UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA DE CONTABILIDAD Y AUDITORÍA

Tesis previa a la obtención del Título de:
INGENIERO COMERCIAL CON ESPECIALIZACIÓN EN CONTABILIDAD Y AUDITORÍA

TEMA:

ADMINISTRACIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN COMO MECANISMO PARA OPTIMIZAR EL ANÁLISIS DE LOS ESTADOS FINANCIEROS
CASO: SUPERMERCADO DE COMPUTADORAS COMPUBUSSINES CÍA. LTDA.

AUTORA:

MARCELA CAROLINA LEROUX SIMONS

DIRECTOR:

LIC. JORGE EDUARDO ZAPATA LARA

Quito, Octubre de 2011

DECLARATORIA DE RESPONSABILIDAD

Los conceptos desarrollados, análisis realizados y las conclusiones del presente trabajo, son de exclusiva responsabilidad de la autora.

Quito, Octubre del 2011.

(f) _____

Marcela Carolina Leroux Simons

AGRADECIMIENTOS

Quiero expresar mi agradecimiento de todo corazón

A Dios por haberme guiado por el camino de la felicidad hasta ahora.

A cada uno de los que son parte de mi familia a mi PADRE Marcelo Leroux, mi MADRE, Paulina Simons y a mi HERMANA Cristina Leroux; por siempre haberme dado su fuerza y apoyo incondicional que me han llevado hasta donde estoy ahora.

A mi hija, Ariana por acompañarme y darme la fuerza para seguir adelante en todos los momentos importantes de mi vida.

A mi mejor amiga Anita Castelo por su calidez y afecto al compartir inquietudes, éxitos y fracasos durante muchos años de amistad.

A mi Director de Tesis, Lic. Jorge Zapata L., por su generosidad al brindarme la oportunidad de recurrir a su capacidad y experiencia científica en un marco de confianza, afecto y amistad, fundamentales para la culminación de este trabajo.

A la UNIVERSIDAD POLITÉCNICA SALESIANA, por haberme formado académicamente e íntegramente, gracias a ella me siento capaz de conquistar nuevos horizontes.

A mis profesores por ser orientadores de todos los conocimientos adquiridos en estos años de estudio.

Por último a todos mis compañeros que a lo largo de la carrera me brindaron su continuo y afectuoso aliento.

DEDICATORIA

Dedico este proyecto de tesis a Dios, a mis padres y a mi hija.

A Dios porque ha estado conmigo a cada paso que doy, cuidándome y dándome fortaleza para continuar.

A mis padres, pilares fundamentales en mi vida, quienes han velado por mi bienestar y educación siendo mi apoyo en todo momento. Depositando su entera confianza en cada reto que se me presentaba sin dudar ni un solo momento en mi inteligencia y capacidad.

A mi hija, compañera inseparable de cada jornada, que es la razón para obtener este título profesional y con ello no desampararle en ningún momento. Ella representó gran esfuerzo y tenacidad en momentos de decline y cansancio.

Sin ellos, jamás hubiese podido conseguir lo que hasta ahora lo he logrado, su tenacidad y lucha insaciable han hecho de ellos el gran ejemplo a seguir y destacar, no solo para mí, sino para mi hermana y familia en general.

Es por ellos que soy lo que soy ahora. “LOS AMO CON MI VIDA”.

RESUMEN

Luego de haber investigado el presente trabajo, nos muestra una alternativa en la Administración de Riesgos, en una empresa del sector privado comercial, cuyo objetivo principal es satisfacer las necesidades de sus clientes dando garantía de su trabajo con mercadería de alta calidad.

La Tecnología de Información (TI) se ha convertido en el corazón de las operaciones de cualquier organización, desde los sistemas transaccionales que ayudan a dichas operaciones diarias, hasta las aplicaciones enfocadas a la alta gerencia que contribuyen a definir el rumbo que tiene que seguir una organización, por esta razón es importante preservar una seguridad razonable respecto de las TI que administra.

Una seguridad razonable se consigue con la identificación de los riesgos y la implementación de controles en toda la organización, sin dejar a un lado al área de TI. La alta gerencia debe decidir el nivel de riesgo que está dispuesta a aceptar. Debe juzgar cual puede ser el nivel tolerable, esto puede ser una decisión difícil para la organización. Por esta razón, la alta gerencia debe trabajar en la identificación de los riesgos y en la consiguiente Administración de los mismos.

Para desarrollar el tema denominado **"ADMINISTRACIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN COMO MECANISMO PARA OPTIMIZAR EL ANÁLISIS DE LOS ESTADOS FINANCIEROS, CASO: SUPERMERCADO DE COMPUTADORAS COMPUBUSSINES CÍA. LTDA."** se ha organizado el presente trabajo en cinco capítulos, manteniendo una secuencia lógica, la misma que se describe a continuación:

- **El capítulo I.-** enmarca los fundamentos teóricos de Riesgos de Tecnología de Información.

Se debe decidir cuál es la inversión razonable en seguridad y en control de TI y cómo lograr un balance entre riesgos e inversiones en el enfoque de control, en un ambiente de Tecnología de Información, frecuentemente impredecible.

Mientras la seguridad y los controles en los sistemas de información ayudan a administrar los riesgos sin eliminarlos, surge la necesidad de administrar esos riesgos, puesto que el exacto nivel de riesgo nunca puede ser conocido ya que siempre existe un grado de incertidumbre.

- **El capítulo II.-** estudia y analiza la situación actual de la empresa Supermercado de Computadoras Compubussines Cía. Ltda.

En este capítulo se da a conocer la estructura organizacional de Supermercado de Computadoras Compubussines Cía. Ltda., ya que es importante conocer la forma en que se dividen, agrupan y coordinan las actividades de la organización, en cuanto a las relaciones que mantiene todo el personal involucrado en la misma.

- **El capítulo III.-** estudia las metodologías de Administración de riesgos de Tecnologías de Información y Seguridad.

El siguiente capítulo describe varias técnicas metodológicas en Administración de Riesgos que pretenden lograr objetividad en la valoración de los riesgos, a través del control, seguimiento y evaluación de la administración de riesgos sobre bases objetivas.

La metodología es el fruto del nivel profesional de cada uno y de su visión de cómo conseguir un mejor resultado en el nivel de control de cada entidad, aunque el nivel de control resultante debe ser similar.

- **El capítulo IV.-** da a conocer la aplicación de Administración de Riesgos de Tecnología de Información como mecanismo para optimizar el análisis de los Estados Financieros.

Para llevar a cabo este objetivo vamos a establecer un plan de contingencia, con la finalidad de asegurar la capacidad de supervivencia de la compañía, ante eventos que pongan en peligro su existencia.

Queremos asegurar que existan controles adecuados para reducir el riesgo por fallas o mal funcionamiento tanto del equipo, como del software, de los datos, y de los medios de almacenamiento.

- **El capítulo V.-** se encarga de enumerar las diferentes conclusiones y recomendaciones establecidas en la investigación.

Este trabajo tiene como una de sus metas primordiales el orientar a las generaciones futuras, sobre los aspectos importantes que se deben considerar en la Administración de Riesgos de Tecnologías de Información de las empresas del sector privado comercial, éste tema es importante por su aproximación científica en el comportamiento de los riesgos, anticipando las posibles pérdidas accidentales con el diseño e implementación de procedimientos que minimicen la ocurrencia de pérdidas o el impacto financiero que se pueda ocurrir.

El principal objetivo de la Administración de Riesgos de TI, tiene como primera ley garantizar la supervivencia de la organización, minimizando los costos asociados con los riesgos. Muchos de los defectos en la administración de riesgos radican en la ausencia de objetivos claros.

La empresa debería designar un grupo de personas que se encarguen de implementar un plan de contingencia ante cualquier eventualidad, de ésta manera se salvaguardará la información contable de todo el sistema.

Con el crecimiento de la empresa aparecen nuevos riesgos, por lo que la Gerencia en conjunto con los Departamentos, debería organizar el Análisis de Riesgos cada cierto tiempo sea trimestral o semestral.

Todos los departamentos de una empresa deben poseer un sistema de análisis de riesgos de TI con la finalidad de brindar soluciones a los posibles riesgos que se puedan presentar en dicha empresa.

INTRODUCCIÓN

La Tecnología de Información (TI) se ha convertido en el corazón de las operaciones de cualquier organización, desde los sistemas transaccionales que ayudan a las operaciones diarias hasta las aplicaciones enfocadas a la alta Gerencia que contribuyen a definir el rumbo que tiene que seguir una organización, por esta razón es importante preservar una seguridad razonable en la Empresa, respecto de la adecuada administración de las TI.

El riesgo informático es un tema que en la actualidad se ha difundido en las empresas, motivo por el cual es un punto de análisis por parte de los expertos. En toda empresa hay riesgos informáticos, ya que hoy en día toda la información se maneja en procesadores. Partiendo de que los riesgos no son eliminados sino mas bien controlados, los controles y las seguridades cada vez se vuelven más indispensables para la protección de la información.

El desconocimiento del tema de los riesgos informáticos, es un peligro latente ya que las empresas pueden perder la eficiencia y la eficacia en el desarrollo de sus actividades. Debido a la gran cantidad de riesgos informáticos que puede haber en una empresa, y a la gama de controles que se pueden aplicar para mitigarlos, existen diferentes maneras de administrarlos, por lo que se han determinado varias metodologías para el efecto. Las metodologías de Administración de Riesgos de TI, pueden ser aplicadas en el área informática de las empresas.

En este mundo globalizado y de constantes cambios, las empresas obligadamente requieren ser cada vez más ágiles y se deben adaptar con mayor facilidad a estos cambios.

Actualmente, las compañías dependen en su totalidad de presentar la información exacta en el momento preciso, las empresas que no son capaces de alcanzar esto, están en peligro de extinción porque con el paso de los años la información se ha convertido en el arma más potente para la toma decisiones, y es aquí donde radica la prioridad de desarrollar nuevas tecnologías que permitan tener la información requerida y lista para ser utilizada.

Cabe aclarar que la Informática no gestiona propiamente la empresa, ayuda a la toma de decisiones, pero no decide por sí misma.

Las empresas que saben manejar los procesos de sistemas de información, tienen el poder de tomar decisiones que las beneficien y es aquí donde la tecnología de información juega un papel fundamental, porque las empresas pueden tener una ventaja competitiva sostenible que les permita posicionarse por encima de sus competidores.

Sin embargo, la mayoría de las organizaciones han fallado al no aprovechar el ambiente existente e implementar ideas innovadoras para mejorar el papel que juegan los sistemas de información dentro de sus organizaciones, algunos de estos errores son:

- Resistencia al cambio por parte de la gente
- Deficiencias para reconocer amenazas competitivas rápidamente.
- Robustez de los sistemas de información.
- Escasez de Recursos apropiados
- Incertidumbre de cómo o porqué automatizar procesos

Supermercado de Computadoras Compubussines Cía. Ltda., es una organización dedicada a la importación y comercialización de productos de maquinaria y equipo de oficina, enmarcados dentro de la línea de computación, electrónica e instrumentos musicales, por lo cual la presente investigación está destinada a presentar los principales controles y seguridades que deben implementarse en uno de los departamentos de la empresa, como es el caso del Departamento Contable y de Sistemas.

Objetivos

Objetivo General

- Desarrollar una Administración de Riesgos de Tecnología de Información como mecanismo para optimizar el Análisis de los Estados Financieros, para el Supermercado de Computadoras Compubussines Cía. Ltda., que permita asegurar el buen uso de la información y la utilización eficiente de los recursos para la toma de decisiones.

Objetivos Específicos

- Conocer y comprender los fundamentos teóricos de Tecnologías de Información y su aplicabilidad en la gestión empresarial.

- Identificar las debilidades de las áreas analizadas, y proponer acciones correctivas.

- Establecer la metodología adecuada para la Administración de Riesgos de Tecnologías de Información.

- Determinar los principales controles y seguridades que deben implementarse en las actividades desarrolladas por el área operativa, de los distintos departamentos de la organización.

- Promover las operaciones metódicas, económicas, eficientes y eficaces, acorde con la misión que la organización debe cumplir.

MARCO METODOLÓGICO

Fundamentación Teórica

Tipo de Estudio

La investigación que se está llevando a cabo es una investigación teórica-explicativa dado que intenta indagar un aspecto de la realidad, explicando su significatividad dentro de una teoría de referencia, a la luz de leyes o generalizaciones que dan cuenta de hechos o fenómenos que se producen en determinadas condiciones.

Métodos de Investigación

El método a ser utilizado es el método hipotético-deductivo. El método hipotético-deductivo es el procedimiento que sigue el investigador para hacer de su actividad una práctica científica. El método hipotético-deductivo tiene varios pasos esenciales: observación del fenómeno a estudiar, creación de una hipótesis para explicar dicho fenómeno, deducción de consecuencias o proposiciones más elementales que la propia hipótesis, y verificación o comprobación de la verdad de los enunciados deducidos comparándolos con la experiencia. Este método obliga al investigador a combinar la reflexión racional o momento racional (la formación de hipótesis y la deducción) con la observación de la realidad o momento empírico (la observación y la verificación). Es decir se formulan hipótesis con el fin de explicar lo que nos intriga, en este caso la importancia de la Administración de Riesgos de Tecnología de Información como mecanismo para optimizar el Análisis de los Estados Financieros en una importadora de maquinaria y equipos de oficinas.

Diagnóstico

Técnicas e instrumentos de procesamiento de la información

Fuentes Primarias

Como fuente primaria para la obtención de información se tiene las encuestas realizadas a administradores, gerentes, líderes y conocedores de la materia a la que se refiere la presente investigación.

Después de revisar y analizar algunos respuestas obtenidas de los cuestionarios realizadas con relación a la Administración de Riesgos de TI, se puede decir que esta administración de riesgos nos permite definir la forma sistemática de como las empresas han visto la necesidad de administrar los riesgos en todos y cada uno de sus operaciones diarias. Dicha administración se debe establecer con el objeto de reducir el riesgo de dar información errónea a la gerencia.

Para evaluar la eficiencia de cualquier conjunto de procedimiento de administración, es necesario definir los objetivos a cumplir. La mayoría de los encuestados expresan que **"la administración de riesgo aplicado de la gestión tiene por meta la mejora de los resultados ligados a los objetivos."** Esto deduce la importancia que tiene la administración de riesgos. Es bueno resaltar que si la Administración de Riesgo de Tecnología de Información se aplica de una forma ordenada y organizada, entonces existirá una información clara, precisa y oportuna, la cual vendría a constituir una administración de riesgo más efectiva.

Fuentes Secundarias

Monografías, libros, folletos, internet

La administración de riesgos es el término asociado al conjunto de pasos secuenciales, lógicos y sistemáticos que debe seguir el analista de riesgos para identificar, valorar y manejar los riesgos asociados a los procesos de TI de la organización, los cuales ejecutados en forma organizada, le permiten encontrar soluciones reales a los riesgos detectados, minimizando las pérdidas o maximizando las oportunidades de mejora.

Técnicas para el análisis de la información

Se debe decidir cuál es la inversión razonable en seguridad y en control de Tecnología de Información y cómo lograr un balance entre riesgos e inversiones en el enfoque de control, en un ambiente de Tecnología de Información, frecuentemente impredecible. Mientras la seguridad y los controles en los sistemas de información ayudan a administrar los riesgos sin eliminarlos, surge la necesidad de administrar

esos riesgos. Puesto que el exacto nivel de riesgo nunca puede ser conocido ya que siempre existe un grado de incertidumbre.

La Administración debe decidir el nivel de riesgo que está dispuesta a aceptar. Debe juzgar cual puede ser el nivel tolerable, particularmente si se tiene en cuenta el costo-beneficio, esto puede ser una decisión difícil para la Administración. Por esta razón, la Administración necesita un marco de referencia de las prácticas generalmente aceptadas de control y seguridad de Tecnología de información para compararlos frente al ambiente de Tecnología de Información existente y planeado.

Existe una creciente necesidad entre los usuarios de los servicios de Tecnología de Información, de estar protegidos a través de la acreditación y la auditoría de servicios de Tecnología de Información proporcionados internamente o por terceras partes, que aseguren la existencia de controles y seguridades adecuadas. Actualmente; sin embargo, es confusa la implementación de buenos controles de Tecnología de Información en sistemas de negocios por parte de entidades comerciales, entidades sin fines de lucro o entidades gubernamentales. Esta confusión proviene de los diferentes métodos de evaluación, como las evaluaciones ISO-9000, nuevas evaluaciones de control interno COSO, COBIT, entre otras. Como efecto, los usuarios necesitan que se establezca una base general como un primer paso.

ÍNDICE DE GRÁFICOS

ÍNDICE

CAPÍTULO I

1. FUNDAMENTOS DE ADMINISTRACIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN

En éste capítulo se da una introducción a lo que son las Tecnologías de Información y su uso en las empresas hoy en día. Podremos ver como las Tecnologías de Información han venido a ocupar una parte principal en cualquier organización que pretenda sobresalir en los mercados tan competidos actualmente. Mucha gente no sabe cómo utilizar las Tecnologías de Información en la administración de su empresa, y la gran mayoría no sabe siquiera de que herramientas puede utilizar para coordinar y controlar eficientemente a su negocio, además se presenta una clara clasificación de lo que son las Tecnologías de Información.

1.1. Tecnología de Información

El avance tecnológico así como: el internet, las comunicaciones móviles, banda ancha, satélites, microondas, etc., están produciendo cambios significativos en la estructura económica y social, y en el conjunto de las relaciones sociales.

La información se ha convertido en el generador de cambios sociales, económicos y culturales. El incremento de las telecomunicaciones ha producido una transformación de las tecnologías de la información, cuyo impacto ha afectado a todos los sectores de la economía y de la sociedad.

La expansión de redes informáticas ha hecho posible la universalización de los intercambios y relaciones, al poner en comunicación a amplios sectores de ciudadanos residentes en espacios geográficos muy distantes entre sí.

La información ha contribuido a que los acontecimientos que se suceden a escala mundial, continental o nacional nos resulten más cercanos por lo que nuestra visión del mundo está adquiriendo una nueva dimensión por encima de países, comunidades y localidades, lo mismo que le sucede a las empresas. Estamos ante un nuevo modelo social, la sociedad globalizada, en el que las fronteras desaparecen en beneficio de los intercambios de ideas, mensajes, productos, servicios y personas.

> La Tecnología de la Información (TI) se entiende como aquellas herramientas y métodos empleados para recabar, retener o distribuir información. La tecnología de la información se encuentra generalmente asociada con las computadoras y las tecnologías para el manejo y procesamiento de información, donde se transformará y se almacenarán datos e información para la toma de decisiones.[1]

La tecnología de la Información está cambiando la forma tradicional de hacer las cosas, en el gobierno, en las empresas privadas, o aquellas personas que trabajan en cualquier campo utilizan las TI cotidianamente mediante el uso de internet, las tarjetas de crédito, el pago electrónico de la nómina, entre otras funciones; es por eso que la función de las TI en los procesos de la empresa como manufactura y ventas se han expandido considerablemente.

La información aporta un enfoque integrado y completo a las empresas. Las empresas y organizaciones dependen de los órdenes económicos, industriales y sociales, puesto que si las tendencias tecnológicas y los entornos económicos e industriales cambian, deben adaptarse a las nuevas circunstancias para sobrevivir. Una de las tendencias actuales más significativas es la que se dirige desde una Sociedad Industrial hacia la llamada Sociedad de Información.

1.1.1. Evolución de la Tecnología de la Información

Los orígenes de las TI aparecen a mediados del siglo XX, durante la segunda guerra mundial. Las diferentes etapas históricas por las que ha atravesado la tecnología han marcado importantes acontecimientos en la historia de la documentación. Al mismo tiempo, el crecimiento de la información y la evidente necesidad de su tratamiento, han provocado la difusión de líneas de investigación en el campo de las Tecnologías de la Información.

Pero es en los últimos 20 años donde ha alcanzado niveles de uso y aplicaciones tan variadas, que se ha convertido en un área de gran amplitud e impacto en todos los

[1] JIMÉNEZ, Jorge, *Sistemas informáticos contables,* http://www.monografias.com/trabajos48

aspectos de la vida cotidiana incluyendo la gerencia de cualquier empresa, por lo que hoy en día es casi indispensable.

La principal clave de las TI es el factor humano, así como también: el diseño de los sistemas, los contenidos de la información, el equipamiento, la infraestructura material, el software y los mecanismos de intercambio electrónico de información, los elementos de política y regulaciones y los recursos financieros.

Estos componentes son los principales protagonistas del desarrollo informático, en una sociedad tanto para su progreso como para su aplicación, además se reconoce como las tecnologías de la información constituyen el núcleo central de una transformación que experimenta la economía y la sociedad, ya que tiende a modificar no sólo sus hábitos y patrones de conducta, sino, incluso, su forma de pensar.

Los factores clave han sido:

- **La computación,** basada en computadoras usadas para adquirir, almacenar, manipular y transmitir información a la gente y unidades de negocios tanto internas como externas.
- Los avances en **las telecomunicaciones** han provocado explosión del uso de las redes de alcances locales y globales.
- **El procesamiento de datos** desarrollado para mejorar su manejo e integración de las necesidades de procesamiento de información en todas las áreas funcionales de la empresa.

Las Tecnologías de Información comprenden todas las tecnologías basadas en computadora y comunicaciones por computadora, usadas para adquirir, almacenar, manipular y transmitir información a la gente y unidades de negocios tanto internas como externas.

Estos factores hacen que cada día los costos se reduzcan y por tanto se amplíe el uso de estos medios en otros sectores, como en el empresarial, en la salud, la educación, hasta incluso en los propios hogares.

La TI es esencial para mejorar la productividad de las empresas, aunque su aplicación debe llevarse a cabo de forma inteligente. El hecho de introducir tecnología en los procesos empresariales no es garantía de un aumento de la productividad. Para que la implantación de nueva tecnología produzca rentabilidad hay que cumplir varios requisitos: tener un conocimiento profundo de los procesos de la empresa, planificar detalladamente las necesidades de tecnología de la información e incorporar los sistemas tecnológicos paulatinamente, empezando por los más básicos. La mayor productividad se consigue mediante una reducción de los costes y el aumento de las ventas, así como mediante una reducción del activo, del pasivo y de los empleados.

1.1.2. Importancia de la Tecnología de la Información

Las TI han cambiado la forma en que operan las organizaciones actuales. A través de su uso se logran importantes mejoras, pues automatizan los procesos operativos, suministran una plataforma de información necesaria para la toma de decisiones y, lo más importante, su implantación logra ventajas competitivas, éxitos en sus objetivos o reducir la ventaja de los competidores. De esta forma, constituye un campo esencial de estudio en administración y gerencia de empresas.

Las TI se han convertido en el éxito empresarial en el entorno global y dinámico de hoy. Por lo tanto, la administración apropiada de las TI es un reto importante para los gerentes. Así, la función de las TI representa:

- Un área funcional principal dentro de la empresa, para el éxito empresarial como las funciones de contabilidad, finanzas, administración de operaciones, marketing y administración de recursos humanos.
- Una ayuda para le eficiencia operacional, la productividad del empleado; y, el servicio y satisfacción del cliente.
- Una fuente de información y respaldo importante para la toma de decisiones efectivas por parte de los gerentes.

- Un elemento para el desarrollo de productos y servicios competitivos que den a las organizaciones una ventaja estratégica en el mercado global.
- Una oportunidad profesional esencial, dinámica y retadora para millones de hombres y mujeres.

Utilizando eficientemente las TI se pueden obtener ventajas competitivas, pero es preciso encontrar procedimientos acertados para mantener tales ventajas, así como disponer de cursos y recursos alternativos de acción para adaptarlas a las necesidades del momento, pues las ventajas no siempre son permanentes. El sistema de información tiene que modificarse y actualizarse con regularidad si se desea percibir ventajas competitivas continuas. El uso creativo de las TI puede proporcionar a los administradores una nueva herramienta para diferenciar sus recursos humanos, productos y/o servicios respecto de sus competidores.

1.1.3. Tipos de Tecnologías

A continuación se definen los tres tipos de tecnologías vigentes en la actualidad. Estos son:

1.1.3.1. Tecnologías Aplicables

Las TI, como muchas otras tecnologías, han cambiado paulatinamente su papel en las organizaciones:

En los comienzos del desarrollo de las TI, ésta se utilizaba para realizar tareas rutinarias y repetitivas, por ejemplo: impresiones de listas “sábanas” fuera de horario de atención.

A medida que transcurrió el tiempo, la tecnología se hizo más permisiva económicamente y empezó a realizar tareas más completas y complejas: libros contables, facturación, etc.

Luego de esto, las TI empiezan a integrar todas las actividades de la empresa, tratando de convertirse en una herramienta de soporte para la toma de decisiones y para el logro de objetivos estratégicos. Su costo de obtención sigue disminuyendo y ya no se la considera como un costo inherente a las actividades, sino como una inversión.

Hoy en día, las posibilidades que las TI nos da, es la de ser en sí misma la ventaja competitiva del negocio, los costos de obtención han disminuido exponencialmente, y es considerada para la empresa, junto con el sistema de información, como un activo más. [2]

Por lo tanto, las TI juega también un papel importante, no sólo como herramienta de implementación de partes del sistema de información, sino por las oportunidades que por sí misma abre a las empresas.

1.1.3.2. Tecnologías Necesarias

La tecnología es importante para la competencia si afecta de manera significativa la ventaja competitiva de la empresa. Por tanto, la tecnología es más o menos necesaria siempre en función de los objetivos estratégicos que persiga el negocio.

La decisión de una empresa de descartar su propia tecnología puede ser difícil, pero esta elección puede ser esencial para mantener la posición competitiva de la empresa.

En consecuencia, las tecnologías necesarias de ser desarrolladas en la empresa serán, ni más ni menos, aquellas que contribuirán directamente al logro de los objetivos estratégicos del negocio.

[2] Estrategia Magazine, *Sistema de información y tecnología de la información. Parte II*, http://www.gestiopolis.com/administracion-estrategia/estrategia/sistemas-y-tecnologias-de-la-informacion-2.htm

1.1.3.3. Tecnologías Deseadas

La tecnología de información implica cambios, como por ejemplo: usar impresoras para realizar una factura, en lugar de realizarla a mano; los vendedores de tiendas virtuales que han tenido que aprender nuevos métodos de inducción a la compra mediante Internet, entre otros.

Y los cambios, hoy en día, pueden verse desde dos puntos de vistas: amenazas del medio que prometen efectos negativos u oportunidades de negocio que implican futuras fortalezas; y dado que actualmente "el cambio es una constante", deberíamos capitalizarlo de la forma que más nos convenga, a pesar de que al principio pareciera natural del ser humano la resistencia a él.

Por tanto, el uso de las nuevas tecnologías a menudo no es deseado por parte de la gente que debe sacrificar las "viejas formas de hacer las cosas" para aceptar los cambios que éste trae consigo. Los individuos han de estar dispuestos al cambio, interesarse en aprender y querer ser diferentes. Es papel del líder crear condiciones para que eso ocurra.

1.2. Riesgos

1.2.1. Concepto

El concepto de riesgo está íntimamente relacionado al de incertidumbre, o falta de certeza, de algo que pueda acontecer y generar una pérdida del mismo.

