UNIVERSIDAD DE EL SALVADOR
Facultad de Ciencias Económicas
Escuela de Contaduría Pública

"Guía de Control Interno Informático para el Área de Activos Corrientes de las Industrias Farmacéuticas"

Trabajo de Graduación Presentado Por:

Clara Patricia Nolasco González
Lorena Patricia Ramirez Flores
Salvador Alfredo Villafuerte Quintanilla

Para Optar al Grado de:

LICENCIADO EN CONTADURIA PUBLICA

Febrero, 2007.

San Salvador El Salvador Centroamérica

AGRADECIMIENTOS

A mi padre Dios, por permitirme culminar esta etapa profesional en mi vida, a mis padres María Nolasco y Napoleón González, por su apoyo y dedicación, a mis hijos Kenneth y Julito, por ser mi inspiración para continuar, a mi esposo, por brindarme siempre su apoyo y comprensión, a mis hermanos, por impulsarme a seguir, a mis amigos en especial a Salvador y Lorena por toda la colaboración y ayuda incondicional que siempre me brindaron, y agradezco de manera muy especial a todos mis maestros que en el transcurso de mi carrera contribuyeron en mi formación académica.

Clara Patricia Nolasco González.

A las tres divinas personas Padre, Hijo y Espíritu Santo junto con la Virgen Maria por permitirme concluir una de mis metas, a mis padres Otilia Flores de Ramírez y Francisco Ramírez Méndez por todo el esfuerzo y apoyo que me brindaron en el transcurso de mi carrera, a mi esposo William Humberto Lima por su comprensión y por darme siempre las fuerzas para seguir adelante, a mis hermanos y amigos que han estado conmigo dándome toda su ayuda incondicionalmente y de manera especial a todos los docentes que formaron parte de mi formación académica y que han contribuido para la culminación de mi carrera.

Lorena Patricia Ramírez Flores

A Dios todo poderoso por permitirme llegar a esta meta, a mis padres Marta Cristina Quintanilla Mejia y José Raúl Villafuerte por toda su comprensión y apoyo que me brindaron durante la carrera, a mis hermanos Raúl y Jacqueline, en especial a mis amigas y compañeras de tesis Clara y Lorena por su apoyo incondicional y su amistad, a mis asesores de tesis y a todos mis amigos que de una u otra forma son parte de la culminación de mi carrera.

Salvador Alfredo Villafuerte Quintanilla

AUTORIDADES UNIVERSITARIAS

Rectora:	**Dra. María Isabel Rodríguez**
Secretaria:	**Licda. Alicia Margarita Rivas**
Decano de la Facultad de Ciencias Económicas:	**Lic. Emilio Recinos Fuentes**
Secretario de la Facultad de Ciencias Económicas:	**Lic. Vilma Yolanda Vásquez de Del Cid**
Jefe de Administración Académica de la Facultad de Ciencias Económicas:	**Lic. José Lauro Vásquez Benítez**
Director de Escuela de Contaduría Pública:	**Lic. Juan Vicente Alvarado**
Docente Director:	**Lic. Juan Vicente Alvarado**
Docente Metodológica:	**Lic. María Margarita de Jesús Martínez de Hernández**

Febrero 2007

San Salvador, El Salvador, Centroamérica

INDICE

RESUMEN EJECUTIVO

“Guía de Control Interno Informático para el Área de Activos Corrientes de las Industrias Farmacéuticas”

Las industrias farmacéuticas son compañías muy complejas por lo que requieren de sistemas de información que generen, procesen y almacenen toda la información originada de cada una de sus áreas o departamentos que la conforman.

A medida que la información es procesada de forma electrónica surge la necesidad de crear controles internos informáticos encaminados asegurar la integridad y veracidad de la misma, así como también utilizar mecanismos de supervisión para verificar su adecuada aplicación sobre todo en aquellas áreas criticas como son los activos corrientes.

Por lo tanto el control interno informático es una herramienta para disminuir los errores, irregularidades o malas aplicaciones, así como operaciones no autorizadas o realizadas por personal ajeno originadas en los sistemas informáticos. Dichos controles sirven para detectar, prevenir y corregir cualquier operación ingresada de manera inadecuada al sistema.

A medida que estos controles sean aplicados y supervisados oportunamente, disminuyen el riesgo que la información presentada en los estados financieros no sea confiable para la toma de decisiones de la compañía.

La investigación de campo se dividió en tres áreas tales como: el conocimiento que tienen los usuarios que utilizan los sistemas, la capacitación que se proporciona al personal involucrado en la generación, procesamiento y almacenamiento de la información y la necesidad de conocer si las industrias farmacéuticas poseen controles internos informáticos en los activos corrientes, considerados como áreas vulnerables y críticas, con el fin de que la información presentada en los estados financieros sea razonable y confiable.

El uso de un sistema computarizado en el procesamiento de datos es vital para la gerencia, la cual se compromete a establecer políticas y procedimientos que les permitan garantizar la toma de decisiones, por lo tanto se vuelve necesario la utilización de una guía de control interno informático para el área de activos corrientes, encaminados a garantizar la confiabilidad y veracidad de la información procesada en los sistemas computarizados.

Esta guía presenta políticas y procedimientos de control interno informático sobre aspectos generales y específicos; como la seguridad física y lógica, planes de contingencia, controles de acceso, cambios y modificaciones en el sistema, creación de respaldos de información, manejo de efectivo, conciliación de saldos bancarios y de cuentas por cobrar, limites de crédito, antigüedad de saldos, requisiciones de inventarios, entradas y salidas, muestras médicas, etc.

Los profesionales de la contaduría pública consideran la importancia del control interno informático en los activos de la empresa, para lo cual, reconocen que es necesario contar con un documento que les ayude a formular medidas de control adecuadas para la administración confiable de la información presentada en los estados financieros de la empresa.

INTRODUCCION

Con la introducción de la informática, en las diversas áreas de las empresas, nace la necesidad de controlar de una manera más eficaz y eficiente la información procesada a través de los sistemas, los medios mecanizados representa un desafío para las compañías, ya que representa una fuerte inversión en bienes tangibles e intangibles, a demás de tener altos costos de desarrollo y mantenimiento de los sistemas.

En una industria farmacéutica es primordial que se utilicen controles internos informáticos, pues los niveles de información son elevados, y sus procesos son muchos, por lo que se vuelve necesario implementar un sistema informático contable, que garantice el adecuado procesamiento electrónico de datos, con el propósito que la información sea eficaz, oportuna y confiable.

El establecer controles garantiza la razonabilidad y confiabilidad de los resultados obtenidos en el procesamiento de la información. Un buen sistema de control es importante, desde el punto de vista de la integridad física y numérica de los bienes, valores y activos de la empresa, tales como el efectivo en caja y bancos, inventarios, cuentas y documentos por cobrar, etc.; es decir, que en la medida que se tenga un sistema eficiente y práctico de control interno se disminuirá la posibilidad de transacciones fraudulentas que conlleven a errores e irregularidades.

CAPITULO I

1. MARCO TEÓRICO

1.1. ANTECEDENTES

1.1.1 ACTIVOS CORRIENTES

En toda empresa es necesario que se informe sobre las operaciones que conforman la gestión empresarial, a fin de coordinar y dirigir en forma eficiente; la información precisa para ser utilizada en el proceso de toma de decisiones; cuyo objetivo es informar sobre la situación económico-financiera, la cual es denominada contabilidad, por lo que su función es registrar y procesar los hechos que componen la actividad económica en que se involucre tal entidad.

Su presentación se debe realizar con una normativa estandarizada, y la mayoría es mediante las Normas Internacionales de Contabilidad (NIC), las cuales contienen los procedimientos básicos para la presentación de los Estados Financieros, para tal efecto una de las clasificaciones importantes son los activos corrientes, los cuales tienen la capacidad de ser convertibles en efectivo dentro de un ciclo de operaciones normales del negocio, es decir en un período de un año o menos, por ejemplo:

a) **Efectivo y equivalentes:** es el dinero que se tiene disponible para ser frente a las necesidades inmediatas de la empresa, así como fondos fijos para realizar gastos menores y

todos aquellos efectivos propios procedentes de las cuentas bancarias.

b) **Cuentas por Cobrar:** son aquellos saldos pendientes de cobro provenientes de las ventas al crédito y todos aquellos montos morosos que no fueron cancelados en los plazos acordados.

c) **Inventario:** Es el detalle completo de las cantidades y valores correspondientes de materias primas, productos en proceso y productos terminados de una empresa.

Para efecto de este estudio se profundizará en estos tres rubros debido a que en las industrias farmacéuticas son de vital importancia para el desarrollo de la actividad económica y requieren una cuidadosa contabilización pues son vulnerables a los fraudes y robos.

Asimismo es necesario el desarrollo de un eficiente control interno que garantice la protección de los bienes más susceptibles; asegurando un buen manejo de efectivo, cuentas por cobrar e inventarios. Por otra parte la creación de un control interno informático para el área de activos corrientes garantiza a la empresa la protección de sus bienes a través de la creación de políticas y procedimientos de planeación, control y contabilización.

En las industrias farmacéuticas, los activos corrientes principalmente del rubro de inventarios, requiere un control especial, debido a que éstos en ocasiones pueden venderse

rápidamente, y convertirse en efectivo con mayor facilidad que las mismas cuentas por cobrar. Sin embargo, por lo general en esta rama, los inventarios tienen que sufrir una transformación para poder ser vendidos; por lo que, se parte de que la mayoría de las ventas, como es usual en los tiempos modernos, se realiza a crédito y por consiguiente, el producto de una venta de inventarios resulta ser una cuenta por cobrar y no directamente el efectivo.

1.1.2. ANTECEDENTES Y ORIGEN DEL CONTROL INTERNO INFORMÁTICO.

Es en la revolución industrial cuando surge la necesidad de controlar las operaciones que por su magnitud eran realizadas por máquinas manejadas por varias personas. Por lo tanto se piensa que el origen del control interno, surge con la partida doble y que fue una de las medidas de control, pero que fue hasta fines del siglo XIX que los hombres de negocios se preocupan por formar y establecer sistemas adecuados para la protección de sus intereses. Por lo que de manera general, se puede afirmar que la consecuencia del crecimiento económico de los negocios, implicó una mayor complejidad en la organización y por tanto en su administración.

1.2. DEFINICIONES DE CONTROL INTERNO INFORMÁTICO

Partiendo que el control interno es un proceso que lleva a cabo la alta dirección de una organización y que debe estar diseñado para dar una seguridad razonable, en relación con el logro de los objetivos previamente establecidos basados en la efectividad y eficiencia de las operaciones, la confiabilidad

en los reportes financieros y el cumplimiento de leyes, normas y regulaciones, surge un concepto más amplio como es el de control interno informático el cual controla diariamente que todas las actividades de los sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijados por la Dirección de la Organización y\o la Dirección Informática, así como los requerimientos legales[1].

En las empresas dedicadas a la producción y comercialización de medicamentos para uso humano, conocidas como Industrias Farmacéuticas, la utilización de controles internos es fundamental para mejorar el desempeño de sus actividades, y por consiguiente el de sus activos corrientes.

1.3. OBJETIVOS DEL CONTROL INTERNO INFORMÁTICO

El establecer controles internos informáticos va encaminado a garantizar la eficiencia y eficacia en el procesamiento, manejo, almacenamiento de la información y de aquellos recursos que permitan mejorar el funcionamiento de la entidad, para ello es necesario enunciar los principales objetivos[2]:

a) Establecer como prioridad la seguridad y protección de la información.

[1] Sobrinos Sánchez, Roberto, Planificación y Gestión de Sistemas de Información, Escuela Superior de informática de la Universidad de Castilla.
[2] Muñoz, Carlos Auditoria de Sistemas Computacionales, Control Interno Informático, Pág. 134

b) Promover la confiabilidad, oportunidad y veracidad de la captación de datos, su procesamiento en el sistema y la emisión de informes en la empresa.

c) Implementar los métodos, técnicas y procedimientos necesarios para coadyuvar al eficiente desarrollo de las funciones, actividades y tareas de los servicios computacionales, para satisfacer los requerimientos de sistemas en la empresa.

d) Instaurar y hacer cumplir las normas, políticas y procedimientos que regulen las actividades de sistematización de la empresa.

e) Establecer las acciones necesarias para el adecuado diseño e implementación de sistemas computarizados, a fin de que permitan proporcionar eficientemente los servicios de procesamiento de información en la empresa.

1.4. IMPORTANCIA DEL CONTROL INTERNO INFORMÁTICO

En la medida en que las empresas farmacéuticas, buscan la manera de optimizar sus recursos, requieren el uso de la tecnología para la implementación de sistemas informáticos, por lo que se vuelve necesario establecer controles que permitan la veracidad y confiabilidad de la información.

El procesamiento de la información financiera implica el uso de la tecnología de información, tales como datos, sistemas de

aplicación, instalaciones adecuadas y personal idóneo, siendo necesario la elaboración de procedimientos que permitan verificar la integridad de la información generada a través de los sistemas, volviéndose necesario la supervisión periódica de los mismos a fin de lograr una mayor seguridad de la información.

1.5. CARACTERÍSTICAS DEL CONTROL INTERNO INFORMÁTICO

Entre las principales características del Control Interno Informático están[3]:

a) Controlar que todas las actividades se realicen cumpliendo los procedimientos y normas fijados por la Dirección.
b) Evaluar su bondad y asegurarse del cumplimiento de las normas legales.
c) Colaborar y apoyar el trabajo de Auditoria Informática, así como de las auditorias externas al grupo.
d) Definir, implantar y ejecutar mecanismos y controles, lo cual no debe considerarse como que la implantación de los mecanismos de medida y la responsabilidad del logro de esos niveles se ubique exclusivamente en la función de Control Interno, sino que cada responsable de objetivos y recursos es encargado de esos niveles, así como de la creación de los medios de medida adecuados.

[3] Normas de Control Interno Informático (el línea), disponible en <htpp://www.mag.gob.sv/admin./publicaciones.

1.6. CLASIFICACIÓN DE LOS CONTROLES INTERNO INFORMÁTICOS

En el ambiente informático, el control interno se materializa fundamentalmente en dos tipos de controles:

Controles Manuales; aquellos que son ejecutados por el personal del área usuaria o de informática sin la utilización de herramientas computacionales.

Controles Automáticos; son generalmente los incorporados en el software, llámense éstos de operación, de comunicación, de gestión de base de datos, programas de aplicación, etc.

Sin embargo estos de acuerdo a su finalidad se clasifican en:

1.6.1 CONTROLES PREVENTIVOS: establecen las condiciones necesarias para que el error no se produzca. Aseguran que los procedimientos programados dentro de un sistema informático se diseñen, implanten, mantengan y operen de forma adecuada y que solo se introduzcan cambios autorizados en los programas y en los datos. Dentro de los cuales se pueden mencionar:

1.6.1.1 Controles de Mantenimiento: destinados a asegurar que las modificaciones de los procedimientos programados están adecuadamente diseñadas, experimentadas, aprobadas e implantadas.

1.6.1.2 Controles de Seguridad de Programas: destinados a garantizar que no se puedan efectuar cambios no autorizados en los procedimientos programados.

1.6.1.3 Controles de Seguridad de Ficheros de datos: destinados a asegurar que no se puedan efectuar modificaciones no autorizadas en los archivos de datos.

1.6.1.4 Controles de la Operación Informática: destinados a garantizar que los procedimientos programados autorizados se aplican de manera uniforme y se utilizan versiones correctas de los ficheros de datos.

1.6.1.5 Controles de Conversión de ficheros: destinados a garantizar una completa y exacta conversión de los datos de un sistema antiguo a uno nuevo.

1.6.1.6 Controles de Software Sistema: destinados a asegurar que se implante un software de sistema apropiado y que se encuentre protegido contra modificaciones no autorizadas.

1.6.1.7 Controles de implantación: destinados a asegurar que los procedimientos programados para los nuevos sistemas son adecuados y están efectivamente implantados.

1.6.1.8 Controles de usuario: Estos controles constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados. Tales como:

1.6.1.8.1 Palabras Claves (Passwords): Generalmente se utilizan para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones. Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo.

1.6.1.8.2 Sincronización de passwords: Consiste en permitir que un usuario acceda con la misma password a diferentes sistemas interrelacionados y, su actualización automática en todos ellos en caso de ser modificada.

1.6.1.8.3 Encriptación: La información solamente puede ser des-encriptada por quienes posean la clave apropiada. La encriptación puede proveer de una potente medida de control de acceso.

1.6.1.8.4 Listas de Control de Accesos: Se refiere a un registro donde se encuentran los nombres de los usuarios que obtuvieron el permiso de acceso a un determinado recurso del sistema, así como la modalidad de ingreso permitido. Este tipo de listas varían considerablemente en su capacidad y flexibilidad.

1.6.1.8.5 Límites sobre la Interfase de Usuario: Estos límites, generalmente, son utilizados en conjunto con las listas de control de accesos y restringen a los usuarios a funciones específicas

1.6.1.8.6 Etiquetas de Seguridad: Consiste en designaciones otorgadas a los recursos (como por ejemplo un archivo) que

pueden utilizarse para varios propósitos como control de accesos, especificación de medidas de protección, etc. Estas etiquetas no son modificables.

1.6.2 CONTROLES DETECTIVOS: Identifican el error pero no lo evitan, actuando como alarmas que permiten registrar el problema y sus causas. Además sirven como verificación del funcionamiento de los procesos y de sus controles preventivos. Estos a su vez se clasifican en.

1.6.2.1 Controles de aplicaciones: los cuales son un conjunto de procedimientos programados y manuales diseñados especialmente para cada aplicación con el fin de cumplir con objetivos específicos de control utilizando una o más técnicas.

1.6.2.2 Controles sobre captura de datos: sobre altas de movimientos, modificaciones de movimientos, consultas de movimientos, mantenimiento de los ficheros.

1.6.2.3 Controles de proceso de datos: normalmente se incluyen en los programas. Se diseñan para detectar o prevenir los siguientes tipos de errores (entrada de datos repetidos, procesamiento y actualización de ficheros o ficheros equivocados, entrada de datos ilógicos, pérdida o distorsión de datos durante el proceso).

1.6.2.4 Controles de salida y distribución: Los controles de salida se diseñan para asegurarse de que el resultado del

proceso es exacto y que los informes y demás salidas los reciben solo las personas que estén autorizadas.

1.6.3. CONTROLES CORRECTIVOS: Permiten investigar y rectificar los errores y sus causas, están destinados a procurar que existan las acciones necesarias para su solución. Como ejemplos tenemos los listados de errores, las evidencias de auditoria o las estadísticas de causas de errores

1.7 ELEMENTOS DEL CONTROL INTERNO INFORMÁTICO

Entre los elementos de control interno informático[4] para el logro los objetivos de un adecuado sistema en las industrias farmacéuticas se pueden mencionar:

a) Organización del área de informática: Garantiza a la industria tener una estructura organizacional eficaz y eficiente, tomando en consideración las siguientes áreas: Dirección, División del trabajo, Asignación de responsabilidades y autoridad, Establecimiento de estándares y métodos y Perfiles de puestos.

b) Análisis, desarrollo e implementación de sistemas: con este elemento se asegura la implantación útil y oportuna de un sistema de información a través del análisis de la factibilidad, costo/beneficio, diseño y medidas de seguridad.

[4] Muñoz, Carlos, Auditoria en Sistemas Computacionales, Control Interno Informático, Pág. 135

c) Operación de los sistemas: al hacer uso de este elemento se estará previniendo posibles errores y deficiencias de operación, así como fraudes, robos, piraterías, alteraciones y modificaciones de la información y de los sistemas, lenguajes y programas.

d) Procesamiento de entrada de datos, de información y emisión de resultados: el establecimiento de controles internos informáticos dentro del área de procesamiento de datos, radica en que la entrada de un dato da origen a una información que puede ser útil a su salida, mediante algún procesamiento interior del sistema.

e) Seguridad de área de sistemas: incluye la confianza de los recursos informáticos, del personal, de la información, de sus programas, etc.

1.8 RELACIÓN DE LOS ELEMENTOS DE CONTROL COSO CON EL CONTROL INTERNO INFORMÁTICO

El control interno según enfoque del Comité of Sponsoring Organization of Treaday Comisión (COSO) fue originalmente instaurado en el año de 1985 con la finalidad de estudiar los factores que permitían la emisión fraudulenta de reportes financieros, a comienzos de los años 90, el comité junto con la asesoría de Price Waterhouse Coopers, realizó un estudio extensivo sobre que controles internos, cuyo resultado fue el marco de control interno COSO. El cual, brinda recomendaciones sobre evaluar, reportar y mejorar los sistemas de control.

En vista de las limitaciones de un sistemas de control interno y los roles y responsabilidades de las partes que afectan a un sistema. Dentro de las cuales se incluyen el juicio humano defectuoso, falta de comprensión de las instrucciones, atropellos de la gerencia y consideraciones de costos versus beneficios.

Revisa la necesidad de capturar la información pertinente interna y externa, el potencial de sistemas estratégicos e integrados y la necesidad de calidad en los datos.

El control interno COSO posee ocho componentes los cuales ayudan a identificar los riesgos y debilidades en los sistemas, encaminados a lograr los objetivos de control de las siguientes áreas: eficiencia y efectividad de las operaciones, preparación de cuentas financieras confiables y el cumplimiento de leyes y regulaciones, los cuales son:

a) Ambiente de control
b) Establecimientos de objetivos
c) Identificación de eventos
d) Evaluación del riesgo
e) Respuesta al riesgo
f) Actividades de control
g) Información y comunicación
h) Supervisión

a) Ambiente de control: Aquí entran los controles influenciados en la organización de la industria farmacéutica,

éstos incluyen los factores, internos o externos, que pudiesen incidir en el ambiente de control tales como: integridad y valores morales del personal, compromiso para contratar y mantener personal de calidad, estructura de la organización y asignación de responsabilidades, conflicto de intereses, transparencia y responsabilidad social.

b) Establecimientos de objetivos: Buscan asegurar que la industria farmacéutica ha establecido un proceso para fijar los objetivos encaminados a promover la confiabilidad y veracidad de las operaciones.

c) Identificación de Riesgos: Acontecimientos internos y externos que pueden afectar los objetivos de la entidad en el área de activos corrientes, a través de la identificación de riesgos relevantes que afecten en el logro de objetivos utilizados para determinar las actividades de control, su impacto negativo y positivo, análisis de los flujos de procesos, entre otros.

d) Evaluación de Riesgos: Consiste en analizar los riesgos detectados así como su impacto e incidencia en los activos corrientes, dentro de estos riesgos están, el riesgo inherente, residual.

e) Respuesta a los Riesgos: En este componente se hace la selección de respuestas posibles, tolerancia al riesgo, aceptación, reducir y evitar que este ocurra.

f) Actividades de Control: Políticas y procedimientos establecidos para asegurar que las respuestas a los riesgos identificados en los activos corrientes se llevan eficazmente, éstas pueden ser: preventivas, detectivas, manuales, computacionales, controles gerenciales, entre otros, y se hacen a lo largo de toda la organización.

Las actividades de control incluyen la administración de los riesgos operacionales en los procesos de negocio, el acceso a los sistemas de información y recursos informáticos, así como la mitigación errores.

g) Información y Comunicación: Identificación, captura y comunicación en forma y plazo adecuado para permitir al personal de la industria farmacéutica a afrontar sus responsabilidades, tanto de las fuentes internas y externas de la organización, asimismo su influencia y su difusión.

h) Monitoreo: Supervisión de la gestión de riesgos en todos los niveles, realizando las modificaciones que se necesiten, mediante el monitoreo continuo desarrollado en el curso normal de las operaciones a través de evaluaciones puntuales por entes internos o externos.

Un sistema de control necesita ser monitoreado para asegurar que el mismo continúa operando efectivamente y el seguimiento incluye el sondeo permanente entre los indicadores de riesgos operacionales y situaciones críticas, así como revisiones periódicas a la efectividad de los controles implantados, la disponibilidad de herramientas para el monitoreo de los

riesgos operacionales y su impacto. Por lo que la industria farmacéutica tiene establecido controles internos relacionados a las diferentes áreas, tales como:

a) Controles en niveles de la compañía: corresponden a los sistemas de planificación, estilo de operación, políticas de las compañías, códigos de conducta y prevención de fraudes.

b) Controles de aplicación: son aquellos relacionados a los controles de procesos de negocio y diseñados para lograr la totalidad, exactitud, validez y segregación de funciones.

c) Controles generales de cómputo: Se refieren a los controles compartidos en los servicios de la organización, como mantenimiento de sistemas, recuperación de desastres, seguridad física y lógica, respuesta a accidentes.

1.9 DIFERENCIAS DE CONTROL INTERNO INFORMÁTICO Y CONTROL INTERNO

El Control Interno es cualquier acción tomada por la Gerencia para aumentar la probabilidad de que los objetivos establecidos y las metas se han cumplido, con el fin de proporcionar un grado razonable de confianza en la consecución de objetivos en los siguientes ámbitos:

a) Eficacia y eficiencia de las operaciones
b) Fiabilidad de la información financiera
c) Cumplimiento de las leyes y normas aplicables

A diferencia del control interno administrativo o contable. El Control Interno Informático puede definirse como el sistema integrado al proceso administrativo, en la planeación, organización, dirección y control de las operaciones con el objeto de asegurar la protección de todos los recursos informáticos y mejorar los índices de economía, eficiencia y efectividad de los procesos operativos automatizados.[5]

En conclusión la diferencia principal es la función que tienen los tipos de controles internos pues uno va encaminado principalmente a la salvaguarda de activos y el control interno informático al aseguramiento de todos los recursos informáticos.

Lo cual se muestra más en detalle en la Tabla No.1:

[5] Pinilla, José Dagoberto, Auditoria Informática, Aplicaciones en producción <en línea> Disponible <http://www.auditi.com// (Consulta 18 de julio 2006)

TABLA:1 Diferencia entre control interno informático y control interno	
CONTROL INTERNO INFORMÁTICO	**CONTROL INTERNO**
Asegurar la protección de todos los recursos informáticos y mejorar los índices de economía, eficiencia y efectividad de los procesos operativos automatizados.	Verificación del cumplimiento de normativa y procedimientos establecidos por la Dirección y la Dirección General
Análisis de los controles: a. Controles detectivos b. Controles correctivos c. Controles preventivos	a) Salvaguarda de activos b) Confiabilidad e integridad de la información. c) Cumplimiento de políticas, planes, procedimientos, leyes y regulaciones. d) Uso eficiente y económico de los recursos. e) Cumplimiento de objetivos establecidos, metas de operaciones y programas

1.10 RELACIÓN DEL CONTROL INTERNO INFORMÁTICO CON LA NORMATIVA REFERENTE A LA INFORMACIÓN Y LA CALIDAD.

1.10.1 COBIT (Objetivos de Control Relativos a la Tecnología de la Información)

La misión del COBIT es buscar, desarrollar, publicar y promover un autoritario y actualizado conjunto internacional de objetivos de control de tecnologías de la información, generalmente aceptadas, para el uso diario por parte de gestores de negocio y auditores.

El COBIT es la orientación a negocios y esta diseñado no solo para ser usado por usuarios y auditores, sino que en forma más importante, para ser utilizado como una lista de verificación detallada para los propietarios de los procesos de negocio. De forma creciente, las prácticas de negocio comprenden la completa autorización de los procesos propios de negocio, con lo que poseen una total responsabilidad para todos los aspectos de dichos procesos.

La norma COBIT, proporciona una herramienta para estos procesos que facilitan la descarga de esta responsabilidad, a través de una simple y pragmática premisa; en orden de proporcionar la información que la organización necesita para llevar a cabo sus objetivos, los requisitos de las tecnologías de la información necesitan ser gestionados por un conjunto de procesos agrupados de forma natural.

La norma esta formada por un conjunto de 34 objetivos de control de alto nivel para cada uno de los procesos de las

tecnologías de la información, agrupados en cuatro dominios que son:

a) Planificación y organización,
b) Adquisición e implementación,
c) Soporte de entrega y,
d) Monitorización.

Esta estructura, abarca todos los aspectos de la información y de la tecnología que la mantiene, y es mediante la dirección de los objetivos de control de alto nivel que los procesos propios del negocio pueden garantizar la existencia de un sistema de control adecuado para los entornos de las tecnologías de la información. En suma, cada uno de estos objetivos, es una directiva de revisión y seguridad para permitir la inspección de los procesos de las tecnologías de la información en contraste con los 302 objetivos de control detallados en el COBIT para el suministro de una gestión de seguridad, así como de un aviso para la mejora (Ver Anexo1).

Esta estructura COBIT le permite a la gerencia comparar la seguridad y prácticas de control de los ambientes de Tecnología de Información (TI), permite a los usuarios de los servicios asegurarse que existe una adecuada seguridad y control por ende permite a los auditores sustentar su opinión sobre el control interno.

La fase ya completada del proyecto COBIT provee un Resumen Ejecutivo, un Marco para el control de Tecnología de Información, una lista de Objetivos de Control, y un conjunto

de Guías de Auditoria. Se considero según Sobrinos Sánchez, en su libro Planificación y Gestión de Sistemas de Información que las fases futuras del proyecto proveerán guías de auto-evaluación para la dirección e identificarán objetivos nuevos o actualizados mediante incorporación de otros estándares globales de control que se identifiquen.

Además, agregar guías de control e identificar indicadores claves de desempeño; no obstante COBIT adaptó su definición de control a partir de Objetivos de Control, ya que las políticas, procedimientos, prácticas y estructuras organizacionales están diseñadas para proveer aseguramiento razonable de que se lograrán los objetivos del negocio y que se prevendrán, detectarán y corregirán los eventos no deseables.

Cabe mencionar que COBIT busca evaluar mediante los siete criterios si se están satisfaciendo los recursos de Tecnología de Información y los requerimientos de información del negocio, que son: efectividad, eficacia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información.

Los controles internos se utilizan en el entorno informático y continúan evolucionando a medida que los sistemas informáticos se vuelven más complejos. Los progresos que se producen en la tecnología de soportes físicos y de software han modificado de manera significativa los procedimientos que se emplean tradicionalmente para controlar los procesos de aplicaciones.

La evaluación de la Tecnología de la Información exige analizar diversos elementos independientes, por ello es importante llegar a conocer bien la configuración del sistema, con el objeto de identificar los elementos, productos y herramientas que existen para saber donde pueden implementarse los controles, así como identificar posibles riesgos.

