

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



"AUDITORÍA EN INFORMÁTICA BASADA EN LAS NIA'S APLICABLES A UN AMBIENTE DE SISTEMAS DE INFORMACIÓN POR COMPUTADORA EN LA MEDIANA EMPRESA DEL SECTOR COMERCIO."

TRABAJO DE GRADUACIÓN PRESENTADO POR:

Evelyn Marlene Claros Cruz
José Max Carrillo Montoya
Rafael Antonio Preza Argueta

PARA OPTAR AL GRADO DE
LICENCIADO EN CONTADURÍA PÚBLICA

SEPTIEMBRE 2,005

SAN SALVADOR

EL SALVADOR

CENTROAMÉRICA

AUTORIDADES UNIVERSITARIAS

Rector (a) : Dra. Maria Isabel Rodríguez

**Secretaria General : Licda. Alicia Margarita Rivas de
Recinos**

Facultad de ciencias Económicas

Decano : Lic. Emilio Recinos Fuentes

**Secretario (a) : Licda. Vilma Yolanda Vázquez de
Del Cid**

Docente Director : Lic. Gilberto Díaz Alfaro.

**Docente Observador : Lic. Juan Vicente Alvarado
Rodríguez.**

SEPTIEMBRE 2,005

SAN SALVADOR

EL SALVADOR

CENTROAMÉRICA

ÍNDICE.

Contenido	Pág. N°
RESUMEN	i
INTRODUCCIÓN	iii
I. MARCO TEÓRICO.	1
1.1. Antecedentes.	1
1.1.1. Historia de la Auditoría.	1
1.1.2. Historia del Procesamiento de Datos en un Ambiente de Sistemas de Información por Computadora.	3
1.2. Auditoría.	6
1.2.1. Concepto.	6
1.2.2. Normas de Auditoría.	7
1.2.3. Control de Calidad en la auditoría	10
1.2.4. Requerimientos Éticos de los Contadores Públicos Profesionales. (Auditores).	14
1.2.5. Tipos de Auditoría.	16
1.3. Auditoría en Informática.	20
1.3.1. Concepto.	20
1.3.2. Importancia.	21
1.3.3. Objetivos.	22
1.3.4. Campo de Acción.	22
1.3.5. Metodología de trabajo de la Auditoría en Informática.	25
1.3.5.1. Planeación de la Auditoría.	28
1.3.5.2. Ejecución de la Auditoría.	30
1.3.5.3. Informe Final.	31
1.4. Sistema de Información Por Computadora (SIC).	32
1.4.1. Generalidades.	32
1.4.1.1. Concepto.	32
1.4.1.2. Importancia.	34
1.4.1.3. La seguridad en los SIC.	35
1.4.1.4. Tipos de Sistemas.	38
1.4.2. Los Sistemas Contables en Ambiente Computarizado.	39
1.4.2.1. Concepto.	40
1.4.2.2. Tipos de Procesamiento.	40
1.4.2.3. Análisis de los Sistemas Contables.	42
1.5. Control Interno.	44
1.5.1. Concepto.	44
1.5.2. Principios del control interno.	45
1.5.3. Tipos de Control.	46
1.5.3.1. Control Interno Administrativo.	46
1.5.3.2. Control Interno Contable.	47

Contenido	Pág. N°
1.5.4. Control Interno en Ambiente Computarizado.	47
1.5.4.1. Controles Generales en un Ambiente SIC.	48
1.5.4.2. Controles de Aplicación en un Ambiente SIC.	50
1.6. La Mediana Empresa del Sector Comercio y la Tecnología.	52
1.6.1. Generalidades.	52
1.6.1.1. Antecedentes.	52
1.6.1.2. Definición.	53
1.6.1.3. Clasificación.	53
1.6.2. Situación Actual.	55
1.6.3. La Tecnología en las Empresas.	56
II. DISEÑO METODOLÓGICO Y DIAGNOSTICO.	59
2.1. Tipo de Investigación.	59
2.2. Unidades de Análisis u Observación.	59
2.3. Investigación.	60
2.3.1. Bibliográfica.	60
2.3.2. De Campo.	60
2.4. Universo y Muestra	60
2.4.1. Universo.	60
2.4.2. Muestra.	61
2.5. Instrumentos para recolectar información	64
2.6. Procesamiento	64
2.7. Análisis de la Información.	64
2.8. Diagnostico.	65
III. AUDITORIA EN INFORMÁTICA BASADA EN LAS NIA's APLICABLES A UN AMBIENTE DE SISTEMAS POR COMPUTADORA EN LA MEDIANA EMPRESA DEL SECTOR COMERCIO	69
3.1 Estructura orgánica en un ambiente SIC en la mediana empresa del sector comercio	69
3.2. Modelo de guía de entrevista para la valuación de la estructura orgánica.	73
3.3. Lineamientos de auditoría en informática basados en NIA's	78
3.3.1. La planeación de la auditoría en informática	78
3.3.1.1. Estructura del memorandum de planeación	78
3.3.1.2. Instrumentos para evaluar el control interno	90
3.3.1.2.1. Cuestionario de Recurso humano (usuarios)	91
3.3.1.2.2. Cuestionario de Seguridad lógica.	94
3.3.1.2.3. Cuestionario Seguridad física	95
3.3.1.3. Cuestionario de procesamiento de datos	106
3.3.1.3.1. Cuestionario Entrada de datos	106
3.3.1.3.2. Cuestionario de procesamiento de datos	111
3.3.1.3.3. Cuestionario de salida de información	113

Contenido	Pág. N°
3.3.2. Ejecución de la auditoría en informática	117
3.3.2.1. Programas de validación de auditoría en informática	119
3.3.2.1.1. Recurso Humano	119
3.3.2.1.2. Área Hardware	121
3.3.2.1.3. Área Software	123
3.3.2.1.4. Entrada de datos	125
3.3.2.1.5. Procesamiento de datos (procesos)	127
3.3.2.1.6. Salida de información	131
3.3.3. Informe de Auditoría	131
3.3.3.1. Estructura del informe	131

IV. CONCLUSIONES Y RECOMENDACIONES.	133
4.1 Conclusiones	133
4.2. Recomendaciones	135

Bibliografía	137
---------------------	-----

ANEXOS.

Anexo 1-	Tabulación y análisis
Anexo 2-	Lista de chequeo
Anexo 3-	Matriz de control interno
Anexo 4-	La simulación y diagramación (Flujograma)
Anexo 5-	Programas de cumplimiento de Auditoría en Informática
Anexo 6-	Narrativa
Anexo 7-	Formato para levantamiento de inventario físico de hardware
Anexo 8-	Informe de control interno
Anexo 9-	Tipos de Opinión
Anexo 10-	Ejemplo de resultados de un área auditada
Anexo 11-	Programas de auditoría de facturación e inventario

GLOSARIO

RESUMEN.

La auditoría en informática es un campo relativamente nuevo en lo que respecta a la auditoría en general; por lo que se parte de los antecedentes de la auditoría y se relaciona con el procesamiento de datos en un ambiente de sistemas de información por computadora, así como aspectos generales de la auditoría como: concepto, normas que la rigen, lo referente a la calidad y sobre todo la ética del profesional.

Se destaca la importancia y conceptos de la auditoría en informática, los objetivos que persigue y su campo de acción. Además se plantea la metodología de la auditoría en tres partes: planeación, ejecución e informe; Considerando de base las Normas Internacionales de Auditoría.

Además, lo relativo a los sistemas de información por computadora enfocando los sistemas contables, los tipos de procesamiento y su análisis en la empresa. Se resalta el control interno enmarcado a los sistemas computarizados, considerando los principios del control interno, los tipos de control, entre otros; relacionado a la mediana empresa del sector comercio en El Salvador.

Se plantea la metodología que se considero en el desarrollo de la investigación desde las unidades de observación hasta llegar al diagnostico.

Lo anterior sentó las bases para el aporte relativo a los lineamientos de auditoría en informática basada en las normas internacionales de auditoría aplicables a un ambiente de sistemas de información por computadora, el cual parte de la estructura organizacional para la mediana empresa, un modelo de guía de entrevista y lo relativo a la auditoría en informática partiendo de la planeación y los instrumentos a utilizar, así como la ejecución, sus programas y procedimientos, para finalizar con el informe.

Dando lugar a conclusiones y recomendaciones relativas a la auditoría en informática que permitirán mejorar los controles internos en el área de informática y el procesamiento de información. Además se da como un valor agregado un conjunto de instrumentos adicionales que facilitan el trabajo del auditor.

INTRODUCCIÓN.

En el mundo actual la utilización intensiva de las herramientas ligadas a los sistemas de información y al sector de las telecomunicaciones se introducen cambios importantes en muchas de las actividades típicas de control y auditoría que son propias de la actividad del contador.

En el caso de la auditoría en informática, no es posible si no hay objetivos y criterios bien establecidos sobre las áreas que se evalúan y el conocimiento de la plataforma tecnológica de las operaciones, transferencia de información, redes de comunicación, transferencia de activos de información, las leyes, normas y reglamentaciones sobre estándares internacionales.

Bajo este contexto se desarrollaron lineamientos de auditoría en informática basados en las Normas Internacionales de Auditoría aplicables a un ambiente de sistemas de información por computadora en la mediana empresa del sector comercio. Para tal efecto se presentan a continuación cuatro capítulos.

En el capítulo I, se presenta un marco teórico que involucra aspectos generales sobre la auditoría, su importancia, los tipos de auditoría y la auditoría en un ambiente de sistemas de información por computadora, así como los sistemas computarizados y sus medidas de control.

En el segundo capítulo, se planteó la metodología aplicada en la realización del trabajo de investigación para la recopilación de datos a través de fuentes primarias, utilizando la técnica del cuestionario.

En el tercer capítulo, es la parte medular de la investigación, ya que se ha desarrollado una propuesta de lineamientos de auditoría en informática, enfocados a facilitar la evaluación del control interno en un ambiente de sistemas de información por computadora (SIC) para contribuir a mejorarlos, en la mediana empresa del sector comercio.

Y finalmente, se plasman las conclusiones determinadas con los resultados obtenidos, así como las recomendaciones pertinentes al caso. Además, se incluye un detalle de la

bibliografía consultada y un apartado donde se agregan algunas herramientas adicionales para la evaluación del control interno en un ambiente SIC y programas de validación de algunas áreas.

I. MARCO TEÓRICO.

1.1. ANTECEDENTES.

1.1.1. HISTORÍA DE LA AUDITORÍA.

Existen antecedentes de que alguna especie de auditoría se práctico en tiempos remotos, es casi tan antiguo como la propia historia de la humanidad, el hecho de que los soberanos exigieran el mantenimiento de las cuentas de su residencia por dos escribanos independientes, pone de manifiesto que fueron tomadas algunas medidas para evitar desfalcos en dichas cuentas.

Por ende, a medida que se desarrollo el comercio y en especial el extraordinario desarrollo de la sociedad anónima como forma jurídica de empresa, surgió la necesidad de las revisiones independientes para asegurarse de la adecuación y finalidad de la información contable en relación a la situación patrimonial y económico-financiera.

La auditoría como profesión fue reconocida por primera vez bajo la Ley Británica de Sociedades Anónimas de 1,862; en la cual se establecía que las empresas llevaran un sistema metódico y normalizado de contabilidad para tener una adecuada información y para la prevención del fraude. Esto se concretizó en 1,879 cuando Gran Bretaña impuso a las entidades bancarias la

obligación de someter las cuentas anuales al juicio de un auditor independiente. Otros acontecimientos importantes se dieron en Francia a través de la ley del 24 de julio de 1,867; en Italia mediante la emisión del Código de Comercio de 1,882 en el cual se dio un importante paso en el control de las sociedades mercantiles por auditores independientes.

Desde 1,862 hasta 1,905; la profesión de la auditoría creció y floreció en Inglaterra. En los Estados Unidos de América se introdujo por el año 1,900; esto debido a que muchos contadores públicos o auditores ingleses y escoceses se habían ido a los Estados Unidos para prestar asistencia técnica a los inversionistas británicos, en aquella era de rápida industrialización en dicho país.

En 1,912 Montgomery dijo: en lo que podría llamarse los días en los que se formó la auditoría, a los estudiantes se les enseñaba que los objetivos primordiales de esta eran: la detección y prevención de fraude y la detección y prevención de errores.

En gran parte del siglo XX, los contadores elaboraron sus informes siguiendo muy pocas orientaciones uniformes; sin embargo, a través de AICPA (Instituto Americano de Contadores

Públicos, 1957) la profesión desarrollo un lenguaje común de información contable-financiera.

Para el caso de El Salvador, quizás el punto de mayor trascendencia en el transcurso de los años de la auditoría, fue el 2 de septiembre de 1,999 en el que el Consejo de Vigilancia de la Profesión de la Contaduría Pública y Auditoría acordó establecer que en la realización de auditorías a los Estados Financieros, el auditor debe aplicar las Normas Internacionales de Auditoría dictadas por la Federación Internacional de Contadores (IFAC); el cual lo ratificó el 11 de Diciembre de 2,003.

1.1.2. HISTORÍA DEL PROCESAMIENTO DE DATOS EN UN AMBIENTE DE SISTEMAS DE INFORMACIÓN POR COMPUTADORA.

Los inicios del procesamiento electrónico de datos parten desde que surgió la primera computadora en 1,944; producto de las investigaciones realizadas por Howard Acken, la cual se denominó MARK I, que fue creada para diversos fines de la sociedad. Tal es el caso que en los años cuarenta fueron utilizadas como sistemas de apoyo para estrategias militares. Es importante señalar que la seguridad y control de estos medios se limitaba a

dar custodia física de los equipos y a permitir el uso de los mismos al personal altamente calificado.

Otro aspecto a señalar, es la comercialización de las computadoras electrónicas en el inicio de la década de los 50's, por su estructura tecnológica en el procesamiento de datos y por el impacto que originó en los sistemas de información.

Hacia la década de los 60's, se incorporaron nuevas características en la arquitectura física y lógica de los procesadores, así como en los equipos periféricos de manejo de datos. Esto propició un mayor desarrollo en los sistemas administrativos y operativos de información, lo que dió lugar a un mayor crecimiento y proliferación de sistemas administrativos de información, esto como consecuencia trajo consigo el surgimiento de la necesidad de la función de contraloría en el área de procesamiento de datos de parte de las empresas.

Para la siguiente década, gran cantidad de gerencias y direcciones financiero-administrativas consientes de la capacidad, del valor de solución y apoyo en la toma de decisiones en función del procesamiento de datos (lo cual se empieza a denominar "informática"), hacen que dependan los niveles de la estructura organizativa. Así como también surgen

los sistemas de información en línea y desarrollo de la estructura de la base de datos.

Durante la década de los 80's, se dieron mejoras y refinamientos a los equipos de computo, tal es el caso del surgimiento de un nuevo recurso el "software", lo cual en esencia integra diversas herramientas que culmina con el desarrollo de sistemas de aplicación orientados a sustituir los súper-lenguajes de programación y con ello la labor misma del programador, lo cual llevo a constituir una de las funciones de mayor importancia en el procesamiento electrónico de datos.

Aunado a lo anterior en los últimos años se ha facilitado el acceso a las computadoras debido al bajo costo, así como el surgimiento equipos pequeños. Esto aumento el uso generalizado de las computadoras, y los sistemas de procesamiento electrónico de datos que frecuentemente son mejorados, proporcionando grandes beneficios en el desarrollo de las operaciones de los entes económicos y de otras áreas en general. Es tanto el avance tecnológico que la creación del Internet así como de otros sistemas de información han trascendido su importancia en el procesamiento de datos en las empresas y la unificación de los mercados.

1.2. AUDITORÍA.

1.2.1. CONCEPTO.

La palabra auditoría es originaria del latín "auditorius" y esta proviene de auditor, que tiene la virtud de oír y revisar. Así como del termino ingles "to audit" que significa verificar, inspeccionar. La acepción o significado de dicho término ha experimentado notables cambios en el transcurso del tiempo.

Este pasó de los países latinos al mundo anglosajón y de allí, de Inglaterra a los Estados Unidos de América, principalmente. Luego volvió al mundo latino ya bien avanzado en el siglo XX, para designar la que en los diferentes países se venia denominando censura jurada de cuentas o revisión de contabilidades. Sin embargo, esta acepción del término auditoría ha sido gradualmente ampliado durante las últimas décadas, y hoy en día se puede conceptuar como:

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

¹ KELL Ziegler, Auditoria Moderna, CECSA.

“Es un proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados, con el fin de determinar el grado de correspondencia del contenido informático, con las evidencias que le dieron origen, así como determinar si dicha información se elaboró de acuerdo a principios establecidos para el caso”.²

1.2.2. NORMAS DE AUDITORÍA.

El Consejo de la Federación Internacional de Contadores (IFAC) ha establecido el Comité de Prácticas de Auditoría (AIPC) para desarrollar y emitir a nombre del Consejo, normas internacionales de auditoría (NIA's), con el propósito de ayudar a mejorar el grado de uniformidad de las prácticas de auditoría y servicios relacionados en todo el mundo.

Considerando que los países miembro de la IFAC, deben aplicar las Normas Internacionales de Auditoría dictadas por ésta, así como las revisiones especiales de los procedimientos previamente acordados, las revisiones de control de calidad y servicios relacionados, entre otros. Por ende es necesario que se realicen revisiones a la calidad del trabajo efectuado por los contadores públicos, tal es el caso en El Salvador que existe el Consejo de

² - Asociación Americana de Contadores.

Vigilancia de la Profesión de Contaduría Pública y Auditoría quien tiene esa función.

A continuación se presenta un esquema básico de las normas que deben seguir los profesionales de la auditoría al realizar su trabajo.³

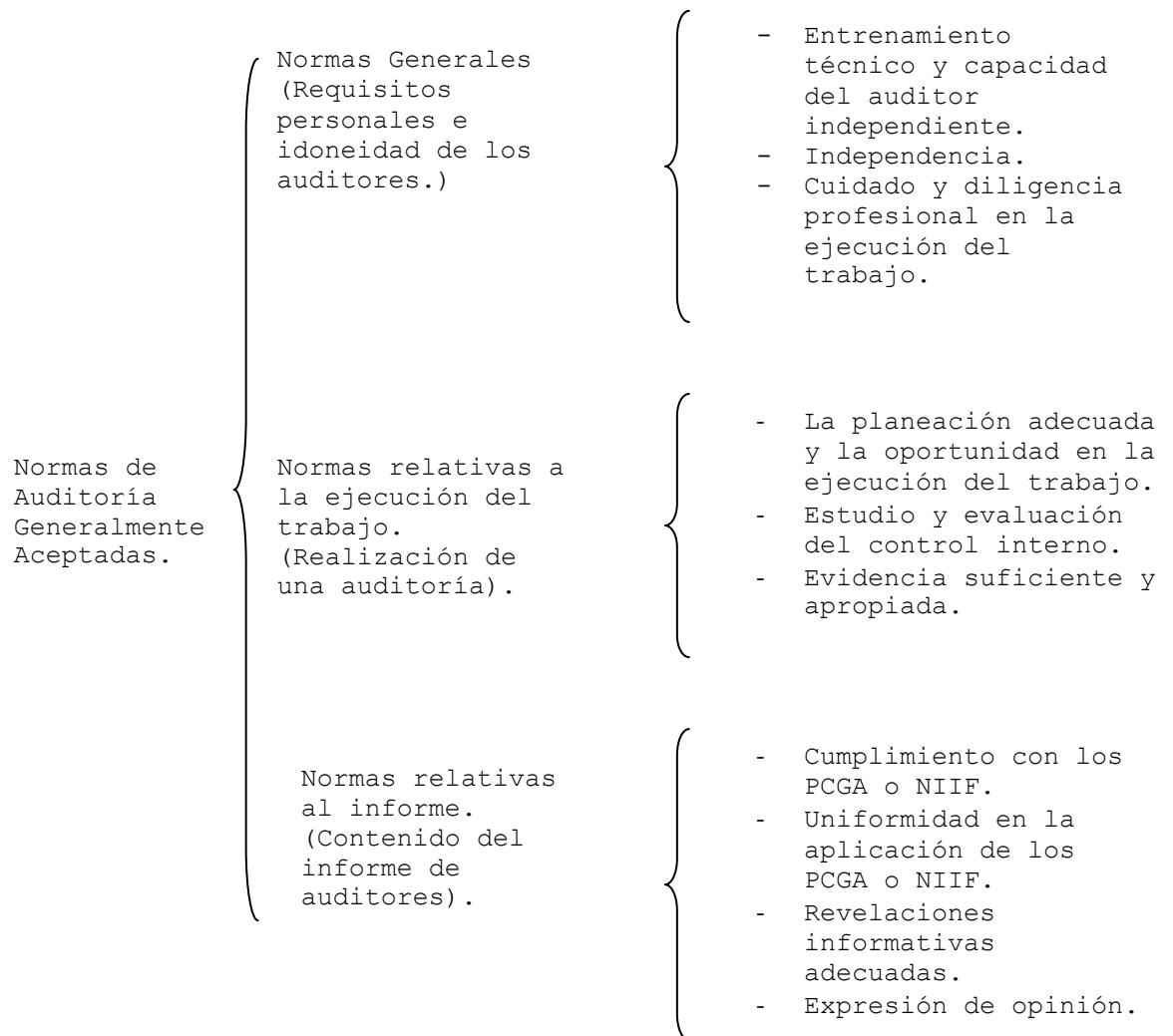


FIGURA 1: Esquema de las Normas de Auditoría Generalmente Aceptadas.

³ Comité Ejecutivo de Normas de Auditoría (AICPA). SAS-01

Las Normas Internacionales de Auditoría (NIA's) deben ser aplicadas, en forma obligatoria, en la auditoría de estados financieros y deben aplicarse también, con la adaptación necesaria, a la auditoría de otra información y de servicios relacionados.

En circunstancias excepcionales, un auditor puede juzgar necesario apartarse de una NIA para lograr en forma más efectiva el objetivo de una auditoría. Cuando tal situación surge, el auditor deberá estar preparado para justificar la desviación.

El contenido de las NIA's se detalla así:

- ✓ Información Introductoria.
- ✓ Asuntos Generales.
- ✓ Planeación.
- ✓ Control Interno.
- ✓ Evidencia de Auditoría.
- ✓ Utilización del Trabajo de Otros.
- ✓ El dictamen de Auditoría.
- ✓ Áreas especializadas.
- ✓ Servicios Relacionados.
- ✓ Declaraciones de Auditoría.

1.2.3. CONTROL DE CALIDAD EN LA AUDITORÍA.

La profesión de la contaduría pública (auditoría) requiere de un monitoreo sistemático y un proceso educacional para obtener una ejecución de alta calidad en la profesión. Por lo que esta debe estar sujeta a una revisión con bases razonables que permita expresar una opinión sobre la competencia necesaria para la realización de los trabajos de contabilidad y auditoría de acuerdo a normas adoptadas por el Consejo de Vigilancia de la profesión de contaduría pública y auditoría.

Para realizar y asegurarse que el personal técnico cumple con los pronunciamientos profesionales aplicables a su práctica, estos deben considerar un sistema de control de calidad con el que se definirá un proceso que provee seguridad de que el personal cumple con los pronunciamientos profesionales y con los estándares de calidad de la firma, y el cumplimiento de los lineamiento del código de ética profesional emitido por la IFAC.

Este sistema de control de calidad debe contener las políticas y procedimientos con respecto al trabajo general de auditoría y los procedimientos a seguir en una auditoría en particular. Estos deben definir la naturaleza, extensión y formalidad en función del tamaño de la firma, y deben implementarse tanto a nivel de la firma como en las auditorías en particular.

En el caso de El Salvador, el auditor deberá cumplir con el código de ética para los contadores profesionales emitidos por la IFAC, en el cual se establecen como principio éticos que gobiernan las responsabilidades del auditor, los siguientes:

- Independencia,
- Integridad,
- Objetividad,
- Competencia profesional y debido cuidado,
- Confidencialidad,
- Conducta profesional, y
- Normas técnicas.

Además, debe conducir las auditorias de acuerdo a Normas Internacionales de Auditoría.

El sistema de control de calidad debe ser responsabilidad de la firma, por lo que debe implementar políticas y procedimientos de control de calidad diseñados para asegurar la calidad del trabajo realizado.

Algo que no debe dejarse de lado, según la NIA's 220 párrafo 7 son, "las políticas y procedimientos generales de control de calidad de la firma deberán comunicarse a su personal en una manera que brinde certidumbre de que las políticas y procedimientos son comprendidos e implementados".

Por lo tanto, dichas políticas y procedimientos deben incorporar los elementos siguientes:

- Requisitos profesionales (Independencia, objetividad e integridad del contador).

En donde la independencia es fundamental y representa un compromiso de imparcialidad no solo con la gerencia y los dueños de la entidad sino con los usuarios de los informes. En el caso de la integridad, se requiere de la honestidad y confidencialidad; y la objetividad es la cualidad que añade valor a los servicios prestados.

- Competencia y habilidad.

El cual debe ser realizado por personal que mantenga los estándares técnicos y la competencia profesional. Además, se deben tener establecidas las políticas y procedimientos que aseguren el cumplimiento del trabajo, así como con los pronunciamientos profesionales y regulaciones legales, y la asignación al personal idóneo.

- Manejo de personal y adiestramiento.

La delegación es un factor determinante en la dirección, supervisión y revisión del trabajo. Este debe cubrir las áreas de contratación, del trabajo y desarrollo profesional,

evaluación y promoción del personal. En lo que se deben de considerar aspectos como: la experiencia y conocimiento técnico, las características éticas, académicas y profesionales, la educación continuada del profesional en seminarios, capacitaciones y otras actividades profesionales.

- Monitoreo y supervisión del control de calidad.

Se debe monitorear la continua adecuación y efectividad operacional de las políticas y procedimientos de control de calidad, la relevancia y competencia de los materiales utilizados, la efectividad de las actividades desarrolladas por el personal y sobre todo el cumplimiento de las políticas y procedimientos de la firma.

- Comunicación.

La comunicación de políticas y procedimientos al personal se debe hacer de tal forma que todos las entiendan y cumplan con ellas. También se debe delinear de qué forma se comunicarán los cambios a esas políticas y procedimientos tan pronto surjan los mismos.

- Documentación.

De alguna manera, se determina que documentación se hará sobre las políticas y procedimientos en consideración del tamaño,

estructura y naturaleza de la práctica de la firma. Aunque la comunicación es mejor por escrito, la efectividad de un sistema de control de calidad no necesariamente se afecta negativamente por la ausencia de un documento escrito.

1.2.4. REQUERIMIENTOS ÉTICOS DE LOS CONTADORES PÚBLICOS PROFESIONALES (AUDITORES).

En la actualidad, la identidad de la profesión contable es importante a nivel mundial debido al papel que los contadores profesionales han desempeñado en los logros de los diversos objetivos que las empresas se han propuesto. Así como de la confianza que han depositado los inversionistas, acreedores, empleadores, gobierno y el público en general, lo que ha influido grandemente en el rol de los profesionales.

Considerando lo anterior, hay una obligación de mantener ese nivel de confianza para seguir ostentando esa posición favorable en el campo profesional, lo cual se ha logrado y se mantendrá a través de la existencia de los requerimientos éticos y la calidad del trabajo.

La IFAC reconoce la importancia y las responsabilidades a la profesión contable y su rol propio; ha dispuesto el proveer de

orientación, fomentando la continuidad de los esfuerzos, promoviendo la armonización de los estándares de desempeño y desenvolvimiento profesional, por lo que ha elaborado un Código de Ética que sea de aplicación internacional y que servirá de base sobre la cual se fundamenten los requerimientos éticos para los contadores profesionales en cada país miembro de la IFAC.

Para el caso de la profesión de auditoría siendo esta una actividad independiente y objetiva del aseguramiento y consulta para generar valor al mejorar las operaciones de una entidad, lo cual ayuda a cumplir con los objetivos y hace un aporte de un enfoque sistemático y disciplinado para evaluar y mejorar la eficiencia de los procesos de gestión del riesgo y control, esta no escapa del alcance de los requerimientos éticos que se establecen en el Código IFAC de ética para Contadores Profesionales.⁴

Este Código, tiene sus fundamentos en los objetivos con los cuales fue creado, es decir que la profesión contable debe de trabajar con los estándares más altos del profesionalismo, con el fin de lograr los mejores niveles de desempeño y generalmente para satisfacción de los requerimientos del interés público.

⁴ Federación Internacional de Contadores. (IFAC) Código de Ética para Contadores Profesionales. Noviembre 2001.

Para lograr dichos objetivos se plantearon satisfacer las necesidades básicas de: la credibilidad, profesionalismo, calidad de los servicios (estándares más altos de desempeño), y la Confianza. En este sentido, los contadores profesionales tienen que observar una cantidad de principios fundamentales (ver 1.2.3. Control de Calidad en la auditoría).

1.2.5. TIPOS DE AUDITORÍA.

Existe una variedad de auditorías en el medio, las que han sido tratadas por varios autores, de los cuales tenemos a O. RAY Whittington; Kurt Pany, e Ignacio Gil Pechuan.

Según, RAY Whittington y Kurt Pany⁵ se pueden agrupar en categorías dentro de las cuales hay una diversidad de tipos de auditoría.

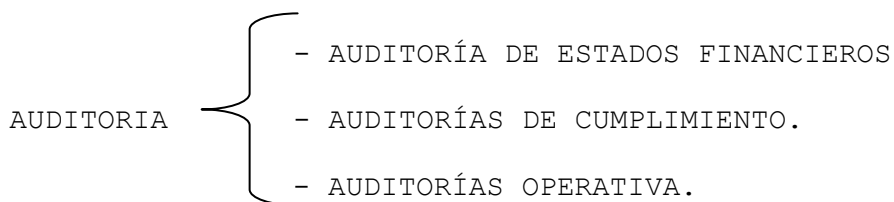


FIGURA 2: Clasificación de la Auditoría en categorías

⁵ O. RAY Whittington; Kurt Pany. Auditoría “un enfoque integral”. 12ª Edición. Mc Graw Hill. Pág. 09

Auditoría de Estados Financieros.

Abarca un examen de los estados financieros de la institución con el fin de expresar una opinión con respecto a si están o no presentados en forma razonable, de conformidad con criterios establecidos; conforme a principios de contabilidad generalmente aceptados o Normas internacionales de Información Financiera. Ejemplos: Auditoría de Estados Financieros, Auditoría por cada uno de los renglones de los Estados Financieros entre otras.

Auditoría de Cumplimiento.

Comprende una revisión de ciertas actividades financieras u operativas de una entidad, con el fin de determinar si se encuentran de conformidad con condiciones, reglas o reglamentos especificados. Ejemplos: Auditoría Fiscal, Auditoría Ambiental entre otras.

Auditoría Operacional.

Involucrar un estudio sistemático de las actividades operativas de una organización en relación con objetivos específicos. También se le conoce como auditoría administrativa o auditoría de resultados; en este tipo de trabajo se espera que el auditor haga una observación objetiva y un análisis completo de operaciones específicas. Esta se centra en la eficiencia,

efectividad y economía de las operaciones. Ejemplos: Auditoría en Informática, Auditoría Administrativa entre otras.

Otra forma de clasificación, Según Ignacio Gil Pechuan en su libro "Sistemas y tecnologías de la Información para la Gestión", es:

- En función de sus objetivos.
- El personal que realice la auditoría.

1- En función de sus objetivos, tenemos:

a) Auditoría Financiera: Aquella auditoría mediante la cual las empresas someten al examen de un experto, su información económico-financiera, al objeto de asegurar su integridad y razonabilidad, en concordancia con los principios de contabilidad generalmente aceptados.

b) Auditoría Organizativa: Aquella auditoría encargada del análisis de la adecuación de los procedimientos establecidos y de las funciones distribuidas físicamente, según las necesidades y problemas de la empresa.

c) Auditoría de Gestión: Su misión fundamental es conocer la consistencia de los principales elementos (decisiones) de gestión en la organización.

d) Auditoría en Informática: Aquella actividad profesional de investigación, evaluación, dictamen y recomendación centrada en las Tecnologías de la Información como actividad o fin en si mismas, como instrumentos al servicio de otras funciones mas o menos dependientes de ellas, o en ambos aspectos.

2- Por el personal que realice la auditoría, esta puede ser:

a) Auditoría Interna: Aquella en la cual el examen es efectuado únicamente por personas que trabajan en la organización objeto de estudio.

b) Auditoría Externa: Aquella que es practicada por personal ajeno (independiente) a la organización objeto de estudio.

1.3. AUDITORÍA EN INFORMÁTICA.

1.3.1. CONCEPTO.

Con el incremento permanente de las expectativas y necesidades relacionadas con la informática, al igual que la actualización continua de los elementos que componen la tecnología, se presenta la necesidad en las empresas que la utilizan de un proceso de contraloría o auditoría en informática con el objetivo de lograr que la información sea más eficiente, confiable y oportuna. A continuación se presentan algunos conceptos para tener una mejor comprensión de lo que es la auditoría en informática.

“Es la revisión y evaluación de los controles, sistemas, procedimientos de informática; de los equipos de computo, su utilización, eficiencia y seguridad, la organización que participa en el procesamiento de la información, a fin de que por medio de señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones”⁶

“Evalúa y verifica políticas, controles, procedimientos y seguridad en los recursos dedicados al manejo de la información”⁷

⁶ ECHENIQUE, José Antonio. “Auditoría en Informática”. Pág. 16

⁷ HERNÁNDEZ Hernández, Enrique. “Auditoría en Informática”. 1ra. Edición. Edit. CECSA. México 1999. Pág. 1

Considerando lo anterior, se puede decir que la auditoría en informática no solo comprende la evaluación de los equipo de computo o de un sistema o procedimiento específico, sino que además evalúa los sistemas de información en general desde sus entradas, procesamientos, comunicación, controles, archivos, seguridad, personal (de desarrollo, operador, usuarios) y obtención de información.

1.3.2. IMPORTANCIA.

Actualmente las empresas incrementan su dependencia de la tecnología y los sistemas de información computarizada, es por ello que este elemento de gestión es cada vez más importante, lo que consecuentemente tendrá más riesgos y la seguridad de activos de información será más vulnerable a los accesos y manipulación tecnológica.

Es en este marco donde se hace necesario la revisión y evaluación de la tecnología de la información, observando su alineación con las estrategias de la organización, el control del aprovechamiento de la tecnología informática y si esta aporta ventajas competitivas, además de la adecuada gestión de los recursos tecnológicos y la seguridad.