En lo relacionado con tecnología, generalmente el riesgo se plantea como amenaza, determinando el grado de exposición a la ocurrencia de una pérdida (por ejemplo el riesgo de perder datos debido a la rotura de un disco de almacenamiento, virus informáticos, etc.).

1.2.2. Clasificación de Riesgos

1.2.2.1. Riesgo de Negocios

Es el riego de los negocios estratégicos de la empresa y de sus procesos claves. En otras palabras es un riesgo crítico de la empresa.

1.2.2.2. Riesgo de Auditoría

Existe al aplicar los programas de auditoría, cuyos procedimientos no son suficientes para descubrir errores o irregularidades significativas.

1.2.2.3. Riesgo Inherente

El riesgo inherente es la tendencia de un área de Tecnología de Información a cometer un error que podría ser material, en forma individual o en combinación con otros, suponiendo la inexistencia de controles internos relacionados.

Por ejemplo, el riesgo inherente asociado a la seguridad del sistema operativo es normalmente alto dado que los cambios en los datos o programas, o aun su divulgación, a través de las deficiencias en la seguridad del sistema operativo podrían tener como resultado una desventaja competitiva o información de gestión falsa.

El riesgo inherente para la mayoría de las áreas de auditoría de TI es normalmente alto dado que, por lo general, el posible efecto de los errores se extiende a varios sistemas de negocios y a un gran número de usuarios.

1.2.2.4. Riesgo de Control

Es el riesgo por el que un error, que podría cometerse en un área de auditoría y que podría ser material, individualmente o en combinación con otros, no pueda ser evitado o detectado y corregido oportunamente por el sistema de control interno.

Por ejemplo, el riesgo de control asociado a las revisiones manuales de registros computadorizados es normalmente alto debido a que las actividades que requieren investigación a menudo se pierden con facilidad por el volumen de información registrada. El riesgo de control asociado a los procedimientos computarizados de validación de datos es normalmente bajo puesto que los procesos se aplican con regularidad.

El Auditor Interno debe evaluar el riesgo de control como un riesgo alto a menos que los controles internos pertinentes:

- Se identifiquen
- Se consideren eficaces
- Se prueben y confirmen como adecuadamente operativos (pruebas de cumplimiento)

1.2.2.5. Riesgo de Detección

Es el riesgo que se produce cuando los procedimientos sustantivos del Auditor Interno no detectan un error que podría ser material, individualmente o en combinación con otros.

Por ejemplo, el riesgo de detección asociado a la identificación de violaciones de la seguridad en un sistema de aplicación es normalmente alto, debido a que en el transcurso de la auditoría, los registros de todo su período no se encuentran disponibles. El riesgo de detección asociado con la identificación de la falta de planes de recuperación ante desastres es normalmente bajo, dado que su existencia puede verificarse con facilidad.

Al determinar el nivel de pruebas sustantivas requeridas, el Auditor Interno debe tener en cuenta:

- La evaluación del riesgo inherente.

- La conclusión sobre riesgos de control a la que se llega luego de las pruebas de cumplimiento.

Cuanto más exhaustiva es la evaluación del riesgo inherente y de control, mayor es la evidencia de auditoría que debería obtener el Auditor Interno mediante la ejecución de los procedimientos sustantivos de auditoría.

1.2.2.6. Riesgo Estratégico

Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con el cumplimiento de la misión de la Entidad, la cual busca la vigilancia de la conducta de los servidores públicos, defender el orden jurídico y los derechos fundamentales.

1.2.2.7. Riesgo Operativo

Comprende tanto el riesgo en sistemas como operativo provenientes de deficiencias en los sistemas de información, procesos, estructura, que conducen a ineficiencias, oportunidad de corrupción o incumplimiento de los derechos fundamentales.

1.2.2.8. Riesgo Financiero

Se relaciona con las exposiciones financieras de la empresa. El manejo del riesgo financiero toca actividades de tesorería, presupuesto, contabilidad y reportes financieros, entre otros.

1.2.2.9. Riesgo de Tecnología

Se asocia con la capacidad de la empresa en que la tecnología disponible satisfaga las necesidades actuales y futuras de la empresa y soporten el cumplimiento de la misión.

1.2.3. Valoración del Riesgo

La valoración del riesgo consta de tres etapas: La identificación, el análisis y la determinación del nivel del riesgo. Para cada una de ellas es necesario tener en cuenta la mayor cantidad de datos disponibles y contar con la participación de las personas que ejecutan los procesos y procedimientos, para lograr que las acciones determinadas alcancen los niveles de efectividad esperados. Para adelantarlas, deben utilizarse las diferentes fuentes de información.

1.2.4. Identificación del Riesgo

El proceso de la identificación del riesgo debe ser permanente, integrado al proceso de planeación y responder a las preguntas qué, cómo y por qué se pueden originar hechos que influyen en la obtención de resultados.

Una manera de realizar la identificación del riesgo es a través de la elaboración de un mapa de riesgos, el cual como herramienta metodológica permite hacer un inventario de los mismos ordenada y sistemáticamente, definiendo en primera instancia los riesgos, posteriormente presentando una descripción de cada uno de ellos y las posibles consecuencias.

1.2.5. Análisis del Riesgo

1.2.5.1. Objetivo General del Análisis de Riesgo

Su objetivo es establecer una valoración y priorización de los riesgos con base en la información ofrecida por los mapas elaborados en la etapa de identificación, con el fin de clasificar los riesgos y proveer información para establecer el nivel de riesgo y las acciones que se van a implementar.

Se han establecido dos aspectos para realizar el análisis de los riesgos identificados:

Probabilidad: La posibilidad de ocurrencia del riesgo, la cual puede ser medida con criterios de frecuencia o teniendo en cuenta la presencia de factores internos y externos que puedan propiciar el riesgo, aunque éste no se haya presentado nunca.
Para el análisis cualitativo se establece una escala de medida cualitativa en donde se establecen unas categorías a utilizar y la descripción de cada una de ellas, con el fin de ponderar el análisis de riesgos, por ejemplo:

ALTA: Es muy factible que el hecho se presente

MEDIA: Es factible que el hecho se presente

BAJA: Es poco factible que el hecho se presente

Impacto: Consecuencias que puede ocasionar a la organización la materialización del riesgo.

Ese mismo diseño puede aplicarse para la escala de medida cualitativa de IMPACTO, estableciendo las categorías y la descripción, por ejemplo:

ALTO: Si el hecho llegara a presentarse, tendría alto impacto o efecto sobre la entidad.

MEDIO: Si el hecho llegara a presentarse tendría medio impacto o efecto en la entidad.

BAJO: Si el hecho llegara a presentarse tendría bajo impacto o efecto en la entidad.

1.2.5.2. Objetivos Específicos del Análisis de Riesgo

- Analizar el tiempo, esfuerzo y recursos disponibles y necesarios para atacar los problemas.
- Definir cuáles son los recursos existentes.
- Llevar a cabo un minucioso análisis de los riesgos y debilidades.

- Identificar, definir y revisar todos los controles de seguridad ya existentes.
- Determinar si es necesario incrementar las medidas de seguridad, los costos del riesgo y los beneficios esperados.

1.2.6. Administración de Riesgos

En la economía global, las organizaciones necesitan tomar riesgos para sobrevivir, la mayoría de ellas necesitan incrementar el nivel de riesgos que toman para ser exitosas a largo plazo. Con el significativo incremento en la competencia, los objetivos y metas agresivos de las corporaciones se están convirtiendo en norma. Para direccionar este cambio, los líderes mundiales están fortaleciendo sustancialmente sus prácticas de administración de riesgos para asegurar que si las iniciativas o el funcionamiento de las unidades de negocio "se descarrilan", esto se identifique rápidamente para poder actuar y corregir la situación.

1.2.6.1. Definición de Administración de Riesgos

Es un proceso interactivo e iterativo basado en el conocimiento, evaluación y manejo de los riesgos y sus impactos, con el propósito de mejorar la toma de decisiones organizacionales.

Es aplicable a cualquier situación donde un resultado no deseado o inesperado pueda ser significativo o donde se identifiquen oportunidades de mejora.

1.2.6.2. Beneficios para la Organización

- Facilita el logro de los objetivos de la organización.
- Hace a la organización más segura y consciente de sus riesgos.
- Mejoramiento continuo del Sistema de Control Interno.
- Optimiza la asignación de recursos.
- Aprovechamiento de oportunidades de negocio.
- Fortalece la cultura de autocontrol.

- Mayor estabilidad ante cambios del entorno.

1.2.6.3. Beneficios para el Departamento de Auditoría

- Soporta el logro de los objetivos de la auditoria.
- Estandarización en el método de trabajo.
- Integración del concepto de control en las políticas organizacionales.
- Mayor efectividad en la planeación general de Auditoría.
- Evaluaciones enfocadas en riesgos.
- Mayor cobertura de la administración de riesgos.
- Auditorías más efectivas y con mayor valor agregado.

1.2.6.4. Factores a considerar

Los principales factores que se deben considerar en la Administración de Riesgos de TI son:

- Seguridades
- Controles: Preventivos, Detectivos y Correctivos
- Objetivos
- Manuales de usuarios
- Políticas

Si no existe una adecuada consideración de los factores antes descritos y si nuestros controles y seguridades fueran errados, nuestros planes organizacionales, financieros, administrativos y de sistemas se verían seriamente afectados, ya que no sólo el área de sistemas será el afectado.

1.3. Riesgos de Tecnología de Información

1.3.1. Concepto

El concepto de riesgo de TI puede definirse como el efecto de una causa multiplicado por la frecuencia probable de ocurrencia dentro del entorno de TI. Es el control el que actúa sobre la causa del riesgo para minimizar sus efectos. Cuando se dice que los controles minimizan los riesgos, lo que en verdad hacen es actuar sobre las causas de los riesgos, para minimizar sus efectos.

La Organización Internacional por la Norma (ISO) define *riesgo tecnológico* como:

"La probabilidad de que una amenaza se materialice, utilizando vulnerabilidad existentes de un activo o grupo de activos, generándole pérdidas o daños". [ISO-13335-1:2004][3]

En la definición anterior se pueden identificar los siguientes elementos que son: probabilidad, amenazas, vulnerabilidades, activos e impactos llamados también daños.

A continuación se analiza cada uno de ellos:

Probabilidad: establecer la probabilidad de ocurrencia puede realizarse de manera cuantitativa o cualitativa, pero siempre debe considerarse en cada caso qué posibilidades existen que la amenaza se presente independientemente del hecho que sea o no contrarrestada.

Existen amenazas, como por ejemplos incendios, para las cuales hay información suficiente (series históricas, compañías de seguros y otros datos) para establecer con razonable objetividad su probabilidad de ocurrencia.

[3] ISO/IEC 13335-1:2004, Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management, 2004.

Amenazas: las amenazas siempre existen y son aquellas acciones que pueden ocasionar consecuencias negativas en la operativa de la empresa. Comúnmente se indican como amenazas a las fallas, a los ingresos no autorizados, a los virus, uso inadecuado de software, los desastres ambientales como terremotos e inundaciones, accesos no autorizados, facilidad de acceso a las instalaciones, etc.

Las amenazas pueden ser de carácter físico o lógico, como ser una inundación en el primer caso, o un acceso no autorizado a una base de datos en el segundo caso.

Vulnerabilidades: son ciertas condiciones inherentes a los activos o presentes en su entorno que facilitan que las amenazas se materialicen llevan a sus activos a ser vulnerables.

Mediante el uso de las debilidades existentes es que las amenazas logran materializarse, pero sin la identificación de una vulnerabilidad no podrán ocasionar ningún impacto.

Estas vulnerabilidades son de naturaleza variada. Por ejemplo: la falta de conocimiento del usuario, tecnología inadecuadamente probada, transmisión por redes públicas, etc.

Una vulnerabilidad común es contar con un antivirus no actualizado, la cual permitirá al virus actuar y ocasionar daños. Si el antivirus estuviese actualizado, el virus no podría materializarse.

Activos: los activos son aquellos relacionados con los sistemas de información. Por ejemplo: los datos, el software, el hardware, servicios, documentos, edificios y recursos humanos.

Impactos: las consecuencias de la ocurrencia de las distintas amenazas son siempre negativas. Las pérdidas generadas pueden ser financieras, no financieras de corto plazo o de largo plazo.

Las más comunes son: la pérdida directa de dinero, la pérdida de confianza, la reducción de la eficiencia y la pérdida de oportunidades de negocio.

1.3.2. Tipos de Causas de Riesgos de TI

Las causas de riesgo más comunes, para efectos del tema, se dividen en:

- Externas e
- Internas.

Las causas de riesgo externas pueden ser de dos clases:

- Naturales y
- Motivadas por el Hombre.

Las causas de riesgo naturales son normalmente las siguientes:

- Inundaciones
- Temblores
- Tornados
- Tormentas Eléctricas
- Huracanes
- Erupciones Volcánicas

Las causas de riesgo originadas por el hombre, son entre otras, las siguientes:

- Incendios
- Explosiones
- Accidentes laborales
- Destrucción intencional
- Sabotaje
- Robo
- Fraude

- Contaminación Ambiental

Las causas internas de riesgo se generan a partir de las mismas empresas, siendo más frecuentes las causas internas de riesgo que las causas externas.

Entre las causas internas de riesgo tenemos básicamente:

- Hurto: de materiales, de dinero y de información
- Sabotaje
- Insuficiencia de Dinero
- Destrucción: de datos y de recursos
- Personal No capacitado
- Huelgas
- Fraudes
- Ausencia de seguridades físicas tanto de la empresa como de la información.

1.4. Administración de Riesgos de Tecnología de Información

1.4.1. Concepto

La Administración de Riesgos de TI es el proceso continuo basado en el conocimiento, evaluación, manejo de los riesgos y sus impactos que mejora la toma de decisiones organizacionales, frente a los riesgos de TI.

Es entonces la administración de riesgos el término asociado al conjunto de pasos secuenciales, lógicos y sistemáticos que debe seguir el analista de riesgos para identificar, valorar y manejar los riesgos asociados a los procesos de TI de la organización, los cuales ejecutados en forma organizada le permiten encontrar soluciones reales a los riesgos detectados minimizando las pérdidas o maximizando las oportunidades de mejora.

1.4.2. Beneficios

Se pueden mencionar los siguientes beneficios:

A nivel organizacional:

- Alcance o logro de los objetivos organizacionales.
- Énfasis en prioridades de negocio: permite a los directivos enfocar sus recursos en los objetivos primarios. Tomar acción para prevenir y reducir pérdidas, antes que corregir después de los hechos, es una estrategia efectiva de administración del riesgo.
- Fortalecimiento del proceso de planeación.
- Apoyo en la identificación de oportunidades.
- Fortalecimiento de la cultura de autocontrol.

Al proceso de administración:

- Cambio cultural que soporta discusiones abiertas sobre riesgos e información potencialmente peligrosa. La nueva cultura tolera equivocaciones pero no tolera errores escondidos. La nueva cultura también hace énfasis en el aprendizaje de los errores.
- Mejor administración financiera y operacional al asegurar que los riesgos sean adecuadamente considerados en el proceso de toma de decisiones. Una mejor administración operacional generará servicios más efectivos y eficientes. Anticipando los problemas, los directivos tendrán mayor oportunidad de reacción y tomar acciones. La organización será capaz de cumplir con sus promesas de servicio.
- Mayor responsabilidad de los administradores en el corto plazo. A largo plazo, se mejorarán todas las capacidades de los directivos.

1.4.3. Características Generales

- La Administración de Riesgos debe estar apoyada por la Alta Gerencia de la Organización.
- La Administración de Riesgos debe ser parte integral del proceso administrativo utilizado por la Dirección de la Organización.
- La Administración de Riesgos es un proceso multifacético y participativo, el cual es frecuentemente mejor llevado a cabo por un equipo multidisciplinario.

1.4.4. Establecimiento de la Metodología de TI

Permite, a través del conocimiento del entorno y de la organización, establecer criterios generales que serán utilizados para implementar el enfoque de Administración de Riesgos de TI en el área de sistemas de la Organización.

Durante esta etapa se debe establecer la metodología que será utilizada para la Administración de Riesgos de TI en el área de sistemas de la empresa.

Consiste en analizar los riesgos existentes en el área y de acuerdo a este análisis, determinar cuál de las alternativas propuestas (metodologías) va a ser la mejor opción para la realización del trabajo.

1.4.5. Identificación de Riesgos de TI

Mediante el establecimiento de un marco de acción específico se puede entender el objeto sobre el cual se aplicará el proceso de Administración de Riesgos de TI.

El propósito final de esta etapa es proveer los mecanismos necesarios para recopilar la información relacionada con los riesgos, impactos y sus causas.

Algo importante en esta etapa, es tener claro la definición de Riesgo.

Para la mayoría de partes, los riesgos son percibidos como cualquier cosa o evento que podría apoyar la forma en que la organización alcance sus objetivos.

Por consiguiente, la Administración de Riesgos de TI no está dirigida exclusivamente a evitarlos. Su enfoque está en identificar, evaluar, controlar y "dominar" los riesgos.

1.4.6. Análisis del Riesgos de TI

En esta etapa se busca obtener el entendimiento y conocimiento de los riesgos identificados de tal manera que se pueda recopilar información que permita el cálculo del nivel de riesgo al cual está expuesto el objeto, Identificar los controles existentes implementados para mitigar el impacto ante la ocurrencia de los riesgos de TI, permitiendo de esta manera valorar los niveles del riesgo, la efectividad de los controles y el nivel de exposición.

El riesgo de TI es analizado a través de la combinación de estimativos de probabilidad y de las consecuencias en el contexto de las medidas de control existentes. El análisis de riesgos de TI involucra un debido examen de las fuentes de riesgo, sus consecuencias y la probabilidad de que esas consecuencias puedan ocurrir. Pueden llegar a identificarse factores que afectan tanto las consecuencias como la probabilidad.

Los estimativos pueden determinarse utilizando análisis, estadísticas y cálculos. Alternativamente donde no hay datos históricos disponibles, se pueden hacer estimativos subjetivos que reflejen el grado de creencia de un grupo o de un individuo en que un evento en particular o suceso ocurran.

1.4.7. Evaluación y Priorización de Riesgos de TI

La evaluación de riesgos de TI incluye comparar el nivel de riesgo encontrado durante el proceso de análisis contra el criterio de riesgo establecido previamente, y decidir si los riesgos pueden ser aceptados.

El análisis de riesgos y los criterios contra los cuales los riesgos son comparados en la valoración deben ser considerados sobre la misma base. Así, evaluaciones cualitativas incluyen la comparación de un nivel cualitativo de riesgo contra criterios cualitativos, y evaluaciones cuantitativas involucran la comparación de niveles estimados de riesgo contra criterios que pueden ser expresados como números específicos, tales como fatalidad, frecuencia o valores monetarios.

El resultado de una evaluación de riesgos es una lista priorizada de riesgos para definirles acciones de tratamiento posteriores.

Para evaluar riesgos hay que considerar, entre otros factores, el tipo de información almacenada, procesada y transmitida, la criticidad de las aplicaciones, la tecnología usada, el marco legal aplicable, el sector de la entidad, la entidad misma y el momento.

1.4.8. Tratamiento de Riesgos de TI (Controles Definitivos)

Después de valorar y priorizar los riesgos de TI, y dependiendo del nivel de exposición, se debe determinar la opción de tratamiento que más conviene aplicar en cada caso. El tratamiento de riesgos de TI incluye la identificación de la gama de opciones de tratamiento del riesgo de TI, la evaluación de las mismas, la preparación de planes de tratamiento de riesgos de TI y su posterior implementación por parte de la Gerencia de la empresa.

Las opciones de tratamiento que se relacionan a continuación no son mutuamente exclusivas ni serán apropiadas en todas las circunstancias:

EVITAR el riesgo: Se decide, donde sea práctico, no proceder con procesos y/o actividades que podrían generar riesgos inaceptables, buscando con ello eludir el riesgo inherente asociado a esos objetos.
Es siempre la primera alternativa que debe considerarse.

REDUCIR el riesgo: La organización decide prevenir y/o reducir el riesgo de TI. Si el riesgo no se puede evitar porque crea grandes dificultades en el departamento, el

siguiente paso es reducirlo al más bajo nivel posible, el cual debe ser compatible con las actividades del área. Se consigue mediante la optimización de los procedimientos y la implementación de controles.

- **REDUCIR la probabilidad de ocurrencia:** Prevención del riesgo a través de la implementación de acciones tendientes a controlar su frecuencia o probabilidad.

- **REDUCIR las consecuencias o MITIGAR el riesgo:** reducción del riesgo a través de la implementación de acciones o medidas de control dirigidas a disminuir el impacto o severidad de las consecuencias del riesgo si éste ocurre.

ASUMIR el riesgo: La organización decide aceptar los riesgos como ellos existen en la actualidad, y establece políticas o estrategias apropiadas para su tratamiento.

Otra manera de ASUMIR los riesgos, pero debe hacerse a un nivel adecuado en la entidad y considerando que puede ser mucho mayor el costo de la inseguridad que el de la seguridad, lo que a veces sólo se sabe cuando ha ocurrido algo. ¿Cuál es el riesgo máximo admisible que puede permitirse una entidad? Alguna vez se nos ha hecho la pregunta, y depende de lo crítica que sea para la entidad la información así como disponer de ella, e incluso puede depender del momento.

Riesgo Residual: Según la norma ISO 27000, es el riesgo que permanece tras el tratamiento del riesgo, es decir, después de que se hayan tomado las medidas de seguridad.

Sin embargo, si acudimos a la norma 27005 ésta deja bien claro que este riesgo residual no se refiere al riesgo efectivo tras la aplicación de las medidas sino al teórico que se calcula durante el análisis de riesgos en la fase de Plan.

En el siguiente cuadro se muestra un ejemplo para calcular el riesgo residual utilizando escalas numéricas del 1 al 5:

Actividad	Nivel de Riesgo	Calidad de Gestión			Riesgo Residual (**)
		Tipo de medidas de control	Efectividad	Promedio (*)	
Riesgo inherente 1	5	Control 1	3	3.6	1.38
		Control 2	4		
		Control 3	4		
Riesgo inherente 2	4	Control 1	5	4.3	0.93
		Control 2	5		
		Control 3	3		
Riesgo inherente 3	4	Control 1	3	3.6	1.11
		Control 2	4		
		Control 3	4		
Riesgo inherente 4	3	Control 1	5	3.5	0.85
		Control 2	2		
Perfil de Riesgo (Riesgo Residual Total) (***)					**1.06**

(*) Promedio de los datos de Efectividad

(**) Resultado de la división entre nivel de riesgo / Promedio de Efectividad

(***) Promedio: Se considera un mismo peso de ponderación a los Riesgos Inherentes.

1.4.9. Monitoreo y Revisión

Pocos riesgos permanecen estáticos. Por ello, los riesgos y la efectividad de sus medidas de control necesitan ser monitoreados continuamente para asegurar que circunstancias cambiantes no alteren las prioridades.

Revisiones progresivas son esenciales para asegurar que los planes de la administración permanecen relevantes. Los factores que afectan la probabilidad y la consecuencia de un resultado pueden cambiar, al igual que los factores que afectan la viabilidad o el costo de las opciones de tratamiento.

1.5. Normas COBIT (Objetivos de Control para Tecnología de Información y Tecnologías relacionadas)

COBIT,[4] es la herramienta innovadora para el gobierno de TI que ayuda a la gerencia a comprender y administrar los riesgos asociados con tecnologías de información.

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales, mini computadoras y ambientes distribuidos. Está basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

1.5.1. Misión de COBIT

Investigar, desarrollar, publicar y promover un conjunto internacional y actualizado de objetivos de control para tecnología de información que sea de uso cotidiano para gerentes y auditores.[5]

1.5.2. Visión de COBIT

Ser el modelo de control para las Tecnologías de Información.

---

[4] The Information Systems Audit and Control Foundation, ISACA. Es la asociación líder en Auditoría de Sistemas, con 23.000 miembros en 100 países.
ISACA propone la metodología COBIT (Control Objectives for Information and related Technology). Es un documento realizado en el año de 1996 y revisado posteriormente, dirigido a auditores, administradores y usuarios de sistemas de información, que tiene como objetivos de control la efectividad y la eficiencia de las operaciones; confidencialidad e integridad de la información financiera y el cumplimiento de las leyes y regulaciones. El COBIT se desarrolla a través de varios capítulos: planificación y organización, adquisición e implementación, desarrollo, soporte y control.

[5] RIVAS, José, *Informe de auditoría de sistemas: Uso del Cobit*, http://www.monografias.com/trabajos70/informe-auditoria-sistemas-uso-cobit

1.5.3. Regla de oro de COBIT

Para promover la información que requiere la organización para lograr sus objetivos, los recursos de TI, deben ser administrados por un conjunto de procesos, agrupados de forma adecuada y ejecutados acorde a prácticas normalmente aceptadas.

1.5.4. Usuarios de COBIT

- *La Gerencia*: para apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.
- *Los Usuarios Finales*: quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.
- *Los Auditores:* para soportar sus opiniones sobre los controles de los proyectos de TI, su impacto en la organización y determinar el control mínimo requerido.
- *Los Responsables de TI:* para identificar los controles que requieren en sus áreas.
- También puede ser utilizado dentro de las empresas por el responsable de un proceso de negocio en su responsabilidad de controlar los aspectos de información del proceso, y por todos aquellos con responsabilidades en el campo de las TI en las empresas.

1.5.5. Características

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

1.5.6. Niveles de COBIT

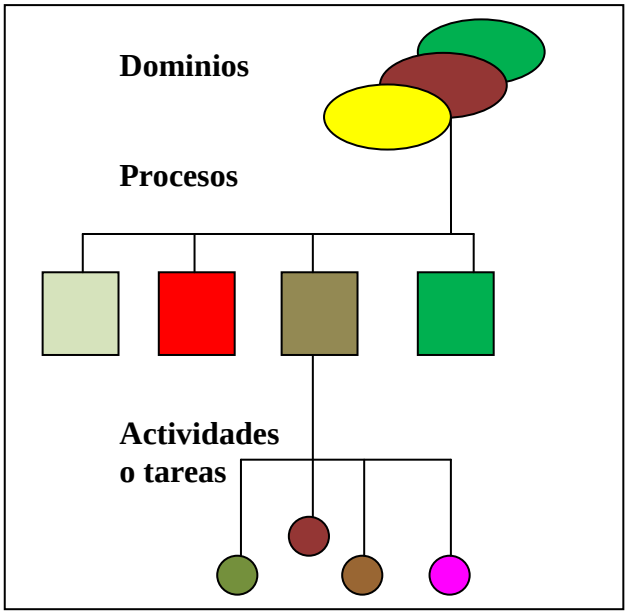
- **Dominio:** Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.

- **Procesos:** Conjuntos o series de actividades unidas con delimitación o cortes de control.

- **Actividades:** Acciones requeridas para lograr un resultado medible.