1.10.2 LEY SARBANES-OXLEY (LEY SOA)

La Ley Sarbanes-Oxley, conocida también como SOX ó SOA (por sus siglas en inglés Sarbanes Oxley Act), es la ley que regula las funciones financieras contables y de auditoria, penalizando en una forma severa, el crimen corporativo y de cuello blanco. Debido a los múltiples fraudes, la corrupción administrativa, los conflictos de interés, la negligencia y la mala práctica de algunos profesionales y ejecutivos que conociendo los códigos de ética, sucumbieron ante el atractivo de ganar dinero fácil y a través de empresas y corporaciones engañando a socios, empleados y grupos de interés, entre ellos sus clientes y proveedores.[6]

Por lo tanto esta Ley busca prevenirlos a través de los diferentes requerimientos con el fin de proteger a los inversores, por lo que las medidas van encaminadas a la seguridad de la fiabilidad de la información revelada por las compañías. En relación a la industria farmacéutica en el país la aplicación de esta normativa es trascendental, en alusión a los activos corrientes que tienen un gran riesgo, ya

[6] Cano C., Miguel Antonio, Auditoria Forense en la investigación criminal del lavado de dinero y activos.

sea a fraudes, robos o mala práctica del personal encargado de ellos.

La sección 404 exige a las compañías sujetas a los requerimientos la inclusión en sus reportes anuales, un informe de la dirección anual evaluando el control interno sobre el reporte financiero en el cual la dirección:

a. Declare su responsabilidad sobre el establecimiento, mantenimiento y operatividad de una estructura, unos procedimientos de control interno adecuados y el establecimiento de controles internos informáticos.
b. Identifique el marco sobre el cual opera la dirección para determinar la evaluación de la efectividad de los controles de la compañía sobre los reportes financieros.
c. Realice y documente una evaluación de la efectividad de los procedimientos y controles internos de la compañía.

Una de las principales aplicaciones de la ley es a la Tecnología de Información para mantener, de manera adecuada y en el tiempo, un esquema de control interno estable y preventivo, basado en los lineamientos de COSO, los que requieren llevar a cabo procesos para la evaluación y mejora del control interno en momentos específicos, la Ley SOX establece que el diseño, evaluación y mejoramiento del control interno será un proceso rutinario y parte importante en el logro de nuevos negocios para las compañías. En este sentido, se juega un papel imprescindible en mantener, de forma

adecuada y en el tiempo, un esquema de control interno estable y preventivo, más que detectivo y correctivo.[7]

Cabe mencionar que en El Salvador la Ley Sarbanees- Oxley (Ley SOA), solo es aplicable para aquellas compañías inversionistas en la Bolsa de Valores.

1.10.3 ISO 9001-2000 (NORMAS DE CALIDAD)

Con el acuerdo del Tratado de Libre Comercio, se exige a la industria farmacéutica mejores estándares de calidad, lo cual es beneficioso para lograr ser más competitivos en el mercado nacional e internacional.

Esto se puede lograr con la aplicación de las Normas de Calidad ISO 9001-2000, lo cual requiere mejorar tanto sus recursos y herramientas de control para lograr un sistema de gestión de calidad eficaz. Lo que garantiza que la empresa planifica, diseña, desarrolla, elabora y suministra productos y/o servicios dentro de un marco de trabajo acorde a estándares internacionales.

La aplicación de las Normas de Calidad ISO 9000 constituye para la industria, una vía de reducir costos y mejorar sus procesos de producción tomando en cuenta que la calidad es un factor clave para la competitividad en cualquier mercado.

[7] Cano C. Miguel Antonio, Auditoria Forense en la investigación criminal del lavado de dinero y activos.

Esta Norma Internacional especifica los requisitos para un sistema de gestión de la calidad, cuando una organización aspira a aumentar la satisfacción del cliente a través de la aplicación eficaz del sistema, incluidos los procesos para la mejora continúa del sistema y el aseguramiento de la conformidad con los requisitos del cliente y los reglamentarios aplicables, como herramienta para el logro de estos objetivos se realiza mediante controles internos informáticos, con el propósito de mejorar los estándares de calidad en la información procesada.

Las empresas farmacéuticas deben establecer, documentar, implementar y mantener un sistema de gestión de la calidad y mejorar continuamente su eficacia de acuerdo con los requisitos que esta norma establece, todo esto encaminado a lograr un buen control interno informático de sus sistemas, en tanto la organización debe: identificar los procesos necesarios para el sistema de gestión de la calidad y su aplicación a través de la organización, determinar la secuencia e interacción de estos procesos, determinar los criterios y métodos necesarios para asegurarse de que tanto la operación como el control de estos procesos sean eficaces, asegurarse de la disponibilidad de los recursos e información necesarios para apoyar la operación y el seguimiento de estos procesos, realizar el seguimiento, la medición y el análisis de estos procesos.

Entre los procedimientos para lograr una gestión de calidad tenemos:

a) **Comunicación Interna**: Se deben de establecer procesos de comunicación apropiados dentro de las compañías para verificar la eficacia de la información procesada; esto no se limita al procesamiento electrónico de datos sino también al personal y las herramientas de control que se han adoptado.

b) **Revisión**: La información procesada en los sistemas de información deben ser supervisada periódicamente para lo cual se asegura la fiabilidad de esta, incluyendo los siguientes aspectos: desempeño de los procesos y conformidad de la información generada, las medidas correctivas y preventivas utilizadas y su aplicación de manera oportuna, acciones tomadas y seguimiento de las revisiones realizadas, recomendaciones para mejorar los procesos de los sistemas de información.

c) **Análisis de los Datos:** La información procesada de los activos corrientes debe de ser analizada periódicamente para demostrar su idoneidad y su eficacia.

d) **Mejora:** Los sistemas de información deben de ser mejorados continuamente con el propósito de alcanzar la eficacia, todo esto se logra a través del análisis de los datos, de las acciones correctivas y preventivas y de la revisión periódica de los procesos.

e) **Acción Correctiva:** Las acciones que tome las compañías farmacéuticas deben de ser aplicadas de manera oportuna con el fin de eliminar la causa de las no conformidades

encontradas en los sistemas de información, y evitar de esta manera que vuelvan a ocurrir.

f) **Acción Preventiva:** Las compañías farmacéuticas deben de determinar acciones para prevenir la ocurrencia de posibles problemas que pudieran surgir en el futuro.

En la medida que las empresas farmacéuticas mejoren sus controles internos informáticos pueden encaminarse a una implementación de ISO 9001, tanto para la gestión de calidad como para la seguridad de la información.

1.10.4 ISO 17799: LA NUEVA NORMATIVA TÉCNICA GLOBAL DE SEGURIDAD

Desde su publicación en diciembre de 2000, por parte de la Organización Internacional de Normas, la ISO 17799 se define como "un completo conjunto de controles que incluye las prácticas exitosas de seguridad de la información"[8]

ISO 17799 ofrece un conjunto de reglas a un sector donde no existen, por lo que enmarca diez áreas de control, que son:

a) Política de Seguridad: dentro de las empresas es necesario que existan políticas que reflejen las expectativas de la organización en materia de seguridad

b) Organización de la Seguridad: la norma establece que se debe diseñar una estructura administrativa dentro de la

[8] Control Interno, Seguridad y Auditoria Informática, ISO, disponible en línea: http://auditi.com/index.htm, (Consulta 22 de julio 2006)

organización que establezca la responsabilidad de los grupos involucrados en el plan de seguridad.

c) Control y clasificación de los recursos de la información: se deberá levantar un inventario de los recursos de información de la organización para asegurar que se brinde un nivel adecuado de protección.

d) Seguridad del personal: establece la necesidad de educar e informar a los empleados sobre lo que se espera de ellos en materia de seguridad y confidencialidad. Además se debe implementar un plan para reportar accidentes.

e) Seguridad Física y Ambiental: responde a la necesidad de proteger las áreas, el equipo y los controles generados.

f) Manejo de las comunicaciones y las operaciones: esta área se enfoca en asegurar el funcionamiento correcto y seguro de las instalaciones, del procesamiento de la información, minimizar el riesgo de fallas de los sistemas, proteger la integridad y la disponibilidad de la información, garantizar la protección de los datos en las redes y la infraestructura de soporte.

g) Control de Acceso: establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para proteger contra abusos internos y externos.[9]

[9] Control Interno, Seguridad y Auditoria Informática, ISO, disponible en línea: http:// auditi.com/index.htm. (Consulta 18 de Julio 2006)

1.11 NORMATIVA TÉCNICA APLICABLE AL CONTROL INTERNO INFORMÁTICO

1.11.1 Normas Internacionales de Auditoria (NIAS)

NIAS (Normas Internacionales de Auditoria), NIA 400, “Auditoria en un Ambiente de Sistemas de Información por Computadora” trata del nivel de habilidades y competencia que necesita el equipo de auditoria para conducir una auditoria en un ambiente de CIS.

Por lo que dentro de las medidas de control interno recomendadas por la NIA 400

a) Autorización de la administración para operación de microcomputadora: La administración puede contribuir a la operación efectiva de microcomputadoras independientes fijando y ejecutando políticas para su control y uso, estos pueden incluir:

1. Responsabilidades de la administración;
2. Instrucciones sobre el uso de las microcomputadoras;
3. Requisitos de entrenamiento;
4. Autorización para el acceso a programas y datos;
5. Políticas para prevenir el copiado no autorizado de programas y datos;
6. Requisitos de seguridad, respaldo y almacenamiento;
7. Desarrollo de aplicaciones y normas de documentación;

8. Normas para formato de informes y controles para distribución de informes;
9. Políticas sobre uso de personal;
10. Normas de integridad de datos;
11. Responsabilidad por los programas, datos y corrección de errores y
12. Segregación apropiada de funciones.

b) Seguridad física relativos a los equipos: A causa de sus características físicas, las microcomputadoras son susceptibles de robo, daño físico, acceso no autorizado, o mal uso; esto puede resultar en la pérdida de información almacenada en la microcomputadora, tales como, datos financieros importantes para el sistema de contabilidad.

Un método de seguridad física es restringir el acceso a las microcomputadoras cuando no están en uso, por medio de cerraduras en las puertas u otra protección de seguridad durante las horas no hábiles.

c) Seguridad física relativa a los medios removibles y no removibles

El control sobre los medios removibles puede establecerse poniendo la responsabilidad por dichos medios, cuyo compromiso incluyen funciones de custodios de software o de bibliotecarios. Se debe reforzar más cuando se usa sistema de verificación de entradas y salidas de archivos de programas y datos y se cierran con llave los lugares de almacenamiento; estos ayudan a asegurar que los medios de almacenamiento removibles no se pierdan, se desubiquen o se den a personal no autorizado. El control físico sobre medios de almacenamiento

no removibles probablemente se establezca mejor mediante aditamentos de cerraduras de seguridad.

d) **Seguridad de programas y datos***:* Cuando las microcomputadoras están accesibles a muchos usuarios, hay un riesgo que los programas y datos pueden ser alterados sin autorización. El software del sistema operativo de la microcomputadora puede no contener muchas características de control y seguridad, por los que existe, control interno que pueden integrarse a los programas de aplicación para ayudar a asegurar que los datos procesados y leídos según se autorice, y que se previene la destrucción accidental de datos. Estas técnicas, que limitan el acceso a programas y datos sólo a personal autorizado, incluyen:

Separar datos en archivos organizados bajo directorios de archivos separados; usar archivos ocultos y nombres secretos de archivos; emplear palabras clave; y usar criptografía.

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

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

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

g) Controles generales de los sistemas de información contable, segregación de funciones: En un ambiente de microcomputadora, es común para los usuarios poder desempeñar dos o más de las siguientes funciones en el sistema de contabilidad, tales como: iniciar y autorizar documentos fuente, alimentar datos del sistema, operar la computadora, cambiar programas y archivos de datos, usar o distribuir datos de salida; y modificar los sistemas operativos.

h) Controles de aplicación de los sistemas de información contable: La existencia y uso de controles apropiados de acceso al software, hardware, y archivos de datos, combinados

con controles sobre la entrada, procesamiento y salida de datos pueden, en coordinación con las políticas de la administración, compensar por algunas de las debilidades en los controles generales de CIS en ambientes de microcomputadoras. Los controles efectivos pueden incluir:

1. Un sistema de registros de transacciones y de contrapartidas por lotes;
2. Supervisión directa; y
3. Conciliación de recuentos de registros o cifras de control.

El control puede establecerse por una función independiente que normalmente incluye la revisión de que todos los datos sean procesados; autorizados y registrados; así como dar seguimiento de todos los errores detectados durante el procesamiento y verificar la distribución apropiada de los datos de salida y restringiría el acceso físico a los programas de aplicación y archivos de datos.

1.11.2 NORMAS DE AUDITORIA DE SISTEMAS

Las Normas de Control Interno Informático aplicables a la industria farmacéutica se mencionan[10]:

[10] Normas de Control Interno Informático (en línea), disponible en <htpp://www.mag.gob.sv/admin/publicaciones// (consulta 20 junio 2006)

1.11.2.1 Norma 500, Sección 03 Controles de Datos Fuentes, de operación y de salida

Deben diseñarse controles con el propósito de salvaguardar los datos fuente de origen, operaciones de proceso y salida de información, con la finalidad de preservar la integridad de los datos procesados por la entidad.

Para implementar los controles sobre datos fuente, es necesario que la entidad designe, a los usuarios encargados de salvaguardar los datos. Para ello, deben establecerse políticas que definan las claves de acceso para los tres niveles de consulta, captura y modificación de datos

Los controles de operación de los equipos de cómputo están dados por procedimientos estandarizados y formales que describen en forma clara y detallada los procedimientos; y asignan los trabajos con niveles efectivos de utilización de equipos.

Los controles de salida de datos deben proteger la integridad de la información, para tal efecto es necesario tener en cuenta aspectos como: copias de la información en otros locales, la identificación de las personas que entregan el documento de salida y, la definición de las personas que reciben la información.

Corresponde a la dirección de la entidad en coordinación con el Área de Informática, establecer los controles de datos fuente, los controles de operación y los controles de

seguridad, con el objeto de asegurar la integridad y adecuado uso de la información que produce la entidad.

1.11.2.2 Norma 500 Sección: 05 Seguridad de programas, de datos y de equipos de cómputo

Deben establecerse mecanismos de seguridad en los programas y datos del sistema para proteger la información procesada por la entidad, garantizando su integridad y exactitud, así como respecto de los equipos de computación.

El Sistema de Información debe estar protegido desde el desarrollo de los sistemas (software), hasta la instalación de los equipos (hardware); clasificándose la seguridad en estos casos en lógica y física, respectivamente.

Partiendo que la seguridad lógica son los mecanismos relacionados con la protección del sistema, su implementación y operatividad.

Los requisitos de control más importante son:

a) Restricciones de acceso a los archivos y programas para los programadores, analistas u operadores.

b) Claves acceso (password) por usuario para no violar la confidencialidad de la información;

c) Elaborar copias de respaldo de los datos procesados en forma diaria, semanal o mensual (backups), y descentralizada para evitar pérdida de la información;

d) Desarrollar un sistema de seguridad como software de control de todas las actividades;

e) Mantener programas antivirus actualizados para evitar el deterioro de la información, según la vulnerabilidad del sistema.

La seguridad física de equipos, tiene como propósito evitar las interrupciones prolongadas del servicio de procesamiento de datos, debido a desperfectos en los equipos, accidentes, incendios y toda serie de circunstancias que haga peligrar el funcionamiento del sistema.

Corresponde a la Oficina de Informática, en coordinación con la administración de la entidad establecer los mecanismos de seguridad de los programas y datos del sistema, que permitan asegurar la integridad, exactitud y acceso a las informaciones que se procesan internamente.

1.11.2.3 Norma 500 Sección: 06 Plan de Contingencias

El Área de Informática debe elaborar el Plan de Contingencias de la entidad que establezca los procedimientos a utilizarse para evitar interrupciones en la operación del sistema de cómputo.

El plan de contingencias es un documento de carácter confidencial que describe los procedimientos que debe seguir la oficina de informática para actuar en caso de una emergencia que interrumpa la operatividad del sistema de cómputo. La aplicación del plan permite operar en un nivel aceptable cuando las facilidades de procesamiento de información no están disponibles.

Además, debe evaluarse la posibilidad de suscribir convenio con otra institución que tenga una configuración informática similar a la propia entidad para utilizarla en caso de desastre total. La puesta en funcionamiento del plan debe efectuarse sobre la base de que la emergencia existe y tienen que utilizarse respaldos posiblemente de otras instituciones. Los supuestos que se utilicen para la simulación deben referirse a los hechos que ocurrirían en caso de una emergencia real, tomando en cuenta todos sus detalles.

Corresponde al Área de Informática elaborar, mantener y actualizar el Plan de Contingencias, a fin de asegurar el funcionamiento de los sistemas de información que requiere la entidad para el desarrollo de sus actividades.

1.11.3TÉCNICAS DE AUDITORIA CON AYUDA DE COMPUTADORA (TAAC’s)

Otra herramienta aplicable es el uso de las TAACs, (1009 - TÉCNICAS DE AUDITORÍA CON AYUDA DE COMPUTADORA), las cuales pueden mejorar la efectividad y eficiencia de los procedimientos de auditoria. Pueden también proporcionar pruebas de control efectivas y procedimientos sustantivos

cuando no haya documentos de entrada o un rastro visible de auditoria, o cuando la población y tamaños de muestra sean muy grandes.

Las TAACs, pueden desempeñar diversos procedimientos de auditoria, los que pueden ser de gran utilidad en el manejo de controles internos informáticos, los cuales se detallan a continuación:

a) Pruebas de detalles de transacciones y saldos
b) Procedimientos analíticos
c) Pruebas de controles generales
d) Muestreo de programas para extraer datos para pruebas de Auditoria
e) Pruebas de controles de aplicación

1.12 ASPECTOS LEGALES RELATIVOS AL CONTROL INTERNO INFORMÁTICO Y LOS ACTIVOS CORRIENTES.

Con el desarrollo de la tecnología informática se dan muchos problemas en relación a la violación de la propiedad intelectual como lo es la manipulación fraudulenta de las computadoras con ánimo de lucro, la destrucción de programas o datos, el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, así como también la piratería (CD’s musicales y de software), En este sentido, la informática puede ser el objeto del ataque o el medio para cometer otros delitos. La importancia de los sistemas de información, en las empresas, tanto públicas como

privadas, los ha transformado en un objeto cuyo ataque provoca un perjuicio enorme, ya que resultan relativamente fáciles de realizar, con resultados altamente satisfactorios y al mismo tiempo procuran a los autores una probabilidad bastante alta de alcanzar los objetivos sin ser descubiertos.
La piratería de software es atentar contra los derechos de la propiedad intelectual. Por ejemplo: copias ilegales en formato de CD-R, producto educativo sin autorización, instalación de software sin una licencia debidamente autorizada, o cuando lo hace en más sistemas de los que está autorizado, por Internet se trata de cualquier tipo de piratería que implique la distribución electrónica no autorizada o la descarga desde Internet de programas de software con copyright.

1.12.1 Ley de Fomento y Protección de la Propiedad Intelectual

Esta ley tiene por objeto asegurar una protección suficiente y efectiva de la propiedad intelectual, estableciendo las bases que la promuevan, fomenten y protejan.

Un Programa de ordenador, ya sea de fuente o de objeto, es la obra literaria constituida por un conjunto de instrucciones expresadas mediante palabras, códigos, planes o en cualquier otra forma que, al ser incorporadas en un dispositivo de lectura automatizada, es capaz de hacer que un computador, o sea, un aparato electrónico o similar capaz de elaborar informaciones, ejecute determinada tarea u obtenga determinado resultado. Se presume que es productor del programa de

ordenador, la persona que aparezca indicada como tal en la obra de la manera acostumbrada, salvo prueba en contrario.
El contrato entre los autores del programa de ordenador y el productor, implica la cesión ilimitada y exclusiva a favor de éste de los derechos patrimoniales reconocidos en la presente ley, así como la autorización para decidir sobre su divulgación y la de ejercer los derechos morales sobre la obra, en la medida que ello sea necesario para la explotación de la misma, salvo pacto en contrario.[11]

1.12.2 Ley de Impuesto sobre la Renta

Las industrias farmacéuticas generalmente poseen software contables, que les permiten procesar su información, es por ello que necesitan conocer las disposiciones legales para su amortización[12] el cual literalmente dice:

Art. 30-A. Es deducible de la renta obtenida mediante amortización, el costo de adquisición o de producción de programas informáticos utilizados para la producción de la renta gravable o conservación de su fuente, aplicando un porcentaje fijo y constante de un máximo del 25% anual sobre el costo de producción o adquisición, todo sin perjuicio de lo dispuesto en los siguientes literales:

[11] Ley de Fomento y Protección de la propiedad Intelectual, Articulo 32-33 , Publicado en el Diario Oficial N° 150, Tomo N° 320, del 16 de Agosto de 1993
[12] Decreto Oficial No. 664, publicado en el Diario Oficial, publicado el 17 de marzo de 2005.

a) En el caso de programas informáticos producidos por el propio contribuyente para su uso, no será deducible el costo capitalizado cuando hayan sido deducidos con anterioridad en un período o ejercicio de imposición las erogaciones que conforman dicho costo.

b) Para efectos de esta deducción no es aplicable la valuación o reevaluación de los programas

c) Cuando se adquiera un programa utilizado, el valor máximo sujeto a amortización será el precio del programa nuevo al momento de su adquisición, ajustado de acuerdo a los siguientes porcentajes:

AÑOS	**PORCENTAJE**
1 AÑO	80%
2 AÑOS	60%
3 AÑOS	40%
4 AÑOS	20%

d) En el caso de los programas o software cuyo uso o empleo en la producción de la renta gravada no comprenda un ejercicio de imposición completo, será deducible únicamente la parte de la cuota anual que proporcionalmente corresponda en función del tiempo en que el bien ha estado en uso de la generación de la renta o conservación de la fuente en el período o ejercicio de imposición.

e) El contribuyente solamente podrá deducirse la amortización del programa o software de su propiedad, y mientras se encuentren en uso en la producción de ingresos gravables.

f) Cuando el software se utilice al mismo tiempo en la producción de ingresos gravables y no gravables o que no constituyan renta, la deducción de la deprecación se admitirá únicamente en la proporción que corresponda a los ingresos gravables en la forma prevista en el Art. 28 inciso final de esta Ley.

g) Si el contribuyente hubiera dejado de descargar en años anteriores la partida correspondiente de amortización del programa o software no tendrá derecho a acumular esas deficiencias a las cuotas de los años posteriores.

1.12.3 Ley del Impuesto a la Transferencia de Bienes Muebles y a la Prestación de Servicios

De acuerdo a la Ley de Impuesto a la Transferencia de bienes muebles y a la prestación de servicios, la industria farmacéutica se encuentra gravada para el pago del respectivo impuesto.

En el Art. 4 de la Ley; constituye como hecho generador del impuesto la transferencia de dominio de bienes muebles corporales, entiéndase dicho tema cualquier bien tangible que sea transportable de un lugar a otro.

Asimismo, el retiro de bienes muebles del activo realizable de la empresa, aun de su propia producción, destinados al uso y consumo propio, de los socios, directivos o personal de la empresa. Entendiéndose como activo realizable, el conjunto de bienes corporales propios del giro o actividad, producidos para venderlos o transferirlos.

Por otra parte son hechos generadores aquellos bienes para la distribución gratuita con fines promociónales de propaganda o publicitarios, como son el caso de las muestras de medicina que se les proporciona a farmacias, médicos y hospitales.

Asimismo establece que los bienes retirados del inventario de la compañía sin justificación, es decir por caso fortuito o por fuerza mayor, constituye un hecho generador para el pago de impuestos por ejemplo: incendio, robo, merma, inundación, entre otros.

Según el art. 22 de la referida ley, son contribuyentes del impuesto, los productores, comerciantes, mayoristas o al por menor, realizan en forma habitual la venta u otras operaciones, es decir la transferencia de bienes muebles corporales.

La industria farmacéutica se encuentra en la categoría de productores de medicina, utilizando la materia prima de su propio autoconsumo.

1.13 PRINCIPALES ÁREAS DE APLICACIÓN DE CONTROL INTERNO INFORMÁTICO EN LAS INDUSTRIAS FARMACÉUTICAS

La aplicación de controles internos informáticos dentro de las industrias farmacéuticas, requiere de mayor atención en áreas susceptibles como lo son los activos corrientes.

La importancia de los activos corrientes radica en que estos son los medios para obtener mercancías y servicios. Asimismo una cuidadosa contabilización pues son vulnerables a los fraudes y robos. En algunos casos en la industria farmacéutica no se tienen creados controles internos informáticos y por otra parte pueden existir pero no se adecuan a las necesidades de la empresa, por lo que se dificulta encontrar o detectar posibles errores que pueden ocasionar que la información procesada en los sistemas no sea efectiva.

1.14 SITUACIÓN ACTUAL DE LA INDUSTRIA FARMACÉUTICA EN RELACIÓN A LOS CONTROLES INTERNOS INFORMÁTICOS.

Las industrias farmacéuticas en El Salvador, se han posicionado dentro del mercado en un mayor porcentaje en los últimos años, lo que les ocasiona que en su mayoría estén a la vanguardia de la tecnología, con sistemas modernos, los cuales les garanticen controlar todas sus operaciones.

Entre los principales productos fabricados por el sector industrial farmacéutico están: analgésicos, antigripales,

antibacterianos, antiparasitarios, analgésicos no esferoidales, expectorantes, antirreumáticos, entre otros.

El personal de la industria farmacéutica, requiere un componente mínimo de profesionales universitarios y técnicos de la carrera de Química y Farmacia, Técnicos en Sistemas y Profesionales en Contaduría Publica.

Los estándares de calidad exigidos por los organismos gubernamentales encargados de supervisar la salud pública, se basan en las normas internacionales. En el país se exige a los laboratorios que cuenten en su organización con una unidad encargada del control de calidad de los productos. Este requisito ocasiona altos costos para los pequeños y medianos laboratorios debido a que sus bajas producciones no les permiten aprovechar las economías a escala. Los cuales se logran a través de la implementación de controles administrativos, contables y de sistemas.

En la industria farmacéutica se manejan grandes volúmenes de operaciones, por lo que es de valiosa importancia contar con sistemas informáticos que logren cubrir la demanda requerida de información para que esta se genere de manera confiable y oportuna para la toma de decisiones. El control interno debe su existencia dentro de la empresa por el interés de la propia gerencia. Ningún administrador desea ver pérdidas ocasionadas por error o fraude o a través de decisiones erróneas basadas en informaciones financieras no confiables. Así, el control interno es una herramienta útil mediante la cual la administración logra asegurar, la conducción ordenada y

eficiente de las actividades de la empresa. Otra parte fundamental lo constituye el control interno informático en ese sentido, la garantía de que los informes, estados financieros y datos generales, sean correctos y estén formulados de acuerdo con las necesidades del caso particular de que se trate la responsabilidad importante de las empresas, y establecer si están operando como se estableció y que están diseñados en forma apropiada, para sugerir los cambios en las condiciones. Esto involucra la valoración del diseño y operación de los controles y tomando las acciones necesarias correctivas; lo cual repercute en el buen manejo de los activos corrientes dentro de la empresa, y por consecuente la confiabilidad de la información presentada en los estados financieros.

CAPITULO II

2. METODOLOGÍA Y DIAGNOSTICO DE LA INVESTIGACION

2.1 METODOLOGIA DE LA INVESTIGACION

2.1.1 Tipo de Estudio

El tipo de estudio realizado fue el Analítico Descriptivo que consistió en un primer momento en identificar la problemática existente, posteriormente se describió y analizó las áreas específicas de Activos corrientes de las Industrias Farmacéuticas.

2.1.2 POBLACION Y MUESTRA

2.1.2.1 Población a Investigar

Para la selección de la población se determino mediante la observación. En donde se identificó que está integrada por las industrias farmacéuticas ubicada en el Departamento de San Salvador, según listado proporcionado por la Dirección General de Estadísticas y Censos, (DIGESTYC).(Ver Anexo 2)

2.1.2.2 Muestra Sujeta de Estudio

Debido a que la población sujeta de estudio es menor a 47 unidades de observación, no se consideró necesario hacer una selección de la muestra a través de fórmulas estadísticas, por lo que se decidió examinarla en su totalidad.

2.1.3 TECNICAS E INSTRUMENTOS DE LA INVESTIGACION

Las técnicas que se utilizaron para obtener la información necesaria fueron:

2.1.3.1 Investigación de Campo

La visita de campo consistió en la observación directa realizada a la población en estudio sobre las políticas y procedimientos de control interno informáticos relativos a los activos corrientes, con el fin de identificar la existencia y aplicación de éstos

2.1.3.2 Investigación Bibliográfica

Se seleccionó como técnica de investigación la revisión documental para lo cual se procedió a la consulta de textos y contenidos de trabajos de graduación relacionados con el tema, información obtenida a través de Internet, revistas y otra documentación con información relacionada.

2.1.3.3 Encuesta

Se seleccionó como técnica para el manejo de los instrumentos el cuestionario, con la cual se recopiló información confiable sobre la aplicación de controles internos informáticos para las áreas de activos corrientes de las industrias farmacéuticas, mediante la obtención de respuestas a las preguntas formuladas sobre diversos indicadores. (Anexo 3)

2.1.3.4 Entrevistas a Funcionarios Claves de las Industrias Farmacéuticas

Se entrevistó a funcionarios claves con el objeto de obtener información importante que ayudó a fortalecer la investigación respecto al control interno informático.

2.1.4 TABULACION

La tabulación se realizó a través de tablas de frecuencias.(Ver anexo 4)

2.1.5 ANALISIS DE LA INFORMACION

El análisis se realizó mediante la interpretación de las frecuencias absolutas (Fa) y relativas (fr) establecidas por cada pregunta.

2.2 DIAGNOSTICO DE LA INFORMACION

El diagnostico de la investigación se dividió para efecto de un mejor análisis en las siguientes áreas:

a) Conocimiento del Sistema de Procesamiento de la información

b) Capacitación del Sistema Informático Computarizado para fines de Control Interno

c) Impacto del control interno informático en la presentación de los activos corrientes en los estados financieros de la empresa.