1.3.3. OBJETIVOS.

La mayoría de estudiosos en el campo, coinciden en que los objetivos de la auditoría en informática son:

- i. Salvaguardar los activos: Se refiere a la protección del hardware, software y recurso humano.
- ii. Integridad de los datos: Se refiere a que los datos deben mantener consistencia y no duplicarse.
- iii. Efectividad de sistema: Los sistemas deben de cumplir con los objetivos de la organización.
- iv. Eficiencia de los sistemas: Estos son los que deben cumplir los objetivos con los menores recursos.
- v. Seguridad y confidencialidad: En este caso se refiere a la adecuada salvaguarda de los activos, la integridad de los datos, la eficiencia de los sistemas.

1.3.4. CAMPO DE ACCIÓN.

Según lo señala Echenique⁸, el campo de acción de la auditoría en informática considera lo siguiente:

- a) La evaluación administrativa del departamento de informática. Esto comprende la evaluación de:
 - Los objetivos del departamento, dirección o gerencia.

⁸ ECHENIQUE García José Antonio. "Auditoría en Informática". 2da edición. Mc Graw Hill. Pág. 20.

- Metas, planes, políticas y procedimientos de procesos electrónicos estándares.
- La organización del área.
- Las funciones y niveles de autoridad y responsabilidad del área de procesos electrónicos.
- Integración de los recursos materiales y técnicos.
- La dirección
- Los costos y controles presupuestales.
- Controles administrativos del área de procesos electrónicos.

b) Evaluación de los sistemas y procedimientos, y de la eficiencia y eficacia que se tiene en el uso de la información, lo cual comprende:

- Evaluación del análisis de los sistemas y sus diferentes etapas.
- La evaluación del diseño lógico del sistema.
- Evaluación del desarrollo físico del sistema.
- Control de proyectos.
- Control de sistemas y programación.
- Instructivos y documentación.
- Formas de implantación.
- Seguridad física y lógica de los sistemas.

- Confidencialidad de los sistemas.
- Controles de mantenimiento y formas de respaldo de los sistemas.
- La utilización de los sistemas.
- Prevención de factores que puedan causar contingencias; seguros y recuperación en caso de desastre.
- Derechos de autor y secretos industriales.

c) Evaluación del proceso de datos y del equipo de computo que comprende:

- Controles de datos fuentes y manejo de cifras de control.
- Controles de operación.
- Control de salida.
- Control de asignación de trabajo.
- Control de medios de almacenamiento masivos.
- Control de otros elementos de cómputo.
- Control de medios de comunicación.
- Orden en el centro de cómputo.

d) La seguridad comprende:

- Seguridad física y lógica.
- Confidencialidad.

- Respaldos.
- Seguridad del personal.
- Seguros.
- Seguridad en la utilización de los equipos.
- Plan de contingencia y procedimientos de respaldo para casos de desastre.
- Restauración de equipos y de sistemas.

e) Aspectos legales de los sistemas y de la información.

En el caso de El Salvador, el uso de sistemas esta regulado por leyes como la Ley de Fomento y Protección de la Propiedad Intelectual y el reglamento de la misma. Otra ley que en algunos casos tiene influencia sobre los sistemas y la información es la Ley de marcas y otros signos distintivos. Es de considerar que esta dependerá de la legislación nacional de cada país.

1.3.5. METODOLOGÍA DEL TRABAJO DE LA AUDITORÍA EN INFORMÁTICA.

Para la realización del trabajo, el auditor tiene diversas herramientas a su alcance lo que facilita la ejecución del mismo, esto con el objeto de obtener información fiable y que le proporcione confianza en la utilidad de las mismas.

En la auditoría, por orden de mayor importancia y generalidad tenemos; las normas, los procedimientos, las técnicas y las herramientas. En el estudio de los distintos aspectos de un sistema a auditar, se tiene que aplicar los procedimientos de auditoría, que son las descripciones de los pasos que se deben seguir para llevar a cabo el trabajo (la investigación), según la naturaleza del área a auditar o el tipo de auditoría a realizar. Él dispone de una serie de técnicas que le ofrecen diversas alternativas para la evaluación de los elementos específicos a auditar.

Sin embargo, el auditor solamente con su intelecto y sus manos no puede llegar muy lejos en la obtención y elaboración de información, y sobre todo cuando el entorno es muy especializado, tal sería el caso en un ambiente de sistemas de información por computadora. Entonces es acá donde hace falta seleccionar las herramientas adecuadas que faciliten su labor.

Para el caso de que las instalaciones del proceso de datos depende en gran medida del uso de la tecnología, ¿Cómo puede la auditoría en informática realizarse de modo que el auditor obtenga una garantía razonable de que las instalaciones tienen salvaguardado sus activos de procesos de datos, mantiene la

integridad de datos y que los sistemas alcanzan la efectividad y eficiencia esperada? Para responder a esta interrogante es necesario que se considere lo siguiente:

El auditor es un profesional que realiza su trabajo de forma muy distinta a otras profesiones u otros oficios que son individualistas y poco formalizados. Esta persona tiene tras de sí un conjunto de personas que le supervisan, asesoran, organizan, dirigen o ayudan, así como puede a su vez, ejercer estas funciones sobre otros empleados.

El desempeño del auditor, debe estar apoyado por una estructura organizada de profesionales y además, gestionada por los mismos. También puede estar inmersa en el conjunto de funciones de una empresa, como la de auditoría interna. Por otra parte, la auditoría de los sistemas de información por computadora es una parte integral de la auditoría estados financieros, aunque ha emergido con tal fuerza que se diferencia sensiblemente del resto de funciones de auditoría.

Considerando lo anterior, la auditoría es una función de los profesionales en contaduría pública y su ejercicio está sujeto a las NIA's emitidas por la Federación Internacional de Contadores

y adoptadas por el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoría.

Para realizar su trabajo, el auditor debe establecer el proceso de auditoría, el que comprende las etapas de: planeación, ejecución y elaboración de informes. En otras palabras; se inicia con la formulación del respectivo programa o plan global de la auditoría y culmina con la remisión del informe al titular de la entidad o quien requiera dicho trabajo. Para comprender mejor dicho proceso, se desarrolla cada una de las etapas de la auditoría haciendo referencia a la normativa técnica de carácter obligatorio.

1.3.5.1. PLANEACIÓN DE LA AUDITORÍA.

Es el primer paso y el más trascendental, ya que si se tiene una buena planeación del trabajo se obtendrán buenos resultados los cuales satisfacen las exigencias del cliente (alta dirección). Así como la realización de las diversas actividades auditoras de manera efectiva.

De acuerdo a la NIA's 300 párrafo 3, "Planeación" significa desarrollar una estrategia general y un enfoque detallado para la naturaleza, oportunidad y alcance esperado de la auditoría.

En el desarrollo de la planeación el auditor debe desarrollar y documentar de manera adecuada un plan global y los programas de la auditoría, en los cuales debe dejar detalladamente, para el primero; el alcance y conducción esperada de la auditoría; y en el segundo, se debe exponer la naturaleza, oportunidad y el alcance de los procedimientos que se requieren para realizar el plan global de la auditoría.

El auditor debe considerar varios asuntos, para poder establecer y desarrollar el plan global de auditoría, entre estos podemos incluir⁹:

- Conocimiento del cliente;
- Comprensión de los sistemas de contabilidad y de control interno;
- Riesgo e importancia relativa;
- Naturaleza, tiempos, y alcance de los procedimientos;
- Coordinación, dirección, supervisión y revisión; y
- Otros asuntos relevantes a su juicio profesional.

Es importante recalcar que hay muchos factores que para unas entidades son más influyentes que en otras, por ende el auditor

⁹ Federación Internacional de Contadores (IFAC). Normas Internacionales de Auditoría 2001. Pág. 182 y 183.

debe poner en práctica su experiencia y conocimiento para la adecuada planeación de la auditoría y en especial cuando se refiere a una auditoría en informática, en donde debe de considerar el efecto de un ambiente de sistemas de información por computadora (SIC), el cual va a determinar varios puntos muy influyentes en el desarrollo de la misma, de los cuales podrían ser el procesamiento, almacenamiento y comunicación de la información lo que como consecuencia puede afectar los sistemas de contabilidad y de control interno empleado por la entidad.

En este caso según la NIA's 401 párrafo 12,...los métodos de aplicación de procedimientos de auditoría para reunir evidencia pueden ser influenciados por los métodos de procesamiento de la computadora.

1.3.5.2. EJECUCIÓN DE LA AUDITORÍA.

Es la parte práctica de la auditoría, por decirlo así; pero en realidad es el desarrollo de los programas de auditoría que llevan como finalidad el determinar el cumplimiento de los estándares establecidos por la administración y la documentación de la evidencia pertinente. Según la NIA 500 párrafo 2. "el auditor deberá obtener evidencia suficiente apropiada de auditoría para poder extraer conclusiones razonables sobre los cuales basar la opinión de auditoría".

Es aquí donde el auditor deberá considerar la relación entre el costo de obtener evidencia de auditoría y la utilidad de la información obtenida, es donde se necesita de la experiencia profesional, pero lo anterior no justifica la falta de realización de un procedimiento en particular. Para ello el auditor puede hacer uso de los procedimientos de auditoría para obtener evidencia, tales como: inspección, observación, investigación, confirmación, cómputo y análisis. Algo que debe tenerse presente, es que la mayor parte de la evidencia de auditoría es persuasiva y no conclusiva.

1.3.5.3. EL INFORME FINAL.

El dictamen del auditor debe contener una clara expresión de opinión escrita...¹⁰

Esto lo debe realizar el auditor previo análisis y evaluación de la evidencia obtenida en el transcurso del desarrollo de las diversas actividades auditoras, y si hay cumplimiento con respecto a las políticas y procedimientos establecidos por la administración o por alguna normativa ya sean las Normas Internacionales de Información Financiera (NIIF), o prácticas nacionales aceptadas.

¹⁰ Federación Internacional de Contadores (IFAC). Normas Internacionales de Auditoría 2001. NIA´s 700 párrafo 4

El dictamen del auditor debe tener ciertas formalidades, entre estas se tienen algunos elementos básicos, como:

- a) Título.
- b) Destinatario.
- c) Entrada o párrafo introductorio.
- d) Párrafo de alcance (describe la naturaleza de la auditoría).
- e) Párrafo de opinión.
- f) Fecha del dictamen.
- g) Dirección del auditor, y
- h) Firma del auditor.

1.4. SISTEMA DE INFORMACIÓN POR COMPUTADORA (SIC).

1.4.1. GENERALIDADES.

1.4.1.1. CONCEPTO.

El término "sistema" es utilizado ampliamente en diversas actividades de los negocios y en distintas áreas del conocimiento, por ejemplo: los sistemas económicos, sistemas políticos, sistemas de derecho, entre otros. Aproximándonos al término como una herramienta gerencial, hay una diversidad de autores que lo definen entre ellos:

Según Fernando Catacora Carpio, un sistema es: "un conjunto de elementos, entidades o componentes que se caracterizan por ciertos atributos identificables que tienen relación entre sí, y que funcionan para lograr un objetivo común."¹¹

Según O'Brien es: Un grupo de componentes interrelacionados que trabajan en conjunto hacia una meta común mediante la aceptación de entradas y generando salidas en un proceso de transformación organizada.

Este tipo de sistema tiene los tres componentes:

- La entrada comprende la captura y el ensamblaje de elementos que entran al sistema para ser procesados.
- El procesamiento incluye procesos de transformación que convierten las entradas en salidas.
- La salida abarca la transferencia de elementos que han sido generados por un proceso de transformación hasta su destino final.

El concepto de sistema de información computarizado se vuelve aun más útil al incluir dos componentes adicionales:

¹¹ CATACORA Carpio, Fernando. "Sistemas y Procedimientos Contables" Mc Graw Hill. 1999. Pág. 25

- La retroalimentación se refiere a los datos sobre el desempeño de un sistema.
- El monitoreo y la evaluación de la retroalimentación para determinar si un sistema se está desplazando hacia el logro de su meta. Entonces, la función de control realiza los ajustes necesarios a los componentes de procesamiento y entrada de un sistema para garantizar que este genera la salida adecuada.

1.4.1.2. IMPORTANCIA.

En la actualidad y con el constante avance de la informática, los sistemas tienen un papel fundamental en los procesos de generación de información dentro de las empresas, la cual es utilizada por las gerencias para la toma de decisiones ya sean estas de tipo financiero o no financiero.

Este proceso de toma de decisiones se basa necesariamente en la calidad de información generada por los sistemas la cual sirve para el logro de los objetivos de las entidades.

En el caso de los sistemas contables son una herramienta de vital importancia en las entidades, ya que estas necesitan tener

información oportuna, que sea confiable y además que tenga adecuados controles sobre las operaciones y transacciones.

Esto se debe a que los sistemas operativos tienen una relación directa con la parte contable, entre más grande sean las empresas y el grado de sus operaciones mayor será la complejidad que tenga el sistema, lo cual conlleva a tener mayores niveles jerárquicos y una mayor división del trabajo, aunado a esto podemos identificar sistemas basados en las principales actividades y funciones de la empresa.

1.4.1.3. LA SEGURIDAD EN LOS SIC.

Los sistemas de información por computadora proporcionan grandes ventajas sobre el manejo de grandes volúmenes de información y contribuyen a la reducción del tiempo requerido para su procesamiento. Sin embargo estos tienen un alto nivel de riesgo, de los cuales se pueden identificar los principales según lo señala la NIA 401 en el párrafo 7:

- Falta de rastros de las transacciones. Se refiere al riesgo de poder detectar errores en la lógica de programación.
- Procesamiento uniforme de transacciones. Consiste en el riesgo de procesar información incorrectamente.

- Falta de segregación de funciones. En este caso, un número de personas involucradas en el procesamiento es significativamente reducido, lo que facilita que se desempeñen funciones incompatibles por una sola persona.
- Alto potencial de errores e irregularidades. Esto debido a que se puede tener acceso a los datos y programas para ser alterados, ya sea por personal dentro de la empresa o fuera de la misma, como consecuencia de la ausencia de controles adecuados.
- Tecnología cambiante. Aquí el riesgo de esto se enmarca por un lado, el riesgo de que las empresas se mantengan al margen de los adelantos tecnológicos y por el otro, a mayor aplicación de los avances tecnológicos, mayor complejidad.

En el ambiente SIC, la seguridad es un elemento altamente prioritario, debido a que surge como consecuencia de las necesidades de obtener una información confiable, integra y oportuna. Ante esto, es necesaria la implementación de políticas de seguridad las que deben incluir guías, estándares y procedimientos que contribuyan y faciliten el cumplimiento de los objetivos generales de la entidad.

Por ello, es necesario iniciar un proceso coherente que involucre:

- Definición de políticas de seguridad.
- Implantación de las políticas de seguridad.
- Seguimiento de las políticas de seguridad. (monitoreo y modificaciones).

En donde cada una de ellas debe enmarcarse al menos en las siguientes áreas:

- a) Recurso Humano, estas políticas se enmarcan a mejorar el uso y conocimiento de la información, administración del personal, entrenamiento técnico, etc.
- b) Telecomunicaciones y redes, esto contribuye a disminuir el riesgo en el uso de Internet, detectar errores, firewalls y router, etc.
- c) Seguridad Física. Políticas en cuanto a diseño físico, instalación eléctrica, ventilación y aire acondicionado, prevención y daño de datos por fuego y agua, controles de acceso físico, guardia y vigilancia
- d) Seguridad Lógica. Políticas en cuanto a rutas de acceso, claves de acceso, software de control de acceso, encriptamiento.
- e) Protección de datos. Con respecto a la administración de datos, protección de comunicación de los datos, destrucción de datos, etc.

A la vez, es importante señalar que las políticas por si solas no constituyen una garantía para la seguridad de la organización y más aun del área o unidad de informática, ellos deben responder a intereses y necesidades únicas, basadas en la visión y misión del negocio, lo que requiere un esfuerzo conjunto de cada miembro de la entidad.

1.4.1.4. TIPOS DE SISTEMAS.

La información generada por las diversas operaciones que se dan en las empresas son procesadas en su mayoría por sistemas; los cuales tienen como función principal la de soportar las decisiones gerenciales para el logro de sus objetivos. Es importante señalar que el sistema contable es el sistema alrededor del cual giran todos los demás, es decir que los sistemas administrativos (facturación, compras, inventarios, entre otros) están relacionados con el sistema contable el cual recibe la información en forma resumida.

Considerando la relación de los sistemas en función del procesamiento y transferencia de información, se identifican los tipos siguientes:

SISTEMAS INTEGRADOS: Estos implican el compartir información entre dos o más sistemas. Dentro de los cuales debe distinguirse

las etapas de: Definición de parámetros, captura de información, transferencia y controles sobre la transferencia.

SISTEMAS NO INTEGRADOS: A diferencia de los sistemas integrados, la transferencia de información se realiza al final de periodos previamente definidos, y de manera resumida.

SISTEMAS AUXILIARES: Son sistemas distintos al sistema contable, en otras palabras son los que manejan operativa y detalladamente todas las transacciones del negocio.

Es importante señalar que hay una diversidad de operaciones para el procesamiento de datos los cuales implican una serie de controles antes y después de efectuarse el traspaso de información a la base de datos. Esto se ve con mayor grado de complejidad por el avance de la tecnología y sistemas que utilizan las empresas; y surge la necesidad de evaluar y supervisar por medio de la denominada auditoría en informática.

1.4.2. LOS SISTEMAS CONTABLES EN AMBIENTE COMPUTARIZADO.

Para una mejor comprensión del contenido ha desarrollarse se debe considerar antes el concepto de sistema contable como: los métodos y registros establecidos para identificar, resumir,

analizar, clasificar, registrar e informar las transacciones de una entidad.¹²

1.4.2.1. CONCEPTO.

Según las NIA's, existe un sistema de información por computadora cuando esta implicada una computadora de cualquier tamaño en el procesamiento por parte de la entidad de información financiera.

1.4.2.2. TIPOS DE PROCESAMIENTO.

El uso del computador para el procesamiento de datos por parte de las empresas consta de varias actividades tales como: el ingreso, procesamiento, almacenamiento, salida y mantenimiento. Y de estos depende la forma o tipo de procesar los datos, los cuales se pueden clasificar:

- a. Procesamiento en lote (procesamiento en batch).
- b. Procesamiento interactivo (sistema on line o en línea).
- c. Procesamiento mixto.

El primero, es una forma de procesamiento en un sistema de cómputo, que se caracteriza por que las transacciones son agrupadas en lote, donde los datos se acumulan en un lapso de

¹² Declaraciones Sobre Normas Internacionales de Auditoría (AICPA) No. 55 Sección 3, abridle 1,988
Pág138

tiempo y se procesan periódicamente. Este procesamiento incluye:¹³

- a. Reunir en grupos documentos fuentes que se originan de las transacciones.
- b. Grabar los datos en algún medio de entrada.
- c. Ordenar las transacciones en un archivo de transacciones.
- d. Procesar datos de transacciones, crear un archivo maestro y documento e informes.
- e. Capturar y almacenar lotes de datos de transacciones en sitios remotos y luego transmitirlos a un computador central.

Este tipo de procesamiento es conveniente para empresas donde no es necesario actualizar las bases de datos a medida que ocurren las transacciones.

Mientras que el segundo, a diferencia del procesamiento en lote los datos de las transacciones se procesan tan pronto se originan o se registran, sin esperar a que se acumulen. Los datos se ingresan directamente a los sistemas computacionales de las terminales de las transacciones en línea, y siempre se

¹³ O'BRIEN, Op cit. Pág. 434.

almacenan en línea en accesos de archivos directos. El procesamiento en línea incluye:¹⁴

- a. Procesamiento de transacciones a medida que se generan.
- b. Actualización de la base de datos, cuando se procesan las transacciones.
- c. Tiempo de procesamiento, unos cuantos segundos después que se captura cada transacción.

Y el procesamiento mixto es una combinación de ambos.

1.4.2.3. ANÁLISIS DE LOS SISTEMAS CONTABLES.

No se puede dejar de lado el hecho de que la información procesada cumpla con los estándares establecidos por la gerencia para lograr lo anterior surge la necesidad del análisis de sistemas cuyo objetivo principal es verificar el cumplimiento de los estándares en relación al procesamiento de la información contable, este puede ser realizado por una auditoría en informática.

Existen diferentes metodologías dentro de las cuales tenemos: Análisis estructurado, análisis orientado a objetos, entre otros.

¹⁴ O'BRIEN, Ibíd. Pág. 436

Para efectuar el análisis es necesario comprender el funcionamiento de forma general del sistema contable de la empresa en especial de los elementos que interactúan en el mismo para el logro del objeto final. Dentro de estos elementos destacan: El hardware o equipo donde se procesa la información, el software o programas, el recurso humano y las políticas y normas contables adoptadas por la entidad.

Es de hacer notar que la realización de un análisis de sistemas persigue diversos objetivos los que están enfocados a¹⁵:

- Adecuados registros y procesamientos de las operaciones: En este caso las operaciones deben efectuarse de acuerdo a las normas y procedimientos establecidos por la gerencia.
- Asegurar la integridad de los datos: Con la cual se persigue que todas las transacciones que deben ser registradas, lo estén.
- Información financiera confiable: Este persigue que los estados financieros tengan un mínimo grado de confianza de las cifras presentadas y su razonabilidad.

¹⁵ CATACTORA, Op. Cit. Pág. 53

- Garantizar la oportunidad en la presentación de la información: La finalidad de este objetivo es que la información debe ser generada y presentada oportunamente como una herramienta para la toma de decisiones.

En resumen, la contabilidad representa uno de los aspectos más importantes para los negocios y para quienes tienen la tendencia al uso de sistemas para ayudar y mecanizar la diversidad de los procesos contables y administrativos. De ahí la importancia de que los sistemas sean sujetos a supervisión y evaluación.

1.5. CONTROL INTERNO.

1.5.1. CONCEPTO.

“Conjunto de planes métodos y procedimientos adoptados por una organización, con el fin de asegurar que los activos estén debidamente protegidos, que los registros contables son fidedignos y que la actividad de la entidad se desarrolla eficazmente de acuerdo con las políticas trazadas por la gerencia, en función a las metas y objetivos previstos”¹⁶

¹⁶ CEPEDA, Gustavo. “Auditoria y Control Interno”. MC Graw Hill Editores,

1.5.2. PRINCIPIOS DEL CONTROL INTERNO.

Los principios del control interno son¹⁷ :

a) Separación de funciones.

Es necesario tener segregadas las actividades que realizan los empleados de tal manera que no existan funciones compatibles o secuenciales, así las responsabilidades de trabajo deben ser segregadas para que una persona no controle todas las etapas críticas de un proceso. Lo que disminuiría el riesgo de colusión en cuanto a quienes corresponden una u otra tarea en la empresa.

b) Autorización de operaciones.

Considera la conveniencia de que las operaciones de la entidad estén autorizadas por un funcionario competente, de acuerdo a lo señalado por la administración de la empresa dentro de la estructura organizativa previamente definida por esta para tal efecto, así como las funciones asignadas y la responsabilidad adquirida.

c) Documentación comprobatoria.

Establece que toda operación debe contar con el respaldo de la documentación necesario según el tipo de transacción.

¹⁷ SEPARATA DE AUDITORÍA, Ciclo II, 2003, Universidad de El Salvador.

d) Registro.

Se considera el paso esencial para la integración de la información, debido a que se hace necesario de instructivos, políticas, criterios que contribuyan a un mejor registro de las operaciones.

e) Control físico.

Establece la necesidad de salvaguarda de los activos a través de la utilización de equipos y medidas de seguridad.

f) Verificación interna.

Se refiere a la actividad de revisar el trabajo contable para conocer el grado de exactitud y presentación, en el cual puede involucrar personal independiente.

1.5.3. TIPOS DE CONTROL.

1.5.3.1. CONTROL INTERNO ADMINISTRATIVO.

Este tipo de control interno comprende el plan de organización, procedimientos y registros concernientes a los procesos de toma de decisiones que conducen a la autorización de las transacciones por parte de los niveles superiores.

Siendo responsabilidad de este nivel la obtención de los resultados con eficiencia, efectividad y economía, la protección

de los recursos y la revelación de errores o desviaciones son su responsabilidad primordial e indelegable. Por eso estos controles fomentan la eficiencia en las operaciones, la observancia de las políticas, normas prescritas, el logro de las metas y objetivos programados.

1.5.3.2. CONTROL INTERNO CONTABLE.

A diferencia del control interno administrativo este tiene una relación directa con las cifras de los estados financieros de una empresa, ya que a través de su consideración se establecen políticas, procedimientos, métodos y sistemas que contribuyen a obtener información financiera confiable y oportuna.

1.5.4. CONTROL INTERNO EN AMBIENTE COMPUTARIZADO.

Comprende el plan de organización, métodos y procedimientos que se coordinan y adaptan en una entidad para salvaguardar sus activos, prevenir sabotajes, errores e irregularidades, verificar la razonabilidad y confiabilidad de su información financiera, produciendo el cumplimiento de sus políticas.

Considerando las Normas Internacionales de Auditoría en relación al control interno este puede dividirse en: Controles Generales

y de Aplicación. Esta división se establece en la Declaración Internacional de Practica de Auditoría 1008 sobre la Evaluación del Riesgo y el Control Interno en un Ambiente SIC.

1.5.4.1. CONTROLES GENERALES EN UN AMBIENTE SIC.¹⁸

El control interno en un ambiente SIC tiene como objetivo reducir el riesgo asociado a este ambiente. Para contribuir a ello los controles generales establecen un marco de referencia de control global sobre las operaciones para proporcionar un grado de certeza razonable sobre el cumplimiento de estos.

Los controles generales pueden incluir:

- Controles de Organización y Administración.

Considera aspectos en los cuales se relaciona la organización con las actividades del ambiente de información por computadora.

- Políticas y procedimientos relativos a funciones de control.
- Segregación apropiada de las funciones.

- Desarrollo de sistemas de aplicación y controles de mantenimiento.

¹⁸ Federación Internacional de Contadores (IFAC). Normas Internacionales de Auditoría. DIPA. N° 1008. Sexta Edición. Pág. 637.

Establecen una razonable certeza de que los sistemas se desarrollan y mantienen de manera eficiente y autorizada; a través de implementar controles sobre:

- Implementación, conversión, pruebas y documentación de sistemas nuevos y usados.
- Cambios a sistemas de aplicación.
- Acceso a documentación de sistemas.
- Adquisición de sistemas de aplicación con terceros.

▪ Controles de operación de computadoras.

Señala la necesidad de establecer controles para tener certeza razonable de que el tipo de operación de los sistemas es:

- Para propósitos autorizados.
- El acceso a la información de la computadora es restringido.
- El uso de programas autorizados.
- Los errores de procesamientos son detectados y corregidos.

▪ Controles de software de sistemas.

Considera la conveniencia de implementar medidas que proporcionen razonable certeza de que el software del sistema se adquiere y desarrolla de manera establecida y eficiente en lo referente a:

- La autorización, aprobación, pruebas, implementación y documentación de software(s) nuevo(s) y modificado(s).
- Restricciones de acceso a software a personal no autorizado.

- Controles de entrada de datos y de programas

Estos controles tratan de disminuir el riesgo a través del establecimiento de una estructura de autorización sobre las transacciones que alimentan al sistema. Así como también, limitar el acceso a datos y programas a personal autorizado.

Además de los controles anteriores existen medidas de salvaguarda los cuales también contribuyen a la continuidad del procesamiento de datos en un ambiente SIC.

1.5.4.2. CONTROLES DE APLICACIÓN EN UN AMBIENTE SIC.¹⁹

Los controles generales tratan de establecer medidas de seguridad en toda la entidad, tratando de conseguir un ambiente propicio para implementar los controles de aplicación, los cuales establecen procedimientos específicos de control sobre las aplicaciones contables, los cuales son:

¹⁹ Federación Internacional de Contadores (IFAC). *Ibíd.* Pág. 638

- Controles sobre datos de entrada.

Estos controles se enmarcan desde establecer la autorización para procesar por la computadora las transacciones, su integridad, exactitud de los datos ingresados hasta rechazarlos al faltar cuando sea necesario, y volverlos a establecer oportunamente.

- Controles sobre el procesamiento y sobre archivos de datos de la computadora.

Incluye aquellos controles que le permiten a la empresa conocer si se procesan las transacciones por la computadora en forma congruente, así como también si estos no son perdidos, añadidos, duplicados o combinación inapropiada; de tal manera que facilite identificar estas anomalías y corregirlas oportunamente.

- Controles sobre los datos de salida.

Son diseñados para lograr obtener al final del procesamiento de los datos resultados exactos así como también restringirle el acceso a personal autorizado y finalmente que pueda servir oportunamente para la toma de decisiones.

1.6. LA MEDIANA EMPRESA DEL SECTOR COMERCIO Y LA TECNOLOGÍA.

1.6.1. GENERALIDADES.

1.6.1.1. ANTECEDENTES.

La situación de la mediana empresa en El Salvador ha sido afectada por una serie de situaciones, las cuales han influido de diversas formas en el que hacer de su participación en la economía, de las cuales se puede señalar:

- En la década de los 70's la crisis política existente, contribuyo al debilitamiento económico lo que trajo como consecuencia la falta de apoyo crediticio, bajo nivel de inversión, etc.

- A partir de la década de los 80's, debido al conflicto armado se encontraba en pleno apogeo, se dio la fuga de capital hacia el extranjero, lo que implico a la mediana empresa en parte a tener una mayor participación.

- A inicios de los 90's, después de los acuerdos de paz se incremento el apoyo a este sector, por parte de instituciones financieras nacionales e internacionales. Por otro lado se ven afectados por la creación de marcos legales que los obliga a cumplir una serie de obligaciones,

tal es el caso de la ley impuesto a la transferencia de bienes muebles y prestación de servicios.

En esa tendencia histórica, la mediana empresa logra incorporarse al uso de la tecnología de la información y al comercio electrónico a finales de los 90's; según conferencia de las Naciones Unidas sobre el comercio y desarrollo del año 2,000.

1.6.1.2. DEFINICIÓN.

La empresa mercantil "esta constituida por un conjunto coordinado de trabajo, de elementos materiales y de valores incorpóreos, con objeto de ofrecer al publico, con propósito de lucro y de manera sistemática, de bienes o servicios".²⁰

1.6.1.3. CLASIFICACIÓN.

Las empresas pueden ser clasificadas de acuerdo a varios criterios, entre los cuales pueden citarse el tipo de actividad a que se dedica y su tamaño.

- Clasificación de acuerdo a la actividad que realiza.

- ✓ Extractivas. - Renovables
- No renovables

²⁰ Código de Comercio DL N° 671, del 8 mayo de 1970. DO N° 140, Tomo 228, del 31 de julio de 1970.

- ✓ Transformación.
- ✓ Comercio.
- ✓ Transporte.
- ✓ Otros servicios públicos.
- ✓ Créditos, seguros y fianzas.

- Clasificación de acuerdo al tamaño de la empresa.

- ✓ Microempresa.
- ✓ Pequeña empresa.
- ✓ Mediana empresa.
- ✓ Gran empresa.

Algunas instituciones clasifican a estas, de la siguiente manera:

Institución	Pequeña	Mediana	Grande
PROPEMI	De 10 a 49 empleados y ventas mensuales menores de \$ 57,142	De 50 a 100 empleados con ventas mensuales de \$ 114,285	
FUNDAMYPE	De 5 a 49 empleados.	De 50 a 99 empleados	
CONAMYPE	Hasta 50 empleados y ventas de \$ 5,714 hasta \$ 57,142		
FUSADES	De 11 a 19 empleados, cuyo activo total no excede los \$ 85,714.29	De 20 a 99 empleados, cuyo activo total no excede los \$ 228,571.43	De 100 o más empleados, cuyo activo total sea mayor a \$ 228,571.43

Fuente: Elaboración propia en base a datos de DIGESTYC.

1.6.2. SITUACIÓN ACTUAL.

La actividad (económica) de las medianas empresas se encuentra representada en diferentes aspectos de los cuales tenemos:

- Económico.

Una variable de importancia en la economía es el producto interno bruto (PIB), del cual se estima que las PYMES aportan el 45%, según datos del Ministerio de Economía.

- Social.

En la actualidad la población salvadoreña siguen preocupados por el desempleo, situación que demanda fuentes generadoras de empleo, una opción viable lo representan las PYMES. Ante ello estas empresas, según datos de FUNDAMYPE representan una población ocupada del 32.9%. (Programa entorno 2002, FUSADES).

- Tecnológico.

En el campo tecnológico, experimentado un avance en las áreas de tecnología de la información y conocimiento, ya que el indicador de tecnología e innovación ascendió a 67 para el año 2,003 según lo señala ANEP.

1.6.3. LA TECNOLOGÍA EN LAS EMPRESAS.

Actualmente la tecnología de la información ha pasado a ser una necesidad en el que hacer empresarial, esta debido a la dinámica a la que están sometidas las empresas por la competitividad internacional, ya que la adopción de mas acuerdos internacionales de comercio aumentan las exigencias en el mercado.

De manera complementaria a lo antes señalado, a continuación tenemos algunos aspectos que contribuyen a la tecnología de la información en las empresas:

1. La amplia disponibilidad de potentes pero económicos equipos informáticos.
2. La amplia disponibilidad de programas potentes, económicos, y relativamente sencillos de usar con interfaces de usuario graficas.
3. A la medida del cliente, cambio de sistemas a software preempacados.
4. El paso de grandes equipos centralizados o mainframes a ordenadores personales, utilizados solos o como parte de redes.
5. La disponibilidad creciente de datos informáticos a los que se accede en tiempo real o diferido, mediante acceso local o remoto, incluido vía Internet.

6. Las nuevas tecnologías de captura de datos y almacenamiento llevan a los datos e información en formato de texto, gráficos, audio y video y enfatiza el gestionar, presentar y comunicar información presentado técnicas multimedia.
7. La convergencia de las tecnologías de la información y la comunicación que afectan a como las personas trabajan y compran.
8. El uso creciente de redes que conectan a los individuos y a las empresas (intraempresas e interempresas) con sistemas como el correo electrónico e Internet, incluyendo el World Wide Web.
9. El uso creciente de Internet para el comercio entre empresas y la venta de productos finales a un consumidor vía sistemas de comercio electrónico como el intercambio electrónico de datos (EDI) y de transferencia electrónica de fondos (EFTS)

El Salvador no ha sido la excepción, en lo referente a la tecnología de la información, ya que en el año 2,003, según encuesta de FUSADES las medianas empresas forman el 38.6% en realizar actividades realizan de desarrollo tecnológico; esto debido a que el país experimentando un avance en las áreas de tecnología de la información.

En este contexto, el nivel de riesgo en el procesamiento de datos se ve incrementado, lo que exige medidas de control que contribuyan a disminuirlo. Así como también aprovechar los beneficios que ofrece la auditoría con informática.