GRÁFICO Nº 1

NIVELES DE COBIT

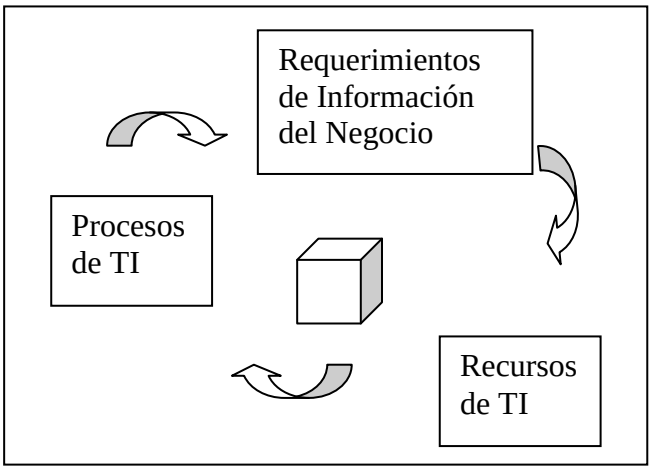


Fuente: ISACA, Principios de COBIT, 2010

1.5.7. Principios de COBIT

GRÁFICO Nª 2

PRINCIPIOS DE COBIT



Fuente: ISACA, Principios de COBIT, 2010

1.5.8. Requerimientos de Información del Negocio

Para satisfacer los objetivos del negocio, la información necesita concordar con ciertos criterios a los que COBIT hace referencia como requerimientos de negocio para la información. Al establecer la lista de requerimientos, COBIT combina los principios contenidos en los modelos referentes existentes y conocidos:

1.5.8.1. Requerimientos de calidad

1) Calidad
2) Costo
3) Oportunidad

1.5.8.2. Requerimientos Fiduciarios (COSO)

1) Efectividad y Eficiencia de operaciones
2) Confiabilidad de la información
3) Cumplimiento de las leyes y regulaciones

1.5.8.3. Requerimientos de Seguridad

4) Confidencialidad
5) Integridad
6) Disponibilidad

1.5.9. Recursos de TI

En COBIT se establecen los siguientes recursos en TI necesarios para alcanzar los objetivos del negocio:

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

1.5.10. Dominios de COBIT

- Planificación y Organización
- Adquisición e Implementación
- Prestación y Soporte
- Monitoreo

1.5.10.1. Planificación y organización

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

Procesos:

- PO1 Definir un Plan Estratégico de TI
- PO2 Definir la Arquitectura de la Información
- PO3 Determinar la Dirección Tecnológica
- PO4 Definir los Procesos, Organización y Relaciones de TI
- PO5 Administrar la Inversión en TI
- PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia
- PO7 Administrar Recursos Humanos de TI
- PO8 Asegurar el cumplimiento con los requerimientos externos
- PO9 Evaluar y Administrar los Riesgos de TI
- PO10 Administrar Proyectos
- PO11 Administrar la Calidad

1.5.10.2. Adquisición e implementación

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

Procesos:

- AI1 Identificar soluciones automatizadas

- AI2 Adquirir y mantener software aplicativo
- AI3 Adquirir y mantener infraestructura tecnológica
- AI4 Facilitar la operación y el uso
- AI5 Adquirir recursos de TI
- AI6 Administrar cambios
- AI7 Instalar y acreditar soluciones y cambios

1.5.10.3. Prestación y soporte

En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

Procesos

- DS1 Definir y administrar los niveles de servicio
- DS2 Administrar los servicios de terceros
- DS3 Administrar el desempeño y la capacidad
- DS4 Garantizar la continuidad del servicio
- DS5 Garantizar la seguridad de los sistemas
- DS6 Identificar y asignar costos
- DS7 Educar y entrenar a los usuarios
- DS8 Administrar la mesa de servicio y los incidentes
- DS9 Administrar la configuración
- DS10 Administrar los problemas
- DS11 Administrar los datos
- DS12 Administrar el ambiente físico
- DS13 Administrar las operaciones

1.5.10.4. Monitoreo

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

Procesos

- ME1 Monitorear y Evaluar el Desempeño de TI
- ME2 Monitorear y Evaluar el Control Interno
- ME3 Garantizar el Cumplimiento Regulatorio
- ME4 Proporcionar Gobierno de TI[6]

1.6. Informe COSO

Los controles internos se diseñan e implantan con el fin de detectar, en un plazo deseado, cualquier desviación respecto a los objetivos de rentabilidad establecidos para cada empresa y de prevenir cualquier evento que pueda evitar el logro de los objetivos, la obtención de información confiable y oportuna y el cumplimiento de leyes y reglamentos.

El control interno se define como un proceso efectuado por el consejo de administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia de las operaciones.
- Confiabilidad de la información financiera.
- Cumplimiento de las leyes y normas aplicables.

[6] GOBIERNO DE TI, es una estructura de relaciones y procesos para dirigir y controlar la empresa con el objeto de alcanzar los objetivos de la organización y añadir valor mientras se equilibran los riesgos y el retorno sobre TI y sus procesos.

La anterior definición refleja ciertos conceptos fundamentales:

- El control interno es un **PROCESO**, un medio utilizado para la consecución de un fin, no un fin en sí mismo.

- El control interno lo llevan a cabo las **PERSONAS**, no se trata solamente de manuales de políticas e impresos, sino de personas en cada nivel de la organización.

- El control interno solo puede aportar un **GRADO DE SEGURIDAD RAZONABLE**, no la seguridad total, a la dirección y al consejo de administración de la entidad.

- El control interno está pensado para facilitar la consecución de **OBJETIVOS** propios de cada entidad.

El control interno consta de cinco componentes relacionados entre sí. Se derivan de la manera en que la dirección dirige la empresa y están integrados en el proceso de dirección.

1.6.1. Ambiente de Control

El ambiente de control marca la pauta del funcionamiento de una organización e influye en la concienciación de sus empleados respecto al control. Es la base de todos los demás componentes del control interno, aportando disciplina y estructura. "Los factores del ambiente de control incluyen integridad, los valores éticos y la capacidad de los empleados en la entidad, la filosofía de dirección y estilo gestión, la manera en que la dirección asigna autoridad y las responsabilidades y organiza y desarrolla profesionalmente a sus empleados y la atención y orientación que proporciona al consejo de administración".[7]

[7] COOPERS & LYBRAND, *Los nuevos conceptos de Control Interno (Informe COSO)*, España, Ediciones Díaz de Santos, pág. 5

1.6.2. Evaluación del Riesgo

Las organizaciones, cualquiera sea su tamaño, se enfrentan a diversos riesgos de origen externos e internos que tienen que ser evaluados. Una condición previa a la evaluación del riesgo es la identificación de los objetivos a los distintos niveles, vinculados entre sí e internamente coherentes. La evaluación de los riesgos consiste en la identificación y el análisis de los riesgos relevantes para la consecución de los objetivos, y sirve de base para determinar cómo han de ser gestionados los riesgos. Debido a que las condiciones económicas, industriales, legislativas y operativas continuarán cambiando continuamente, es necesario disponer de mecanismos para identificar y afrontar los riesgos asociados con el cambio.

1.6.3. Actividades de Control

"Las actividades de control son las políticas y los procedimientos que ayudan a asegurar que se lleven a cabo las instrucciones de la dirección de la empresa". [8]Ayudan a asegurar que se tomen las medidas necesarias para controlar los riesgos relacionados con la consecución de los objetivos de la empresa. Hay actividades de control en toda la organización, a todos los niveles y en todas las funciones. Incluye una gama de actividades tan diversa como aprobaciones, autorizaciones verificaciones, conciliaciones, revisiones de rentabilidad operativa, salvaguarda de activos y segregación de funciones.

1.6.4. Información y comunicación

Se debe identificar, recopilar y comunicar información pertinente en forma y plazo que permitan cumplir a cada empleado con sus responsabilidades. "Los sistemas informáticos producen informes que contienen información operativa, financiera y datos sobre el cumplimiento de las normas que permite dirigir y controlar el negocio de forma adecuada"[9].

[8] COOPERS & LYBRAND, *Los nuevos conceptos de Control Interno (Informe COSO)*, España, Ediciones Díaz de Santos, pág. 5

[9] PÉREZ SOLORZANO Pedro Manuel, Op. Cit. http://www.degerencia.com

Dichos sistemas no sólo manejan datos generados internamente, sino también información sobre acontecimientos internos, actividades y condiciones relevantes para la toma de decisiones de gestión así como para la presentación de información a terceros. También debe haber una comunicación eficaz en un sentido más amplio, que fluya en todas las direcciones a través de todos los ámbitos de la organización, de arriba hacia abajo y a la inversa.

1.6.5. Supervisión

Los sistemas de control interno requieren supervisión, es decir, un proceso que comprueba que se mantiene el adecuado funcionamiento del sistema a lo largo del tiempo. Esto se consigue mediante actividades de supervisión continuada, evaluaciones periódicas o una combinación de ambas cosas.

La supervisión continuada se da en el transcurso de las operaciones. Incluye tanto las actividades normales de dirección y supervisión, como otras actividades llevadas a cabo por el personal en la realización de sus funciones. El alcance y la frecuencia de las evaluaciones periódicas dependerán esencialmente de una evaluación de los riesgos y de la eficacia de los procesos de supervisión continuada. Las deficiencias detectadas en el control interno deberán ser notificadas a niveles superiores, mientras que la alta dirección y el consejo de administración deberán ser informados de los aspectos significativos observados.

1.6.6. Limitaciones del Control Interno

a) Lo que se puede lograr con el Control Interno

El control interno puede ayudar a que una entidad consiga sus objetivos de rentabilidad y a prevenir la pérdida de recursos, puede ayudar a la obtención de información financiera confiable, puede reforzar la confianza en que la empresa cumple con la normatividad aplicable.

b) Lo que no se puede lograr con el Control Interno

Un sistema de control interno, no importa lo bien concebido que esté y lo bien que funcione, únicamente puede dar un grado de seguridad razonable, no absoluta, a la dirección y al consejo en cuanto a la consecución de los objetivos de la entidad.

El control interno no puede hacer que un gerente malo se convierta en un buen gerente. Asimismo, los cambios en la política o en los programas gubernamentales, las acciones que tomen los competidores o las condiciones económicas pueden estar fuera de control de la dirección.

El control interno (incluso un control interno eficaz) funciona a diferentes niveles con respecto a los diferentes objetivos. En el caso de los objetivos relacionados con la eficacia y eficiencia de las operaciones (consecución de su misión básica, de los objetivos de rentabilidad y análogos) el control interno puede ayudar a asegurar que la dirección sea consciente del progreso o del estancamiento de la entidad.

1.6.7. Juicio Humano

La eficacia de los controles se verá limitada por el riesgo de errores humanos en la toma de decisiones, estas decisiones se tienen que tomar basadas en el juicio humano, dentro de unos límites temporales, en base a la información disponible y bajo la presión diaria de la actividad laboral.[10]

1.6.8. Disfunciones del Sistema

A pesar de estar bien diseñados, los controles internos pueden fallar, puede que el personal comprenda mal las instrucciones o que se cometan errores de juicio, errores debido a la dejadez, fatiga o despistes.

[10] COOPERS & LYBRAND, *Los nuevos conceptos de Control Interno (Informe COSO)*, España, Ediciones Díaz de Santos, pág. 108

1.6.9. Elusión de los controles por la dirección

El sistema de control interno no puede ser más eficaz que las personas responsables de su funcionamiento, incluso aquellas entidades que tienen un buen ambiente de control (aquellas que tienen elevados niveles de integridad y conciencia del control) existe la posibilidad de que el personal directivo eluda el sistema de control interno.

El término "elusión de los controles por la dirección" en el sentido en que se emplea aquí se refiere a la omisión de políticas o procedimientos establecidos con finalidades ilegítimas, con ánimo de lucro personal o para mejorar la presentación de la situación financiera o para disimular el incumplimiento de obligaciones legales.[11]

La elusión incluye prácticas tales como actos deliberados de falsificación ante bancos, abogados, contadores y proveedores, así como la emisión intencionada de documentos falsos entre otras.

La elusión no se debe confundir con la intervención, términos que se refiere a los actos de la dirección efectuados con finalidades legítimas, que se desvían de las políticas y procedimientos establecidos. La intervención de la dirección es necesaria para hacer frente a transacciones o acontecimientos puntuales y no recurrentes que, de otra forma no serían procesados correctamente por el sistema de control. Las intervenciones se hacen de manera abierta y tienen su correspondiente soporte documental, mientras que la elusión normalmente ni se documenta ni se comunica, en un claro intento de encubrir los hechos.

1.6.10. Confabulación

La confabulación de dos o más personas puede provocar fallas en el sistema de control. Cuando las personas actúan de forma colectiva para cometer y encubrir un acto, los datos financieros y otras informaciones de gestión pueden verse alterados de un modo no identificable por el sistema de control.

[11] COOPERS & LYBRAND, *Los nuevos conceptos de Control Interno (Informe COSO)*, España, Ediciones Díaz de Santos, pág. 109

1.6.11. Relación Costo/Beneficio

Las entidades deben considerar los costos y beneficios relativos a la implantación de controles. A la hora de decidir si se ha de implantar un determinado control, se considerarán tanto el riesgo de fracaso como el posible efecto en la entidad, junto a los costos correspondientes a la implantación del nuevo control.

Existen distintos niveles de precisión en cuanto a la determinación del costo y el beneficio de la implantación de controles. Generalmente resulta más fácil determinar el costo, pudiéndose cuantificar de forma bastante precisa. Normalmente se tienen en cuenta todos los costos directos correspondientes a la implantación de un control, así como los costos indirectos si resultan cuantificables. Algunas empresas también incluyen los costos de oportunidad asociados al uso de recursos.

1.6.12. Funciones y responsabilidades

Todos los miembros de la organización son responsables del control interno.

- ✓ **LA DIRECCIÓN.-** O cualquier denominación para el máximo ejecutivo, en el cual recae en primer lugar la responsabilidad del control, el cual debe liderar y revisar la manera en que los miembros controlan el negocio, estos a su vez designan responsables de cada función y establecen políticas y procedimientos de control interno más específicos. La responsabilidad se organiza en cascada.

- ✓ **RESPONSABLES DE LAS FUNCIONES FINANCIERAS**.- Los directores financieros y sus equipos tienen una importancia vital porque sus actividades están estrechamente vinculadas con el resto de unidades operativas y funcionales de una entidad. Normalmente están involucrados en el desarrollo de presupuestos y en la planificación financiera. Controlan, siguen y analizan el rendimiento, no sólo desde una perspectiva financiera sino también, en muchas ocasiones, en relación al resto de operaciones de la

entidad y al cumplimiento de requisitos legales. [12]El director financiero, el jefe de contabilidad, el "controller" y otros responsables de las funciones financieras de una entidad son claves para determinar la forma en que la dirección ejerce el control.

- ✓ **EL CONSEJO DE ADMINISTRACIÓN.-** La dirección es responsable ante el Consejo el cual debe de ofrecer asesoría, pautas de actuación y conocer a profundidad las actividades de la entidad. Debe de estar preparado para una posible falla de la dirección a través de una comunicación con los niveles altos, con los responsables financieros, jurídicos y de auditoría. Muchos consejos de administración llevan a cabo sus tareas a través de comités. Sus funciones y la importancia de sus trabajos varían de una entidad a otra, pero suelen incluir las áreas de auditoría, remuneraciones, finanzas, nombramientos etc. Cada comité puede poner un énfasis específico en determinados elementos del control interno.

- ✓ **COMITE DE AUDITORIA.-** El comité de auditoría o en su defecto el consejo) está en una posición privilegiada, tiene la autoridad para interrogar a los directivos sobre la forma en que están asumiendo sus responsabilidades en cuanto a la información financiera, y para asegurar que se tomen medidas correctivas. El comité de auditoría, junto con, o además de una función de auditoría interna fuerte, está muchas veces en la mejor posición dentro de una entidad para identificar situaciones en que los altos directivos intentan eludir los controles internos o tergiversar los resultados financieros y actuar en consecuencia. Por ello, existen situaciones en las que el comité de auditoría o el consejo deben afrontar directamente asuntos o circunstancias graves.

- ✓ **AUDITORES INTERNOS.-** Desempeñan un papel importante en la evaluación de la eficiencia de los sistemas de control y recomiendan mejoras a los mismos. Según las normas emitidas por el Institute of Internal Auditors, los auditores internos deberían:

[12] COOPERS & LYBRAND, *Los nuevos conceptos de Control Interno (Informe COSO)*, España, Ediciones Díaz de Santos, pág. 41

- “Revisar la confiabilidad y la integridad de la información financiera y operativa y los procedimientos empleados para identificar, medir, clasificar y difundir dicha información.”

- “Revisar los sistemas establecidos para asegurar el cumplimiento de aquellas políticas, planes, procedimientos, leyes y normativas susceptibles de tener un efecto importante sobre las operaciones e informes, así como determinar si la organización cumple con los mismos.”

- “Revisar los medios utilizados para la salvaguarda de activos y verificar la existencia de los mismos”.

- “Valorar la eficiencia en el empleo de los recursos”.

- “Revisar las operaciones o programas para cerciorarse de si los resultados son coherentes con los objetivos y las metas establecidas y si se han llevado a cabo según los planes previstos”.

Todas las actividades de una entidad recaen, potencialmente, dentro del ámbito de responsabilidad de los auditores internos.

Los auditores internos solo pueden ser imparciales cuando no están obligados a subordinar su juicio sobre asuntos de auditoría al juicio de otros. El principal medio de asegurar la objetividad de la auditoría interna es la asignación de personal adecuado para la función de auditoría, evitando posibles conflictos de intereses y prejuicios.

Debería haber una rotación periódica en el personal asignado y los auditores internos no deberían asumir responsabilidades operativas. Igualmente, no deberían estar asignados a la auditoría de actividades en las cuales hubiesen tenido alguna responsabilidad operativa reciente.

Debe recordarse que la función de auditoría interna (en contra de lo que cree algún sector de opinión) no tiene como responsabilidad principal el establecimiento o mantenimiento del sistema de control interno.

- ✓ **OTROS EMPLEADOS.-** El control interno es hasta cierto punto responsabilidad de todos los empleados, casi todos producen información utilizada en el sistema de control o realizan funciones para efectuar el control.

- ✓ **AUDITORES EXTERNOS.-** Algunos terceros como los auditores externos contribuyen al logro de los objetivos, aportan opinión independiente y objetiva, contribuyen directamente mediante la auditoria a los estados financieros.

CAPÍTULO II

2. ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA EMPRESA SUPERMERCADO DE COMPUTADORAS COMPUBUSSINES CÍA. LTDA.

En este capítulo se da a conocer la estructura organizacional de Supermercado de Computadoras Compubussines Cía. Ltda. Cía. Ltda., ya que es importante conocer la forma en que se dividen, agrupan y coordinan las actividades de la organización en cuanto a las relaciones que mantienen todo el personal involucrado en la misma, además implica un proceso de recolección y análisis de la información proveniente de documentos existentes y de procesos participativos (entrevistas y cuestionarios), que permita tener un conocimiento de cómo son, como se manejan y que recursos utilizan los distintas áreas de la organización, los procesos y procedimientos que utilizan.

2.1. Antecedentes y Reseña Histórica

SUPERMERCADO DE COMPUTADORAS COMPUBUSSINES CÍA. LTDA. CÍA. LTDA., bajo la inspiración de cuatro hermanos socios y su madre, representado por su Gerente General ECO. SANTIAGO TEJADA ROSERO, fue fundado en el año 2001.

SUPERMERCADO DE COMPUTADORAS COMPUBUSSINES CÍA. LTDA. CÍA. LTDA., es una empresa líder en la distribución y venta de equipos tecnológicos tales como computadoras, laptops, impresoras, accesorios, mp3, mp4, LCD´s, entre otros; con más de 8.000 productos en cada uno de nuestros locales en Quito, Ambato e Ibarra estratégicamente ubicados para brindar un servicio rápido y oportuno.

SUPERMERCADO DE COMPUTADORAS COMPUBUSSINES CÍA. LTDA. CÍA. LTDA., está comprometida con las tendencias mundiales de crecimiento de la demanda de la tecnología ofreciendo un valor agregado hacia todos los grupos de interés, basado en sus principios y ética profesional.

2.2. Factores que influyen en el desarrollo empresarial de Supermercado de Computadoras Compubussines Cía. Ltda.

Los aspectos importantes que debemos considerar es el tipo de mercado en el que está inmersa la empresa, los clientes y los proveedores que maneja a estos factores se los conoce como micro ambiente.

También es necesario tener en cuenta la competencia a la que se enfrenta, las disposiciones del Estado con relación a su política interna y externa, a estos factores se les conoce como macro ambiente.

Los factores que se detallan a continuación son útiles para conocer las influencias de las fuerzas internas y externas del ambiente que rodea a la organización:

2.2.1. Micro Ambiente de Supermercado de Computadoras Compubussines Cía. Ltda.

El microambiente está integrado por factores y fuerzas cercanas a la organización capaces de afectar su habilidad de servir a sus clientes. Los factores que incluyen son la organización, los proveedores y los clientes.

A continuación describiremos cada uno de ellos:

2.2.1.1. La Organización

Incluye los distintos departamentos que forman parte de la organización, Supermercado de Computadoras Compubussines Cía. Ltda., cuenta con el Departamento de Administración dirigido por la Lic. Cristina Orellana y el Departamento de Ventas en representación de la Ing. Marianela Jiménez; estos departamento a su vez cuentan con sub divisiones.

La organización además incluye la misión, la visión, los valores éticos que practica, la competitividad, la filosofía que maneja, las funciones de la Junta Directiva, dado

que los objetivos de la empresa y la forma de alcanzarlos se encuentran basados en distintas prioridades, juicios de valor y estilos de gestión, éstas son llevadas a normas de comportamiento, el cliente siempre espera más de lo que la organización ofrece, es por ello que las normas de comportamiento van más allá del cumplimiento de la ley.

A continuación se detalla la Misión, Visión, análisis Foda, Valores y Estructura Organizacional de la empresa:

2.2.1.1.1. Misión

A través de nuestro equipo humano altamente capacitado, con tecnología de punta, canales de distribución, satisfacer las múltiples necesidades de nuestros clientes mediante la entrega de productos de última generación en computación, línea blanca y telefonía celular.

2.2.1.1.2. Visión

La Gerencia por el momento no ha desarrollado la Visión que debe poseer la empresa.

2.2.1.1.3. Análisis FODA

Fortalezas

1. Atención al cliente dando un producto y servicio de calidad y a un bajo precio.
2. Variedad en el producto de acuerdo a la tendencia de desarrollo de la tecnología.
3. Amplio mercado para las ventas.
4. Recurso Humano capacitado.
5. Maquinaria disponible para la transportación del producto.

Oportunidades

1. Facilidades para adquirir el producto.
2. Concienciación por parte de las personas por la obtención del producto de primera calidad.
3. Ser una de las empresas líderes en el país en brindar productos de última tecnología.
4. Ingresar con productos nuevos en el mercado.
5. Promocionar las ofertas comerciales de los artículos novedosos.

Debilidades

1. Dependencias de Financieras Locales.
2. No contar con un espacio físico propio.
3. No contar con manuales de procedimientos específicos.
4. Poco emprendimiento de algunos trabajadores hacia la empresa.
5. Los procesos internos cambian constantemente.

Amenazas

1. Políticas municipales.
2. Políticas del estado
3. Delincuencia en el sector
4. Baja en la venta en temporadas malas
5. Políticas de Importación

2.2.1.1.4. Valores de la organización

El trabajo de Supermercado de Computadoras Compubussines Cía. Ltda., se fundamenta en principios que fortalecen su imagen y extienden su mercado en la venta de productos de última generación, los valores más relevantes de la organización son:

- *Honestidad***,** para la empresa Supermercado de Computadoras Compubussines la honestidad es tener y exigir integridad en cada una de las actividades realizadas externa e internamente de la organización.

- *Fidelidad,* es importante para la empresa Supermercado de Computadoras Compubussines mantener confidencia en la información, documentación de valor, identidad corporativa y estructura organizacional de la empresa.

- *Liderazgo,* para Supermercado de Computadoras Compubussines, el liderazgo es una función dentro de la organización, ya que todo el personal que forma parte de la entidad, integra y organiza sus actividades hacia el logro de los objetivos institucionales, para ser los primeros y los que ejercen mayor influencia en el medio en el que la entidad se desenvuelve.

- *Compromiso*, Supermercado de Computadoras Compubussines al involucrarse en cada uno de las actividades y procesos que sirven de guía para cumplir con los objetivos establecidos adquiere compromisos con sus clientes y personal.

- *Trabajo en Equipo,* para la empresa Supermercado de Computadoras Compubussines es importante ejercer un trabajo en equipo mediante la difusión de misión, visión, valores, capacidad de planta y permanente capacitación direccionar todos los esfuerzos a un objetivo común.

- *Competitividad*, Supermercado de Computadoras Compubussines toma la competitividad como una estrategia de carácter motivacional, capacitación permanente, estableciendo un modelo que constantemente impulsa al Recurso Humano a ser eficiente, eficaz y efectivo

- *Identidad Corporativa,* para la empresa Supermercado de Computadoras Compubussines es importante crear una Cultura Organizacional que le identifique como marca de renombre en el mercado, mediante el uso de una comunicación fluida, imagen y diseño de la estructura de la empresa.

- *Excelencia,* Supermercado de Computadoras Compubussines ejerce un conjunto de prácticas sobresalientes en la gestión de la organización que incluyen: la orientación hacia los resultados, orientación al cliente, liderazgo y perseverancia, procesos y hechos, implicación de las personas, mejora continua e innovación.

- *Innovación,* Supermercado de Computadoras Compubussines, toma la innovación como el motor para su crecimiento, con innovación la organización convierte sus ideas y conocimientos en servicios mejorados que el mercado en el que se desenvuelve reconoce y valora.

2.2.1.1.5. Estructura Organizacional de Supermercado de Computadoras Compubussines Cía. Ltda.

Supermercado de Computadoras Compubussines Cía. Ltda., es una organización de profesionales altamente calificados, que se dedica a la venta de productos de última generación, para lo cual su estructura organizacional identifica tres niveles: Superior, Funcional y Operacional.

La empresa tiene una estructura que le permite desarrollar sus actividades con fluidez y precisión, especializando cada una de sus áreas hacia una meta específica. Este organigrama es utilizado como herramienta de trabajo de los administradores y ejecutivos, dado que en este se demuestra las líneas de autoridad y las unidades administrativas que integran la organización.

Es importante que el organigrama de la organización sea difundido entre todo el personal, para que conozcan su ubicación, nivel de jerarquía, grado de responsabilidad y campo funcional.

Nivel Superior

El nivel superior de Supermercado de Computadoras Compubussines Cía. Ltda., está conformado por la Junta General de Socios integrada por sus cinco socios, la madre de familia y cuatro hermanos; ellos son quienes forman la base y el pilar fundamental

sobre el cual se construye la organización, y sobre quienes recae la responsabilidad del establecimiento y manejo de las estrategia de la organización y la filosofía de la gestión.

La función principal que desempeña el nivel superior es la administración de la organización a través del gerente general.

La Junta General de Accionistas está conformada por cinco accionistas, los cuales son los únicos que pueden resolver cualquier asunto relativo a los negocios de la empresa y para tomar las decisiones. A continuación se detalla el número de participaciones con el que cuentan cada uno de los socios:

GRÁFICO Nº 3
DISTRIBUCIÓN PARTICIPACIONES DE SOCIOS
SUPERMERCADO DE COMPUTADORAS COMPUBUSSINES CÍA. LTDA.