2.2.1 CONOCIMIENTO DEL CONTADOR PÚLICO ACERCA DEL SISTEMA DE PROCESAMIENTO DE LA INFORMACION

CUADRO No.1
CONOCIMIENTO DEL CONTADOR PÚBLICO ACERCA DE LOS SISTEMAS DE PROCESAMIENTO DE INFORMACION

No. PREG	CRITERIOS	CONTADORES PUBLICOS ENCUESTADOS	FRECUENCIA RELATIVA
1	Grado académico del contador publico.		
	Licenciatura en Administración de Empresas	6	11.76%
	Licenciatura en Contaduría Pública	27	52.94%
2	Áreas en las cuales el profesional de la contaduría publica tiene mayor experiencia		
	Contabilidad	38	65.52%
	Auditoria en Sistemas	5	8.62%
	Auditoria Interna	9	15.52%
3	Años de experiencia del contador en el área relacionada con los controles internos informáticos		
	1 a 5 años	19	40.43%
	6 a 10 años	18	38.30%
4	Compañías que poseen un sistema de información contable	47	100%
5	Origen del software de contabilidad de las compañías farmacéuticas encuestadas		
	Adquirido en el mercado	28	57.14%
	Contrato de Servicios	12	24.49%
	Desarrollado Internamente	9	18.37%
6	Valor de adquisición del software de contabilidad de las compañías encuestadas es más de $4,000.00	30	63.83%
22	Software de contabilidad que le permiten al contador publico controlar el procesamiento electrónico de datos	29	61.70%

Al analizar e interpretar los resultados obtenidos en la investigación de campo las situaciones detectadas son las siguientes:

La primera área como se muestra en el cuadro No. 1, trata del conocimiento del Contador Publico acerca de los sistemas de información, se puede analizar que el grado académico de los profesionales encuestados un 11.76% pertenece a la Carrera en Administración de Empresas por otra parte un porcentaje significativo de un 52.94% corresponde a Licenciatura en Contaduría Publica, cabe mencionar que este dato es importante ya que se cuenta con los conocimientos básicos necesarios para definir procedimientos, políticas que vayan encaminadas a la salvaguarda y al control de las operaciones de la compañía farmacéutica.

El área de conocimiento y de experiencia que tienen los profesionales en un 65.52% corresponde al área de contabilidad y en un porcentaje muy reducido del 8.62% tienen experiencia en auditoria de sistemas, el cual indica que los profesionales de la contaduría publica necesitan capacitarse en el área informática como una demanda del medio en el cual se desenvuelven, ya que la mayoría de estas empresas todas sus operaciones se llevan a través de sistemas de información.

Los años de experiencia que el contador público tiene en el área relacionada del control informático oscila entre los uno y cinco años el cual representa el 40.43%, es importante este porcentaje ya que si bien es cierto que el profesional cuenta con la experiencia debida en las áreas de su competencia no cuenta con la experiencia en el área relacionada de auditoria de sistemas que es una herramienta básica para efecto de poder llevar a cabo el trabajo de auditoria interna e incluso el trabajo contable.

Es importante recalcar que las compañías tienen un sistema de información contable como se muestra en el cuadro No. 1, el total de la muestra cuenta con un sistema computarizado. En muchas ocasiones este sistema es elaborado a la medida ya que las compañías optan por desarrollar sus propias operaciones dentro de la digitalización de la información.

El origen del software de contabilidad de las compañías farmacéuticas en el 57.14% ha sido adquirido en el mercado con las empresas pioneras en desarrollar este tipo de sistemas. Por otra parte también es evidente el uso de la figura de contrato de servicios la cual se desarrolla a través de outsourcing de la información el cual representa el 24.49% un

porcentaje muy significativo del 18.37% lo han desarrollado internamente, dependiendo de la forma en la que se haya adquirido este sistema de información es necesario que el profesional lo conozca de tal forma que pueda disponer de la información útil para efecto de poder desarrollar adecuadamente los controles internos que se ameriten.

En cuanto el valor de adquisición de los software de las compañías encuestadas el 63.83% que representan 30 compañías dicen que el valor de adquisición del software es significativo en términos monetarios por lo tanto estas compañías tratan de utilizarlos en un 100% en cuanto a la eficiencia y eficacia que les proporcionen.

Colateralmente a este los encuestados mencionaron que el software de la contabilidad también les permite controlar el procesamiento electrónico de datos, la cual genera para los fines de la empresa; dicha herramienta, el cual representa el 61.70% de la muestra que corresponde a 29 profesionales encuestados.

2.2.2 CAPACITACION DEL SISTEMA INFORMÁTICO COMPUTARIZADO PARA FINES DEL CONTROL INTERNO INFORMÁTICO.

CUADRO No.2
CAPACITACION ACERCA DEL SISTEMA DE INFORMACION DE CONTABILIDAD

No. PREG	CRITERIOS	CONTADORES PUBLICOS ENCUESTADOS	FRECUENCIA RELATIVA
7	Empresas que no tienen conocimiento de los costos de mantenimiento del sistema de información	20	42.56%
13	Contadores encuestados que han recibido capacitación sobre el sistema de información que trabaja	41	87.23%
14	Empresas que sus planes de capacitación los ejecuta a través de servicios externos de consultoría	22	46.81%
15	Medios a través de los cuales se capacitan al personal involucrado con la operatización del sistema de información contable		
	Demostraciones	23	44.23%
	Seminarios	20	38.46%
8	Compañías que sus SI no cuentan con un modulo de auditoria	33	70.21%
9	Empresas que cuenta con un módulo de auditoria y que ejecutan controles a través del mismo	14	30%
16	Compañías que consideran que es importante la capacitación en el área de sistemas relacionados con su área de trabajo	46	97.87%
17	Frecuencia con que las empresas capacitan a su personal en cuanto a las modificaciones que haya sufrido el sistema		
	Anual	17	36.17%
	No la ha recibido	11	23.40%

En la segunda área del diagnóstico, sobre la capacitación del sistema informático computarizado para fines de control interno se determinaron los siguientes aspectos:

Que de las empresas encuestadas 20 de ellas contestaron que tienen conocimiento acerca de los costos de mantenimiento de los sistemas de información los cuales representan un 42.56%. Cabe mencionar que parte de los contadores encuestados que han recibido capacitación sobre el uso de los sistemas de información representan el 87.23% el cual es un porcentaje significativo, es decir, que estos conocen las bondades, utilidades y beneficios que el sistema les proporciona.

Mientras que otras empresas, sus planes de capacitación han sido recibidos a través de los servicios externos de consultores que hasta cierto punto resulta ser rentable. Un 46.81% de la muestra, significa que las empresas en su mayoría optan por capacitar a uno de los empleados y luego éste les reproduce la capacitación a través de seminarios internos.

Los medios a través de los cuales se les ha capacitado se encuentran, las demostraciones que tienen un porcentaje significativo del 44.23%, los seminarios con 38.43% lo cual coopera a que el personal pueda conocer a fondo las utilidades del sistema y poderlas utilizar adecuadamente a los diferentes controles internos. Si bien es cierto las empresas cuentan con esta herramienta no en su totalidad le dan uso,

ya que el control interno informático a los activos corrientes es limitado, pues buena parte de los profesionales solo conocen el control interno limitándose a la salvaguarda de los activos de la empresa, y no se enfocan en el control interno informático el cual vendría en gran medida a complementar la seguridad de la información procesada dentro los mismos sistemas.

En tal sentido las empresas que cuentan con el módulo de auditoria que se ejecuta a través del software, se limita al 30% de la muestra, significa que la mayoría de empresas no poseen un sistema de información que cuente con herramientas de auditoria, por lo que es necesario desarrollar a través de esta, diferentes controles de auditoria y que permitan asegurar y salvaguardar la información que se presenta en los estados financieros.

Las compañías que consideran que es importante la capacitación en el área relacionada a su trabajo es el 97.87% es decir, las empresas están concientes de la necesidad que tienen de especializarse en el área de informática, pues quiérase o no todas las operaciones están involucradas en el ambiente informático, en tal sentido es importante que estén a la

vanguardia de las innovaciones y en lo relativo al área de trabajo como la contabilidad y las finanzas sin obviar además la auditoria que es importante para efecto de poder hacer un examen sistemático detallado de control que pueda garantizar la razonabilidad y confiabilidad de las cifras presentadas en los estados financieros.

Muchas compañías no cuentan con planes de actualización en cuanto se hace un cambio en el sistema lo que implica una remodelación de la base de datos que en alguna medida ayuda a los reportes o en algunas actividades monetarias de la organización.

En tal sentido de las personas encuestadas 17 de ellas que representan el 36.17% dicen que se les capacita con respecto a estos cambios, sin embargo un porcentaje significativo del 23.40% dice que no, lo cual implica una reestructuración o reingeniería de los procesos que incide directamente sobre los controles internos que se ejecutan para efecto de llevar a cabo un adecuado control interno y más aun un adecuado control interno informático de las áreas criticas que representa el área de los activos corrientes.

2.2.3 IMPACTO DEL CONTROL INTERNO INFORMÁTICO EN LA PRESENTACION DE LOS ACTIVOS CORRIENTES EN LOS ESTADOS FINANCIEROS DE LA EMPRESA.

CUADRO No.3
IMPACTO DEL CONTROL INTERNO INFORMATICO EN LOS ESTADOS FINANCIEROS.

No. PREG	CRITERIOS	CONTADORES PUBLICOS ENCUESTADOS	FRECUENCIA RELATIVA
11	Compañías que no se interesan por que Sistemas de información contenga controles internos relacionados con áreas de interés como los activos corrientes.	14	29.79%
12	Compañías que se interesan por la implementación de controles internos mediante los siguientes medios		
	Capacitaciones	13	27.66%
	Demostraciones	9	19.15%
	Manuales	9	19.15%
25	Áreas de activos corrientes que se manejan a través del SI de la empresa		
	Efectivo y Equivalentes	43	0.7963
	Inventarios	44	0.8148
	Documentos por cobrar	40	0.7407
	Cuentas por cobrar	44	0.8148
10	Activos corrientes a los cuales se les aplican la rutina de control interno informático		
	Efectivo	23	26.44%
	Inventario	33	37.93%
	Cuentas por cobrar	27	31.03%
20	Tipos de Registros que se generan en el sistema de información		
	Partidas contables	45	66.17%
	Estados Financieros	43	63.23%
	Disponibilidad	42	61.76%
	Manejo de existencias	44	64.70%
	Detalle de costos	39	57.35%
	Detalle de Cuentas por cobrar	45	66.17%

No. PREG	CRITERIOS	CONTADORES PUBLICOS ENCUESTADOS	FRECUENCIA RELATIVA
18	Empresas donde se toma en cuenta al contador para efecto de hacer modificaciones en el SI	21	44.68%
19	Empresas que cuenta con controles de autorización para efecto de las modificaciones y mejores del SI	25	53.19%
23	Compañías que no supervisan los constantemente los controles que genera el sistema de contabilidad	19	40.43%
21	Empresas que consideran que la información procesada en SI es confiable	37	78.72%
24	Controles que permite generar el sistema de información		
	Preventivos	8	11.11%
	Detectivos	9	12.50%
	Informáticos	6	8.33%
	Administrativos	16	22.22%
	Contables	16	22.22%
	Ninguno	12	16.67%
26	Principales reportes que genera el software contable		
	Emisión de cheques	11	13.92%
	Generación de costos	11	13.92%
	Antigüedad de Saldos	11	13.92%
27	Profesionales que tienen acceso a los controles que emite el sistema	27	57.45%
28	Empresas que accedan a través de passsword a los distintos controles informáticos. del SI	28	59.47%
30	Empresas que cuenta con la evidencia de los controles que genera el sistema a través de los usuarios	32	68.09%
29	Medios a través de los cuales se puede obtener la información de los controles que genera el sistema		
	Impresa	46	74.19%
	Previo de pantalla	44	70.97%
	Medios magnéticos	34	54.84%

No. PREG	CRITERIOS	CONTADORES PUBLICOS ENCUESTADOS	FRECUENCIA RELATIVA
31	Profesionales que consideran que es importante el Control Interno Informático para el manejo adecuado de los Activos Corrientes	45	95.74%
32	Empresas que consideran que los Controles Internos Informáticos aplicados los activos corrientes son confiables de acuerdo a SI	32	68.09%
34	Contadores que consideran que es necesario contar con un documento que le ayude a formular los Controles Internos Informáticos adecuados para el manejo confiable de la información presentada en los activos corrientes de la empresa	42	89.36%

Como se puede analizar el cuadro 3 impacto del Control Interno Informático en los estados financieros, 14 compañías encuestadas que representan el 29.79%, no se interesen de tener controles internos en el área de activos corrientes lo cual es importante analizar debido a que si toda la información es llevada a través de sistemas de información debe ser analizada con mucha atención. Cabe mencionar que las compañías que se interesan por la implementación de controles internos lo han logrado a través de los siguientes medios como lo es la capacitación ya que 13 de los encuestados que representan el 27.66% dicen que la capacitación es un medio efectivo para la implementación de controles internos, no obstante los demás medios tienen un porcentaje significativo tales como demostraciones con 19.15%, lo cual es importante ya

que muchos de los usuarios o profesionales se capacitaran mejor mediante la técnica: aprender haciendo, es decir entrando de lleno en el sistema y ver a través de demostraciones o capacitaciones como se obtiene la información confiable de las diferentes bases de datos o de las diferentes rutinas del sistema.

Por otra parte los manuales tienen un porcentaje significativo de 19.15% ya que éstos manuales en su mayoría ayudan a los usuarios para poder efectuar toda las operaciones que están dentro del sistema que al momento de una capacitación o de una demostración no se tomaron en cuenta, es importante que las compañías que tienen un sistema de información para efecto de poder llevar adecuadamente sus controles hagan referencia o tomen en consideración en sus planes de capacitación las demostraciones y contar con los manuales pertinentes.

En las áreas de los activos corrientes a los cuales se les aplica la rutina de control interno informático principalmente se pudo observar en la investigación que el efectivo y equivalentes de efectivo, representa el 26.44% así el área de cuentas por cobrar un 31.03%, el inventario de 37.93%, son las áreas de mayor riesgo por lo tanto las compañías están concientes de la necesidad que tienen de implementar

adecuadamente estos controles internos a fin de reflejar en los estados financieros razonable y confiablemente la información que es base para la toma de decisiones.

Los tipos de registros que generalmente se generan en los sistemas de información va desde la parte contable hasta detalles más específicos, en tal sentido las personas encuestadas contestaron en el siguiente orden de prioridad:

Partidas contables 66.17%

Estados financieros 63.23%

Disponibilidad 61.76%

Manejo de existencias 64.70%

Detalle de costos 57.35%

Detalle de cuentas por cobrar 66.17%

Las empresas que realizan controles internos informáticos en el área de activos corrientes representan significativamente el 53.19% lo cual es importante ya que estas compañías tratan en lo posible de tener actualizado no solamente el sistemas información sino también tener actualizado en sistemas de control lo cual ayuda significativamente al examen que el auditor realiza o bien a las operaciones que el contador

público realiza dentro de su función de contabilidad y finanzas.

Sin embargo las compañías que no supervisan constantemente los controles que generan los sistemas de información contable constituye, el 40.43% que representa 19 empresas, esto implica que corren el riesgo que la información que es presentada en sus estados financieros este viciada o tenga errores de sistema ya sea interno o externo, de seguridad física o lógica, que debido a que no se supervisa constantemente o no hay una rutina especifica para poder evaluar el procesamiento electrónico de datos se puede estar presentando errores importantes dentro de la situación económica y financiera de la empresa.

Por otra parte las empresas que consideran que la información que se procesa en los sistemas de información es confiable representa el 78.72% que significa 37 empresas, estas confían en la información que se emite en el sistema debido a la seguridad que proporciona sin embargo es necesario tomar en cuenta ciertas rutinas de controles detectivos, preventivos, informativos, administrativos entre otros.

En tal sentido mediante este tipo de controles se puede observar de acuerdo a la investigación realizada, las empresas farmacéuticas le procuran dar importancia a los controles administrativos y contables, y obvian los controles detectivos y preventivos, en un 11.11% y 12.50 respectivamente no se interesan por este tipo de controles lo cual debe ser de rutina ya que cuando se trabaja en un sistema de información es necesario la revisión lógica del sistema y así como la revisiones constantes que determine que el procesamiento electrónico de datos sea efectivo y eficiente para los fines que la empresa persigue.

Los principales reportes que genera el software contable son la emisión de cheques generación de costos y la antigüedad de saldos principalmente la generación de costos que representa 13.92% que debido al giro de estas empresas farmacéuticas es importante contar con este módulo ya que debido al uso adecuado de la información que se procesa en el se puede obtener un uso confiable de los costos.

Por otra parte se averiguo el acceso de los controles a que tiene los profesionales a estos sistemas en tal sentido el 57.45% que representa 27 contadores encuestados tienen acceso a estos sistemas. Por lo tanto es evidente que no todos tienen

acceso a esta información ya sea por política de la compañía como prevención o por cualquier manipulación de la información.

Las empresas que cuentan con evidencia de los controles que genera el sistema informático a través de los usuarios significativamente son 32 empresas de las encuestada, ya que tienen estos controles lo cual representa un 68.09% en tal sentido las empresas tratan de asegurar el rastro que hacen los profesionales a través de los diferentes controles a fin de poder identificar en cualquier momento ya sea presunción de fraude o malversación de estas áreas tan importantes de las compañías. Y con ello poder identificar quienes han sido las personas que han entrado al sistema inadecuadamente o de forma indebida.

En tal sentido los medios a través de los cuales se puede obtener información de los controles internos que genera el sistema 70.97% los previos de pantalla, impresión de pantalla 74.19% y significativamente el 54.84% medio magnéticos, que son los tres medios básicos para que un auditor pueda cerciorarse de cómo se está manejando el sistema y la

metodología del control interno informático para fines de canalizar la calidad de la información.

Por otra parte los profesionales que consideran que es importante el control interno informático en el manejo adecuado de los activos corrientes son el 95.74% es decir los profesionales están concientes de que no es suficiente tener un sistema de información que se encargue de todas las operaciones rutinarias de la compañía sino más bien tener un adecuado sistema de control que permita confiar en que las cifras se presentan en cada uno de esos reportes están de acuerdo a la realidad de las operaciones.

Los contadores conocen la debilidad de esta área de control interno informático también, por lo que consideran importante contar con un documento que les ayude a formular los controles internos informáticos a fin de tener un adecuado manejo de la información y por ende que los activos corrientes de la compañía con el propósito que se presenten razonablemente y fiablemente en los reportes financieros para la toma de decisiones.

CAPITULO III

3. GUIA DE CONTROL INTERNO INFORMATICO PARA LAS PRINCIPALES AREAS DE ACTIVOS CORRIENTES DE LAS INDUSTRIAS FARMACEUTICAS.

3.1 SITUACION ACTUAL

Actualmente en las industrias farmacéuticas el uso de sistemas informáticos es necesario, debido a los grandes volúmenes de información y las exigencias del mundo globalizado, lo que les obliga a estar a la vanguardia de la tecnología.

El uso inadecuado de los medios computarizados para el procesamiento de datos, implica estar expuestos a un sin fin de riesgos para los cuales se requiere dentro de lo posible estar preparados para minimizarlos y en el mejor de los casos a neutralizarlos.

La utilización de un sistema computarizado en el procesamiento de datos vuelve a la información, muy valiosa para las industrias, por lo que la Gerencia deberá establecer políticas y procedimientos para la custodia y salvaguarda de dichos bienes.

Siendo la Administración la encargada de establecer mecanismos idóneos que permitan que la información generada sea fiable, oportuna, integra, completa y confidencial, deberá establecer medios que le permitan garantizar la toma de decisiones, considerando la vulnerabilidad del hardware y los programas, se ve obligada a elaborar un plan de contingencia que le permita garantizar la seguridad de la información.

Tomando en cuenta la necesidad y la importancia de establecer controles que le permitan a la Gerencia seguridad en la información se vuelve necesario la elaboración de una Guía de Controles Internos Informáticos, que les garanticen la protección de los bienes tan importantes como lo esta la información generada por los sistemas.

3.2 GUIA PARA LA ELABORACION DE CONTROLES INTERNOS INFORMATICOS PARA LAS PRINCIPALES AREAS DE ACTIVOS CORRIENTES DE LAS INDUSTRIAS FARMACEUTICAS.

La presente guía podrá ser utilizada por cualquier empresa que decida adoptarla, siempre y cuando se adapte a las políticas y procedimientos definidos por la administración, puesto que constituye un instrumento de orientación para la implantación de Controles Internos Informáticos para el Área de Activos Corrientes, abordando las áreas criticas de toda empresa, tales como Efectivo y Equivalentes, Cuentas por Cobrar e Inventarios.

Guía para la Elaboración de Controles Internos Informáticos para las Principales Áreas de Activos Corrientes de las Industrias Farmacéuticas.

Índice

1. Objetivo

Proporcionar una herramienta para la implementación de Controles Internos Informáticos, para el área de activos corrientes de las industrias farmacéuticas encaminados a garantizar la confiabilidad y veracidad de la información procesada en los sistemas computarizados.

2. Alcance

La presente guía es un instrumento que proporciona políticas y procedimientos de control interno informáticos aplicados a las principales áreas activos corrientes de una industria farmacéutica, tales como Efectivo y Equivalentes, Cuentas por Cobrar e Inventarios.

3. Dirigido a

- Gerentes Financieros
- Profesionales de la Contaduría Publica
- Auditores Internos y Externos
- Departamentos de Informática

4. Delimitación de Responsabilidad

El uso de la guía de control interno informáticos esta bajo la responsabilidad de la administración de aquellas entidades que deseen adoptarla.

5. Políticas y Procedimientos Generales de Control Interno Informático

5.1 Establecimiento de Funciones

La gerencia debe determinar funciones y responsabilidades

Procedimientos:

1. La gerencia debe asegurarse que el personal de la entidad conoce sus funciones y responsabilidades

2. El personal debe tener autoridad suficiente para ejercer las funciones y responsabilidades que se le asignen.

5.2 Implementación de la Seguridad Física y Lógica

Es responsabilidad de la gerencia la implementación de la seguridad física y lógica.

Procedimientos:

1. La gerencia debe asignar formalmente la responsabilidad del aseguramiento de la seguridad física y lógica de los activos.

2. Se debe crear un procedimiento para nombrar formalmente los responsables de los datos y sistemas en cuanto a decidir respecto a la seguridad y acceso a los sistemas.

5.3 Hardware de Respaldo

La gerencia deberá contar con hardware de respaldo, el cual deberá ser utilizado en el momento necesario.

Procedimientos:

1. La gerencia debe asegurarse de tener identificadas las alternativas con respecto al hardware a ser utilizado en caso de desastres u otra contingencia.

2. Se debe asegurar con un contrato formal para alternativas de uso del hardware en caso de pérdidas.

5.4 Seguridad de los Sistemas

La gerencia deberá garantizar la seguridad de los sistemas

Procedimientos:

1. Se debe salvaguardar la información contra el uso o divulgación no autorizados, daño o pérdida.

2. Implementar controles de acceso, que aseguren que el ingreso a los sistemas, datos y programas se deben restringir el ingreso de usuarios no autorizados.

3. Tener en cuenta para la seguridad de los sistemas los siguientes aspectos: la autorización, autenticación del acceso, perfiles de usuario, identificación,

administración de claves de encriptación, detección y prevención de virus.

5.5 Administración de Sistemas

La seguridad de los sistemas debe ser administrados de tal manera que dichos concuerden con las necesidades de la empresa.

Procedimientos:

1. Implementar un plan de seguridad
2. Actualizar el plan de seguridad
3. Evaluar el impacto de la demanda de cambio en la seguridad de los sistemas.
4. Se debe supervisar la aplicación del plan de seguridad a través de rutinas de verificación del uso del sistema
5. Adecuación de los procedimientos por parte de la empresa.

5.6 Acceso a los Sistemas

La gerencia será la única para determinar la identificación, autenticación y acceso a los sistemas.

Procedimientos:

1. El acceso lógico y el uso de los recursos del sistema debe estar restringido a personas no autorizadas.

2. Se debe minimizar la cantidad de veces que un usuario autorizado debe ingresar sus contraseñas.
3. Deben existir mecanismos de acceso que incorporen medidas de seguridad efectiva, como lo es el cambio regular de contraseñas.

5.7 Lineamientos de Seguridad

Establecer lineamientos de seguridad.

Procedimientos:

1. Los lineamientos estarán dados de acuerdo a los niveles jerárquicos, tomando en consideración a los usuarios del sistema.

2. Se debe clasificar la información y creando mayor control de los niveles de acceso.

3. Determinar lineamientos para establecer privilegios a los usuarios

4. Delimitar las responsabilidades de acuerdo a cada área o departamento que administren la información y programas

5.8 Suministro de Información

La información procesada y almacenada deberá ser suministrada al personal apropiado de manera oportuna

Procedimientos:

1. Enseñar a los usuarios las especificaciones detalladas del sistema.

2. Uso de directrices para asegurar la apropiada dirección del desarrollo de actividades en el sistema.

3. Involucrar a los usuarios en la revisión y aprobación para asegurarse de que los sistemas están diseñados para conocer los requerimientos de los usuarios.

5.9 Modificaciones de los Sistemas

Las modificaciones en el sistema deben ser implementadas correctamente de acuerdo a la hoja de requerimientos de los usuarios.

Procedimiento:

1. Aprobación apropiada del sistema/solicitud de cambios en el sistema.

2. Revisión y aprobación final de los cambios sugeridos por los usuarios.

3. Todos los cambios, incluyendo los hechos en el procesamiento electrónico de datos deberán estar sujetos a las pruebas adecuadas por la dirección encargada.

4. Notificar a los departamentos afectados por los cambios hechos al sistema por medios escritos sean estos memos o correo interno.

5.10 Supervisión de Programas

Supervisar el manejo adecuado del sistema para prevenir fallas en programas, archivos y procedimientos.

Procedimientos:

1. Usar informes de control y ciertos parámetros en el procesamiento electrónico de datos que estén de acuerdo con los procesos apropiados del Modelo Relacional.

2. Establecer procedimientos adecuados para identificar, reportar y aprobar operaciones como: carga inicial del sistema y de las aplicaciones del sistema, reconocer fallas del sistema, situaciones de emergencia y cualquier otra situación inusual.

5.11 Plan de Contingencia

Se deberán elaborar un plan de contingencia para la protección física del hardware y software.

Procedimientos:

1. Para hacerle frente a los desastres, lluvias, terremotos, etc., se debe contar con una bóveda de almacenamiento fuertemente construida para almacenar los archivos y los documentos que se están utilizando.

2. Elaborar con periodicidad Backups de respaldo en medios magnéticos los cuales deberán almacenarse un lugar seguro.

3. Deberán emplearse dispositivos de protección de archivos para evitar un borrado accidental bajo condiciones de casos fortuitos.

5.12 Estrategias de Respaldo y Recuperación

Se deberán implementar estrategias de respaldo y recuperación para sistemas de procesamiento electrónico de datos en línea.

Procedimientos:

1. Deberán elaborarse copia de todas las bases de datos o grandes porciones de la misma en un medio magnético las cuales servirán de respaldo.

2. Se crearan bitácoras de registro de entradas, indicadores de tiempo, fechas, programas y diversos parámetros de modificación realizadas en el sistema.

5.13 Control de Usuarios

Establecer medidas de control de los usuarios del sistema a través de un sub-módulo dentro del sistema en la que se puedan verificar las actividades del personal.

Procedimientos:

1) La gerencia deberá tener acceso a una ventana del sistema en el que le indique los usuarios que lo están utilizando en un determinado momento, con el fin de monitorear el tipo de información a la cual se esta accesando.

2) Monitorear si existen datos compartidos, y que tipo de información se esta distribuyendo a través de la red y quienes son los usuarios.

3) En el caso que existan datos compartidos, entre departamentos que no tengan ninguna relación directa, se debe verificar qué tipo de información es y quiénes son los usuarios finales.

5.14 Salida de Información

Se deben instalar controles de salida para asegurar la exactitud, integridad, oportunidad, y distribución correcta de los datos.

Procedimientos:

1) El sistema deberá generar un registro de cómo fue extraída la información, ya sea esta a través de reportes impresos, medios magnéticos o previos de pantallas.

2) La salida deberá dirigirse inmediatamente a un área controlada, y esa distribución solamente se hará entre personas autorizadas.

3) Los totales de controles de salida deberán conciliarse con los totales de los controles de entrada para asegurar que ningún dato haya sido modificado, perdido o agregado durante el procesamiento o la transmisión, en caso de haber irregularidades, es decir, que no cuadren los totales de control, se aplicarán las sanciones correspondientes, para evitar futuros errores.

5.15 Control de Documentación

Se deberán tener controles de documentación de la información que es almacenada en el sistema, a través de la creación de una carpeta pre-direccionada.

Procedimientos:

1) Se tendrán documentación general del sistema el cual será una guía y proporcionará reglas de operación para los usuarios cuando interactúan con el sistema.

2) Se tendrá una documentación acerca de los procedimientos del sistema el cual consta del manual de procedimientos el cual introduce a todo el personal de operación, de programación y de sistemas al plan maestro del sistema.

3) Se deberá tener documentación de programas y la componen todos los documentos, diagramas y esquemas que explican los aspectos del programa que soporta un diseño de sistemas en particular.

5.16 Control Sobre Operaciones Realizadas por los Usuarios

Se deberá tener un control sobre las operaciones realizadas por los usuarios con cada Terminal utilizada.

Procedimientos:

1. Los usuarios deberán firmar tanto de forma escrita como digital la bitácora de operación de la computadora al inicio y al final de cada turno.

2. El supervisor deberá solicitar reportes de todas las operaciones realizadas dentro de su área durante el día

y el auditor deberá revisar los reportes periódicamente.

3. El usuario debe de ser el único que pueda operar la computadora; se debe tener un control sobre los operadores cuando estos tengan accesos a cintas, discos, programas o documentos importantes.

4. El acceso al área de computadoras deberá estar restringido, con el fin de tener un control más exacto de las operaciones realizadas y las personas que las realizan.

5.17 Impresión de Rutinas de Errores en cada Módulo

El sistema deberá emitir un informe de los errores que hayan ocurrido en el sistema, de los cuales se llevará una bitácora de control.

Procedimiento

1. Cuando ocurra un error en el sistema, este automáticamente enviara a una carpeta pre-establecida un informe de este error.

2. Con una frecuencia de dos semanas, el Ingeniero en Sistemas, verificara cada uno de los errores emitidos y la frecuencia de éstos.

3. Una vez verificados uno a uno los errores, emitirá un diagnostico que permita eliminar la ocurrencia de éstos en el futuro.