Es de esta manera como la mediana empresa va a aprovechar los beneficios que ofrece lo sistemas de información por computadora, y así pueda contar con información de calidad que contribuyan a tomar mejores ediciones para las empresas.

II. DISEÑO METODOLÓGICO Y DIAGNOSTICO.

2.1 TIPO DE INVESTIGACIÓN.

En cuanto al nivel de investigación, esta se realizó en forma Descriptiva ya que se pretende conocer las Normas Internacionales de Auditoría y el procesamiento de datos en un ambiente de Sistemas de Información por Computadora en el departamento de Informática de la Mediana Empresa del Sector Comercio.

Además, se considera analítico, porque se analizó los resultados obtenidos en la investigación de campo, lo cual permitió hacer un diagnóstico sobre los controles internos y su evaluación en un Sistema de Información por Computadora a fin de proponer mejoras en base a lo que establece las Normas Internacionales de Auditoria.

2.2. UNIDADES DE ANÁLISIS U OBSERVACIÓN.

Las unidades de análisis u observación lo comprendieron el jefe o encargado del Departamento de Informática del cual se obtuvo la información relacionada a los controles internos existentes en el Procesamiento de datos en la Mediana empresa del Sector Comercio en el Área Metropolitana de San Salvador.

2.3 INVESTIGACIÓN.

2.3.1 BIBLIOGRÁFICA.

Se utilizó la técnica que permitió recopilar información sobre los antecedentes y la situación del objeto de estudio conocida como "Sistematización Bibliográfica". Por medio de la cual se recopiló, analizó y clasificó toda la información investigada en libros de texto, Normas, trabajos de graduación y además direcciones en Internet relacionadas con el tema objeto de estudio.

2.3.2 DE CAMPO.

Para la investigación de campo, se utilizó la técnica de cuestionario dirigida al jefe del departamento de informática o encargado del mismo. En la que se hicieron preguntas abiertas y cerradas necesarias para obtener datos que permitieron realizar un diagnóstico.

2.4 UNIVERSO Y MUESTRA.

2.4.1 UNIVERSO.

El universo de la investigación lo constituyeron las Medianas Empresas del Sector Comercio que se caracterizan por procesar su información en un ambiente de sistemas de información por computadora en El Salvador.

2.4.2 MUESTRA.

La población comprendió la Mediana Empresa del sector comercio ubicado en el área Metropolitana de San Salvador. La cantidad de estas fue determinada en base al número de empresas establecidas en el área metropolitana; dicha información fue suministrada por la Dirección General de Estadísticas y Censo, y clasificada como mediana empresa según los parámetros definidos por la Comisión Nacional para la Micro y Pequeña Empresa (CONAMYPE), a la vez se consideró las empresas que se caracterizan por tener un procesamiento de datos por medio de sistemas computarizados, lo cual dio un total de 106.

De estas, la muestra se obtuvo por medio de la fórmula siguiente:

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

En donde:

M : Muestra a obtener al sustituir valores y efectuar las operaciones respectivas.

Z : Valor crítico que corresponde a un coeficiente de confianza del 90% donde Z Es 1.64 de acuerdo al área bajo la curva normal.

P : Proporción poblacional de empresas que procesan información en un ambiente SIC, el porcentaje determinado según prueba piloto es 63%.

Q : Proporción poblacional de empresas que no procesan información en un ambiente SIC, el porcentaje determinado según prueba piloto es 37%.

N : Total de medianas empresas del sector comercio en el área metropolitana de San Salvador.

E : Error muestral, donde E es 10%.

Sustituyendo valores en la formula:

$$M = \frac{(1.64)^2 (0.63) (0.37) (106)}{(106-1) (0.10)^2 + (1.64)^2 (0.63) (0.37)}$$

$$M = \frac{66.4562506}{1.05 + 0.62694576}$$

$$M = \frac{66.4562506}{1.67694576}$$

$$M = 39.6293381$$

$$M = 40$$

Desarrollando la fórmula se determinó que la muestra es de aproximadamente 40 empresas.

Como el tamaño de la muestra se consideró muy grande, se procedió a disminuir el tamaño de la muestra mediante la siguiente fórmula estadística:

$$n = n_0 / (1 + (n_0 - 1) / N)$$

Donde:

n = Muestra calculada.

n₀ = Muestra inicial, que es la muestra calculada anteriormente.

N = Total de la población.

Sustituyendo:

$$n = 40 / (1 + (40 - 1) / 106)$$

$$n = 40 / 1.36792453$$

$$n = 29.2413793$$

$$n = 29$$

Así, la muestra fue de 29 empresas.

2.5. INSTRUMENTOS PARA RECOLECTAR INFORMACIÓN.

El instrumento de investigación que se utilizó fue: El Cuestionario.

El Cuestionario: El cual contiene preguntas abiertas y cerradas para el jefe del Departamento o encargado de informática; lo cual permitió conocer el control interno existente, áreas de riesgo, su supervisión y el ambiente de control en el procesamiento de datos en un ambiente SIC.

2.6. PROCESAMIENTO.

La información recolectada se procesó por medio del paquete computacional Excel, mediante una aplicación de este diseñada para la tabulación de datos, la elaboración de gráficas y la relación de variables.

En cuanto al análisis de la información se hizo por medio de los datos obtenidos en el cuestionario, referentes ha: control interno existente, áreas de riesgo y supervisión en el procesamiento de datos en un ambiente SIC, que facilitó la elaboración del diagnóstico acerca de su situación actual.

2.7. ANÁLISIS DE LA INFORMACIÓN.

Realizado el procesamiento de los datos, se determinó el análisis de la información que permitió realizar un estudio de

los sistemas de información por computadora y su control interno, así como la supervisión y monitoreo del mismo, que en conjunto sirvió para elaborar el diagnóstico de las medianas empresas del sector comercio que procesan sus datos en un ambiente SIC.

2.8. DIAGNOSTICO.

Teniendo en consideración los resultados obtenidos en las encuestas pasadas se presenta los siguientes resultados:

- Los sistemas de información por computadora utilizados actualmente por la mediana empresa del sector comercio tienden a aumentar su complejidad.
- Para la preparación de manuales de usuarios y de funciones en el área de informática no se ha tenido un consenso coordinado entre la administración y él (los) responsable(s) del área o unidad de informática.
- De alguna manera las empresas tienen algún tipo de control diseñado para monitorear los cambios que se realizan en el sistema.

- En la mayoría de las medianas empresas del sector comercio, con respecto a la detección de errores, poseen pocos controles en las diversas etapas del procesamiento de datos.
- Para realizar cambios y modificaciones a la información procesada por el sistema en la mediana empresa, estas en cierta medida han utilizado algún tipo de procedimiento limitado y además no se encuentra documentado.
- En relación a los controles generales alrededor del procesamiento de datos para su posterior emisión de reportes de información financiero-contable, en su mayoría son limitados y no permiten disminuir el riesgo de los problemas ocasionados por el personal interno o personas ajenas a la empresa.
- Las empresas no poseen controles adecuados o suficientes que permitan supervisar o monitorear la salida de información contable o financiera de las instalaciones de la empresa.
- La mayoría de empresas del sector comercio no tienen diseñados medida contingenciales de seguridad.

- Con respecto a las políticas y procedimientos internos relativos al procesamiento de datos en el área o unidad de informática, estas empresas no los tienen definidos mucho menos documentados.

- En su mayoría las medianas empresas que procesan información por computadora poseen pocos controles en la entrada de datos al sistema computarizado.

- La mediana empresa del sector comercio se limita a utilizar controles manuales para determinar la confiabilidad y oportunidad de los informes financiero-contables.

- El recurso humano relacionado con el manejo de la aplicación a través de los programas no están suficientemente capacitados en el procesamiento de datos.

- En su mayoría las empresas no tienen una herramienta que le permita estudiar e identificar las posibles amenazas a las que esta expuesta el área o unidad de informática.

- En el área o unidad de informática de las medianas empresas del sector comercio, conocen muy poco en que consiste la auditoría en informática.

En resumen, las medianas empresas que procesan la información por sistemas de información por computadora no están preparadas adecuadamente para el uso de la tecnología, ya que estas han decidido incluir el uso de sistemas computarizados por el simple hecho de que les permite acelerar el procesamiento de datos y la consecuente emisión de información.

Y descuidan los controles internos del procesamiento de datos ya que no consideran monitorearlos periódicamente para su posterior modificación, diseño o reestructuración de los mismos.

III. AUDITORÍA EN INFORMÁTICA BASADA EN LAS NORMAS INTERNACIONALES DE AUDITORÍA APLICABLES A UN AMBIENTE DE SISTEMAS DE INFORMACIÓN POR COMPUTADORA EN LA MEDIANA EMPRESA DEL SECTOR COMERCIO.

3.1. ESTRUCTURA ORGÁNICA EN UN AMBIENTE DE SISTEMAS DE INFORMACIÓN POR COMPUTADORA EN LA MEDIANA EMPRESA DEL SECTOR COMERCIO.

Antes de entrar en materia de los lineamientos de auditoría en informática es importante tomar en cuenta la estructura orgánica del ambiente de sistemas de información por computadora, ya que representa un elemento que indicara el grado de complejidad y organización de la entidad, conocimiento necesario según la NIA 310 "Conocimiento del negocio"

Para lograr la evaluación de la estructura orgánica se deberá solicitar el manual de organización de la dirección, en el cual se deberá comprender, como mínimo:

- Organigrama con jerarquías.

- Funciones.
- Objetivos y políticas.
- Análisis, descripción y evaluación de pruebas.
- Manual de normas.
- Instructivos de trabajo o guías de actividad.

También se debe obtener y revisar:

- Los objetivos de la dirección enfocadas al área de informática.
- Políticas y normas de la dirección enfocadas al área de informática.
- Planeación.

El departamento o unidad de informática depende de la gerencia general; esto puede ser en línea o bien en forma de asesoría.

La ventaja de esta organización es que el director de informática podrá tener un nivel adecuado dentro de la organización, lo cual le permitirá lograr una mejor comunicación con los departamentos usuarios, y por lo tanto, proporcionales un mejor servicio y asignar las prioridades de acuerdo con los lineamientos dados por la gerencia general.(ver figura 1)

La desventaja es que aumenta los niveles de organización, lo que eleva el costo de utilización de los sistemas de cómputo.

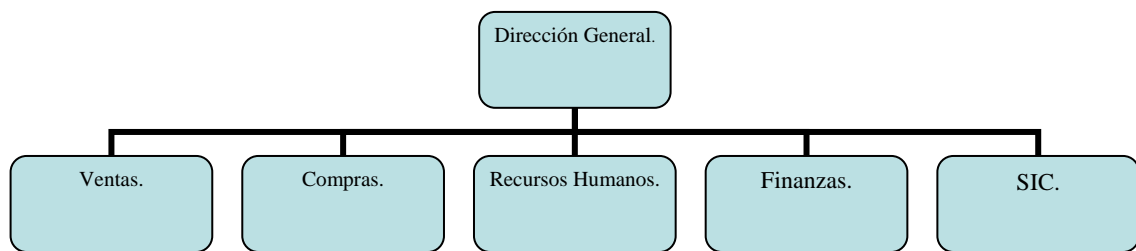


FIGURA 1: Ubicación en línea.

Cabe la posibilidad de que el departamento de informática dependa de otros niveles administrativos dentro de los cuales podemos citar:

- a) Depende de alguna dirección o gerencia, la cual normalmente es la dirección de finanzas. Esto se debe a que inicialmente informática o departamento de procesamiento electrónico de datos procesa principalmente información de tipo contable, financiero o administrativo.

La ventaja que tiene, es que no se crea una estructura adicional para el área o unidad de informática y permite

que el usuario principal tenga un mayor control sobre los sistemas.

La desventaja es que los otros usuarios son considerados como secundarios y normalmente no se les da la importancia y prioridad requerida, así como existe una acumulación de funciones en un solo usuario.

Este tipo de organización se usaba cuando inició el área de informática, y en la actualidad solo es recomendable para instalaciones muy pequeñas.

- b) Una segunda posibilidad es para estructuras muy grandes, en las que hay bases de datos, redes o bien equipos en diferentes lugares. En esta estructura se considera la administración corporativa. La dirección de informática depende de la gerencia general, y existen departamentos de informática dentro de las demás gerencias, las cuales reciben todas las normas, políticas, procedimientos y estándares de la dirección de informática, aunque funcionalmente dependan de la gerencia a la cual están adscritas.

La ventaja principal de esta organización consiste en que se puede tener centralizada la información (base de datos)

y descentralizados los equipos; pero se debe tener una adecuada coordinación entre la dirección de informática y los departamentos de informática de las áreas usuarias para evitar duplicar esfuerzos o la duplicidad de mando. La desventaja principal de este tipo de organizaciones es el alto costo por el mantenimiento de dichas áreas.

- c) La tercera forma de organización es la creación de una compañía independiente que de servicio de informática a la organización.

Considerando las características de las medianas empresas y su estructura organizativa permitirán al auditor tener un mejor panorama que le facilitara la planeación de una auditoría en informática en este tipo de empresas. Para lo cual se destaran algunos lineamientos que permitirán la realización de dicho trabajo.

3.2. MODELO DE GUÍA DE ENTREVISTA PARA LA EVALUACIÓN DE LA ESTRUCTURA ORGÁNICA.

La entrevista es una de las fuentes de información mas importantes par saber como opera un sistema. Aunque no siempre tiene la efectividad que se desea, ya que en ocasiones las

personas entrevistadas pueden ser presionadas por los entrevistadores, o piensan que si se hacen algunos cambios, estos podrían afectar sus trabajos.

Esta herramienta es con la que se debe iniciar la auditoría ya que permitirá obtener los primeros conocimientos del cliente. Esta se debe pasar al encargado de informática así como a los usuarios en el momento oportuno. Y con los datos obtenidos el auditor debe hacer una interpretación o lectura.

MODELO DE ENTREVISTA.

Nombre de la firma de auditoría	
Nombre del cliente _____	Periodo auditado _____ Elaborado por: _____
Entrevistado	:
Nombre del puesto	:
Puesto del jefe inmediato	:
Fecha	:
<p>Objetivo.</p> <p>Conocer los aspectos generales y específicos relativos a la organización, administración y la dirección de la entidad y la relación con la unidad de informática.</p>	
<p>1.- Se ajusta la estructura orgánica actual a las disposiciones vigentes. Preguntar por que si o no.</p> <p>2.- La estructura actual esta encaminada a la consecución de los objetivos del área. Indagar en que forma.</p> <p>3.- Pedir explicación sobre si permite la estructura actual que se lleven a cabo con eficiencia:</p> <ul style="list-style-type: none">* Las atribuciones encomendadas* Las funciones establecidas* La distribución del trabajo* El control interno	

4.- Permiten los niveles jerárquicos actuales que se desarrolle adecuadamente la:

- * Operación

Nombre de la firma de auditoría

- * Supervisión

- * Control

5.- Permiten los niveles actuales que se tenga una ágil:

- * Comunicación ascendente
- * Comunicación descendente
- * Toma de decisiones

6.- El área y sus sub-áreas de la unidad de informática tienen delimitadas con claridad sus responsabilidades

7.- Existen los manuales de:

- * Análisis.
- * Programación.
- * Técnicos.
- * Operación.
- * Captura.
- * Administrador de bases de datos.
- * Comunicación y redes.
- * Dirección.
- * Administrativos.
- * Otros.

8.- Considera que debe revisarse la estructura actual, a fin de hacerla mas eficiente.

9.- Su autoridad va de acuerdo a su responsabilidad

Nombre de la firma de auditoría

10.- Existe en el área algún sistema de sugerencias y quejas por parte del personal

11.- Se han establecido funciones del área

12.- Quién elaboro las funciones

13.- Participo el área de informática en su formulación

14.- Las funciones están encaminadas a la consecución de los objetivos institucionales e internos

15.- Están delimitadas las funciones

16.- Las actividades que realiza el personal son acordes a las funciones que tiene asignadas

17.- La falta de cumplimiento de sus funciones es por:

- * Falta de personal
- * Personal no capacitado
- * Carga de trabajo excesivo
- * Por que realiza otras actividades
- * La forma en que las ordena

18.- Tiene programas y tareas encomendadas

19.- Existe duplicidad de funciones en la misma área

20.- Se pueden transferir funciones

3.3. LINEAMIENTOS DE AUDITORÍA EN INFORMÁTICA BASADOS EN NIA's.

3.3.1. LA PLANEACIÓN DE LA AUDITORÍA EN INFORMÁTICA.

3.3.1.1. ESTRUCTURA DEL MEMORANDUM DE PLANEACIÓN.

En este apartado se detallara cada elemento que forma parte integrante del memorandum de planeación apegado a los aspectos que la Normas Internacionales de Auditoría considera importantes:

- Identificación del alcance y Objetivo de la auditoría.

Es de hacer notar que el alcance y los objetivos de la auditoría no cambian en un ambiente SIC. Por ende, para realizar un buen trabajo se debe conocer el entorno y los limites que se tendrán al realizar la auditoría.

Además debe comprenderse con exactitud los deseos y pretensiones del cliente (alta dirección) para poder cumplir con los diversos objetivos que previamente se ha trazado y hasta donde se pretende llegar.

En el caso de la auditoría en informática estos dependen del tipo o área a auditar aunque en el fondo siempre se persigue dar cumplimiento a los objetivos generales de la auditoría, por ejemplo:

Objetivo General.

- Operatividad de los sistemas informativos.
- Controles generales de gestión.
- Seguridad de la tecnología y de los sistemas de información.

Objetivos Específicos:

- Evaluación del funcionamiento de áreas informáticas;
- Aumento de seguridad física y lógica;
- Disminución de costes o plazos;
- Planificación y organización de sistemas;
- Plan de contingencia y su documentación;
- Origen, captura y validación de datos;
- Procesamiento y actualización de datos;
- Utilización y control de resultado;
- Entre otros.

En resumen, en el desarrollo de la auditoría en informática, la seguridad de información es el objetivo fundamental, ya que en esta auditoría se comprueban los objetivos de control sobre las políticas y organización de la seguridad física y lógica, el desarrollo de aplicaciones, la seguridad de los datos, las comunicaciones y redes, la continuidad de las operaciones todo esto para evaluar y opinar sobre la integridad de los activos, humanos, lógicos y materiales; y plantear las medidas que minimizan el riesgo de fallas antes, durante y después de los procesos de información²¹.

- Conocimiento del entorno a auditar

Según NIA's 310 párrafo 2, "... el auditor debería tener u obtener un conocimiento suficiente del negocio para que sea posible al auditor identificar y comprender los eventos, transacciones y políticas, que a juicio del mismo pueda tener un efecto importante sobre..."

Siempre enmarcándonos en un ambiente SIC, en la medida en que las empresas incrementan su dependencia en el uso de la tecnología y de los sistemas de información computarizados; este elemento de gestión será cada vez más importante ya que tendrá

²¹ Tomo III. Panamá 2003. Pág. 1647.

más riesgos y la seguridad de que los activos de información serán más vulnerables a los accesos y manipulación tecnológica.

Por lo cual, es importante que el auditor obtenga el conocimiento suficiente y que lo actualice continuamente, ya que este es un marco de referencia que le permitirá ejercer su juicio profesional y usar adecuadamente la información, la que ayudara a:

- a. Evaluar el riesgo e identificar los problemas;
- b. Planear y desempeñar la auditoría en forma efectiva y eficiente;
- c. Evaluar evidencia de auditoría; y
- d. Proporcionar mejor servicio.

Otro punto de importancia, es lo que establece la NIA's 400 párrafo 4; "El auditor debería tener suficiente conocimiento del SIC para planear, dirigir, supervisar y revisar el trabajo desarrollado...", esto le permitirá asegurarse de la adecuada ejecución de los programas y además comprender la necesidad de información adicional para soportar sus opiniones o conclusiones.

- Comprensión del sistema contable y control interno.

Para poder planear la auditoría de forma adecuada, es necesario tener una comprensión del sistema contable y de control interno de la entidad. Es necesario conocer entre otros puntos; las políticas contables y sus cambios, el efecto de nuevos pronunciamientos de contabilidad y auditoría, así como los procedimientos de control y otros.

Para ser más específicos en este apartado, el auditor debería obtener una comprensión del sistema de contabilidad suficiente para identificar y entender:

- a. Las principales clases de transacciones en las operaciones de la entidad;
- b. Como se inician dichas operaciones;
- c. Los registros contables importantes, documentos de soporte y cuentas; y
- d. El proceso contable y de informes financieros, desde el inicio de transacciones importantes y otros eventos hasta su inclusión en los Estados Financieros.

En relación al control interno contable, el auditor debe considerar y entender los diversos tipos de riesgos a los que se esta expuesto, tales como: el riesgo inherente, el riesgo de control y el riesgo de detección. Estos componen lo que se conoce como riesgo de auditoría, que consiste en el riesgo de

que se de una opinión de auditoría inapropiada. Debe tenerse presente la influencia que tiene el uso de la tecnología y de los sistemas de información para el procesamiento de datos y de los controles internos que se establecen por ello.

En este caso y en lo relativo a los controles internos sobre el procesamiento por computadora, se incluyen tanto procedimientos manuales como procedimientos integrados en programas de computadoras, esto básicamente comprenden los controles globales que afectan al SIC que se conocen como controles generales, y los controles específicos sobre las aplicaciones contables²².

- Comprensión de las actividades del ambiente SIC.

Obtener el conocimiento de las actividades del ambiente SIC, es una actividad con un grado de mayor detalle por la importancia y complejidad que revisten estas. Para obtener la comprensión de estos se debe incluir, según la NIA 401, párrafo 6:

- a. La importancia y complejidad del procesamiento por computadora en cada operación importante de contabilidad. Ejemplo: el volumen de transacciones; transacciones automáticas; cálculos complicados de información financiera; e intercambio electrónicamente de transacciones.
- b. La estructura organizacional de las actividades SIC.

²² Federación Internacional de Contadores (IFAC). 1008. Pág. 637

c. La disponibilidad de datos.

Estas son algunas de muchas actividades que el auditor debe identificar y considerar para comprenderlo, con lo cual podrá realizar la planeación adecuada, el diseño de los procedimientos de auditoría, entre otros.

- Evaluación del control interno.

Las NIA's establecen que un sistema de control interno, significa todas las políticas y procedimientos adoptados por la administración de una entidad para ayudar a lograr el objetivo de asegurar tanto sea factible la conducción ordenada y eficiente de su negocio, lo cual también incluye, adherirse a las políticas de administración, la salvaguarda de activos, la prevención y detección de fraude y error, así como también la precisión e integridad de los registros contables y preparación de la información financiera contable.

Para lograr la efectividad del sistema de control, la entidad sienta sus bases en sus dos componentes principales, los cuales son:

- ✓ Ambiente de Control.
- ✓ Procedimientos de Control.

Para el primer caso, significa la actitud global, conciencia y acciones de los directores y administración respecto del sistema de control interno y su importancia en la entidad. Un ambiente de control es muy importante, sin embargo, por si solo no garantiza la efectividad del sistema.

En lo que respecta al segundo componente, este significa aquellas políticas y procedimientos además del ambiente de control que la administración ha establecido para lograr objetivos específicos.

Es importante aclarar que tanto el ambiente de control y los procedimientos de control se complementan entre si, para lograr la efectividad del control interno. De acuerdo con la NIA "Evaluación del riesgo y control interno", el auditor debería hacer una evaluación de los riesgos inherentes y de control para las aseveraciones importantes...²³

Considerando que el sistema de control interno comprende todas las políticas y procedimientos (control interno) adoptados por la administración para lograr los objetivos trazados por la misma; así como el ambiente de control y los procedimientos de control. Los cuales deben ser sometidos a una evaluación

²³ Federación Internacional de Contadores. (IFAC). Normas Internacionales de Auditoría 2001 Pág. 209.

preliminar para determinar su nivel de riesgo y poder determinar su naturaleza, oportunidad y alcance de los procedimientos sustantivos, todo con el objeto de evaluar el control interno de la entidad.

Un instrumento que facilitaría la identificación de áreas o actividades con mayor nivel de riesgo, es la matriz de control interno. (Ver Anexo 3)

Para observar como puede variar el nivel aceptable del riesgo de detección, basados en las evaluaciones de los riesgos inherentes y de control, se presenta la siguiente tabla en la cual se ilustra la interrelación de los componentes del riesgo de auditoría ya citados.

	La evaluación del riesgo por el auditor es:			
		Alta	Media	Baja
La evaluación del auditor, del riesgo inherente.	Alta	Lo mas bajo	Más baja	Media
	Media	Más baja	Media	Más alta
	Baja	Media	Más alta	Lo más alta

FUENTE: APÉNDICE DE LA NIA 400-2001

Para comprender la tabla, se debe considerar que hay una relación inversa entre el riesgo de detección y el nivel combinado de los riesgos inherente y de control. Por ejemplo; cuando los riesgos inherentes y de control son altos, los

niveles aceptables del riesgo de detección necesitan ser bajos para reducir el riesgo de auditoría a un nivel aceptablemente bajo. Por otra parte, cuando los riesgos inherentes y de control son bajos, un auditor puede aceptar un riesgo de detección más alto y aun así reducir el riesgo de auditoría a un nivel aceptablemente bajo²⁴.

- Elaboración del plan de trabajo.

Es el proceso en el cual el auditor debe documentar el plan global de la auditoría a ejecutar en la entidad, previamente este debe ser discutido con el comité de auditoría, administración y personal de la entidad, esto con el objeto de mejorar la efectividad y eficiencia de la auditoría y para una mejor coordinación de los procedimientos con el trabajo de los empleados de la entidad. Para lograr lo anterior, se necesita que el plan global de auditoría este lo suficientemente detallado que permita guiar el desarrollo de las actividades de los programas en su forma y contenido.

También se debe documentar un cronograma de tiempo por actividad para cada área o procedimientos, en los cuales debe de considerarse los tiempos para las pruebas de control,

²⁴ Federación Internacional de Contadores. (IFAC). Normas Internacionales de Auditoría 2001. Pág. 216

procedimientos sustantivos, el involucramiento de otros auditores o expertos, entre otros.

En general, debe documentar todo lo relativo a la planificación de la auditoría en la entidad, que sea de importancia y le permita ejecutar su trabajo de manera eficiente y oportuna. Y sobre todo no deje lugar a interpretaciones erróneas.

- Procedimientos de auditoría.

Según la NIA 300 párrafo 10; el auditor deberá desarrollar y documentar un programa de auditoría que exponga la naturaleza, oportunidad y alcance de los procedimientos de auditoría Planeados que se requieren para implementar el plan de auditoría global.

En realidad, el programa de auditoría tiene como función principal la de guiar la ejecución del trabajo del auditor o de sus asistentes, ya que establece un conjunto de instrucciones y sirve como un medio de control y registro de la ejecución apropiada del trabajo.

Algo muy importante es el diseño de estos procedimientos cuando se tiene un ambiente SIC, ya que se deben considerar las características del mismo para tener un adecuado programa, entre

algunos aspectos que se deben considerar se tienen: la consistencia de funcionamiento, los procedimientos de control programados, la actualización sencilla de una transacción en archivos múltiples o de base de datos, las transacciones generadas por sistemas, la vulnerabilidad de datos y medios de almacenamiento de programas²⁵, entre otras.

- Determinación de los recursos.

En este punto se debe considerar el conocimiento del entorno a auditar, lo que permitirá determinar los recursos humanos y materiales a utilizar en la auditoría. Para este caso la NIA 400 párrafo 4, establece que "...el auditor debería considerar si se necesitan habilidades especializadas en SIC en una auditoría".

Para ello el auditor debe evaluar si dentro de su personal hay alguien con dicha habilidad, sino lo tuviere, se debe buscar la ayuda de un profesional con los suficientes conocimientos y habilidades en SIC. Si este es el caso, se planea el uso de dicho profesional y el auditor debe obtener suficiente evidencia apropiada de que dicho trabajo es adecuado para los fines de la auditoría, de acuerdo con la NIA 600.

²⁵ Federación Internacional de Contadores. (IFAC). Normas Internacionales de Auditoría 2001. Pág. 636.

El auditor debe establecer los recursos humanos y materiales necesarios, por ejemplo:

Recursos humanos: - Cantidad: depende el alcance de la auditoría.
 - Perfil: depende de la materia (área) a auditar.

Recursos Materiales: - Software: paquetes de auditoría, compiladores, etc.
 - Hardware: PC's, impresoras, etc.
 - Determinación de incremento de carga del auditado. Y consenso en fechas y duración de actividades.

3.3.1.2. INSTRUMENTOS PARA EVALUAR EL CONTROL INTERNO

Los cuestionarios deben ser dirigidos al encargado de informática así como a los usuarios en el momento oportuno. Y con los datos obtenidos el auditor debe hacer una interpretación

o lectura. En la que el juicio profesional debe prevalecer al momento de interpretar o dar lectura a los resultados obtenidos.

3.3.1.2.1. CUESTIONARIO DE RECURSO HUMANO (usuarios).

OBJETIVO: Conocer la actitud de la administración hacia el área o unidad de informática, así como el papel de los usuarios de la misma.

PREGUNTAS	Si	No	N/A
1. ¿Existen requerimientos definidos para determinar la idoneidad del personal a contratar para laborar en el área de SIC?			
2. ¿Son tomados en cuenta por el departamento que se encarga de evaluar el personal a contratar?			
3. ¿Una vez contratado, existen procedimientos enmarcados a una buena integración del personal?			
4. ¿El personal involucra en el SIC, participa en capacitaciones cada cierto periodo?			
5. ¿Cuáles de las siguientes temáticas han sido consideradas en las capacitaciones?: <ul style="list-style-type: none"> • Seguridad física • Programación 			

<ul style="list-style-type: none"> • Utilización del equipo • Seguridad lógica • Confidencialidad • Otros: <p style="text-align: center;">PREGUNTAS</p>	Si	No	N/A
<p>6. ¿Son evaluadas las capacitaciones recibidas por el personal?</p> <p>7. ¿Cuenta el departamento de informática con un plan de monitoreo del personal?</p> <p>8. ¿Existe manual de procedimientos de servicio al usuario?</p> <p>9. ¿Es el jefe de informática o un delegado, el responsable de designar quién desarrollará el servicio de apoyo solicitado por el usuario?</p> <p>10. ¿Existen políticas de rotación de personal?</p> <p>11. ¿Son documentados los servicios utilizado y otorgados?</p> <p>12. ¿Existen controles y registros de cualquier servicio proporcionado a los usuarios?</p> <p>13. ¿Es documentado todo tipo de solicitud de los usuarios?</p>			

<p>14. ¿Existe coordinación entre las áreas prestadoras de servicios de apoyo a los usuarios en la organización?</p> <p>PREGUNTAS</p>	Si	No	N/A
<p>15. ¿Cuenta el área de informática con normas y procedimientos que orienten a los usuarios, analistas, programadores ante la necesidad de servicios en materia informática?</p>			
<p>16. ¿Estas normas y procedimientos son divulgados de tal manera que los interesados sean conocedores de ellos?</p>			
<p>17. ¿Cuenta el departamento de informática con los controles convencionales basados en la segregación adecuada de funciones incompatibles?</p>			
<p>18. ¿Existe plan de trabajo que permita prever las necesidades en torno al personal relacionado con el SIC?</p>			
<p>19. ¿Se estimula y se recompensa al personal del</p>			

<p>área?</p> <p>20. ¿Existe oportunidad de ascenso y promociones?</p>			
---	--	--	--

3.3.1.2.2. CUESTIONARIO DE SEGURIDAD LÓGICA.

Uno de los objetivos importantes trazados por la administración, es conservar la integridad, confidencialidad y disponibilidad de los sistemas de información. Por lo que el control implantado para minimizar el riesgo debe considerar los factores de:

- El valor de los datos siendo procesados.
- La probabilidad de que ocurra un acceso no autorizado.
- Las consecuencias para la organización si ocurre un acceso no autorizado.
- El riesgo y repercusiones en caso de que un usuario no autorizado utilice la información.

Por lo que el auditor, debe considerar la seguridad lógica en áreas (ver anexo 6), las que podrían ser:

- Rutas de acceso.

- Claves de acceso.
- Software de control de acceso.
- Encriptamiento.

Es de importancia resaltar que para el estudio y evaluación de esta área es necesaria la contratación de un especialista con experiencia en el ramo. Esto amparado a la NIA's 620.

3.3.1.2.3. CUESTIONARIO DE SEGURIDAD FÍSICA.

Para verificar el cumplimiento y el establecimiento de políticas, procedimientos y prácticas dirigidas a evitar las interrupciones prolongadas del servicio de procesamiento de información debido a contingencias y a continuar en un medio de emergencia hasta que sea restaurado el servicio. El auditor debe considerar una gama de aspectos relativos a cumplir su objetivo, para lo cual podría hacer uso del cuestionario.

