de Cómputo. Adicionalmente, el Director de Cómputo pasa revista al registro y examina los listados en busca de actividad inusual durante su ausencia.

Políticas y Procedimientos sobre acceso a Archivo de Datos

4. Describir la estructura general de la función de seguridad de datos.

Los factores que pueden ser relevantes incluyen:

- Estructura de la función independiente de seguridad de datos y/o de administradores descentralizados de seguridad.
- Políticas de comunicación y observancia de seguridad de información
- Nombre (y, en su caso, sistema operativo) de los programas de seguridad sobre acceso
- Características del sistema operativo específico y/o aplicaciones de seguridad en uso
- El efecto de sistemas integrados sobre la seguridad de la información
- El impacto sobre seguridad de la información del uso de productos de seguridad múltiple (Por ejemplo: programas de control de acceso, seguridad sobre programas de aplicación)
- Si es aplicable, los efectos de redes, acceso por MODEM, etc.

Se desarrolló durante el año una política escrita de seguridad. La política fue diseñada por el comité ejecutivo y se refiere a todos los aspectos de seguridad, incluyendo sobre sistemas de información. Se pidió a todo el personal que firmara una copia de la política en señal de haberla leído. Al ser contratados, los nuevos empleados deberán leer la política y firmarla en reconocimiento.

El Director de Cómputo realiza la función de seguridad de información y es responsable de mantener los perfiles de usuarios y las listas de autorizaciones. La identificación QSECOFR ID se utiliza solamente para el mantenimiento de seguridad y es la única ID, con las autorizaciones especiales de SECOFR o SECADM, que se necesitan para mostrar o actualizar los perfiles de usuarios. El Director de Cómputo también es el propietario de todas las bibliotecas de producción y de datos y, por lo tanto, la única persona que puede actualizar las listas de autorización para las bibliotecas de producción y de datos.

El acceso al sistema está controlado mediante perfiles de usuarios y contraseñas en el OS/400.
El acceso a las bibliotecas de programas de producción y a los datos está controlado mediante el uso de listas de autorización combinado con menús iniciales restrictivos y capacidades limitadas.

Cada persona que conecta una Terminal debe introducir su identificación ID (nombre en el perfil de usuario) y su contraseña. Las contraseñas no se proyectan en la Terminal y los usuarios las cambian cada 90 días. Las contraseñas del Director de Cómputo y del operador se modifican más frecuentemente – cuando menos cada 30 días.

Para mejorar la integridad de las contraseñas, Distribuidora de Repuestos, S. A., ha instalado un sistema de opciones que impiden caracteres repetidos en una contraseña y que obligan a que cada contraseña nueva contenga en cada posición un carácter diferente al de la contraseña anterior. En los perfiles de los usuarios se almacena información sobre cada uno de ellos, incluyendo contraseña, clase de usuario y autorizaciones especiales. De las cinco clases de usuarios que maneja el sistema, las tres que utiliza Distribuidora de Repuestos, S.A., se describen más adelante y corresponden a autorizaciones predefinidas en el nivel de Seguridad 30. Las autorizaciones especiales han sido otorgadas a medida que se han necesitado.

- **Oficial de seguridad** – esta clase permite a la persona acceso total a todos los recursos del sistema. Ello incluye la habilidad para cambiar, remover, mostrar o incorporar perfiles de usuarios (excepto contraseñas); otorgar los privilegios del oficial a otros usuarios; controlar la existencia y propiedad de los programas objeto; incorporar, eliminar y mantener listas de autorización para todos los programas objeto; cambiar el nivel de seguridad del sistema; realizar operaciones de almacenamiento y restitución para todos los recursos del sistema; realizar las funciones de revelación y modificación que permiten a un usuario mostrar y modificar datos; controlar la secuencia de salidas para todas las aplicaciones operadas en el sistema; detener subsistemas y almacenar información; y funciones de control sobre operaciones simultáneas en el sistema. Este nivel de autorización sólo se ha otorgado al Director de Cómputo.

- **Operador del sistema** – Las personas que pertenecen a esta clase pueden realizar operaciones de almacenaje y restitución en todos los recursos del sistema; controlar la secuencia de salidas del sistema y todas las aplicaciones que trabajan en el mismo; detener subsistemas; y almacenar en el sistema. Esta clase sólo ha sido asignada al operador.

- **Usuarios** – Estas personas no cuentan con ninguna autorización especial. Los usuarios y el programador/analista pertenecen a esta clase. Todos los usuarios y el programador/analista tienen asignados menús iniciales y programas iniciales. A todos los usuarios finales se les ha limitado su capacidad a *YES para evitar que puedan alterar el

programa inicial, la biblioteca actual, o el valor del programa “Attention-Key-Handling”. La autorización pública en todos los perfiles de usuarios se estableció como *EXCLUDE. Todos los usuarios tienen acceso solamente a un tipo de dispositivo para evitar que varios usuarios compartan un mismo perfil, y sólo pueden conectarse a terminales localizadas en su propio departamento.
Todas las contraseñas estándar que vinieron originalmente en el equipo IBM han sido modificadas. Se ha asignado QSECOFR al Director de Cómputo, y QSYSOPR al Operador. No se están usando QUSER ni QPGMR. En la caja fuerte de la oficina del Director General, en sobre cerrado, se encuentra una copia de las contraseñas correspondientes a las siguientes identificaciones: QSECOFR, QSRV, QSRVBAS, QPGMR, y QUSER. Con excepción de QSECOFR, estas identificaciones sólo pueden utilizarse por un representante de IBM o en caso de emergencia. Cada departamento en donde se encuentran usuarios cuenta, cuando menos, con un grupo de perfiles, y todos los usuarios últimos en cada departamento han sido asignados a su respectivo grupo. Se ha otorgado acceso de usuarios últimos a los perfiles de los grupos en lugar de a los perfiles de usuario individuales. Hasta ahora, no se ha utilizado la ADOPT AUTHORITY. No parece haber alguna razón para utilizarla en un futuro cercano.
La autorización para utilizar o tener acceso a las terminales en el almacén, departamento de nóminas y oficinas sucursales de ventas se ha restringido a los usuarios localizados en esas áreas. El sistema operativo niega el acceso a estas terminales a cualquier otro perfil de usuario. Sólo el Director de Cómputo puede cambiar las personas que utilizan estas terminales. El sistema operativo desconecta automáticamente las terminales que han estado inactivas por más de 15 minutos. La Terminal en el departamento de nóminas, dedicada a la aplicación de nóminas, está equipada con un sistema de cerradura mediante llave.
Solamente el Director de Cómputo puede modificar, incorporar o eliminar información en los perfiles de usuarios. El es el propietario de todos los archivos de producción de datos. Realizamos una gira del departamento de cómputo con el Director de Cómputo. El computador está colocado en una sala cerrada, con acceso solamente mediante tarjeta magnética. Los programadores no tienen acceso a la sala del computador. La consola del sistema está localizada dentro de la sala del computador y estaba bajo el control del operador. La cerradura del sistema estaba en la posición automática y la llave **no** estaba colocada en la cerradura. **La llave se encuentra en un cajón de la oficina del Director General.**

5. Describa la participación de los usuarios y del departamento de sistemas de información en la autorización de acceso a los programas y archivos de datos importantes, incluyendo cómo se incorporan, monitorean, modifican y eliminan autorizaciones de acceso.

   Los factores que pueden ser relevantes incluyen:

   - Quién mantiene los perfiles de usuarios
   - Aprobación y documentación requeridas para autorizaciones de acceso nuevas, modificadas o terminadas
   - Oportunidad con que se realizan las modificaciones y eliminaciones

- Conciencia de los usuarios y del personal de sistemas de información sobre las convenciones prudenciales de seguridad para prevención de riesgos
- Señalar si las autorizaciones de acceso se basan en el nivel de necesidades de acceso (Por ejemplo: lectura solamente, actualización, sólo ciertas aplicaciones del menú) en comparación con autorizaciones de acceso basadas en la naturaleza de las aplicaciones.
- En ambientes de bases de datos, describir el alcance del administrador de bases de datos