4. Emitirá un informe que enviara a la Gerencia General, la cual autorizada realizar si fuera necesario modificaciones al Sistema.

6. Políticas y Procedimientos para el Área de Efectivo y Equivalentes

6.1 Manejo de Efectivo

Ingresar las remesas al módulo de bancos de forma diaria.

Procedimientos:

1. El tesorero o encargo de fondos enviará las remesas al encargado de bancos, para que éste las ingrese de diariamente.

2. Una vez ingresada al sistema al final del día se emitirá un reporte el cual refleje el ingreso total que ha percibido la compañía.

6.2 Arqueos de Efectivo

Los arqueos se llevaran a cabo por medio de Bitácoras las cuales estarán identificadas por vendedor.

Procedimientos:

1. Para los arqueos de los vendedores se llevaran por medio de Bitácoras ingresadas en el sistema con el propósito de tener un archivo de cada uno.

2. La Bitácoras contendrán entre otra información: nombre del vendedor, monto entregado, correlativo de recibo de ingreso, día y persona encargada de arqueo.

6.3 Conciliación de Saldos

Se realizaran conciliaciones de saldos de manera mensual el módulo de bancos con el de contabilidad.

Procedimientos:

1. Al cierre de cada mes se realizará conciliación de saldos imprimiendo un reporte del modulo de bancos contra el reporte del modulo de contabilidad.

2. El saldo ingresado de todas las remesas en el modulo de banco deberá ser igual al saldo contabilizado en la cuenta de bancos.

3. En caso de encontrar diferencias se realizaran las averiguaciones pertinentes con el fin de realizar las modificaciones necesarias.

4. Todo cambio o ajuste será realizado únicamente por el jefe de cada departamento.

5. El cambio o ajuste realizado en el sistema se hará mediante requerimiento solicitado.

6.4 Manejo de Cheques Devueltos

Los cheques devueltos por el banco serán descargados del módulo de bancos de manera oportuna.

Procedimientos:

1. Los cheques devueltos serán ingresados al módulo de bancos identificando la siguiente información: banco, monto y fecha que se remeso dicho cheque.
2. Una vez identificada la remesa dar de baja en el sistema.

6.5 Salvaguarda del Efectivo

Salvaguardar el efectivo y registrarlo en su debida cuenta a través del módulo de Caja y Bancos

Procedimientos:

1. Se deben tener claves de acceso para registrar las transacciones de efectivo al sistema.

2. Para la entrada de datos provenientes de operaciones en efectivo se utilizará un documento fuente o un formato de pantalla.

3. Se deben preparar un reporte de control de efectivo para asegurar que los datos no se hayan perdido y que las transacciones de efectivo se hayan procesado correctamente.

4. El acceso a los registros debe ser restringido, tanto de la información que contenga el sistema así como de los archivos físicos, utilizados en el procesamiento de datos.

5. Todas las recepciones de efectivo deben ser registradas en el sistema y depositadas en forma diaria.

6. Todos los pagos de efectivo se deben realizar mediante cheques emitidos a través del sistema de información contable, y vales de caja cuando el monto sea inferior a $100.00.

6.6 Reporte de Ingresos Diarios

Se generará un reporte diario de los ingresos de efectivo los cuales deberán ser cotejados con el modulo de contabilidad.

Procedimientos:

1. El sistema estará diseñado para emitir un reporte diario, en la que detalle los movimientos de efectivo que se hayan realizados.

2. Luego esta información será enviada al departamento de contabilidad quienes verificaran que la información ingresada al modulo de Caja y Bancos haya sido migrada correctamente al modulo de Contabilidad.

3. En caso de encontrarse diferencias, se conciliaran los reportes de ingresos con la documentación física y se procederá a realizar los ajustes pertinentes.

4. Si la diferencia detectada corresponde a fallas de los sistemas deberá elaborarse un memorando en el que se informe las deficiencias del sistema.

6.7 Emisión de Vales de Caja Chica

Los formularios para Vales de Gastos Menores Caja Chica deben ser emitidos a través del sistema el cual asignara un correlativo a cada uno de estos vales, y estos deberán estar autorizados el jefe del departamento que lo solicita y el Jefe de Tesorería.

Procedimientos:

1. Todos los vales de caja chica deberán estar prenumeradas por el sistema.

2. Deberán ser firmados digital del responsable.

3. Cada Vale de Gastos Menores pagados y liquidados deberá anexárseles los documentos que justifiquen el egreso.

4. La liquidación de la caja chica se realizaran mediante un reporte de los vales emitidos por el sistema junto con los anexos de cada uno de ellos, la cual se liquidara cuando se estime conveniente.

5. Una vez que recibe la liquidación de caja chica en el Departamento de contabilidad se verificara la suma aritmética de cada uno de los anexos, a los cuales se les asignaran su cuenta contables para poder procesarlo en el modulo de Contabilidad.

6.8 Recibos de Ingreso de Efectivo

Los Recibos de Ingresos deben estar prenumerados por el sistema.

Procedimientos:

1. El sistema deberá emitir un recibo de ingreso de efectivo los cuales automáticamente se le asignara un correlativo.

2. Se emitirá un reporte en el cual se detallen todos los recibos que han sido emitidos durante el día, estos deberán cotejarse con los documentos físicos, verificando el correlativo del sistema y los montos ingresados.

3. Los recibos de ingreso deberán estar firmados por las personas que los liquidan por medio de una boleta que se emitirá a través del sistema la cual servirá para posteriores revisiones.

4. Diariamente deberá supervisarse los correlativos emitidos en el sistema contra los impresos, para

asegurase que no existan anomalías o duplicidad en los correlativos.

6.9 Emisión de Reporte de Cheques Pre-fechados y Post-fechados

Se emitirá un reporte en el sistema de los cheques Pre-fechados y Post-fechados.

Procedimientos:

1. Antes de realizar la conciliación bancaria se deberá verificar el reporte que emite el sistema de los cheques pre-fechados y post-fechados y revisar contra chequera y el estado de cuenta del banco.

2. Cotejar los saldos bancarios con las respuestas de confirmaciones bancarias que emite el sistema.

3. Verificar la validez de las partidas que componen la conciliación, tal como los depósitos en transito y cheques expedidos por la empresa y aun pendientes de pago por el banco.

4. Examinar los estados bancarios en búsqueda de alteraciones o modificaciones de cifras y cotejarlo con la información que se encuentra en el sistema de información contable.

7. Políticas y Procedimientos para el Área de Cuentas por Cobrar

7.1 Asignación de Código a Cliente

Asignar un código a cada cliente, que los identifique al momento de la facturación y cobro, es decir que al ingresar al modulo de cuentas por cobrar éste muestre de forma general el código, nombre del cliente, vendedor, zona y saldo adeudado del mismo.

Procedimientos:

1. El código del cliente estará compuesto por la zona geográfica, tipo de cliente y cartera de visitador médico

2. El código deberá comprender dos letras y cuatro números, los cuales serán cambiados únicamente por el administrador de redes y base de datos una vez creado.

3. Deberá existir un código único e irrepetible

4. El encargado de establecer los códigos será el administrador de redes y base de datos.

5. Antes de ingresar al modulo de cuentas por cobrar un nuevo cliente se deberá verificar los datos generales de la empresa, tales como NIT, Registro de IVA, dirección completa, teléfono, e-mail, descuento autorizado, plazo de crédito, visitador medico, entre otros datos.

6. Luego de verificar los datos del cliente, se ingresara se crea el expediente en el modulo de cuentas por cobrar.

7. Una vez ingresado se procederá a imprimir la boleta que contenga todo la información del cliente, para luego archivarla en el expediente físico del mismo.

8. Emitir reportes para conciliar la información ingresada al sistema con la documentada en el archivo físico del cliente.

7.2 Manejo de Expediente de Clientes

Cada cliente contara con un expediente magnético el cual estará almacenado en el módulo de cuentas por cobrar, este contendrá toda aquella información necesaria y suficiente, que permita la adecuada identificación del cliente.

Procedimientos:

1. El expediente del cliente en el sistema estará dividido por los datos generales y datos del crédito recopilados por el visitador medico y autorizado por la gerencia.

2. Los datos generales que contendrá el expediente son: Código de cliente, Nombre completo de la persona natural o jurídica, dirección, teléfono, fax, número de registro de IVA, NIT, entre otros.

3. Los datos de crédito por: Descuento aplicado, monto autorizado del crédito, plazo del crédito, saldo que adeuda, etc.

4. Todo cambio que se realice en el expediente de cliente deberá ser solicitado mediante un requerimiento y autorizado por el jefe del departamento.

5. El expediente del cliente se alimentara mediante la opción modificar o actualizar datos, siempre y cuando este autorizado por el Jefe de Cuentas por Cobrar.

6. Toda actualización o cambio realizado deberá de imprimirse un reporte el cual será archivado en el expediente físico del cliente.

7. Realizar rutinas de revisión de la información registrada en los expedientes, a fin de cerciorarse que lo establecido en el documento físico del cliente se este cumpliendo.

7.3 Reporte de Antigüedad de Saldos

El sistema deberá emitir un reporte de la cartera de clientes estará organizado de acuerdo a la antigüedad de saldos.

Procedimientos:

1. El reporte de la cartera de clientes estará compuesto por la siguiente información: nombre de la compañía,

nombre del reporte, código y nombre de cada cliente, detalle de facturas, fecha de aplicación y vencimiento, antigüedad de saldo, total por cliente y general.

2. La antigüedad de saldos se presentara por intervalos de 30,60,90 y 120 días

3. Esta contendrá un apartado en la cual se refleje el monto activo y el vencido, así como los porcentajes que representa cada uno del total.

4. Por otra parte estará clasificada de acuerdo a la categoría o tipo de cliente es decir excelente, bueno, regular o malo.

5. La cartera presentara la gestión de cobro realizada de aquellos clientes morosos, es decir se llevara un reporte de las llamas realizadas al cliente, los acuerdos a que se llegaron la hora y fecha de la gestión, luego se imprimirá y archivara en el expediente físico del mismo.

6. Presentará información sobre los descuentos o devoluciones realizada a las facturas adeudadas.

7. El control de descuentos suspendidos o liquidados, llevando un reporte por cada cliente de la forma que se proceso el saldo adeudado del cliente, es decir si este se realizo por vía jurídica o acuerdo de plan de pagos.

7.4 Estado Control de Clientes

El módulo de cuentas por cobrar deberá indicar el estado del cliente ya sea este activo o pasivo

Procedimientos:

1. Para la autorización de pedidos el sistema mandará un mensaje de alerta del estado de cliente

2. El estado del cliente será activo o pasivo

3. El estado activo del cliente indicara que su plazo y limite de crédito aun esta vigente

4. El estado pasivo indicara que el cliente esta en mora o fue suspendido por no presentar ningún movimiento durante los tres meses anteriores.

5. Se pedirá una autorización por parte del jefe superior para poder despachar mercadería aunque el cliente se encuentre con mora.

7.5 Despacho de Mercadería

El sistema no permitirá realizar despachos de mercadería con un monto que supere el límite de crédito autorizado

Procedimientos:

1. Cuando se ingrese el código del cliente este deberá reflejar el saldo que tiene de crédito y el saldo disponible a la fecha, por lo tanto cuando se efectúe

una venta está no podrá exceder del límite de crédito autorizado, a no ser que haya autorización de un nivel de crédito mayor.

2. Cuando se ingrese una nueva venta y dicho valor exceda del límite de crédito autorizado, este solo podrá ser despacho si existe una autorización por el personal indicado.

7.6 Modificaciones al Módulo de Cuentas por Cobrar

Podrá realizar cambios y modificaciones en el módulo de cuentas por cobrar únicamente el Jefe de Créditos.

Procedimientos:

1. El jefe de créditos es el único que deberá contar con el nivel de confianza más alto, lo que le permitirá realizar cambios en el módulo de cuentas por cobrar, ya sean cambios correctivos o de anulación de documentos, a nivel de usuario no de base de datos.

2. Deberá pedir autorización a la Gerencia General, únicamente para aquellos cambios que tengan una implicación en la presentación de resultados.

3. Pasara un requerimiento de cambios cuando estos afecten la base de datos

4. Estos cambios solo los podrá realizar el administrador de redes y base de datos.

7.7 Asignación de Password

Cada miembro del departamento de crédito tendrá un pass Word, el cual será de identificación en cada operación registrada en el módulo de cuentas por cobrar.

Procedimientos:

1. Todas las transacciones y operaciones realizadas en el módulo de cuentas por cobrar quedarán registradas con el código de identificación del usuario como una firma digital

2. Establecer un pass Word para cada usuario, el cual deberá estar compuesto por las palabras “crédito” y un número de identificación del equipo.

3. El password se cambiara cada mes, con el propósito de mantener controles de seguridad de la información almacenada.

7.8 Bitácora de Password

El Jefe del Departamento de Créditos, deberá manejar una bitácora de password de todo el personal de su departamento.

Procedimientos:

1. El jefe del departamento de créditos y cobros tendrá un detalle de todos los passsword de su personal, con los cuales podrá tener acceso en un momento determinado.

2. el jefe del departamento de Cuentas por Cobrar será el encargado de asignar los pass Word al personal a su cargo.

3. El password deberá contener caracteres alfa y numéricos.

7.9 Conciliaciones Mensuales

Realizar mensualmente conciliaciones de saldos entre el departamento de Tesorería, Contabilidad y Créditos y Cobros, en los cuales deberá verificarse los reportes generados por cada módulo.

Procedimientos:

1. Los saldos de la cartera de clientes se conciliaran de manera mensual con el saldo de Tesorería, correspondientes a depósitos de clientes y el reflejado por la cuenta por cobrar

2. Se cotejaran los saldos que presenta el módulo de contabilidad con los que presenta Cuentas por Cobrar.

3. Al existir diferencias estas deberán conciliarse.

4. Los reportes se harán por escrito y magnético, dejando evidencia de las diferencias encontradas.

7.10 Manejo de Cheques Devueltos

Los cheques devueltos por el banco se ingresaran al sistema de manera inmediata, afectando la cuenta del cliente correspondiente y la cuenta de bancos.

Procedimientos:

1. Cuando la empresa reciba cheques devueltos por el banco, éstos serán entregados al departamento de crédito y cobro quienes realizaran las investigaciones pertinentes en el módulo de cuentas por cobrar con el fin de determinar a que cliente corresponde dicho abono efectuado.

2. Una vez identificado el cliente, se ingresa y aparecerá en el estado de cuenta del mismo bajo la denominación de Cheque Devuelto.

7.11 Manejo de Cheques Posfechados

Los cheques posfechados se ingresaran al sistema tomando en cuenta la fecha de recepción y cobro.

Procedimientos:

1. Cuando se reciban cheques posfechados por los clientes se ingresaran al sistema tomando en cuenta los siguientes aspectos: fecha de recepción del documento, fecha de pago, nombre del cliente, detalle de facturas que se están cancelando entre otros.

2. El sistema emitirá un reporte de cheques posfechados diario con el propósito de verificar si estos están siendo remesados de manera oportuna.

7.12 Limites de Crédito

El monto de crédito autorizado de los clientes debe de ser igual al contemplado en el expediente del cliente en el sistema y al momento de excederse en el crédito el módulo deberá enviar un mensaje al usuario en el que le indique que no puede facturar porque ha excedido el límite autorizado.

Procedimientos:

1. Una vez autorizado el crédito del cliente por gerencia este debe de ingresarse al expediente del cliente de manera inmediata.

2. El monto autorizado debe de ser igual al valor reflejado en el expediente del cliente registrado en el módulo de cuentas por cobrar.

3. En caso de encontrar diferencias deberá de reportarse al jefe del departamento de crédito para que este realice las gestiones necesarias y los respectivos cambios.

4. Soportar las garantías del crédito a través de escaneo de imágenes.

7.13 Registro de las Ventas

Se registrara en el módulo de contabilidad una partida diaria por la facturación de las ventas realizadas, ya sean estas al crédito o al contado.

Procedimientos

1. Sumar las ventas diarias facturadas en el sistema y cotejarlas con el modulo de facturación.

2. Una vez realizada y cotejada la suma aritmética de todas las ventas se efectuara el registro contable.

3. El monto total registrado deberá ser igual al monto ingresado en el modulo de cuentas por cobrar.

4. En caso de encontrar diferencias realizar las gestiones necesarias con el fin de determinar en que modulo se encuentra dicha diferencia

7.14 Alimentación de Información del Modulo de Cuentas por Cobrar

El modulo de facturación alimentara el modulo de cuentas por cobrar, es decir que el monto facturado deberá ser igual al monto reflejado en la cartera de clientes.

Procedimientos

1. Al momento de ingresar la venta en el modulo de facturación este alimentara el modulo de cuentas por cobrar.

2. Se realizara de forma diaria conciliación de saldos entre el modulo de cuentas por cobrar con el modulo de facturación.

3. En caso de encontrar diferencia determinar si esta fue por error del sistema o una mala aplicación realizada.

4. Cuando en el modulo de cuentas por cobrar no aparezca alguna factura, esta se ingresara de forma manual, mediante autorización del jefe del departamento.

5. Este ingreso de factura deberá de realizar mediante una requisición firmada de autorización.

7.15 Registro de los Abonos de Clientes

Los abonos realizados por el cliente deberán registrarse diariamente.

Procedimientos

1. Los abonos de los clientes deberán de registrarse diariamente con base a las remesas cotejándose el monto del recibo de ingreso con el valor remesado al banco.

2. El monto abonado quedará registrado en el histórico de cliente.

3. Los abonos se conciliaran con los ingresos reflejados en el estado de cuenta del banco.

4. En caso de encontrar diferencias conciliar cada cliente con el propósito de detectar la diferencia.

7.16 Descuentos a Clientes

Elaborar nota de crédito para los descuentos autorizados, ingresándolas posteriormente al módulo de cuentas por cobrar.

Procedimientos:

1. Para los descuentos de clientes autorizados por gerencia, se elaborara una nota de crédito a través del sistema, el cual asignara un número correlativo de comprobante.

2. Una vez elaborada se ingresará al módulo de cuentas por cobrar afectando la factura correspondiente y disminuyendo el saldo de cuenta del cliente.

3. Luego se ingresara contablemente disminuyendo el saldo de cuenta del cliente.

7.17 Devoluciones de Productos

Elaborar nota de devolución por mala aplicación registrada en el módulo de facturación o por producto dañado entregado.

Procedimientos:

1. Elaborar nota de devolución mediante requisición autorizada por gerencia.

2. Ingresar la nota de devolución al modulo de cuentas por cobrar, afectando la factura correspondiente y disminuyendo el saldo del cliente.

7.18 Devoluciones o Cambios de Facturas

Elaborar nota de abono en aquellos casos que se realice devolución, cambio de factura o liquidación de producto de consumidores finales locales o pago de facturas correspondientes de clientes del exterior.

Procedimientos:

1. Elaborar nota de abono mediante requisición autorizada por gerencia.

2. Ingresar al modulo de cuentas por cobrar las notas de abono disminuyendo el saldo de cuenta del cliente.

8. Políticas y Procedimientos para el Área de Inventarios

8.1 Política de Manejo de Inventarios

Deberá establecerse límites de inventario, para mantenerlos como stock.

Procedimientos:

1. Se deberá determinar cuales con los requerimientos de inventarios necesarios que permitan la continuidad de las operaciones de la empresa.

2. El sistema deberá monitorear estos parámetros de stock, enviando una alerta al momento de llegar a esa cantidad

3. Una vez el sistema indica que se ha llegado al límite mínimo de inventario, el auxiliar de inventarios deberá preparar en el sistema la requisición de materiales o materias primas.

8.2 Requisiciones de Materias Primas y Materiales de Empaque

Toda requisición de materias primas y materiales de empaque, deberá ser elaborado en el sistema, tomando en cuenta los stocks de inventarios preestablecidos y el número de orden de producción.

Procedimientos:

1. El departamento de inventarios deberá elaborar una requisición por cada necesidad de materia prima, la cual deberá considerar el stock de inventarios establecidos.

2. La requisición deberá ser autorizada por el Jefe del Departamento de Inventarios, posteriormente se enviará al departamento de compras para procesar su debida orden de compras, todas estas autorizaciones deberán realizarse en el sistema de información.

3. El sistema deberá contener la opción de requisición igual a orden de producción y sus respectivas requisiciones.

8.3 Emisión de Comprobante de Ingreso a Bodega

Emitir un comprobante de ingreso de materia prima a bodega por cada recepción de mercadería.

Procedimientos.

1. Verificar físicamente, contra Orden de Compra y Comprobante de Crédito Fiscal, las cantidades recibidas

2. Al llamar la Orden de Compra, en el sistema, estará deberá mostrar un columna en la que el personal de bodega pueda digitar las cantidades que se están recibiendo en ese momento

3. Una vez ingresado en el sistemas las cantidades, se deberá imprimir un recibo de Compras, en el que se indique que cantidades y de que ítems, de la orden de compra se ha recibido

4. El responsable de bodega deberá firmar y sellar este recibo para garantizar que la mercadería fue recibida.

5. Si al momento de contar la mercadería, el responsable de bodega, encuentra diferencias entre las cantidades recibidas y las cantidades ordenadas, no deberá recibir sin previa autorización.

6. Cotejar los ingresos de mercadería diarios.

7. Verificar los Ingresos de Materiales a Bodega, contra documentos y productos físicos.

8. Cotejar datos de los ingresos de mercadería así como sus costos, en cuanto al beneficio – costo.

9. Revisar las estadísticas de los incrementos y disminuciones en los costos de inventarios.

8.4 Ingreso de Mercaderías al Inventario

El departamento de bodega deberá enviar la documentación de recepción de mercadería al departamento de costos para que sea este el que afecte los inventarios.

Procedimientos:

1. Confrontar la Orden de Compra, el Comprobante de Crédito Fiscal, y el Recibo de Ingreso

2. Una vez verificada la documentación, le podrá dar ingreso a los inventarios a través del sistema, este contara con un proceso en el cual pasara la información capturada en el recibo de ingreso de mercaderías al modulo de inventarios.

8.5 Requisición de Materiales

Toda solicitud de materiales deberá realizarse a través de una orden de requisición de materiales.

Procedimientos:

1. Toda requisición de materiales deberá realizarse a través del sistema de información computarizado.

2. El sistema generará un hoja en la cual se detallaran los siguientes campos: Localización, fecha, numero de requisición, departamento solicitante, código del departamento, código del material o materia prima solicitado, descripción del producto, cantidad requerida

3. Una vez ingresada la solicitud de materiales esta será enviada vía e-mail al jefe de bodega para que autorice el despacho de dichos productos

4. Luego de autorizado el despacho, deberá elaborarse en el sistema la orden de entrega de materiales, la cual será realizada por el encargado de bodega incluyendo el día y la hora en que se esta haciendo entrega.

5. Ya elaborada la orden de despacho el material podrá ser entregado al responsable o al requeriente.

8.6 Movimientos de Inventarios por Entregas de Materiales y Materias primas

Los inventarios serán afectados en el momento en que se entregue o se reciba materiales o materias primas.

Procedimientos:

1. Al momento de recibir o entregar los materiales o materias primas, automáticamente el sistema deberá estar realizando las debidas afectaciones de inventario.

2. Para realizar estas afectaciones el encargado de inventarios, deberá ingresar su password al sistema para la actualización de información, con la cual todos los recibos de ingreso y las requisiciones pasaran a afectar los inventarios.

3. De todas las afectaciones de inventarios realizados quedaran pistas de auditoria que permitan rastrear quien ingreso o afecto los inventarios.

8.7 Movimientos de Inventarios por Ventas

Se afectaran los inventarios al momento que se realice una venta, o sea colocado un pedido.

Procedimientos:

1. Se deberá elaborara una orden de pedido, para cada venta que se efectúe, la cual será ingresada al sistema, e inmediatamente se afectaran los inventarios.

2. La orden de pedido será ingresada al sistema por el encargado de ventas, en el cual el software informara si hay existencias o no.

3. Una vez ingresada la orden de pedido el sistema enviara el requerimiento al departamento de crédito para que este lo autorice.

4. El sistema asignara que lote será entregado o despachado, de acuerdo a los parámetros establecidos.

8.8 Manejo de Obsolescencia

Se deberá controlar las fechas de vencimientos de los productos a través del sistema.

Procedimientos:

1. Una vez culminado el proceso de producción, los productos que forman parte del inventario de productos terminados, deberá ingresarse al sistema su fecha de vencimiento.

2. Clasificar los productos dentro del sistema de acuerdo a su fecha de elaboración y fecha de vencimiento.

3. Despachar los productos más antiguos, cuando se realice una venta.

4. El sistema deberá emitir un mensaje de alerta que indique al usuario, que mercadería esta mas pronta a vencer.

5. Si no se pudieran despachar en ese momento, el sistema enviara un reporte de producto vencido, el cual será entregado al Departamento de Auditoria, para que autorice la baja del Inventario.

8.9 Manejo de Inventario de Productos en Proceso

Deberá controlarse a través de los sistemas los inventarios de productos en proceso.

Procedimientos:

1. Toda orden de producción esta ingresada al sistema y es este el que determinara los costos de producción y el estado de cada producto.

2. Si existen productos que a un no han sido terminados y están el fase de productos en proceso, estos deberán controlarse a través del sistemas, detallando en que estado y lugar de cada uno de estos productos.

3. Deberán asignarse códigos a los productos en proceso, lo que permitirá un mejor control, estos productos solo podrán estar un tiempo prudencial en este inventario.

4. Con la orden de producción se estará monitoreando el avance de los productos y en que estado se encuentran.

5. Para pasar el inventario en proceso de un lugar físico a otro, deberán elaborarse actas de envío de materiales, las cuales detallaran cantidades, nombre del producto, nivel de proceso que lleva, y detallar porque esta siendo enviado a otro lugar físico, ya sea este para empaque o procedimientos manuales. Deberá haber un encargado que haga entrega de dichos productos.

8.10 Manejo de Productos Terminados

Se deberá llevar un control detallado de los productos terminados y su locación, a través de la asignación de un código de ingreso al sistema.

Procedimientos:

1. Una vez concluido la fase de producción, los productos deberán ser clasificados de acuerdo a su descripción, para se enviados a las diferentes bodegas.

2. Se deberá elaborar una hoja de envío de productos de producción a bodega, en el que se detallara cantidades, y descripción de productos enviados, tipo de presentación, fecha de vencimiento, lotes de producción, etc.

3. Los productos se almacenan por lotes, los cuales deberán incluir su fecha de vencimiento, lotes, fechas de producción, etc.

4. El sistema asignara a cada producto un código de bodega.

8.11 Inventarios Ociosos

Los inventarios ociosos por exceso o por desuso deben controlarse separadamente y activarse las gestiones para su eliminación, para lo cual el sistema deberá emitir un informe de estos.

Procedimientos:

1. El sistema deberá emitir un informe de las fechas de vencimiento de la materia prima, productos en proceso, y producto terminado.

2. Si existen materiales ociosos, el sistema no permitirá que se compren o adquieran materiales de iguales características, emitiendo un mensaje de alerta al momento de emitir una requisición de dichos materiales.

3. Si el inventario ocioso se convierte en obsoleto, el Jefe de Bodega deberá autorizar el traslado de los materiales a través del sistema, para su debida eliminación

4. El sistema emitirá una estadística mensual en la que indique cantidades y tipos de materiales que hayan sido enviados a inventarios obsoletos.

8.12 Manejo de Inventario de Muestras Médicas

Se llevara por separado un control sobre los inventarios de muestras medicas.

Procedimientos:

1. Las ordenes de procesos destinadas para muestras medicas, deberán identificarse, anteponiéndoles las iniciales MM, las que indicaran que ese inventario es para regalías

2. Una vez terminada la orden de producción los inventarios pasaran a ser clasificados dentro de la bodega como Muestras Medicas, los cuales serán afectados cada vez que el Gerente de Ventas, autorice la entrega de regalías a los clientes

3. Se llevara un control en el sistema de quienes tienen acceso a las muestras médicas y el número de estas.

4. Para la entrega de Muestras Medicas, se deberá elaborar en el sistema una orden de requisición la cual, estará autorizada por el Gerente de Ventas, y el encargado de bodega, los cuales al hacerse efectivas afectaran directamente el inventario.

CAPITULO IV
CONCLUCIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

El conocimiento del profesional de la contaduría pública que tiene de los sistemas informáticos es limitado, ya que por lo general el contador tiene acceso, solo a nivel de usuario, lo cual lo limita a poder ejecutar a través de herramientas de control informáticos que salvaguarden la información con la que se preparan los estados financieros. Asimismo las actualizaciones del sistema por lo general se hacen a nivel externo; por lo tanto los planes de capacitación sin necesarios para una, mejor aplicación de las rutinas del sistema.

Las empresas farmacéuticas encuestadas se preocupan por la capacitación al personal, sin embargo dichas capacitaciones solamente incluyen contenido general del sistema y no se profundiza en las bondades de los sistemas; de tal forma este contribuye a disminuir el riesgo inherente den el procesamiento electrónico de datos.

Si bien es cierto las empresas se interesan por la implementación de controles internos informáticos, pero no reciben por parte del personal especializado en sistemas informáticos, la adecuada capacitación con respecto a estos, aun cuando los sistemas poseen módulos o herramientas básicas para poder ejecutar el control interno informático.

La falta de controles internos informáticos en los sistemas informáticos genera poca confiabilidad en algunos activos corrientes, ya que si bien se controlan los activos a través del control interno contable, no se tiene realmente asegurada la salvaguarda de la información cuantitativa de esta.

El profesional de la contaduría publica reconoce la importancia del control interno informático en el manejo de los activos, por lo tanto es necesario darle una guía que le permita identificar los puntos críticos de los activos corrientes y la forma de prevenir errores e irregularidades del sistema.

4.2 RECOMENDACIONES

Se debe hacer énfasis en la importancia de que el personal sea capacitado adecuadamente no solo en aspectos generales del sistema de información, sino también en todas las herramientas y aplicaciones del mismo, para un mejor aprovechamiento.

Elaborar manuales de procedimientos de control interno informático de acuerdo a la medida de los sistemas y necesidades de la organización con el fin de tener un instrumento para que la información procesada sea confiable y exacta.

Para una mejor ejecución del control interno se deberá capacitar al personal correspondiente sobre el uso adecuado de las herramientas de control con que se cuenta en el sistema como lo son los módulos de auditoria con el propósito de identificar y detectar los riesgos de manera oportuna logrando de esta manera que la información procesada en los sistemas carezca de sesgos o errores.