Objetivo: Obtener datos que sirvan para conocer las medidas de seguridad implantadas en el hardware

PREGUNTAS	Si	No	N/A
-----------	----	----	-----

<p>1. El edificio donde se encuentra la computadora esta situado a salvo de:</p> <p>Inundación</p> <p>Terremoto</p> <p>Fuego</p> <p>Sabotaje</p> <p>2. ¿El centro de cómputo da al exterior?</p> <p style="text-align: center;">PREGUNTAS</p>			
<p>3. ¿Tiene el área de informática una instalación de escape y, si es así, pueden ser rotos los vidrios con facilidad?</p> <p>4. ¿Esta el centro de computo en un lugar de alto tráfico de personas?</p> <p>5. ¿Se tiene materiales o paredes inflamables dentro del centro de cómputo?</p> <p>6. ¿Se tiene paredes que no están adecuadamente selladas?</p>			

<p>7. ¿Se tiene grandes ventanales orientados a la entrada o salida del sol?</p> <p>8. ¿Esta sobresaturada la instalación?</p> <p>9. ¿Se tiene lugar previsto? Este es el adecuado para:</p> <ul style="list-style-type: none"> • Almacenamiento de equipo magnético • Formatos y papel para impresora <p style="text-align: center;">PREGUNTAS.</p>	Si	No	N/A
<ul style="list-style-type: none"> • Área y mobiliario para mantenimiento • Equipo de telecomunicaciones • Área de programación • Consolas de operador • Área de recepción • Microcomputadoras • Fuentes de poder • Bóveda de seguridad (Bóveda antiincendio bajo máxima protección) <p>10. ¿La temperatura en la que trabajan los equipos es la recomendada por el proveedor?</p>			

<p>11. ¿Los conductos de aire acondicionado cuentan con alarmas contra intrusos?</p> <p>12. ¿Se controla la humedad de acuerdo con las especificaciones del proveedor?</p> <p>13. ¿Los cables se encuentran debidamente identificados (positivo, negativo, tierra física)?</p> <p style="text-align: center;">PREGUNTAS</p>	Si	No	N/A
<p>14. ¿Se cuenta con planos de instalación eléctrica actualizados?</p> <p>15. ¿Se tiene instalación eléctrica de equipo de cómputo independiente de otras instalaciones eléctricas?</p> <p>16. ¿Se utiliza material antiestático?</p> <p>17. ¿Se tienen reguladores para los equipos de cómputo?</p>			

<p>18. ¿Se posee equipo ininterrumpible?</p> <p>19. ¿El equipo ininterrumpible da el tiempo suficiente para respaldar o guardar los archivos o continuar trabajando?</p> <p>20. ¿Se tiene generadores de corriente ininterrumpida y se prueba su funcionamiento?</p> <p>21. ¿Con qué periodicidad?</p> <p style="text-align: center;">PREGUNTAS</p>	Si	No	N/A
<p>22. ¿Se tiene interruptor de apagado en caso de emergencia en un lugar visible?</p> <p>23. ¿Se han adoptado medidas de seguridad en la dirección de informática?</p> <p>24. ¿Existe una persona responsable de la seguridad?</p> <p>25. ¿Existe personal de vigilancia en la institución?</p>			

<p>26. ¿Se controla el trabajo fuera del horario?</p> <p>27. ¿Se identifica a la persona que ingresa?</p> <p>28. ¿Cómo se controla el acceso?</p> <ul style="list-style-type: none"> • Vigilante • Recepcionista • Tarjeta de control de acceso • Puerta de combinación • Puerta con cerradura <p style="text-align: center;">PREGUNTAS</p>			
<ul style="list-style-type: none"> • Puerta electrónica • Puerta sensorial • Registro de entradas • Puertas dobles • Escolta controlada • Alarmas • Tarjetas magnéticas • Identificación personal <p>29. ¿Existe vigilancia en el cuarto de maquinas las 24 horas?</p>			

<p>30. ¿Se ha instruido a estas personas sobre que medidas tomar en caso de que alguien pretenda entrar sin autorización?</p> <p>31. ¿Se registra el acceso al cuarto de personas ajenas a la dirección de informática?</p> <p>Existe alarma para:</p> <ul style="list-style-type: none"> • Detectar fuego, calor o humo en forma automática. <p style="text-align: center;">PREGUNTAS.</p>	Si	No	N/A
<ul style="list-style-type: none"> • Detectar magnéticos • No existe <p>Estas alarmas están:</p> <ul style="list-style-type: none"> • En el cuarto de maquinas • En la cintoteca y discoteca • En las bodegas • En otros lados <p>32. ¿Existe alarma para detectar condiciones anormales del ambiente?</p> <ul style="list-style-type: none"> • En el cuarto de maquinas 			

<ul style="list-style-type: none"> • En la cintoteca y discoteca • En las bodegas • En otros lados <p>33. ¿Existen extintores de fuego?</p> <ul style="list-style-type: none"> • Manuales • Automáticos • No existen <p>34. Los extintores manuales o automáticos, funcionan</p> <p style="text-align: center;">PREGUNTAS</p>			
<p>a base de:</p> <ul style="list-style-type: none"> • Agua • Gas • Otros <p>35. ¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores?</p> <p>36. Si es que existen extintores automáticos, ¿Son activados por los detectores automáticos de fuego?</p> <p>37. ¿Si los extintores automáticos son a base de</p>			

<p>agua, se han tomado medidas para evitar que el agua cause más daño que el fuego?</p> <p>38. ¿Existe salida de emergencia?</p> <p>39. Se han tomado medidas para minimizar la posibilidad de fuego:</p> <ul style="list-style-type: none"> • Evitando artículos inflamables en el cuarto de maquinas. <p style="text-align: center;">PREGUNTAS.</p>			
<ul style="list-style-type: none"> • Prohibiendo fumar • Vigilando y manteniendo el sistema eléctricos • No se ha previsto. <p>40. ¿Se tienen identificadas y señaladas las salidas de emergencia?</p> <p>41. Se controla el préstamo de:</p> <ul style="list-style-type: none"> • Elementos magnéticos • Equipo • Software 			

<p>42. ¿Se cuenta copias de los archivos en un lugar diferente al de la computadora?</p> <p>43. Expliqué la forma en que están protegidas estas copias:</p> <p>44. ¿Se tienen establecidos procedimientos de actualización para estas copias?</p> <p>45. ¿Existe departamento de auditoría interna?</p> <p style="text-align: center;">PREGUNTAS</p>	Si	No	N/A
<p>46. ¿Esté departamento de auditoría interna conoce todos los aspectos de los sistemas?</p> <p>47. ¿Auditoría interna ha propuesto controles?</p> <p>48. ¿Se cumplen?</p> <p>49. ¿Se auditan los sistemas en operación?</p> <p>50. ¿A iniciativa de quien se efectúan las modificaciones a los programas?</p> <ul style="list-style-type: none"> - Usuario - Director de informática 			

<ul style="list-style-type: none"> - Gerente - Contador - Otros: <p>51. La solicitud de modificaciones a lo programas se hace en forma:</p> <ul style="list-style-type: none"> - Oral - Escrita <p>52. ¿Se revisa que tengan la fecha de las modificaciones cuando se hayan efectuado?</p> <p style="text-align: center;">PREGUNTAS</p>	Si	No	N/A
<p>53. ¿Se ha establecido el nivel de usuario para la información?</p> <p>54. ¿Se ha establecido el número máximo de violaciones en sucesión para que la computadora?</p> <p>55. ¿Se registra cada violación a los procedimientos con el fin de llevar estadísticas y frenar las tendencias mayores?</p> <p>56. ¿Existen controles y medidas de seguridad</p>			

sobre las siguientes operaciones? <ul style="list-style-type: none"> • Recepción de documentos. • Información confidencial. • Computo electrónico. • Documentos de salida. • Archivos magnéticos. • Operación del equipo de computación. • Identificación del personal. • Políticas. • Seguros contra robo e incendio. 			
---	--	--	--

3.3.1.3. CUESTIONARIO DE PROCESAMIENTO DE DATOS.

3.3.1.3.1. CUESTIONARIO ENTRADA DE DATOS

Objetivo: Conocer los controles utilizados en la fuente de datos.

PREGUNTAS	Si	No	N/A
-----------	----	----	-----

<p>1. ¿Se ha considerado algún procedimiento en caso de encontrarse en una situación de duplicidad de datos?</p> <p>2. ¿Se determinan los usuarios o propietarios posibles?</p> <p>3. ¿Se determina al responsable de su actualización y consistencia?</p> <p>4. En el caso que los usuarios son los que se encargan de la Captura y modificación de la información ¿Se ha determinado que usuario es responsable de cada uno de los datos que ingresan?</p> <p style="text-align: center;">PREGUNTAS.</p>	si	no	N/A
<p>5. ¿Existe un responsable de la entrada de datos de cada uno de los datos ingresados al sistema?</p> <p>6. ¿La generación de alguna transacción es generada por el personal del sistema informático?</p>			

<p>7. ¿Se especifica por escrito la preparación de los documentos fuente?</p> <p>8. De un documento fuente para la entrada de datos ¿Se registra la siguiente información?</p> <ul style="list-style-type: none"> • Origen del documento • Autorización • Responsable de preparación de datos • Responsable de retener el documento • Responsable de manipular errores <p>9. ¿Existe una numeración correlativa de los documentos fuente?</p> <p style="text-align: center;">PREGUNTAS</p>			
<p style="text-align: center;">I. EVALUACIÓN DE ENTRADA DE DATOS EN LÍNEA</p> <p>10. ¿Qué porcentaje de datos se hacen en forma directa o en línea?</p> <p>11. ¿Se registran las transacciones efectuadas en</p>			

<p>las entradas directas?</p> <p>12. ¿Cómo?</p> <ul style="list-style-type: none"> • En forma automática • Algún tipo de comprobante • Otros_____ <p>13. ¿Son verificadas al momento de su captura?</p> <p>14. ¿Se tiene un registro de los posibles errores que pueden existir?</p> <p>15. ¿Se tiene un registro de los errores encontrados?</p> <p>16. De tenerse este tipo de registros. ¿En qué forma se hace?</p> <ul style="list-style-type: none"> • Por periodo de tiempo <p style="text-align: center;">PREGUNTAS</p>			
<ul style="list-style-type: none"> • Por función de la organización • Por persona responsable • Otro <p style="text-align: center;">II. EVALUACIÓN DE LOS DOCUMENTOS FUENTE.</p>			

<p>17. ¿Se revisan los datos contenidos en los formularios que se usaran como documentos fuente?</p> <p>18. De esos formularios, ¿Se crean lotes, identifican y forman totales de control?</p> <p style="text-align: center;">III. EVALUACIÓN DEL INGRESO Y VALIDACIÓN</p> <p>19. ¿Existe alguna manera de determinar si todos los datos fueron incorporados al sistema?</p> <p>20. ¿Existe algún procedimiento para corregir el ingreso de datos, si se llegan a encontrar errores?</p> <p>21. ¿Qué aspectos se consideran en la validación de los datos?</p> <p style="text-align: center;">PREGUNTAS</p>			
<ul style="list-style-type: none"> • Caracteres en forma individual • Registro o transacciones completas • Controles totales de registros <p>22. ¿Se registra la cronología de eventos desde</p>			

<p>la captura de información (datos e instrucciones), validación, corrección (si fuese necesario) e ingreso al sistema?</p> <p>23. De responder afirmativamente ¿Se obtiene la siguiente información?</p> <ul style="list-style-type: none"> • Origen. • Elaboración. • Autorización. • Digitación. • Fechas de los diferentes eventos. • Tiempo de digitación. • Número de errores, tipos de errores. • Tiempo de corrección y recursos consumido. 			
---	--	--	--

3.3.1.3.2. CUESTIONARIO PROCESAMIENTO DE DATOS.

Objetivo: Obtener la información necesaria que permita determinar grado de controles internos del sistema y políticas par el procesamientote daros.

PREGUNTAS	Si	No	N/A
-----------	----	----	-----

<p>1. ¿Existen procedimientos formales para la operación del sistema?</p> <p>2. ¿Estos procedimientos describen detalladamente tanto la organización del centro de procesamiento de datos como la operación del sistema?</p> <p>3. ¿Están actualizados los procedimientos?</p> <p>4. ¿Con qué periodicidad se actualizan?</p> <ul style="list-style-type: none"> - Mensual. - Semestral. <p>5. ¿Se tiene un adecuado orden y control en los procesos por lotes?</p> <p>6. ¿Existen órdenes de proceso par cada corrida en la computadora?</p> <p style="text-align: center;">PREGUNTAS</p>	Si	No	N/A
<p>7. ¿Existe un control que asegure la justificación de los procesos en el computador? (Que los procesos que están trabajando están autorizados y tengan una razón de ser procesados)</p>			

8. ¿El sistema genera copias de respaldo automáticamente?			
9. ¿Si no las genera, existe un encargado de hacerlas?			
10. ¿Quién es el encargado? - Responsable del Sistema. - El usuario de cada aplicación. - Otro.			
11. ¿Con qué periodicidad se hace?			
12. ¿Son guardadas en lugares seguros?			
13. ¿En qué lugar se resguardan?			

3.3.1.3.3. SALIDA DE INFORMACIÓN

Objetivo: Conocer los controles utilizados en el resguardo y salida de información.

PREGUNTAS	Si	No	N/A
-----------	----	----	-----

<p>1. Cuando los informes quedan almacenados en archivos. ¿Se tienen copias de estos en otros locales?</p> <p>2. ¿En qué lugar se encuentran esos locales?</p> <ul style="list-style-type: none"> - Fuera de la empresa. - Dentro de la empresa. <p>3. ¿Qué seguridad física se tiene en esos locales?</p> <ul style="list-style-type: none"> * MUCHA * POCA * NINGUNA <p>4. ¿Qué confidencialidad se tiene en esos locales?</p> <ul style="list-style-type: none"> * MUCHA * POCA * NINGUNA <p style="text-align: center;">PREGUNTAS</p>	Si	No	N/A
<p>5. ¿Existe una persona encargada de la entrega de los documentos de salida?</p> <p>6. ¿Existen procedimientos en caso de pérdida de información de un informe?</p>			

<p>* Del total de informes</p> <p>De la mitad de los informes</p> <p>* De algún informe</p> <p>7. ¿Existen procedimientos en caso de modificación de un informe?</p> <p>8. ¿Se han previsto planes de contingencia si se llega a destruir algún informe, por cualquier razón?</p> <p>9. ¿Se registran las siguientes informaciones de los recursos que consume un informe?</p> <p>* Tiempo de utilización</p> <p>* Equipo</p> <p>* Humano</p> <p>* Otro</p> <p style="text-align: center;">PREGUNTAS</p>	Si	No	N/A
<ul style="list-style-type: none"> • Se encuentra al día • Existe confidencialidad • Existe oportunidad • Son aprobados por alguna autoridad 			

<p>10. ¿Son controlados los datos grabados en los archivos magnéticos con respecto a su concordancia con los informes impresos?</p>			
<p>11. ¿Se da el caso de tener salidas en medios de almacenamiento par imprimir en otro equipo periférico?</p>			
<p>12. ¿Existen procedimientos al efectuar la impresión?</p>			
<p>13. ¿Se da el caso en que los datos son remitidos a sectores externos al sistema para preparar informes?</p>			
<p>14. ¿Por qué se procede de esta manera?</p>			
<p>15. ¿Existe comunicación adecuada entre lo puntos de emisión y recepción?</p>			

Además de estos instrumentos (ver anexo del 2 al 4), el auditor debe hacer uso de otros que cree según su juicio profesional necesarios para ampliar los conocimientos obtenidos, lo que permitirá establecer e identificar las áreas de riesgo en el procesamiento de datos.

3.3.2. LA EJECUCIÓN DE LA AUDITORÍA EN INFORMÁTICA.

Es la parte práctica en la que el auditor debe poner a trabajar su juicio profesional para el adecuado desarrollo de los programas diseñados y la obtención de evidencia suficiente y apropiada por medio de las pruebas sustantivas. Tal como se muestra en la figura siguiente:

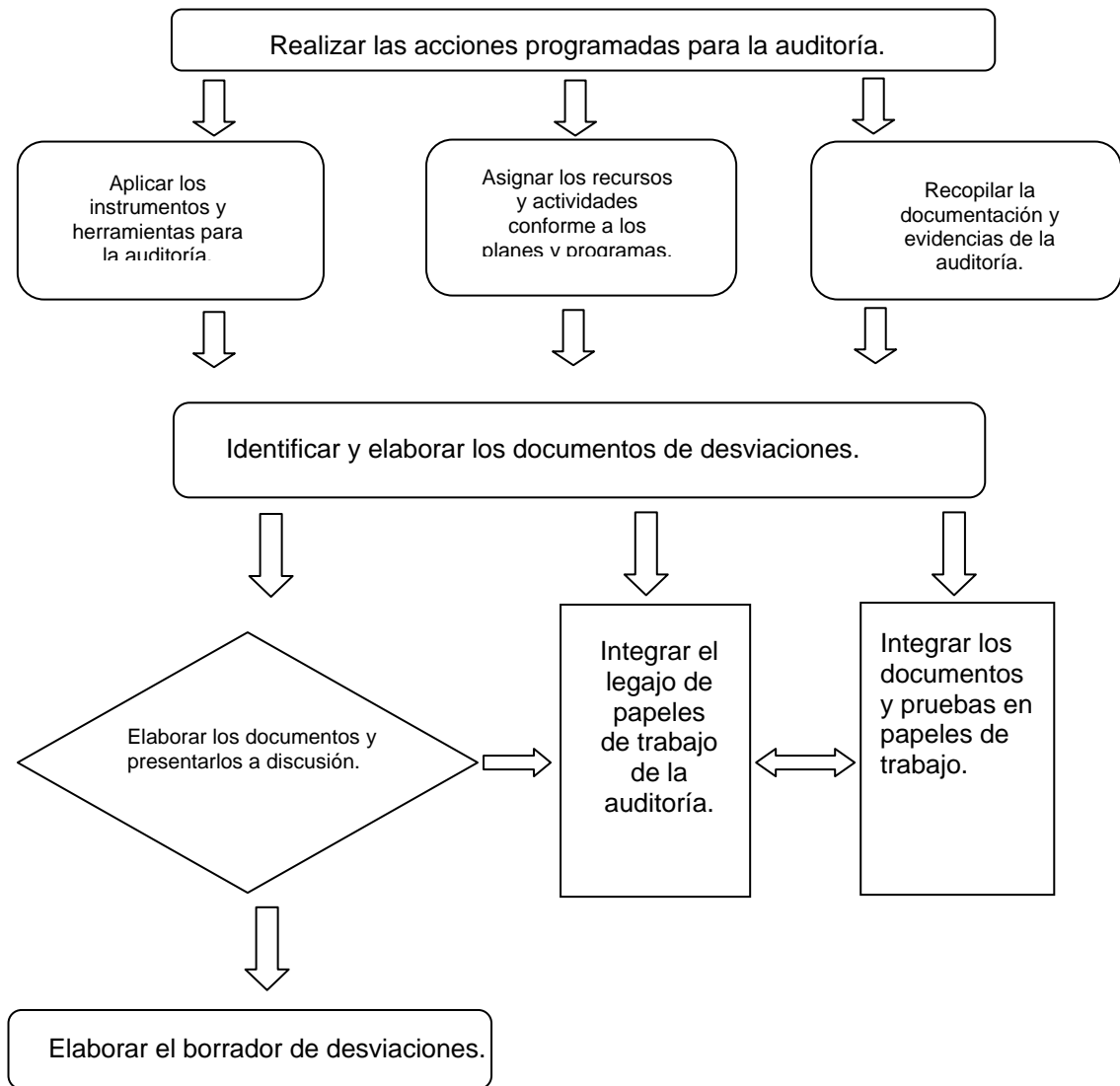


FIGURA 2: Ejecución de la auditoría en informática.

Los programas de auditoría son una de la herramientas más utilizadas y quizás las más importantes; este es un documento formal que guía los procedimientos de evaluación que debe seguir el auditor, así mismo le indica todos los puntos, aspectos concretos y áreas que deben ser revisadas, así como las

técnicas, herramientas y procedimientos que deben ser utilizados en la auditoría en informática.

Las áreas ha considerar en una auditoría en informática pueden ser divididas: recurso humano (usuarios), hardware y software (seguridad física y lógica) y procesamiento de datos (entrada, proceso y salida). Por lo que para cada una de estas se diseña un programa.

3.3.2.1. PROGRAMAS DE VALIDACIÓN DE AUDITORÍA EN INFORMÁTICA.

3.2.2.1.1. RECURSO HUMANO.

NOMBRE DE LA FIRMA

NOMBRE DEL CLIENTE

PROGRAMA DE VALIDACIÓN DE AUDITORÍA EN INFORMÁTICA

ÁREA RECURSO HUMANO.

PERIODO _____

OBJETIVO: Obtener evidencia acerca de las políticas, procedimientos y normas establecidos por la administración en el área de informática.

N	ACTIVIDAD
1	Evaluar la estructura orgánica de la empresa y la consideración del área o unidad de informática y comprobar las líneas de autoridad y responsabilidad.
2	Verificar la existencia de los elementos mínimos del manual de organización de la dirección: <ul style="list-style-type: none"> - Organigrama con jerarquía. - Funciones. - Objetivos y políticas. - Análisis, descripción y evaluación de puestos. - Manual de procedimientos. - Manual de normas. - Instructivos de trabajo o guías de actividad. - Otras.
3	Evaluar los manuales de procedimientos y de normas por medio del personal en función de: <ul style="list-style-type: none"> - Desempeño y comportamiento. - Condiciones de ambiente de trabajo. - Organización en el trabajo. - Desarrollo y motivación. - Capacitación y supervisión.
4	Verificar la existencia, adecuación y cumplimiento de funciones, por el personal encargado del procesamiento de datos.
5	Comprobar la existencia de objetivos y políticas propias del área de informática, así como el conocimiento del personal, la adecuación de los mismos y su respectivo cumplimiento.

6	Realizar entrevistas con el personal operativo del área de informática y elaborar narrativas respectivas al caso.
7	Identificar y verificar los deberes y responsabilidades del personal encargado de la seguridad y riesgos del área.
8	Evaluar el acceso del personal del área de informática y sus aplicaciones: <ul style="list-style-type: none"> - Restricción de acceso físico. - Restricción de acceso lógico.
9	Revisar la segregación de funciones en función de tareas incompatibles y normas o políticas establecidas al respecto.
10	Elaborar un informe del área de recursos humanos.

Elaborado por _____

Revisado por _____

3.3.2.1.2. ÁREA DE SEGURIDAD FÍSICA (HARDWARE)

NOMBRE DE LA FIRMA

NOMBRE DEL CLIENTE

PROGRAMA DE AUDITORÍA EN INFORMÁTICA

ÁREA DE SEGURIDAD FÍSICA (HARDWARE)

PERIODO _____

OBJETIVO: Obtener evidencia de la adecuada aplicación del control interno en la seguridad del equipo de cómputo.

No	ACTIVIDAD
1	Prepare cedula de auditoría que muestre los movimientos del hardware en el ejercicio, considerando lo siguiente: <ul style="list-style-type: none">- Saldo inicial- Compra o incrementos- Bajas- Saldos finales
2	Respecto a las compras e incrementos del año, examinar la siguiente documentación con objeto de verificar: <ul style="list-style-type: none">- Autorización- Requisiciones, Pedidos y contratos- Facturas- Inspeccionar físicamente las principales adquisiciones- Aplicación contable
3	En relación a las bajas por destrucción, sustitución o venta, verifique: <ul style="list-style-type: none">- Autorización- Documentación comprobatoria
4	
5	Verifique las especificaciones del equipo a través de una lista de chequeo. Elabore una cedula de auditoría en donde evalúe y califique las características mas importantes de los siguientes elementos del hardware: <ul style="list-style-type: none">- Tarjeta madre del sistema- Procesador

6	<ul style="list-style-type: none"> - Unidades adicionales, características, interfaz y capacidad - Tarjetas adicionales al sistema - Periféricos externos asociados al sistema - Aprovechamiento y utilidad del sistema computarizado - Mantenimiento básico para el sistema computarizado. <p>Prepare cedula de hallazgo, que contenga como mínimo:</p> <ul style="list-style-type: none"> - Condición. - Causa. - Efecto. - Recomendación.
---	---

Elaborado por _____

Revisado por _____

3.3.2.1.3. ÁREA DE SEGURIDAD LÓGICA. (SOFTWARE)

NOMBRE DE LA FIRMA

NOMBRE DEL CLIENTE

PROGRAMA DE AUDITORÍA EN INFORMÁTICA

ÁREA DE SEGURIDAD LÓGICA (SOFTWARE).

PERIODO _____

OBJETIVO: Obtener evidencia a cerca del cumplimiento del control interno en el área de informática en relación a los softwares.

No	ACTIVIDAD
1	Entrevistar al administrador respecto al cumplimiento de sus funciones apoyándose en el manual de organización, de procedimientos y de operación.
2	Prepare cedula de auditoría que muestre los movimientos del software en el ejercicio, considerando lo siguiente: <ul style="list-style-type: none">- Saldo inicial- Compra o incrementos- Bajas- Saldos finales
3	Respecto a las compras e incrementos del año, examinar la siguiente documentación con objeto de verificar: <ul style="list-style-type: none">- Autorización- Requisiciones, Pedidos y contratos- Facturas
4	<ul style="list-style-type: none">- Inspeccionar las adquisiciones <p>En relación a las bajas y sustitución, verifique:</p> <ul style="list-style-type: none">- Autorización
5	<ul style="list-style-type: none">- Documentación comprobatoria <p>Elabore cedulas de auditoría en donde contenga los resultados de los siguientes procedimientos.</p> <ul style="list-style-type: none">- Solicitar la asignación de una terminal para entrar al sistema y acceder a la información, cambiar datos, bases de datos, instrucciones y programas, hasta donde lo permita el sistema.- Ingresar al administrador y cambiar privilegios, atributos y contraseñas de usuarios.

<p>6</p> <p>7</p>	<ul style="list-style-type: none"> - Entrar al sistema y dar de alta a distintos accesos sin tener autorización. - Solicitar a un usuario sin forzarlo, que ingrese a un nivel que no le corresponde y verificar si el sistema le permite tal operación o hacer por nuestros propios medios previa autorización. - Entrar al sistema de red sin ninguna autorización y acceder a la información, alterar bases de datos o cambios al sistema hasta donde lo permita el mismo. - Reiniciar el sistema y utilizar teclas F5 o F8 al encender el sistema e ingresar sin contraseña. - Entrar al sistema con disco de arranque externo e ingresar sin contraseña. - Tratar de acceder al sistema alterando las veces necesarias la contraseña y obtener los resultados del sistema. - Hacer una revisión a la bitácora y verificar la información de los usuarios: La fecha, hora de ingreso y la salida del sistema, registro de sus actividades y cualquier incidencia durante su estancia. - Hacer la revisión documental a cada una de las bitácoras de las incidencias y evaluar la magnitud del impacto y la solución de las mismas <p>Monitorear aleatoriamente a los usuarios y evaluarles las actividades que realice. Si es necesario aplicar encuestas y/o entrevistas sobre el control de la bitácora de acceso</p> <p>Hacer una narrativa de los resultados encontrados o las cédulas respectivas.</p>
-------------------	---

Elaborado por _____

Revisado por _____

3.3.2.1.4. ENTRADA DE DATOS.

NOMBRE DE LA FIRMA

NOMBRE DEL CLIENTE

PROGRAMA DE VALIDACIÓN DE AUDITORÍA EN INFORMÁTICA

ÁREA PROCESAMIENTO DE DATOS (ENTRADA)

PERIODO _____

OBJETIVO: Verificar la aplicación de las medidas de control en el acceso al sistema, la clasificación y registro de datos en la fuente de información.

N	ACTIVIDAD
1	<p>Preparar cedula de auditoría que contenga los resultados de los siguientes procedimientos:</p> <ul style="list-style-type: none">- Solicitar la asignación de una terminal para entrar al sistema y acceder información, hasta donde lo permita el sistema.- Comprobar la efectividad de las contraseñas de varios usuarios.- Solicitar a un usuario, sin forzarle, que ingrese a un nivel que no le corresponda y verificar si el sistema le permite la operación.- Hacer pruebas con operaciones hipotéticas, y verificar el resultado de la entrada de datos.- Comprobar los controles detectivos cuando se ingresen datos incorrectos.
2	<p>Evaluar la entrada de datos considerando los elementos siguientes:</p> <ul style="list-style-type: none">- Los datos de entrada directos.- La codificación.- Los documentos fuentes.

	<ul style="list-style-type: none"> - El ingreso y validación. - Recuperación de datos. - Control de los datos. - Segregación de funciones.
3	<p>Visitar la biblioteca de archivos para determinar si los procedimientos que ahí se usan, en verdad restringen el acceso a los datos, programas y a la documentación, ya que esta es otra forma de acceder indirectamente el sistema informático.</p>
4	<p>Hacer un diagrama de la operación de acceso y validación al sistema.</p>
5	<p>Si es necesario apoyarse en los servicios de un especialista en programación y análisis, para acceder a la configuración del programa.</p>
6	<p>Hacer una narrativa de los resultados encontrados o la cedula respectiva.</p>

Elaborado por _____

Revisado por _____

3.3.2.1.5. PROCESAMIENTO DE DATOS.

NOMBRE DE LA FIRMA

NOMBRE DEL CLIENTE

PROGRAMA DE AUDITORÍA EN INFORMÁTICA

ÁREA PROCESAMIENTO DE DATOS (PROCESAMIENTO)

PERIODO _____

OBJETIVO: Validar la aplicación de procedimientos de control y seguridad del sistema y de los usuarios durante el procesamiento de datos.

No	ACTIVIDAD
1	<p>Preparar cedula de auditoría que contenga los resultados de los siguientes procedimientos:</p> <ul style="list-style-type: none">- Verificar cálculos aritméticos (ejecutados a satisfacción), para corroborar exactitud en los reportes con la del libro mayor y auxiliares, entre otros- Verificar si es posible el reinicio en una sesión de trabajo después de haber corregido un error detectado- Hacer una revisión a la bitácora y verificar la información de los usuarios: La fecha, hora de ingreso y salida del sistema, registro de sus actividades y cualquier incidencia durante su estancia.- Monitorear aleatoriamente usuarios y evaluar si las actividades que realizan están registradas en la bitácora. Si es necesario, aplicar encuestas y entrevistas sobre el control de la bitácora de accesos.
2	<p>Elaborar Flujograma que describa detalladamente el proceso por actividades para una mejor comprensión del mismo.</p>
3	<p>Evaluar las siguientes actividades en el procesamientos:</p> <ul style="list-style-type: none">- Los controles en las operaciones.

	<ul style="list-style-type: none"> - Controles en la asignación de trabajo. - Controles de los medios de almacenamiento. - Controles de mantenimiento.
4	Si es necesario apoyarse en los servicios de un especialista en programación y análisis, para acceder a la configuración del programa.
5	Hacer una narrativa de los resultados encontrados o la cedula respectiva.

Elaborado por _____

Revisado por _____

3.3.2.1.6. SALIDA DE INFORMACIÓN.

NOMBRE DE LA FIRMA

NOMBRE DEL CLIENTE

PROGRAMA DE AUDITORÍA EN INFORMÁTICA

ÁREA PROCESAMIENTO DE DATOS (SALIDA DE INFORMACIÓN)

PERIODO _____

OBJETIVO: Verificar la aplicación de medidas de seguridad en la salida de información en medios magnéticos e impresos.

No	ACTIVIDAD
1	<p>Preparar cedula de auditoría que contenga los resultados de los siguientes procedimientos:</p> <ul style="list-style-type: none">- Verificar que cada reporte cumpla con requerimientos preestablecidos de presentación y distribución- Relacionar aleatoriamente los datos de entrada con la base de datos y el contenido de los reportes- Verificar si existen registros de salida de los reportes a las áreas destino o usuarios de la información.- Indagar sobre el tratamiento que se le da a la información que no es utilizada.- Indagar el número de copias que permite el sistema por reporte y la autorización para ello.- Verificar el inventario.
2	Verificar los controles manuales para el monitoreo de la salida de información.
3	Elaborar Flujograma que describa detalladamente el proceso por actividades para una mejor comprensión del mismo.

4	Si es necesario apoyarse en los servicios de un especialista en programación y análisis, para acceder a la configuración del programa.
5	Hacer una narrativa de los resultados encontrados o una cedula respectiva

Elaborado por _____

Revisado por _____

Para complementar la evaluación del área lógica, el auditor utilizara la simulación o Flujogramas de procesos, para entender la lógica del sistema, analizando el proceso existente y comparándolo con el proceso que debería realizar el sistema o programa (ver anexo 6)

Además, una práctica recomendable para ampliar los hallazgos es la elaboración de una narrativa, en la cual las características quedan a criterio del auditor (ver anexo 7), así como la elaboración de formularios prediseñados que permitan llevar un control de ciertas áreas, tal caso seria el formulario para levantamiento físico del hardware (ver anexo 8).

3.3.3. INFORME DE AUDITORÍA.

El producto final de este tipo de auditoría al igual que la de estados financieros es un dictamen que expresa la opinión de los auditores (ver anexo 9) sobre la situación actual del área de informática de la empresa. (Ver sección 1.3.5.3).Ejemplo:

3.3.3.1. ESTRUCTURA DEL INFORME.

- 1.- Portada.
- 2.- Índice.
- 3.- Introducción.
- 4.- Dictamen.
- 5.- Áreas.
- 6.- Notas.

Sres. Junta Directiva.

Empresa Ejemplo.

Presente.

Hemos auditado el área de informática de la empresa EJEMPLO, del 01 de enero al 31 de diciembre de 2,004., para evaluar la seguridad física, seguridad lógica, los usuarios y el procesamiento electrónico de datos. Dicha área es responsabilidad de la administración. Nuestra responsabilidad es expresar una opinión acerca de las áreas basadas en nuestra auditoría.

Nuestro examen fue desarrollado de acuerdo con las Normas Internacionales de Auditoría y las declaraciones internacionales de prácticas de auditoría. Las cuales requieren que planeemos y desarrollemos a la auditoría para obtener certeza razonable de la situación del área de informática. La auditoría incluye el estudio y evaluación del control interno y comprensión del ambiente SIC, con el propósito de obtener evidencia que apoye la información no financiera revelada.

En dicho examen determinamos que el área del hardware en la parte de seguridad física tiene deficiencias en los controles de salvaguarda. Las cuales afectan el procesamiento de datos en el área de informática.

En nuestra opinión, excepto por el efecto sobre el área de informática del asunto que nos referimos en el párrafo precedente, el área de informática da un punto de vista de certeza razonable sobre el buen funcionamiento de dicha área.

Auditor _____

San Salvador, 15 de febrero de 2004.

IV. CONCLUSIONES Y RECOMENDACIONES.

4.1. CONCLUSIONES.

Una vez procesados los resultados obtenidos del cuestionario, dirigidos a los encargados del área o unidad de informática de la Mediana Empresa del sector comercio, se concluye lo siguiente:

- La complejidad de los sistemas de información por computadora utilizados para el procesamiento de datos carecen del debido cuidado de parte de la administración.
- El área o unidad de informática no poseen políticas y procedimientos enmarcados al control interno relacionado al procesamiento de datos.
- Los controles generales en el sistema de información por computadora en la mediana empresa son insuficientes, lo que hace que el riesgo de representaciones erróneas sea mayor en los sistemas.
- Los controles aplicables a la entrada, procesamiento y salida de información son insuficiente por lo que la garantía de la información procesada es limitada.

- La mediana empresa del sector comercio, no tiene definida políticas o procedimientos enfocados a la evaluación y monitoreo de los controles internos en el área o unidad de informática.

- La mayoría de errores que se presentan en el procesamiento de datos en el sistema de información por computadora son ocasionados por el personal (recuso humano) encargado del mismo.

- Las empresas carecen de una herramienta que les permita identificar y estudiar las posibles amenazas o riesgos a los que está expuesta el área o unidad de informática.

4.2. RECOMENDACIONES

- Debido a la importancia y complejidad del procesamiento de datos por computadora en la mediana empresa del sector comercio, la alta dirección debe prestar la debida atención al área o unidad de informática y considerarla como una sección importante.

- La administración de la empresa debe definir y divulgar políticas y procedimientos del área o unidad de informática, con el propósito de establecer criterios para la creación de normas internas y definir controles necesarios para el cumplimiento de los requerimientos definidos en el procesamiento de datos.