SOCIOS	N° ACCIONES O APORTACIONES
Marianela Del Pilar Jiménez Palmay	60
Betty Germania Jiménez Palmay	90
Julia Elizabeth Jiménez Palmay	90
Jaime Patricio Jiménez Palmay	90
Emma Yolanda Jiménez Palmay	270
TOTAL	**600**

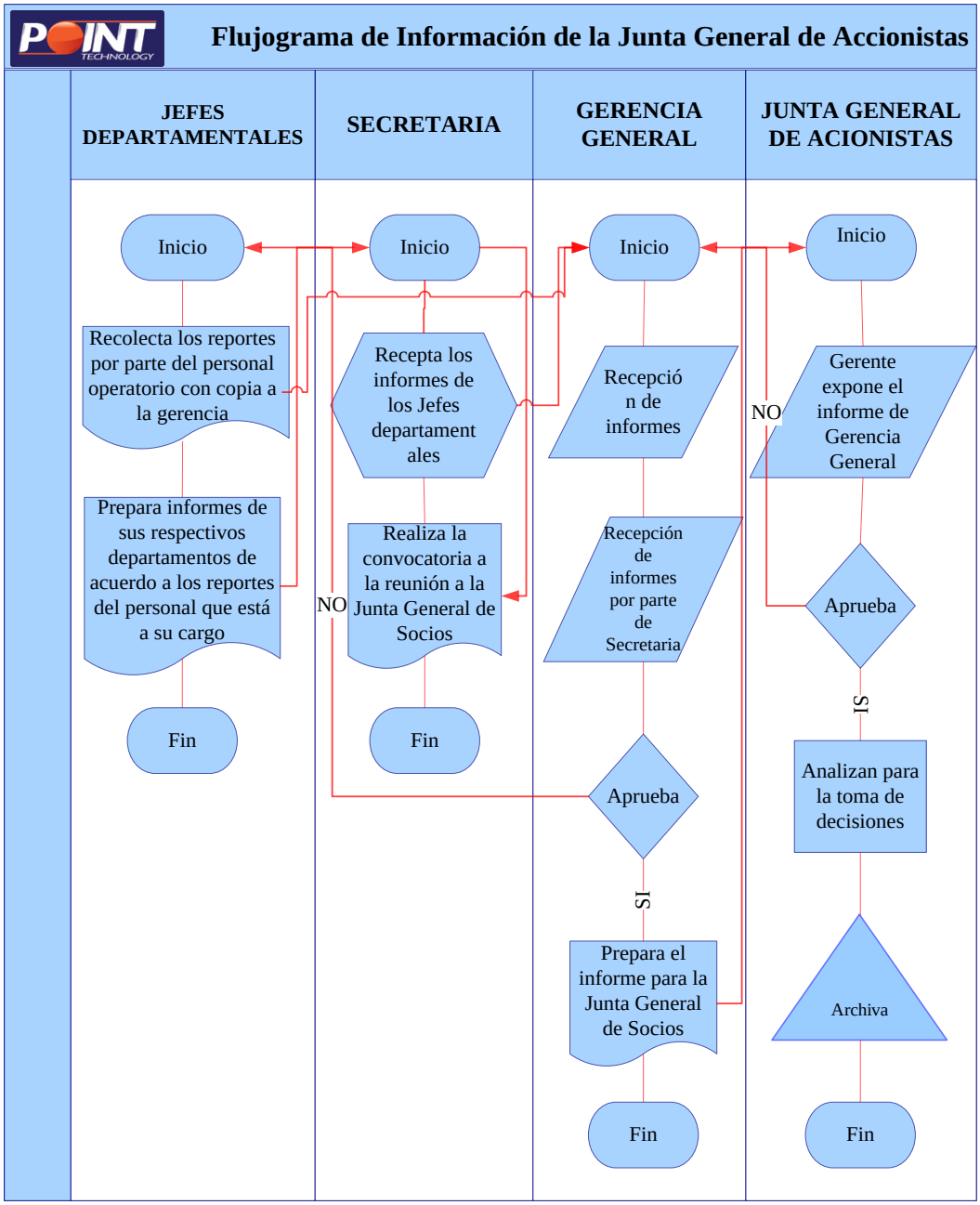
Preparado por: Carolina Leroux S.
Fuente: Escritura de Constitución de Supermercado de Computadoras Compubussines Cía. Ltda.

Funciones de la Junta General de Socios:

- Nombrar al gerente general de la compañía.
- Remover por causas legales de su cargo a la persona designada como gerente general.
- Conocer y aprobar anualmente las cuentas, el balance y los informes que presente el gerente general.

GRÁFICO Nº 4

FLUJOGRAMA DE PROCEDIMIENTO DE INFORMACIÓN DE LA JUNTA GENERAL DE ACCIONISTAS



Elaborado por: Carolina Leroux S.

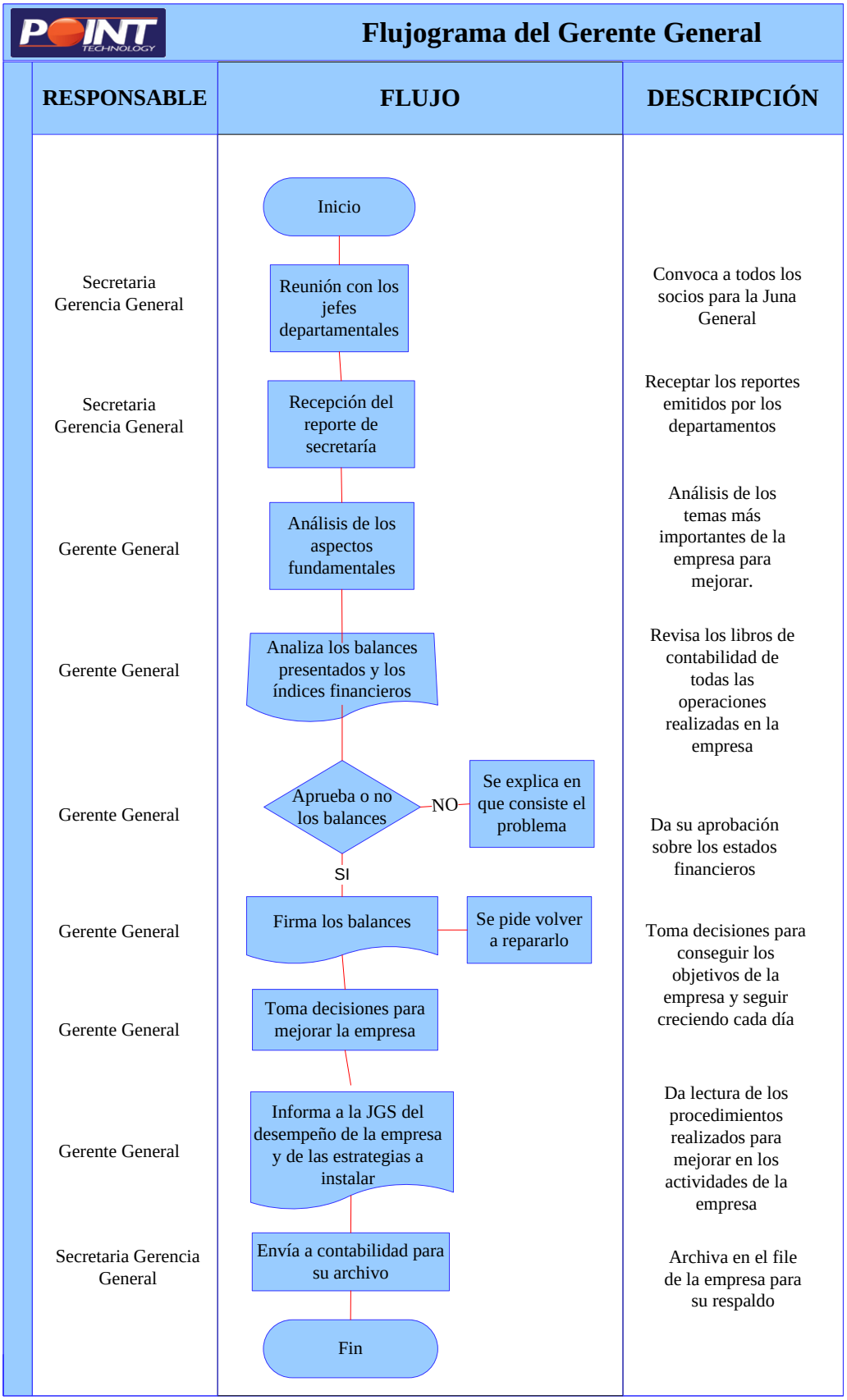
Funciones del Gerente General:

Eco. Santiago Fabián Tejada Rosero, esposo de Betty Jiménez.

- Define, orienta y planifica las políticas y objetivos generales de la Empresa.
- Dirigir las sesiones de la junta general de socios;
- Administrar y dirigir la marcha de la compañía;
- Autorizar o suscribir todo acto o contrato a nombre y en representación de la compañía;
- Cumplir y hacer cumplir las resoluciones y acuerdos de la junta general;
- Programar y planificar las actividades económicas y financieras de la compañía;
- Convocar a las juntas generales;
- Designar a los empleados que creyere necesarios y fijarles sus atribuciones y deberes;
- Cuidar y hacer que se lleven los libros de contabilidad y llevar por sí mismo el libro de actas de la junta general;
- Presentar cada año a la junta general una memoria razonada acerca de la situación de la compañía; acompañada del balance y de la cuenta de pérdidas y ganancias;
- Informar a la junta general cuando se le solicite o lo considere necesario o conveniente acerca de la situación administrativa y financiera de la compañía, y ;
- Ejerce autoridad funcional sobre el resto de cargos ejecutivos, administrativos y operacionales de la organización.
- Ejercer todas las funciones que les señale la junta general y además todas aquellas que sean necesarias y convenientes para el funcionamiento de la compañía.
- Generar mecanismos de control de las actividades.
- Revisar informes de gestión.
- Atender requerimientos de los clientes en cuanto al servicio y la calidad del mismo.

GRÁFICO Nº 5

FLUJOGRAMA DE LOS PROCESOS DEL GERENTE GENERAL



Elaborado por: Carolina Leroux S.

Responsabilidades del Gerente General

- Responder por los procesos de planeación, organización, dirección, evaluación y control a desarrollar en la entidad.
- Informar a la Junta General de Accionistas de la situación actual de la empresa.
- Utilizar toda su capacidad intelectual en forma eficaz, innovadora y creativa, para dar a la Empresa las herramientas necesarias para el cumplimiento de su misión, visión y objetivos institucionales, efectuando los estudios técnicos y proponiendo la prestación de servicios que considere se puedan implementar con el fin de buscar el desarrollo regional y nacional.
- Mantener una línea directa de comunicación con sus colaboradores para estar bien informado.
- Lograr ventajas competitivas para la empresa que se vean reflejadas en una mayor remuneración económica necesaria para seguir siendo líder en su ramo.
- Establecer un claro liderazgo dentro de un ambiente de respeto y productividad, proyectando y consolidando la imagen de la institución.
- Responder de los perjuicios que por dolo o culpa ocasione a la Sociedad, a los socios o a terceros.

Nivel Funcional

El nivel funcional de Supermercado de Computadoras Compubussines Cía. Ltda., está conformado por miembros que tienen a su cargo desarrollar en forma concreta las estrategias y filosofías de la gestión, indicando las acciones y metas que deben alcanzarse de manera inmediata en cada oportunidad en tiempo y espacio.

En el nivel funcional se distingue la Administración Financiera; encargada del departamento de Contabilidad, Crédito y Cobranzas, de Recursos Humanos, departamento Técnico y Servicios Generales.

Los miembros que conforman este nivel son: como Gerente Administrativa Financiera Lic. Cristina Orellana, Contadora General Dra. Verónica Troya, Crédito y Cobranzas Sra. Andrea Freire, Recursos Humanos Lic. Cristina Orellana, departamento Técnico Srta. Estefanía Gómez y en Servicios Generales Lic. Hugo Correa.

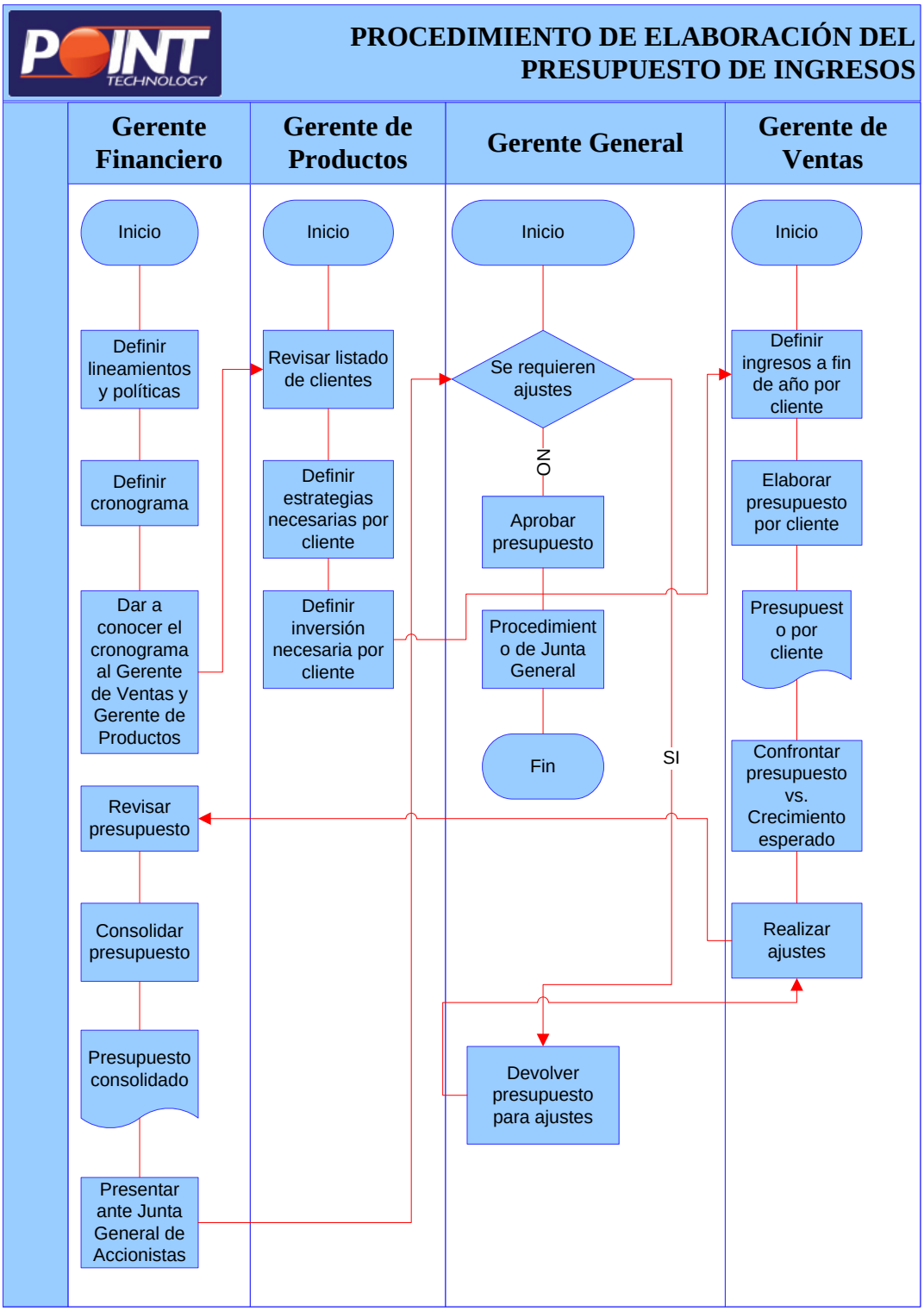
Funciones del Gerente Administrativo Financiero

Lic. Cristina Orellana tiene las siguientes funciones:

- En conjunto con el Jefe de Recursos Humanos llevar a cabo la valoración de cargos y salarios de todo el personal.
- Convocar y dirigir reuniones con el personal del área administrativa para coordinar la ejecución de las acciones y procedimientos
- Dirigir el proceso de selección de personal, de acuerdo a las necesidades de la empresa.
- Supervisar semanalmente la gestión realizada por Servicios Generales, Transporte, Comedor, etc.
- Realizar negociaciones con instituciones financieras para la obtención de créditos y préstamos
- Estar al tanto de las novedades de personal que se presenten.
- Supervisar el rendimiento y oportunidad del proceso contable.
- Revisión de los estados financieros.
- Evaluar y aprobar las compras de la Compañía.
- Garantizar el pago oportuno de los diferentes compromisos adquiridos por la compañía.
- Mantener un control adecuado de los diferentes gastos de la Compañía.
- Garantizar la producción oportuna y de calidad de la información financiera.
- Garantizar el cumplimiento de las obligaciones laborales y tributarias de la compañía.
- Hacer seguimiento mensual al cumplimiento de los presupuestos asignados.

GRÁFICO Nº 6

FLUJOGRAMA DEL PROCEDIMIENTO DE ELABORACIÓN DEL PRESUPUESTO DE INGRESOS



Elaborado por: Carolina Leroux S.

Responsabilidades del Gerente Administrativo Financiero

- Se ocupa de la optimización del proceso administrativo
- Controla el manejo de las bodegas y el inventario
- Monitorea todo el proceso de administración financiera de la organización.
- Planificar, dirigir, ejecutar y controlar las actividades de los departamentos de su competencia: Personal, Servicios Generales y Seguros.

Documentos Generados

- Presupuesto por cliente y Consolidado.

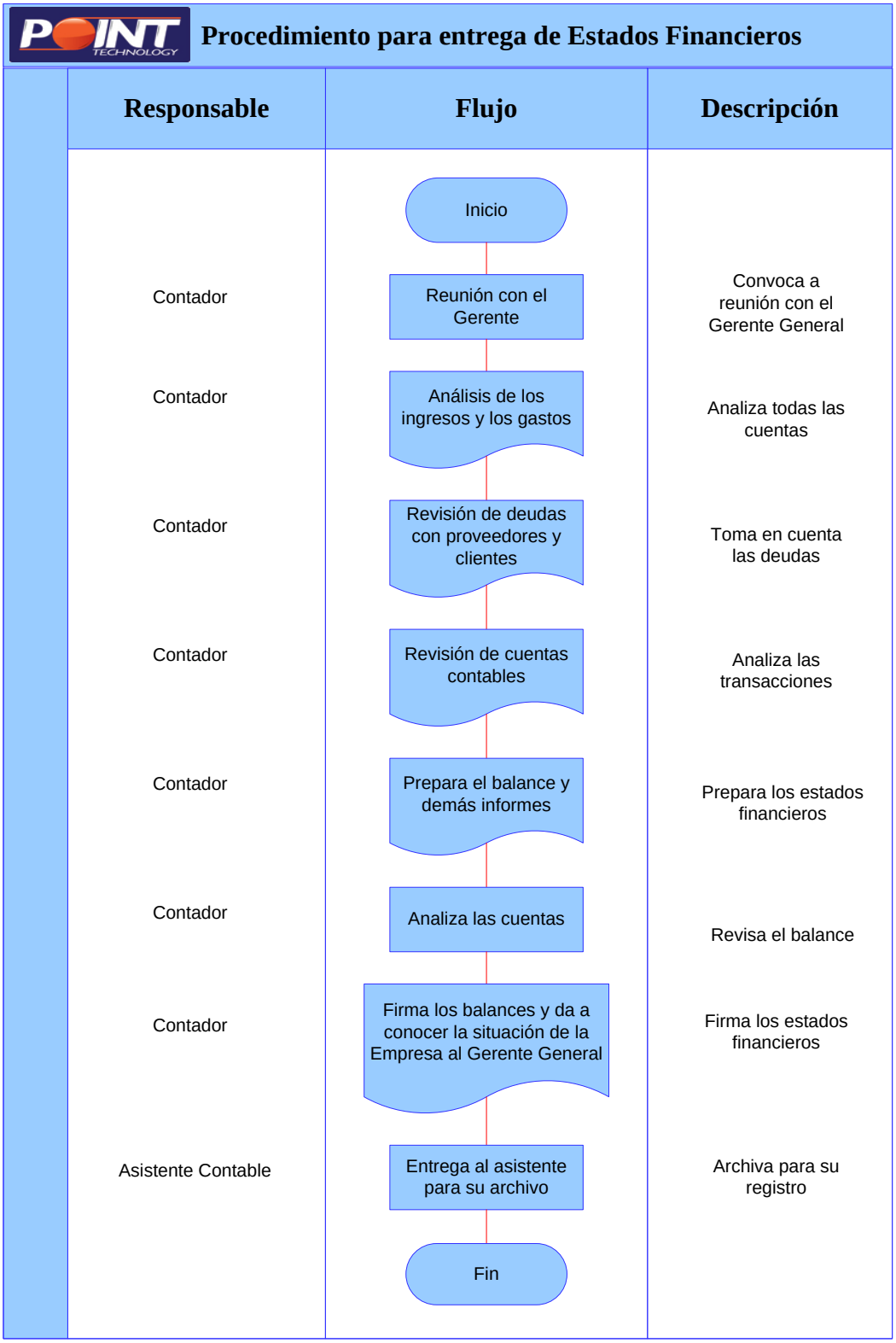
Funciones de la Contadora General

Dra. Verónica Troya tiene las siguientes funciones:

- Preparar los informes financieros que requieren los altos funcionarios de la organización.
- Establece las cuentas adecuadas, que servirán para la debida clasificación y análisis de la información que haya de someterse a los altos funcionarios.
- Analiza los registros diarios que realizan los asistentes para hacer los pases a las cuentas y poder condensar eficazmente la información contenida en las mismas.
- Revisa los diferentes tipos de comprobantes de Diario, que han de obrar como medio para resumir los detalles y transferirlos desde el registro inicial al de recopilación.
- Analiza y prepara los informes, cuentas, registros y comprobantes constituye todo el proceso de la contabilidad, desde que se inicia cada operación hasta que se refleja en los informes y su efecto final en la situación financiera de la empresa.

GRÁFICO Nº 7

FLUJOGRAMA DE PROCEDIMIENTO PARA ENTREGA DE ESTADOS FINANCIEROS



Elaborado por: Carolina Leroux S.

Responsabilidades del Contador General

- Garantizar que las normas vigentes aplicables a las operaciones contables y financieras, sean manejadas de manera exitosa y precisa en los asientos contables a fin de contribuir a la satisfacción de los requerimientos de los clientes internos y órganos de control y vigilancia.

- Proponer, velar, procurar y controlar que los objetos y metas de la Empresa en lo referente a operaciones contables, manejo de presupuesto y demás recursos financieros se manejen de manera exitosa y precisa a fin de satisfacer los requerimientos de los altos directivos, órganos de control y vigilancia.

- Diseñar, proponer y ejecutar las acciones de capacitación para funcionarios, empresarios y la comunidad en general en los temas tributarios, contable, financiero y demás temáticas del área.

Documentos Generados

- Estado de Situación General
- Estado de Resultados
- Flujo de Efectivo
- Estado de Cambios en el Patrimonio

GRÁFICO Nº 8

EMPRESA SUPERMERCADO DE COMPUTADORAS COMPUBUSSINES CÍA. LTDA.
BALANCE GENERAL
DEL 1 DE ENERO AL 31 DE DICIEMBRE DEL 2009

ACTIVO			
CORRIENTES			134955,19
Caja		28750,00	
Caja Chica		100,00	
Bancos		41541,49	
Documentos por Cobrar Clientes	7515,70	6676,91	
(-) Provisión Cuentas Incobrables	838,79		
Clientes a Plazos		5677,70	
Suministros de Oficina		345,00	
Inventario Mercaderías	40555,11	40352,33	
(-) Provisión Invent Obsoletos	202,78		
Seguros Prepagados		1200,00	
Arriendos Prepagados		2400,00	
Publicidad Prepagada		800,00	
IVA Pagado		6451,91	
Anticipo IRF		659,85	
PROPIEDAD PLANTA Y EQUIPO			54537,40
Terrenos		11300,00	
Muebles de Oficina	750,00	512,22	
(-) Dep. Acum.Muebles de Oficina	237,78		
Instalaciones y Decoraciones	865,00	621,74	
(-) Dep. Acum. Instalaciones y Decoraciones	243,26		
Muebles y Enseres	1120,00	747,83	
(-) Dep. Acum Muebles y Enseres	372,17		
Equipo de Oficina	2050,00	1097,07	
(-) Dep. Acum Equipo de Oficina	952,93		
Equipo de Computación	1300,00	800,17	
(-) Dep. Acum Equipo de Computación	499,83		
Vehículos	15500,00	12555,83	
(-) Dep. Acum Vehículos	2944,17		
Edificios	28850,00	26902,54	
(-) Dep. Acum Edificios	1947,46		
OTROS ACTIVOS			1435,00
Gastos de Constitución y Organización		1950,00	
(-) Amort. Acum Gastos de Constitución y Organización		515,00	
TOTAL ACTIVOS			**190927,60**

PASIVOS			
CORRIENTES			39724,80
Servicios Básicos por Pagar		285,00	
Servicios de Vigilancia por Pagar		240,00	
IESS por Pagar		179,82	
Beneficios Sociales por Pagar		1150,00	

Cuentas por Pagar Proveedores	28615,00	
Documentos por Pagar otros acreedores	3750,00	
IRF por Pagar	200,35	
IVA Retenido por Pagar	32,90	
IVA Cobrado	2273,04	
Impuesto a la Renta por Pagar	4,56	
Servicio de Mantenimiento por Pagar	130,00	
Comisariato por Pagar	95,00	
Dividendos por Pagar	503,69	
15% Trabajadores por Pagar	756,42	
25% del Impuesto por Pagar	1071,59	
Provisión décimo tercer sueldo	172,83	
Provisión décimo cuarto sueldo	5,36	
Provisión Fondos de Reserva	172,83	
Provisión Vacaciones	86,41	
NO CORRIENTE		20.302,36
Utilidades por Realizar	2084,57	
Préstamo Bancario por Pagar	11210,95	
Hipotecas por Pagar Largo Plazo	7006,84	
TOTAL PASIVOS		**60.027,16**
PATRIMONIO		
Capital y Reservas		130.900,44
Capital Social	125000,00	
Reserva Legal	2101,48	
Reserva Estatutaria	100,74	
Reserva Especial	100,74	
Utilidades Retenidas de Ejercicios Anteriores	2500,00	
Utilidad del Ejercicio	1108,12	
Déficit por evaluación de inventarios	10,64	
TOTAL PATRIMONIO + PASIVO		**190.927,60**

Contador **Gerente**

GRÁFICO Nº 9

EMPRESA SUPERMERCADO DE COMPUTADORAS COMPUBUSSINES CÍA. LTDA.
ESTADO DE PÉRDIDAS Y GANANCIAS
DEL 1 DE ENERO AL 31 DE DICIEMBRE DEL 2009

RENTAS OPERACIONALES			
Ventas			50000,00
(-) Costo de Ventas			36094,03
(=) Utilidad Bruta en Ventas			**13905,97**
(+) Utilidades Realizadas			110,15
(=) Rentas Operacionales			**14016,12**
(-) Gastos Operacionales			9315,75
Gastos Administrativos		8915,75	
Gasto Servicios Básicos	690,00		
Gasto Sueldos	2329,88		
Gasto Aporte Patronal	251,98		
Gasto Beneficios Sociales	437,43		
Gasto Mantenimiento de Act. Fijos	365,00		
Gasto Servicio de Vigilancia	480,00		
Gasto de Transporte	15,00		
Gasto Combustibles y Lubricantes	18,00		
Gastos Generales	17,00		
Gasto Suministros de Oficina	70,00		
Gasto Arriendo	1600,00		
Gasto Seguros	600,00		
Gasto Alimentación	25,00		
Gasto Depreciación Muebles de Oficina	12,78		
Gasto de Depreciación Instalación y Decoración	13,26		
Gasto Depreciación Muebles y Enseres	17,17		
Gasto Depreciación Equipo de Oficina	34,93		
Gasto Depreciación Equipo de Computación	49,83		
Gasto Depreciación Vehículos	594,17		
Gasto Depreciación Edificios	147,46		
Gasto Amortz. Gastos de Constitución	65,00		
Gasto Prov. Inventario Obsoleto	202,78		
Gasto Chequera	25,00		
Gasto Interés	799,29		
Gasto Servicios Bancarios	38,00		
Gasto Cuentas Incobrables	16,79		
Gastos de Ventas		400,00	
Gasto Publicidad	400,00		
(=) Utilidad Operacional			**4700,37**
(-) Otros Gastos			2309,60
Descuento en Ventas		2309,60	
(+) Otras Rentas			1452,00
Comisiones Ganadas		1117,50	
Intereses Ganados		275,00	
Descuento en Compras		59,50	
(=) UTILIDAD BRUTA DEL EJERCICIO			**3842,77**
(-) 15% PARTICIPACION TRABAJADORES			756,42
(=) UTILIDAD ANTES DE IMPUESTO A LA			**3086,35**

RENTA	
(-) 25% IMPUESTO A LA RENTA EMPRESARIAL	1071,59
(=) UTILIDAD NETA DEL EJERCICIO	**2014,77**
(-) 10% Reserva Legal	201,48
(=) Utilidad Antes de Dividendos	**1813,29**
(-) 25% Dividendos	503,69
(=) Utilidad Antes de otras Reservas	**1309,60**
(-) 5% Reserva Especial	100,74
(-) 5% Reserva Estatutaria	100,74
UTILIDAD DEL EJERCICIO	**1108,12**

Conciliación Tributaria	
Utilidad Bruta del Ejercicio	3842,77
(+) Gastos no deducibles	1200,00
Utilidad antes de repartición a trabajadores	**5042,77**
15% Trabajadores	756,42
Utilidad Antes de Impuesto a la Renta	**4286,35**
25% Impuesto a la Renta	1071,59
Utilidad Neta del Ejercicio	**3214,77**

Contador **Gerente**

Notas a los Estados Financieros

1. A la utilidad bruta del ejercicio, se procedió a sumarle los gastos no deducibles, para cálculos de las utilidades trabajadores y del impuesto a la renta. (Conciliación Tributaria).