Establecer dentro de la empresa controles internos informáticos que aseguren la salvaguarda de la información generando confiabilidad suficiente de los reportes generados por el sistema.

Bibliografía

- Cano C. Miguel Antonio, Auditoria Forense en la investigación criminal del lavado de dinero y activos, 368 paginas.

- Control Interno Informático, Seguridad y Auditoria Informática, ISO, disponible en línea <http://auditi.com/index.htm>

- Lardent, Alberto, Sistemas de información para la gestión empresarial. Procedimientos, Seguridad y Auditoria. 2001, 443, páginas.

- Muñoz, Carlos, Auditoria de Sistemas Computacionales, Control Interno Informático

- Normas de Control Interno Informático disponible en <<hpt://www.mag.gob.sv/admin/publicaciones//>>

- Parra Iglesias, Enrique; Tecnologías de la información en el control de gestión, Editor Díaz de Santos, 1ª edición 1998

- Pinilla, Jose Dagoberto, Auditoria informatica, Aplicaciones en producción, Disponible en <http://www.auditi.com>

- Rojas Soriano, Guía para realizar investigaciones sociales. 8ª Edición 1985

- Sobrinos Sánchez, Planificación y Gestión de Sistemas de Información, Escuela Superior de Informática de Universidad de Castilla, 19 de Mayo de 1999 1er. Edición 66 Pág.

- Vásquez Orantes, José Luís, Recopilación de Leyes Tributarias, 18ª Edición 2005

Anexos

ANEXO 1 OBJETIVOS DE CONTROL SEGÚN COBIT (OBJETIVOS DE CONTROL RELATIVOS A LA TECNOLOGIA INFORMATICA)

PLANEACIÓN Y ORGANIZACIÓN

1.0 Definición de un Plan Estratégico de Tecnología de Información

1.1 Tecnología de Información como parte del Plan de la Organización a corto y largo plazo

1.2 Plan a largo plazo de Tecnología de Información

1.3 Plan a largo plazo de Tecnología de Información - Enfoque y Estructura

1.4 Cambios al Plan a largo plazo de Tecnología de Información

1.5 Planeación a corto plazo para la función de Servicios de Información

1.6 Evaluación de sistemas existentes

2.0 Definición de la Arquitectura de Información

2.1 Modelo de la Arquitectura de Información

2.2 Diccionario de Datos y Reglas de cinta de datos de la corporación

2.3 Esquema de Clasificación de Datos

2.4 Niveles de Seguridad

3.0 Determinación de la dirección tecnológica

3.1 Planeación de la Infraestructura Tecnológica

3.2 Monitoreo de Tendencias y Regulaciones Futuras

3.3 Contingencias en la Infraestructura Tecnológica

3.4 Planes de Adquisición de Hardware y Software

3.5 Estándares de Tecnología

4.0 Definición de la Organización y de las Relaciones de TI

4.1 Comité de planeación o dirección de la función de servicios de información

4.2 Ubicación de los servicios de información en la organización

4.3 Revisión de Logros Organizacionales

4.4 Funciones y Responsabilidades

4.5 Responsabilidad del aseguramiento de calidad

4.6 Responsabilidad de la seguridad lógica y física

4.7 Propiedad y Custodia

4.8 Propiedad de Datos y Sistemas

4.9 Supervisión

4.10 Segregación de Funciones

4.11 Asignación de Personal para Tecnología de Información

4.12 Descripción de Puestos para el Personal de la Función de TI

4.13 Personal clave de TI

4.14 Procedimientos para personal por contrato

4.15 Relaciones

5.0 Manejo de la Inversión en Tecnología de Información

5.1 Presupuesto Operativo Anual para la Función de Servicio de información

5.2 Monitoreo de Costo - Beneficio

5.3 Justificación de Costo - Beneficio

6.0 Comunicación de la dirección y aspiraciones de la gerencia

6.1 Ambiente positivo de control de la información

6.2 Responsabilidad de la Gerencia en cuanto a Políticas

6.3 Comunicación de las Políticas de la Organización

6.4 Recursos para la implementación de Políticas

6.5 Mantenimiento de Políticas

6.6 Cumplimiento de Políticas, Procedimientos y Estándares

6.7 Compromiso con la Calidad

6.8 Política sobre el Marco de Referencia para la Seguridad y el Control Interno

6.9 Derechos de propiedad intelectual

6.10 Políticas Específicas

6.11 Comunicación de Conciencia de Seguridad en TI

7.0 Administración de Recursos Humanos

7.1 Reclutamiento y Promoción de Personal

7.2 Personal Calificado

7.3 Entrenamiento de Personal

7.4 Entrenamiento Cruzado o Respaldo de Personal

7.5 Procedimientos de Acreditación de Personal

7.6 Evaluación de Desempeño de los Empleados

7.7 Cambios de Puesto y Despidos

8.0 Aseguramiento del Cumplimiento de Requerimientos Externos

8.1 Revisión de Requerimientos Externos

8.2 Prácticas y Procedimientos para el Cumplimiento de Requerimientos Externos

8.3 Cumplimiento de los Estándares de Seguridad y Ergonomía

8.4 Privacidad, Propiedad Intelectual y Flujo de Datos

8.5 Comercio Electrónico

8.6 Cumplimiento con Contratos de Seguros

9.0 Evaluación de Riesgos

9.1 Evaluación de Riesgos del Negocio

9.2 Enfoque de Evaluación de Riesgos

9.3 Identificación de Riesgos

9.4 Medición de Riesgos

9.5 Plan de Acción contra Riesgos

9.6 Aceptación de Riesgos

10.0 Administración de proyectos

10.1 Marco de Referencia para la Administración de Proyectos

10.2 Participación del Departamento Usuario en la Iniciación de Proyectos

10.3 Miembros y Responsabilidades del Equipo del Proyecto

10.4 Definición del Proyecto

10.5 Aprobación del Proyecto

10.6 Aprobación de las Fases del Proyecto

10.7 Plan Maestro del Proyecto

10.8 Plan de Aseguramiento de la Calidad de Sistemas

10.9 Planeación de Métodos de Aseguramiento

10.10 Administración Formal de Riesgos de Proyectos

10.11 Plan de Prueba

10.12 Plan de Entrenamiento

10.13 Plan de Revisión Post Implementación

11.0 Administración de Calidad

11.1 Plan General de Calidad

11.2 Enfoque de Aseguramiento de Calidad

11.3 Planeación del Aseguramiento de Calidad

11.4 Revisión de Aseguramiento de Calidad sobre el Cumplimiento de Estándares y Procedimientos de la Función de Servicios de Información

11.5 Metodología del Ciclo de Vida de Desarrollo de Sistemas

11.6 Metodología del Ciclo de Vida de Desarrollo de Sistemas para Cambios Mayores a la Tecnología Actual

11.7 Actualización de la Metodología del Ciclo de Vida de Desarrollo de Sistemas

11.8 Coordinación y Comunicación

11.9 Marco de Referencia de Adquisición y Mantenimiento para la Infraestructura de Tecnología

11.10 Relaciones con Terceras Partes como Implementadores

11.11 Estándares para la Documentación de

Programas

11.12 Estándares para Pruebas de Programas

11.13 Estándares para Pruebas de Sistemas

11.14 Pruebas Piloto/En Paralelo

11.15 Documentación de las Pruebas del Sistema

11.16 Evaluación del Aseguramiento de la Calidad sobre el Cumplimiento de Estándar de Desarrollo

11.17 Revisión del Aseguramiento de Calidad sobre el Logro de los Objetivos de la Función de Servicios de Información

11.18 Métricas de Calidad

11.19 Reportes de Revisiones de Aseguramiento de la Calidad

ADQUISICIÓN E IMPLEMENTACIÓN

1.0 Identificación de Soluciones

1.1 Definición de Requerimientos de Información

1.2 Formulación de Acciones Alternativas

1.3 Formulación de Estrategias de Adquisición.

1.4 Requerimientos de Servicios de Terceros

1.5 Estudio de Factibilidad Tecnológica

1.6 Estudio de Factibilidad Económica

1.7 Arquitectura de Información

1.8 Reporte de Análisis de Riesgos

1.9 Controles de Seguridad Económicos

1.10 Diseño de Pistas de Auditoría

1.11 Ergonomía

1.12 Selección de Software de Sistema

1.13 Control de Abastecimiento

1.14 Adquisición de Productos de Software

1.15 Mantenimiento de Software de Terceras Partes

1.16 Contratos de Programación de Aplicaciones

1.17 Aceptación de Instalaciones

1.18 Aceptación de Tecnología

2.0 Adquisición y Mantenimiento de Software de Aplicación

2.1 Métodos de Diseño

2.2 Cambios Significativos a Sistemas Actuales

2.3 Aprobación del Diseño

2.4 Definición y Documentación de Requerimientos de Archivos

2.5 Especificaciones de Programas

2.6 Diseño para la Recopilación de Datos Fuente

2.7 Definición y Documentación de Requerimientos de Entrada de Datos

2.8 Definición de Interfases

2.9 Interfases Usuario-Máquina

2.10 Definición y Documentación de Requerimientos de Procesamiento

2.11 Definición y Documentación de Requerimientos de Salida de Datos

2.12 Controlabilidad

2.13 Disponibilidad como Factor Clave de Diseño

2.14 Estipulación de Integridad de TI en programas de software de aplicaciones

2.15 Pruebas de Software de Aplicación

2.16 Materiales de Consulta y Soporte para Usuario

2.17 Reevaluación del Diseño del Sistema

3.0 Adquisición y Mantenimiento de Arquitectura de Tecnología

3.1 Evaluación de Nuevo Hardware y Software

3.2 Mantenimiento Preventivo para Hardware

3.3 Seguridad del Software del Sistema

3.4 Instalación del Software del Sistema

3.5 Mantenimiento del Software del Sistema

3.6 Controles para Cambios del Sofware del Sistema

4.0 Desarrollo y Mantenimiento de Procedimientos relacionados con Tecnología de Información

4.1 Futuros Requerimientos y Niveles de Servicios Operacionales

4.2 Manual de Procedimientos para Usuario

4.3 Manual de Operación

4.4 Material de Entrenamiento

5.0 Instalación y Acreditación de Sistemas

5.1 Entrenamiento

5.2 Adecuación del Desempeño del Software de Aplicación

5.3 Conversión

5.4 Pruebas de Cambios

5.5 Criterios y Desempeño de Pruebas en Paralelo/Piloto

5.6 Prueba de Aceptación Final

5.7 Pruebas y Acreditación de Seguridad

5.8 Prueba Operacional

5.9 Promoción a Producción 5.10 Evaluación de la Satisfacción de los Requerimientos del Usuario

5.11Revisión Gerencial Post - Implementación

6.0 Administración de Cambios

6.1 Inicio y Control de Requisiciones de Cambio

6.2 Evaluación del Impacto

6.3 Control de Cambios

6.4 Documentación y Procedimientos

6.5 Mantenimiento Autorizado

6.6 Política de Liberación de Software

6.7 Distribución de Software

ENTREGA DE SERVICIOS Y SOPORTE

1.0 Definición de Niveles de Servicio

1.1 Marco de Referencia para el Convenio de Nivel de Servicio

1.2 Aspectos sobre los Acuerdos de Nivel de Servicio

1.3 Procedimientos de Ejecución

1.4 Monitoreo y Reporte

1.5 Revisión de Convenios y Contratos de Nivel de Servicio

1.6 Elementos sujetos a Cargo

1.7 Programa de Mejoramiento del Servicio

2.0 Administración de Servicios prestados por

Terceros

2.1 Interfases con Proveedores

2.2 Relaciones de Dueños

2.3 Contratos con Terceros

2.4 Calificaciones de terceros

2.5 Contratos con Outsourcing

2.6 Continuidad de Servicios

2.7 Relaciones de Seguridad

2.8 Monitoreo

3.0 Administración de Desempeño y Capacidad

3.1 Requerimientos de Disponibilidad y Desempeño
3.2 Plan de Disponibilidad

3.3 Monitoreo y Reporte

3.4 Herramientas de Modelado

3.5 Manejo de Desempeño Proactivo

3.6 Pronóstico de Carga de Trabajo

3.7 Administración de Capacidad de Recursos

3.8 Disponibilidad de Recursos

3.9 Calendarización de recursos

4.0 Aseguramiento de Servicio Continuo

4.1 Marco de Referencia de Continuidad de Tecnología de Información

4.2 Estrategia y Filosofía de Continuidad de Tecnología de Información

4.3 Contenido del Plan de Continuidad de Tecnología de Información

4.4 Minimización de requerimientos de Continuidad de Tecnología de Información

4.5 Mantenimiento del Plan de Continuidad de Tecnología de Información

4.6 Pruebas del Plan de Continuidad de Tecnología de Información

4.7 Capacitación sobre el Plan de Continuidad de Tecnología de Información

4.8 Distribución del Plan de Continuidad de Tecnología de Información

4.9 Procedimientos de Respaldo de Procesamiento para Departamentos Usuarios

4.10 Recursos críticos de Tecnología de Información

4.11 Centro de Cómputo y Hardware de respaldo

4.12 Procedimientos de Refinamiento del Plan de Continuidad de TI

5.0 Garantizar la Seguridad de Sistemas

5.1 Administrar Medidas de Seguridad

5.2 Identificación, Autenticación y Acceso

5.3 Seguridad de Acceso a Datos en Línea

5.4 Administración de Cuentas de Usuario

5.5 Revisión Gerencial de Cuentas de Usuario

5.6 Control de Usuarios sobre Cuentas de Usuario

5.7 Vigilancia de Seguridad

5.8 Clasificación de Datos

5.9 Administración Centralizada de Identificación y Derechos de Acceso

5.10 Reportes de Violación y de Actividades de Seguridad

5.11 Manejo de Incidentes

5.12 Re-acreditación

5.13 Confianza en Contrapartes

5.14 Autorización de Transacciones

5.15 No Rechazo

5.16 Sendero Seguro

5.17 Protección de funciones de seguridad

5.18 Administración de Llave Criptográfica

5.19 Prevención, Detección y Corrección de Software "Malicioso"

5.20 Arquitecturas de FireWalls y conexión a redes públicas

5.21 Protección de Valores Electrónicos

6.0 Identificación y Asignación de Costos

6.1 Elementos Sujetos a Cargo

6.2 Procedimientos de Costeo

6.3 Procedimientos de Cargo y Facturación a Usuarios

7.0 Educación y Entrenamiento de Usuarios

7.1 Identificación de Necesidades de Entrenamiento

7.2 Organización de Entrenamiento

7.3 Entrenamiento sobre Principios y Conciencia de Seguridad

8.0 Apoyo y Asistencia a los Clientes de Tecnología de Información

8.1 Buró de Ayuda

8.2 Registro de Preguntas del Usuario

8.3 Escalamiento de Preguntas del Cliente

8.4 Monitoreo de Atención a Clientes

8.5 Análisis y Reporte de Tendencias

9.0 Administración de la Configuración

9.1 Registro de la Configuración

9.2 Base de la Configuración

9.3 Registro de Estatus

9.4 Control de la Configuración

9.5 Software no Autorizado

9.6 Almacenamiento de Software

10.0 Administración de Problemas e Incidentes

10.1 Sistema de Administración de Problemas

10.2 Escalamiento de Problemas

10.3 Seguimiento de Problemas y Pistas de Auditoría

11.0 Administración de Datos

11.1 Procedimientos de Preparación de Datos

11.2 Procedimientos de Autorización de Documentos Fuente

11.3 Recopilación de Datos de Documentos Fuente

11.4 Manejo de Errores de Documentos Fuente

11.5 Retención de Documentos Fuente

11.6 Procedimientos de Autorización de Entrada de Datos

11.7 Chequeos de Exactitud, Suficiencia y Autorización

11.8 Manejo de Errores en la Entrada de Datos

11.9 Integridad de Procesamiento de Datos

11.10 Validación y Edición de Procesamiento de Datos

11.11 Manejo de Error en el Procesamiento de Datos

11.12 Manejo y Retención de Salida de Datos

11.13 Distribución de Salida de Datos

11.14 Balanceo y Conciliación de Datos de Salida

11.15 Revisión de Salida de Datos y Manejo de Errores

11.16 Provisiones de Seguridad para Reportes de Salida

11.17 Protección de Información Sensible durante transmisión y transporte

11.18 Protección de Información Crítica a

de los Servicios de TI

3.4 Evaluación Independiente de la Efectividad de proveedores externos de servicios

3.5 Aseguramiento Independiente del Cumplimiento de leyes y requerimientos regulatorios y compromisos contractuales

3.6 Aseguramiento Independiente del Cumplimiento de leyes y requerimientos regulatorios y compromisos contractuales

3.7 Competencia de la Función de Aseguramiento Independiente

3.8 Participación Proactiva de Auditoría

4.0 Proveer Auditoría Independiente

4.1 Estatutos de Auditoría

4.2 Independencia

4.3 Ética y Estándares Profesionales

4.4 Competencia

4.5 Planeación

4.6 Desempeño del Trabajo de Auditoría
-
4.7 Reporte

4.8 Actividades de Seguimiento
ser Desechada

11.19 Administración de Almacenamiento

11.20 Períodos de Retención y Términos de Almacenamiento

11.21 Sistema de Administración de la Librería de Medios

11.22 Responsabilidades de la Administración de la Librería de Medios

de proveedores externos de servicios

11.23 Respaldo y Restauración

11.24 Funciones de Respaldo

11.25 Almacenamiento de Respaldo

11.26 Archivo

11.27 Protección de Mensajes Sensitivos

11.28 Autenticación e Integridad

11.29 Integridad de Transacciones Electrónicas

11.30 Integridad Continua de Datos Almacenados

12.0 Administración de Instalaciones

12.1 Seguridad Física

12.2 Discreción de las Instalaciones de Tecnología de Información

12.3 Escolta de Visitantes

12.4 Salud y Seguridad del Personal

12.5 Protección contra Factores Ambientales

12.6 Suministro Ininterrumpido de Energía

13.0 Administración de Operaciones

13.1 Manual de procedimientos de Operación e Instrucciones

13.2 Documentación del Proceso de Inicio y de Otras Operaciones

13.3 Calendarización de Trabajos

13.4 Salidas de la Calendarización de Trabajos Estándar

13.5 Continuidad de Procesamiento

13.6 Bitácoras de Operación

13.7 Operaciones Remotas

MONITOREO

1.0 Monitoreo del Proceso

1.1 Recolección de Datos de Monitoreo

1.2 Evaluación de Desempeño

1.3 Evaluación de la Satisfacción de Clientes

1.4 Reportes Gerenciales

2.0 Evaluar lo adecuado del Control Interno

2.1 Monitoreo de Control Interno

2.2 Operación oportuna del Control Interno

2.3 Reporte sobre el Nivel de Control Interno

2.4 Seguridad de operación y aseguramiento de Control Interno

3.0 Obtención de Aseguramiento Independiente

3.1 Certificación / Acreditación Independiente de Control y Seguridad de los servicios de TI

3.2 Certificación / Acreditación Independiente de Control y Seguridad de proveedores externos de servicios

3.3 Evaluación Independiente de la Efectividad

ANEXO 2 LISTADO DE INDUSTRIAS FARMACEUTICAS UBICADAS EN EL DEPARTAMENTO DE SAN SALVADOR. (SEGÚN LA DIRECCION GENERAL DE ESTADISTICAS Y CENSOS)

Ministerio de Economía
Dirección General de Estadísticas y Censos (DIGESTYC)
Directorio de Establecimientos A Nivel Nacional por Departamentos
Departamentos SANSALVADOR,
todas las empresas

Correlativo	DEPTO	MUNIC	ESTABLECIMIENTO
1	6	17	BIOKEMICAL S.A. DE C.V.
2	6	9	CORPORACION BONIMA S.A DE C.V
3	6	18	DELMED S.A. DE C.V.
4	6	6	DROGERIA LA REFORMA
5	6	1	DROGUERIA RIALSA
6	6	1	DROGUERIA VIDES
7	6	18	EXPON S.A. DE C.V.
8	6	1	FARMINDUSTRIA, S.A. DE C.V.
9	6	1	FUENTE DE SALUD EL SALVADOR
10	6	1	INDUSTRIAS QUIMICAS S.A. DE C.V.
11	6	14	INFARMA S.A. DE C.V.
12	6	1	LAB. Y DROGUERIA FARMACEUTICA UNIVERSALES
13	6	1	LABORATORIO BIOLOGICO DE EL SALVADOR S.A. DE C.V.
14	6	1	LABORATORIO DB S.A. DE C.V.
15	6	1	LABORATORIO FARDEL
16	6	1	LABORATORIO LAKINSACA S.A. DE C.V.
17	6	18	LABORATORIO LOPEZ S.A. DE C.V.
18	6	1	LABORATORIO RADON
19	6	1	LABORATORIO TECNOFORM S.A. DE .C.V.
20	6	1	LABORATORIO TERAPEUTICO MEDICNALES
21	6	1	LABORATORIO WOHLER, S.A. DE C.V.
22	6	1	LABORATORIO Y DROGUERIA BILLCA S.A. DE C.V.
23	6	1	LABORATORIO Y DROGUERIA LAINEZ, S.A DE C.V.
24	6	18	LABORATORIO Y DROGUERIA QUICASA DE C.V.
25	6	4	LABORATORIO Y DROGUERIA REAL
26	6	1	LABORATORIO Y DROGUERIA UNIVERSAL S.A. DE C.V.
27	6	1	LABORATORIOS ARSAL S.A. DE C.V.
28	6	1	LABORATORIOS FARMA, S.A DE C.V.
29	6	1	LABORATORIOS FARMACEUTICOS INTERMEDICAL FARMACORP

30	6	1	LABORATORIOS FERSON
31	6	1	LABORATORIOS INTERMEDICAL
32	6	18	LABORATORIOS LAFAR S.A. DE C.V.
33	6	1	LABORATORIOS LAKINSACA S.A. DE C.V.
34	6	1	LABORATORIOS MEDIKEM S.A. DE C.V.
35	6	1	LABORATORIOS PAILL S.A. DE C.V.
36	6	18	LABORATORIOS PHARMASIL S.A.DE C.V.
37	6	1	LABORATORIOS PHARMATOR.
38	6	18	LABORATORIOS PHARMEDIC ACTIVA S.A. DE C.V.
39	6	1	LABORATORIOS RADON
40	6	1	LABORATORIOS S & M, S.A. DE C.V.
41	6	1	LABORATORIOS WOHLER S.A. DE C.V.
42	6	18	LOPEZ DAVIDSON S.A. DE C.V.
43	6	1	PHARMACIA & UPJOHN.
44	6	1	PROFARGA S.A. DE C.V.
45	6	18	QUIMICA INDUSTRIAL CENTROAMERICANA S.A. DE C.V.
46	6	1	SALUD INTEGRAL DE EL SALVADOR ,LTDA. DE C.V.
47	6	1	SOPERQUIMIA S.A. DE C.V.

ANEXO 3 ENCUESTA

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

Objetivo: Conocer la existencia de Controles Internos Informáticos, para el procesamiento de la información contable.

Propósito: La presente guía de preguntas, ha sido elaborada por estudiantes de la carrera de Licenciatura en Contaduría Publica, con el propósito de sustentar su trabajo de investigación relativo a uso de controles internos informáticos. De antemano le agradecemos su colaboración.

Indicaciones: Elija la respuesta que considere conveniente, seleccionando con una "X"

1 ¿ Cual es su grado Académico?

☐ Bachiller ☐ Lic. En Contaduría Publica

☐ Lic. En Admón. de Empresas ☐ Técnico en Contaduría Publica

☐ Otros Especifique: _____

2 ¿En que área de las siguientes posee experiencia?

☐ Contabilidad ☐ Auditoria Interna

☐ Auditoria de Sistemas ☐ Auditoria Interna y Externa

☐ Auditoria Externa ☐ Todas las anteriores

3 ¿ Cuántos años tiene usted de experiencia?

☐ 1-5 años ☐ 6-10 años

☐ 11-15 años ☐ Mas

4 ¿Posee su compañía su Sistema de Información Contable?

☐ SI ☐ NO

5 Si su respuesta es Sí, ¿Qué tipo de software como sistema de información utiliza?

☐ Adquirido en el mercado como paquete comercial ☐ Desarrollado Internamente

☐ Contrató servicios de programación ☐ Otro _____

6 ¿Qué rango es el costo de adquisición aproximado del tipo de software que utiliza?

☐ Menos de $ 1,000.00

☐ Mas de $ 1,000.00 y menos de $ 2,500.00

☐ Mas de $ 2,500.00 y menos de $ 4,000.00

☐ Mas de $ 4,000.00

7 ¿Qué rango es el costo de mantenimiento mensual del sistema?

☐ Menos de $ 1,000.00

☐ Mas de $ 1,000.00 y menos de $1,500.00

☐ Mas de $ 1,500.00

☐ No se tienen costos de mantenimiento

☐ Se tienen costos de mantenimiento, pero no se han calculado

8 ¿Si posee sistema de información computarizado, tiene éste un módulo de auditoria interna?

☐ SI ☐ NO

9 Si su respuesta anterior es SI, ¿ ejecuta los controles internos relativos a los activos?

☐ SI ☐ NO

10 ¿ A que tipo de activos corrientes le aplica la rutina de control interno ?

☐ Efectivo y equivalente ☐ Inventario

☐ Cuentas por cobrar ☐ otros

11 Si su sistema no emite los Controles Internos pertinentes ¿Se interesa la Gerencia o Auditoria Externa por la implantación de estos?

☐ SI ☐ NO

12 Si se interesan, ¿De que forman implementan estos controles?

☐ Capacitaciones ☐ Manuales

☐ Demostraciones ☐ Otros Especifique:

13 ¿Ha recibido usted, alguna capacitación para conocer el funcionamiento del Sistema Información que opera en su empresa?

☐ SI ☐ NO

14 ¿Quiénes proveen las capicitaciones?

☐ Personal Externo

☐ Personal Interno

☐ Ambos

15 Si su respuesta es si, ¿a través de qué medios los reciben?

☐ Demostraciones ☐ Seminarios

☐ Manuales de Usuarios ☐ Otros Especifique

16 ¿Considera usted que es importante la capacitación ante un sistema información a la medida?

☐ SI ☐ NO

17 ¿Con que frecuencia se le capacita en cuanto a los cambios que haya tenido el sistema?

☐ Mensual ☐ Trimestral

☐ Semestral ☐ Anual

☐ No la ha recibido

18 ¿ Participa usted de las modificaciones que le efectúan al Sistema de Información Computarizado?

☐ SI ☐ NO

19 Si, su respuesta es Si. ¿Existen controles de las personas que tienen acceso a modificar los Sistemas?

☐ SI ☐ NO

20 ¿Qué tipo de registros se llevan en el Sistema de Información Contable?

☐ Partidas Contables ☐ Detalle de costos

☐ Elab. Estados Financieros ☐ Detalle de Cuentas por cobrar

☐ Disponibilidad de Efectivo ☐ Todas las anteriores

☐ Manejo de Existencias

21 ¿Considera usted, que la información procesada en el Sistema de Información Contable de su compañía es confiable?

☐ SI ☐ NO

¿Por qué?

☐ Hay caídas de sistemas ☐ No hay capacitaciones

☐ No existe soporte técnico ☐ Complejidad del sistema

☐ Todas las anteriores

22 ¿El Sistema de Información Contable, que usted utiliza le permite generar controles al procesamiento electrónico de datos?

☐ SI ☐ NO

23 ¿Se supervisan constantemente los controles generados por el sistema contable?

☐ SI ☐ NO

¿Por qué? Explique:_____

24 ¿Qué tipos de controles le permite generar?

☐ Controles Preventivos ☐ Controles de Administración

☐ Controles Detectivos ☐ Control Contable

☐ Control Informático ☐ Ninguno

☐ Todos las anteriores

25 ¿ Qué áreas de Activos Corrientes maneja el Sistema de Información Contable?

☐ Efectivo y Equivalentes ☐ Cuentas por Cobrar

☐ Inventarios ☐ Todos los anteriores

☐ Documentos Por Cobrar

☐ Todos las anteriores

26 ¿ Qué tipo de reportes genera el Sistema de Información Contable dentro de los activos corrientes?

☐ Emisión de Cheques y/o arqueos

☐ Disponibilidad ☐ Desperdicios

☐ Generación de Costos ☐ 1-3 Controles

☐ Obsolescencia ☐ 4-7 Controles

☐ Muestras ☐ Todos los anteriores

☐ Antigüedad de Saldos

27 ¿ Tiene acceso a los controles que emite el sistema?

☐ SI ☐ NO

28 ¿De qué forma accesa usted a estos controles?

☐ Password ☐ Acceso Directo

29 ¿De qué manera puede disponer de la información generada por el Sistema de Información Contable?

☐ Impresa ☐ Medios Magnéticos

☐ Previo de Pantalla ☐ Otros Especifique _____

☐ Todos las anteriores

30 ¿Queda alguna evidencia de los controles que genera el sistema?

☐ SI ☐ NO

¿Cuáles?

_____

31 ¿Considera usted, que el control interno informático es importante para el manejo adecuado de los activos corrientes?

☐ SI ☐ NO

¿De qué manera?

_____

32 ¿Considera usted que los controles informáticos aplicados a los activos corrientes son confiables?

☐ SI ☐ NO

¿Por qué? _____

33 ¿Se realizan mejoras a los controles internos informáticos aplicados a los activos corrientes?

☐ SI ☐ NO

34 ¿Cree usted, que con un documento que le indique que Control Interno Informático puede aplicar a su compañía para el área de Activos Corrientes, es necesario?

☐ SI ☐ NO

¿Por qué?