- La alta dirección debe adoptar una actitud proactiva a efecto de realizar evaluaciones y considerar la reestructuración de los controles internos cuando lo ameriten, los que deben estar en función de: la competencia y responsabilidad, valores y reglas, evaluaciones de riesgo, controles incorporados a los procesos y flexibilidad en los controles.

- La mediana empresa debe considerar el uso o diseño de algún instrumento o mecanismo que le permita una adecuada identificación y manejo de los riesgos a los que esta expuesta el área o unidad de informática.

- Debe de realizarse una evaluación periódica por personal interno o externo, que permita la revisión y evaluación de los controles referentes a la entrada, procesamiento y salida de información.

- Se debe promover la capacitación periódica del personal en cuanto al uso y manejo adecuado del equipo y programas, en función de mejorar el procesamiento de datos y la calidad del mismo.

- Dada la importancia de la información para la toma de decisiones debe hacerse uso de una herramienta (Checklist) que le permita evaluar el cumplimiento de los estándares de calidad definidos por la empresa.

BIBLIOGRAFÍA.

ASOCIACIÓN INTERAMERICANA DE CONTABILIDAD. (AIC)

La profesión contable hacia la nueva visión de negocios.
Tomo III. Panamá 2,003.

CATACORA Carpio, Fernando.

Sistemas y Procedimientos Contables. Mc Graw Hill. 1,999

COMITÉ EJECUTIVO DE NORMAS DE AUDITORÍA. (AICPA)

Declaraciones sobre normas internacionales de auditoría.
Tomo I. 3ª Edición, Mayo de 1991.

ECHENIQUE García, José Antonio.

Auditoría en Informática. 2º Edición. Mc Graw Hill. 2,000

FEDERACIÓN INTERNACIONAL DE CONTADORES. (IFAC)

Normas Internacionales de Auditoría 2001. Publicados por el
Instituto Mexicano de Contadores Públicos, A.C.

HERNÁNDEZ Hernández, Enrique.

Auditoría en informática. 1ª edición. Editorial CECSA.
México. 1,999.

HERNÁNDEZ Sampieri, Roberto; Fernández C. y P. Baptista L.

Metodología de la Investigación. Mc Graw Hill
Interamericana. México. 2,000.

LAZCAN, Juan Manuel, Rivas Z, Enrique.

Auditoría e informática estructura en evolución. IMCP. 1^a
edición 1,998.

MUÑOZ Razo, Carlos.

Auditoría en sistemas computacionales. 1^a edición 2,002.
Editorial Pearson Educación. México 2,001.

O'BRIEN James A.

Sistemas de Información Gerencial. 4ta. Edición. Mc Graw
Hill.

O. RAY Whittington, Kart Pany

Auditoría "Un Enfoque Integral". 12^a Edición. Mc Graw Hill.
2,000

PÉREZ Toraño, Luis Felipe.

Auditoría de Estados Financieros. Teoría y Práctica. 2^a
Edición. Mc Graw Hill. 1,999.

ROJAS Soriano, Raúl.

Guía para realizar Investigaciones Sociales. 23^a Edición.
Universidad Autónoma de México. 1,999.

SÁNCHEZ CURIEL, Gabriel.

Auditoría de Estados Financieros. Un caso practico. 1^a
edición. Editorial Mc Graw Hill. México 1,997.

SUÁREZ, Andrés S.

La moderna auditoría un análisis conceptual y metodológico.
1^a edición. Editorial Mc Graw Hill. España 1,990.

WILLINGHAM, John J.; D. R. Carmichael.

Auditoria concepto y método. 3a edición. Editorial Mc Graw
Hill. 1,979.

ANEXO

ANEXO No. 1

TABULACIÓN Y ANÁLISIS.

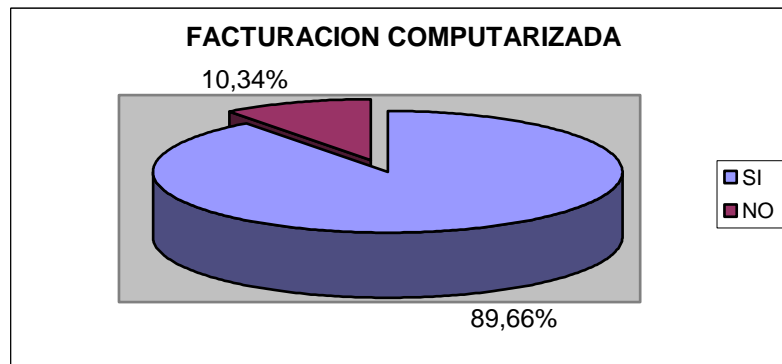
Los resultados obtenidos en el cuestionario administrado a las diferentes medianas empresas del sector comercio de la zona metropolitana de san salvador permitió conocer el control interno aplicado al área o unidad de informática. El objetivo de la investigación esta orientado a proponer lineamientos de auditoría en informática basados en las normas internacionales de auditoría que contribuyan a mejorar los controles internos en el procesamiento de datos en este tipo de empresa.

1. ¿Que actividades son procesadas por medio de sistema de información por computadora en la empresa?

CUADRO N° 1.

FACTURACIÓN COMPUTARIZADA.

FACTURACIÓN	CANTIDAD	PORCENTAJE
SI	26	89.65%
NO	3	10.35 %
TOTAL	29	100.00%



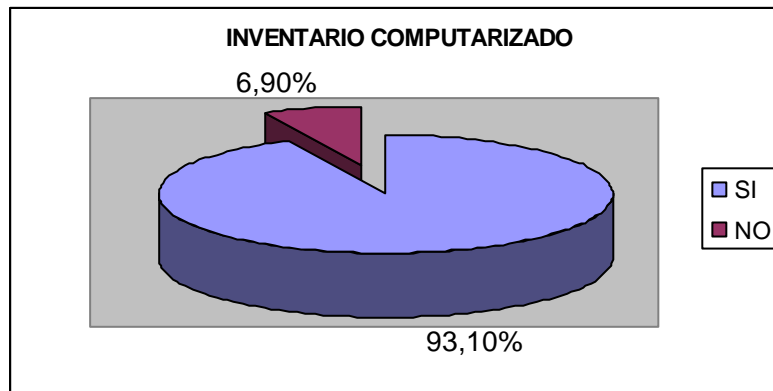
FUENTE: INVESTIGACIÓN DE CAMPO.

Las medianas empresas del sector comercio utilizan en un 89.65% la facturación computarizada, y por el contrario el 10.35% lo realizan manualmente. Esto muestra que la mayoría de las empresas han mecanizado la facturación.

CUADRO N° 2.

INVENTARIO COMPUTARIZADO

INVENTARIO	CANTIDAD	PORCENTAJE
SI	27	93.10%
NO	2	06.90%
TOTAL	29	100.00%



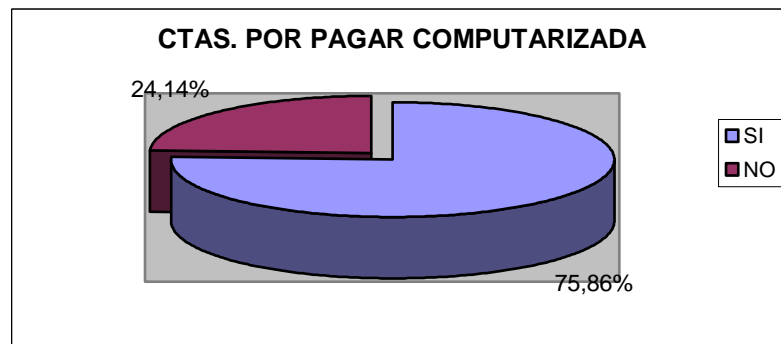
FUENTE: INVESTIGACIÓN DE CAMPO.

Con respecto al registro y administración del inventario, un 93.10% de las empresas encuestadas lo registran a través de un programa computacional; mientras que el resto lo registran por medios manuales. Lo que demuestra que una minoría no lo tiene mecanizado.

CUADRO N° 3.

CUENTAS POR PAGAR COMPUTARIZADA.

CUENTAS POR PAGAR	CANTIDAD	PORCENTAJE
SI	22	75.86%
NO	7	24.14%
TOTAL	29	100.00%



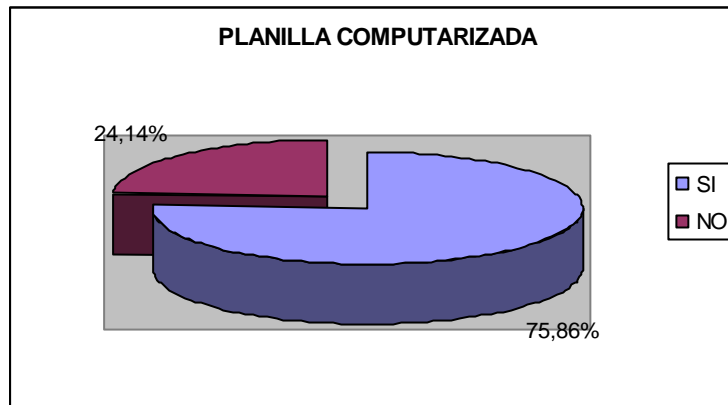
FUENTE: INVESTIGACIÓN DE CAMPO.

Con respecto al control de las cuentas por pagar, las empresas en su mayoría tienen módulos computarizados, representado en un 75.86%, mientras que un 24.14% lo registra y controla manualmente.

CUADRO N° 4.

PLANILLAS COMPUTARIZADAS.

PLANILLAS	CANTIDAD	PORCENTAJE
SI	22	75.86%
NO	7	24.14%
TOTAL	29	100.00%

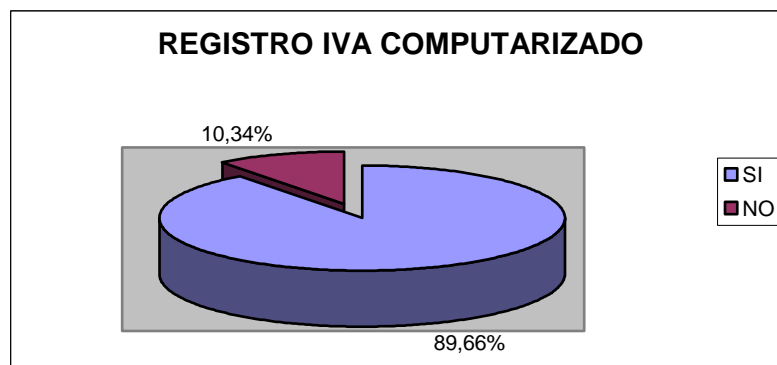


FUENTE: INVESTIGACIÓN DE CAMPO.

Para la determinación del gasto mensual en sueldos y salarios las empresas hacen uso de un software especializado, esto representa un 75.86% de la muestra objeto de estudio, y por el contrario un 24.14% lo hacen por medios manuales. Por lo que la mayoría procesa sus planillas de empleados por computadora.

CUADRO N° 5.
REGISTRO DE IVA COMPUTARIZADO.

REGISTROS IVA	CANTIDAD	PORCENTAJE
SI	26	89.65%
NO	3	10.35 %
TOTAL	29	100.00%



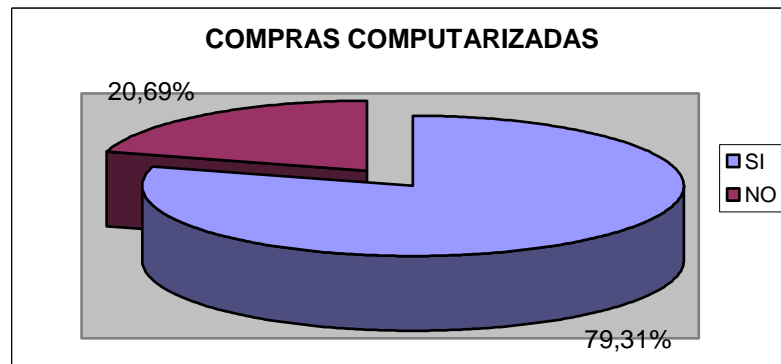
FUENTE: INVESTIGACIÓN DE CAMPO.

Para establecer un adecuado control en el registro del Impuesto al Valor Agregado (IVA) las empresas utilizan un programa mecanizado, lo que representa un 89.65% de la muestra objeto de estudio y un 10.35% no hace uso de sistemas computarizados para dicho procesamiento.

CUADRO N° 6.

REGISTRO DE COMPRAS COMPUTARIZADO.

COMPRAS	CANTIDAD	PORCENTAJE
SI	23	79.31%
NO	6	20.69%
TOTAL	29	100.00%



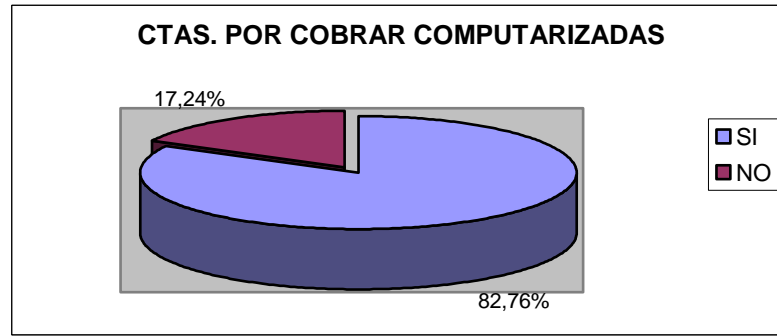
FUENTE: INVESTIGACIÓN DE CAMPO.

Las medianas empresas del sector comercio poseen un modulo especializado de compras en su sistema de información, esto se ve reflejado en un 79.31%. Esto demuestra la importancia del uso de la tecnología en el procesamiento de datos, mientras que el resto realizan sus registros por medios manuales.

CUADRO N° 7.

CUENTAS POR COBRAR COMPUTARIZADO.

CUENTAS POR COBRAR	CANTIDAD	PORCENTAJE
SI	24	82.76%
NO	5	17.24%
TOTAL	29	100.00%



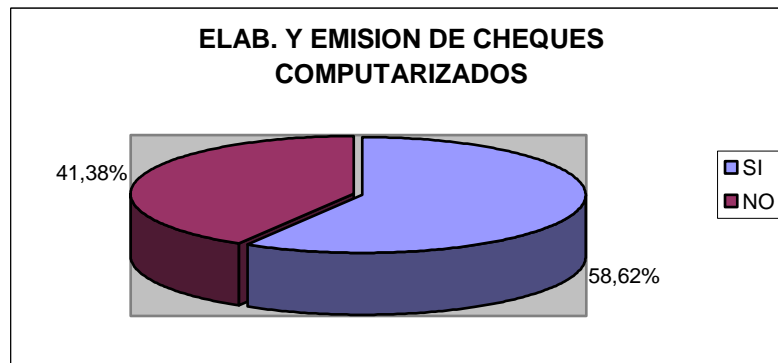
FUENTE: INVESTIGACIÓN DE CAMPO.

En el caso de las cuentas por cobrar según los datos de la investigación, un 82.76% de las empresas poseen un módulo especializado para el registro y control de estas, y un 17.24% no tienen sistema computarizado.

CUADRO N° 8.

ELABORACIÓN Y EMISIÓN DE CHEQUES COMPUTARIZADO.

ELABORACIÓN Y EMISIÓN DE CHEQUES	CANTIDAD	PORCENTAJE
SI	17	58.62%
NO	12	41.38%
TOTAL	29	100.00%



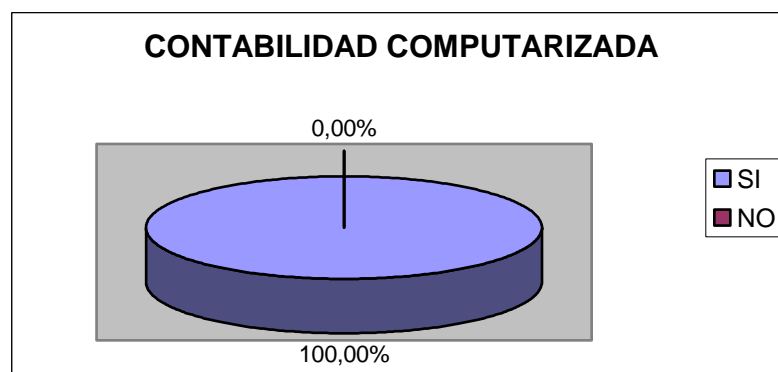
FUENTE: INVESTIGACIÓN DE CAMPO.

En lo relacionado a la elaboración y emisión de cheques en las empresas del sector comercio en su mayoría lo realizan por medio de sistemas computarizados, es decir un 58.62%, y por el contrario un 41.38% no hacen uso de estos medios.

CUADRO N° 9.

CONTABILIDAD COMPUTARIZADA.

CONTABILIDAD	CANTIDAD	PORCENTAJE
SI	29	100.00%
NO	0	0.00%
TOTAL	29	100.00%



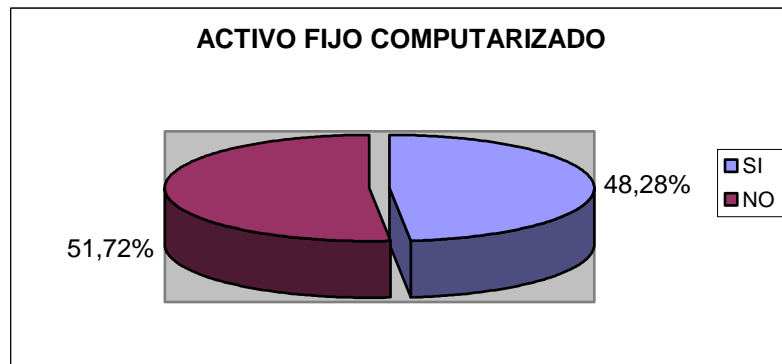
FUENTE: INVESTIGACIÓN DE CAMPO.

Para la obtención de información financiera-contable, confiable y oportuna dentro de las empresas, estas hacen uso de medios mecanizados para el procesamiento de su información, esto se ve reflejado en un 100% de las medianas empresas que poseen un sistema contable computarizado.

CUADRO N° 10.

ACTIVO FIJO COMPUTARIZADO.

ACTIVO FIJO	CANTIDAD	PORCENTAJE
SI	14	48.28%
NO	15	51.72%
TOTAL	29	100.00%



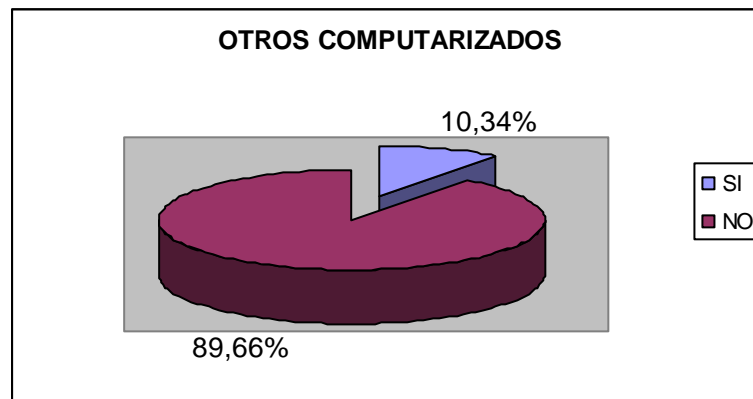
FUENTE: INVESTIGACIÓN DE CAMPO.

Para los registros y detalles del activo fijo en las empresas, estas lo procesan por medios computacionales auxiliares en un 48.28%, mientras que un 51.72% lo manejan manualmente. Se observa el poco uso de los sistemas auxiliares.

CUADRO N° 11.
OTROS MÓDULOS COMPUTARIZADOS.

OTROS	CANTIDAD	PORCENTAJE
SI	3	10.34%
NO	26	89.66%
TOTAL	29	100.00%

NOTA: En otros se considera los Costos, retaceos y despachos.



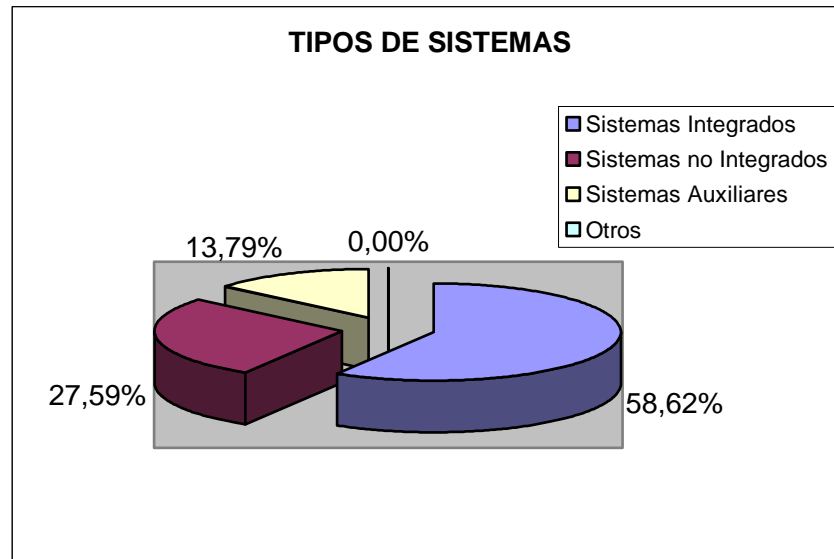
FUENTE: INVESTIGACIÓN DE CAMPO.

En un 10.34% de las empresas del sector comercio tienen mecanizado otras actividades complementarias para la contabilidad; como lo es el manejo y registro de los costos, retaceos y despachos.

2. ¿El sistema contable esta relacionado con los sistemas administrativos a través de?

CUADRO N° 12.
TIPOS DE SISTEMAS.

CRITERIO/ACTIVIDAD	CANTIDAD	PORCENTAJE
Sistemas Integrados	17	58.62%
Sistemas no Integrados	8	27.59%
Sistemas Auxiliares	4	13.79%
Otros	0	0.00%
TOTAL	29	100.00%



FUENTE: INVESTIGACIÓN DE CAMPO.

Para el manejo y la concatenación de los datos y la producción de la información se determinó que las empresas manejan en un 58.62% sistemas integrados lo que implica un cierto grado de complejidad en el manejo del mismo, mientras que un 27.59% hacen uso de sistemas no integrados, y solo un 13.79% utiliza sistemas auxiliares.

En base a los datos anteriores, se establece que la empresa del sector comercio procesan la información financiero-contable y administrativa por medio de un sistema computarizado con un cierto grado de complejidad, debido a que esta compuesto por diversos módulos (facturación, inventario, cuentas por pagar,

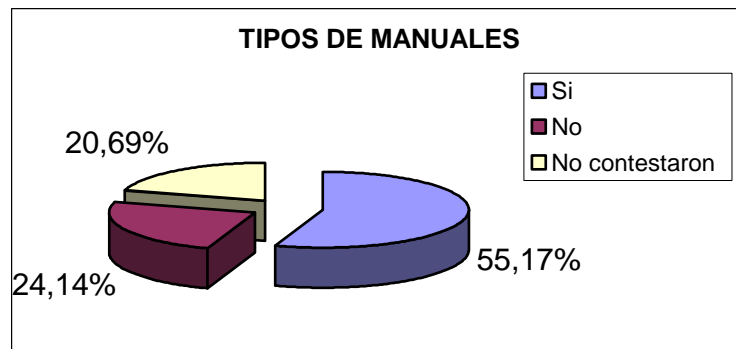
planillas, entre otros) en donde cada uno de ellos está relacionado directamente; lo que implica un mayor grado de complejidad en el procesamiento de datos.

3. ¿Cuenta el área o unidad de informativa con los manuales respectivos de?

CUADRO N° 13.

MANUAL DE FUNCIONES.

FUNCIONES	CANTIDAD	PORCENTAJE
Si	16	55.17%
No	7	24.14%
No contestaron	6	20.69%
TOTAL	29	100.00%



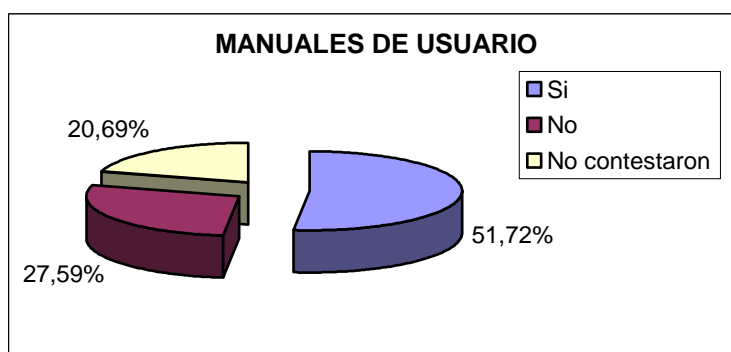
FUENTE: INVESTIGACIÓN DE CAMPO.

El uso de los manuales de funciones dentro de las empresas del sector comercio se da en un 55.17%, mientras que un 24.14% no tiene manuales diseñados. Pero se tuvo la dificultad de que un 20.69% que no proporciono información al respecto.

CUADRO N° 14.

MANUAL DE USUARIO.

USUARIOS	CANTIDAD	PORCENTAJE
Si	15	51.72%
No	8	27.59%
No contestaron	6	20.69%
TOTAL	29	100.00%



FUENTE: INVESTIGACIÓN DE CAMPO.

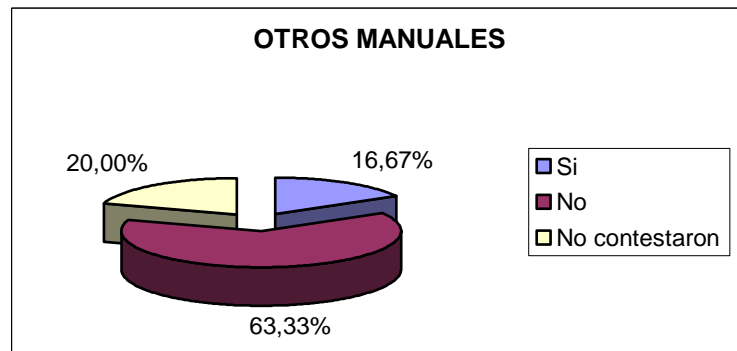
En un 51.72% de las medianas empresas del sector comercio, que hacen uso de medios computarizados tienen elaborados manuales de usuarios para cada puesto, en cambio un 27.59% no posee este tipo de manuales. Y un 20.69% no dio información al respecto.

CUADRO N° 15.

OTROS TIPOS DE MANUALES.

OTROS	CANTIDAD	PORCENTAJE
Si	5	17.24%
No	19	65.52%
No contestaron	6	20.69%
TOTAL	29	100.00%

Nota: otros constituyen manuales técnicos, diccionario de datos, bitácoras de procesos, entidad de relación.



FUENTE: INVESTIGACIÓN DE CAMPO.

Dentro de estas empresas, algunas tienen otro tipo de manuales las que representan un 17.24% entre los cuales figuran los manuales técnicos, diccionarios de datos, bitácoras de procesos y entidad de relación. Y un 65.52% se limita al uso de los de funciones y de usuarios.

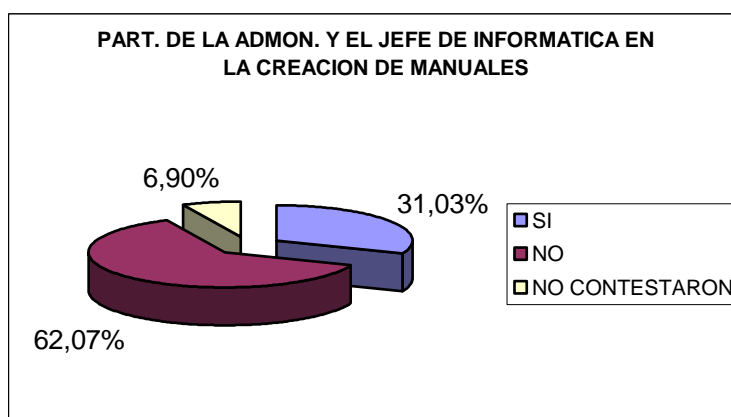
En general, en las medianas empresas del sector comercio es muy poca la cultura del uso de los manuales de funciones y de usuarios en el área o unidad de informática.

4. ¿Para la creación de los manuales, estos fueron elaborados conjuntamente entre la administración y el (los) encargado(s) del área o unidad de informática?

CUADRO N° 16.

CREACIÓN DE MANUALES DE FUNCIONES Y DE USUARIOS.

CRITERIO/ACTIVIDAD	CANTIDAD	PORCENTAJE
SI	9	31.03%
NO	18	62.07%
NO CONTESTARON	2	6.90%
TOTAL	29	100.00%



FUENTE: INVESTIGACIÓN DE CAMPO.

Para la creación de los manuales en las empresas del sector comercio, un 62.07% de estas no consideró a los encargados del área de informática para la creación de los mismos, mientras que un 31.03% de estas, demuestra que si se trabajo en conjunto para el diseño y elaboración de los manuales. Y un 6.90% no proporciono información al respecto.

Considerando las preguntas 3 y 4 se determino: que un poco más del cincuenta por ciento de las medianas empresas del sector comercio de la zona metropolitana hacen usos de los manuales de funciones y de usuarios en el área o unidad de informática pero

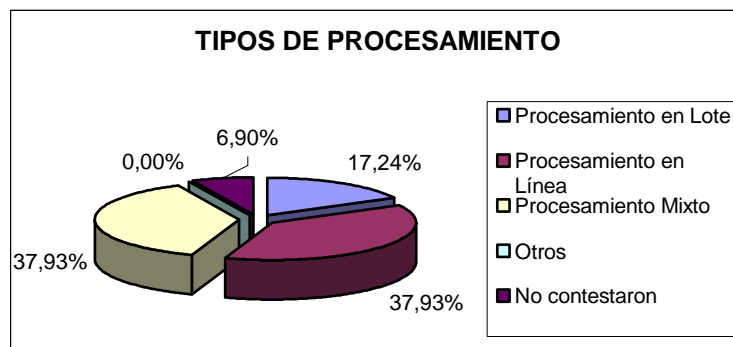
con la deficiencia de que estos no fueron elaborados conjuntamente entre la administración y el encargado de informática.

Esto implica que no han sido elaborados por personas conocedoras del área, así como la poca coordinación entre los mandos alto y medios.

5. ¿El procesamiento de datos para la generación de información se realiza por?

CUADRO N° 17.
TIPOS DE PROCESAMIENTO.

CRITERIO/ACTIVIDAD	CANTIDAD	PORCENTAJE
Procesamiento en Lote	5	17.24%
Procesamiento en Línea	11	37.93%
Procesamiento Mixto	11	37.93%
Otros	0	0.00%
No contestaron	2	6.90%
TOTAL	29	100.00%



FUENTE: INVESTIGACIÓN DE CAMPO.

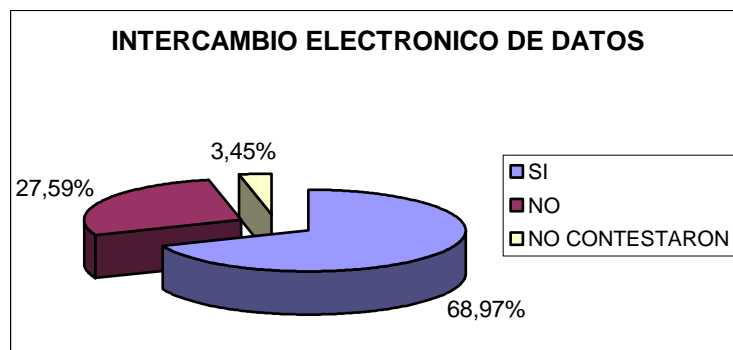
El procesamiento de datos en la mediana empresa se realiza por el procesamiento en línea y el mixto lo que representa un 37.93% cada uno, y al mismo tiempo queda claro que no todas las empresas pueden mantener un procesamiento en línea debido a su alto costo, mientras que el procesamiento en lote es utilizado en un 17.24%.

En base a los datos anteriores, el procesamiento de datos por medios computarizados en la mediana empresa del sector comercio se realiza por medio del procesamiento mixto y en línea, este último se limita a ciertos módulos dentro de las empresas.

6. ¿Existe intercambio electrónico de datos o información entre unidades remotas, en la entidad?

CUADRO N° 18.
INTERCAMBIO ELECTRÓNICO DE DATOS.

CRITERIO/ACTIVIDAD	CANTIDAD	PORCENTAJE
SI	20	68.97%
NO	8	27.59%
NO CONTESTARON	1	3.45%
TOTAL	29	100.00%



FUENTE: INVESTIGACIÓN DE CAMPO.

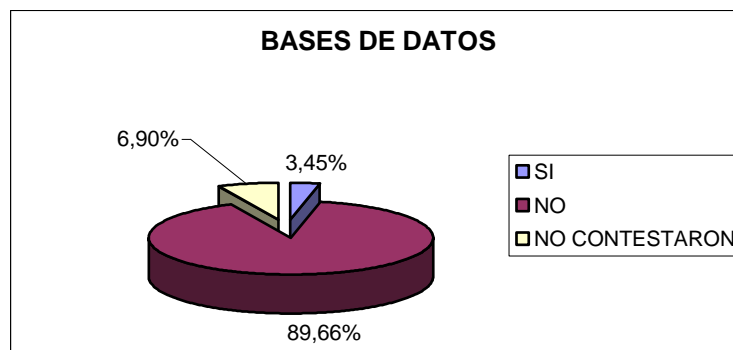
La mediana empresa por estar en un proceso constante de crecimiento les exige tener una ampliación del mercado, lo que les exige un intercambio electrónico de datos con sus unidades remotas (sucursales, bodegas, etc.), lo que se ve reflejado en un 68.97%, y por el contrario un 27.59% no tiene este tipo de intercambio de información.

El uso de sistemas computarizados en las medianas empresas del sector comercio tienden a ser más complejos, por su forma de procesamiento de datos y el intercambio de los mismos.

7. ¿Qué tipo de controles son utilizados en la entrada de datos al sistema de información por computadora?

CUADRO N° 19.
TIPOS DE CONTROL: BASES DE DATOS.

BASES DE DATOS	CANTIDAD	PORCENTAJE
SI	1	3.45%
NO	26	89.65%
NO CONTESTARON	2	6.90%
TOTAL	29	100.00%



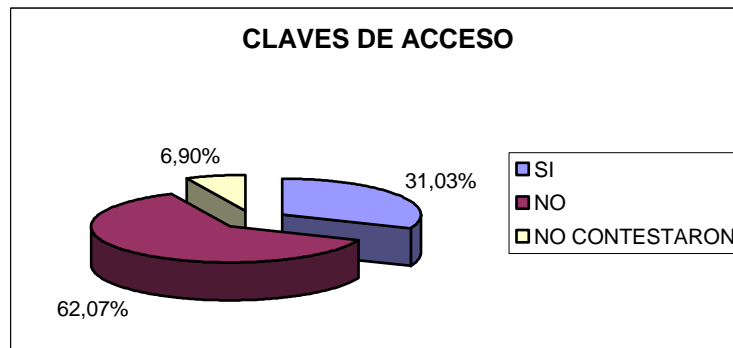
FUENTE: INVESTIGACIÓN DE CAMPO.