Se requiere aprobación escrita del jefe del departamento para los cambios en el alcance de las reglas de seguridad (es decir, los archivos y bibliotecas sujetos a control y las personas que requieren acceso a archivos y bibliotecas). El Director de Cómputo verifica la aprobación del jefe del departamento, aprueba/rechaza la solicitud, y efectúa el cambio. El perfil de usuario QSECOFR, que solamente utiliza el Director de Cómputo y solamente para funciones relativas a seguridad, es el único con autorización especial tanto para SECOFR como SECADM. En la oficina del Director General hay un sobre cerrado que contiene una copia de la contraseña del perfil de usuario QSECOFR. En la misma oficina del Director General también se mantiene en sobre cerrado la contraseña para herramientas de servicio dedicadas (DST-"dedicated service tools"), que normalmente sólo la utiliza el Director de Cómputo.
Semanalmente el departamento de recursos humanos entrega al Departamento de cómputo un informe listando las transferencias y bajas de empleados. Este informe resume a todos los empleados transferidos y dados de baja. Las identificaciones de los empleados de baja se eliminan. El director de cómputo imprime el perfil de los usuarios y a continuación los elimina del sistema. **El director de cómputo sella el perfil del usuario con la palabra "eliminado", lo iníciala y lo fecha, y lo archiva con el informe de bajas. También se imprimen los perfiles de usuarios de empleados transferidos.**

Los jefes del nuevo departamento y del anterior departamento de usuarios revisan el perfil del empleado transferido y anotan los cambios necesarios, que son inicialados por los dos jefes. **El director de cómputo espera hasta una semana para recibir esta información. Si después de una semana no se recibe el perfil de usuario actualizado y firmado, se revoca la identificación del empleado y no puede reintroducirse hasta que se reciba el perfil.** **Cuando se ha recibido el nuevo perfil de usuario y se introduce el sistema, se firma la documentación y se archiva con las demás solicitudes de acceso de usuarios.** **Anualmente el director de cómputo realiza una auditoria de usuarios. Imprime los perfiles de los usuarios y los examina con los jefes de departamentos usuarios. Con base en este examen se hacen cambios a los perfiles que lo ameritan. El director de cómputo vigila que se le regresen todos los perfiles de usuario provenientes de la auditoria. Los listados de la auditoria de usuarios se mantienen archivados por un año.**

6. Respecto de contraseñas (y otros códigos de seguridad) utilizados para tener acceso a archivos de datos o programas:

	Usar una columna para cada programa, paquete o sistema listado en el Resumen de Sistemas de Información, que permite o restringe el acceso a archivos de datos o programas. **OS/400**	**VALORES EN EL SISTEMA**
a) ¿Existe una norma formal de contraseñas en la organización?	SI	
b) ¿Firman los usuarios (incluyendo personal de sistemas de información) convenios de seguridad sobre la confidencialidad de las contraseñas?	NO	
c) ¿Con qué frecuencia se modifican las contraseñas?	30 días	QPWDEXPITV=30
d) ¿Pueden elegir los usuarios sus contraseñas libremente?	SI	QPWDMAXLEN=10 QPWDMINLEN=5 QPWDVLDPGM=*NONE
e) ¿Se toman medidas para asegurar que las contraseñas son aleatorias (y no valores sistemáticos como fecha de nacimiento, nombres de familiares, iniciales, etc.) y para evitar el uso de la misma contraseña repetidamente?	**SI**	**QPWDRQDDIF=1** QPWDLMTAJC=0 QPWDLMTCHR=0 QPWDLMTREP=0 QPWDPOSDIF=0
f) ¿Se requieren contraseñas adicionales para tener acceso a información sensitiva confidencial?	NO	
g) ¿Se utilizan técnicas que impiden la proyección de contraseñas y de mensajes importantes en las terminales y en los listados?	SI	

h) ¿Después de un cierto número de intentos de acceso fallidos, se suspenden las identificaciones de los usuarios respectivos?	**SI**	**QMAXSIGN=3** **QMAXSGNACN=2**
En caso afirmativo, indicar el número	3	
i) ¿Después de un cierto período de inactividad, se desactivan las terminales?	SI	QINACTITV=15 QINACTMSGQ=*ENDJOB
¿En caso afirmativo, indique el número de minutos de inactividad necesarios para que las terminales/programas queden desconectados automáticamente?	15 minutos	
j) ¿Para reactivar la identificación del usuario y/o la Terminal se requiere la intervención de otro personal de sistemas de información?	**SI (A)**	**QMAXSGNACN=2**
k) ¿está restringido el funcionamiento de ciertas terminales a determinadas funciones (por ejemplo: sólo las terminales del supervisor de nóminas pueden actualizar el archivo maestro de nóminas)?	SI	

(A) Sólo el director de cómputo puede reactivar las contraseñas de usuarios. Las terminales realmente no se desactivan, pero el usuario está obligado a un nuevo procedimiento de acceso.

Al estudiar el listado sobre valores del sistema, se debe haber determinado lo siguiente:

QINACTITV	QINACTITV es el número de minutos en que una tarea puede permanecer inactiva sin que se tome ninguna medida. El valor estándar es *NONE y el rango válido de minutos que puede especificarse es de 5 a 300. El valor presente de QINACTITV es de 15 minutos antes de que se tome la acción QINACTMSGQ.
QINACTMSGQ	Si una tarea permanece inactiva un número especificado de minutos (el número definido en QINACTITV) el sistema automáticamente toma acción con base en el valor asignado a QINACTIMSGQ. Al especificarse el valor *ENDOJOB, se cierra la tarea inactiva, las tareas secundarias y/o las tareas grupales.
QMAXSGNACN	Este valor define la acción que se ejercita cuando se acumula el número de intentos de acceso definido en QMAXIGN. El valor de “1” incapacita a la Terminal. El valor de “2” incapacita únicamente al perfil de usuario. El valor de “3” incapacita tanto al perfil del usuario como a la Terminal. El valor en vigor es “2” que incapacita sólo al perfil de usuario. (Esta opción es diferente a la del año precedente).
QMAXSIGN	Este valor define el número de intentos de acceso antes de que se ejercite la acción definida por QMAXSGNACN. El valor en vigor es “3” y por lo tanto, los usuarios tienen tres oportunidades de introducir una contraseña válida y su identificación antes de que esta última se incapacite. (Esta opción es diferente a la del año precedente).
QPWDEXPITV	Indica el número de días de validez de una contraseña. El rango de valores que puede especificarse es de 1 a 366. El valor estándar de *NOMAX indica que las contraseñas no tienen límite de expiración. El valor en vigor es de “30”. Por lo tanto, deben modificarse las contraseñas cada treinta días.
QPWDLMTAJC	El valor de “1” impide al usuario diseñar su contraseña con dígitos

	contiguos (0-9). El valor en vigor es de “0” que sí permite dígitos contiguos.
QPWDLMTCHR	Permite al cliente especificar hasta diez caracteres inválidos para utilizarse en contraseñas. El valor en vigor es *NONE. Por lo tanto, todos los caracteres son válidos en contraseñas.
QPWDLMTREP	El valor “1” impide que se repitan caracteres en una misma contraseña. El valor en vigor es “0” que permite la repetición de caracteres en contraseñas.
QPWDMAXLEN	El número máximo de caracteres que se permite en una contraseña. El valor en vigor es “10” por lo que las contraseñas pueden constar hasta de 10 caracteres.
QPWDMINLEN	Número mínimo de caracteres permitido en una contraseña. El valor en vigor es “5” por lo que las contraseñas deben contar cuando menos con 5 caracteres.
QPWDPOSDIF	El valor “1” requiere que cada carácter en la nueva contraseña sea distinto al carácter en la misma posición de la contraseña anterior. El valor en vigor “ 0 “especifica que esta restricción no está en vigor.
QPWDRQDDIF	El valor de “1” impide al usuario usar la misma contraseña antes de 32 cambios. El valor de “0” permite al usuario repetir una contraseña utilizada en el pasado. El valor en vigor es “1” por lo tanto, las contraseñas deben ser diferentes a la inmediata anterior. (Esta opción es diferente a la del año anterior).
QPWDVLDPGM	Este valor es el nombre del programa utilizado por el sistema para validar contraseñas nuevas. El valor en vigor es *NONE indica que la validación de contraseñas no está siendo utilizada.