_____

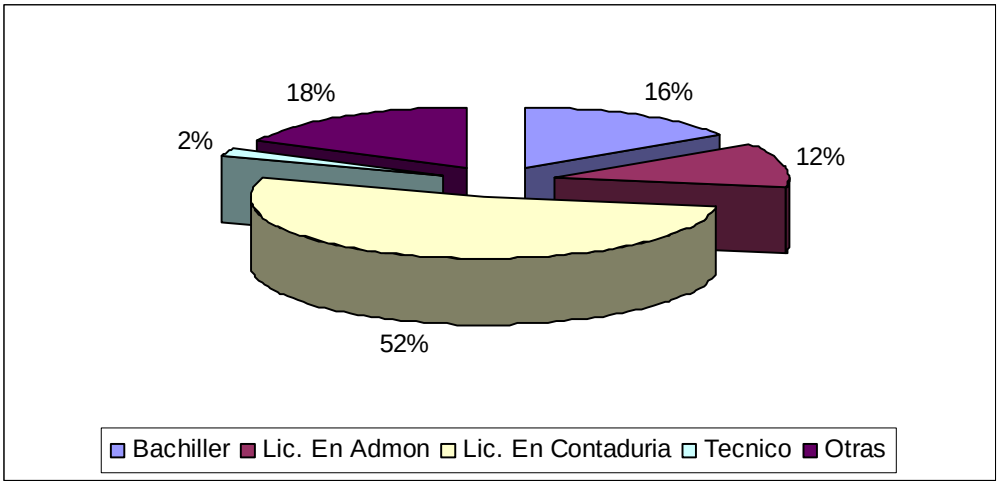
_____

ANEXO 4 TABULACION Y GRAFICOS

1. ¿Cual es su grado Académico?

Objetivo: Conocer el nivel académico de la persona encargada del manejo, proceso y recopilación de información.

Alternativas	Fa	Fr
Bachiller	8	15.69%
Licenciado en Administración de Empresas	6	11.76%
Licenciatura en Contaduría Pública	27	52.94%
Técnico en Contabilidad	1	1.96%
Otras	9	17.65%
Totales	**51**	**100.00%**

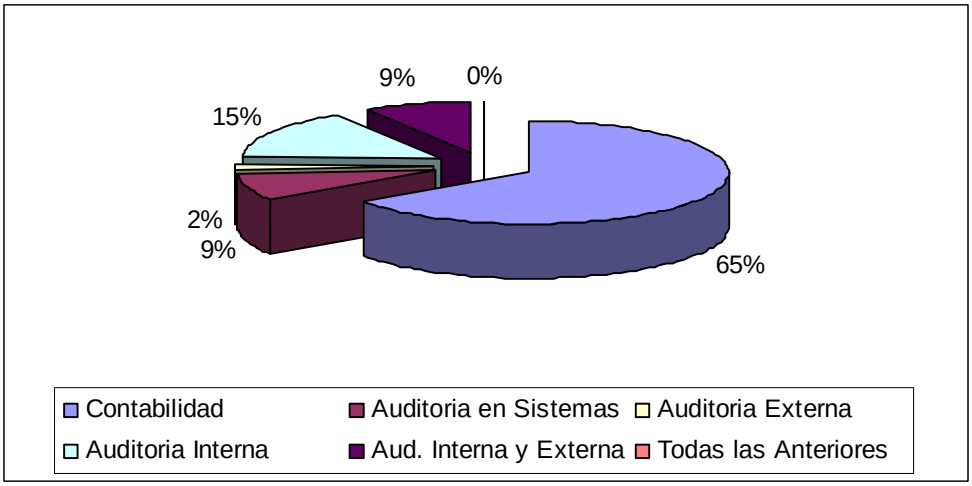


Análisis: Con base a los resultados obtenidos de nuestro trabajo de investigación de campo el 52.94 de las personas encuestadas son profesionales de la contaduría pública.

2. ¿En que área de las siguientes posee experiencia?

Objetivo: Determinar el grado de conocimiento del personal que utiliza los sistemas informáticos.

Alternativas	Fa	Fr
Contabilidad	38	65.52%
Auditoria en Sistemas	5	8.62%
Auditoria Externa	1	1.72%
Auditoria Interna	9	15.52%
Auditoria Interna y Externa	5	8.62%
Todas las Anteriores	0	0.00%
Totales	**58**	**100.00%**

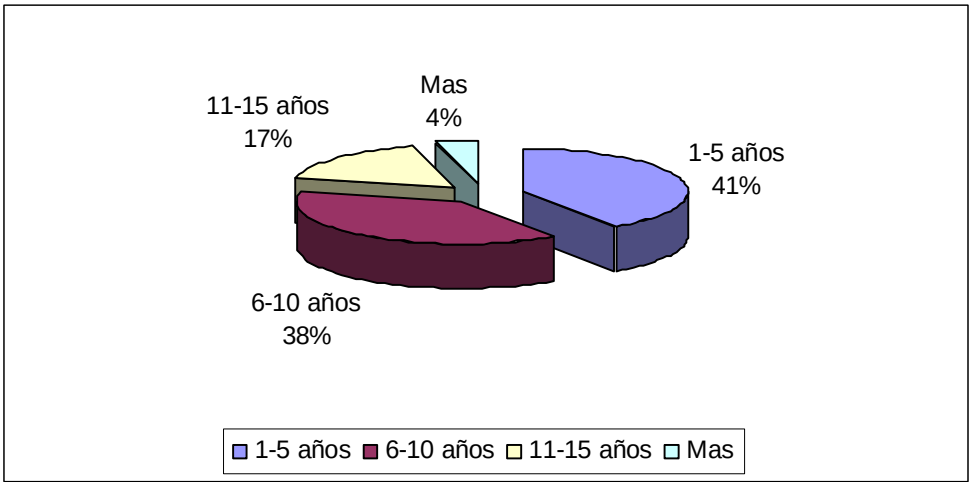


Análisis: Del total de las personas encuestadas el 65.52%, poseen experiencia en el área de contabilidad.

3. ¿Cuántos años tiene usted de experiencia?

Objetivo: Investigar el tiempo que tiene el personal de la compañía en laborar en el procesamiento de información contable.

Alternativas	Fa	Fr
1-5 años	19	40.43%
6-10 años	18	38.30%
11-15 años	8	17.02%
Mas	2	4.26%
Totales	**47**	**100.00%**

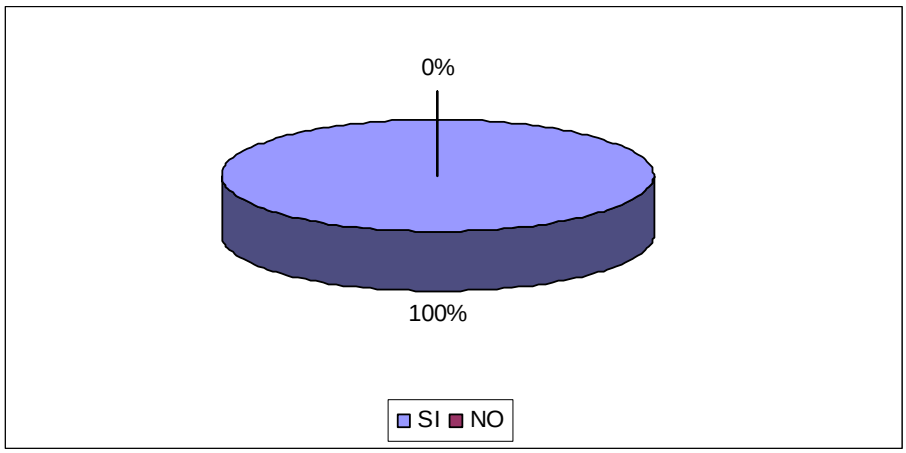


Análisis: El 40.43% de la población encuestada posee experiencia en el área de contabilidad entre un rango de uno a cinco años.

4. ¿Posee su compañía su Sistema de Información Contable?

Objetivo: Determinar si la compañía posee un sistema contable computarizado o manual.

Alternativas	Fa	Fr
SI	47	100%
NO	0	0%
Totales	**47**	**100%**

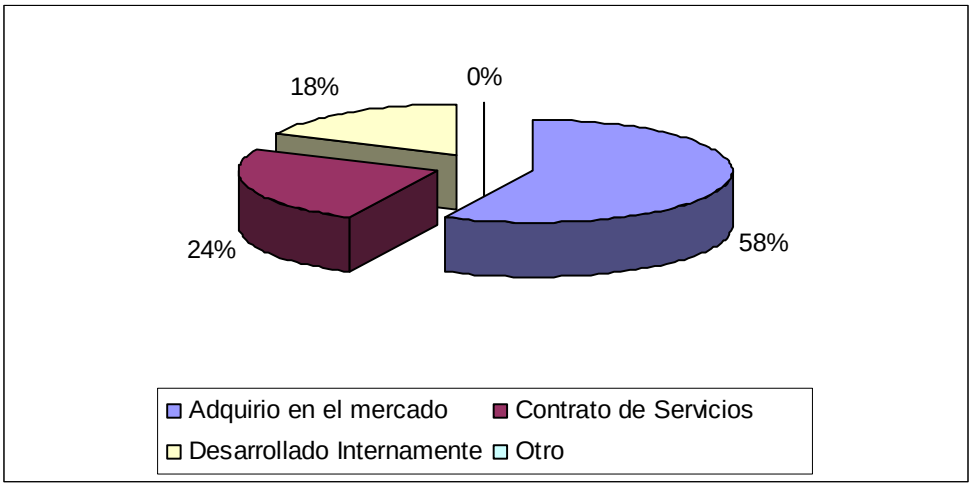


Análisis: El 100% de los laboratorios farmacéuticos que existen en nuestro país poseen un sistema de información contable para el registro de sus operaciones.

5. Si su respuesta es Sí, ¿Qué tipo de software como sistema de información utiliza?

Objetivo: Determinar la forma en que la compañía adquirió el software.

Alternativas	Fa	Fr
Adquirido en el mercado	28	57.14%
Contrato de Servicios	12	24.49%
Desarrollado Internamente	9	18.37%
Otro	0	0.00%
Totales	**49**	**100.00%**

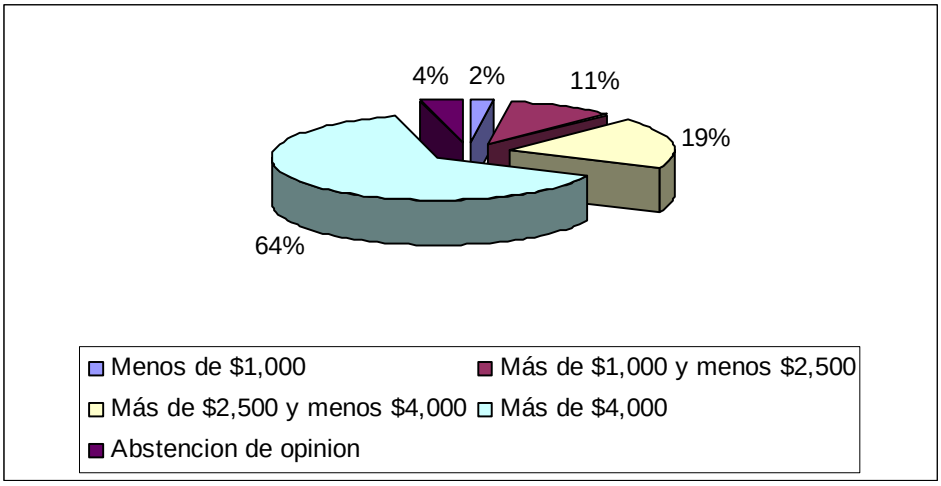


Análisis: Del 100% de los laboratorios el 57.14% de los encuestados confirmo que el software utilizado actualmente ha sido adquirido en el mercado nacional.

6. ¿Qué rango es el costo de adquisición aproximado del tipo de software que utiliza? (No se solicita presentar facturas ni consultar registros)

Objetivo: Determinar el costo estimado del software.

Alternativas	Fa	Fr
Menos de $1,000	1	2.13%
Más de $1,000 y menos $2,500	5	10.64%
Más de $2,500 y menos $4,000	9	19.15%
Más de $4,000	30	63.83%
Abstención de opinión	2	4.26%
Totales	**47**	**95.74%**

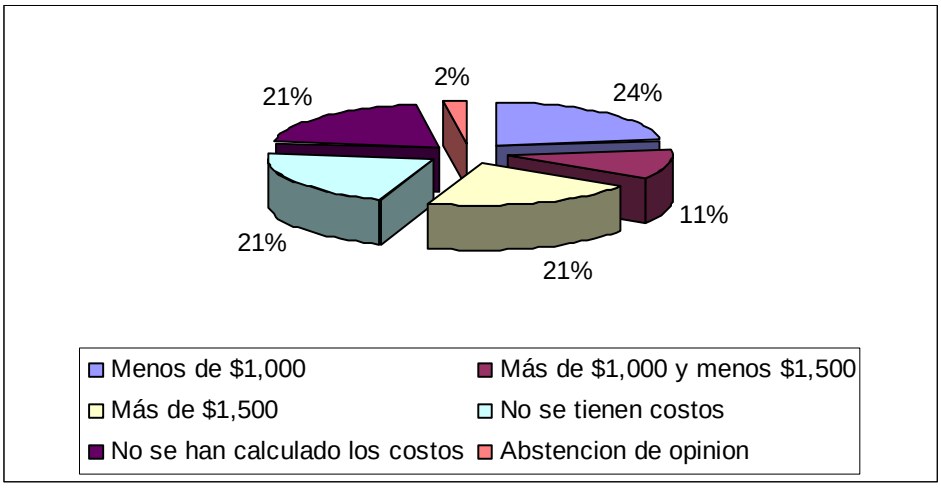


Análisis: El software adquirido por las compañías farmacéuticas ha tenido un costo aproximado mayor de $ 4,000 ya que el 63.83% de la población se encuentra considerada dentro de este rango.

7. ¿Qué rango es el costo de mantenimiento mensual del sistema?

Objetivo: Determinar el costo de mantenimiento mensual.

Alternativas	Fa	Fr
Menos de $1,000	11	23.40%
Más de $1,000 y menos $1,500	5	10.64%
Más de $1,500	10	21.28%
No se tienen costos	10	21.28%
No se han calculado los costos	10	21.28%
Abstención de opinión	1	2.13%
Totales	**47**	**100.00%**

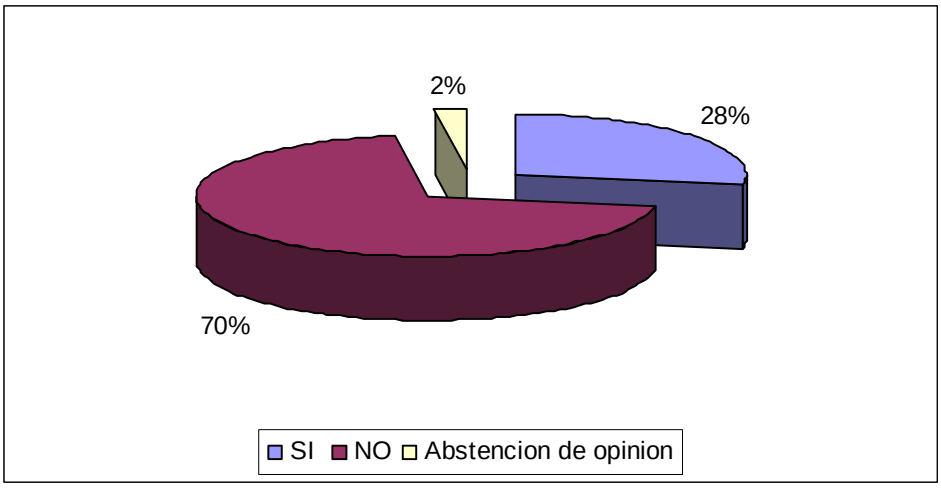


Análisis: En la mayor parte de los laboratorios se tiene estimado en su presupuesto anual un costo por mantenimiento de sistemas el cual es menor a $ 1,000 ya que del total de la población el 23.40% se encuentra en este rango.

8. ¿Si posee sistema de información computarizado, tiene éste un modulo de auditoria interna?

Objetivo: Identificar si en las compañías se tiene un departamento de auditoria interna que supervise y revise periódicamente las operaciones procesadas en los sistemas.

Alternativas	Fa	Fr
SI	13	27.66%
NO	33	70.21%
Abstención de opinión	1	2.13%
Totales	**47**	**97.87%**

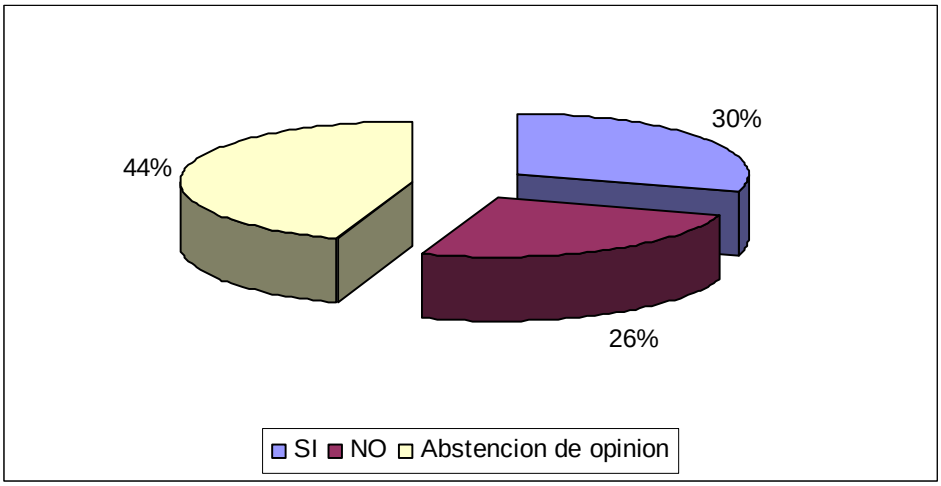


Análisis: En su mayoría, los encuestados respondió que no cuentan con un modulo de auditoria externa, este corresponde el 70.21% y el porcentaje restante si cuenta con controles internos.

9. Si su respuesta anterior es SI, ¿ejecuta los controles internos relativos a los activos?

Objetivo: Determinar si se poseen procedimientos para la evaluación de los saldos razonables reflejados en los estados financieros de los activos de la compañía.

Alternativas	Fa	Fr
SI	14	30%
NO	12	26%
Abstención de opinión	21	44%
Totales	**47**	**100%**

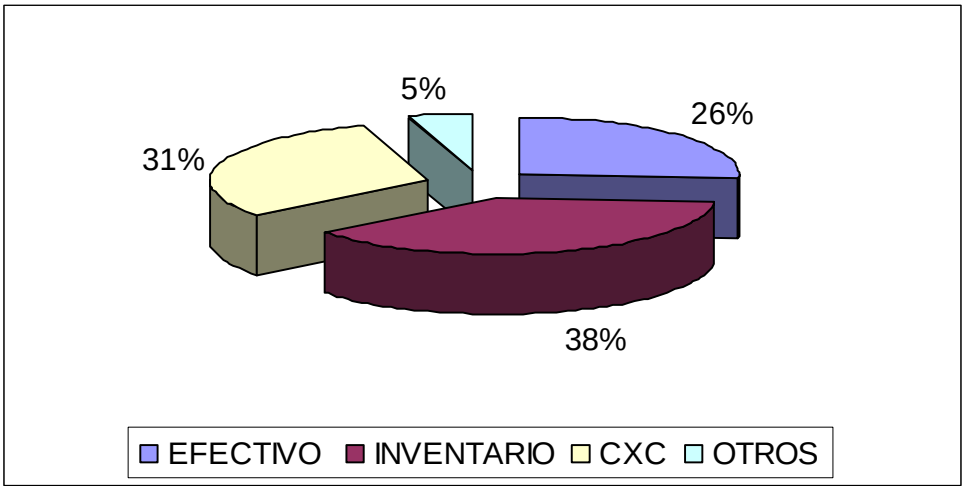


Análisis: el 45% de los encuestados no respondieron debido a que no se cuentan con controles internos.

10. ¿A que tipo de activos corrientes le aplica la rutina de control interno?

Objetivo: Conocer la existencia de controles y procedimientos para la evaluación de los activos corrientes de la compañía.

Alternativas	Fa	Fr
EFECTIVO	23	26.44%
INVENTARIO	33	37.93%
CXC	27	31.03%
OTROS	4	4.60%
Totales	**87**	**100.00%**

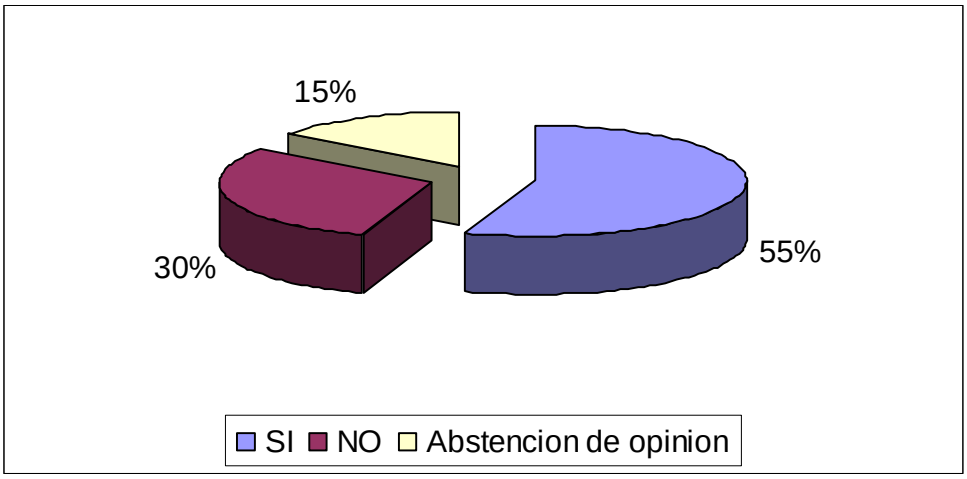


Análisis: según lo investigado el 37.93% de los encuestados respondió que los controles aplicados lo hacen mas al modulo de inventario.

11. Si su sistema no emite los Controles Internos pertinentes ¿Se interesa la Gerencia o Auditoria Externa por la implantación de estos?

Objetivo: Determinar si gerencia o auditoria externa implementa controles o procedimientos para la evaluación de activos corrientes de forma periódica.

Alternativas	Fa	Fr
SI	26	55.32%
NO	14	29.79%
Abstención de opinión	7	14.89%
Totales	**47**	**100.00%**

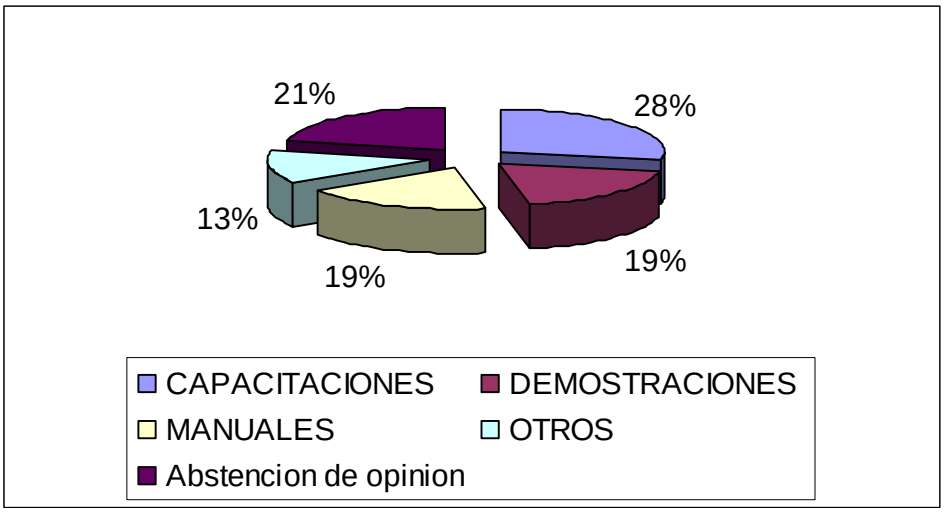


Análisis: en la mayoría la gerencia se interesa por la implementación de controles cuando no se cuentan con ellos, ya que fue del 55.32%.

12 Si se interesan, ¿De que forman implementan estos controles?

Objetivo: Conocer la forma en que se aplican los controles o procedimientos en el área de activos corrientes.

Alternativas	Fa	Fr
CAPACITACIONES	13	27.66%
DEMOSTRACIONES	9	19.15%
MANUALES	9	19.15%
OTROS	6	12.77%
ABSTENCION DE OPINION	10	21.28%
Totales	**47**	**100.00%**

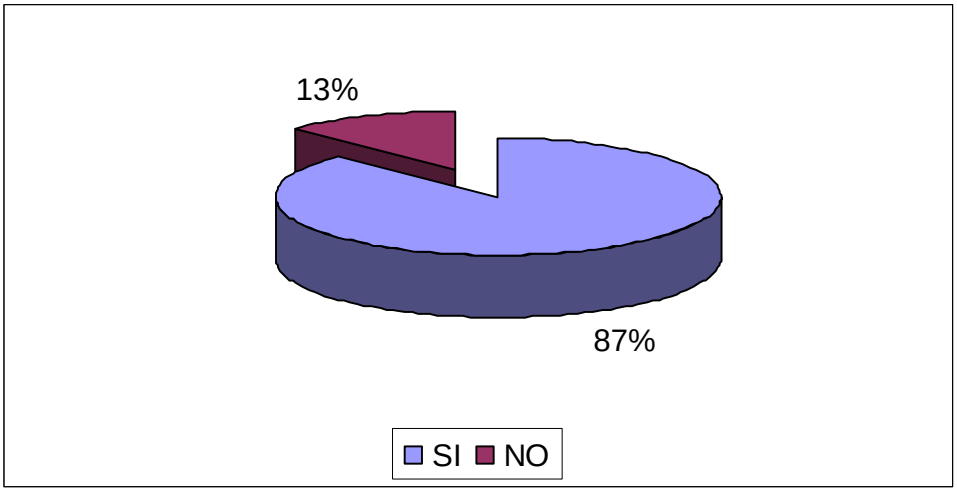


Análisis: la gerencia da a conocer los controles en su mayoría a través de capacitaciones con un 27.66%, demostraciones con 19.15%, manuales con 19.15%.

13. ¿Ha recibido usted, alguna capacitación para conocer el funcionamiento del Sistema Información que opera en su empresa?

Objetivo: Investigar si el personal involucrado para el procesamiento de la información en los sistemas automatizados se encuentra debidamente capacitado.

Alternativas	Fa	Fr
SI	41	87.23%
NO	6	12.77%
Totales	**47**	**100.00%**

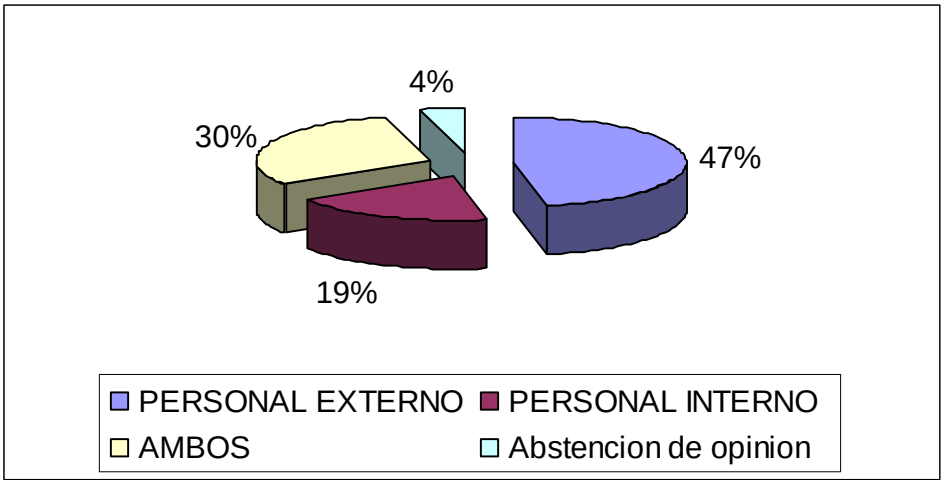


Análisis: un 87.23% de los encuestados han recibido capacitación del funcionamiento del sistema de información bajo el cual opera la empresa.

14. ¿Quiénes proveen las capacitaciones?

Objetivo: Investigar si el personal que provee las capacitaciones es altamente capacitado.

Alternativas	Fa	Fr
PERSONAL EXTERNO	22	46.81%
PERSONAL INTERNO	9	19.15%
AMBOS	14	29.79%
Abstención de opinión	2	4.26%
Totales	**47**	**100.00%**

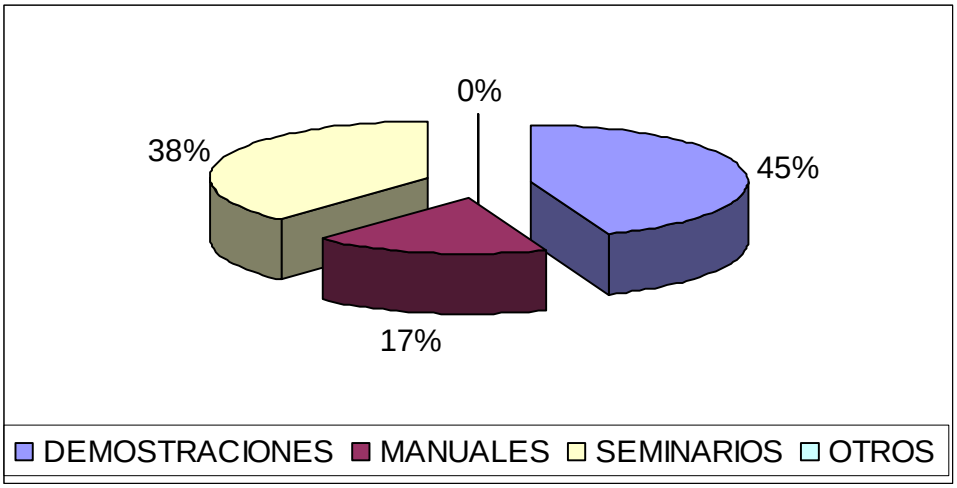


Análisis: De la mayoría de los encuestados un 46.81% recibe capacitaciones a través de personal externo.

15. Si su respuesta es si, ¿a través de qué medios los reciben?

Objetivo: Conocer que medios utiliza la compañía para la capacitación del personal involucrado en el procesamiento de la información en los sistemas informáticos.