Como control en las empresas, es muy poco utilizado el control de bases de datos ya que representan un 3.45% dentro de estas. Por el contrario un 89.65% no los ha implantado, y un 6.90% no proporciono información.

CUADRO N° 20.

TIPOS DE CONTROL: CLAVES DE ACCESO.

CLAVES DE ACCESO	CANTIDAD	PORCENTAJE
SI	9	31.03%
NO	18	62.07%
NO CONTESTARON	2	6.90%
TOTAL	29	100.00%



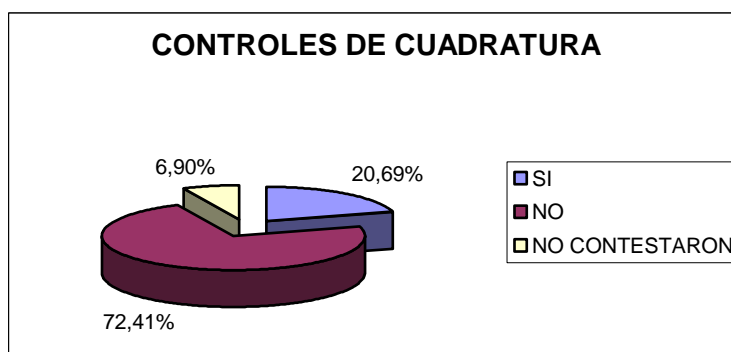
FUENTE: INVESTIGACIÓN DE CAMPO.

Las claves de acceso a módulos específicos son utilizados en un 31.03% en los equipos de computo debido a la importancia de la información que se procesa y su confiabilidad, pero un 62.07% no tiene diseñado y creado este tipo de control. Mientras un 6.90% no dio dato alguno.

CUADRO N° 21.

TIPOS DE CONTROL: DE CUADRATURA.

CONTROLES DE CUADRATURA	CANTIDAD	PORCENTAJE
SI	6	20.69%
NO	21	72.41%
NO CONTESTARON	2	6.90%
TOTAL	29	100.00%



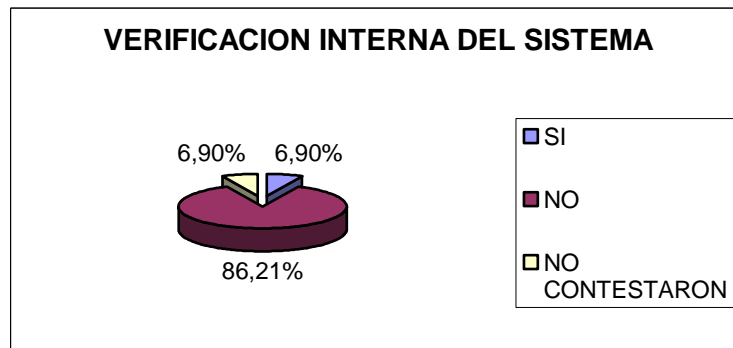
FUENTE: INVESTIGACIÓN DE CAMPO.

Con respecto al uso de controles de cuadratura, las empresas tienen en un 20.69% que si los utiliza, pero un 72.41% no les da importancia alguna por lo que no los utiliza, y no proporcionaron información un 6.90%.

CUADRO N° 22.

TIPOS DE CONTROL: VERIFICACIÓN INTERNA DEL SISTEMA.

VERIFICACIÓN INTERNA DEL SISTEMA	CANTIDAD	PORCENTAJE
SI	2	6.90%
NO	25	86.21%
NO CONTESTARON	2	6.90%
TOTAL	29	100.00%

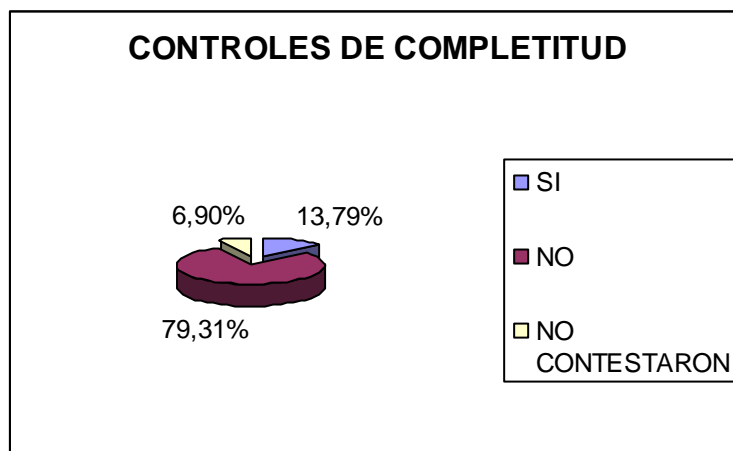


FUENTE: INVESTIGACIÓN DE CAMPO.

Los programas no poseen una aplicación de verificación interna en un 86.21%; sin embargo solamente un 6.90% si lo tiene, y el resto no dio información.

CUADRO N° 23.
TIPOS DE CONTROL: DE COMPLETITUD.

CONTROLES DE COMPLETITUD	CANTIDAD	PORCENTAJE
SI	4	13.79%
NO	23	79.31%
NO CONTESTARON	2	6.90%
TOTAL	29	100.00%



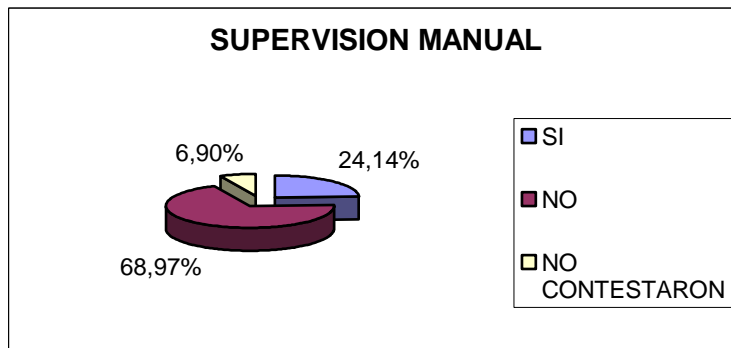
FUENTE: INVESTIGACIÓN DE CAMPO.

Las empresas del sector comercio no dan mucha importancia al control de completitud ya que un 79.31% no posee dicho control y por el contrario un 13.79% si cree y usa este tipo de controles.

CUADRO N° 24.

TIPOS DE CONTROL: SUPERVISIÓN MANUAL.

SUPERVISIÓN MANUAL	CANTIDAD	PORCENTAJE
SI	7	24.14%
NO	20	68.96%
NO CONTESTARON	2	6.90%
TOTAL	29	100.00%



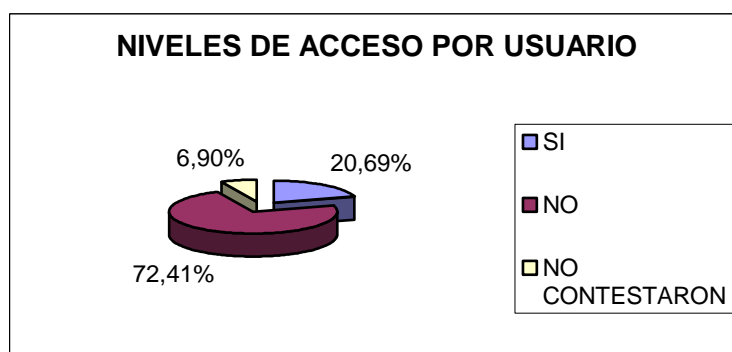
FUENTE: INVESTIGACIÓN DE CAMPO.

La supervisión manual en el procesamiento de datos es muy limitada ya que apenas un 24.14% de las medianas empresas lo practican, pero un 68.96% no realiza ningún tipo de control manual. Mientras que un 6.90% no dio dato alguno.

CUADRO N° 25.

TIPOS DE CONTROL: NIVELES DE ACCESO.

NIVELES DE ACCESO	CANTIDAD	PORCENTAJE
SI	6	20.69%
NO	21	72.41%
NO CONTESTARON	2	6.90%
TOTAL	29	100.00%



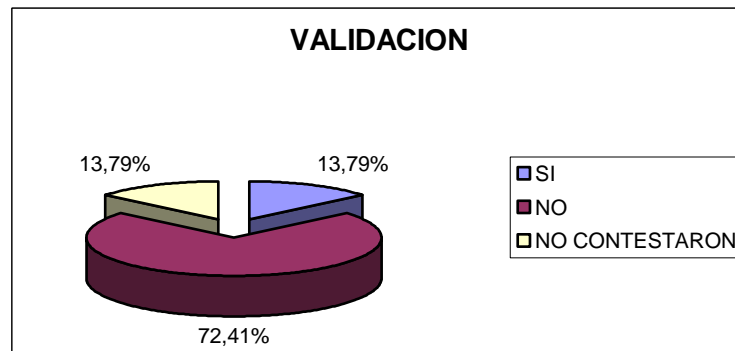
FUENTE: INVESTIGACIÓN DE CAMPO.

En un 20.69% el uso de los equipos de computo poseen niveles de acceso definidos acorde al rol de cada usuario, y un 72.41% no tiene definido este tipo de control que es muy importante dentro de la estructura de controles de cualquier empresa.

CUADRO N° 26.

TIPOS DE CONTROL: VALIDACIÓN AUTOMÁTICA.

VALIDACIÓN	CANTIDAD	PORCENTAJE
SI	4	13.79%
NO	21	72.42%
NO CONTESTARON	4	13.79%
TOTAL	29	100.00%



FUENTE: INVESTIGACIÓN DE CAMPO.

La validación de los datos procesados por sistemas computarizados, es un control muy poco utilizado en el procesamiento de datos, ya que representa un 13.79% en las empresas. Pero un 72.42% de los equipos computarizados no poseen este tipo de control. Y el resto no dio información.

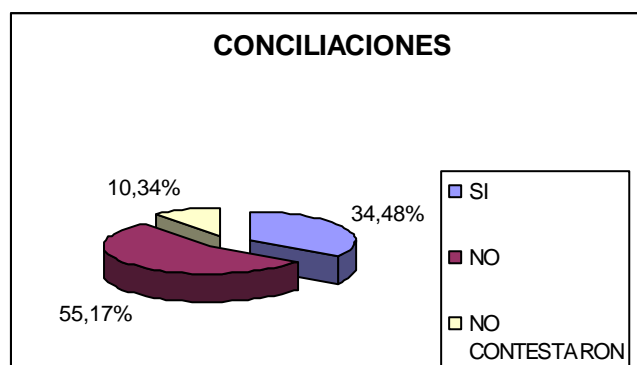
En su mayoría las medianas empresas que procesan información por computadora poseen muy pocos controles en la entrada de datos al sistema computarizado.

8. ¿Cómo se determina que los informes de información contable y financiera extraídos del sistema computarizado son confiables y adecuados?

CUADRO N° 27.

TIPOS DE CONTROL: CONCILIACIONES.

CONCILIACIONES	CANTIDAD	PORCENTAJE
SI	10	34.48%
NO	16	55.17%
NO CONTESTARON	3	10.35%
TOTAL	29	100.00%



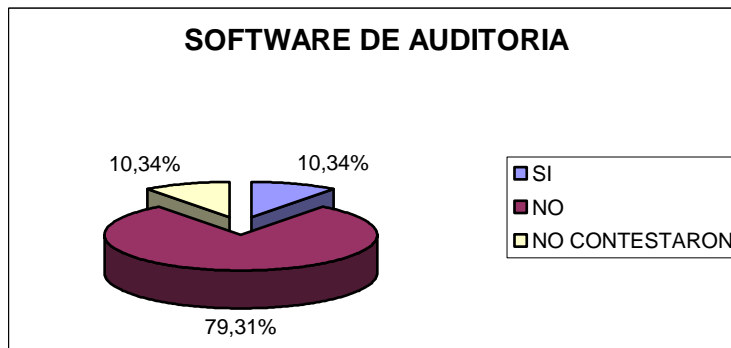
FUENTE: INVESTIGACIÓN DE CAMPO.

Para establecer la confiabilidad y adecuación de los informes, las empresas se limitan a emplear las conciliaciones en un 34.48%, mientras que un 55.17% no pone mayor atención a este tipo de control. Un 10.35% no dio información.

CUADRO N° 28.

TIPOS DE CONTROL: SOFTWARE DE AUDITORÍA.

SOFTWARE DE AUDITORIA	CANTIDAD	PORCENTAJE
SI	3	10.35%
NO	23	79.31%
NO CONTESTARON	3	10.35%
TOTAL	29	100.00%

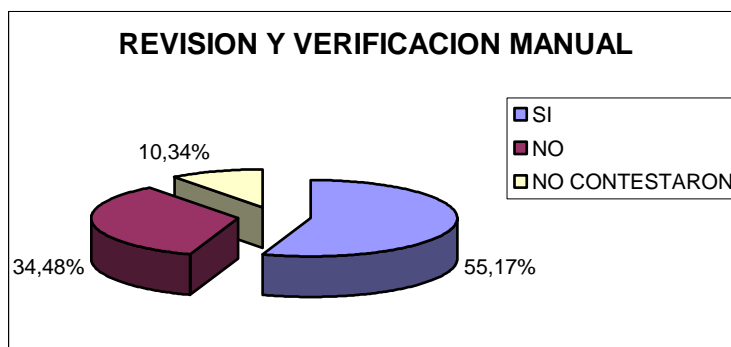


FUENTE: INVESTIGACIÓN DE CAMPO.

Los sistemas computarizados en las medianas empresas utilizan software de auditoría, en un 10.35% para verificar la confiabilidad de sus informes, mientras que un 79.31% no utiliza este medio de control. Un 10.35% no contestó.

CUADRO N° 29.
TIPOS DE CONTROL: REVISIÓN Y VERIFICACIÓN MANUAL.

REVISIÓN Y VERIFICACIÓN	CANTIDAD	PORCENTAJE
SI	16	55.17%
NO	10	34.48%
NO CONTESTARON	3	10.35%
TOTAL	29	100.00%



FUENTE: INVESTIGACIÓN DE CAMPO.

La verificación manual es utilizada en un 55.17% en los sistemas de información por computadora. Por el contrario, un 34.48% no lo aplica y un 10.35% no respondió.

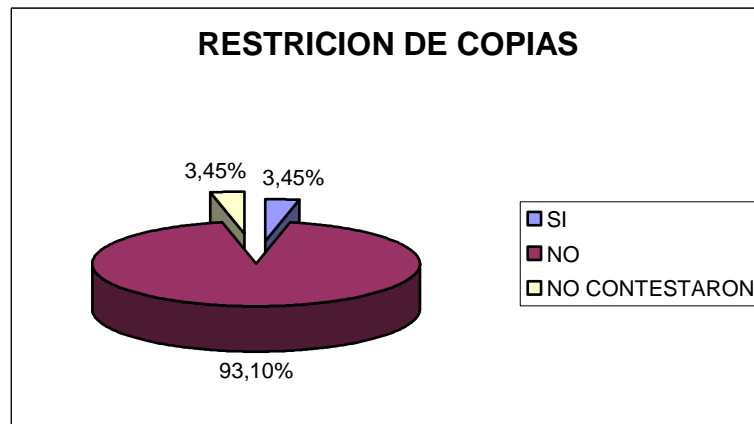
La mediana empresa del sector comercio se limita a utilizar controles manuales para determinar la confiabilidad y oportunidad de los informes financiero-contables, estas lo realizan a través de: conciliaciones, revisiones y verificaciones.

9. ¿Cómo se controla la salida de información contable y financiera de la empresa, ya sea en reportes o almacenada en dispositivos de parte de los usuarios?

CUADRO N° 30.

CONTROLES DE SALIDA: RESTRICCIÓN DE COPIAS.

RESTRICCIÓN DE COPIAS	CANTIDAD	PORCENTAJE
SI	1	3.45%
NO	27	93.10%
NO CONTESTARON	1	3.45%
TOTAL	29	100.00%



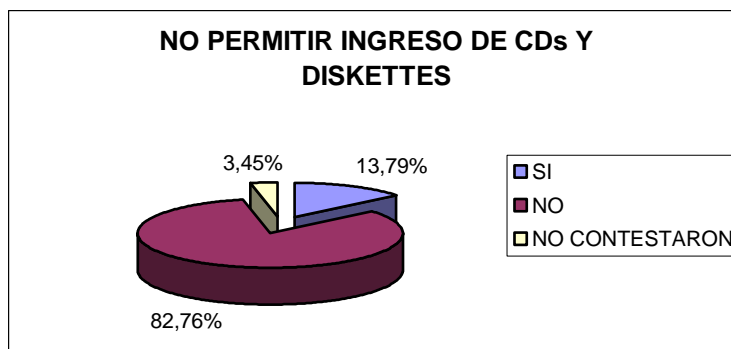
FUENTE: INVESTIGACIÓN DE CAMPO.

Como medios de control de salida de información, las empresas tienen la restricción de copias por medios alternos, esto simboliza un 3.45%, mientras la gran mayoría el 93.10% no la utilizan o no tiene control alguno. Un 3.45% no contestaron.

CUADRO N° 31.

CONTROLES DE SALIDA: RESTRICCIÓN DE INGRESO DE CD's Y DISKETTES.

NO PERMITIR INGRESO DE CD'S Y DISKETTES	CANTIDAD	PORCENTAJE
SI	4	13.79%
NO	24	82.76%
NO CONTESTARON	1	3.45%
TOTAL	29	100.00%



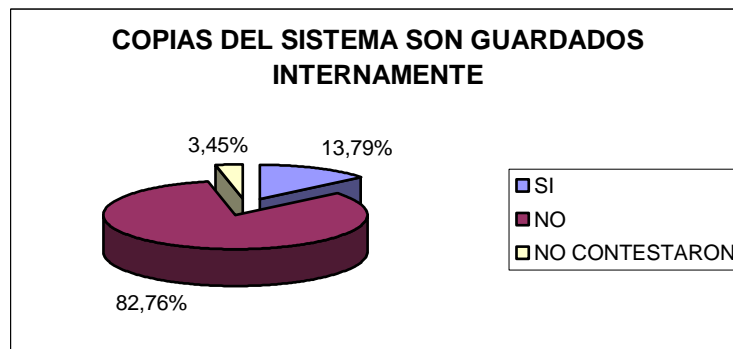
FUENTE: INVESTIGACIÓN DE CAMPO.

La restricción del ingreso al Centro de Informática con medios de almacenamiento magnético de información, es un control poco utilizado ya que figura apenas en un 13.79% de las empresas encuestadas, mientras un 82.76% no tiene controles sobre los mismos, y un 3.45% no contesto.

CUADRO N° 32.

CONTROLES DE SALIDA: RESGUARDO DE COPIAS INTERNAMENTE.

COPIAS DEL SISTEMA SON GUARDADAS INTERNAMENTE	CANTIDAD	PORCENTAJE
SI	4	13.79%
NO	24	82.76%
NO CONTESTARON	1	3.45%
TOTAL	29	100.00%



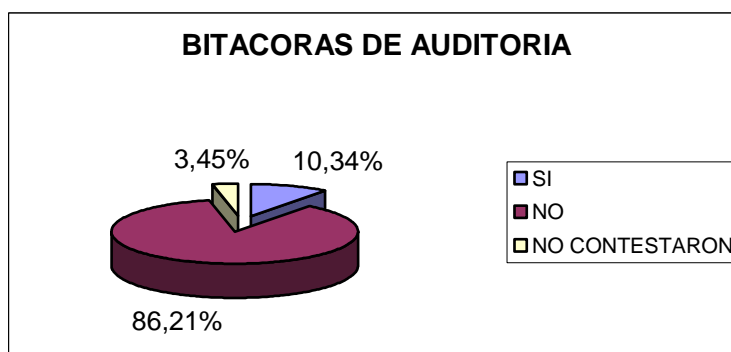
FUENTE: INVESTIGACIÓN DE CAMPO.

El resguardo de las copias de seguridad del sistema a través de cajas de seguridad representan u otro medio alternativo, representa un 13.97% contra un 82.76% que no le presta atención a dicho control. Y un 3.45% no respondieron.

CUADRO N° 33.

CONTROLES DE SALIDA: BITÁCORAS DE AUDITORÍA.

BITÁCORAS DE AUDITORIA	CANTIDAD	PORCENTAJE
SI	3	10.34%
NO	25	86.21%
NO CONTESTARON	1	3.45%
TOTAL	29	100.00%



FUENTE: INVESTIGACIÓN DE CAMPO.

Las bitácoras de auditoría como medios de control representan un 10.34% de la población, mientras un 86.21% no la utilizan. Y un 3.45% no contestó.

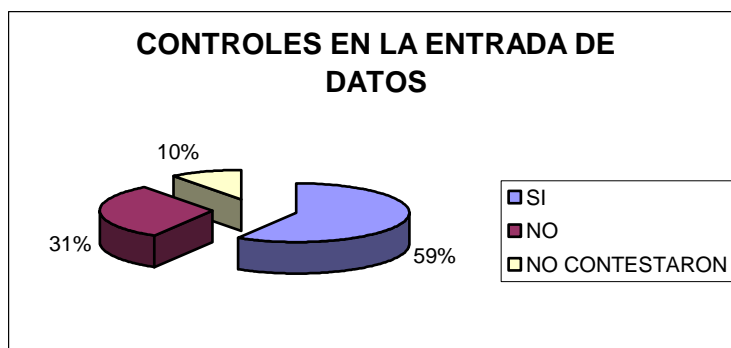
En base a lo anterior, las empresas no poseen controles adecuados o suficientes que permitan supervisar o monitorear la salida de información contable o financiera de las instalaciones de la empresa tanto del personal interno como del externo.

10. ¿Cuáles son los controles establecidos para detectar los errores en las diferentes etapas del procesamiento de datos en el sistema computarizado?

CUADRO N° 34.

CONTROLES DE ENTRADA.

ENTRADA	CANTIDAD	PORCENTAJE
SI	17	58.63%
NO	9	31.03%
NO CONTESTARON	3	10.34%
TOTAL	29	100.00%



FUENTE: INVESTIGACIÓN DE CAMPO.

Nota: los controles los constituyen: Triggers, supervisión, validación, software de auditoría, conciliaciones, completitud, niveles de acceso, claves de acceso, ambiente de prueba.

Del 58.63% de las empresas que tiene controles en la entrada de datos al sistema, en su mayoría se limitan a controles manuales, mientras que un 31.03% no los tiene y un 10.34% no se sabe ya que no respondió.

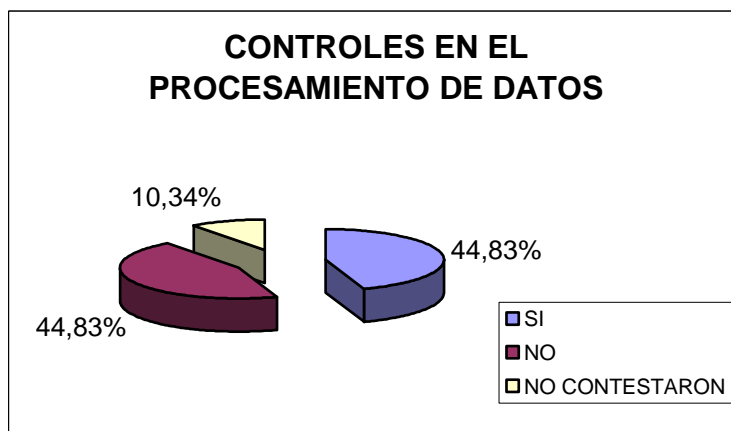
Los controles usados en la entrada, procesamiento y salida de datos, por el personal de la mediana empresa, se limitan a: controles limitados que trae el sistema y controles manuales.

CUADRO N° 35.

CONTROLES EN EL PROCESAMIENTO.

PROCESAMIENTO	CANTIDAD	PORCENTAJE
SI	13	44.83%
NO	13	44.83%
NO CONTESTARON	3	10.34%
TOTAL	29	100.00%

Nota: los controles los constituyen: Triggers, supervisión, validación, software de auditoría, conciliaciones, ambiente de prueba.



FUENTE: INVESTIGACIÓN DE CAMPO.

Para el caso del procesamiento de datos estos si se poseen en un 44.83%, y de estos la mayoría son controles manuales los que son realizados por los usuarios del mismo sistema. Pero un 44.83% de

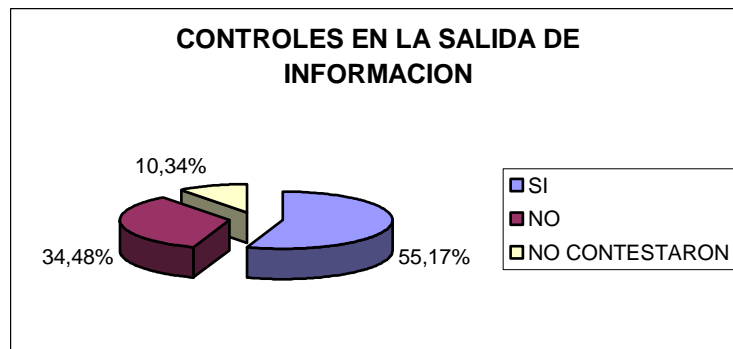
las mismas no tienen control alguno sobre esta etapa del procesamiento y un 10.34% no contestó.

CUADRO N° 36.

CONTROLES DE SALIDA.

SALIDA	CANTIDAD	PORCENTAJE
SI	16	55.17%
NO	10	34.48%
NO CONTESTARON	3	10.35%
TOTAL	29	100.00%

Nota: los controles los constituyen: Triggers, supervisión, validación, software de auditoría, conciliaciones, ambiente de prueba, restricción por niveles de acceso



FUENTE: INVESTIGACIÓN DE CAMPO.

El 55.17% de la muestra de las empresas tienen controles en la salida de información, siempre limitados a los realizados por los usuarios, sin embargo un 34.48% no tiene definido control alguno en la salida de la información por personal interno o externo, y un 10.35% no respondió la pregunta.

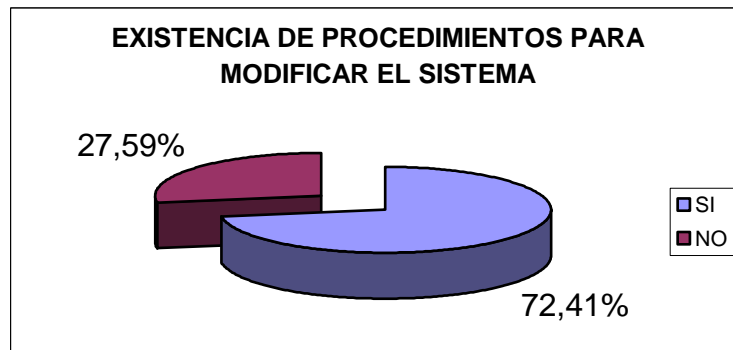
En la mayoría de las medianas empresas del sector comercio, con respecto a la detección de errores, tienen controles en las diversas etapas del procesamiento de datos, pero estos se limitan a controles realizados por el mismo personal interno.

11. ¿Qué tipo de procedimientos se han establecido para la realización de modificaciones o correcciones al sistema?

CUADRO N° 37.

PROCEDIMIENTOS DE MODIFICACIÓN Y/O CORRECCIONES.

CRITERIO/ACTIVIDAD	CANTIDAD	PORCENTAJE
SI	21	72.41%
NO	8	27.59%
TOTAL	29	100.00%



FUENTE: INVESTIGACIÓN DE CAMPO.

Las empresas que tienen en uso un sistema de información computarizado utilizan en un 72.41% procedimientos para realizar

modificaciones o correcciones al sistema. Y un 27.59% no pueden realizar cambio alguno o no tienen procedimientos establecidos.

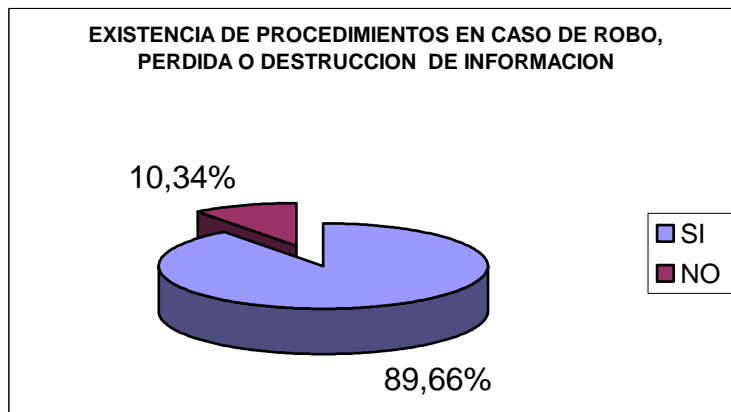
Para realizar cambios y modificaciones a la información procesada por el sistema en la mediana empresa, estas en cierta medida han utilizado algún tipo de procedimiento limitado y además no se encuentra documentado.

12. ¿Qué procedimientos se han establecido en los casos de robo, pérdida o destrucción intencional o accidental de información contable o financiera?

CUADRO N° 38.

PROCEDIMIENTOS EN CASOS FORTUITOS.

CRITERIO/ACTIVIDAD	CANTIDAD	PORCENTAJE
SI	26	89.65%
NO	3	10.35%
TOTAL	29	100.00%



FUENTE: INVESTIGACIÓN DE CAMPO.

Para proteger la información de robo, pérdida o destrucción de la información las empresas en un 89.65% tienen procedimientos establecidos para dichos casos, pero se limitan al uso de las copias de respaldo guardadas dentro de la empresa. Y un 10.35% no tiene considerado algún tipo de medida al respecto.

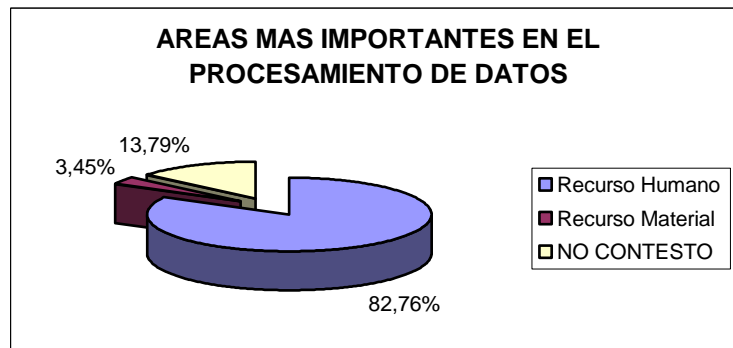
La mayoría de empresas del sector comercio se limitan a utilizar como procedimiento para evitar robos, pérdidas o destrucción de información la extracción de backup o copias de respaldo y documentación impresa., y no hay medidas en concreto para cada situación.

13. ¿Qué aspectos o áreas considera usted que deben ser de mayor atención en el procesamiento de datos para la obtención de información contable y financiera por medio del sistema de información por computadora?

CUADRO N° 39.

ÁREAS DE MAYOR ATENCIÓN EN EL PROCESAMIENTO DE DATOS.

CRITERIO/ACTIVIDAD	CANTIDAD	PORCENTAJE
Recurso Humano	24	82.76%
Recurso Material	1	3.45%
NO CONTESTO	4	13.79%
TOTAL	29	100.00%



FUENTE: INVESTIGACIÓN DE CAMPO.

Un 82.76% de las empresas consideran que el factor humano es el área de mayor importancia y por lo que requiere una atención especial debido a que este se involucra en todas las etapas del procesamiento de datos, y un 3.45% cree que es el recurso material, y el resto no dio mayor aporte.

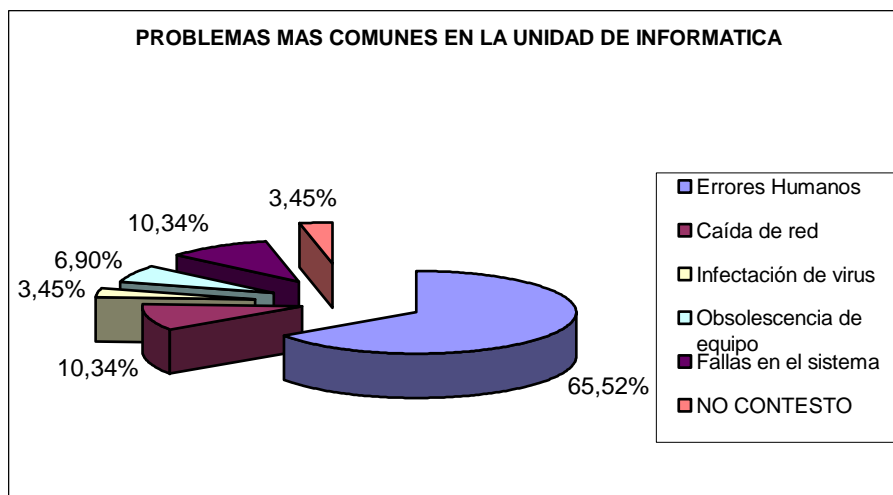
El Recurso Humano en las medianas empresas del sector comercio es un elemento esencial en el procesamiento de datos, y es identificado como uno de los elementos de mayor atención.

14. ¿Cuáles son los problemas más comunes en el área o unidad de informática, con respecto al procesamiento de datos?

CUADRO N° 40.

PROBLEMAS COMUNES EN EL ÁREA O UNIDAD DE INFORMÁTICA.

CRITERIO/ACTIVIDAD	CANTIDAD	PORCENTAJE
Errores Humanos	19	65.52%
Caída de red	3	10.34%
Infectación de virus	1	3.45%
Obsolescencia de equipo	2	6.90%
Fallas en el sistema	3	10.34%
NO CONTESTO	1	3.45%
TOTAL	29	100.00%



FUENTE: INVESTIGACIÓN DE CAMPO.

Sobresalen los errores humanos con un 65.52%, en las diversas etapas del procesamiento de datos por medios computarizados, le sigue con un 10.34% las fallas del sistema y la caída de la red. Otro problema es la obsolescencia de los equipos con un 6.90%, y en un 3.45% la infestación de virus e igual porcentaje no contesto.

En el área o unidad de informática se considera que los usuarios del sistema son los que más contribuyen a generar errores en el procesamiento de la información.