Otros valores comunes que pueden detectarse en el sistema incluyen:

QAUDLVL	IBM tiene la opción de un Diario de Auditoria que puede activarse asignando valor a este comando. En el Diario de Auditoria puede almacenarse cuatro tipos de eventos: fallas en la autorización (*AUTFAIL), reinicio de operaciones (*SAVRST); eliminación de operaciones (*DELETE); funciones relativas a seguridad (*SECURITY) y fallas en el programa (*PGMFAIL). Para que puedan almacenarse en el Diario de Auditoria, cada categoría de eventos debe activarse por separado. El valor en vigor es *SECURITY y *SAVRST.
QCRTAUT	Si el acceso no se ha otorgado o impedido explícitamente, el nivel estándar de autoridad es “Public Authority”. QCRTAUT permite establecer un nivel estándar de autoridad para todo el sistema. El valor en vigor de QCRTAUT está establecido en *EXCLUDE. Por lo tanto, a menos que se otorgue poder específicamente, el acceso queda impedido.
QLMTDEVSSN	El sistema puede impedir el acceso simultáneo de varias terminales. El valor estándar es de “0”, que sí permite sesiones simultáneas. El valor de “1” limita a un dispositivo por sesión únicamente. El valor en vigor es de “1” por lo que los usuarios sólo pueden tener acceso de un dispositivo a la vez.
QLMTSECOFR	Se corre mediante el valor de “1”, se puede impedir a los usuarios privilegiados que tengan acceso de terminales distintas a las especificadas en sus perfiles de usuarios. El valor de “0” permite a los usuarios acceso de cualquier dispositivo. Puesto que el valor en vigor es de “0”, los usuarios privilegiados no tienen acceso restringido en cuanto a terminales.
QMODEL	Indica el número de modelo de la máquina para la cual se genera el Informe de Valores en el Sistema.
QPWDRQDDGT	El valor de “1” requiere que todas las contraseñas incluyan cuando menos un carácter numérico. El valor en vigor es “0” no requiere ningún carácter numérico.

QSECURITY — Este valor indica el nivel de seguridad en vigor (10, 20, 30, 40, 50). El valor en vigor es “30” indica que las instalación trabaja a un nivel de seguridad de 30, cuáles identificaciones y contraseñas se requieren y qué accesos a programas y archivos se verifican contra el perfil de los usuarios.

7. Se reconoce que pueden presentarse algunas desviaciones (ver pregunta 8). Para cada una de las aplicaciones listadas en la pregunta 1 del Resumen de Sistemas de Información, indicar con una (X) en los siguientes cuadros, los niveles de acceso permitido a programas y archivos de datos importantes.

	Programas de Producción			**Archivos Maestros Relevantes**		**Archivos de Transacciones Relevantes**	
	Ejecución	**Actualización**	**Lectura**	**Actualización**	**Lectura**	**Actualización**	**Lectura**
Programadores (A)							
Apoyo Técnico N/A							
Operaciones	***X***	***X***	***X***	***X***	***X***	***X***	***X***
Todos los usuarios							
Usuarios seleccionados con base en sus necesidades	***X(B)***			***X(B)***	***X(B)***	***X(B)***	***X(B)***
Otros:							
Director de cómputo	***X***	***X***	***X***	***X***	***X***	***X***	***X***

8. Describir brevemente desviaciones importantes de la información proporcionada en la tabla anterior, en cuanto a su efecto sobre aplicaciones relevantes.

(A) el programador no tiene acceso a las bibliotecas de producción.
(B) Las funciones están restringidas a través de menús iniciales y capacidades limitadas.

9. Describir los procedimientos de monitoreo de violaciones al acceso.
Los factores a considera pueden incluir:

- Revisiones centralizadas y/o descentralizadas, más seguimiento de las anotaciones en las bitácoras de actividades

- Uso de la función “iaudit” en los programas de control de acceso para monitorear las actividades de determinadas personas, terminales, programas, archivos de datos, etc.
- Registro por el sistema de intentos de acceso no autorizados y su investigación
- Suspensión automática de las identificaciones de usuarios y/o de terminales después de un determinado número de intentos de acceso fallidos, así como los relativos procedimientos de re-inicialización
- Documentación adecuada.

.

El sistema almacena las violaciones de acceso en el diario histórico por procedimiento estándar, y por definición en el diario de auditoria.

También se almacenan en el diario de auditoria las modificaciones en las funciones relacionadas con seguridad y las funciones especificadas por IBM para restitución de operaciones. El director de cómputo pasa revista mensualmente a estos diarios para detectar actividades insólitas (Por ejemplo: violaciones múltiples de un usuario o modificaciones que no realizó él mismo). Cuando se observa actividad insólita, el director de cómputo notifica al jefe del departamento a que corresponde el usuario. El jefe del departamento investiga la actividad reportada e informa de sus hallazgos al director de cómputo. No se archiva documentación escrita de las revisiones del director de cómputo ni de los procedimientos seguidos.

.

10. Describir las principales políticas, procedimientos y monitoreo que aseguren que los programas del sistema solamente son objeto de ejecución autorizada (Por ejemplo: programas de utilería, compiladores, programas de eliminación de información, utilería para archivos de datos).

Todos los programas del sistema se encuentran en la biblioteca *QSYS. En general, el director de cómputo es el propietario de todas las bibliotecas y archivos de bases de datos, y se ha otorgado acceso a los demás usuarios con base en sus funciones.

Raramente se utilizan programas de utilería. Solo el director de cómputo tiene contraseña para utilizar las herramientas de servicio dedicado.

11. Describir los procedimientos aplicados (Por ejemplo: indagación, observación) para obtener esta información. Incluir los nombres y títulos de las personas entrevistadas. Hacer referencia cruzada a los papeles de trabajo aplicables de recorridos.

Entrevistamos a Miguel Paredes (director de cómputo), Rita Icerman (analista/programadora), Dimas Díaz (operador), y a personal de contabilidad seleccionado. A continuación se describen nuestros procedimientos de recorrido sobre modificaciones a programas primarios y acceso a archivos de información.

Recorrido a los Controles sobre Sistemas de Información

Controles sobre cambios a Programas: Obtuvimos un formulario de solicitud a Sistemas de Información (anexo) y verificamos que estuviese completo. Todas las secciones apropiadas del formulario fueron llenadas y se obtuvieron todas las aprobaciones.

Mediante conversaciones con Sergio Juárez, Cuentas a Cobrar, y Alicia Malher, Cuentas a Pagar,

confirmé que los usuarios se involucran activamente en el diseño y prueba de los cambios a programas. El perfil de usuario del programador de Distribuidora de Repuestos, S.A., fue revisado para asegurarnos de que no tiene acceso a las bibliotecas de Producción. También conversé con el operador para determinar si durante el año había habido necesidad de procesamientos insólitos, incluyendo cambios de emergencia a programas. No hubo tal actividad.

Controles sobre acceso a Archivos de Información: La mayoría de los controles en esta área se corroboró a través del Informe sobre Valores del Sistema (incluido con los papeles de trabajo del Formulario - DISC). Durante mi diálogo con Sergio Juárez y Alicia Malher, pregunté si conocían alguna política de seguridad de Distribuidora de Repuestos, S.A., me dijeron que así es y que se les pidió que firmaran el reconocimiento de la política.

En cuanto al mantenimiento de perfiles de usuarios, pasé revista al informe de transferencias y terminaciones del personal y a los listados de perfiles de usuarios a que dieron lugar. Como parte de esa revista, observé que todas las aprobaciones requeridas se obtuvieron y que se hicieron las modificaciones oportunamente.

Por último, busqué en todos los perfiles de usuarios las capacidades asignadas como oficiales o administradores de seguridad. Encontré que solamente el director de cómputo tiene tales capacidades.

Distribuidora de Repuestos, S.A.

ANEXO 1:

FORMULARIO DE SOLICITUD A SISTEMAS DE INFORMACIÓN

SISTEMA:
PROGRAMA:
RESUMEN DE LA SOLICITUD (si es necesario, acompañar documentación adicional)
APROBACION DE LA SULICITUD DEL USUARIO

Solicitado por	Fecha	Jefe del departamento	Fecha

APROBACIÓN DE LA SOLICITUD POR SISTEMAS DE INFORMACIÓN

COMENTARIOS

_____ _____
Solicitud No. Proyecto No.

_____
Horas estimadas de programación

_____ _____
Director de Computo Fecha

_____ _____
Comité Orientador de Fecha
Sistemas de Información

APROBACION DE LAS PRUEBAS

_____ _____
Programador/Analista Fecha

_____ _____
Jefe de departamento Fecha

Jefe de departamento (seleccione una)
_____ He revisado, y estoy satisfecho con el diseño y resultados de las pruebas.
_____ He discutido la naturaleza de las modificaciones al programa con el programador/analista y he

decidido no revisar los resultados de las pruebas.

_____ _____
Director de Cómputo Fecha

APROBACION DE LA DOCUMENTACION

_____ _____
Programador/Analista Fecha

_____ _____
Director de Cómputo Fecha

APROBACION DE LA ACEPTACION

_____ _____
Jefe de departamento Fecha

_____ _____
Director de Cómputo Fecha

TRANSFERIDO A PRODUCCION

Distribuidora de Repuestos, S.A.