Alternativas	Fa	Fr
DEMOSTRACIONES	23	44.23%
MANUALES	9	17.31%
SEMINARIOS	20	38.46%
OTROS	0	0.00%
Totales	**52**	**100.00%**

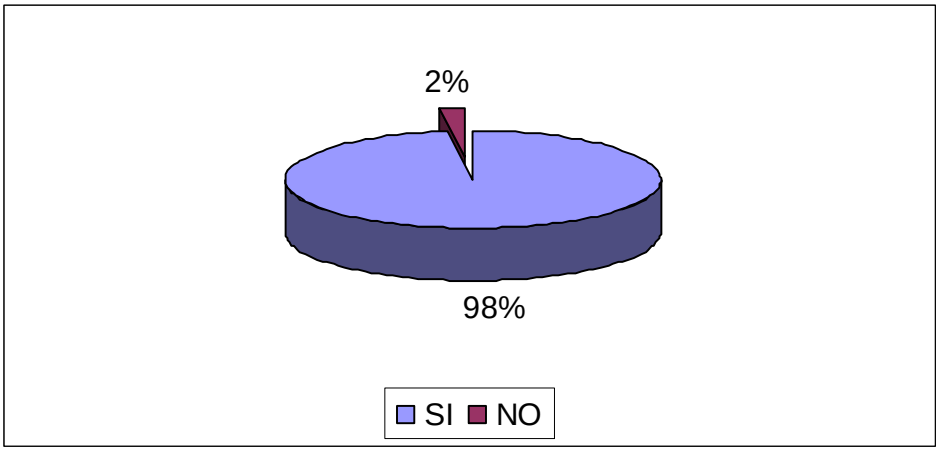


Análisis: buen porcentaje de los encuestados un 44.23% se reciben a través de demostraciones, un 38.46% a través de seminarios.

16. ¿Considera usted que es importante la capacitación ante un sistema información a la medida?

Objetivo: Conocer el grado de importancia que le da el personal, a la necesidad de estar debidamente informado del manejo del sistema de información automatizado que utiliza.

Alternativas	Fa	Fr
SI	46	97.87%
NO	1	2.13%
Totales	**47**	**100.00%**

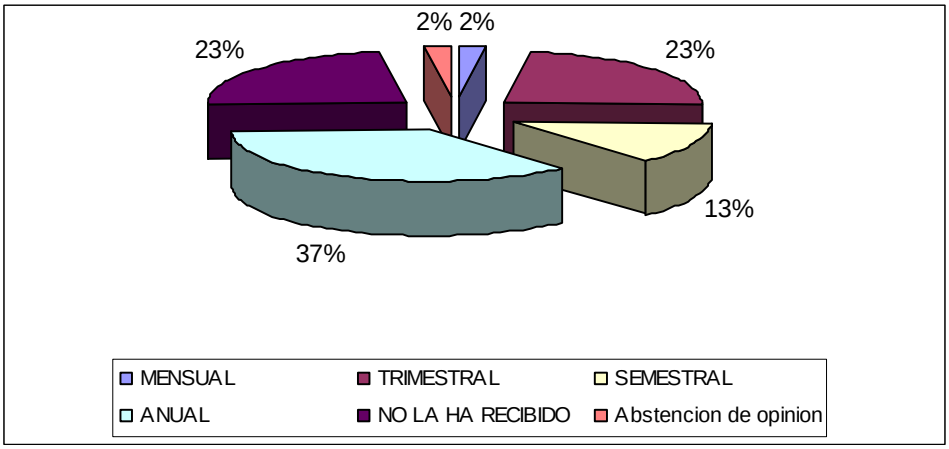


Análisis: casi el 100% de los encuestados respondió que si es importante conocer del funcionamiento del sistema a la medida.

17. ¿Con que frecuencia se le capacita en cuanto a los cambios que haya tenido el sistema?

Objetivo: Determinar si el personal es capacitado acorde a las necesidades de la compañía.

Alternativas	Fa	Fr
MENSUAL	1	2.13%
TRIMESTRAL	11	23.40%
SEMESTRAL	6	12.77%
ANUAL	17	36.17%
NO LA HA RECIBIDO	11	23.40%
Abstención de opinión	1	2.13%
Totales	**47**	**100.00%**

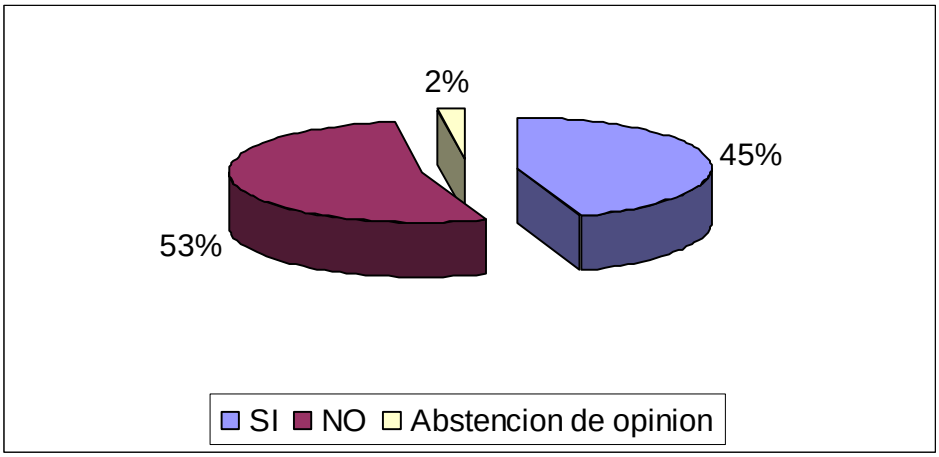


Análisis: Con base a los resultados obtenidos verificamos que el 36.17% de personal es capacitado una vez al año, esto se debe a que no se realizan periódicamente cambios o mejoras a los sistemas continuas.

18. ¿Participa usted de las modificaciones que le efectúan al Sistema de Información Computarizado?

Objetivo: Verificar que las actualizaciones realizadas al sistema son efectuadas únicamente por el personal que tiene autorización para este proceso.

Alternativas	Fa	Fr
SI	21	44.68%
NO	25	53.19%
Abstención de opinión	1	2.13%
Totales	**47**	**100.00%**

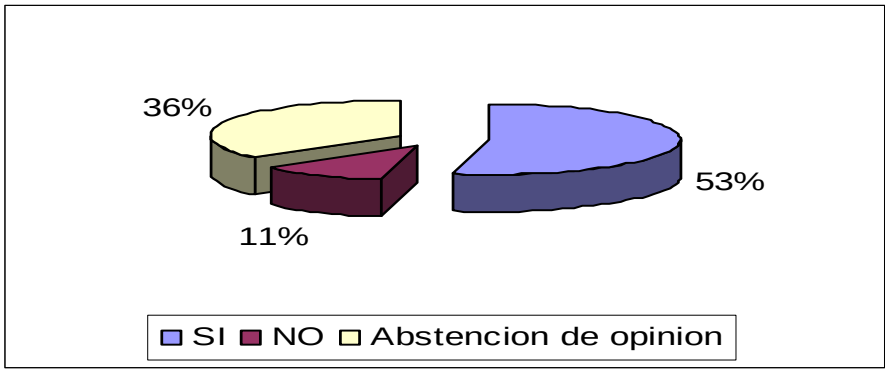


Análisis: El 53.09% de la personas que utilizan los sistemas no participan de los cambios o mejoras realizadas a los mismos, esto debido a que en su mayoría estas son realizadas por quienes proporcionaron el software.

19. Si, su respuesta es Si. ¿Existen controles de las personas que tienen acceso a modificar los Sistemas?

Objetivo: Determinar si se manejan registros de las actualizaciones o modificaciones efectuadas al los sistemas informáticos.

Alternativas	Fa	Fr
SI	25	53.19%
NO	5	10.64%
Abstención de opinión	17	36.17%
Totales	**47**	**100.00%**

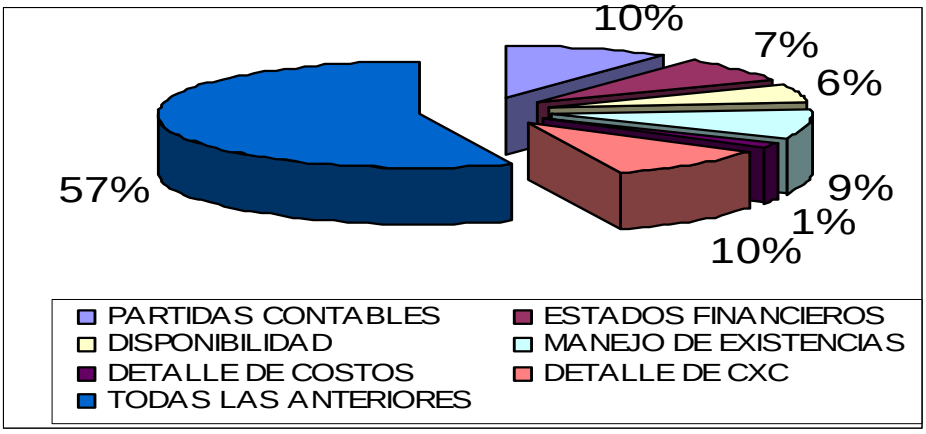


Análisis: Del total de los encuestados el 53% confirmaron que se tienen controles encaminados a la salvaguarda de los sistemas debido a que los cambios realizados en estos son por personal autorizado por la administración, dejando evidencia de quienes realizaron dichas modificaciones.

20. ¿Qué tipo de registros se llevan en el Sistema de Información Contable?

Objetivo: Conocer que tipos de información es procesada en los sistemas computarizados.

Alternativas	Fa	Fr
PARTIDAS CONTABLES	7	10.29%
ESTADOS FINANCIEROS	5	7.35%
DISPONIBILIDAD	4	5.88%
MANEJO DE EXISTENCIAS	6	8.82%
DETALLE DE COSTOS	1	1.47%
DETALLE DE CXC	7	10.29%
TODAS LAS ANTERIORES	38	55.88%
Totales	**68**	**100.00%**

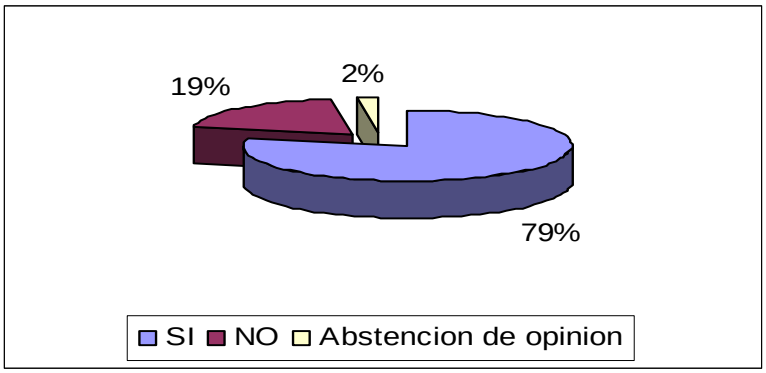


Análisis: Los sistemas de información contable generan una serie de reportes los cuales son útiles para respaldar las operaciones e información generada en estos en su mayoría son las partidas de diario, manejo de las existencias de inventarios y la cartera de clientes.

21. ¿Considera usted, que la información procesada en el Sistema de Información Contable de su compañía es confiable?

Objetivo: Determinar la confiabilidad de la información generada por el sistema de información confiable.

Alternativas	Fa	Fr
SI	37	78.72%
NO	9	19.15%
Abstención de opinión	1	2.13%
Totales	**47**	**100.00%**

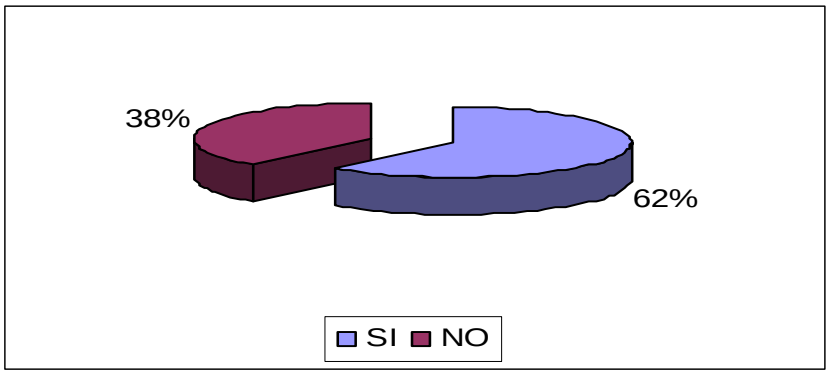


Análisis: El 79% de los laboratorios consideran que la información procesada en el sistema de información contable es confiable, debido que no se tienen caídas de sistemas, se tiene soporte de las operaciones registradas y no se detectan errores importantes que haga durar de la razonabilidad de las cifras reflejadas en los estados financieros.

22. ¿El Sistema de Información Contable, que usted utiliza le permite generar controles al procesamiento electrónico de datos?

Objetivo: Verificar la existencia de controles internos aplicados al procesamiento electrónico de datos.

Alternativas	Fa	Fr
SI	29	61.70%
NO	18	38.30%
Totales	**47**	**100.00%**

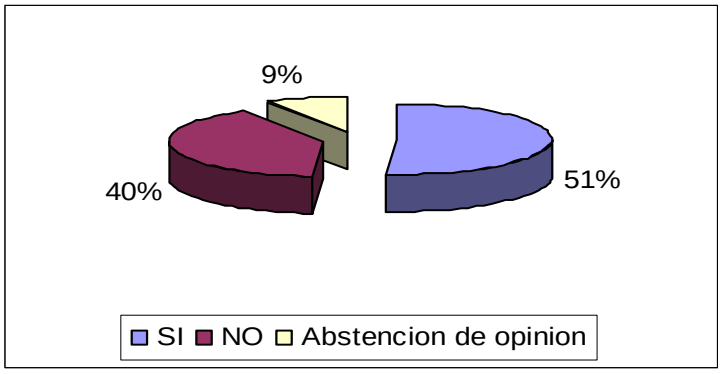


Análisis: Del total de los laboratorios encuestados consideran que su sistema de información contable le permite generar controles adecuados para el procesamiento electrónico de datos, debido a que cada persona tiene un pass Word el cual queda plasmado en cada transacción registrada.

23. ¿Se supervisan constantemente los controles generados por el sistema contable?

Objetivo: Verificar si son monitoreados de manera oportuna los controles internos informáticos.

Alternativas	Fa	Fr
SI	24	51.06%
NO	19	40.43%
Abstención de opinión	4	8.51%
Totales	**47**	**100.00%**

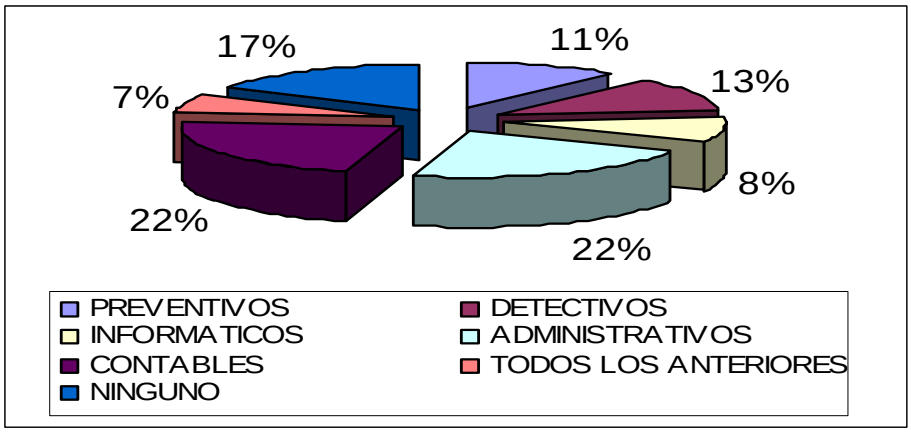


Análisis: En la mayoría de las compañías farmacéuticas se tienen controles establecidos por la administración encaminados a la salvaguarda de la información generada en los sistemas de información contable los cuales son supervisados periódicamente por personal idóneo debido a que el 51% realizada dicha gestión.

24. ¿Qué tipos de controles le permite generar?

Objetivo: Conocer con que tipos de controles cuenta la entidad para mejorar la confiabilidad de la información.

Alternativas	Fa	Fr
PREVENTIVOS	8	11.11%
DETECTIVOS	9	12.50%
INFORMATICOS	6	8.33%
ADMINISTRATIVOS	16	22.22%
CONTABLES	16	22.22%
TODOS LOS ANTERIORES	5	6.94%
NINGUNO	12	16.67%
Totales	**72**	**100.00%**

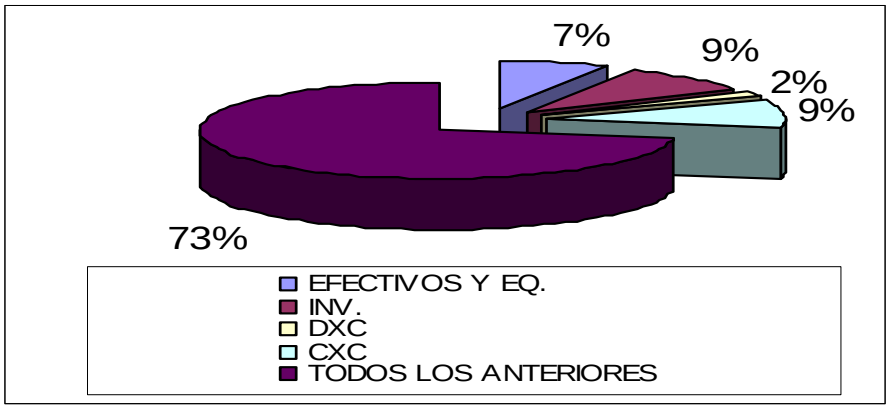


Análisis: Dentro de los controles generados por los sistemas de información contable en su mayoría son los administrativos y contables, todo esto encaminado a la veracidad y efectividad de las operaciones realizadas

25. ¿Qué áreas de Activos Corrientes maneja el Sistema de Información Contable?

Objetivo: Conocer los módulos del sistema de información contable en el área de los activos corrientes de la compañía.

Alternativas	Fa	Fr
EFECTIVOS Y EQ.	4	7.41%
INV.	5	9.26%
DXC	1	1.85%
CXC	5	9.26%
TODOS LOS ANTERIORES	39	72.22%
Totales	**54**	**100.00%**

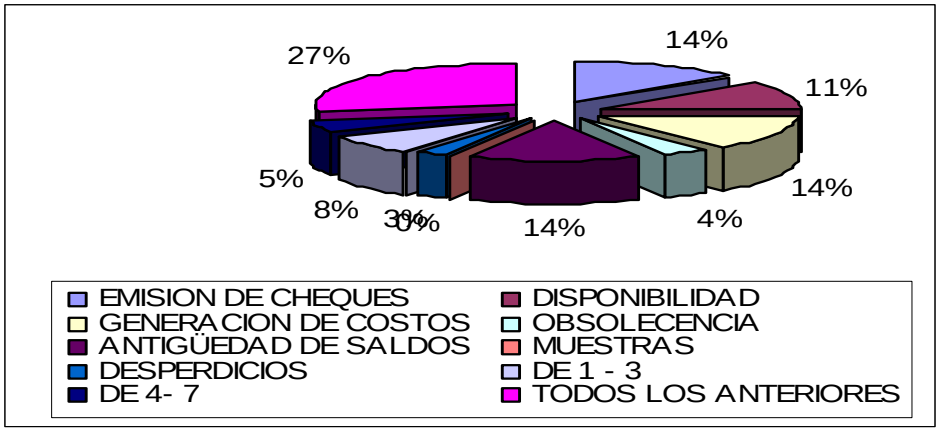


Análisis: Los laboratorios consideran que las áreas más importantes y de mayor atención son las de inventarios y las cuentas por cobrar, debido a que en estas áreas se encuentran en su mayoría irregularidades que afectan de manera significativa la razonabilidad de las cifras reflejadas en los estados financieros

26. ¿Qué tipo de reportes genera el Sistema de Información Contable dentro de los activos corrientes?

Objetivo: Conocer los diferentes reportes que emite el sistema de información contable.

Alternativas	Fa	Fr
EMISION DE CHEQUES	11	13.92%
DISPONIBILIDAD	9	11.39%
GENERACION DE COSTOS	11	13.92%
OBSOLECENCIA	3	3.80%
ANTIGÜEDAD DE SALDOS	11	13.92%
MUESTRAS	0	0.00%
DESPERDICIOS	2	2.53%
DE 1 – 3	6	7.59%
DE 4- 7	4	5.06%
TODOS LOS ANTERIORES	22	27.85%
Totales	**79**	**100.00%**

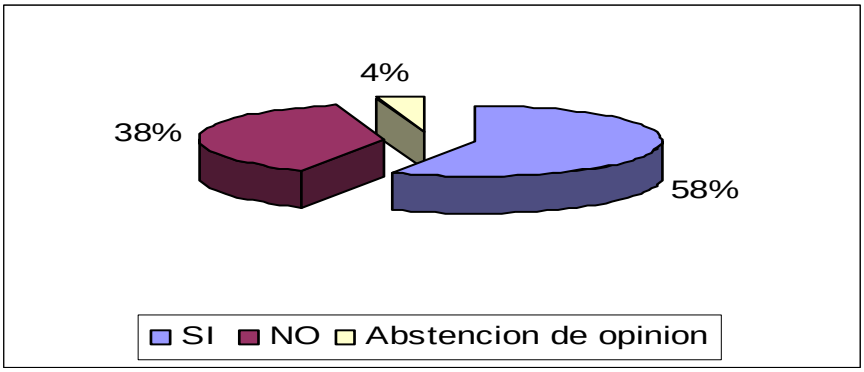


Análisis: La mayoría de los encuestados respondió que su sistema si genera reportes relativos a los activos corrientes, en su gran mayoría son relativos a las cuentas por cobrar y efectivo y equivalentes, siendo el área de inventarios con menos reportes emitidos por el sistema.

27. ¿Tiene acceso a los controles que emite el sistema?

Objetivo: Conocer que personas tienen acceso a los controles generados por el sistema.

Alternativas	Fa	Fr
SI	27	57.45%
NO	18	38.30%
Abstención de opinión	2	4.26%
Totales	**47**	**100.00%**

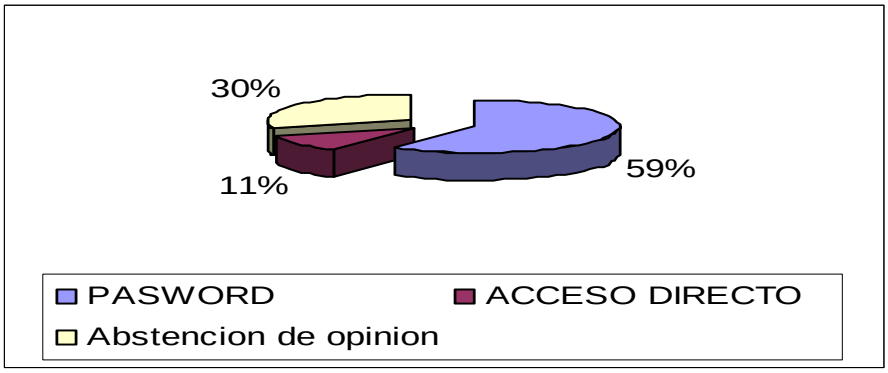


Análisis: En un 58% de los encuestados contestaron que si tienen acceso a los controles que emite el sistema de contabilidad que utilizan en su empresa.

28. ¿De qué forma accesa usted a estos controles?

Objetivo: Determinar las formas de acceso a los sistemas de información.

Alternativas	Fa	Fr
PASWORD	28	59.57%
ACCESO DIRECTO	5	10.64%
Abstención de opinión	14	29.79%
Totales	**47**	**100.00%**

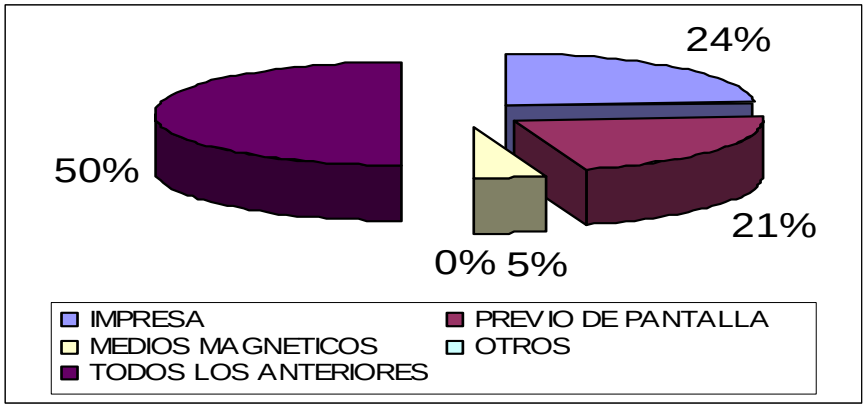


Análisis: En su mayoría los encuestados si tienen acceso a los controles emitidos por el sistema de información, y lo hacen a través de un medio seguro como lo es el uso de password.

29. ¿De qué manera puede disponer de la información generada por el Sistema de Información Contable?

Objetivo: Conocer a través de que medios se puede disponer de la información puede ser consultada.

Alternativas	Fa	Fr
IMPRESA	15	24.19%
PREVIO DE PANTALLA	13	20.97%
MEDIOS MAGNETICOS	3	4.84%
OTROS	0	0.00%
TODOS LOS ANTERIORES	31	50.00%
Totales	**62**	**100.00%**

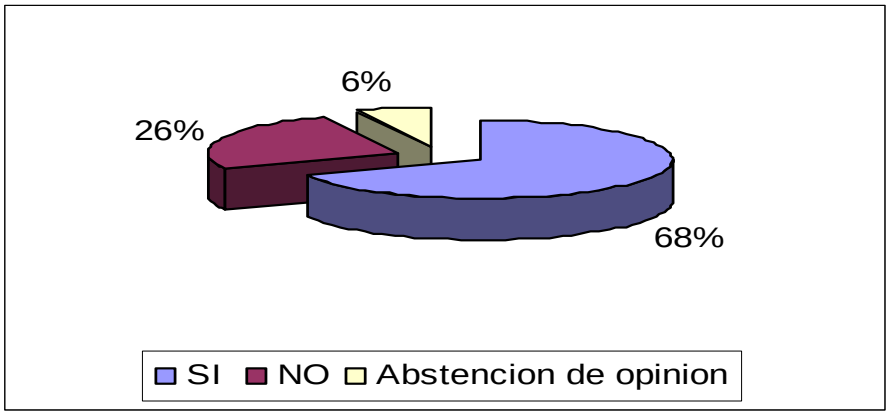


Análisis: Los usuarios de sistemas de información encuestados en un 50% indico que dispone de la información a través de los medios de previo de pantalla, impresa y medios magnéticos, siendo los medios magnéticos el menos utilizado

30. ¿Queda alguna evidencia de los controles que genera el sistema?

Objetivo: Conocer si existen medios de verificación de los diferentes reportes y controles generados por el sistema.

Alternativas	Fa	Fr
SI	32	68.09%
NO	12	25.53%
Abstención de opinión	3	6.38%
Totales	**47**	**100.00%**

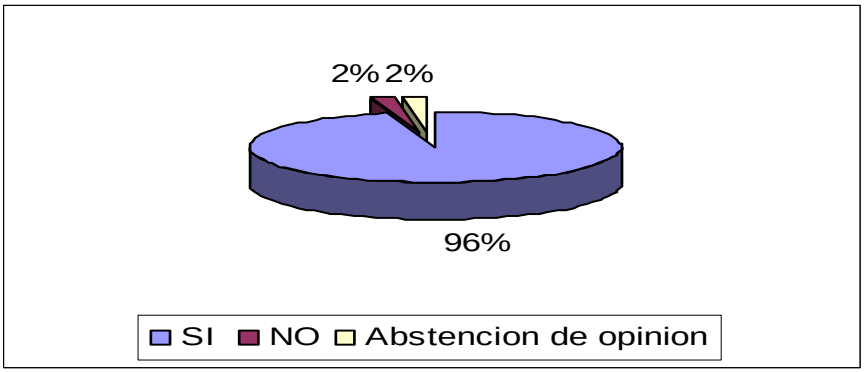


Análisis: En un 68% de los encuestados asevero que el sistema maneja una secuencia de las operaciones realizadas por los usuarios, permitiendo guardar evidencias para futuras revisiones

31. ¿Considera usted, que el control interno informático es importante para el manejo adecuado de los activos corrientes?

Objetivo: Conocer la importancia del control interno informático para el manejo de las cuentas de activo corriente.

Alternativas	Fa	Fr
SI	45	95.74%
NO	1	2.13%
Abstención de opinión	1	2.13%
Totales	**47**	**100.00%**

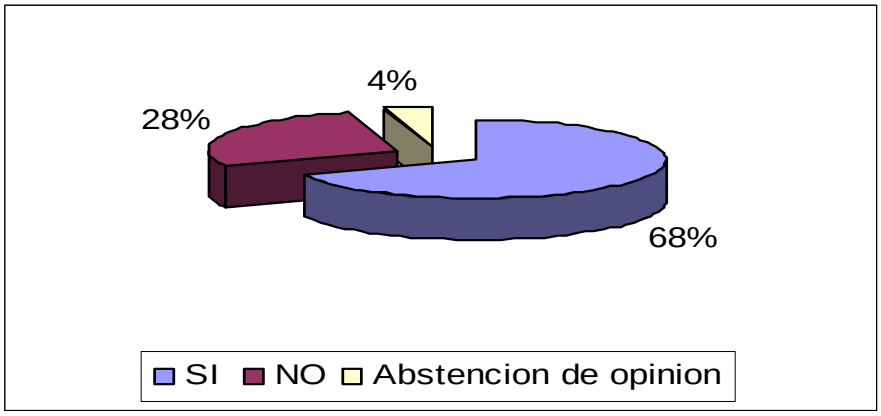


Análisis: Un 96% considera que el aplicarles controles internos informáticos al área de activos corrientes, es de gran importancia, debido a que es una área de mucha importancia para las industrias.

32. ¿Considera usted que los controles informáticos aplicados a los activos corrientes son confiables?

Objetivo: Determinar la confiabilidad de los controles informáticos que posee la industria farmacéutica en el área de los activos corrientes.