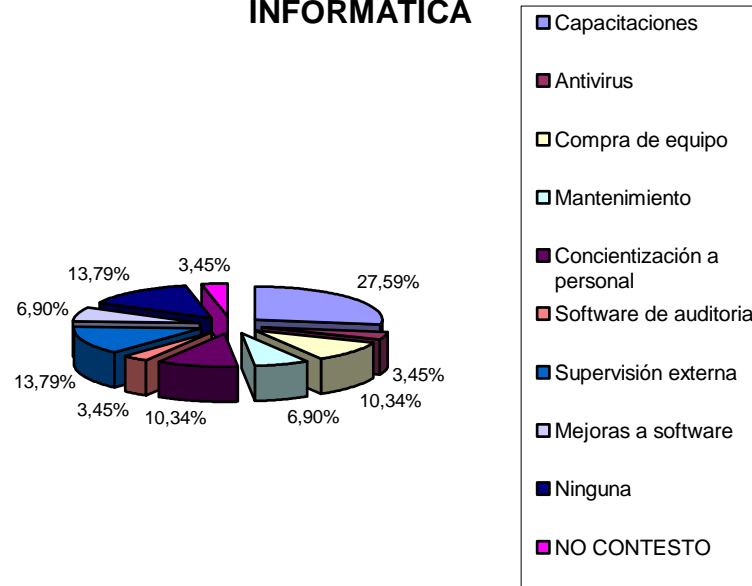
15. De los problema antes señalados. ¿Qué medidas se han implementado para minimizar el efecto de estos, y su prevención en un futuro?

CUADRO N° 41.

MEDIDAS PARA MINIMIZAR PROBLEMAS EN EL ÁREA O UNIDAD DE
INFORMÁTICA.

CRITERIO/ACTIVIDAD	CANTIDAD	PORCENTAJE
Capacitaciones	8	27.59%
Antivirus	1	3.45%
Compra de equipo	3	10.34%
Mantenimiento	2	6.90%
Concientización a personal	3	10.34%
Software de auditoria	1	3.45%
Supervisión externa	4	13.79%
Mejoras a software	2	6.90%
Ninguna	4	13.79%
NO CONTESTO	1	3.45%
TOTAL	29	100.00%

MEDIDAS PARA MINIMIZAR LOS PROBLEMAS EN EL AREA DE INFORMATICA



FUENTE: INVESTIGACIÓN DE CAMPO.

Entre las medidas que las empresas consideran para minimizar los problemas están las capacitaciones con un 27.59%; un 13.79% consideran la supervisión externa, mientras que un 10.34% se enfocan a concientizar al personal y la adquisición de nuevos equipos, así como el mantenimiento y las mejorar al software en un 6.90%; y otras medidas que representan el 3.45% son los antivirus, los software de auditoría.

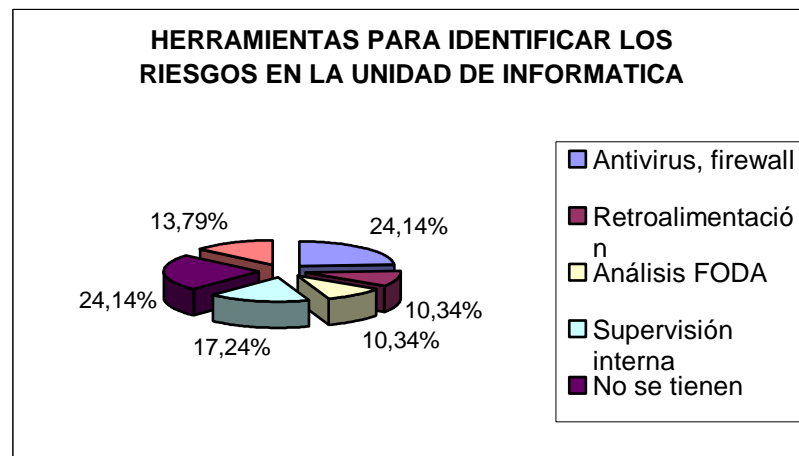
El principal problema dentro de la mediana empresa específicamente en el procesamiento de datos en el área o unidad de informática son lo errores humanos.

16. ¿Que herramientas se utilizan para identificar y estudiar las amenazas del área o unidad de informática?

CUADRO N° 42.

HERRAMIENTAS PARA IDENTIFICAR EL RIESGO EN EL ÁREA O UNIDAD DE INFORMÁTICA.

CRITERIO/ACTIVIDAD	CANTIDAD	PORCENTAJE
Antivirus, firewall	7	24.14%
Retroalimentación	3	10.34%
Análisis FODA	3	10.34%
Supervisión interna	5	17.24%
No se tienen	7	24.14%
NO CONTESTO	4	13.80%
TOTAL	29	100.00%



FUENTE: INVESTIGACIÓN DE CAMPO.

Las herramientas utilizadas en la mediana empresa para identificar amenazas en el área o unidad de informática se limita en un 24.14% a la utilización de los antivirus, seguidamente se piensa que la supervisión interna realizada por

el usuario en un 17.24% servirá para tal efecto. Otros consideran en un 10.34% a la retroalimentación y el análisis FODA como herramientas adecuadas. Pero cabe destacar que un 24.14% no tiene herramienta alguno para identificar amenazas internas y externas. Y un 13.80% no respondió.

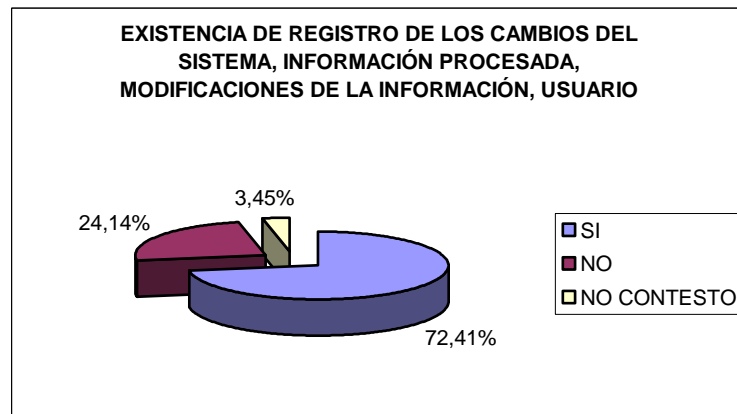
En su mayoría las medianas empresas del sector comercio no tienen una herramienta adecuada que les permita estudiar e identificar las posibles amenazas a la que esta expuesto el área o unidad de informática.

17. ¿El sistema computarizado permite llevar un registro de los cambios del sistema, información procesada, modificaciones de la información, usuario, entre otros?

CUADRO N° 43.

REGISTRO DE CAMBIOS AL SISTEMA E INFORMACIÓN.

CRITERIO/ACTIVIDAD	CANTIDAD	PORCENTAJE
SI	21	72.41%
NO	7	24.14%
NO CONTESTO	1	3.45%
TOTAL	29	100.00%



FUENTE: INVESTIGACIÓN DE CAMPO.

En un 72.41% los sistemas computarizados de las empresas poseen de alguna manera un registro de los cambios, modificaciones, correcciones e información procesada realizadas por los usuarios; mientras que un 24.14% no posee dicha base. Y un 3.45% no respondió la interrogante.

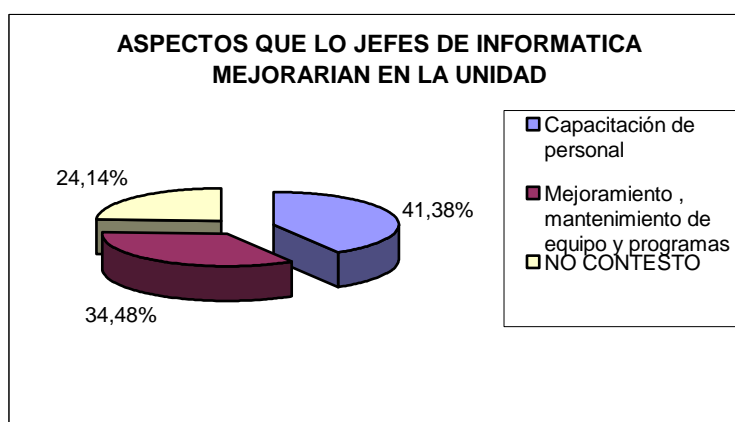
De alguna manera las empresas tienen algún tipo de control diseñado para monitorear los cambios que se realizan en el sistema.

18. ¿Qué aspectos o actividades propondría para mejorar el procesamiento de datos por medio del sistema computarizado y como debería realizarse para la obtención de información contable y financiera?

CUADRO N° 44.

PROPUESTAS PARA MEJORAR EL ÁREA O UNIDAD DE INFORMÁTICA.

CRITERIO/ACTIVIDAD	CANTIDAD	PORCENTAJE
Capacitación de personal	12	41.38%
Mejoramiento , mantenimiento de equipo y programas	10	34.48%
NO CONTESTO	7	24.14%
TOTAL	29	100.00%



FUENTE: INVESTIGACIÓN DE CAMPO.

Para mejorar el procesamiento de datos, las empresas consideran en un 41.38% la capacitación técnica del recurso humano, un 34.48% manifiesta que el mantenimiento y mejoramiento del equipo y programas mejoraría el procesamiento de datos internamente. Y un 24.14% no respondió.

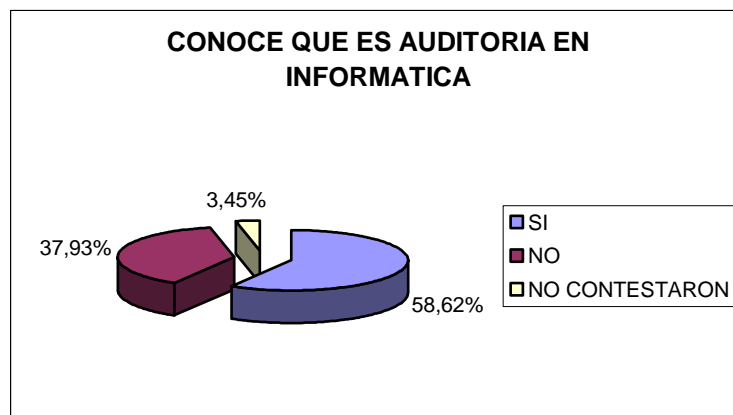
La formula ideal que propone el área o unidad de informática para solucionar los problemas en el procesamiento de datos seria la capacitación del recurso humano acompañado de la adquisición de equipo y programas adecuados. La mayoría de los encuestados coinciden en dicha solución.

19. ¿Conoce en que consiste una auditoría en informática?

CUADRO N° 45.

CONOCE LA AUDITORÍA EN INFORMÁTICA.

CRITERIO/ACTIVIDAD	CANTIDAD	PORCENTAJE
SI	17	58.62%
NO	11	37.93%
NO CONTESTARON	1	3.45
TOTAL	29	100.00%



FUENTE: INVESTIGACIÓN DE CAMPO.

De los encuestados, un 58.62% dijo conocer en que consiste una auditoría en informática, mientras que un 37.93% expreso no saber en que consiste. Y un 3.45% no respondió.

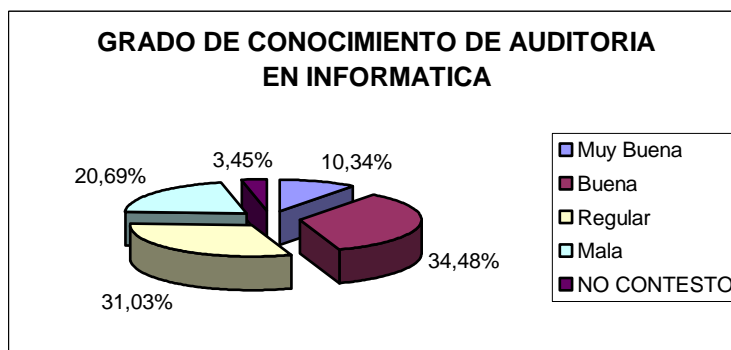
La mayoría de los responsables del área o unidad de informática respondieron conocer en que consiste una auditoría en informática. Lo cual se comprobara con las respuestas de la siguiente pregunta.

20. Independientemente de su respuesta a la pregunta anterior. ¿Qué entiende por auditoría en informática?

CUADRO N° 46.

ENTIENDE LA AUDITORÍA EN INFORMÁTICA.

CRITERIO/ACTIVIDAD	CANTIDAD	PORCENTAJE
Muy Buena	3	10.34
Buena	10	34.48%
Regular	9	31.03%
Mala	6	20.70%
NO CONTESTO	1	3.45%
TOTAL	29	100.00%



FUENTE: INVESTIGACIÓN DE CAMPO.

Solamente un 10.34% se podría decir que entiende muy bien en que consiste una auditoría en informática, mientras que un 34.48% tiene buenos conocimientos al respecto, sin embargo un 31.03% tiene una idea regular, y un 20.70% tiene mala apreciación de dicha actividad. Y el 3.45% no dio información al respecto.

En realidad, las personas del área de informática no tienen un concepto o idea adecuada de lo que realmente es una auditoría en informática, ya que más del cincuenta por ciento de los encuestados tiene una mala conceptualización al respecto.

ANEXO 2

LISTA DE CHEQUEO.

Lista de chequeo para la auditoría a la administración del factor humano en el área de sistema.

Calificar el grado de cumplimiento de:	100%	75%	50%	25%
La coordinación de las funciones, actividades, tareas, y operaciones del personal informático del área de sistemas.				
La división funcional de las actividades y operaciones del factor humano del área de sistemas.				
Los planes y programas de capacitación, adiestramiento y promoción del personal y usuarios del área de sistemas.				
La rotación y movilidad del personal de área.				
La motivación para el personal y usuarios del área.				
Los procesos de selección de personal para el área de sistemas.				
La remuneración y prestaciones para el personal del área.				
Integración de grupos de trabajo.				
La evaluación del cumplimiento de funciones y actividades del personal, del perfil de puestos y la asignación de puestos en el área.				
La gestión directiva de funcionarios, empleados y usuarios.				

Auditoría a la administración de los recursos informáticos en el área de sistemas.

Calificar el grado de cumplimiento de:	100%	75%	50%	25%
La administración de los sistemas computacionales. (Hardware) del área de sistemas y del sistema de las demás áreas de la empresa.				
La administración de los sistemas computacionales. (Software) del área de sistemas y del sistema de las demás áreas de la empresa.				
La administración de las instalaciones del sistema computacional del área de sistema y demás áreas que cuenten con sistemas.				
La administración de las telecomunicaciones del sistema.				
La administración de las bases de datos e información del área de sistemas.				
La administración del mobiliario y equipo asignado al área de sistemas.				
La administración de los bienes materiales, consumibles y materiales de oficina utilizada en el área de sistemas.				
La administración de las adquisiciones de sistemas computacionales, hardware, software, componentes, periféricas, equipos, consumibles y demás implementos para el funcionamiento del área de sistema.				
La administración de los bienes informáticos y activos del área de sistemas.				
Los planes, programas y presupuestos que afectan el área de sistemas.				
La gestión financiera y contable de los recursos del área de sistemas.				

Auditoría a los controles informáticos del área de sistemas.

Calificar el grado de cumplimiento de:	100%	75%	50%	25%
Los controles internos sobre la organización del área de sistemas.				
Los controles internos sobre el desarrollo de sistemas.				
Los controles internos sobre la operación del sistema.				
Los controles sobre los procedimientos de entrada, procesamiento de información y emisión de resultados.				
Los controles internos sobre la seguridad en el área de sistemas.				

Evaluación de los métodos de acceso, seguridad, salvaguarda de los activos informáticos del área de sistemas.

Evaluar y calificar el cumplimiento de los siguientes aspectos:	Excelente	Bueno	Regular	Mínimo	No Cumple
Planes y programas de prevención contra contingencias en el funcionamiento de los sistemas, de la información y datos de la empresa y en los demás bienes informáticos del centro de cómputo y demás áreas que cuenten con sistemas.					
Identificar de acceso, almacenamiento y custodia de la información, sistemas operativos, lenguajes, archivos y programas institucionales.					
Evaluación de controles y sistemas de seguridad, protección y salvaguarda de los activos, del personal, instalaciones, información, mobiliario y equipo del área de sistemas y de las demás áreas.					
Planes contra contingencias para seguridad y protección de los programas, información, instalaciones, empleados y usuarios del sistema.					
Sistemas de control de accesos lógicos al sistema y a las bases de datos.					
Sistemas de control de accesos físicos al					

centro de cómputo.					
Prevención y erradicación de virus informáticos.					
Sistemas de protección y de supresión de sistemas piratas y juegos en los sistemas computacionales.					

El levantamiento de inventarios a fin de hacer un recuento de los bienes informáticos del área de sistemas

Evaluar y calificar el cumplimiento de los siguientes aspectos:	Excelente	Bueno	Regular	Mínimo	No Cumple
Inventarios de los equipos de computo, contemplando las marcas, procesadores, tarjetas madres, velocidad, configuración, componentes, memorias, sistemas de almacenamiento, tarjetas adicionales, números de serie, responsables de su resguardo y todos los demás aspectos relacionados con estos equipos					
Inventario de los sistemas operativos, lenguajes, programas, paqueterías, utilerías y demás software institucional, incluyendo licencias, resguardos, originales, copias autorizadas y copias piratas					
Inventario de personal informático y usuarios del sistema, a fin de evaluar sus perfiles de puestos, conocimientos características y preparación para el uso de los sistemas computacionales de la empresa					
Inventario de bienes muebles, inmuebles, materiales y consumibles del área de sistemas					
Inventario de los sistemas de redes cuando el sistema este diseñado de esta manera					
Inventario de instalaciones físicas, protecciones, características y funcionalidad de las áreas del sistema, contemplando su medio ambiente de trabajo, iluminación, aire acondicionado, ruidos,					

temperatura, estática y demás peculiaridades de su funcionamiento					
Otros inventarios acordes a las necesidades de la auditoría					
El diseño físico del área de sistemas y de las áreas de la empresa que cuenten con sistemas computacionales					
El análisis y aprobación de las propuestas para la adquisición del software, hardware, periféricas, equipos adicionales y bienes muebles, consumibles y materiales diversos que permitan el funcionamiento del sistema					
El medio ambiente de trabajo en el que se realiza la función de informática de la empresa					
La gestión administrativa de la función de informática de la empresa					
El diseño de proyectos de nuevos sistemas computacionales en el área de sistemas					
El diseño de formato, formas y métodos para la recopilación de información que será utilizada en el sistema					
La administración y control de los sistemas de seguridad y salvaguarda de los activos informáticos, la información, el personal y los usuarios del sistema					
La administración y control de accesos a las instalaciones del área, a los sistemas, a la información y los bienes informáticos del área					
Todos aquellos aspectos especiales que intervienen de alguna manera en el aprovechamiento y explotación del sistema computacional y en la gestión administrativa del centro de cómputo. Con la condición indiscutible de no interferir directamente en el uso del equipote computo					

ANEXO 3

MATRIZ DE CONTROL INTERNO

En la Matriz tenemos que en las columnas se registran las Normativas Externas e Internas, como así también los Principios y Políticas relacionadas al SIC cuya aplicación debe verificarse.

Por el lado de las filas tenemos los Productos, Servicios, Áreas / Sectores - Actividades / Procesos que tienen lugar en la compañía.

Así pues, una vez colocados los títulos de las columnas y filas, corresponde interrelacionar los mismos (Ejemplo: Ventas / Recurso Humano) en función de las normativas, procedimientos y funciones los cuales deberán dar cumplimiento las áreas, actividades. En caso de no existir interrelación entre el ítem de la fila con el de la columna, dicho espacio se anula (sombreado) (Ejemplo: Ventas y Registro de la propiedad Intelectual).

A cada punto de los casilleros le corresponde un cuestionario de control aplicable al ambiente SIC, así también servirán para asignar recursos en el presupuesto de control, como también para

establecer cantidad de controles por períodos y delegar responsabilidad del control respectivo.

Se debe resaltar que el juicio del auditor prevalecerá al momento de asignar el estándar para identificar las áreas deficientes.

Ejemplo: Si un cuestionario posee 8 preguntas de las cuales tienen 5 SI, el porcentaje es de 62,50%, en tanto que el puntaje es de 6,25 puntos. De igual forma si otro cuestionario tuviera 10 preguntas de las cuales 5 fueran sí, el porcentaje sería de 50% y el puntaje de 5. De ésta forma se logra un análisis bastante objetivo. Pero no todas las preguntas tienen igual importancia, razón por la que puede mejorarse el sistema otorgándole una ponderación. De tal forma a aspectos menores se le daría un puntaje de 1 punto, a aspecto de nivel medio 2 puntos y a cuestiones fundamentales 3 puntos.

Ejemplo: Para un cuestionario de 10 preguntas, con 3 de valor 1, cuatro de valor 2 y 3 de valor tres, el puntaje máximo sería de 20 puntos. Si las respuestas positivas fueron 2 de un punto, 2 de dos puntos y 1 de tres puntos, lo obtenido asciende a 9 puntos, con lo que se tiene un porcentaje de efectividad del 45% y un puntaje de 4,5.

Los puntajes en lugar de uno, dos y tres, podrían ser de uno, tres y cinco, para hacer más sensible el puntaje final a los aspectos más importantes.

Se aplica el mismo razonamiento para obtener el puntaje correspondiente a cada punto de la matriz, así si de contar un determinado punto de la matriz con cuatro cuestionarios cuyo puntaje máximo de responderse a todas las preguntas positivamente sería de 40 puntos y se obtuvo un total de 35 puntos, el porcentaje de efectividad es del 87,05% y el puntaje de 8,71 puntos.

Por último y dado que no todas las áreas - actividades o productos están sujetos a las mismas cantidades de puntos de control, se multiplica por 10 todos los puntos de control obteniéndose el puntaje máximo posible, se suman los puntos obtenidos de acuerdo al párrafo anterior y se divide por dicho máximo obteniéndose el puntaje de efectividad por área.

Veamos: el área o actividad "Ventas" de un total de 9 casilleros, tiene 8 puntos de control. Si multiplicamos 8 por diez tenemos un puntaje máximo de 80 puntos. Supongamos que de los controles realizados surge un puntaje máximo de 43.2 puntos, el porcentaje de efectividad es de 54.00%, o sea un puntaje de 5.4.

Igual criterio es aplicable a las columnas, así tenemos que "Registro de la Propiedad Intelectual" tiene dos casilleros puntuables de un total de 9, por lo que el puntaje máximo es de 20 puntos. Si el puntaje obtenido es de 9.28 puntos tendremos un 0.464% de efectividad y un puntaje de 4.64.

MATRIZ DE CONTROL INTERNO.

ÁREAS - PRODUCTOS - ACTIVIDADES.		NORMAS Y ÁREAS A VERIFICAR.									
		1	2	3	4	5	6	7	8	9	
		LEYES NACIONALES	NORMATIVA CONTABLE. (NIIF)	POLÍTICA ORGANIZACIONAL	NORMAS INTERNAS	PRINCIPIOS DE CONTROL INTERNO	REGISTRÓ PROPIEDAD INTELECTUAL.	RECURSO HUMANO.	SEGURIDAD LÓGICA.	SEGURIDAD FÍSICA	
1	VENTAS	6,00	6,30	7,00	8,00	4,50		5,00	4,50	1,90	5,40
2	COMPRAS	6,56	5,00	6,50	9,40	6,00		2,30	4,00	2,90	5,33
3	RR.HH.	5,50	6,15	8,34	7,22	4,00		3,30	3,40	3,90	5,23
4	CÓMPUTOS	8,00	7,32	6,22	5,77	5,00	4,14	4,30	4,40	4,90	5,56
5	CONTABLE	6,50	6,80	7,55	5,11	6,00	5,14	5,30	5,40	5,90	5,97
6	CRÉDITOS Y COBROS.	6,00	6,00	5,80	5,00	6,00		6,00	5,00	7,00	5,85
7	FINANZAS	7,00	6,00	7,00	8,20	6,00		7,00	6,00	6,50	6,71
8	DISTRIBUCIÓN	6,50	6,75	7,00	6,20	5,00		8,00	6,50	7,00	6,62
9	SERVICIOS	6,00	6,00	5,00	7,15	4,00		12,30	7,00	5,00	6,56
		6,45	6,26	6,71	6,89	5,17	4,64	5,94	5,13	5,00	

ANEXO 4

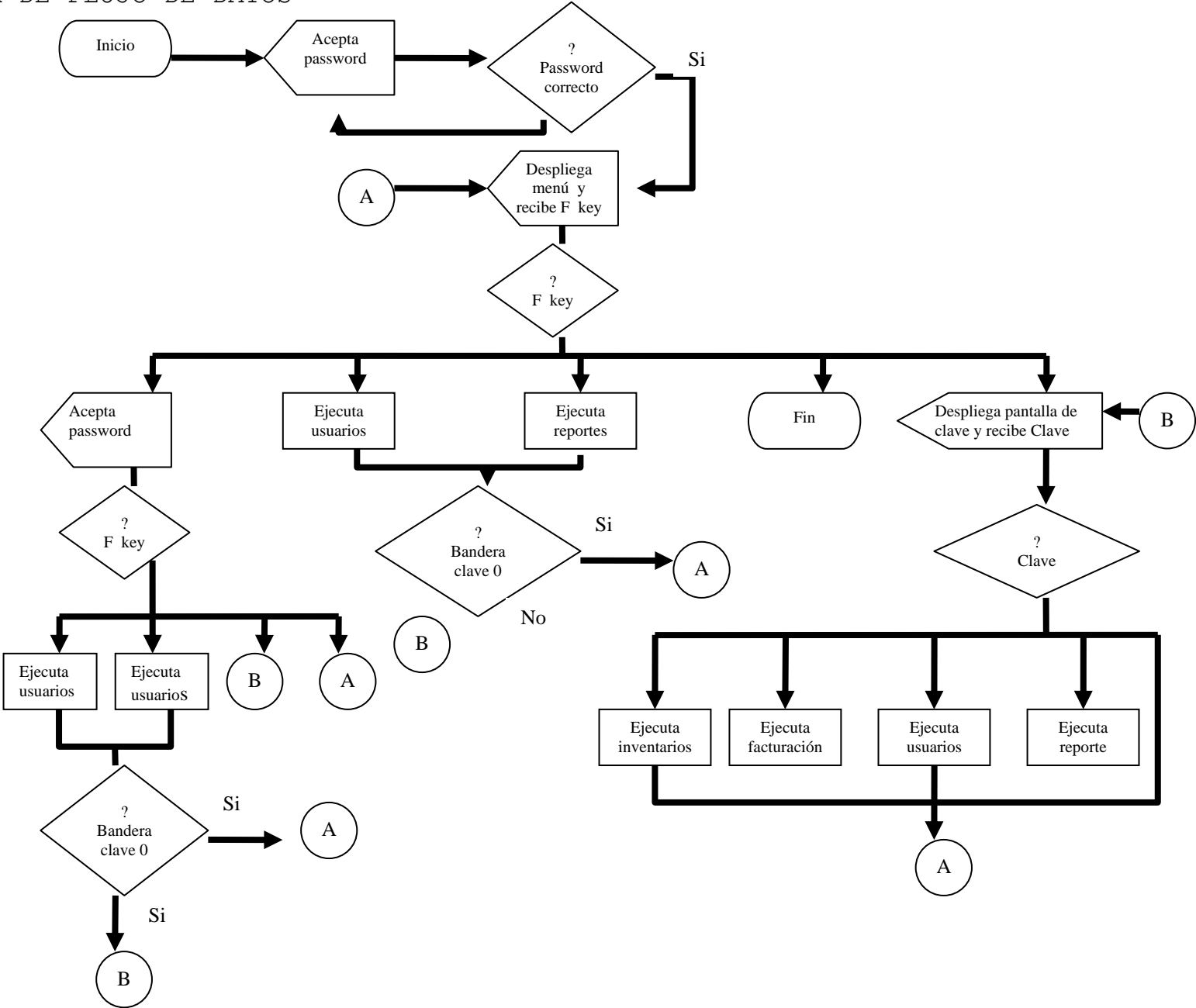
SIMULACIÓN Y DIAGRAMACIÓN (FLUJOGRAMA).

Como ya se leyó antes simular significa aparentar, fingir. En auditoría en informática, simular significa:

“La imitación formal del sistema computacional, mediante un modelo simulado, en cuanto al funcionamiento del hardware, software, información, instalaciones o aplicaciones, en la cual se representan sus principales características de operación, forma de captura, procesamiento de datos y emisión de resultados del sistema original, con el propósito de estudiar el comportamiento del sistema y evaluar su funcionamiento real. En estos modelos se pueden aplicar datos ficticios o reales, pero sin que esta simulación llegue a influir en la actividad normal del sistema original”.

Esta simulación se puede realizar a través de software diseñados para correrlo con el software original o realizar procedimientos que debería hacer el sistema original. Pero no solo a través de software diseñados, se puede realizar una simulación, otra forma es a través de diagramas de flujo que demuestran una situación específica y como debería ser tratada por el sistema y el resultado que debería de dar. Estos diagramas pueden representar