ANEXO 2:

REGISTRO DE SOLICITUDES

Número de proyecto	Fecha de recibo	Departamento solicitante	Aceptada/Rechazada	Fecha de transferencia a producción	Firma Director de Cómputo

5.5 Evaluar el Riesgo en el Entorno de Control

Se deberá obtener una comprensión de los sistemas de contabilidad y de control interno suficiente para planear y desarrollar un enfoque de auditoria efectivo. Deberá usarse juicio profesional para evaluar el riesgo de auditoria y diseñar los procedimientos de auditoria para asegurar que el riesgo se reduce a un nivel bajo.

Evaluar todas las políticas y procedimientos (controles internos) adoptados por la administración de una entidad para ayudar a lograr el objetivo de la administración de asegurar, tanto como sea factible, la conducción ordenada y eficiente del negocio, incluyendo adhesión a las políticas de administración, la salvaguarda de activos, la prevención y detección de fraude y error, la precisión e integridad de los registros contables, y la oportuna preparación de información financiera confiable.

Evaluar el riesgo de auditoria, permitirá detectar cuando los estados financieros están elaborados en forma errónea de una manera importante, analizando los tres componentes:

Riesgo inherente, evaluar la susceptibilidad del saldo de una cuenta o clase de transacciones a una representación errónea que pudiera ser de importancia relativa, individualmente para cada aseveración de los estados financieros o cuando se agrega con representaciones erróneas en otras cuentas o clases, asumiendo que no hubo controles internos relacionados.
Riesgo de control, verificar el riesgo de que una representación errónea que pudiera ocurrir en el saldo de cuenta o clase de transacciones y que pudiera ser de importancia relativa individualmente o en relación a otros saldos o clases, que no sea prevenido o detectado y corregido con oportunidad por los sistemas de contabilidad y de control interno.
Riesgo de detección, considerar el riesgo de que los procedimientos sustantivos no detecten una representación errónea que existiera en un saldo de cuenta o clase de transacciones que podría ser de importancia relativa, que puedan impactar los estados financieros sujetos a auditoria.

5.6 Sistemas Contables y Control Interno

En la auditoria de estados financieros, se deberá considerar sólo en aquellas políticas y procedimientos dentro de los sistemas de contabilidad y de control interno que son relevantes para las aseveraciones de los estados financieros.

Evaluar los sistemas que identifican, reúnen, analizan, calculan, clasifican, registran, resumen e informan transacciones y otros eventos. La comprensión de los aspectos relevantes de los sistemas de contabilidad y de control interno, junto con las evaluaciones del riesgo inherente y de control descritas en el inciso 5.5

Evaluar el riesgo en el Entorno de Control y otras consideraciones, ayudan al auditor a:

a) Identificar los tipos de potenciales representaciones erróneas de importancia relativa que pudieran ocurrir en los estados financieros;
b) Considerar los factores que afectan el riesgo de representaciones erróneas sustanciales; y
c) Diseñar procedimientos de auditoria apropiados.

Además deberá documentar todas las políticas y procedimientos (controles internos) adoptados por la administración del cliente Distribuidora de Repuestos, S.A., para ayudar a lograr el objetivo de la administración de asegurar, tanto como sea factible, la conducción ordenada y eficiente de su negocio, incluyendo adhesión a las políticas de administración, la salvaguarda de activos, la prevención y detección de fraude y error, la precisión e integridad de los registros contables y la oportuna preparación de información financiera contable.

El sistema de control interno comprende:

1) El ambiente de control, significa la actitud global, conciencia y acciones de directores y administración respecto del sistema de control interno y su importancia en la entidad. Ver la forma de evaluación del entorno de control en el punto 5.3 anterior. El ambiente de control tiene un efecto sobre la efectividad de los

procedimientos de control específicos. Un Control presupuestal estricto y una función de auditoria interna efectiva, pueden complementar en forma muy importante los procedimientos específicos de control. Los factores reflejados en el ambiente de control incluyen:

- La función del consejo de directores y sus comités;
- Filosofía y estilo operativo de la administración;
- Estructura organizacional de la entidad y métodos de asignación de autoridad y responsabilidad;
- Sistema de control de la administración incluyendo la función de auditoria interna, políticas de personal y procedimientos y segregación de funciones o deberes.

2) Procedimientos de control, significa aquellas políticas y procedimientos además del ambiente de control que la administración ha establecido para lograr los objetivos específicos de la entidad. Los procedimientos específicos de control incluyen:

- Reportar, revisar y aprobar conciliaciones;
- Verificar la exactitud aritmética de los registros;
- Controlar las aplicaciones y ambiente de los sistemas de información por computadora, por ejemplo, estableciendo controles sobre:
  - Cambios a programas de computadora;
  - Acceso a archivos de datos
- Mantener y revisar las cuentas de control y las balanzas de comprobación;
- Aprobar y controlar documentos;
- Comparar datos internos con fuentes externas de información;
- Comparar los resultados de cuentas del efectivo, valores e inventarios con los registros contables;
- Limitar el acceso físico directo a los activos y registros;
- Comparar y analizar los resultados financieros con las cantidades presupuestadas.

El enfoque de auditoria, se puede apreciar en el punto 5.9 del Plan de enfoque de Auditoria y la evaluación preliminar del riesgo de control (conjuntamente con la evaluación de riesgo inherente) para determinar el riesgo de detección apropiado se puede apreciar en el punto 5.4 anteriormente descrito.

Distribuidora de Repuestos, S.A.
Al 31 de diciembre del 200x

Descripción de la Organización y Políticas Contables

Organización – Distribuidora de Repuestos, S.A., fue fundada en el año 1963 como entidad privada lucrativa, siendo reconocida legalmente el 3 de junio de 1963 por medio de Acta Notarial. Sus objetivos son orientados a impulsar la compra venta de repuestos y accesorios para el progreso integral de las áreas rurales de Guatemala y sus núcleos urbanos.

Principales Políticas Contables - A continuación se presenta un resumen de las principales políticas contables utilizadas en la preparación de los estados financieros.

Contabilidad por Fondos – Distribuidora de Repuestos, S.A. divide sus operaciones por fondos, los cuales fueron constituidos de acuerdo con las operaciones que se realizan con las líneas de créditos y aportes recibidos. Existen registros contables que presentan la información financiera por cada uno de esos fondos.

a. ***Inversiones -*** Las inversiones están representadas por certificados de custodia de inversión y los intereses devengados son pagaderos mensual, semestralmente y al vencimiento, así como por la constitución de un fondo de administración a través de un fideicomiso, del cual los intereses devengados no se capitalizan.

b. ***Préstamos -*** Los préstamos son otorgados a las personas más necesitadas integrantes de grupos localizados en áreas rurales. En el año 200x no se otorgaron préstamos para compra de repuestos para tractores. Los créditos agrícolas devengan el 20% de interés anual. Los de ventas de tractores el 0%. Los intereses devengados no percibidos se registran en cuentas por cobrar contra otros pasivos y se trasladan a resultados cuando se perciben.

c. ***Estimación para Cuentas de Dudosa Recuperación -*** La estimación se calcula en un 100% para aquellos créditos a grupos con dos años de vencidos; así como para la cartera que fue considerada en conflicto y que no ha sido renegociada y un 25% sobre el total de las otras carteras.

d. ***Inventarios –*** Los repuestos y accesorios están valuados al costo, bajo el método de costo identificado de compra.

e. ***Inmuebles y Equipo -*** Los inmuebles y equipo están valuados al costo de adquisición. En los casos de bienes rescatados se valúan al valor de la deuda de los clientes. Los bienes se deprecian por el método de línea recta de acuerdo con la vida útil estimada, en los siguientes porcentajes:

Edificios	5%
Vehículos	20%
Maquinaria	20%
Mobiliario y equipo	20% y 25%
Equipo de taller	25%
Equipo de computación	33.33%

f. ***Provisión para Indemnizaciones –*** De acuerdo con las disposiciones del Código de Trabajo del país, las compensaciones a favor de los empleados por tiempo de servicio deben pagarse en caso de despido injustificado o muerte.

g. ***Patrimonio -*** Los resultados obtenidos en las operaciones de la empresa por el año terminado el 31 de diciembre del 200x disminuyeron directamente el saldo del Patrimonio, tomando como base las disposiciones específicas de sus estatutos.

5.7 Determinar la Materialidad

Distribuidora de Repuestos, S. A.
Al 31 de diciembre del 200x

Se ha estimado la materialidad preliminar tomando como base o componente crítico los ingresos antes de impuestos previstos al 31 de diciembre del año 20x0 en Q 1,257,679 por un 6% de materialidad.

Históricamente el pronóstico ha sido sustancialmente preciso. Se ha estimado la materialidad preliminar en Q 75,400 y se ha establecido el error tolerable en 75% de la materialidad preliminar, o sea Q 56,500, porque se esperará que, según la experiencia anterior con el cliente, el alcance de las diferencias de auditoria, para la auditoria completa será pequeño en relación con la materialidad preliminar y que el riesgo de errores importantes será bajo.