Alternativas	Fa	Fr
SI	32	68.09%
NO	13	27.66%
Abstención de opinión	2	4.26%
Totales	**47**	**100.00%**

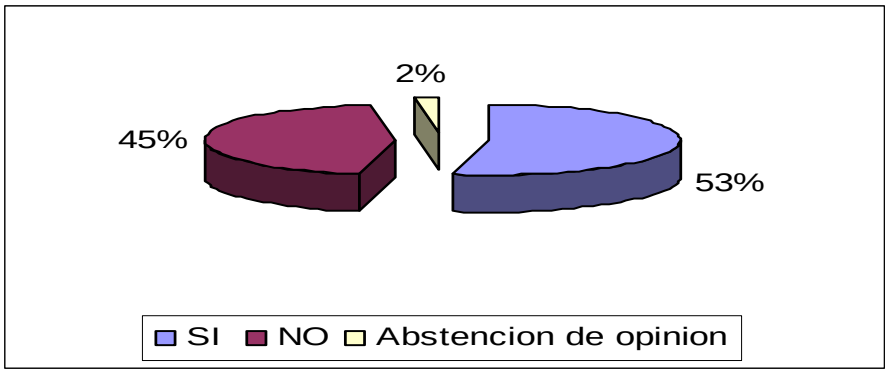


Análisis: Un 68% de la población encuestada considera que los controles aplicados a los activos corrientes si cumplen con sus necesidades en cuanto a confianza y seguridad de la información, pero por otra parte el 28% de los encuestados dijo que los controles no son fiables pues dentro de los sistemas existen caídas de sistema, no hay capacitaciones o el sistema es muy complejo. Además dentro del numero de personas que dijeron que su información es confiable, aclararon que si existen caídas en sus sistemas y que manejan sistemas complejos.

33. ¿Se realizan mejoras a los controles internos informáticos aplicados a los activos corrientes?

Objetivo: Verificar que los controles internos informáticos se adecuan a los cambios o mejoras que sufren los sistemas.

Alternativas	Fa	Fr
SI	25	53.19%
NO	21	44.68%
Abstención de opinión	1	2.13%
Totales	**47**	**100.00%**

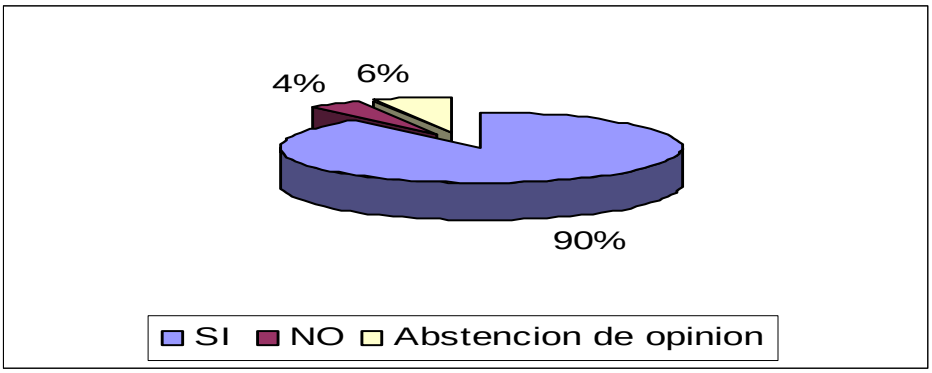


Análisis: En un 53% de los encuestados, indican que los controles aplicados a los activos corrientes se estan cambiando a medida que surgen nuevas necesidades dentro de la compañía.

34. ¿Cree usted, que con un documento que le indique que Control Interno Informático puede aplicar a su compañía para el área de Activos Corrientes, es necesario?

Objetivo: Conocer sobre la importancia de tener una herramienta que proporcione una guía para la elaboración del control interno informático.

Alternativas	Fa	Fr
SI	42	89.36%
NO	2	4.26%
Abstención de opinión	3	6.38%
Totales	**47**	**100.00%**



Análisis: El 90% de los encuestados opino que si es necesario contar con una guía que les permita tomar parámetros para establecer controles internos informáticos, debido a que esta área es muy compleja y pocas personas conocen como se pueden establecer y manejar los controles internos informáticos.

ANEXO 5 FORMATOS SUGERIDOS

Recibo de Ingreso

Recibo de Ingresos

Fecha:_____ Codigo:_____

Nombre del cliente: _____

Efectivo: Cheque: Deposito:

Banco:_____ No. Cheque:_____

La cantidada: _____

Cancelacion: Abono: Reintegro:

No. Factura	Monto de factura	Monto recibido
Total:		

(-)Descuento aplicado:

Porcentaje aplicado:

Valor:…… US$_____

TOTALES…… US$_____

_____ _____

Elaborado por Autorizado por

Vale de Caja Chica

No. Correlativo:

Empresa:_____

Vale de caja chica por:_____

Recibi la cantidad de:_____

Para:_____

_____

Autorizado por:_____ Recibido por:_____

Nombre:_____

San Salvador,_____ de _____ de _____

Reporte de Antigüedad de Saldos

Nombre de la Empresa

Antigüedad de Saldos

Periodo del: _____ al:_____

Del cliente:_____ al Cliente:_____

Reporte detallado

Clasificacion:_____

Codigo Fecha venc.	Nombre del cliente	Desgloce de saldos vencidos en dias 1 - 30	 30 - 60	 61 - 90	 91- o mas
TOTALES:					

Estado de Cuenta Clientes

Nombre de la empresa

Fecha:_____

Estado de cuenta detallado

Nombre del cliente:_____ Codigo: _____

Direccion:_____ Clasificacion: _____

No. Registro:_____ Dias de credito: _____

Telefono:_____ Limite de credito:_____

Atencion Cobranza:_____ Saldo disponible:_____

Concepto	Documento	Fecha de aplicación	Fecha de vencimiento	Referencia	Cargos	Abonos	Saldos
TOTALES:							

Expediente del Cliente

EXPEDIENTE DE CLIENTES

Datos Generales
Clave:_____

Nombre del cliente:_____

Direccion:_____

Colonia:_____

R.F.C._____

Telefono:_____ Fax:_____
E- mail:_____
Clasificacion:_____

Datos de venta

Codigo: _____
Nombre del cliente: _____
Dias de credito: _____
Limite de credito: _____

Atencion ventas: _____

Atencion Cobranza: _____

Vendedor: _____ Codigo:_____ Nombre: _____

Datos Historicos
Clave: _____

Nombre del cliente: _____
Limite de credito: _____
Ventas anuales: _____

Ultimo pago		**Ultima venta**	
Fecha:	_____	Fecha:	_____
Documento:	_____	Documento:	_____
Monto:	_____	Monto:	_____

Requisición de Materiales a Bodega

NOMBRE DE LA EMPRESA
REQUISICION DE MATERIALES

FECHA _____

DEPARTAMENTO CODIGO DPTO

OBSERVACIONES:_____

CODIGO	DESCRIPCION DEL PRODUCTO	CANTIDAD

Orden de Compra de Materiales

NOMBRE DE LA EMPRESA
ORDEN DE COMPRA DE MATERIALES

CODIGO DE PROVEEDOR	COMPRADOR
NOMBRE DEL PROVEEDOR	NOMBRE DE LA EMPRESA
CONTACTO	DIRECCION
DIRECCION	CONTACTO
TELEFONO	TELEFONO
TIPO DE CONTRIBUYENTE	

No.	CTA. CONTABLE	DESCRIPCION DEL PRODUCTO	BODEGA	UNIDADES	PRECIO UNITARIO	TOTAL

TOTALES

COMPRADOR

AUTORIZADO POR

Recibo de Ingreso a Bodega

NOMBRE DE LA EMPRESA
RECIBO DE INGRESO A BODEGA

RECIBO DE COMPRA	ORDEN DE COMPRA
CODIGO DE PROVEEDOR FECHA DE ORDEN CODIGO DE COMPRADOR	FECHA DE RECIBIDO CODIGO DE USUARIO FECHA DE ELABORACION

No.	DESCRIPCION DEL PRODUCTO	UNIDADES	CANTIDAD SOLICITADA	CANTIDAD RECIBIDA

RECIBIDO POR:

SELLO DE BODEGA

ANEXO 6 GLOSARIO

Acceso lógico: Se refiere a la acción del usuario que le lleva a utilizar y/o visualizar, y/o modificar y/o borrar datos o programas. Para que el usuario tenga acceso lógico, en ocasiones no es necesario que tenga acceso físico a los medios computacionales, pues el usuario que se encuentra en una ubicación remota respecto a los sistemas computacionales a los cuales desea tener acceso lógico, puede tener dicho acceso a través de sistemas de comunicación que hacen posible el acceso.

Acreditación: Documento que le da a uno la facultad de hacer alguna cosa.

Actualización: Actualización de datos se refiere principalmente a las modificaciones que van sufriendo ciertos datos de Archivos Maestros a causa de las operaciones.

Afectación de inventarios:
Es el proceso de dar ingreso o salida de la mercadería en el modulo de inventarios.

Archivo Maestro: Archivo de Datos principales, la mayoría de los cuales no varían con la ejecución de operaciones.

Calificación: Se refiere a las condiciones necesarias para que el profesional desempeñe cierto tipo de funciones. Quien tiene la formación académica, la experiencia y puede asumir los niveles de responsabilidad descriptos para el cargo, está calificado para desempeñar ese cargo.

Cambios correctivos:
Son aquellos cambios de malas aplicaciones registradas en el sistema, efectuadas mediante autorización y solo por personal autorizado.

Certificación: Documento emitido por alguien con la autoridad correspondiente para comprobar de manera fehaciente alguna cosa.

Control de Cambios: La Gerencia debe establecer un Procedimiento de Control de Cambios. Las solicitudes de Cambio provienen en general de los usuarios, pero pueden originarse por iniciativa de alguna de las Unidades Funcionales a cargo de la Gerencia

Comprobante de ingreso de mercadería:
Formulario que se utiliza para la recepción de mercadería a bodega, el cual es ingresado posteriormente a modulo de inventarios para alimentar las existencias.

Cuenta del Usuario: Un ambiente de empresarial de TI debe estar protegido por procedimientos de Seguridad de acceso. El

administrador de Seguridad de Acceso habilita una Cuenta del Usuario para cada Usuario que puede acceder a los recursos del Sistema.

Custodio: Persona o Unidad Funcional que es nombrada responsable de la ejecución del Sistema o ejecución de los Procedimientos en nombre del Usuario.

Cliente activo:
Son aquellos clientes que tienen su crédito al corriente.

Cliente pasivo:
Son aquellos clientes que por alguna razón o motivo tienen facturas vencidas pendientes de pago.

Cheque devuelto:
Son aquellos cheques ingresados al sistema una vez rechazados y devueltos por el banco por alguna razón o motivo.

Cheques posfechados:
Son aquellos cheques entregados por el cliente emitidos para ser cobrados posteriormente, los cuales son ingresados al sistema con fecha de vencimiento de su emisión.

Diccionario de Datos: Es el Diccionario de Datos que se refiere a todos los datos de la Entidad.

En línea: En informática se dice que la información está en línea, cuando el Usuario puede acceder a la información desde una Terminal.

Encriptar: Uno de los procedimientos de seguridad de datos más utilizados es la encriptación, que consiste en transformar los datos a un formato no reconocible por el usuario que no posea la clave para volver a transformarlos a un formato legible

Entrada: Se refiere al ingreso de datos al Sistema de TI.

Esquema: Documento que define de manera esquemática algo. Definición de alto nivel, en base a las cuales se efectúan definiciones de menor nivel.

Estructurado: Método de Depuraciones Sucesivas, que consiste en tener en primer lugar una visión poco profunda del todo, e ir luego teniendo una visión cada vez más profunda de cada una de sus partes, y así sucesivamente.

Identificación: se refiere a un código único e inmutable que corresponde a cada usuario.

Incidente de Seguridad: En general, el término Incidente se refiere a hechos ocurridos que pueden significar intento de

irregularidades, o directamente hechos que se refieren a irregularidades.

Integridad referencial: Se refiere a la existencia de datos relacionados en diferentes archivos.

Inventario ocioso:
Producto que se encuentra en stop, es decir que tiene poca rotación y por lo tanto tiende a vencerse.

Limites de inventarios:
Son los niveles máximos y mínimos de inventarios que han sido establecidos previamente por gerencia.

Limite de crédito autorizado:
Es aquel monto autorizado por gerencia el cual es igual al valor registrado en sistema dentro del modulo de cuentas por cobrar.

Mantenimiento: Mantener es sinónimo de hacer que permanezca actualizado.

Monitorear: Mantener bajo observación. Observar frecuentemente. Verificar continuamente.

Niveles de Seguridad de Datos: El Esquema de Clasificación de Datos define las diversas “Clases de Datos”.

Muestras medicas:
Son aquellos productos elaborados en concepto de regalías para distribuirlas a las diferentes farmacias y hospitales.

Nota de crédito:
Son aquellos documentos utilizados para la aplicación de descuentos de clientes autorizados, anulación, aumento o disminución del valor de la factura.

Nota de abono
Son aquellos formularios utilizados para cancelar o modificar el valor de las facturas de consumidor final.

Oportuno: Realizado en el tiempo justo, en el momento preciso. Que no tiene retrasos.

Orden de compra:
Es un reporte interno utilizado para realizar los requerimientos de materia prima.

Obsolescencia:
Producto que ha llegado a su fecha de vencimiento y no se logro sacar a la venta, convirtiéndose en mercadería obsoleta.

Orden de producción:

Formulario que se utiliza para solicitar la fabricación de lotes de productos.

Plan de Contingencia: que forma parte del Plan de Infraestructura Tecnológica debe estar en constante revisión y evolución, puesto que ello llevará a soluciones de mayor calidad.

Procedimientos de Flujo de Datos: se refieren al transporte de datos de un medio computacional a otro, o de un medio computacional a un depósito de almacenamiento de respaldo, por medio de soportes o cualquier tipo de transmisión por cables u ondas electromagnéticas.

Productos en proceso:
Es todo aquel producto que se encuentra en proceso de fabricación.

Producto terminado:
Es aquel producto que se encuentra listo para su distribución y venta.

Pasword:
Es aquella clave asignada a cada usuario para ingresar al sistema.

Respaldo: (back-up) copia de archivos de datos o de software igual a aquella que será o está siendo utilizada.

Salida: Todo dato o información producidos por la TI puede ser llamado Salida. Las Salidas pueden estar impresas en papel, grabadas en medios magnéticos, ópticos, o diversos otros medios.
Software de Aplicación: Se refiere a los programas o sistemas mediante los cuales los usuarios ejecutan sus actividades laborales propias de la Entidad.

Software de Base: Es el conjunto de programas que sirven para hacer que el computador funcione. Esta constituido generalmente por una serie de programas tales como: El Sistema Operativo, los utilitarios, los compiladores, software de comunicación, software de interfase con periféricos, etc. En ocasiones incluye software de seguridad y software de acceso a datos.

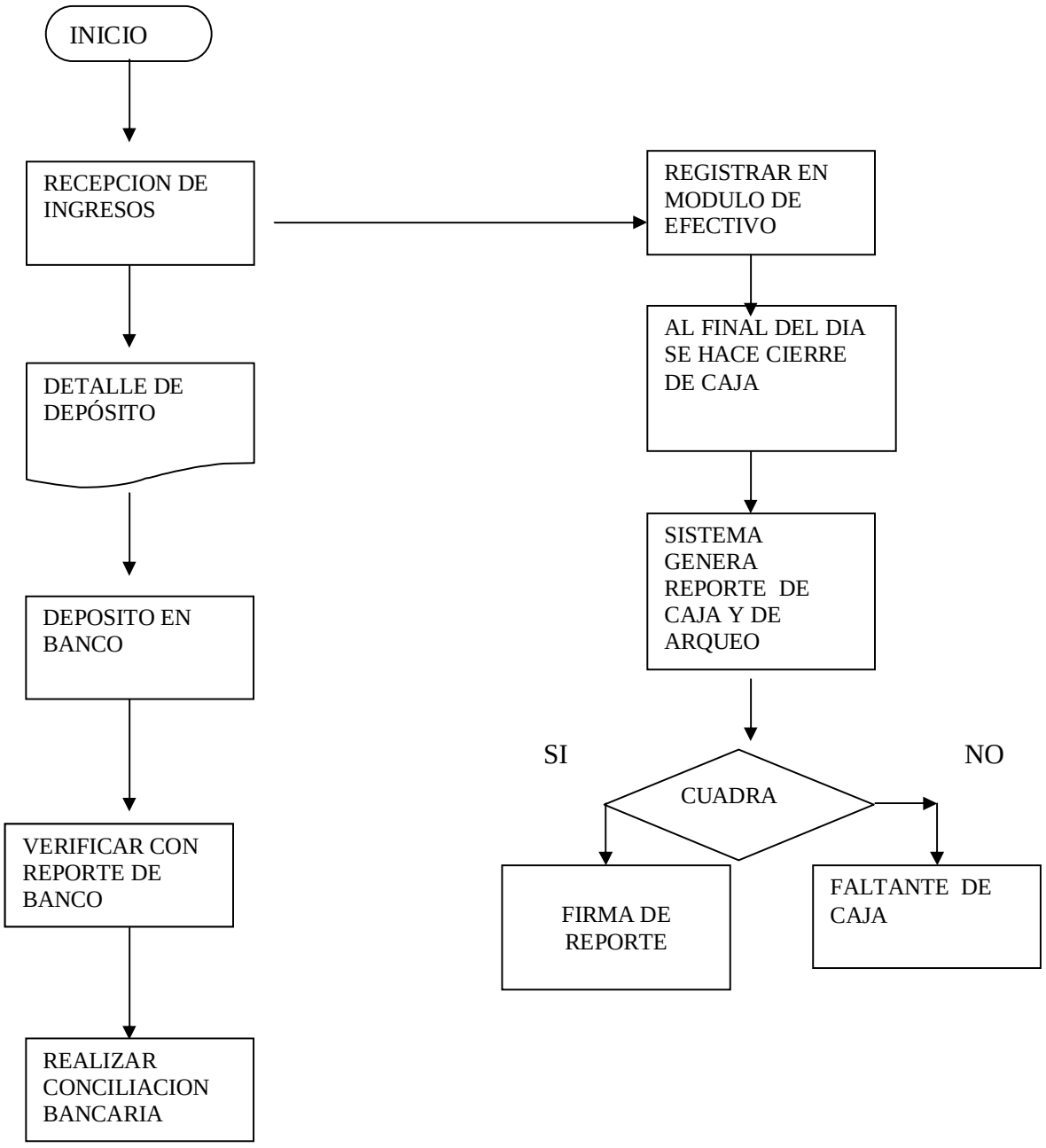
Transacción: Conjunto de instrucciones que ejecutan operaciones sobre datos almacenados.

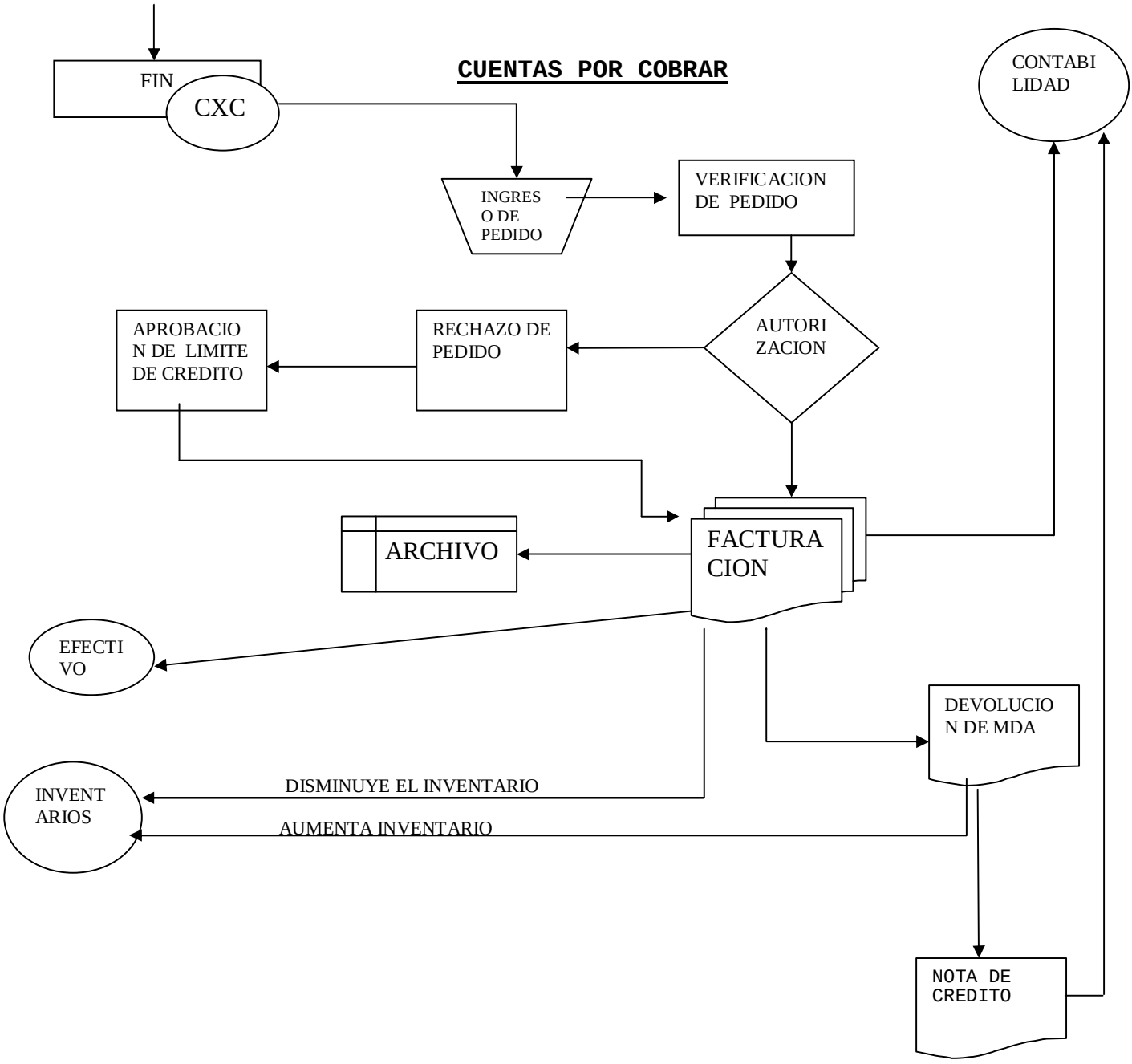
Virus: Es una porción de código ejecutable, que tiene la habilidad única de reproducirse. Se adhieren a cualquier tipo de archivo y se diseminan con los archivos que se copian y envían de persona a persona.

Volúmenes: Un volumen es una unidad física de Almacenamiento de datos y/o programas.

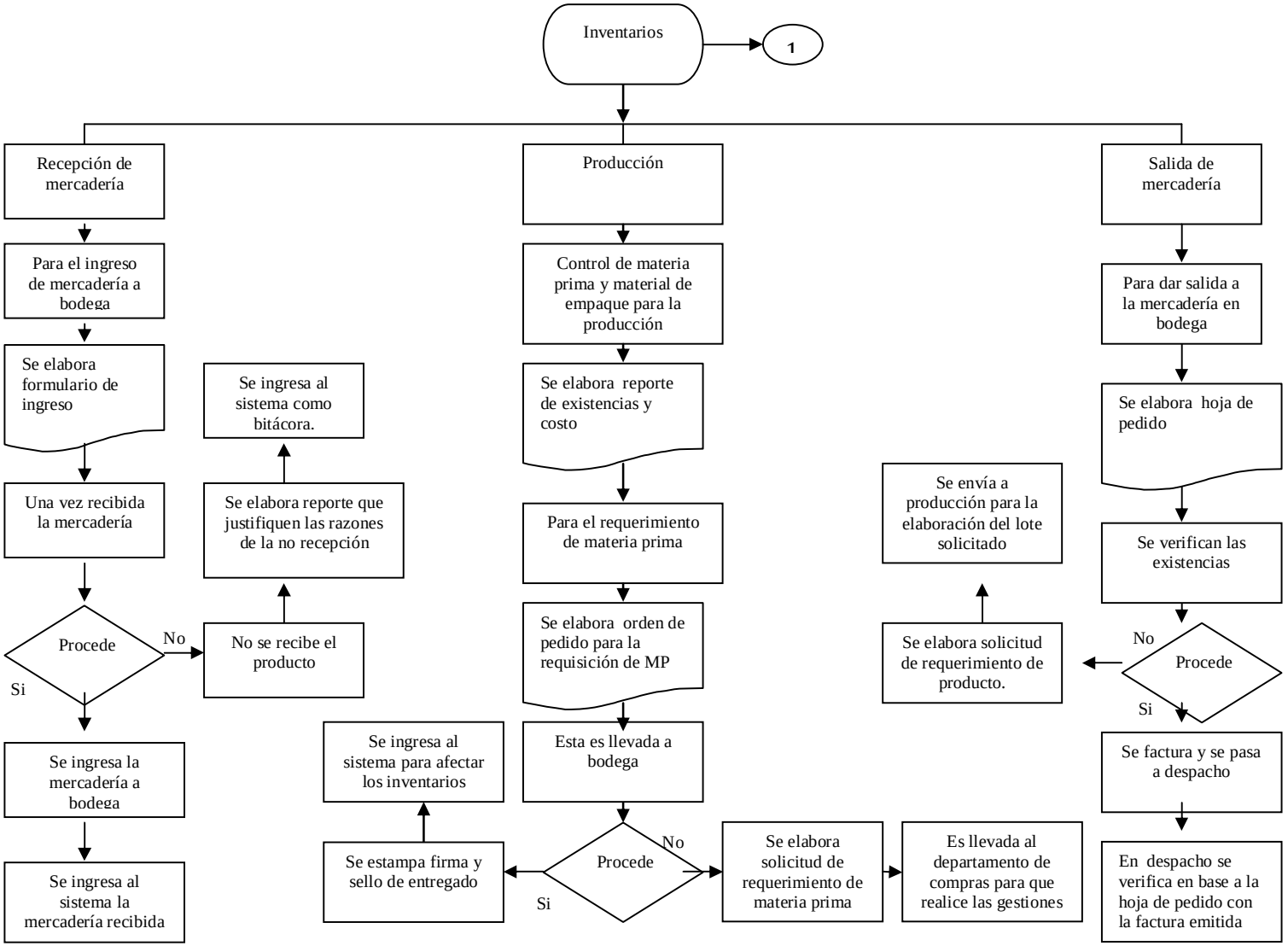
ANEXO 7 DIAGRAMAS DE FLUJO

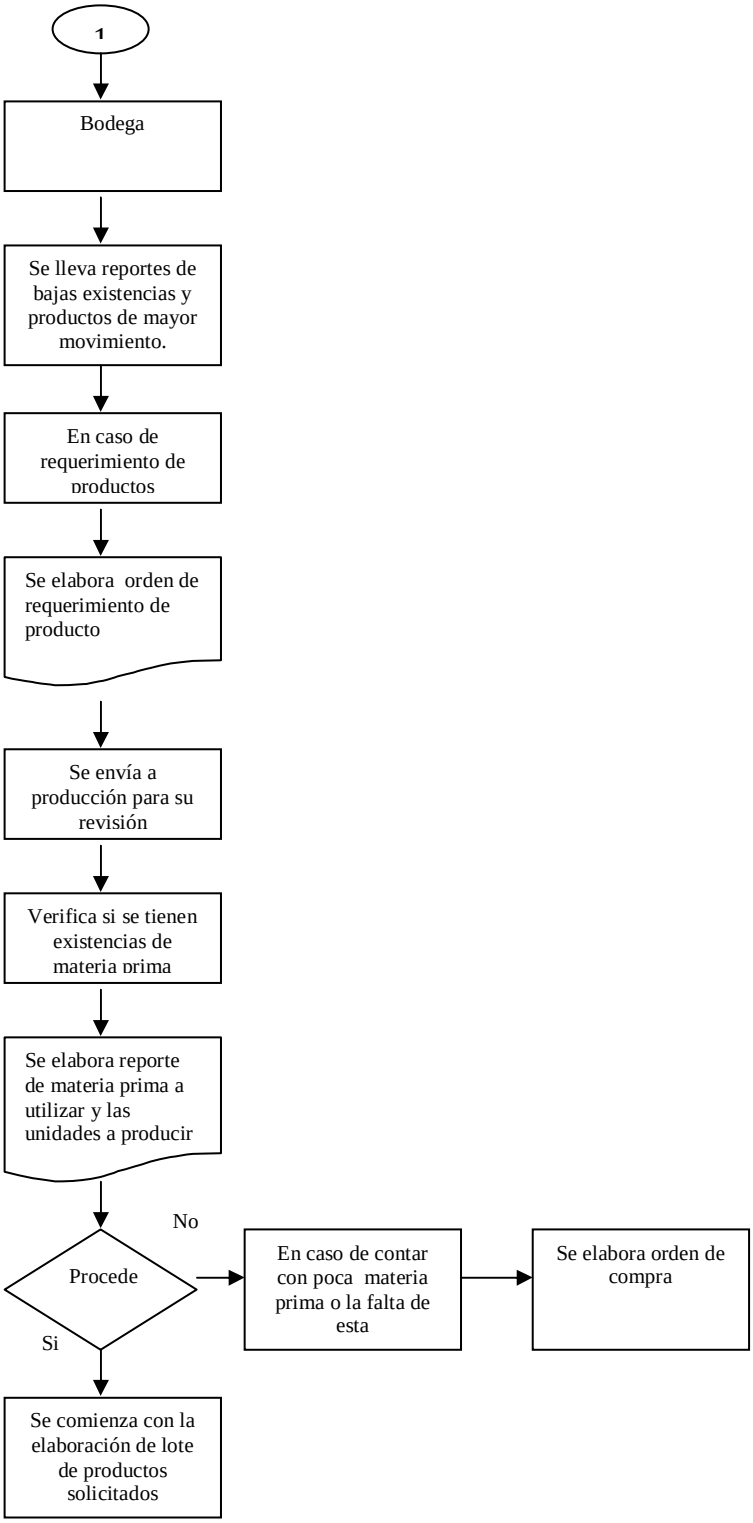
EFECTIVO Y EQUIVALENTES




CUENTAS POR COBRAR
FIN
CXC
INGRES O DE PEDIDO
VERIFICACION DE PEDIDO
CONTABI LIDAD
AUTORI ZACION
RECHAZO DE PEDIDO
APROBACIO N DE LIMITE DE CREDITO
ARCHIVO
FACTURA CION
EFECTI VO
DEVOLUCIO N DE MDA
INVENT ARIOS
DISMINUYE EL INVENTARIO
AUMENTA INVENTARIO
NOTA DE CREDITO

INVENTARIOS




1
Bodega
Se lleva reportes de bajas existencias y productos de mayor movimiento.
En caso de requerimiento de productos
Se elabora orden de requerimiento de producto
Se envía a producción para su revisión
Verifica si se tienen existencias de materia prima
Se elabora reporte de materia prima a utilizar y las unidades a producir
Procede
No
Si
En caso de contar con poca materia prima o la falta de esta
Se elabora orden de compra
Se comienza con la elaboración de lote de productos solicitados