2. Estos valores fueron contabilizados en nuestro Estado de Pérdidas y Ganancias; lo cual nos dan una utilidad de Neta del Ejercicio de 2.014,77; de donde se deduce los dividendos y reservas según la política de la empresa.

GRÁFICO Nº 10

EMPRESA SUPERMERCADO DE COMPUTADORAS COMPUBUSSINES CÍA. LTDA.
ESTADO DE FLUJO DEL EFECTIVO
DEL 01 DE ENERO AL 31 DE DICIEMBRE DEL 2009

A. FLUJO EFECTIVO ACTIVIDADES DE OPERACIÓN			
A1 RECIBIDO DE CLIENTES			38304,91
Ventas	50000,00		
Utilidades Realizadas en Ventas a Plazos	110,15		
(-) Descuento en Ventas	2309,60	47800,55	
Cuentas por Cobrar clientes y a plazos	-13193,40	-13193,40	
Anticipo de Impuesto a la Renta	-659,85	-659,85	
IVA Cobrado en Ventas	2273,04	2273,04	
Utilidades por Realizar	2084,57	2084,57	
A2 RECIBIDO DE OTROS CLIENTES			1452,00
Comisiones Ganadas	1117,50	1117,50	
Intereses Ganados	275,00	275,00	
Descuento en Compras	59,50	59,50	
A3 PAGADO A PROVEEDORES			-50513,4
Costo de Ventas	-36094,03	-36094,03	
Inventario de Mercaderías	-40555,11	-40555,11	
Revalorización de Inventarios	-10,64	-10,64	
IVA Compras	-6451,91	-6451,91	
Impuestos por Pagar (IVA E IRF)	233,25	233,25	
Cuentas por Pagar o Proveedores	32365,00	32365,00	
A4 CUENTAS POR PAGAR OTROS PROVEDORES			-8053,07
Gastos Administrativos	-8915,75	-8915,75	
Gastos de Ventas	-400,00	-400,00	
Depreciaciones y Amortizaciones	1154,17	1154,17	
Prepagados (arriendos, seguros, etc.)	-4400,00	-4400,00	
Inventario de Suministros de Oficina	-345,00	-345,00	
IESS por Pagar	179,82	179,82	
Beneficios Sociales por Pagar	2847,54	2847,54	
Otras cuentas por Pagar (gastos varios)	750,00	750,00	
Impuesto a la Renta por Pagar	1076,15	1076,15	
FLUJO POR ACTIVIDAD DE OPERACIÓN			
B. FLUJO DE ACTIVIDADES DE INVERSIÓN			0,00
Entradas	0,00	0,00	
Salidas	0,00	0,00	
FLUJO DE ACTIVIDADES DE FINANCIAMIENTO			18217,79
Entradas	0,00	0,00	
Salidas	0,00	0,00	
Préstamos Bancarios a Largo Plazo	11210,95	11210,95	
Hipotecas por Pagar	7006,84	7006,84	
FLUJO NETO TOTAL			**-591,81**

Contador **Gerente**

GRÁFICO Nº 11
EMPRESA SUPERMERCADO DE COMPUTADORAS COMPUBUSSINES CÍA. LTDA.
ESTADO DE EVOLUCIÓN EN EL PATRIMONIO
DEL 1 DE ENERO AL 31 DE DICIEMBRE DEL 2009

FECHA	CONCEPTO	CAPITAL SOCIAL	UTILIDAD DEL EJERCICIO	RESERVAS			REVALORIZACION DE INVENTARIOS	TOTAL
				LEGAL	ESTATUT.	ESPECIAL		
01/01/2005	Saldo Inicial	125000,00	2500,00	1900,00	0,00	0,00	-10,64	129389,36
01/01/2006	Utilidad Neta del Ejercicio		2014,76					2014,76
	Dividendos		-503,69					-503,69
	Apropiación de Reservas		-402,96	201,48	100,74	100,74		0,00
	TOTALES	**125000,00**	**3608,11**	**2101,48**	**100,74**	**100,74**	**-10,64**	**130900,43**

Contador **Gerente**

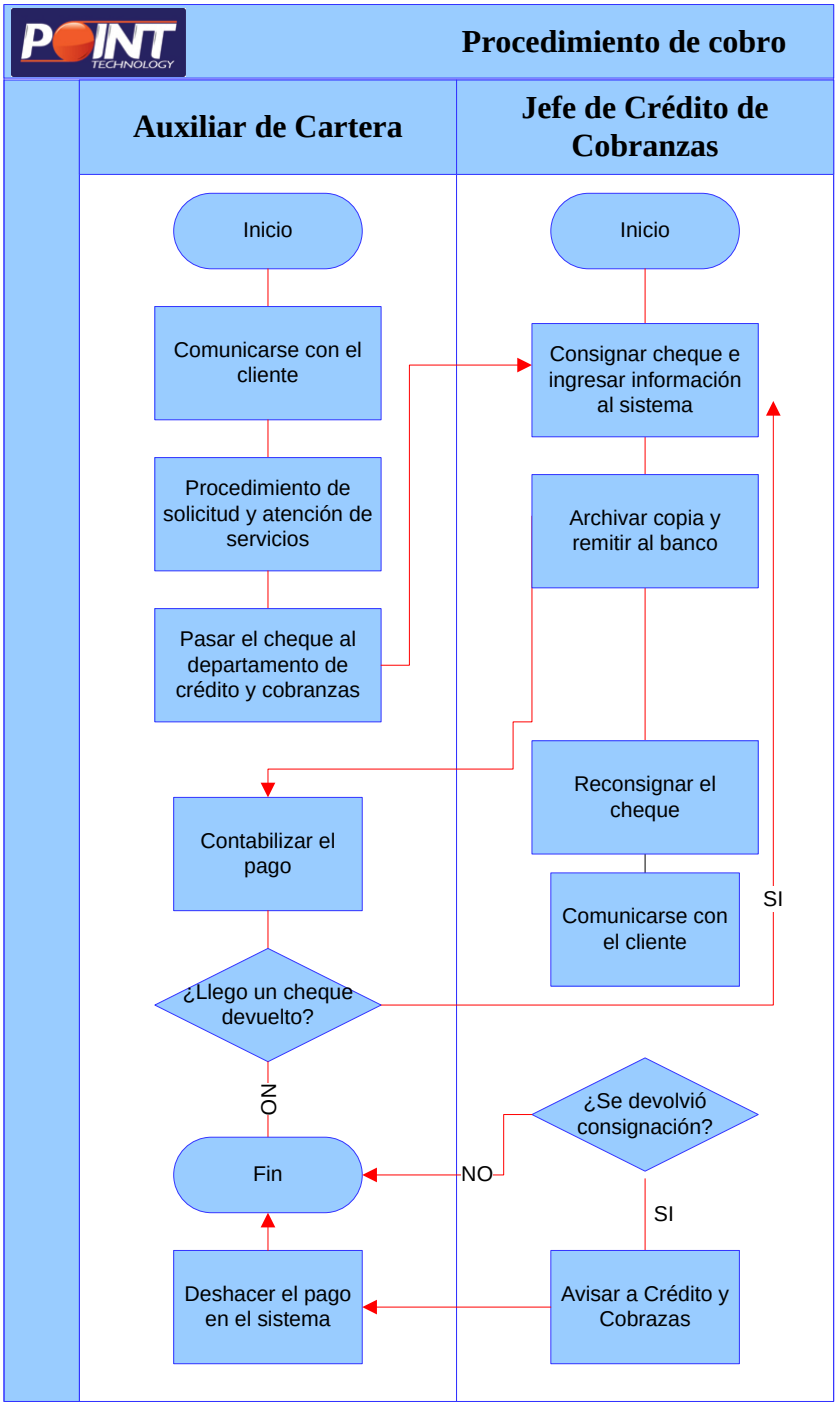
Funciones del Departamento de Crédito y Cobranzas

Sra. Andrea Freire tiene las siguientes funciones:

- Coordinar y supervisar el proceso de recuperación de cuentas por cobrar, y verificar su registro.
- Supervisar y validar las notas de crédito
- Autorizar los créditos y ampliación de los mismos a favor de terceros
- Controlar y custodiar los documentos que correspondan al Departamento.
- Efectuar la investigación crediticia de posibles clientes para el otorgamiento de créditos.
- Programar, controlar y supervisar las actividades de los cobradores adscritos al Departamento.
- Llevar un control documental y electrónico de los clientes acreditados y concesionarios.

GRÁFICO Nº 12

FLUJOGRAMA DE PROCEDIMIENTO DE COBRO



Elaborado por: Carolina Leroux S.

Responsabilidades del Departamento de Crédito y Cobranzas

- Proponer estrategias y diseñar controles administrativos para la recuperación de las cuentas por cobrar.
- Diseñar, proponer e implementar controles administrativos que permitan reducir las cuentas incobrables.
- Informar a las Gerencia sobre el comportamiento de los clientes morosos.

Documentos Generados

- Cheque

GRÁFICO Nº 13

CHEQUE PAGADO A LA EMPRESA

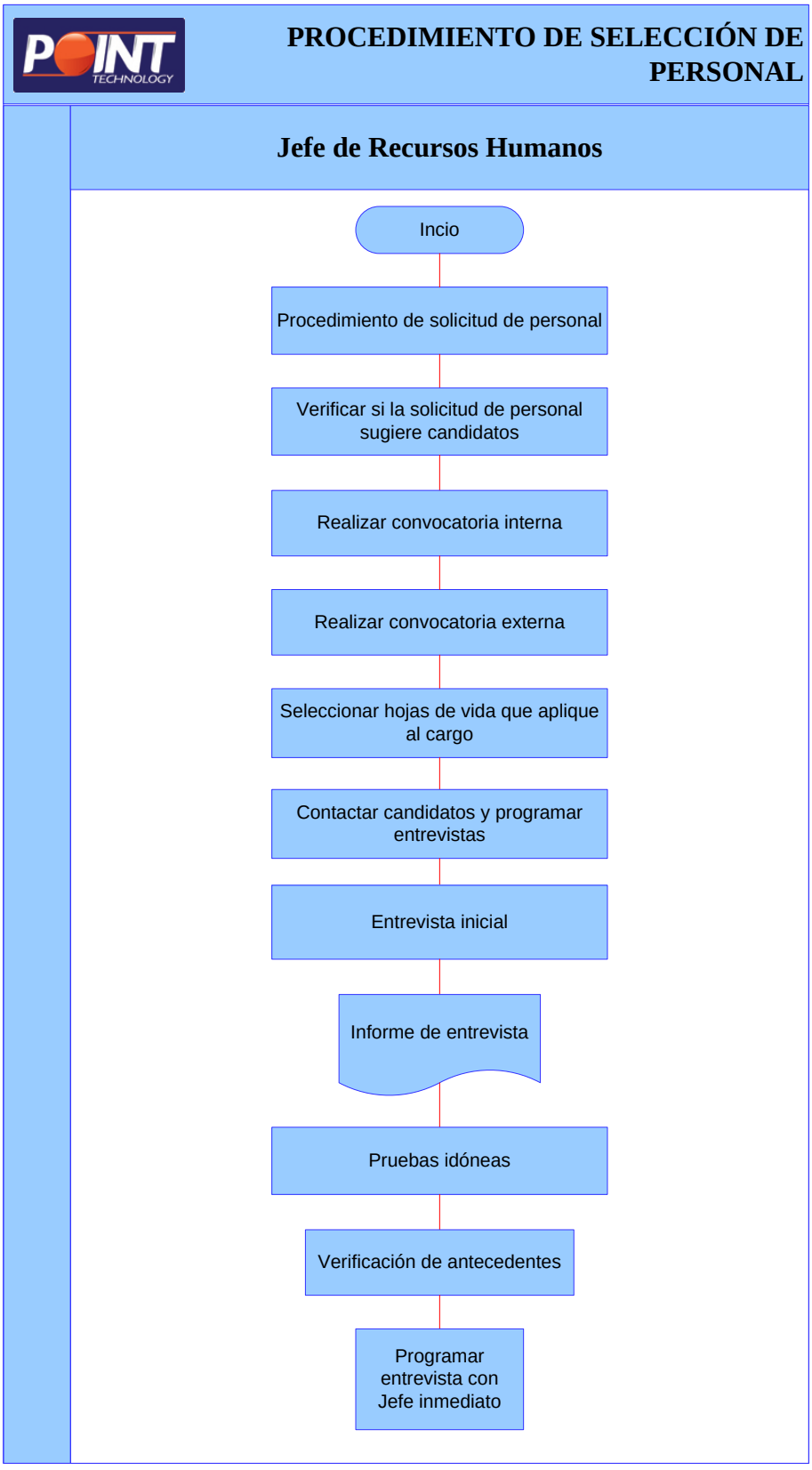
Funciones del Departamento de Recursos Humanos

Lic. Cristina Orellana tiene las siguientes funciones:

- Describe las responsabilidades que definen cada puesto laboral y las cualidades que debe tener la persona que lo ocupe.
- Prepara el cuadro de requerimiento de necesidades de personal, de igual manera efectúa las comunicaciones referente a las acciones de rotación, contratación, transferencias, promociones, ascensos y despidos de los colaboradores.
- Tiene a su cargo los registros y control de personal, incluyendo su documentación e historial laboral, destacándose entre algunos las de promoción, méritos, deméritos y felicitaciones.
- Vela por los derechos y deberes de los trabajadores (permisos, vacaciones, movilidad, salud laboral, seguridad e higiene en el trabajo, etc.), así como lo relativo a cuestiones disciplinarias.
- Evaluar el desempeño del personal, promocionando el desarrollo del liderazgo.
- Calcular remuneraciones y demás Beneficios económicos

GRÁFICO Nº 14

FLUJOGRAMA DE PROCEDIMIENTO DE SELECCIÓN DE PERSONAL



Elaborado por: Carolina Leroux S.

Responsabilidades del Departamento de Recursos Humanos

- Tiene la responsabilidad de administrar su unidad administrativa
- Conducir el proceso de selección de personal, inducirlo, capacitarlo y velar por su bienestar económico o social
- Planificar o programar con su equipo, la capacitación del personal a través de cursos, seminarios u otros.
- Mantener los puestos cubiertos y dar apoyo a los otros departamentos.
- Asesorar y participar en la formulación de la política de personal
- Dar a conocer las políticas de personal y asegurar que se cumpla por completo.
- Relacionarse con las oficinas de colocaciones y otras fuentes de mano de obra.

Documentos Generados

- Solicitud de trabajo
- Informe de entrevista
- Hoja de vida del empleado
- Rol de pagos

GRÁFICO Nº 15

ROL DE PAGOS

ROL DE PAGOS

NÓMINA MENSUAL — Desde el 01-12-2010 hasta el 31-12-2010

Ficha: 17134752 Cédula No: 1713475232 Sueldo: *******600.00 | Recibo No: 000047

Nombre: **FREIRE PIEDRA, ANDREA KATERINE** | Página: 1 de 1

Cód.	Concepto	Asignaciones	Deducciones
A01	SUELDO MENSUAL	600.00	
D01	I.E.S.S.		56.10
D08	COMIDA		20.00
D16	MULTAS		4.25
D99	OTROS		30.00
	Totales	********600.00	*******110.35
		Neto a pagar	******489.65

RECIBI CONFORME

Elaborado por: Carolina Leroux S.

GRÁFICO Nº 16

SOLICITUD DE TRABAJO

Solicitud de Empleo

Es importante contestar de manera completa la información requerida para la presentación adecuada de sus capacidades. Es indispensable mantener actualizados sus datos para lograr una mejor promoción.
En el momento de ser contratado (a) deberá hacerlo saber de inmediato a la bolsa de trabajo, al Teléfono 3343474. O al email. pointtechnology@empleos.ec

FECHA_____

Datos Personales			
Nombre Completo:			
Lugar y fecha de Nacimiento:		Estado Civil:	
Domicilio:	Colonia	Ciudad	C.P
Tel. (1) casa	Tel. (2) recados		Fax:
En caso de no vivir en León especificar Lugar de origen y Tel.		E-mail:	

Datos Escolares
Carrera: Generación de: a: Promedio General:
Institución: Pasante: ( ) Titulado: ( )

Otros Estudios **Grado**	Especialidad	Institución	Periodo	Título Obtenido
Maestría				
Diplomado				
Otros				
Otros				

Habilidades en Computación:	**Áreas de interés para trabajar:**

Disponibilidad

De viaje ○ sí ○ No
De automóvil ○ sí ○ No
De cambio de residencia ○ sí ○ No

Idioma (s)	Conversación %	Escritura %	Lectura %	Documento que lo acredite

Elaborado por: Carolina Leroux S.

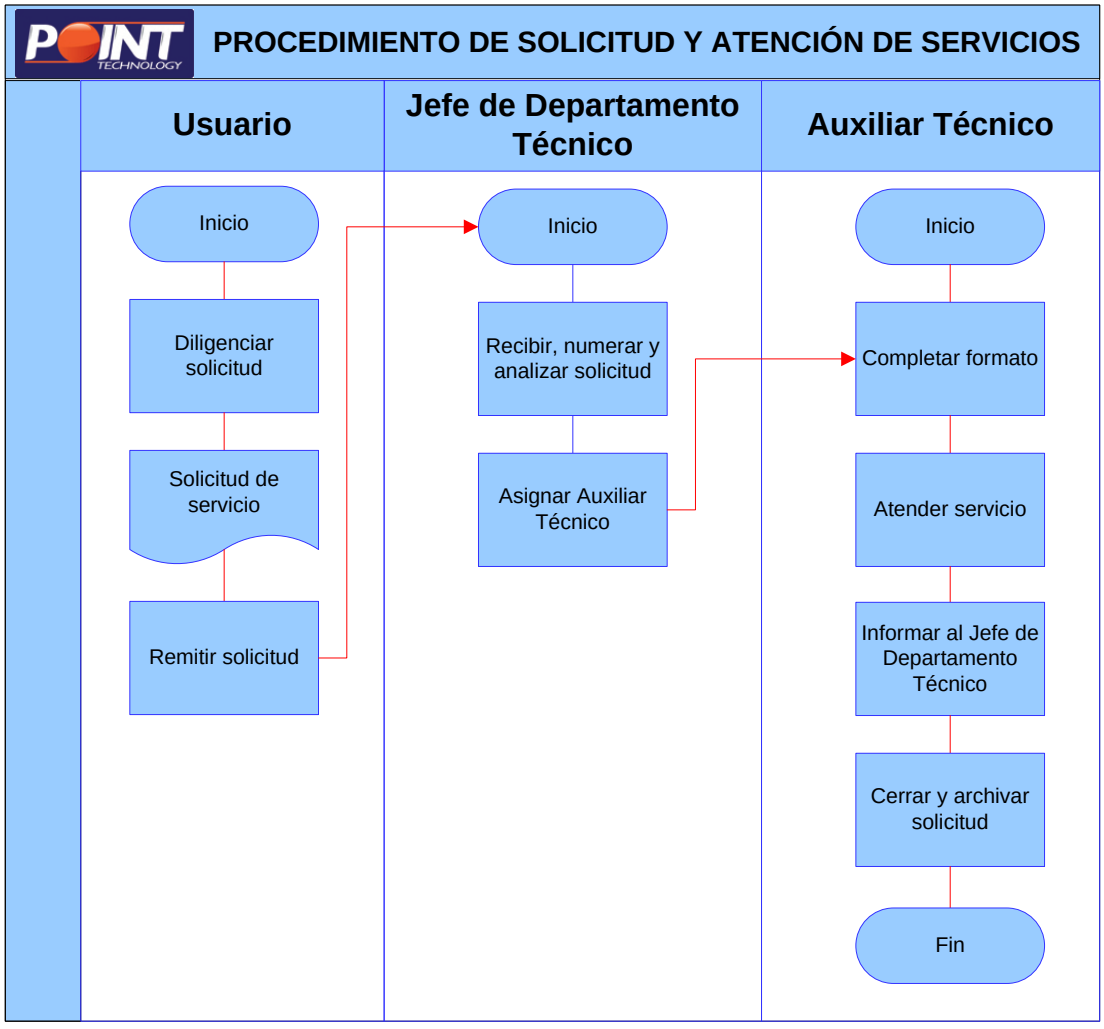
Funciones del Departamento Técnico

Srta. Estefanía Gómez tiene las siguientes funciones:

- Responder a las necesidades del cliente
- Brindar asesoramiento técnico
- Llevar a cabo revisión de los equipos antes de la entrega del producto al cliente.
- Realizar mantenimiento integral a todos los equipos en reparación que se encuentren con algún daño.

GRÁFICO Nº 17

FLUJOGRAMA DE PROCEDIMIENTO DE SOLICITUD Y ATENCIÓN DE SERVICIOS



Elaborado por: Carolina Leroux S.

Responsabilidades del Departamento Técnico

- Brindar un servicio con profesionalismo y cuidar de los productos que estén a su cargo por reparación.

Documentos Generados

- Solicitud de servicio

GRÁFICO Nº 18

SOLICITUD DE SERVICIO

CENTRO DE SERVICIO POINT
COMPROBANTE DE RECEPCION DE EQUIPOS Y ACCESORIOS

MATRIZ Quito – Ecuador: Av. El parque Entrada 2 Paseo C.C. EL BOSQUE º Local 27-112 º Teléfono: (593-2) 227-2322 º 225-8018 Email: edwin@pointecuador.com

Nº 14769

Fecha: 15/12/2010

Cliente: RIVERA CEPEDA IVAN MAURICIO Teléfono: 096057985

Problema: NO LEE USB NI CD

Accesorios del Equipo:

CANT	FACTURA Nº	DETALLE	SERIE	GARANTÍA
1		CD2. 6/2GB/500GB/DVDRW/	121210P596E08	2 AÑOS

CONDICIONES GENERALES ENTRE EL DEPARTAMENTO TÉCNICO Y EL CLIENTE

1. La mercadería que no sea retirada en **30 días** para distribuidores y **20** para consumidor final a partir de la fecha de ingreso, la mercadería será rematada sin reclamo alguno.
2. El problema del diagnóstico será dado en 48 horas a partir del ingreso del equipo.
3. Una vez que el cliente de su aprobación se procederá a la reparación. El tiempo de entrega será de acuerdo a la magnitud del problema.
4. El departamento técnico no se responsabiliza por la información que pueda perderse durante la revisión técnica, es responsabilidad del cliente tener los respaldos.
5. Si el equipo fue comprado en la empresa (Point Technology), al ingresar al Departamento Técnico automáticamente se somete a las políticas de garantía de la empresa.

Este documento es el único comprobante válido para retirar su equipo.

Point Technology Cliente

****CONTACTENOS ANTES DE RETIRAR SU EQUIPO****

Elaborado por: Carolina Leroux S.

Funciones del Departamento de Servicios Generales

Lic. Hugo Correa tiene las siguientes funciones:

- Proporcionar el servicio de cafetería a empleados y visitantes.
- Labores de mensajería local.
- Limpieza de oficinas.

Nivel Operativo

El nivel operativo de Supermercado de Computadoras Compubussines Cía. Ltda., está conformado por miembros que realizan y ejecutan las actividades y tareas en forma rutinaria y permiten el cumplimiento de las acciones tácticas que acercan a la organización al cumplimiento de los objetivos estratégicos.

Los miembros que conforman este nivel son: como Gerente de Administración en Ventas Ing. Marianela Jiménez, Compras Nacionales Lic. Elisa Asitimbay, Compras Internacionales Ing. Marianela Jiménez, como Gerente de Productos Ing. Santiago Canelos.