Se registrará todas las partidas mayores de Q 18 mil, en el resumen de diferencias de auditoria.

MATERIALIDAD PRELIMINAR		AL 31-12-200X
COMPONENTE CRÍTICO		
INGRESOS ANTES DE IMPUESTOS		**1,257,679**
MATERIALIDAD 6% SOBRE LOS INGRESOS ANTES DE IMPUESTOS	**6%**	**75,400**
ERROR TOLERABLE 75% DEL MONTO TOTAL DE LA MATERIALIDAD ESTIMADA	**75%**	**56,500**
DIFERENCIAS DE AUDITORÍA	**25%**	**18,000**

5.8 Preparar el Memorando de Planeación – Guía de Auditoria

Distribuidora de Repuestos, S. A.
Al 31 de diciembre del 200x

Memorando de Planeación de Auditoria (MPA)

Cambios en el negocio del cliente y en el alcance de la auditoria:
En 200v la Distribuidora de Repuestos S. A., adquirió la Agropecuaria X, S.A., una empresa multinacional con ventas de Q 10 millones. (Ver discusión sobre la adquisición y nuestra participación en memorando separado)

Asuntos de contabilidad y auditoria:

Adquisición de Agropecuaria X, S.A.:
En relación con la adquisición de Agropecuaria X, S.A., revisaremos los ajustes contables de compra para determinar si todos los importes están registrados en forma correcta.

Deuda a Largo Plazo:
En el 200w la Agropecuaria X, S.A., incurrió en una deuda por Q 5 millones para financiar futuras adquisiciones. Necesitaremos determinar si la Agropecuaria X, S.A., ha registrado apropiadamente todos los importes relacionados con la deuda y si está cumpliendo con todas las cláusulas del convenio de deuda.

Impuesto sobre la Renta:
La Agropecuaria X, S.A., está adoptando una nueva norma contable en el 200w y, por consiguiente, necesitamos determinar si todos los importes han sido registrados correctamente al fin del año según tal norma.

Revisión analítica general:
Ver los estados financieros intermedios con los comentarios de la revisión analítica que se acompañan, según se discutió durante la reunión con el cliente.

Cambios en el entorno de control y la estructura de control interno:

Con base en nuestra revisión, no han ocurrido cambios importantes en el entorno general de control y continuamos evaluándolo como confiable. En relación con la adquisición de la Agropecuaria X, S.A., la Distribuidora de Repuestos, S. A., convirtió su sistema de cuentas por pagar al sistema utilizado por la Agropecuaria X, S.A. Hemos obtenido del cliente la documentación relativa a este nuevo sistema y preparamos el análisis de control y otra documentación a fin de adquirir una comprensión sobre el sistema y evaluar los controles relevantes. Con base en nuestra revisión (incluyendo recorridos) evaluamos los controles sobre el nuevo sistema como eficaces.

No hubo más cambios importantes en los sistemas y controles del cliente.

Cambios en las estrategias del plan de auditoria y evaluaciones de controles:

Con base en la información del equipo de trabajo, hemos determinado que el uso de una estrategia de confiable para la auditoria del 200x será lo más eficiente para aquellas áreas donde hemos evaluado los controles como eficaces. Por consiguiente, hemos cambiado nuestra estrategia de auditoria de no confiable a confiable en tales áreas. Puesto que hemos identificado, documentado y evaluado los controles relevantes en los años anteriores, nuestra documentación continúa siendo apropiada. Los controles relevantes en relación con el nuevo sistema de cuentas por pagar han sido identificados y documentados y los hemos evaluado como eficaces. Someteremos a prueba los controles y algunos saldos a una fecha intermedia y aplicaremos procedimientos limitados de conexión para el período intermedio y prueba de cortes a la fecha intermedia y al fin del año.

Como se menciona anteriormente, se ha preparado un memorando de estrategias del plan de auditoria separado en relación con la auditoria de alcance total de los estados financieros de Agropecuaria X, S.A.

Materialidad Preliminar:

Hemos estimado la materialidad preliminar con base en Q 1,257,679 por 6% de los ingresos antes de impuestos previstos al 31 de diciembre del 200x. Históricamente el pronóstico ha sido sustancialmente preciso. Hemos estimado la materialidad preliminar en Q 75,400 y hemos establecido el error tolerable en 75% de la materialidad preliminar, o sea Q 56,500, porque esperamos que, según nuestra experiencia anterior con el cliente, el alcance de las diferencias de auditoria para la auditoria completa será pequeño en relación con la materialidad preliminar y que el riesgo de errores importantes será bajo. Registraremos todas las partidas mayores de Q 18 mil, en el resumen de diferencias de auditoria.

Expectativas del cliente:

Según nuestras discusiones con altos ejecutivos de la gerencia, ellos esperan recibir los estados financieros auditados antes de lo previsto el año pasado. Quieren que, además de los procedimientos que realizamos como parte de nuestra auditoria, realicemos una evaluación del proceso de entrega del nuevo producto de la Agropecuaria X, S.A., y que investiguemos algunos ajustes del inventario en libros contra el físico (inferior a nuestro alcance normal en la auditoria) que han tenido lugar en una de las bodegas. Observaremos uno de los conteos del inventario X_INV en tal bodega.

5.9 Desarrollar el Plan de Enfoque de Auditoria

FORMULARIO DE ACTUALIZACION Y APROBACION DEL PLAN DE ENFOQUE DE AUDITORIA

Cliente: Distribuidora de Repuestos, S.A.
Fecha: al 31 de diciembre del 200x

Si se trata de actualización del plan, resumir brevemente los cambios significativos respecto del plan anterior. Los factores que con frecuencia influyen en modificaciones al enfoque de auditoria son:

- Cambios identificados durante la fase de planificación general en el entorno del control, en el negocio del cliente o su industria. (por ejemplo: prejuicio adquirido por la dirección para sobrevaluar utilidades, que puede requerir mayores procedimientos en busca de subvaluación en las cuentas de estimación de activos).
- Cambios en el riesgo inherente o características de las cuentas evaluadas.
- Cambios en las evaluaciones de riesgo sobre los ciclos de negocios como fuente de información.
- Otros cambios en el enfoque (por ejemplo: procedimientos para aumentar la eficiencia, tales como técnicas de auditoria con ayuda del computador, uso de auditores internos).

Cuentas Significativas afectadas por cambios en el Enfoque de Auditoria.	Saldos al 31/12/200x	Saldos al 31/12/200w	Razones de los cambios
Cuentas de Balance			
• **Cuentas por Cobrar**	806,112	788,112	El cliente ha mejorado sus controles en esta área al grado que podemos otorgar confianza. Por la naturaleza de estas mejorías, podremos utilizar puntos de referencia y otras técnicas de auditoria con ayuda del computador (CAATs).
• **Relacionadas por cobrar**	400,215	450,632	
• **Otras cuentas por cobrar**	35,000	0	
• **Provisión de incobrables**	(22,000)	(22,000)	
• **Total Cuentas por cobrar**	**1,219,327**	**1,216,744**	
• **Inventarios Repuestos**	1,653,784	1,576,197	El cliente ha mejorado sus controles en esta área al grado que podemos otorgar confianza. Por la naturaleza de estas mejorías, podremos utilizar puntos de referencia y otras técnicas de auditoria con ayuda del computador (CAATs).
• **Accesorios**	922,352	1,089,880	
• **Otros Repuestos**	322,587	342,270	
• **Provisión obsolescencia**	(140,390)	(140,208)	
• **Total Inventarios**	**2,758,333**	**2,868,139**	
• **Cuentas por Pagar**	(428,257)	(579,429)	El cliente ha mejorado sus controles en esta área al grado que podemos otorgar confianza. Por la naturaleza de estas mejorías, podremos utilizar puntos de referencia y otras técnicas
• **Relacionadas por pagar**	(335,002)	(367,350)	
• **Gastos**	(196,719)	(147,408)	

acumulados			de auditoria con ayuda del computador
• **Total Cuentas por Pagar**	**(959,978)**	**(1,094,187)**	(CAATs).
Cuentas de Resultados			
• **Ventas Netas**	**(16,463,641)**	**(17,002,392)**	El cliente ha mejorado sus controles, podremos utilizar puntos de referencia de cuentas de balance y técnicas de auditoria con ayuda del computador (CAATs).
• **Costos de ventas**	**15,001,229**	**13,967,679**	El cliente ha mejorado sus controles, utilizaremos los resultados de las pruebas de cuentas de balance con ayuda del computador (CAATs).
• **Gastos Administrativos**	693,541	659,158	Sus controles son efectivos en esta área, podremos utilizar puntos de
• **Gastos de ventas**	120,486	93,456	referencia y otras técnicas de auditoria
• **Total Gastos**	**814,027**	**752,614**	con ayuda del computador (CAATs).