DIAGRAMA DE FLUJO DE DATOS

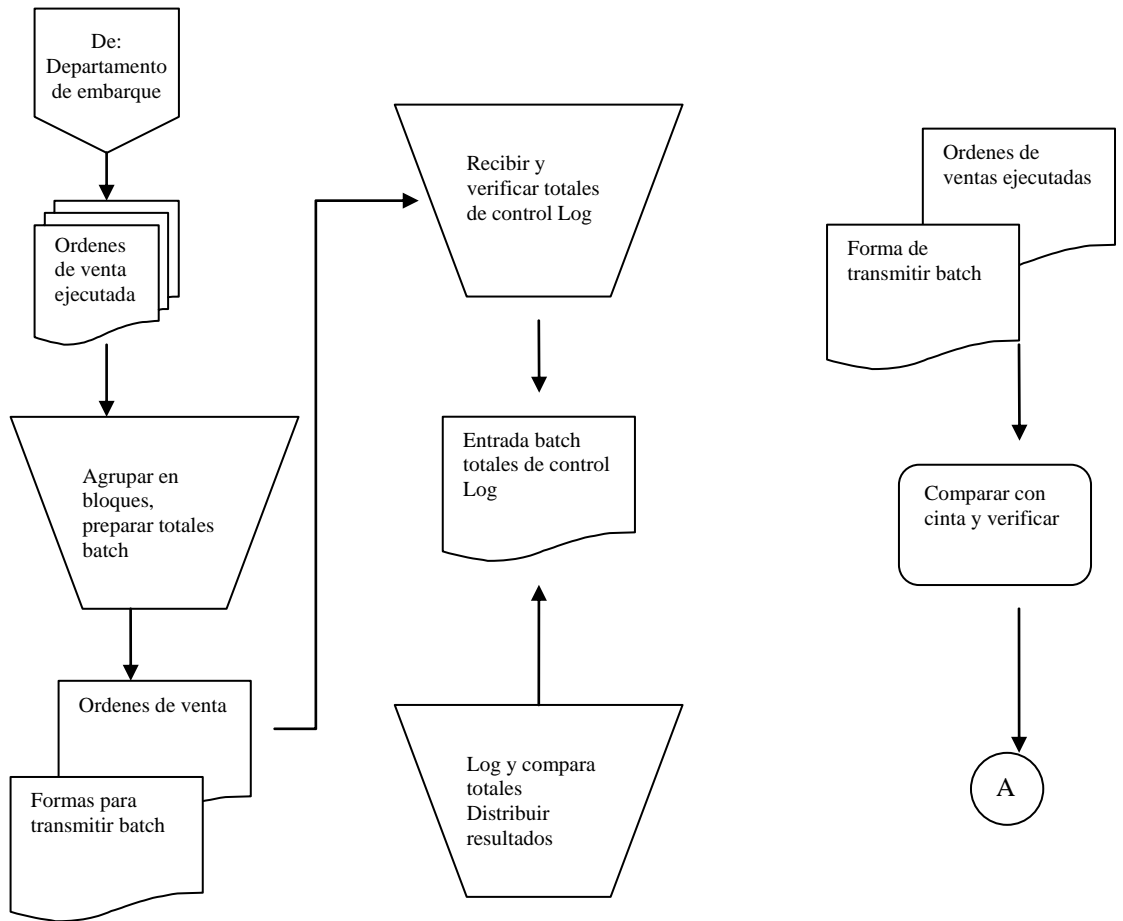


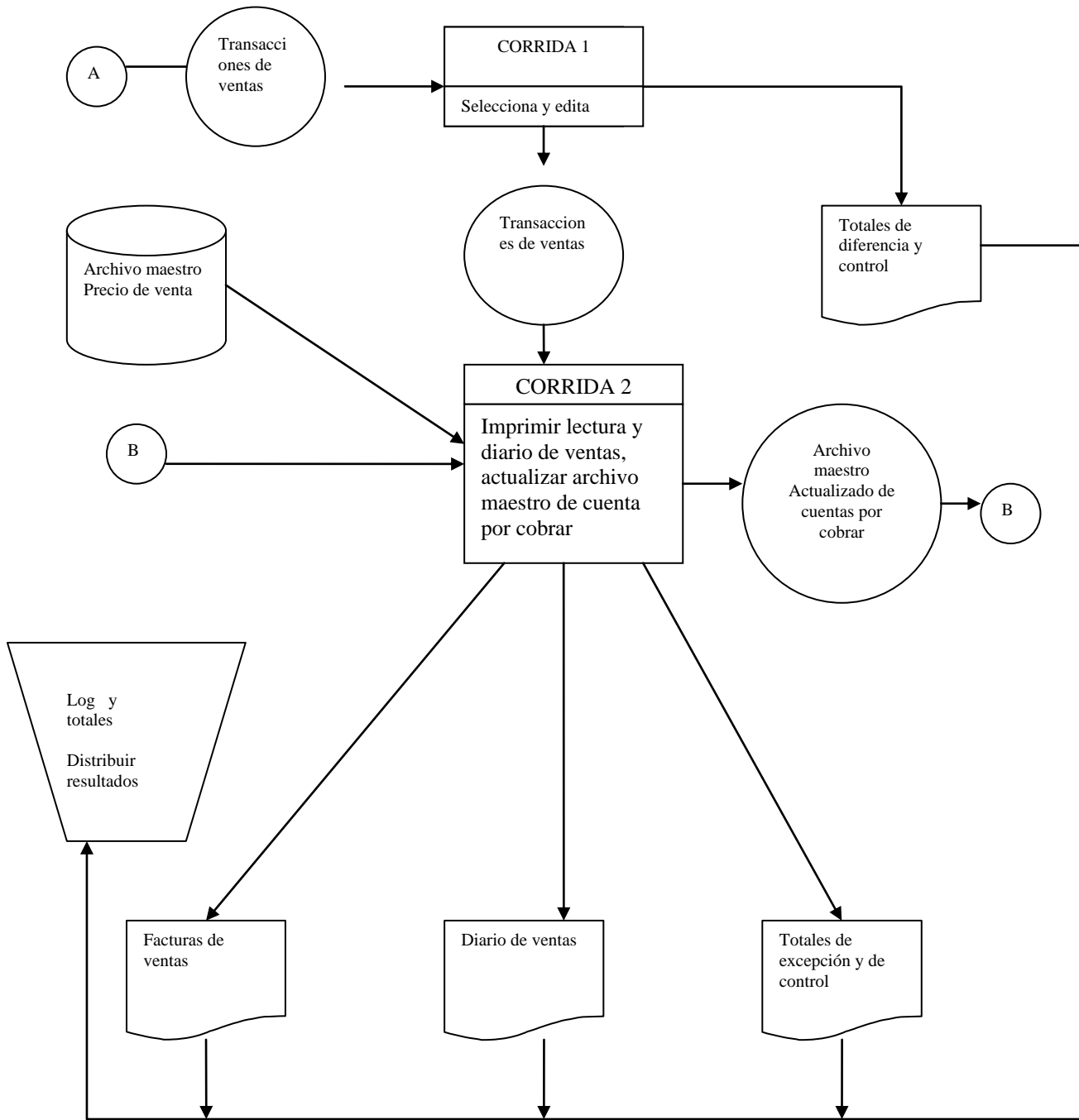
FLUJOGRAMA DE SISTEMAS PARA TRANSACCIONES DE VENTAS

DEPARTAMENTO FACTURACIÓN

GRUPO DE CONTROL DE DATOS

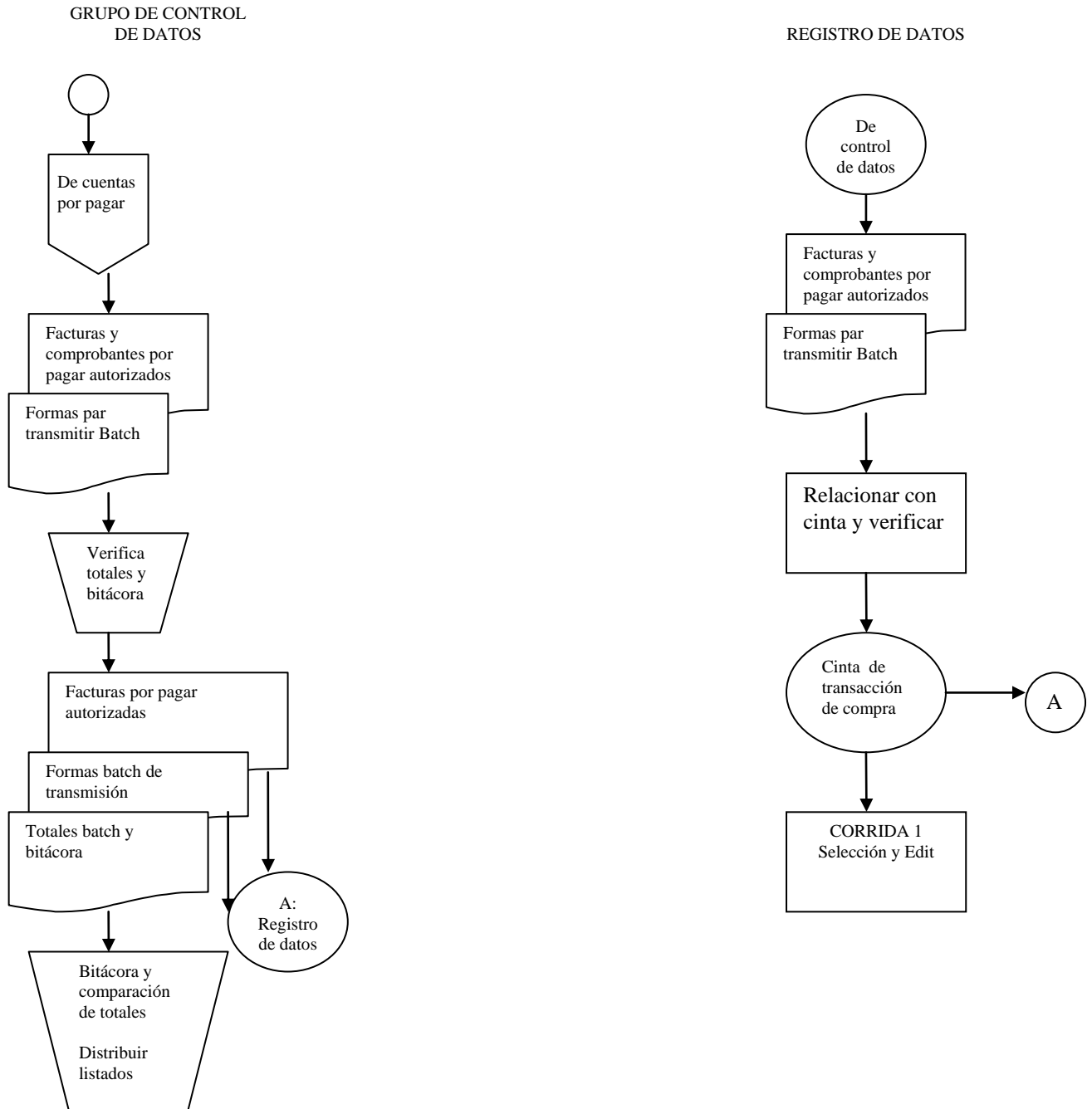
ACCESO DE DATOS

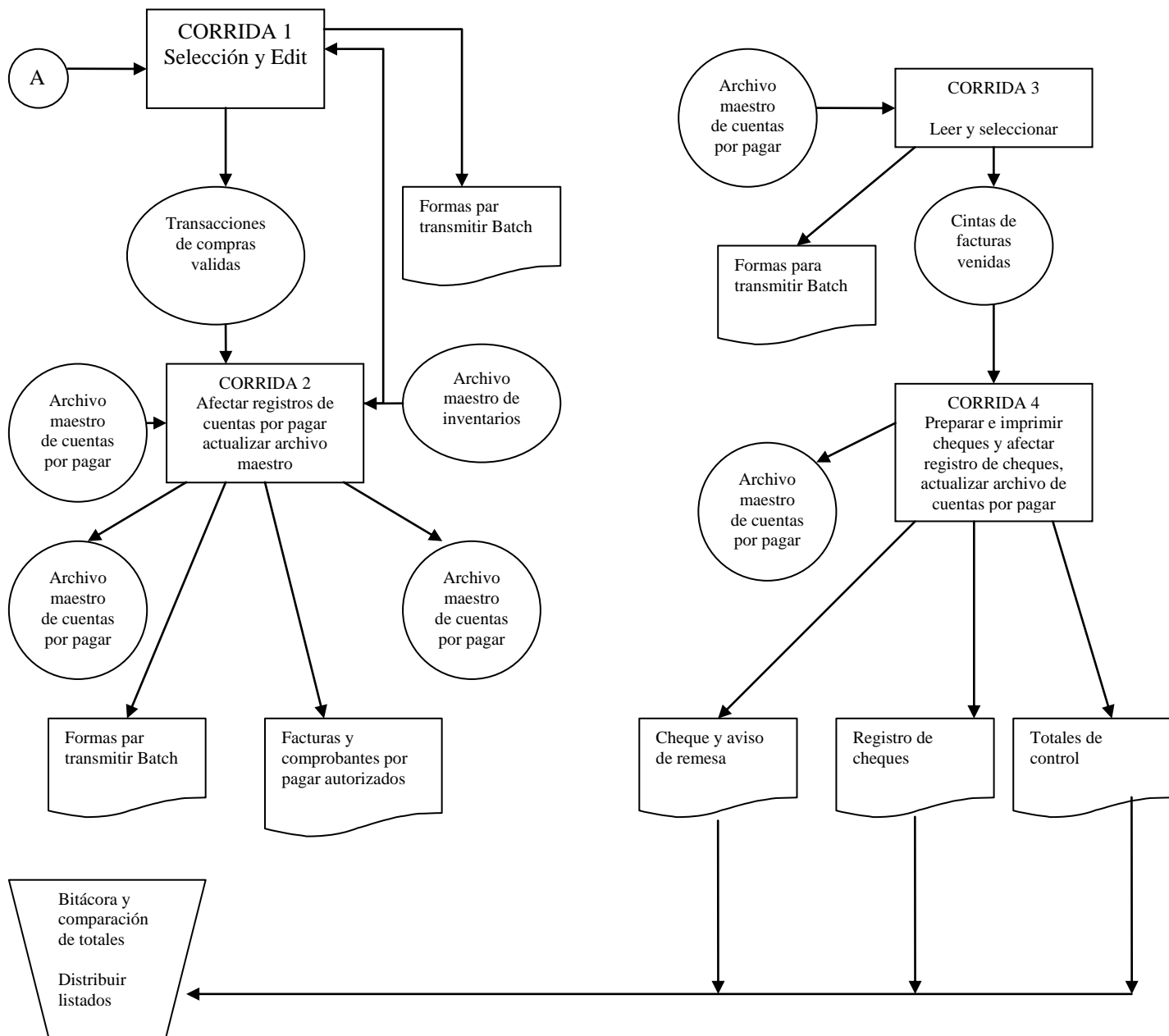




FLUJOGRAMA SISTEMA PARA TRANSACCIONES DE COMPRAS Y

DESEMBOLSOS EN EFECTIVO





ANEXO 5.

PROGRAMAS DE CUMPLIMIENTO DE AUDITORÍA EN INFORMÁTICA

NOMBRE DE LA FIRMA

NOMBRE DEL CLIENTE

PROGRAMA AUDITORÍA EN INFORMÁTICA

ÁREA ESTRUCTURA ORGANIZATIVA Y RECURSO HUMANO

PERIODO _____

OBJETIVO: Conocer políticas, procedimientos y normas establecidos por la administración en el área de informática.

No	ACTIVIDAD
1	Solicite la estructura organizativa del departamento de informática
2	Elabore una guía de entrevista dirigida al personal de informática
3	Elabore una narrativa que contenga el proceso que se lleva a cabo en la introducción y desarrollo del personal del área
4	Solicite la programación de las necesidades de personal en donde se le especifique calidad y cantidad
5	Cerciorese de la distribución de las 3 funciones de ingreso de datos y la obtención de la información
6	Determinar los resultados sobre cada uno de los elementos contenidos en el cuestionario. (Narrativa y cedula de hallazgo.)
7	Considerar el uso de la matriz de control interno para evaluar el riesgo de control de esta área.

Elaborado por: _____

Revisado por: _____

NOMBRE DE LA FIRMA

NOMBRE DEL CLIENTE

PROGRAMA DE AUDITORÍA EN INFORMÁTICA

ÁREA HARDWARE

PERIODO _____

OBJETIVO: Evaluar el cumplimiento del control interno relacionado con el equipo

No	ACTIVIDAD
1	Obtener las políticas de seguridad establecidas para los sistemas y programas, y toda información que se relacione con esta área.
2	Encuestar al personal del área de informática y los usuarios del sistema al menos en lo relacionado a: <ul style="list-style-type: none">- Características del equipo con que cuenta la empresa.- Controles de los medios de almacenamiento.- Seguridad ambiental.- Pólizas de seguro.- Seguridad en la utilización de equipo.
3	Entrevistar al encargado de informática. En relación a los resultados obtenidos en el cuestionario; juzgué los elementos a tener en cuenta.
4	Elabore cedula en donde refleje los resultados obtenidos de los procedimientos siguiente: <ul style="list-style-type: none">- Observar si existen reguladores de voltaje para protección del fluido eléctrico, así como baterías par la interrupción de ese servicio.- Inspeccionar que los ductos de aire acondicionado se encuentren limpios.- Verificar la existencia de un sistema de aislamiento de las oficinas de informática con el resto de las

	<p>oficinas de la empresa.</p> <ul style="list-style-type: none"> - Inspeccionar que las instalaciones físicas estén provistas de extintores y que el personal tenga la capacidad de hacer uso de ello en caso de emergencia. - Observar si existen suficientes salidas de emergencia. - Verificar si existe un sistema de aislamiento ambiental como cerraduras, puertas herméticas, entre otras. - Verificar la cobertura de las pólizas de los riesgos, garantía de los proveedores. - Observar la existencia de rótulos de prohibición en el área tales como: "no comer", "no fumar", "acceso solo a personal autorizados". - Observar que el personal que hace uso del equipo este debidamente autorizado para ello.
5	Determinar los resultados sobre cada uno de los elementos contenidos en el cuestionario. (Narrativa y cedula de hallazgo.)
6	Considerar el uso de la matriz de control interno para evaluar el riesgo de control de esta área.

Elaborado por: _____

Revisado por: _____

NOMBRE DE LA FIRMA

NOMBRE DEL CLIENTE

PROGRAMA DE AUDITORÍA EN INFORMÁTICA

ÁREA HARDWARE

PERIODO _____

OBJETIVO: Obtener evidencia de la adecuada aplicación del control interno en la seguridad del equipo de cómputo

No	ACTIVIDAD
1	Prepare cedula de auditoría que muestre lo movimientos del hardware en el ejercicio, considerando lo siguiente: <ul style="list-style-type: none">- Saldo inicial- Compra o incrementos- Bajas- Saldos finales
2	Respecto a las compras e incrementos del año, examinar la siguiente documentación con objeto de verificar: <ul style="list-style-type: none">- Autorización- Requisiciones, Pedidos y contratos- Facturas- Inspeccionar físicamente las principales adquisiciones- Aplicación contable
3	En relación a las bajas por destrucción, sustitución o venta verifique: <ul style="list-style-type: none">- Autorización- Documentación comprobatoria

4	<p>Elabore una cedula de auditoría en donde evalúe y califique las características mas importantes de los siguientes elementos del hardware:</p> <ul style="list-style-type: none"> - Tarjeta madre del sistema - Procesador - Unidades adicionales, características, interfaz y capacidad - Tarjetas adicionales al sistema - Periféricas externos asociados al sistema
5	<ul style="list-style-type: none"> - Aprovechamiento y utilidad del sistema computarizado - Mantenimiento básico para el sistema computarizado.
6	<p>Determinar los resultados sobre cada uno de los elementos contenidos en el cuestionario. (Narrativa y cedula de hallazgo.)</p> <p>Considerar el uso de la matriz de control interno para evaluar el riesgo de control de esta área.</p>

Elaborado por: _____

Revisado por: _____

NOMBRE DE LA FIRMA

NOMBRE DEL CLIENTE

PROGRAMA DE AUDITORÍA EN INFORMÁTICA

ÁREA PROCESAMIENTO DE DATOS (ENTRADA)

PERIODO _____

OBJETIVO: Conocer la existencia de controles en la entrada de datos, así como procedimientos escritos

N	ACTIVIDAD
1	Solicitar los informes de auditoria interna (si existe esta unidad) acerca de la seguridad que ofrece el sistema de acceso al sistema informático y las conclusiones.
2	Solicitar el diagnostico que la compañía aseguradora (si existe), ha hecho en torno al sistema de seguridad del sistema informático.
3	Solicitar los informes y dictámenes de auditoria en informática anteriores y las medidas que la administración ha tomado.
4	Encuestar al encargado del área o unidad de informática así como a los usuarios, considerando. <ul style="list-style-type: none">- Segregación de funciones.- Asignación de responsabilidades.- Los controles de datos de entrada directa.- Los controles de codificación.- Controles de documentos fuentes.- Controles de ingreso y validación- Controles de recuperación de datos.- Pistas de auditoría.

5	Revisar el esquema de autorizaciones para determinar si las autorizaciones de acceso son consistentes con la segregación de tareas, y si se proporciona confidencialidad a los datos más sensibles
6	Identificar los métodos a través de los cuales se hace efectivo el acceso en la comunicación de los datos, y diagnosticar si las intromisiones son solo una posibilidad remota.
7	Verificar que las llaves de usuarios se encuentran a salvo dentro de la base de datos.
8	Debe verificarse la capacidad de la base de datos, en cuanto a la capacidad de recuperación ante fallas
9	Determinar los resultados sobre cada uno de los elementos contenidos en el cuestionario. (Narrativa y cedula de hallazgo.)
10	Considerar el uso de la matriz de control interno para evaluar el riesgo de control de esta área.

Elaborado por: _____

Revisado por: _____

NOMBRE DE LA FIRMA

NOMBRE DEL CLIENTE

PROGRAMA DE AUDITORÍA EN INFORMÁTICA

ÁREA PROCESAMIENTO DE DATOS (PROCESAMIENTO)

PERIODO _____

OBJETIVO: Obtener información básica que nos permita identificar los controles aplicados en la etapa procesamiento de datos.

No	ACTIVIDAD
1	Pasar un cuestionario al personal encargado del procesamiento de datos en el sistema.
2	Verificar la existencia de políticas y normas interna que guíen el procesamiento de datos.
3	Solicitar los procedimientos para evitar interrupciones prolongadas del procesamiento de datos
4	Solicitar los manuales de usuarios y revisar los tipos de controles en el procesamiento de datos.
5	Verificar la existencia de planes de contingencias.
6	Revisar los procedimientos en casos de modificaciones.
7	Determinar los resultados sobre cada uno de los elementos contenidos en el cuestionario. (Narrativa y cedula de hallazgo.)
8	Considerar el uso de la matriz de control interno para evaluar el riesgo de control de esta área.

Elaborado por: _____

Revisado por: _____

NOMBRE DE LA FIRMA

NOMBRE DEL CLIENTE

PROGRAMA DE AUDITORÍA EN INFORMÁTICA

ÁREA PROCESAMIENTO DE DATOS (SALIDA DE INFORMACIÓN)

PERIODO _____

OBJETIVO: Obtener la información necesaria para la determinación de medidas de seguridad en la salida de información en forma magnética y de reporte

No	ACTIVIDAD
1	Solicitar las políticas y procedimiento diseñados por al administración para controlar la salida de información.
2	Realizar una entrevista al encargado o usuarios del sistema a fin de obtener una opinión sobre los controles del sistema y sus problemas.
3	Solicitar, verificar y analizar listado de todos los reportes clasificados por área de operación.
4	Evaluar los métodos utilizados para almacenar la información (Si existen respaldo fuera de la empresa como cajas de seguridad)
5	Revisar los controles, formatos y registros documentales de las salidas de información del área de informática
6	Determinar los resultados sobre cada uno de los elementos contenidos en el cuestionario. (Narrativa y cedula de hallazgo.)
7	Considerar el uso de la matriz de control interno para evaluar el riesgo de control de esta área.

Elaborado por: _____

Revisado por: _____

ANEXO 6.

NARRATIVA

Nombre de la firma de auditoría:
Empresa:
Elaborado por:
Periodo:
Área auditada:

DESCRIPCIÓN	OBSERVACIÓN O COMENTARIO
<ol style="list-style-type: none">1. El departamento de informática e encuentra en un lugar separado del área operativa de la empresa, es una habitación de sistema mixto, con ventanas de vidrio y cortinas de plástico. Se mantienen extintores contra incendios y se renuevan cada año.2. El gerente administrativo de la empresa no ha accedido a adquirir un seguro contra incendios y robos; se puede observar que el techo presenta pequeñas grietas por lo que se filtra el agua en épocas lluviosas ocasionando inconvenientes.3. Es de hacer notar que las instalaciones cuentan con alarma contra robo, el cual se activa al momento de tratar de desplazar alguna maquina de su ubicación.4. A los empleados nuevos, según lo informa el jefe de informática se le da una inducción de 15 días para el cuidado y uso de la computadora ya que no existe manual de procedimientos adecuados al área	

ANEXO 7FORMATO PARA LEVANTAMIENTO DE INVENTARIO FÍSICO DEL
HARDWARE

Nombre de la firma de auditoria:

Auditor:

Periodo:

Área auditada:

INVENTARIO INDIVIDUAL DE HARDWARE

No.	EQUIPO	MARCA	NO DE INVENTARIO	CARACTERÍSTICAS	OBSERVACIONES
1	Conexión en red				
2	Computador	HACER	AS-1002-1		
3	Procesador	Pentium IV		Intel 4	
4	Coprocesador	N/A			
5	Motherboard	Biostar			
6	Velocidad procesador	2.26 ghz			
7	RAM instalado	128 Mb			Inicio con 64 mb y se aumento a 128 mb
8	RAM instalable	256 Mb			
9	Memoria CACHE	800 Mb			
10	Monitor	LG	AS-1002-2	1024X768	
11	Tarjeta de multimedia	Sond elaster		64 bits	
12	Tarjeta de sonido	N/A			
13	Tarjeta de video	CIRRUS LOGIA		4 mb	
14	Tarjeta de red	NOVELL	Ra-20006	Lm 4.0	
15	Tarjeta de tv	PÍXEL VIEW	AS-1002-3		
16	Bocinas	GOLD STAR	AS-1002-4	150 watts	
17	Disco duro	SEAGATE	AS-1002-5	40 gb	
18	CD- ROM	MITSUMI	AS-1002-6	56X	
19	DVD				
20	CR-W				
21	Fax modems	36.9 KEFS	AS-1002-7	Full duplex	
22	Impresor	Hp 620	AS-1002-8	A color	
23	Teclado	Microsoft	AS-1002-9	At- 101	
24	Mouse	Microsoft	AS-1002-C		

ANEXO 8

INFORME DE CONTROL INTERNO

1. Portada.
2. Índice.
3. Introducción.
4. Contenido del informe.
5. Anexos (carta a la gerencia y cédulas de cumplimiento de hallazgos)

San Salvador, 27 Noviembre de 2,004

Señores

Junta Directiva

SKF S.A. DE C.V.

Presente.

Estimados señores:

Hacemos de su conocimiento que este despacho de Auditoría y consultoría ha realizado la evaluación del control interno, mediante cuestionarios con el objeto de establecer los alcances para examen del área de informática para el año, 2004. De dicha evaluación se determinaron observaciones y recomendaciones en los puntos que se presentan a continuación:

OBSERVACIONES Y RECOMENDACIONES

1. El equipo no esta protegido con cubiertas especiales, siendo esta actividad necesaria para la vida útil del equipo de cómputo.

2. No existe contrato de mantenimiento preventivo y correctivo par el equipo informático.

3. No se posee contraseña para acceder a cada uno de los programas que se utilizan.

Es necesario que todo el personal involucrado posea claves de acceso a todos los programas que utiliza en el área de producción.

4. Es necesario adquirir estos contratos para evitar fallas en el equipo y prolongar su vida útil.

5. Existe poca seguridad contra riesgos inesperados.

Se recomienda suscribir pólizas de seguro de fidelidad y otras pertinentes para garantizarla seguridad tanto del equipo como de los programas.

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

Por lo delicado del caso se efectuar un estudio técnico a fin de superar las deficiencias par la seguridad física del equipo y de los empleados que laboran en la unidad.

7. Las impresiones no utilizadas, no son destruidas.

Se recomienda girar instrucciones e incorporar al manual de procedimientos, el hecho de destruir todos los reportes generados y no utilizados.

8. No existen copias de seguridad de los archivos fuera de la empresa.

Se estima conveniente que por cualquiera eventualidad se mantengan copias de archivos fuera del área de informática.

Se espera de nuestras observaciones y recomendaciones sean de utilidad a su empresa.

Atentamente.

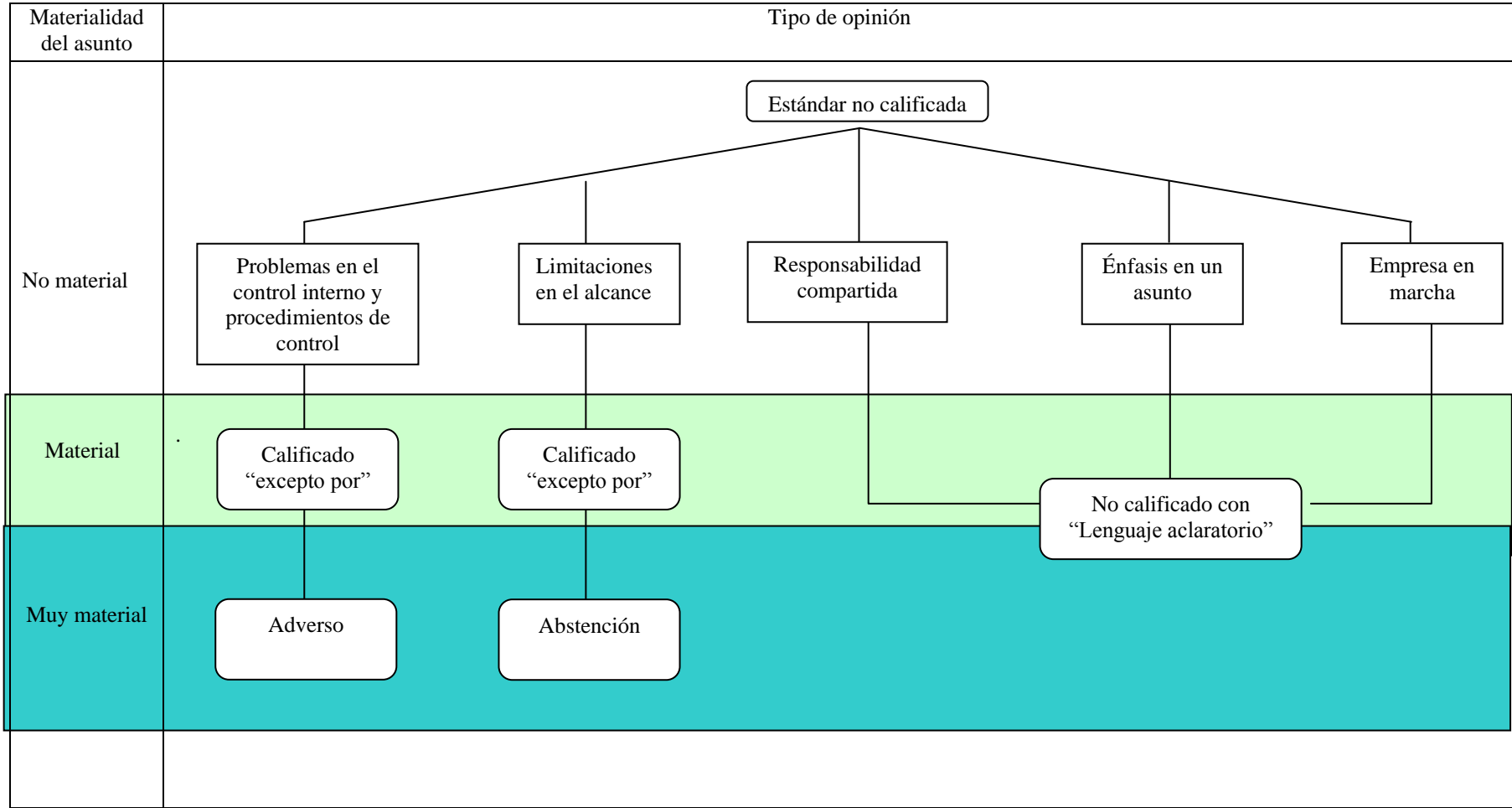
Evelyn Marlene Claros Cruz.

Jefe de auditoría en Informática

Ruiz Ruiz y Asociados

ANEXO 9.

TIPOS DE OPINIÓN.



ANEXO 10.

Detalle de los resultados obtenidos por área auditada.

ÁREA AUDITADA	AMBIENTE DE CONTROL.	PROCEDIMIENTOS DE CONTROL.	COMENTARIO.
RECURSO HUMANO (USUARIOS).	<ul style="list-style-type: none">- Hay conciencia de la importancia del procesamiento de datos en una ambiente SIC.- Se tienen políticas y procedimientos definidos para el área de informática.- Sobre todo se capacita constantemente al personal encargado del procesamiento de datos.	<ul style="list-style-type: none">- Se monitorea constantemente el cumplimiento de los procedimientos definidos en el SIC.- Hay evaluación de personal.- Se verifica la asignación de funciones y responsabilidad.	La actitud de la organización y dirección de la empresa respecto al área de informática es satisfactoria, ya que se tienen las normas, procedimientos y políticas para el cumplimiento de los estándares previamente definidos.

ÁREA AUDITADA	AMBIENTE DE CONTROL.	PROCEDIMIENTOS DE CONTROL.	COMENTARIO.
SOFTWARE. (Seguridad Lógica).	<ul style="list-style-type: none"> - Hay políticas propias para el establecimiento de medidas mínimas de control interno. - Se tiene una norma específica para la confidencialidad de la información. - Se ha diseñado un plan de contingencias de seguridad adicional (Bases de datos, bitácoras, etc.) 	<ul style="list-style-type: none"> - Se tiene una evaluación y supervisión constante del procesamiento de datos. - Se tienen los servicios de un especialista para el monitoreo y mantenimiento de los controles propios del software. Y se considera la modificación y cambio de controles existentes. 	<p>Los controles implementados en los programas son buenos ya que están diseñados para detectar y prevenir errores e irregularidades en el procesamiento de datos. Así como la flexibilidad que tiene el programa de hacerle cambios y mejoras en los diversos controles existentes. Y sobre todo hay conciencia administrativa de la importancia de estos para mejorar la calidad y oportunidad de la información.</p>

ÁREA AUDITADA	AMBIENTE DE CONTROL.	PROCEDIMIENTOS DE CONTROL.	COMENTARIO.
<p>HARDWARE. (Seguridad física).</p>	<p>- La dirección del área de informática no ha intervenido en las desviaciones de las políticas establecidas para la salvaguarda del equipo de cómputo y de los programas.</p>	<p>- Los controles descritos del manual de procedimientos no son aplicados por los usuarios.</p>	<p>Debido a la falta de interés en la seguridad física, no se han considerado las amenazas de no aplicar las políticas de seguridad en el procesamiento de datos.</p>

ANEXO 11

PROGRAMA DE AUDITORÍA DE FACTURACIÓN E INVENTARIO

NOMBRE DE LA FIRMA

NOMBRE DEL CLIENTE

PROGRAMA DE AUDITORÍA EN INFORMÁTICA

ÁREA FACTURACIÓN E INVENTARIO

PERIODO _____

OBJETIVO: Conocer y evaluar la existencia y aplicación de políticas de control, medidas de seguridad en los módulos de inventario y facturación en el ambiente de información por computadora.

No	ACTIVIDAD
1	<p>Evaluar el riesgo de control interno y diseñar pruebas de controles adicionales para el área de facturación e inventario, como:</p> <ul style="list-style-type: none">- comparar una muestra de documentos de despacho de facturas de venta con el registro en el sistema.- Conciliar las cintas de las cajas registradoras y los tiquetes de ventas seleccionados.- Inspeccionar documentos disponibles y confirmar aquellos no disponibles.- Seleccionar una muestra de las facturas de ventas y comparar detalles con lo documentos de despacho, pedidos u ordenes de compra y pedidos de venta.- Obtener listados de inventario y conciliar con registros del sistema.

<p>2</p> <p>3</p>	<ul style="list-style-type: none"> - Conciliar el inventario físico con inventario registrado en sistema y modulo de compras. - Indagar quien es el encargado de bodega y de el modulo de compras. - Obtener un flujo grama de la interrelación de los módulos facturación, inventario y compras. - Evaluar el formulario de inventario que lleva el sistema - Determinar el modo de integración de los módulos de inventario, facturación si es en lote o en línea. - Comparar los resultados de los conteos de prueba de inventario con el archivo de inventario permanente o pormenorizado <p>Determinar los resultados sobre cada uno de los elementos contenidos en el cuestionario. (Narrativa y cedula de hallazgo.)</p> <p>Considerar el uso de la matriz de control interno para evaluar el riesgo de control de esta área.</p>
-------------------	--

Elaborado por: _____

Revisado por: _____

GLOSARIO.

ADMINISTRADOS DE LA BASE DE DATOS.

Es el responsable de la gestión de la base de datos del sistema, encargándose de facilitar su uso al personal informático y del asesoramiento sobre la misma a los jefes de proyectos y analistas.

ANTIVIRUS.

Programas especializados en la detección y si es posible, en la destrucción de virus informáticos.

ARCHIVO.

Sinónimo de fichero y esencia de almacenamiento informático. Delimitado por una cabecera y una marca, lugar donde puede estar ubicado cualquier tipo de información ya sea texto, programas, imágenes, sonidos, etc.

AUDITORÍA EN INFORMÁTICA.

Es una función desarrollada para asegurar la salvaguarda de los activos de los sistemas de computadoras, mantener la integridad de los datos y lograr los objetivos de la organización en forma eficaz y eficiente.

BACKUP.

Copias de seguridad. Proceso para salvaguardar los datos en un medio distinto al disco que normalmente se esta utilizando.

BASE DE DATOS.

Es una colección de datos integrados, con redundancia controlada, y con una estructura que refleja las interrelaciones y restricciones semánticas existentes en el mundo real. Los datos que han de ser compartidos por diferentes usuarios y aplicaciones, su definición y descripción, y almacenamiento de los mismos. Los procesos de actualización y recuperación, comunes y bien determinados, habrán de ser capaces de conservar la integridad, seguridad y confidencialidad del conjunto de datos.

EDI. (Electronic Data Interchange)

Es el intercambio de datos en un formato normalizado entre los sistemas informáticos de quienes participan en transacciones comerciales con reducción al mínimo de la intervención manual.

ENCRIPTACIÓN.

Encriptar es hacer ilegible un escrito por medio de aplicar al texto un algoritmo.

HARDWARE.

Se denomina así al conjunto de componentes físicos dentro de la informática. (Teclado, cpu's, mouse, etc.).

INFORMÁTICA.

Ciencia del tratamiento sistemático y eficaz, realizado especialmente mediante maquinas automáticas, de la información contemplada como vehículo del saber humano y de la comunicación de los ámbitos técnicos, económicos y sociales.

OPERADOR.

Se encarga del funcionamiento del sistema, lanzamiento de procesos, preparación de soporte, periféricas y material necesario.

PASSWORD.

Es un identificador y depende del contexto, puede ser la identificación o confirmación de la palabra de pase.

PROGRAMACIÓN.

Son secuencias de instrucciones, más o menos parecidas al lenguaje humano, que permiten, una vez traducidas o compiladas ejecutar las órdenes incluidas en el programa.

PROGRAMADOR.

Recibe el análisis de la aplicación, y a partir de él diseña los códigos y la codificación del lenguaje de programación elegido.

RESTRICCIÓN.

Es una regla que limita los valores de los datos contenidos en la base de datos.

SERVIDOR.

Se denomina así al ordenador que se encarga de suministrar lo necesario a una red, dependiendo de cual sea la finalidad de esta.

SISTEMAS DE INFORMACIÓN.

Es el sistema encargado de coordinar los flujos de información necesarios para llevar a cabo las funciones de la organización y procesar esta, de acuerdo con su planteamiento y estrategia de negocio.

SOFTWARE.

Todos los componentes informáticos de carácter no físico si no lógico (se denomina también logical), como pueden ser sistemas operativos, programas dedicados a la gestión, de diseño, etc.

SQL.

Es un lenguaje de cuarta generación. Es un lenguaje muy potente y a la vez muy sencillo de utilizar.

TERMINAL.

Punto de introducción y salida de datos de un ordenador central.