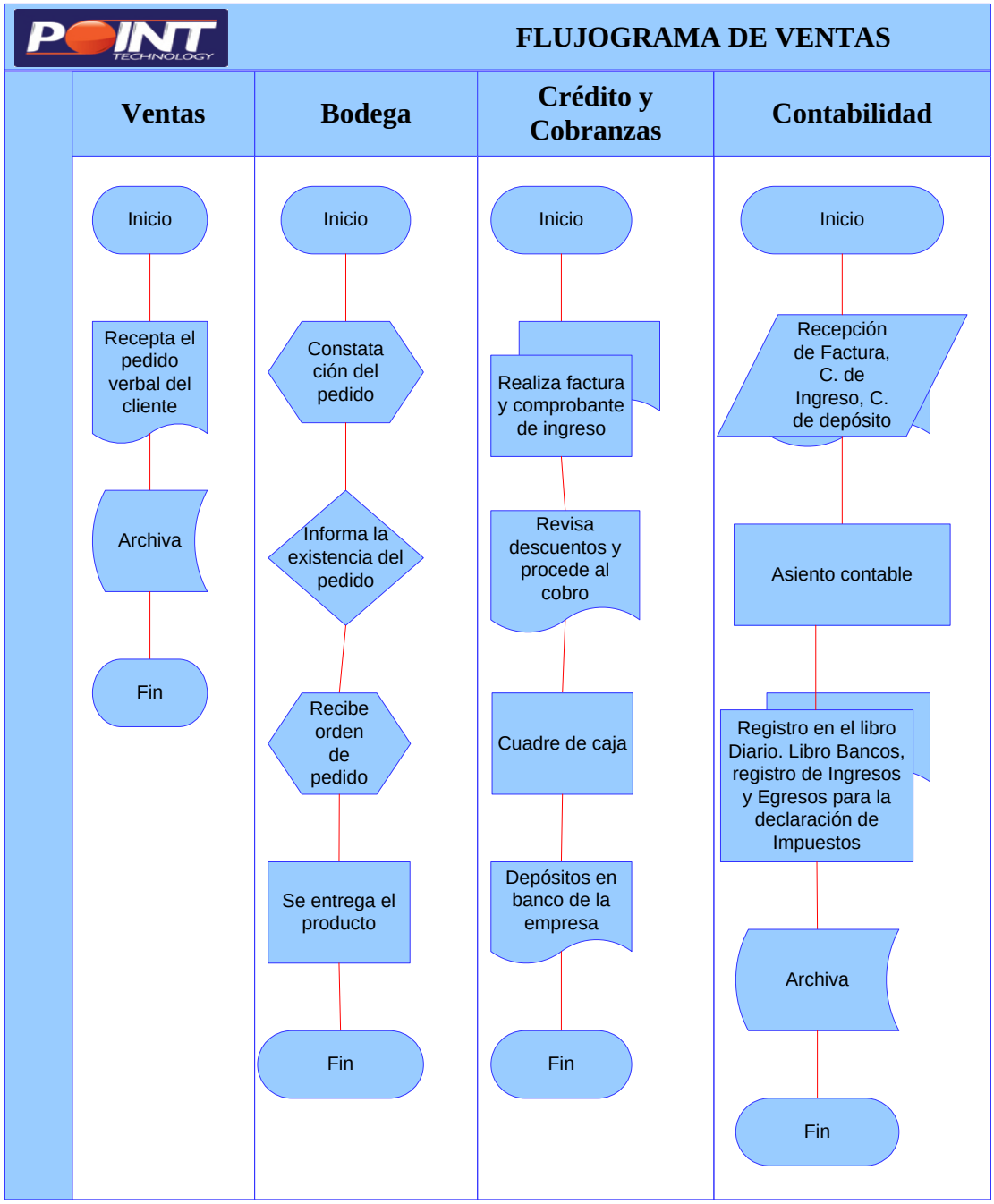
Funciones del Gerente de Administración en Ventas

Ing. Marianela Jiménez tiene las siguientes funciones:

- Administrar las ventas a nivel Nacional
- Supervisar y recibir informes de las zonas a su cargo
- Solucionar problemas de rango mayor.
- Diseñar mecanismos que impulsen la actividad de los vendedores y su consecuente alcance del cupo.
- Planeación y presupuesto de ventas.
- Estructura de la organización de ventas.
- Análisis del volumen de ventas, costos y utilidades.
- Medición y evaluación del desempeño de la fuerza de ventas.

GRÁFICO Nº 19

FLUJOGRAMA DEL DEPARTAMENTO DE VENTAS



Elaborado por: Carolina Leroux S.

Responsabilidades del Gerente de Administración en Ventas

- La responsabilidad del gerente de ventas es hacer que se cumplan los objetivos previstos de ventas a través de los esfuerzos de sus vendedores
- El gerente de ventas debe crear y mantener un equipo de vendedores estable.
- Establecer políticas de ventas.
- Planeación y presupuesto de ventas.
- Compensación, motivación y dirección de la fuerza de ventas.
- Análisis del volumen de ventas, costos y utilidades.
- Medición y evaluación del desempeño de la fuerza de ventas.
- Monitoreo, control del ámbito de la comercialización.

Documentos Generados

- Pedido de cliente
- Nota de Crédito
- Nota de Débito
- Factura
- Recibo de Caja

GRÁFICO Nº 20

PEDIDO DEL CLIENTE

PEDIDO DEL CLIENTE

Fecha: _____ **Número de pedido de cliente: _____**

Sr. (es): _____ **Fecha de Emisión: _____**
RUC o CI: _____ **Ciudad: _____**
Dirección: _____ **Email: _____**
Contacto: _____ **Embarcar a: _____**

Cantidad	Código	Descripción	Precio Unitario	Total

Sub total
Descuento
IVA 12%
Valor Total

Flete:

Pagado	
Por Cobrar	

Elaborado por: Carolina Leroux S.

GRÁFICO Nº 21

NOTA DE CRÉDITO

SUPERMERCADO DE COMPUTADORAS
COMPUBUSSINES Cía. Ltda.
RUC. 1791774682001

MATRIZ Quito – Ecuador: Av. El parque Entrada 2
Paseo C.C. EL BOSQUE º Local 27-112 º Teléfono:
(593-2) 227-2322 º 225-8018
Email: edwin@pointecuador.com

NOTA DE CRÉDITO Nº. 001 - 001-0000209

Nº. Autorización
1106724516

Sr. (es): _____ Fecha de Emisión: _____
RUC o CI: _____

Comprobante que modifica: Factura Nº

Razón de la Modificación	Valor de la modificación

IVA 12%

IVA 0%

VALOR TOTAL

Válido para su emisión hasta 05/2011

Granda Porras Yolanda / Graficas Granda
RUC: 1710501420001 / Nº. Autorización 2304
Original: Adquiriente / Copia: emisor

Elaborado por: Carolina Leroux S.

GRÁFICO Nº 22

NOTA DE DÉBITO

SUPERMERCADO DE COMPUTADORAS COMPUBUSSINES Cía. Ltda.
1791774682001

MATRIZ Quito – Ecuador: Av. El parque Entrada 2
Paseo C.C. EL BOSQUE º Local 27-112 º Teléfono: **RUC.**
(593-2) 227-2322 º 225-8018
Email: edwin@pointecuador.com

NOTA DE DÉBITO
Nº. 004 - 003-0000095

Nº. Autorización
1047844855

Sr. (es): _____ Fecha de Emisión: _____
RUC o CI: _____

Comprobante que modifica: Factura Nº _____

Razón de la Modificación	Valor de la modificación

IVA 12% _____

IVA 0% _____

VALOR TOTAL _____

Válido para su emisión hasta 05/2011
Granda Porras Yolanda / Graficas Granda
RUC: 1710501420001 / Nº. Autorización 2304

Original: Adquiriente / Copia: emisor

Elaborado por: Carolina Leroux S.

GRÁFICO Nº 23

FACTURA

SUPERMERCADO DE COMPUTADORAS COMPUBUSSINES Cía. Ltda.
RUC. 1791774682001

MATRIZ: ESTABLECIMIENTO 002: Quito – Ecuador: El Ejido º Av. 10 de Agosto N19-86 Esq. y Río de Janeiro
Teléfonos: 250-1594 /5/6 º Fax: 254-4262 º Cel. 099235051
Email: fabian@pointecuador.com
ESTABLECIMIENTO 005: C.C. EL RECREO
ESTABLECIMIENTO 006: C.C. SAN LUIS
ESTABLECIMIENTO 008: C.C. EL CONDADO
ESTABLECIMIENTO 009: C.C. IÑAQUITO

Fecha: _____ Vendedor: _____
Señor (es): _____
Dirección: _____
R.U.C./C.I.: _____ Teléfono: _____

FACTURA
Serie 002-001
Nº 0143914
Aut. SRI. 1108826694
Fecha de Caducidad: 20/10/2012

Cant.	Detalle	V. Unitario	V. Total

Son: _____
_____
Vendedor _____ Cliente _____

DESCUENTO	
SUBTOTAL	
I.V.A %	
TOTAL $	

Favor girar cheques a nombre de

SUPERMERCADO DE COMPUTADORAS COMPUBUSSINES Cía. Ltda.

SALIDA LA MERCADERÍA NO SE ACEPTAN RECLAMOS

Elaborado por: Carolina Leroux S.

GRÁFICO Nº 24

RECIBO DE CAJA

SUPERMERCADO DE COMPUTADORAS COMPUBUSSINES Cía. Ltda.
RUC. 1791774682001

MATRIZ Quito – Ecuador: Av. El parque Entrada 2 Paseo C.C. EL BOSQUE º Local 27-112 º Teléfono: (593-2) 227-2322 º 225-8018
Email: edwin@pointecuador.com
ESTABLECIMIENTO 002: Quito – Ecuador: Av. 10 de Agosto 983 y Río de Janeiro º Teléfonos: 250-1594 /5/6
Fax: 254-4262 º Cel. 099235051
ESTABLECIMIENTO 003: Quito – Ecuador: Av. 6 de Diciembre 26-66 y San Ignacio de Núñez Teléfonos: 222-4144 º 252-2389

RECIBO DE CAJA

Nº 001862

Por $

Fecha: _____
Recibí de: _____
La cantidad de: _____
_____

Dólares

Por concepto de: _____

☐ FORMA DE PAGO ☐ CHEQUE ☐ EFECTIVO ☐ TARJETA DE CREDITO	CHEQUE: _____ EFECTIVO: _____ TARJETA DE CREDITO: _____ BANCO: _____ GIRADOR: _____ FECHA DE COBRO: _____

Recibido	Es conforme	
_____	_____	_____
CAJA	**CONTABILIDAD**	**GERENCIA**

Elaborado por: Carolina Leroux S.

Funciones del Departamento de Compras Nacionales e Internacionales

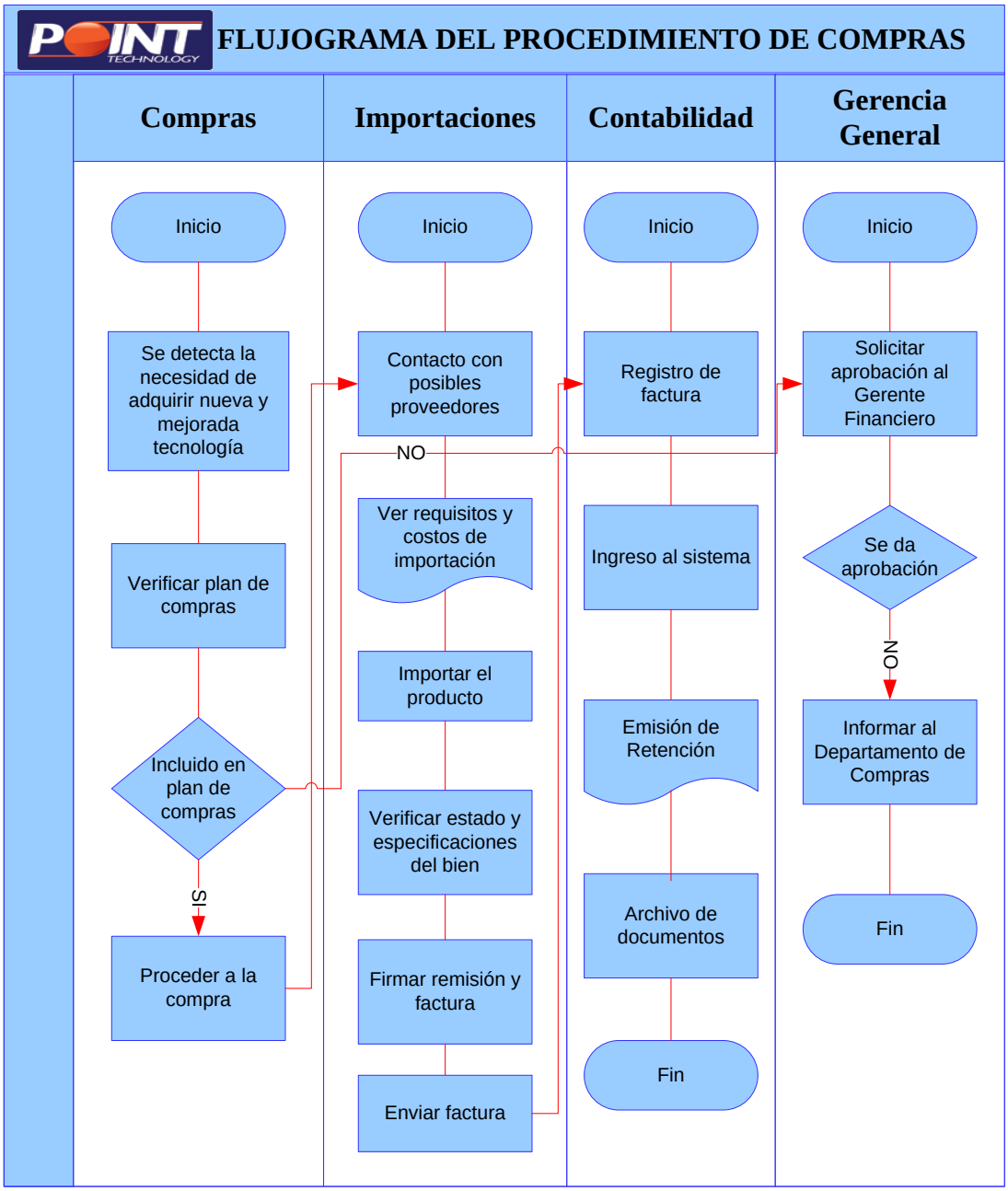
Lic. Elisa Asitimbay y la Ing. Marianela Jiménez tienen las siguientes funciones:

- Tener listas de precios con o sin impuestos.
- Controlar los descuentos, bonificaciones, recargos de administración de compras y cambios de precios al facturar.
- Emitir de comprobantes por lote.

- Realizar las retenciones de impuestos a los proveedores.
- Controlar el stock por unidades
- Mantener una base de datos de proveedores calificados, representantes, transportistas, vendedores.
- Disponer del número de cuentas corrientes de los proveedores.
- Agrupamientos y subagrupamientos de artículos.

GRÁFICO Nº 25

FLUJOGRAMA DEL PROCESAMIENTO DE COMPRAS



Elaborado por: Carolina Leroux S.

Responsabilidades del Departamento de Compras Nacionales e Internacionales

- Solicitar información sobre las características de los productos
- Tomar en cuenta los servicios, políticas de ventas, seriedad, calidad y precio que los proveedores ofrecen, todo esto para tomar la decisión con quién se va hacer el negocio.

Documentos Generados

- Ingresos
- Documentos de importación
- Factura o remisión

GRÁFICO Nº 26

FACTURA DE PROVEEDOR

TECNOMEGA **RUC: 1790040275001**

Factura
Nº. 011 - 002-0066367

MATRIZ: Av. Colón E4-81 y Av. 9 de Octubre

Nº. Autorización
1107832292

Sr. (es): _____ Fecha de Emisión: _____
RUC o CI: _____Guía de emisión: _____
Dirección: _____

Cantidad	Descripción	Precio Unitario	Valor de Venta

Sub total 12%
Descuento
Sub total
IVA 12%
Valor Total

Industria Manufacturera de Productos de Oficina
RUC: 0990579385001 / Nº. Autorización 1102
Original: Adquiriente/ Copia: emisor
Válido para su emisión hasta 10/2010

Elaborado por: Carolina Leroux S.

Funciones del Gerente de Productos

Ing. Santiago Canelos tiene las siguientes funciones:

- Ejerce la administración comercial de los productos actuales, realiza estudios sobre el mercado, la clientela y la competencia.
- Busca el desarrollo de nuevos productos
- Realiza la preparación y coordinación de los planes de mercadeo relacionados con sus productos.
- Mide, evalúa y da seguimiento de los presupuestos y de la rentabilidad integral de los productos a su cargo.
- Es responsable de la capacitación y el conocimiento de los funcionarios de la cadena comercial que vendan sus productos.
- En las etapas de introducción de un producto nuevo es responsable de la promoción y las ventas iniciales.
- Investiga al consumidor acerca de sus necesidades y gustos.
- Desarrolla canales de distribución
- Fija precios

Responsabilidades del Gerente de Productos

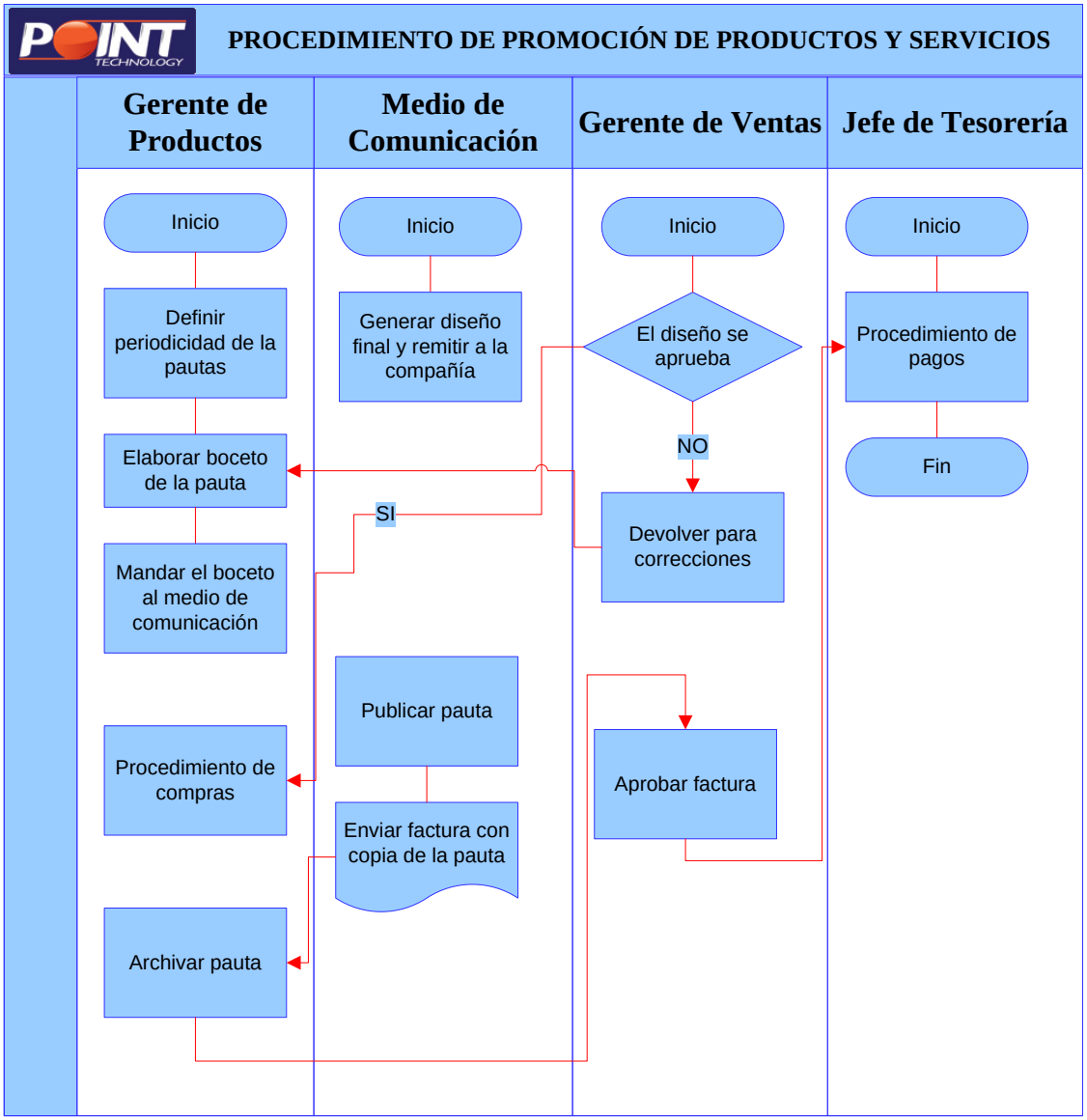
- Coordinar el personal a su cargo de manera eficiente y respetuosa.
- Dirigir la ejecución de los diferentes proyectos que se estén llevando a cabo al interior de la Compañía.
- Atender cualquier duda o requerimiento de los clientes en cuanto al servicio prestado.
- Controlar el uso del presupuesto asignado a cada proyecto.
- Tener constante comunicación con el Departamento Técnico con el fin de elevar la calidad del servicio y ampliar el alcance del mismo.

Documentos Generados

- Boceto de publicidad y Factura

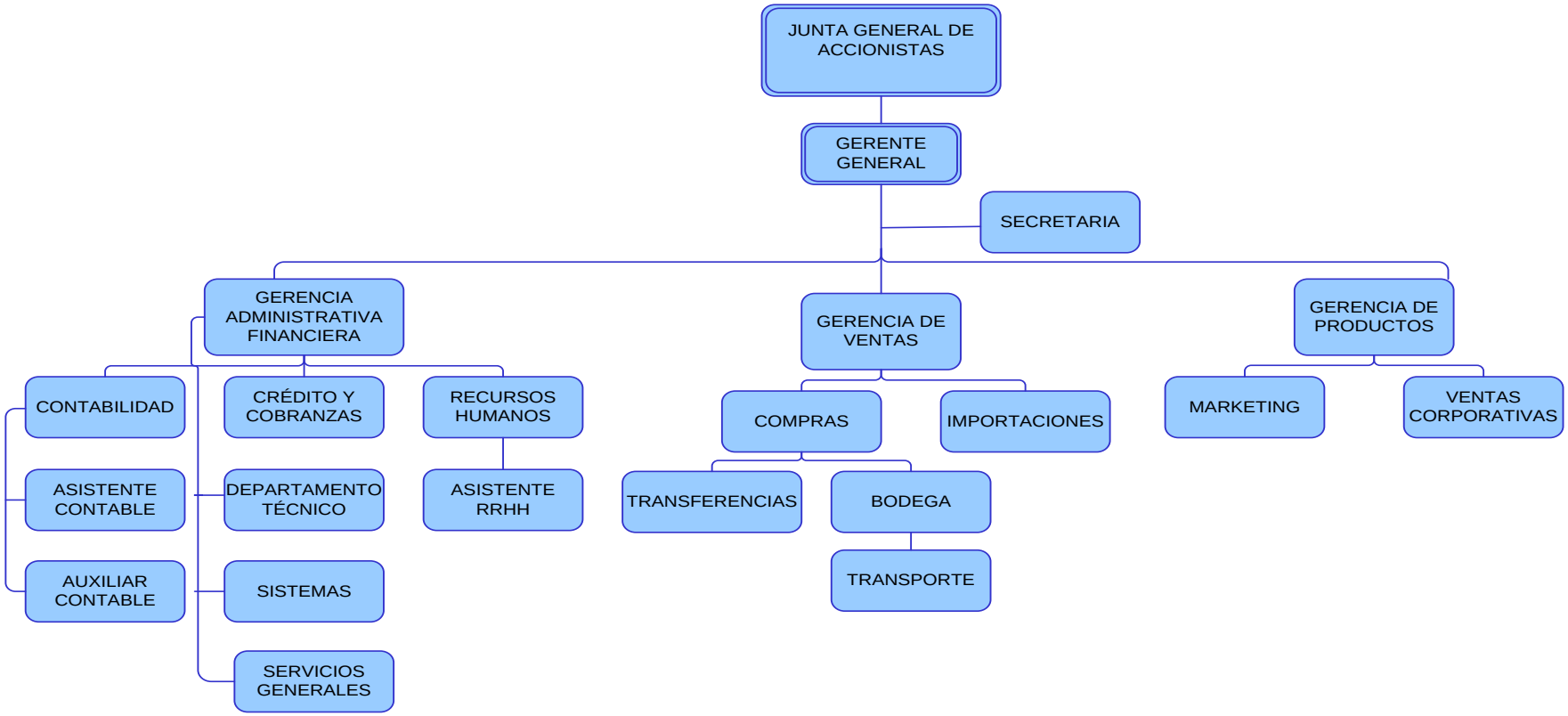
GRÁFICO Nº 27

FLUJOGRAMA DE PROCEDIMIENTO DE PROMOCIÓN DE PRODUCTOS Y SERVICIOS



Elaborado por: Carolina Leroux S.

ORGANIGRAMA ESTRUCTURAL SUPERMERCADO DE COMPUTADORAS COMPUBUSSINES CIA. LTDA.



Preparado por: Carolina Leroux S.
Fuente: Supermercado de Computadoras Compubussines Cía. Ltda.

2.2.1.2. Los Proveedores

Son las empresas que proporcionan los recursos requeridos por la organización para la venta de sus productos, entre los proveedores más importantes con los que cuenta la entidad tenemos:

a. A nivel nacional contamos con: Siglo 21, Intcomex, Tecnomega, entre otros
b. A nivel internacional contamos con: Bell micro, Ingram micro, Max Usa Corps, entre otros.

Políticas de compras:

- Las adquisiciones son realizadas en la matriz por:
  a. A nivel nacional está encargada la Sra. Elisa Asitimbay
  b. A nivel internacional la Ing. Marianela Jiménez.
- Las adquisiciones no son respaldadas por una orden de compra.
- Por ser una empresa con innovación en la tecnología adquiere lo primero que sale al mercado sin cotizar precios.
- Solamente el almacén está autorizado para recibir los pedidos y las facturas respectivas.
- Los descuentos concedidos por proveedores son aplicados como notas de créditos.

2.2.1.3. Los Clientes

Son todas las personas naturales o jurídicas, las cuales adquieren productos o servicios de la empresa, entre los principales clientes con los que cuenta la empresa tenemos:

a. Consumidor final como las tiendas de almacén de centros comerciales que representan el 80 % de las ventas.
b. El otro 20% representa los clientes corporativos, entre ellos están: Jaher, Paco, Dilipa, TVentas, entre otros.

Políticas de ventas:

- Se dan líneas de crédito directo abiertas para el público en general
- El producto vendido está garantizado contra defectos en material y mano de obra.

2.2.2. Macro Ambiente de Supermercado de Computadoras Compubussines Cía. Ltda.

El macro ambiente comprende las fuerzas sociales que afectan a todo el microambiente e incluye las fuerzas demográficas, económicas, políticas, competitivas.

2.2.2.1. Ambiente competitivo

Cada organización debe tomar en cuenta su tamaño y posición en el mercado con respecto a sus competidores. Para Supermercado de Computadoras Compubussines Cía. Ltda., su estrategia para sobrevivir es satisfacer las necesidades y los deseos de los consumidores mejor que como lo hace la competencia.

Los principales competidores a los que se enfrenta la organización son: Colambay, Computron, Cinticomp, TVentas, entre otros.

2.2.2.2. Ambiente demográfico

Es muy importante conocer la ubicación de la organización, Supermercado de Computadoras Compubussines Cía. Ltda., está ubicado en la República del Ecuador, Provincia de Pichincha, Ciudad de Quito, Sector El Ejido, en la Av. 10 de Agosto N1- y Rio de Janeiro.

Es un sector comercial propicio para la venta de computadoras, línea blanca, línea café (equipos de sonido), y artículos para el hogar; atrae al público ya que a muy pocos pasos se encuentra el IESS y esto crea mayor comercio.

2.2.2.3. Ambiente económico

Consiste en los factores que afectan el poder de adquisición y los patrones de gasto de los consumidores. El poder de adquisición depende del ingreso, el precio, los ahorros y el crédito del momento; se deben conocer las principales tendencias económicas, tanto en el ingreso como en los de gastos que enfrentan los consumidores.