Riesgo Inherente y características de las cuentas:

- Cuentas por Cobrar: El aumento en el margen de utilidad bruta al 31 de diciembre del año en curso se atribuye a algunos problemas en el descargo de inventarios (es decir, el reconocimiento del costo de ventas). La dirección considera que podrá corregir ese problema para el final del ejercicio. En años anteriores no han sido necesarios ajustes significativos en la estimación de cuentas dudosas. El saldo al 31 de diciembre del año anterior consistía de aproximadamente 1,100 cuentas, con 1,000 de ellas inferiores a Q 10,000; 73 entre Q 10,000 y Q 50,000; y 21 entre Q 50,000 y Q 100,000.
- Inventarios: El aumento en Inventario de Repuestos al 31 de diciembre del año en curso se relaciona con las descargas inadecuadas, pero consideran que se corregirán al final del ejercicio. Los Accesorios reportan una disminución derivado del problema que se ha manejado en la declaración del costo de ventas, pero dicho procedimiento está siendo depurado por la entidad y consideran superarlo para el fin de año. Se atribuye a algunos problemas en el descargo de inventarios (es decir, el reconocimiento del costo de ventas). La dirección considera que podrá corregir ese problema al cierre. En años anteriores no han sido necesarios ajustes significativos en la provisión de obsolescencia.
- El total de cuentas por pagar: refleja una disminución que se atribuye a algunos problemas en el descargo de inventarios (es decir, el reconocimiento del costo de ventas). La dirección considera que podrá corregir ese problema para el final del ejercicio.
- Para las cuentas de resultados: se considera que se harán revisiones analíticas para estimar las desviaciones importantes y los eventos inusuales de dichas cuentas.

Detalle de las Estrategias de Auditoria:

Cuentas por Cobrar:

- Pasar revista a las conciliaciones de cuentas a cobrar con el mayor general.
- Para comprobar el funcionamiento apropiado de programas de entrada y salida de pedidos, observar la introducción de combinaciones válidas e inválidas, en los procedimientos en línea de ingresos a bodega de repuestos y accesorios, pedidos o traslados.
- Utilizando programas de auditoria de selección e impresión, circularizar confirmaciones de cuentas por cobrar. Utilizar muestreo Estadístico.
- Ejecutar procedimientos alternativos sobre confirmaciones regresadas con diferencias o confirmaciones no regresadas.
- Para cuentas relacionadas conciliar el efectivo recibido y estudiar el margen de utilidad bruta por línea de producto.
- Revisar las definiciones de menús, la autoridad pública estándar y las listas de autorización para verificar que: a) El acceso al archivo maestro de ventas/ cuentas por cobrar, está restringido a personal no autorizado. b) El acceso a los archivos de datos para registro de pedidos y facturas de venta, se encuentra adecuadamente restringido a personal no autorizado.

Inventarios:

- Estudiar la actualización preparada por el cliente de los movimientos de ingresos y salidas de inventarios de Repuestos, Accesorios y Otros repuestos.
- Para comprobar el funcionamiento apropiado de programas de entrada y salida de existencias, observar la introducción de combinaciones válidas e inválidas, en los procedimientos en línea de ingresos a bodega y requisiciones o traslados.
- Comparar el nivel de estos movimientos con las cuentas relacionadas de resultados.
- Con el apoyo del programa herramienta de auditoria (CAATs), establecer puntos de referencia sobre la totalización de ventas diarias y la contabilización de ventas, costos de ventas y descargos de inventarios.
- Mediante la investigación y observación actualizar los puntos de referencia para traslados de Repuestos y Accesorios a otras bodegas, verificar la correcta valuación del costo de de las mercancías trasladadas a otras bodegas y relacionar con cuentas de resultados.
- Investigar eventos inusuales y mayores a Q 25 mil emitidos después de nuestra revisión preliminar, como procedimiento de conexión con el cierre.
- Revisar las definiciones de menús, la autoridad pública estándar y las listas de autorización para verificar que: a) El acceso al archivo maestro de inventarios/costo de ventas está restringido a personal no autorizado. b) El acceso a los archivos de datos para registro de ingresos, salidas y traslados de existencias, se encuentra adecuadamente restringido a personal no autorizado.

Cuentas por Pagar:

- Mediante de observación, indagación y recorridos, verificar el funcionamiento de los controles programados para evitar errores potenciales en el registro de ordenes de compra, recepción de las mercancías o servicios y la provisión contable respectiva.
- Para comprobar el funcionamiento apropiado de programas de entrada y salida de cuentas por pagar, observar la introducción de combinaciones válidas e inválidas, en los procedimientos en línea de ingresos a bodega, requisiciones, traslados o emisión de cheques de pago a proveedores.
- Revisar las definiciones de menús, la autoridad pública estándar y las listas de autorización para verificar que: a) El acceso al archivo maestro de compras/cuentas por pagar está restringido a personal no autorizado. b) El acceso a los archivos de datos para registro de

órdenes de compras y facturas de proveedores se encuentra adecuadamente restringido a personal no autorizado.

Generales:

- Comprobar el funcionamiento consistente a través de todo el año en cuanto a cambios a programas y accesos a archivos de información:
- Construir una muestra de cambios a programas seleccionada de la lista del directorio en la aplicación de ventas y cuentas a cobrar, Inventarios y costo de ventas, también las cuentas por pagar y constatar que se sometieron a prueba y aprobación adecuada.
- Estudiar las conciliaciones de los diferentes listados de cambios a programas con los Paquetes de Control de Cambios. Mediante indagación y observación, determinar que esos procedimientos se realizaron consistentemente durante todo el año.
- Construir una muestra de "Formas de Solicitud de Autorización de Perfiles de Usuario" para probar lo adecuado de las autoridades otorgadas a los usuarios para accesos a las diferentes aplicaciones seleccionadas para prueba de controles.
- Evaluar la efectividad de la asignación de autoridades específicas sobre objeto, autoridades definidas por el sistema y capacidades limitadas.

5.10 Programa de Procedimientos de Auditoria

Distribuidora de Repuestos, S.A.
Al 31 de diciembre del 200x

Programa de Evaluación de Controles:

No.		Ref. Pts
1.	**Conceptos de Control:** Hay ciertos principios de control que aplican a todos los tipos de controles ya sean éstos generales, programados o manuales. Indagar sobre los controles que afectan al ambiente informático. Algunos controles pueden realizarse ya sea en forma manual o en forma sistémica. Por ejemplo: antes del pago de una factura se genera una confrontación entre el informe de recepción, las órdenes de compra y las facturas recibidas. Verificar las fuentes de información para hacer pruebas sobre estos controles	
2.	Controles Efectivos:	
21.	Un control efectivo es aquel que está adecuadamente diseñado para alcanzar el objetivo propuesto y que ha estado operando efectivamente durante el período de tiempo esperado. Esto se deberá probar relacionado al punto anterior.	
22.	Los objetivos de un control frecuentemente cubren los atributos de integridad (Integridad, Validez, Corte, Registro, Valuación, Presentación). Se deberá evaluar dichos objetivos y recolectar cualquier observación y hallazgos sobre dichos objetivos.	
23.		
3.	**Clasificación de los controles: (controles de entrada, de procesamiento y de salida),** **Controles de entrada:**	
31.	Chequeos o validaciones de campos; chequeos de registro; totales y chequeos de lotes (batch); chequeos de Archivos; Controles de Accesos; Autorización y Aprobación; Controles de Interfaces. Si se tiene las fuentes de información y los ambientes probar su cumplimiento.	
4.	**Controles de Procesamiento:**	
41.	Revisión de edición (validación); Entrada Pregrabada; Controles de Hardware; Totales Batch. Los controles de procesamiento generalmente incluyen la programación de validaciones de edición de cambios, de entradas pregrabadas y de controles de hardware, hacer pruebas sobre este aspecto.	
5.	**Controles de Edición Programadas (Validaciones)**	
51.	Las revisiones de edición programadas o	

validaciones de campos son procedimientos programados utilizados para verificar la exactitud de la información ingresada. Probar si hay pistas sobre dichas validaciones programadas y documentar.

52. Las rutinas de validación de la aplicación a menudo incluyen diversas revisiones de la edición. Chequear dichas revisiones.