Actualmente la empresa cuenta con líneas de crédito directo abiertas para todo el público en general, para así poder generar mayores ventas para la empresa e ir creciendo con el tiempo y dar mejor servicio a su clientela.

2.2.2.4. Ambiente político

Está integrado por leyes, oficinas gubernamentales y grupos de presión que influyen y limitan las actividades de diversas organizaciones e individuos en la sociedad.

Con la política actual que está viviendo el país se ha visto afectado por los aranceles que implementó el gobierno ya que las ventas decayeron un poco, pero sin embargo la empresa no pierde sus ganancias y siempre vive a la expectativa de las decisiones políticas.

2.3. Departamento de Sistemas; Evaluación del Desempeño

Todas las empresas u organizaciones, también llamadas instituciones están compuestas por áreas o departamentos, los cuales permiten confortar una estructura organizacional basada en centros especializados de actividades y una distribución mejor definida de responsabilidades.

Hasta hace algunos años un Departamento de Sistemas pertenecía al último grupo, y solo lo consideraban aquellas organizaciones con los suficientes recursos para mantenerlo, aún cuando no generara ingresos, pero poco a poco esta idea ha dejado de existir para convertirse en la convicción de que un Departamento de Sistemas es de vital importancia dentro de la compañía ya que es el encargado de proveer a esta, de información, lo cual en nuestros días es indispensable para la sobrevivencia de las empresas.

2.3.1. Finalidad del Departamento de Sistemas

- Tiene por objetivo mantener los sistemas informáticos y de los equipos computacionales y colaborar a la optimización de los procedimientos administrativos, con el apoyo del hardware y/o software que sea necesario.

2.3.2. Objetivo General del Departamento de Sistemas

- Diseñar, desarrollar, implantar y mantener los sistemas de información que requieran la organización, conforme a las normas, estándares y prioridades establecidos.

2.3.3. Principales Funciones del Departamento de Sistemas

- La principal función de un Departamento de Sistemas es crear y ofrecer sistemas de información que permitan dar solución a las necesidades informáticas y de toma de decisiones de la institución.
- La administración y mantenimiento de los sistemas existentes en el grupo
- Asesoría y capacitación a los diferentes departamentos y empresas del grupo
- Estudios de factibilidad, compra e instalación de equipo
- Evaluación y adquisición de software y paquetería
- Desarrollo de nuevos sistemas
- Elaboración de manuales y documentación
- Administración y mantenimiento de Pcs, Redes y equipo
- Prestar soporte a usuarios en todo lo relativo a la plataforma computacional

- Revisión periódica de las necesidades de información
- Contratación de servicios y asesorías externas
- Mantenimiento y reparación de equipo de computo
- Control de compras de todo lo relacionado con equipo, software, consumibles y accesorios computacionales.
- Implementación y administración de los servicios de Internet e Intranet y correo electrónico.
- Velar por la integridad de la información almacenada en equipos computacionales, además de elaborar y ejecutar los planes de contingencia necesarios en caso de pérdida de dicha información

2.4. Departamento de Contabilidad; Evaluación del Desempeño

Es importante que la organización cuente con los instrumentos que permitan a la administración de la empresa determinar cuán efectiva y eficiente está siendo la labor de los empleados en el logro de los objetivos y, por ende, el cumplimiento de la misión organizacional, la evaluación de desempeño se convierte en un instrumento que estimula en el empleado, en las áreas organizacionales y en la empresa en su conjunto, un comportamiento adecuado y genera una mejora continua.

2.4.1. Finalidad del Departamento Contable

- Este Departamento tiene como finalidad instrumentar y operar las políticas, normas, sistemas y procedimientos necesarios para garantizar la exactitud y seguridad en la captación y registro de las operaciones financieras, presupuestales y de consecución de metas de la entidad, a efecto de suministrar información que contribuya a la toma de decisiones, a promover la eficiencia y eficacia del control de gestión, a la evaluación de las actividades y facilite la fiscalización de sus operaciones, cuidando que dicha contabilización se realice con documentos y justificativos originales, y vigilando la debida observancia de las leyes, normas y reglamentos aplicables.

2.4.2. Objetivos Generales

- Generar de manera oportuna, confiable y consistente, de acuerdo a las normas generales de contabilidad, la información contable producto de las distintas operaciones y/o transacciones financiero-presupuestarias de la empresa.
- Asesorar a las autoridades y dependencias de la empresa, acerca de las normas y leyes que rigen, específicamente aquellas que guardan relación con la parte contable.
- Velar por el cumplimiento de las normas de contabilidad de aceptación general y reglamentaciones establecidas.
- Supervisar y controlar el uso y custodia, por parte de cada departamento de la empresa, de los distintos bienes muebles e inmuebles, tangibles e intangibles propiedad de la misma.

2.4.3. Principales Funciones

- Registrar y controlar las cuentas de balance y de gastos que genere la organización de acuerdo al Catálogo de Cuentas, Guía Contabilizadora y principios de Contabilidad.
- Registrar y controlar los movimientos correspondientes a la cuenta de impuestos.
- Supervisar y cotejar el registro de las operaciones contables de acuerdo a la normatividad establecida.
- Recopilar, analizar y consolidar la información contable generada por las áreas administrativas.
- Revisar, integrar y archivar las pólizas cheque, de diario e ingreso que se generen durante el periodo.
- Elaborar mensualmente los Estados Financieros y los informes correspondientes, como son: Registro de Diario, Registros al Mayor, Subcuentas, Estado de Resultados, Balance de Comprobación y Balance General.

2.4.4. Principales Procesos que ejecuta el Departamento Contable.

Sección Contabilidad General:

- El departamento de Contabilidad General lleva, para los efectos de control, un registro sumario de la información obtenida y empleada por todas las demás secciones.
- Elabora el Mayor General, que contiene las cuentas de control para cada sección de la empresa.
- Elabora El Diario General como medio de pase para hacer los asientos en las cuentas de Mayor General.
- Elabora la preparación de comprobantes relativos a todos los cargos.
- Elabora la preparación de los informes financieros que se establecen periódicamente.
- Elabora la preparación de informes específicos que requieran la presidencia, gerencia general o gerencia financiera.
- Elabora la preparación de informes específicos que requieren las entidades gubernamentales. (SRI, SUPERINTENDENCIA DE COMPAÑIAS, MUNICIPIO. ETC.).

Sección Contabilidad de Costos:

Esta contabilidad es complementaria a la Contabilidad General y cuyo ámbito es el departamento técnico. Esta sección tiene a su cargo el siguiente trabajo:

- Todas las cuentas relativas a las operaciones del departamento técnico.
- Las hojas detalladas de trabajo que determina cada obra o pedido en particular.
- Registro de todas las actividades en el departamento técnico, es decir, la mano de obra directa, las materias primas (repuestos), los materiales y los gastos de fabricación.

- La supervisión de los vales o requisiciones de salidas de repuestos y materiales, con objeto de hacer la clasificación necesaria para su asiento en los registros de costo.

Clasificación y análisis de ventas:

La clasificación de las ventas es muy extensa por lo que es conveniente que haya una sección separada del departamento de Contabilidad para clasificar cada partida de las facturas de ventas. Como las facturas se toman como base para los análisis del costo de ventas, esta sección será responsable de la exposición de su resultado y de la clasificación que se haga con este fin:

- Tabulación de las facturas de ventas en la forma que convenga a los efectos de control.
- La preparación de informes con los resultados de las tabulaciones efectuadas.

Sección de nóminas:

La sección de Nóminas tiene a su cargo el trabajo detallado a continuación:

- Revisar el cálculo de las nóminas
- La transferencia de pago a los empleados y trabajadores de la empresa de manera mensual
- La preparación y elaboración de planillas del IESS en forma mensual.

Sección de acreedores:

La información que recibe esta sección se genera directamente del departamento de adquisiciones el cual tiene dos flujos de ingresos de datos: compras locales e importaciones. Es de la competencia de esta sección:

- Registro de las facturas de compras a pagar con la distribución contable de las mismas.

- Elaboración de los comprobantes de retenciones que obliga el Estado Ecuatoriano.
- Preparación de los comprobantes de pago para todas las facturas
- Preparación de cheques para el pago de comprobantes, que han de someterse a la firma de la gerencia financiera.
- Archivo de comprobantes pagados y de los pendientes de pago.
- Contabilización de los desembolsos de Caja Menor.

Sección de Deudores:

- El Mayor de las partidas a cobrar, que contienen las cuentas de los clientes.
- La preparación de los extractos mensuales de cuenta que hayan de enviarse a los clientes y utilizarse como información en el departamento de Créditos.
- Realiza la gestión de cobranza vía telefónica o personal.

Sección de facturación:

- Elaboración y cálculo de las facturas que se cursen a los clientes previa inspección del pedido en el departamento de ventas, o la proforma elaborada en el departamento técnico.

Sección de inventarios:

- Efectúa constataciones de inventarios físicos en los almacenes de repuestos y materiales en forma semestral, anual o cuando se requiera.
- Registro del ingreso de mercaderías tanto por compras locales como por importaciones.
- Registro del egreso de mercaderías según requisiciones de las diferentes áreas de la empresa, tanto para ventas de almacén como para trabajos del taller.
- Emite informes de las novedades de los kárdex de mercaderías.
- Fija precios de venta según política antes establecida por costumbre.
- Verifica en el sistema informático los costos a través del recalculo
- Cruza información con contabilidad.

CAPÍTULO III

3. METODOLOGÍAS DE ADMINISTRACIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN Y SEGURIDAD.

La metodología es el fruto del nivel profesional de cada uno y de su visión de cómo conseguir un mejor resultado en el nivel de control de cada entidad, aunque el nivel de control resultante debe ser similar. Pero en realidad todas ellas son herramientas de trabajos mejores o peores que ayudan a conseguir mejores resultados.

El siguiente capítulo describe a varias técnicas metodológicas en Administración de Riesgos, que pretenden lograr objetividad en la valoración de los riesgos, permitiendo el control, seguimiento y evaluación de la administración de riesgos sobre bases objetivas.

3.1. Introducción a las Metodologías

A la palabra *Metodología* se la define como el "Conjunto de métodos que se siguen en una investigación científica o en una exposición doctrinal".

Las Metodologías usadas por un profesional dicen mucho de su forma de entender su trabajo y están directamente relacionadas con su experiencia profesional acumulada como parte del comportamiento humano de acierto/error.

La metodología es necesaria para que un equipo de profesionales alcance un resultado homogéneo tal como si lo hiciera una solo, por lo que resulta habitual el uso de metodologías en las empresas auditoras/consultoras.

Seguridad de los Sistemas de Información; es la doctrina que trata de los riesgos informáticos o creados por la informática.

La informática crea unos riesgos informáticos de los que hay que proteger y preservar a la entidad con un entramado de contramedidas, y la calidad y la eficacia de las mismas.

Para explicar este aspecto se puede decir que cualquier contramedida nace de la composición de varios factores expresados en el siguiente grafico:

GRÁFICO Nº 29

SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Elaborado por: Carolina Leroux S.

- **NORMATIVA**, debe definir todo lo que debe existir y ser cumplido tanto desde el punto de vista conceptual, cómo práctico.

- **ORGANIZACIÓN**, es la que integran personas con funciones específicas y con actuaciones concretas; éste es el aspecto más importante, dado que in él, nada es posible.

- **METODOLOGÍAS**, son necesarias para desarrollar cualquier proyecto que nos propongamos de manera ordenada y eficaz.

- **OBJETIVOS DE CONTROL**, son los objetivos a cumplir en el control de procesos, este es el segundo más importante.

- **PROCESAMIENTO**, son los procedimientos operativos de las distintas áreas de la empresa, la tendencia habitual de los informáticos es la de dar más peso a las herramientas que al control o contramedida, pero no debemos olvidar que: "UNA HERRAMIENTA NUNCA ES UNA SOLUCION SINO UNA AYUDA PARA CONSEGUIR UN CONTROL MEJOR"

- **TECNOLOGÍAS DE SEGURIDAD,** es donde están todos los elementos ya sean Hardware o software, que ayudan a controlar un riesgo informático.

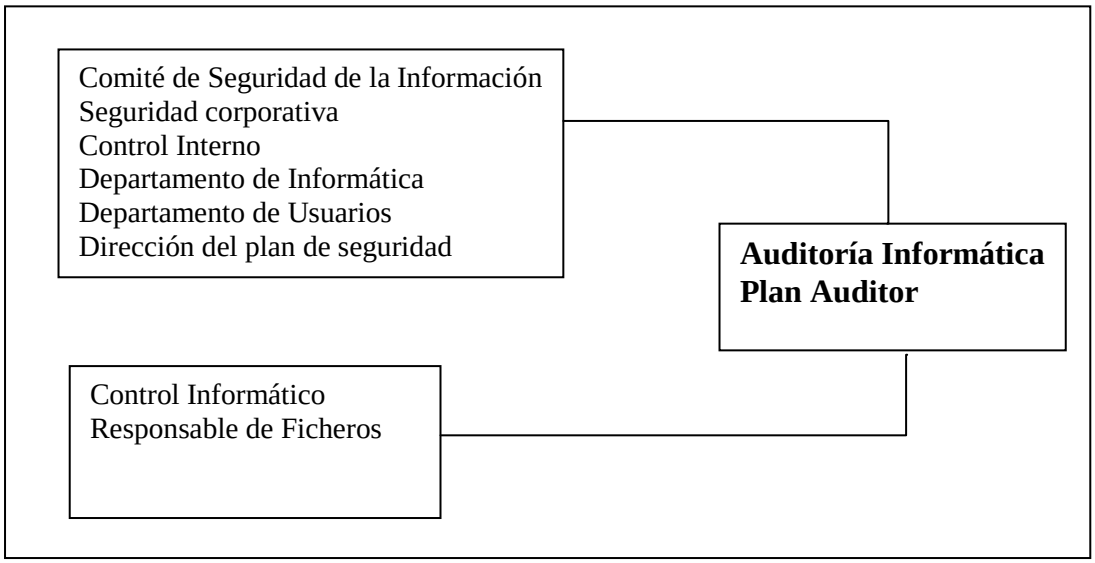
- **LAS HERRAMIENTAS DE CONTROL**, son elementos software que permiten definir uno o varios procedimientos de control para cumplir una normativa y un objetivo de control

Plan de Seguridad; es una estrategia planificada de acciones y productos que lleven a un sistemas de información y sus centros de proceso de una situación inicial determinada a una situación mejorada.

En el siguiente grafico se observa la tendencia actual en la organización de la seguridad de sistemas en la empresa.

GRÁFICO Nº 30

ORGANIZACIÓN INTERNA DE LA SEGURIDAD INFORMÁTICA



Elaborado por: Carolina Leroux S.

3.2. Metodologías de Evaluación de Sistemas

3.2.1. Conceptos Fundamentales

El sistema de evaluación para determinar la calificación es el de considerar dos metodologías de evaluación de sistemas que son:

- **Análisis de Riesgos:** El análisis de riesgos facilita la "evaluación" de los riesgos y recomienda acciones en base al costo-beneficio de las mismas.

- **Auditoría Informática:** La auditoría informática sólo identifica el nivel de "exposición" por la falta de controles. mientras

A continuación algunas definiciones para profundizar en estas metodologías.

Amenaza: Una(s) persona(s) o cosa(s) vista(s) como posible fuente de peligro o catástrofe. Ejemplo: inundación, incendio, robo de datos, sabotaje, aplicaciones mal diseñadas, etc.

Vulnerabilidad: La situación creada, por la falta de uno o varios controles, con la que la amenaza pudiera suceder y así afectar el entorno informático. Ejemplos: falta de control de acceso lógico, inexistencia de un control de soportes magnéticos, falta de cifrado en las telecomunicaciones, etc.

Riesgo: La probabilidad de que una amenaza llegue a suceder por una vulnerabilidad. Ejemplo: los datos estadísticos de cada evento de una base de datos de incidentes.

Exposición o Impacto: La evaluación del efecto del riesgo. Ejemplo: es frecuente evaluar el impacto en términos económicos, aunque no siempre lo es, como vidas humanas, imagen de la empresa, honor, defensa nacional, etc.

Todos los riesgos que se presentan podemos:

- *Evitarlos* (por ejemplo: no construir un centro donde hay peligro constante de inundaciones).

- *Transferirlos* (por ejemplo: uso de un centro de cálculo controlado).

- *Reducirlos* (por ejemplo: sistema de detección y extinción de incendios).

- *Asumirlos*. Que es lo que se hace si no se controla el riesgo en absoluto.

Para los tres primeros, se actúa si se establecen controles. Todas las metodologías existentes en seguridad de sistemas van encaminadas a establecer y mejorar los controles que garanticen que la probabilidad de que las amenazas se materialicen en hechos (por falta de control) sea lo más baja posible o al menos quede reducida de una forma razonable en costo – beneficio.

3.2.2. Tipos de Metodologías

Las metodologías utilizadas en la auditoría y el control informático, se dividen en dos grandes familias. Éstas son:

3.2.2.1. Cuantitativas

Basadas en un modelo matemático numérico que ayuda a la realización del trabajo, están diseñadas para producir una lista de riesgos que pueden compararse entre sí con facilidad, por tener asignados unos valores numéricos. Estos valores son datos de probabilidad de ocurrencia de un evento que se debe extraer de un riesgo de incidencias donde el número de incidencias tiende al infinito.

3.2.2.2. Cualitativas/Subjetivas

Basadas en el criterio y raciocinio humano capaz de definir un proceso de trabajo, para seleccionar en base al experiencia acumulada. Puede excluir riesgos significantes desconocidos (depende de la capacidad del profesional para usar el check-list/guía). Basadas en métodos estadísticos y lógica borrosa, que requiere menos recursos humanos / tiempo que las metodologías cuantitativas.

A continuación se presenta un cuadro comparativo en donde se destaca las ventajas y desventajas entre las Metodologías Cuantitativa y Cualitativa:

	CUANTITATIVA	**CUALITATIVA / SUBJETIVA**
PROS	- Enfoca pensamientos mediante el uso de números. - Facilita la comparación de vulnerabilidades muy distintas. - Proporciona una cifra "justificante" para cada contramedida	- Enfoca lo amplio que se desee. - Plan de trabajo flexible y reactivo. - Se concentra en la identificación de eventos. - Incluye lectores intangibles.
	CUANTITATIVA	**CUALITATIVA / SUBJETIVA**
CONTRAS	- Estimación de probabilidad depende de estadísticas fiables inexistentes. - Estimación de las pérdidas potenciales solo si son valores cuantificables. - Metodologías estándares. - Difíciles de mantener o modificar. - Dependencia de un profesional.	- Dependencia fuertemente de la habilidad y calidad del personal involucrado. - Puede excluir riesgos significantes desconocidos (depende de la capacidad del profesional para usar el check-list/guía). - Identificación de eventos reales más claros al no tener que aplicarles probabilidades complejas de calcular. - Dependencia de un profesional.

Por consiguiente, los dos grandes inconvenientes o problemas que presentan estas metodologías son: por una parte la debilidad de los datos de la probabilidad de ocurrencia por los pocos registros y la poca significación de los mismos a nivel mundial, y por otra la imposibilidad o dificultad de evaluar económicamente todos los impactos que pueden suceder frente a la ventaja de poder usar un modelo matemático para el análisis.

3.3. Auditoría Informática

Las tecnologías de la información son vitales para una organización en la medida en la que éstas dan soporte a sus procesos esenciales de negocio, no obstante, todos los beneficios que de esto se deriva se ven amenazados por numerosos riesgos que requieren ser controlados para garantizar que este soporte sea efectivo; en otras palabras se requiere de un sistema de control interno eficaz, eficiente y una labor periódica de supervisión o de auditoría informática.

La Auditoría Informática permite detectar la falta de un control, comprobar su correcto o deficiente funcionamiento así como la verdadera utilidad del mismo, recomendando el perfeccionamiento necesario al sistema de control interno sobre la base de la relación costo – beneficio de este sistema para el servicio informático a la entidad.

La Auditoría Informática es un campo de importancia actual y de excelente proyección futura ya que va de la mano con el avance de las tecnologías de la información.

La Auditoria Informática certifica la integridad de los datos informáticos que usan los auditores financieros para que puedan utilizar los sistemas de información para sus dictámenes.

3.3.1. Conceptos de Auditoría Informática

- Proceso metodológico que tiene el propósito principal de evaluar todos los recursos (humanos, financieros, tecnológicos, etc.) relacionados con la

función de informática para garantizar al negocio que dicho conjunto opera con criterio de integración y desempeño de niveles altamente satisfactorios para que apoyen la productividad y rentabilidad de la organización.

- El conjunto de acciones que realiza el personal especializado en las áreas de auditoría y de informática para el aseguramiento continuo de que todos los recursos de informática operen en un ambiente de seguridad y control eficiente, con la finalidad de proporcionar a la alta dirección o niveles ejecutivos, la certeza de que la información que pasa por el área se maneja con los conceptos básicos de integridad, totalidad, exactitud, confiabilidad, etc.

- La verificación de controles en el procesamiento de la información, desarrollo de sistemas e instalaciones, con el objeto de evaluar su efectividad y presentar recomendaciones a la gerencia.

3.3.2. Importancia de la Auditoría Informática

Entre los puntos clave que reflejan la importancia de la auditoría informática, destacamos los siguientes:

- La alta sistematización de las organizaciones
- Nuevas tecnologías
- Automatización de los controles
- Integración de la información
- Importancia de la información para la toma de decisiones

3.3.3. Objetivo de la Auditoría Informática

El objetivo fundamental de la Auditoría Informática es asesorar a los diferentes niveles de la Administración de la empresa en el cumplimiento efectivo de sus responsabilidades, facilitándoles análisis, apreciaciones, comentarios y recomendaciones relacionados con las actividades del procesamiento de la información en el computador.

- **EFECTIVIDAD.-** Es el logro de las metas establecidas después de considerar las alternativas.

- **EFICIENCIA.-** Es el logro de las metas con el menor costo posible. Los costos se expresan en términos de recursos.

- **ECONOMÍA.-** Consiste en eliminar todo desperdicio, extravagancia y duplicación.

3.3.4. Organismo Regulador de Auditoría Informática

ISACA (Information Systems Audit and Control Association - Asociación de Auditoría y Control de Sistemas de Información)

Certificaciones Otorgadas:

ISACA mantiene el programa de certificación CISA que es reconocida en forma global y ha sido obtenida por más de 30.000 profesionales alrededor del mundo. De otro lado, su nueva certificación CISM (Certified Information Security Manager - Gerente Certificado de Seguridad de Información) se concentra exclusivamente en el sector de gerencia de seguridad de la información.

3.3.5. Metodologías de Auditoría Informática

Las metodologías de auditoría informática son del tipo cualitativo / subjetivo. Se puede decir que son las subjetivas por excelencia. Por lo tanto, están basadas en profesionales de gran nivel de experiencia y formación, capaces de dictar recomendaciones técnicas, operativas y jurídicas, que exigen una gran profesionalidad y formación continuada. [13]

Existen dos metodologías de Auditoria Informática:

[13] PIATTINI, Mario, *Auditoría Informática: Un Enfoque Práctico*, 2da. Edición, Editorial RA-MA, Madrid – España 2004, p. 65.

a) **Auditorias de Controles Generales**: como producto estándar de los auditores profesionales.

Objetivo de las Auditorías de Controles Generales:

Dar una opinión sobre la fiabilidad de los datos del computador para la auditoría financiera, cuyo resultado es un informe donde se destacan las vulnerabilidades encontradas.

b) **Auditorías Internas:** Esta formada por recomendaciones de Plan de trabajo de auditoría.

Características de las Auditorías de Controles Generales y Auditorías Internas:

- Están basadas en pequeños cuestionarios estándares que dan como resultado informes muy generalistas.
- Tiene apartados para definir "pruebas" y anotar sus resultados.
- Deben demostrar con pruebas todas sus afirmaciones, y por ello siempre debe contener el anexo de pruebas.

El Plan Auditor Informático

Es el esquema más importante del auditor informático. En este documento se debe describir todo sobre esta función y el trabajo que realiza en la entidad. Debe estar en sintonía con el plan auditor del resto de los auditores de la entidad.

Las partes con las que cuenta un plan auditor informático son:

- **Funciones**, ubicación de la figura en el organigrama de la empresa. Debe existir una clara segregación de funciones con la Informática y de control interno informático, y éste debe ser auditado también. Deben describirse las funciones de forma precisa, y la organización interna del departamento, con todos sus recursos.

- **Procedimientos** para las distintas tareas de las auditorias, entre ellos están el procedimiento de apertura, el de entrega y discusión de debilidades, entrega de informe preliminar, cierre de auditoría, redacción de informe final, etc.

- **Tipos de auditoría** que realiza, metodologías y cuestionarios de las mismas. *Ejemplo*: revisión de la aplicación de facturación, revisión de seguridad física, revisión de control interno, etc. Existen tres tipos de auditorías según su alcance: la Full o completa de una área (por ejemplo: control interno, informática, limitada a un aspecto; por ejemplo: una aplicación, la seguridad lógica, el software de base, etc.), la Corrective Action Review (CAR) que es la comprobación de acciones correctivas de auditorías anteriores.

- **Sistema de evaluación** y los distintos aspectos que evalúa. Independientemente de que exista un plan de acciones en el informe final, debe hacerse el esfuerzo de definir varios aspectos a evaluar como nivel de gestión económica, gestión de recursos humanos, cumplimiento de normas, etc., así como realizar una evaluación global de resumen para toda la auditoría.

- **Nivel de exposición** permite en base a la evaluación final de la última auditoría realizada sobre ese tema definir la fecha de la repetición de la misma auditoría.

- **Lista de distribución de informes**

- **Seguimiento de acciones correctoras**

- **Plan quincenal.** Todas las áreas a auditar deben corresponderse con cuestionarios metodológicos y deben repartirse en cuatro o cinco años de trabajo. Esta planificación, además de las repeticiones y añadido de las auditorías no programadas que se estimen oportunas, deberá componer anualmente el plan de trabajo anual.

- **Plan de trabajo anual.** Deben estimarse tiempos de manera racional y componer un calendario que una vez terminado nos dé un resultado de horas de trabajo previstas y, por tanto, de los recursos que se necesitarán.

3.4. Ejemplo de Metodología de Auditoría de una aplicación.

Metodología de Trabajo

Revisión de controles sobre aplicaciones

Objetivo

Determinar que los sistemas producen informaciones exactas y completas en el momento oportuno. Esta área es tal vez la más importante en el trabajo de auditorías informativas.

Programa de revisión

1. Identificar el área a revisar (por ejemplo, a partir del calendario de revisiones), notificar al responsable del área y prepararse utilizando papeles de trabajo de auditorías anteriores.

2. Identificar las informaciones necesarias para la auditoría y para las pruebas.

3. Obtener informaciones generales sobre el sistema. En esta etapa, se definen los objetivos y el alcance de la auditoría, y se identifican los usuarios específicos que estarían afectados por la auditoría (plan de entrevista).

4. Obtener un conocimiento detallado de la aplicación/sistema. Se pasan las entrevistas con los usuarios y el personal implicado en el sistema a revisar; se examina la documentación de usuarios, de desarrollo y de operación, y se identifican los aspectos más importantes del sistema (entrada, tratamiento, salida de datos, etc.), la periodicidad de procesos, los programas fuentes, características y estructuras de archivos de datos, así como pistas de auditoría.