53. Las formas más comunes de chequeos programados de edición pueden incluir lo siguiente:

Formato; Rango; Razonabilidad; Firma; Revisión Cruzada; Control de Totales (contabilidad monetarios e ítems); Revisión de secuencias; Revisión de dependencia; Control de existencia, Digito verificador, Conciliación de la documentación fuente, Conciliación de los Inputs procesados con información previa al proceso.

Buscar las fuentes de información, establecer una muestra y probar que cumpla con los chequeos programados de edición.

54. Entrada previamente gravada: Corresponden a información que ha sido impresa con anterioridad en un documento fuente. La aplicación frecuentemente vuelve a leer los items de información: OCR, MICR; Números de series preimpresos.

Verificar si hay entradas previamente gravadas, identificar y documentar su ubicación.

55. Controles de Hardware: Son considerados como una parte de los controles generales de la computadora. Un control de hardware puede incluir lo siguiente:

Revisión de paridad, ubicación y chequeo de un código de operación válida; Validación de existencia de carácter; Doble lectura/escritura, lectura posterior a la escritura; chequeos por réplica; Autochequeo del equipamiento. Además se pueden utilizar controles de revisión del tipo punto/reinicio (check point restarts), los cuales son útiles cuando ocurre un error de procesamiento, si el error no ha corrompido los datos (es decir ante un error de hardware, como ejemplo, cuando el operador cargó un archivo equivocado o el programa terminó en forma anormal).

Seleccionar algunos controles de hardware mencionados anteriormente y probar, (por ejemplo, validación de la existencia de carácter de paridad, chequeos por replica, etc).

56. Totales Batch: Pueden consistir en lo siguiente: Total hash, Conteo de Registros, Totales de conciliaciones cruzadas.

Tomar una muestra y rastrear con la documentación fuente dichos totales batch.

6. **Controles de Salidas:**

61. Controles de Interface: Procedimientos programados; Informes de Control; Registro de Control Header/Trailer. Verificar si existen dichos controles de salida.

62. Control de información: Conciliación y Revisión; Distribución de salidas solo a personal autorizado; Manipulación adecuada de Salidas con información privada y confidencial.

Verificar los controles de información y documentar la conciliación, revisión y distribución de dichas salidas.

63. Revisión de Salidas por el Usuario: Notificación de Salidas Pérdidas; Revisiones y Conciliación. Verificar la evidencia de revisión de salidas por el usuario.

Buscar las notificaciones de salidas pérdidas, las conciliaciones y documentar las pruebas realizadas.

64. Solución de Errores: Los errores que son detectados por medio de los controles que acabamos de analizar deben ser resueltos de alguna manera. Los errores identificados por computadora frecuentemente se informan o registran como sigue:

* Informe y registros de error -- En ellos se enumera todos los errores encontrados durante la entrada y el procesamiento de los datos.
* Informe de Excepción: -- Los registros o transacciones pueden ser realizados por diversas razones, incluyendo ítems de información inválida o fuera de rango. Los ítems rechazados frecuentemente se imprimen en el informe de excepción.
* Archivos en suspenso -- Las transacciones rechazadas durante las validaciones no son procesadas con las transacciones aceptadas. Usualmente éstas son capturadas en un archivo de transacciones en suspenso o retenidas para la acción siguiente de corrección y reproceso.

En base a los controles anteriormente analizados, tomar una muestra de solución de errores y documentar la prueba.

El informe y registro de errores, el informe de excepciones y archivos en suspenso deben estar sujetos a los mismos controles que otras aplicaciones y archivos. Particularmente, el acceso a tales ítems debe restringirse solamente a personas y programas autorizados.

Indagar sobre el informe de registro de errores, observar dicha información durante el período que se revisa y documentar.

65. Los errores que son detectados por los controles que hemos analizado requieren acciones correctivas posteriores. En particular, los

siguientes asuntos deben considerarse:

* Identificación y Corrección de error en línea -- Muchas revisiones de edición o verificaciones pueden realizarse interactivamente por la aplicación. En estos casos el sistema puede notificar la entrada errónea de información al operador inmediatamente después del descubrimiento de un error y el operador puede realizar inmediatamente las correcciones en línea.
* Procedimiento de revisión y corrección -- deben establecerse procedimientos para revisar todos los errores identificados y proceder a corregir.
* Procedimientos para la investigación y solución de excepciones -- Deben establecerse procedimientos relacionados con el manejo de todas las excepciones.
* Procedimiento de Reenvió y Revalidación de Errores de Entrada -- Las entradas de información rechazadas deben ser revisadas, solucionadas y luego enviadas nuevamente para su procesamiento mediante el ciclo normal de entrada de información o por el siguiente ciclo de corrección de errores. Este es un control muy importante...

En base a las declaraciones de este punto, haga cedula de hallazgos y sugerencias para mejoría.

66. Las pruebas en una fecha intermedia, pueden requerir que adicionalmente llevemos a cabo investigaciones al termino del año contable para obtener seguridad en que los controles identificados y probados durante la fecha intermedia no han cambiado o han sido afectados por ciertos cambios, como por ejemplo, la rotación de personal.

Indagar sobre la rotación del personal del Centro de Tecnología de la Información y documentar los hallazgos.

67. Las pruebas a los controles pueden diferenciarse de las pruebas sustantivas como se muestra a continuación:

68. ¿Como realizamos pruebas a controles?

Como probar los controles

* Investigación corroborativa.
* Observación
* Análisis de la evidencia de los documentos
* Reejecución de los controles.

Las pruebas a los controles generalmente consisten de una combinación de investigación y observación corroborativa además del análisis de los documentos o una nueva reejecución para probar el control. Frecuentemente la investigación de una muestra de documentos no es la manera más efectiva y eficiente de obtener un adecuado grado de seguridad en la auditoria al

efectuar nuestras pruebas a los controles.
No olvide en aplicar estos procedimientos.

69. Investigación corroborativa: consiste en entrevistas de sondeo cuidadosamente dirigidas para ganar una comprensión sobre la efectividad de los controles. La investigación corroborativa puede ser directa o indirecta.

70. Observación del funcionamiento de Control: A menudo el observar la realización de un procedimiento de control o de una actividad de monitoreo provee importante evidencia de su efectividad.

71. Examen de documentos: Si la realización de un control es documentada. (UNA FIRMA O TILDE) podemos obtener evidencia de su realización por medio de examinar la documentación.

72. Reejecución de Control: A veces entrega la evidencia de su efectividad. Normalmente esta es una prueba útil para los controles programados. Sin embargo para los controles manuales, la reejecución del control no es una buena prueba. Por ejemplo: realizar nuevamente una revisión de un informe de excepción no asegura que el cliente realizó regularmente esta revisión durante el año.

Programa para pruebas de auditoria (TAACs)

No.	Procedimiento	Hecho por
1.	Crear el directorio Cuentas por Cobrar y crear el proyecto ANALISIS DE CARTERA dentro del directorio anterior.	
2.	Importar el archivo de CARTERA.DBF	
3.	Realice un análisis estadístico sobre los campos de Saldo	
4.	Determine los totales de CARTERA por rango de CLIENTES considerando variaciones de SALDO.	
5.	Determine los totales por tipo de CLIENTE.	
6.	Suponiendo que la recuperación es mensual, calcule la tasa de recuperación anual, calcule los intereses de un mes completo.	
7.	Construya las columnas que sean necesarias para distribuir las cuentas en función del plazo en periodos de 30 días. (similar a la construcción de columnas realizada para estratificar los inventarios)	
8.	Tomando la información anterior totalice por bodega para determinar la distribución de cartera por plazo y por bodega.	
9.	En función de la fecha de vencimiento y fecha de corte 01/jul/200x determine cuantos días faltan para el vencimiento de las cuentas.	
10.	Tomando como base lo anterior estratifique los saldos en función de los días para vencimiento en forma mensual con meses de 30 días.	
11.	Conclusión sobre las pruebas TAACs realizadas.	

CONCLUSIONES

1. La auditoria financiera en una Distribuidora de Repuestos, consiste en un examen sistemático de los libros, documentos y demás registros contables, para formarse un criterio y obtener evidencia comprobatoria suficiente y competente para fundamentar objetiva y profesionalmente la opinión del Auditor sobre los estados financieros que prepara la administración de la entidad. Por consiguiente es necesario definir los procedimientos para la planeación de la auditoria, los cuáles deberán ser determinados por el Auditor y deberá tomar en cuenta las Normas de Auditoria, los requerimientos de Organismos Profesionales importantes, la legislación, los reglamentos y, también los términos del contrato de auditoria que incluye los requisitos para dictaminar.

2. El auditor en su carta de compromiso, considerará cómo afecta a la auditoria un ambiente de Sistemas de Información Computarizada (SIC). Porque el objetivo y alcance de auditoria se modificarán debido a que tendrá que evaluar el sistema contable, el control interno y aparte la evaluación que deberá hacerse al ambiente de Sistemas de Información Computarizada (SIC), debido a que el uso de una computadora cambia el procesamiento, almacenamiento y comunicación de la información financiera y contable, y para obtener una comprensión suficiente de los sistemas contables y de control interno, por lo tanto deberá evaluar los riesgos inherente y de control a través de los cuales se establece el riesgo global que puede afectar el alcance de los procedimientos aplicables en la auditoria financiera.

3. Es importante considerar los lineamientos en la planeación de auditoria financiera tales como conocer el negocio del cliente, la complejidad de la auditoria, identificar los eventos, transacciones y prácticas que puedan tener un efecto importante sobre los estados financieros; evaluación de la competencia de la administración, comprender los sistemas contables, el control interno, y las políticas contables aceptadas por la entidad, evaluar el riesgo e importancia relativa, evaluar la posibilidad de representaciones erróneas, incluyendo la experiencia de períodos pasados o de fraude, para tener elementos de juicio y poder identificar las áreas de contabilidad complejas incluyendo las que implican estimaciones contables, y establecer la naturaleza, tiempos y alcance de los procedimientos que serán aplicados en el desarrollo del trabajo.

4. En la Planeación de la evaluación de los ambientes de Sistemas de Información Computarizada (SIC) se debe tomar en cuenta los lineamientos siguientes: Al efectuar la planeación de auditoria financiera deberá considerarse sí el auditor financiero tiene el suficiente conocimiento del ambiente SIC, para planear, dirigir, supervisar y revisar el trabajo desarrollado, considerando si se necesitan habilidades especializadas en SIC.

5. La aplicación de procedimientos para entender el impacto del ambiente de sistemas de información sobre los sistemas de contabilidad y control interno, el riesgo inherente y riesgo de control a nivel de saldo de cuenta y tipo de transacciones, comprender la importancia y complejidad del ambiente SIC en cada operación importante de contabilidad, la importancia relativa de las aseveraciones de los estados financieros que se ven afectadas por el SIC, considerando compleja una aplicación si el volumen de transacciones es tal que los usuarios encontrarían difícil identificar y corregir errores en el procesamiento.

6. Al planear la auditoria de las áreas afectadas por el ambiente SIC, obtener una comprensión de la importancia y complejidad de dichas actividades y la disponibilidad de datos para uso de auditoria; la computadora automáticamente genera transacciones o entradas de importancia relativa que no pueden ser (o no son) validadas independientemente, por lo cuál se deberá entender los controles de aplicación en el ambiente SIC; considerar también si las transacciones son intercambiadas electrónicamente con otras entidades (como los sistemas electrónicos de intercambio de datos – (EDI- Electronical Data Interchange) sin revisión manual para determinar la exactitud o razonabilidad.

7. Evaluar la estructura organizacional de las actividades del ambiente 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 funciones; verificar la disponibilidad de datos, los documentos fuente, los archivos electrónicos SIC y otro material de evidencia que puede ser requerido para revisión por el Auditor, los cuales pueden existir por un corto período de tiempo o sólo en forma legible electrónica.

RECOMENDACIONES

1. Es necesario conocer el negocio del cliente y sus actividades administrativas para formarse un criterio y obtener evidencia suficiente para soportar adecuadamente la opinión del Auditor sobre los estados financieros que prepara la administración de la entidad. Siendo necesario hacer una planeación de auditoria, tomando en cuenta las Normas de Auditoria, los requerimientos de Organismos Profesionales importantes, la legislación, los reglamentos y, también los términos del contrato de auditoria que incluye los requisitos para dictaminar.

2. Derivado de la necesidad que se tiene de especificar los lineamientos en el proceso de auditoria, el auditor deberá definir su carta de compromiso, dejando plasmado en dicho documento la consideración y el impacto del ambiente de Sistemas de Información Computarizada para que el objetivo y alcance de auditoria no sean modificados en el desarrollo del trabajo tanto para evaluar los riesgos inherente y de control a través de los cuales se establece el riesgo global que puede afectar el alcance de los procedimientos aplicables en la auditoria financiera.

3. Se recomienda considerar los lineamientos en la planeación de auditoria financiera tales como conocer el negocio del cliente, la complejidad de la auditoria, identificar los eventos, transacciones y prácticas que puedan tener un efecto importante sobre los estados financieros; comprender y evaluar los sistemas contables, el control interno, y las políticas contables aceptadas por la entidad, para tener elementos de juicio y poder identificar las áreas de contabilidad complejas incluyendo las que implican estimaciones contables.

4. Es importante recomendar que en la Planeación de la evaluación de los ambientes de Sistemas de Información Computarizada (SIC) se considere lo siguiente: Considerar sí el auditor financiero tiene el suficiente conocimiento del ambiente SIC, para planear, dirigir, supervisar y revisar el trabajo desarrollado, considerando si se necesitan habilidades especializadas en SIC haciendo uso de un experto.

5. En la aplicación de procedimientos para entender el impacto del ambiente de sistemas de información computarizada, sobre los sistemas de contabilidad y control interno, y evaluar el riesgo inherente y riesgo de control a nivel de saldo de cuenta y tipo de transacciones, es necesario comprender la importancia y complejidad del ambiente SIC en cada operación importante de

contabilidad, tomando en cuenta el impacto de las aseveraciones de los estados financieros, considerando compleja una aplicación si el volumen de transacciones es tal que los usuarios encontrarían difícil identificar y corregir errores en el procesamiento.

6. Se recomienda que cuando se realice la planeación de la auditoria de las áreas afectadas por el ambiente SIC, se obtenga una comprensión de la importancia y complejidad de dichas actividades y la disponibilidad de datos para uso de auditoria, considerando transacciones de importancia relativa que no pueden ser (o no son) validadas independientemente. Y considerar si las transacciones son intercambiadas electrónicamente con otras entidades sin revisión manual para determinar su exactitud y razonabilidad.

7. La evaluación de la estructura organizacional, las actividades del ambiente SIC del cliente y el grado de concentración o distribución del procesamiento por computadora en toda la entidad, pueden afectar la segregación de funciones; por lo tanto es necesario verificar la disponibilidad de datos, los documentos fuente, los archivos electrónicos SIC y otro material de evidencia, los cuales pueden existir por un corto período de tiempo o sólo en forma legible electrónica.

BIBLIOGRAFÍA

1. ACL Services.—Manual Guía del Usuario.--Vancouver, Canadá: 1998.--125 páginas.

2. American Institute of Accountants.-- Auditoria para Contadores Públicos y Auditores. — Estados Unidos de Norte América.-- 1992.--1020 páginas.

3. Comité Internacional de Práctica de Auditoria.-- Normas Internacionales de Auditoria.-- 1999.—603 páginas.

4. Deloitte, Touche & Tomatsu – Manual de auditoria. – 1997. – 204 páginas.

5. Ernst & Young. — Manual de Auditoria Financiera.--1995. —193 páginas.

6. Holmes, Arthur W.-- Estrategia para la planeación y control empresarial.-- México, Editorial Trillas Mexicana. Casillas, 1990.--Francisco Javier.--Auditoria UTHEA.-- 1991.

7. Kolher, Erick L.-- Diccionario para contadores. —México, 1995, 428 páginas.

8. Koontz, Harold.--Planeación en Administración. —México: McGraw-Hill. —1990.-- 771 páginas.

9. Martínez, Eduardo.—Estrategia, Planificación y Gestión de Ciencia y Tecnología.-- Eduardo Martínez.--Venezuela: Nueva Sociedad, UNESCO/CEPAL/ILPES,1993.-- 518 páginas.

10. Robbins, Stephen P.--Administración Teoría Y Práctica.-- 4a. ed. México: Prentice-Hall, 1994.-- 697 páginas.

11. Saldivar, Antonio.—Planeación Financiera de la Empresa.-- México: Trillas, 1999.-- 3ª. Edición. –- 184 páginas.

12. Instituto Guatemalteco de Contadores Públicos y Auditores. —Guía de Auditoria No. 1 – Conceptos Básicos de Auditoria Interna. —1996. – 5ª. Edición septiembre 2000. – 11 páginas.

Bibliografía electrónica

13. Centro Web -- La mejor información en línea sobre Seguridad informática. --
Selección del equipo editorial de Encarta -- Hispasec -- 1993-2003 -- Microsoft Corporation.

14. Echenique García, José Antonio. AUDITORIA EN INFORMATICA**.** McGRAW-HILL. México. D.F. Enero de 1993.