5. Identificar los puntos de control críticos en el sistema. Utilizando organigramas de flujos de informaciones, identificar los puntos de control críticos en entrevistas con los usuarios con el apoyo de la documentación sobre el sistema. El auditor tiene que identificar los peligros y los riesgos que podrían surgir en cada punto. Los puntos de control críticos son aquellos donde el riesgo es más grave, es decir, donde la necesidad de un control es más importante. A menudo, son necesarios controles en los puntos de interfaz entre procedimientos manuales y automáticos

6. Diseño y elaboración de los procedimientos de la auditoría.

7. Ejecución de pruebas en los puntos críticos de control. Se podría incluir la determinación de las necesidades de herramientas informativas de ayuda a la auditoría no informática. Se revisa el cumplimiento de los procedimientos para verificar el cumplimiento de los estándares y los procedimientos formales, así como los procesos descritos por los organigramas de flujos. Así se verifican los controles internos del cumplimiento de

    a. planes, políticas, procedimientos, estándares,
    b. del trabajo de la organización,
    c. requerimientos legales,
    d. principios generales de contabilidad y
    e. prácticas generales de informática

Se hacen revisiones substantivas y pruebas, como resultado de la revisión del cumplimiento de procedimientos. Si las conclusiones de la revisión de cumplimentación fuesen generalmente positivas, se podían limitar las revisiones substantivas.

Dentro de este punto del programa de la revisión podríamos analizar si existen los siguientes controles:

Controles de preparación de datos

Revisar procedimientos escritos para iniciar, autorizar, recoger, preparar y aprobar los datos de entrada en la forma de un manual de usuario. Verificar que los usuarios entienden y siguen estos procedimientos.

Revisar que se dé la formación del "uso del terminal" necesaria a los usuarios.

Revisar los documentos fuente u otros documentos para determinar si son numerados. También revisar códigos de identificación de transacciones y otros campos de uso frecuentes para determinar si son codificados previamente para minimizar errores en los procesos de preparación, entrada y conversión de datos.

Cuando sea necesario, verificar que todos los datos de entrada en un sistema pasan por validación y registro antes de su tratamiento.

Determinar si los usuarios preparan totales de control de los datos de entrada por terminales. Comprobar la existencia de una reconciliación de los totales de entrada con totales de salida.

Comprobar la existencia y seguimiento de calendarios de entrada de datos y de distribución de informes (listados).

Determinar si el archivo y retención de documentos fuente y otros formularios de entrada son lógicos y accesibles, y cumple las normas y requerimientos legales.

Revisar los procedimientos de corrección de errores.

Comprobar la existencia de períodos de retención para documentos fuente y soportes magnéticos.

Controles de entrada de datos

Establecer los procedimientos de entrada y control de datos que explican las revisiones necesarias de entradas y salidas, con fecha límite, criterios de validación de datos de entrada; códigos, mensajes y detección de errores; la corrección de errores y la reentrada de datos.

Para sistemas interactivos, verificar el uso de métodos preventivos para evitar la entrada incorrecta de datos funciones de ayuda a la pantalla, formatos fijos, el uso de menús y mensajes para el operador.

Para sistemas interactivos, determinar la grabación de datos de entrada con fecha y hora actual, así como con una identificación del usuario/terminal y ubicación.

Revisar log's de acceso por líneas de telecomunicaciones para determinar posibles accesos y entradas no autorizados.

Revisar los programas para determinar si contienen procesos internos de validación de datos (por ejemplo, chequeos de dígitos, test razonables, totales de batch, número de cuentas, etc.). Evaluar su exactitud.

Comparar, validar, apuntar y recalcular campos o elementos de datos críticos por métodos manuales o automáticos.

Para sistemas interactivos determinar que los datos se verifican en el momento de su entrada en el sistema.

Comprobar que los usuarios revisan regularmente las tablas internas del sistema para validar sus contenidos.

Revisar funciones matemáticas que redondean cálculos para ver si tienen implicaciones negativas.

Determinar que existen pistas de auditoría adecuadas en el diccionario de datos. Identificar la interrelación entre los programas y los datos para dejar la posibilidad de seguir la pista de datos dentro de programas y sistemas en los errores.

Revisar los procedimientos de corrección de errores.
Identificar con los usuarios cualquier código de errores críticos que deberían aparecer en momentos específicos pero que nunca surgen.

Controles de tratamiento y actualización de datos

Ver si hay establecidos controles internos automatizados de proceso, tales como rutinas de validación, en el momento de la actualización de los archivos de transacción, referencia y maestros.

Identificación de transacciones por el uso de números de batch, códigos de transacción y otros indicadores.

Revisión del log de transacciones para identificar problemas encontrados por el operador y las medidas seguidas.

Restricción de la posibilidad de pasar por encima de procesos de validación.

Aceptación por los usuarios finales de todas las transacciones y cálculos de la aplicación.

Revisar los totales de control de entrada de datos.

Verificar que existen totales de control para confirmar la buena interfaz entre jobs o programas.

Comprobar que existen validaciones entre totales de control, manuales y automáticos, en puntos de la interfaz entre procesos manuales y automatizados.

Verificar que los log's de actividad de sistemas son revisados por los responsables, para investigar accesos y manipulaciones no autorizados.

Ver los controles sobre la entrada de datos.

Controles de salida de datos

Determinar si los usuarios comparan totales de control de los datos de entrada con totales de control de datos de salida.

Determinar si el control de datos revisa los informes de salida (listados) para detectar errores evidentes tales como campos de datos que faltan, valores no razonables o formatos incorrectos.

Verificar que se hace una identificación adecuada sobre los informes, por ejemplo, nombre y número de informe, fecha de salida, nombre de área/departamento, etc.

Comparar la lista de distribución de informes con los usuarios que los reciben en realidad. ¿Hay personas que reciben el informe y que no deberían recibirlo?

Verificar que los informes que pasan de aplicabilidad se destruyen, y que no pasan simplemente a la basura, sin seguridad de destrucción.

Revisar la justificación de informes, que existe una petición escrita para cada uno y que se utilizan realmente, así como que está autorizada la petición.

Verificar la existencia de períodos de retención de informes y su suficiencia.

Revisar los procedimientos de corrección de los datos de salida.

Controles de documentación

Verificar que dentro de las actividades de desarrollo y mantenimiento de aplicaciones se produce la documentación de sistemas, programas, operaciones y funciones, y procedimientos de usuario.

Existencia de una persona específica encargada de la documentación y que mantiene un archivo de documentos ya distribuidos y a quiénes.

Comprobar que los jefes de área se informen de faltas de documentación adecuada para sus empleados.
Destrucción de toda la documentación de antiguos sistemas.

Que no se acepten nuevas aplicaciones por los usuarios sin una documentación completa.

Actualización de la documentación al mismo tiempo que los cambios y modificaciones en los sistemas.

La existencia de documentación de sistemas, de programas, de operación y de usuario para cada aplicación ya implantada.

Controles de backup y rearranque

Existencia de procedimientos de backup y rearranque documentados y comprobados para cada aplicación en uso actualmente.

Procedimientos escritos para la transferencia de materiales y documentos de backup entre el C.P.D. (Centro de Procesos de Datos) principal y el sitio de backup (centro alternativo). Mantenimiento de un inventario de estos materiales.

Existencia de un plan de contingencia.

Identificación de aplicaciones y archivos de datos críticos para el plan de contingencia.

Revisar los contratos del plan de contingencia y backup para determinar su adecuación y actualización.

Pruebas de aplicaciones críticas en el entorno de backup, con los materiales del plan de contingencia (soportes magnéticos, documentación, personal, etc.).

Determinación de qué se revisa, si cada aplicación de un sistema es crítica y si debería incluirse en el plan de contingencia

Grabación de todas las transacciones ejecutadas por teleproceso, cada día; para facilitar la reconstrucción de archivos actualizados durante el día en caso del fallo del sistema.

Existencia de procesos manuales para sistemas críticos en el caso del fallo de contingencia.

Actualización del plan de contingencia cuando es necesario; pruebas anuales.

Controles sobre programas de auditoría

Distribución de políticas y procedimientos escritos a auditores y responsables de áreas sobre la adquisición, desarrollo y uso de software de auditoría.

Uso de software de auditoría únicamente por personas autorizadas.

Participación del auditor en la adquisición, modificación/adaptación, instalación de paquetes de software de auditoría.

Participación del auditor en la planificación, diseño, desarrollo e implantación de software de auditoría desarrollado internamente.

Formación apropiada para los auditores que manejan software de auditoría.

Participación del auditor en todas las modificaciones y adaptaciones del software de auditoría, ya sea externo o de desarrollo propio. Actualización de la documentación de software.

Verificación de que los programas de utilidad se utilizan correctamente (cuando no se puede utilizar el software de auditoría).

Revisión de tablas de contraseñas para asegurar que no se guardan identificaciones y contraseñas de personas que han causado baja.

Controles de la satisfacción de los usuarios

Disponibilidad de políticas y procedimientos sobre el acceso y uso de la información.

Resultados fiables, completos, puntuales y exactos de las aplicaciones (integridad de datos).

Utilidad de la información de salida de la aplicación en la toma de decisión por los usuarios.

Comprensión por los usuarios de los informes e informaciones de salida de las aplicaciones.

Satisfacción de los usuarios con la información que produce la aplicación.

Revisión de los controles de recepción, archivo, protección y acceso de datos guardados sobre todo tipo de soporte.

Participación activa de los usuarios en la elaboración de requerimientos de usuarios, especificaciones de diseño de programas y revisión de resultados de pruebas.

Controles por el usuario en la transferencia de informaciones por intercambio de documentos.

Resolución fácil de problemas, errores, irregularidades y omisiones por buenos contactos entre usuarios y el personal

Revisiones regulares de procesos que podrían mejorarse por automatización de aspectos particulares o reforzamientos de procesos manuales

Evaluación de la revisión y/o resultados de pruebas. En esta etapa se identifican y se evalúan los puntos fuertes y débiles de los procedimientos y prácticas de control interno en relación con su adecuación, eficiencia y efectividad. Cuando se identifique una debilidad, se determinará su causa.

Se elaboran las conclusiones basadas sobre la evidencia; lo que deberá ser suficiente, relevante, fiable, disponible, comprobable y útil.

Preparación del informe. Recomendaciones.

Informe previo

Para mantener una relación buena con el área revisada, se emite un informe previo de los puntos principales de la revisión. Esto da a los responsables del área revisada la posibilidad de contribuir a la elaboración del informe final y permitirá una mejor aceptación por parte de ellos.

Informe final de la revisión

Se emite el informe final después de una reunión con los responsables del área implicados en la revisión. El contenido del informe debería describir los puntos de control interno de la manera siguiente:

- Opinión global (conclusión).
- Problema(s) específico(s).

- Explicación de la violación de los controles internos, planes organizacionales, estándares y normas.
- Descripción de los riesgos, exposición o pérdidas que resultarían de las violaciones.

Cuando sea posible, se identificará el impacto de cada problema en términos económicos. Se da una solución específica y práctica para cada debilidad. Se identificarán las personas que se responsabilizarán de cada aspecto de las soluciones. Las recomendaciones son razonables, verificables, interesantes económicamente y tienen en cuenta el tamaño de la organización.

El informe debe tener un tono constructivo. Si es apropiado se anotan los puntos fuertes.
Para su distribución, se preparará un resumen del informe.

Después de la revisión del informe final con los responsables del área revisada se distribuirá a las otras personas autorizadas.

El área auditada tiene la posibilidad de aceptar o rechazar cada punto de control. Todos los puntos rechazados se explicarán por escrito. El área acepta los riesgos implícitos de la debilidad encontrada por el auditor.

CAPÍTULO IV

4. APLICACIÓN DE ADMINISTRACIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN COMO MECANISMO PARA OPTIMIZAR EL ANÁLISIS DE LOS ESTADOS FINANCIEROS.

El principal objetivo de la administración de riesgos para la empresa Supermercado de Computadoras Compubussines Cía. Ltda., es garantizar la supervivencia de la organización, minimizando los costos asociados con los riesgos.

Para llevar a cabo con este objetivo vamos a establecer un *plan de contingencia*, con la finalidad de asegurar la capacidad de supervivencia de la compañía, ante eventos que pongan en peligro su existencia.

También queremos proteger y conservar los activos de la empresa, de riesgos, desastres naturales o actos mal intencionados. Así como también reducir la probabilidad de las pérdidas, a un mínimo de nivel aceptable, a un costo razonable y asegurar la adecuada recuperación.

Queremos asegurar que existan controles adecuados para reducir el riesgo por fallas o mal funcionamiento tanto del equipo, como del software, de los datos, y de los medios de almacenamiento.

Nuestra función es comunicar a todo el personal activo de la empresa los pasos a seguir en caso de cualquier riesgo.

Los Papeles de Trabajo que se va utilizar se detallan a continuación:

1. **Análisis de Riesgos.**

A – 1 Programa de Auditoría para el Análisis de Riesgos de Tecnologías de Información de la Empresa Supermercado de Computadoras Compubussines Cía. Ltda.

A – 2 Cuestionario de Control Interno.

A – 3 Carta a la empresa solicitando información para la Verificación de Control Interno.

A – 4 Entrevista de Control Interno.

A – 5 Carta a la empresa solicitando información para sustentar los procedimientos de protección de información.

A – 6 Test para evaluación de competencias y cualidades profesionales.

A – 7 Detalle de Hallazgos.

2. Medidas Preventivas.

B – 1 Programa de Auditoría para Medidas Preventivas.

B – 2 Cuestionario de Control Interno.

B – 3 Lista de Chequeo para inspecciones de seguridad.

B – 4 Lista de Chequeo para observaciones de seguridad.

B – 5 Detalle de Hallazgos.

3. Informe Final.

C – 1 Programa de Auditoría para la Elaboración del Informe Final sobre los resultados del Análisis de Riesgos.

C – 2 Detalle de Hallazgos obtenidos en etapas anteriores.

C – 3 Detalle de Hallazgos sobre el mismo tema.

C – 4 Hallazgos eliminados.

C – 5 Borrador del Informe de Auditoría.

C – 6 Minuta de reunión con el personal directivo.

C – 7 Informe definitivo.

4.1. Información Preliminar

4.1.1. Introducción

Supermercado de Computadoras Compubussines Cía. Ltda., ubicada en el centro de la ciudad, es una líder en la distribución y venta de equipos tecnológicos, teniendo

por ello, un mercado competitivo muy grande de donde quiere resaltar por la calidad y combinación de sus productos.

El edificio de Casa Central se encuentra aislado de los edificios aledaños, con vigilancia las 24 horas del día. Tanto la Matriz, como las sucursales cuentan con sistemas de alarmas.

Con respecto a la disposición física de los servidores de la Matriz se encuentran ubicados en el segundo piso del edifico, para protegerlos de cualquier tipo de inundación. Los pisos de las sucursales y la Matriz son de tablón, por debajo del mismo pasan los cableados, separados los de datos, con los de energía eléctrica.

Ambos edificios (Matriz / sucursales), cuentan con salidas de emergencia. También cuentan con extinguidores de clase A, B y C (aptos para instalaciones eléctricas), y tanto la Matriz, como las sucursales cuentan con sistemas de detección de humo e irrigación.

En la Matriz se cuenta con Encargados de Mantenimiento y Sistemas. Cada persona deberá registrarse con su tarjeta magnética para el control de ingreso y salida al edificio.

La empresa Supermercado de Computadoras Compubussines Cía. Ltda., cuenta con un Departamento de Sistemas destinado al uso del desarrollo. En el área informática se cuenta con el desarrollo de software utilizados para la misma organización. Además cuenta con el Departamento de Contabilidad que es el encargado de reflejar el estado de situación económica que posee la empresa.

Los responsables de estos departamentos tienen que buscar el equilibrio deseado entre todos sus elementos. Su objetivo, en la Administración de Riesgos de TI, será el optimizar el análisis de los estados financieros.

Las evaluaciones de los controles y seguridades de los sistemas de la empresa constituyen uno de los pilares básicos que contribuyen a alcanzar los objetivos y por ende el crecimiento y desarrollo de la empresa.

4.2. Análisis de Riesgos

PROGRAMA DE AUDITORÍA PARA EL ANÁLISIS DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN DE LA EMPRESA SUPERMERCADO DE COMPUTADORAS COMPUBUSSINES CÍA. LTDA.

CLIENTE **:** SUPERMERCADO DE COMPUTADORAS
FECHA AUDITADO **:** 01 de Enero al 31 de Diciembre de 2009
FECHA DE ELABORACIÓN **:** 17 de Febrero de 2010

1. ALCANCE

Todas las áreas administrativas y operativas de la entidad.

2. OBJETIVO GENERAL:

Analizar los procesos de protección, administración y disposición de la información, identificando sus diferentes fases, los flujos de información que se generan y los instrumentos que se utilizan.

3. OBJETIVOS ESPECÍFICOS:

3.1 Obtener un conocimiento general del control interno sobre los procesos de información.
3.2 Evaluar el sistema de control y diseñar pruebas de cumplimiento adicionales para las afirmaciones sobre los procesos de información.
3.3 Realizar pruebas adicionales a los controles que los auditores piensan considerar para soportar sus niveles evaluados y planificados de control.
3.4 Verificar la adecuada presentación y revelación en los estados financieros.

FECHA	Nº	PROCEDIMIENTOS	REF.	RESPONSABLE	OBS.
	1	Realice la evaluación del control interno de la empresa, utilizando para el efecto el cuestionario incluido en este programa y realice pruebas de cumplimiento de los procedimientos descritos.	A – 2	Carolina Leroux	
	2	Verifique en los Manuales los procedimientos, políticas y normativa de la empresa y examine la documentación sustentatoria.	A – 3	Carolina Leroux	
	3	Realice pruebas visuales para comprobar los procesos administrativos que se realizan para obtener la información.	A – 4	Carolina Leroux	
	4	Investigue los procedimientos de protección de información.	A – 5	Carolina Leroux	
	5	Verifique la documentación sustentatoria de los procedimientos de protección de información.	A – 5	Carolina Leroux	
	6	Establezca lo adecuado del procedimiento de protección de información.	A – 5	Carolina Leroux	
	7	Evaluar la competencia y cualidades de los profesionales, la experiencia en el tipo de trabajo ejecutado y su reputación.	A – 6	Carolina Leroux	
	8	Prepare una hoja en la que se muestre un detalle de los hallazgos encontrados: la hoja deberá	A – 7	Carolina Leroux	

FECHA	Nº	PROCEDIMIENTOS	REF.	RESPONSABLE	OBS.
		contener las siguientes columnas: • Condición • Causa • Criterio • Efecto • Recomendación			

Elaborado por:

Fecha: 12/12/2010

Supervisado por:

Fecha: 12/12/2010

A continuación se observa el desarrollo del programa de auditoría:

CUESTIONARIO DE CONTROL INTERNO

1. ¿Describa el uso de los reportes de trabajos realizados por el Departamento?

Una vez realizado el reporte de algún cliente, éste es entregado al Jefe del Departamento y éste a su vez es el encargado de archivarlo.

2. ¿Qué criterio tiene en cuanto a la eliminación o modificación desautorizadas de reportes?

Si se llegase a dar el caso, todo depende del Jefe del Departamento ya que es él quien se encarga de ellos.

3. Se cuenta con un manual de usuario de los siguientes programas:

PROGRAMA	SI	NO	COMPRENSIBLE
Sistema Financiero		X	
Sistema Contable		X	
Sistema de Facturación	X		SI
Sistema de Compras	X		SI
Sistema de Ventas	X		SI
Sistema de Inventarios		X	
Sistema de Pagos		X	
Sistema de Cuentas por Cobrar		X	

4. Existen los siguientes manuales técnicos en el departamento de Sistemas:

PROGRAMA	SI	NO	OBSERVACIONES
Manual de Laptops		X	
Manual de Computadoras		X	
Manual de Drivers	X		
Manual de Computación		X	
Manual de Photoshop		X	

PROGRAMA	SI	NO	OBSERVACIONES
Manual de Programación		X	

5. ¿Existen tareas no escritas que se realicen periódicamente? Descríbalas.

1.- SI (X) 2.- NO ( )

- ✓ Revisión y reparación de equipos y artefactos
- ✓ Limpieza de equipos de computación
- ✓ Mantenimiento de equipos

6. ¿Existen procedimientos formales para la operación del Departamento de Sistema?

1.- SI ( ) 2.- NO (X)

Por el momento no disponen de un manual en donde se detallen los procedimientos de trabajo, pero con el tiempo lo van a implantar para que queden materializados.

7. ¿Están actualizados los procedimientos?

1.- SI ( ) 2.- NO (X)

En forma escrita no lo están, pero cada técnico se actualiza a través de su trabajo diario.

8. Conocimientos:

CONTENIDO	CAPACITACIÓN		SABE	
	SI	NO	SI	NO
Conectar sistemas TI a Internet antes de protegerlos	X		X	
Conectar a Internet sistemas de prueba con cuentas y contraseñas por defecto		X		X

CONTENIDO	CAPACITACIÓN		SABE	
	SI	NO	SI	NO
Actualización los sistemas operativos de los equipos corporativos	X		X	
Autentificación de los usuarios que solicitan servicios técnicos por teléfono		X		X
Mantener y probar las copias de seguridad	X		X	
Confirmar que el plan de recuperación ante desastres realmente funciona	X		X	
Implantar o actualizar programas de detección de virus	X		X	
Informar a los usuarios en materia de seguridad	X		X	
Fallos a la hora de reconocer las amenazas internas	X			X

9. Las intervenciones de los técnicos en los sistemas son:

- Muchas
- Buenas
- Correctivas X
- Preventivas

Son de manera correctivas, ya que cuando se presenta algún problema ahí si lo resuelven.

10. ¿Cuentan los técnicos con una bitácora para mantener registros de cualquier evento y acción tomada por ellos?

1.- Si, por máquina ( ) 2.- Si, escrita manualmente (X) 3.- NO ( )

Sí, todos los escritos se los realizan manualmente en un folleto de la empresa, se lo archiva en carpetas y se guarda en cubículos.

11. ¿Existe un lugar para archivar las bitácoras de los sistemas diseñados por el Departamento? ¿Dónde es?

1.- SI (X) 2.- NO ( )

Sí, se los guarda en bodegas cada caja que contiene los archivos de la empresa por períodos de 2 años.

Quito, 15 de Abril de 2011

Ingeniera
Cristina Orellana
Gerente Administrativa Financiera
SUPERMERCADO DE COMPUTADORAS
Ciudad.-

De mi consideración:

Yo Carolina Leroux, en calidad de auditor designada, solicito se me proporcione toda la información que necesitaré para realizar la auditoria de Análisis de Riesgos de Tecnología de Información por el periodo comprendido desde enero hasta diciembre de 2009.

La información requerida es la siguiente:

Verificación de Control Interno:
Manual de Procedimientos
Políticas y normativa de la empresa
Documentos sustentatorios[14]

Atentamente,

Carolina Leroux

Recibido a nombre de la empresa Supermercado de Computadoras

Ing. Cristina Orellana

[14] **Verificación de Control Interno:**

No existen Manuales de Procedimientos, políticas y normativa de la empresa.

ENTREVISTA A TÉCNICO DEL DEPARTAMENTO DE SISTEMAS DE SUPERMERCADO DE COMPUTADORAS

Persona Entrevistada: Supervisor Técnico (Hugo Correa)

1. **¿Cómo utiliza los reportes de trabajos realizados por el Departamento?**

Cuando se hacen los reportes aunque no siempre, se los entrega al Jefe como constancia de lo que se hizo.

2. **¿Qué criterio tiene en cuanto a la eliminación o modificación desautorizadas de reportes?**

Es algo de lo cual no se darían cuenta hasta después de un tiempo, pero personalmente no estoy de acuerdo.

3. **¿Qué piensa de la seguridad en el manejo de la información en el Departamento de Sistema?**

1.- Nula ( )
2.- Riesgosa (X)
3.- Satisfactoria ( )
4.- Excelente ( )
5.- Lo desconoce ( ) ¿Por qué?

4. **Indique cuál(es) control(es) interno(s) existe(n) en la organización:**

1.- Procedimientos para operar en el departamento ( )
2.- Inventario de activos (X)
3.- Claves de acceso a los sistemas (X)
4.- Seguridades de las Bases de Datos ( )
5.- Manuales de Funciones ( )
6.- Control de archivos de seguridades ( )
7.- Paquetes Comerciales ( )

5. ¿Quién(es) tiene(n) acceso a las Bases de Datos?

Jefe y Técnico 1

6. ¿Existe un registro de anomalías de los Programas?

No.

7. ¿La solicitud de modificaciones a los programas se hacen en forma?

1.- Oral (X)
2.- Escrita ( )

8. ¿Se hace un reporte diario, semanal o mensual de las actividades de cada departamento a la Gerencia?

SI ( ) NO (X)

9. ¿Se tienen respaldos de las Bases?

SI ( ) NO (X)

10. ¿Se cuenta con respaldos actualizados de las bases en lugar distinto al de las computadoras?

SI ( ) NO (X)

11. ¿Existen procedimientos de actualización de las copias que se encuentran fuera de la empresa?

SI ( ) NO (X)

12. ¿Existen procedimientos formales para la operación de los procesos?

SI ( ) NO (X)

13. ¿Están actualizados los procedimientos?

SI ( ) NO (X)

14. Determine la eficiencia con que se ejecutan los trabajos dentro de la empresa tomando en cuenta equipo y técnico, a través de inspección visual.

1.-Mala ( ) 2.-Regular ( ) 3.-Buena (X) 4.-Muy Buena ( ) 5.-Excelente ( )

15. ¿Tiene el conocimiento necesario para actuar en caso de errores en los sistemas?

SI ( ) NO (X)

16. Las intervenciones de los técnicos en los sistemas son:

Son muy numerosas	SI ( )	NO (X)
Se limitan a los mensajes	SI (X)	NO ( )

17. ¿Se tiene un control adecuado sobre el programa que está en operación?

SI ( ) NO (X)

Quito, 8 de Marzo de 2011

Ingeniera
Cristina Orellana
Gerente Administrativa Financiera
SUPERMERCADO DE COMPUTADORAS
Ciudad.-

De mi consideración:

Solicitamos se sirva suministrar la información de documentos que sustenten los procedimientos de protección de información, esta información es de vital importancia para completar el examen de auditoría externa de nuestros Estados Financieros, por lo que agradeceremos su colaboración.

Atentamente,

Carolina Leroux

Manifieste de recibo a nombre de Supermercado de Computadoras

FIRMA
Ing. Cristina Orellana

La información obtenida se resume a continuación:

No existen documentos que sustenten los procedimientos de protección de información de la empresa.

TEST DE PERSONALIDAD

¿Cuál es tu nombre? José Parrales

¿Qué edad tienes? 32 años

¿Cuál es tu grado de estudio? Bachiller

¿Cuál es tu sexo? **(**X**) Hombre** **( ) Mujer**

		Totalmente de acuerdo	**De acuerdo**	**En desacuerdo**	**Totalmente en desacuerdo**
1	Me dejo llevar por los demás			X	
2	Me disgustan las obras de ficción			X	
3	Me desanimo con facilidad				X
4	No me gusta involucrarme en los problemas de los demás				X
5	Lloro durante las películas				X
6	Me encanta soñar despierto			X	
7	No rehúso hablar de mí mismo				X
8	Intento seguir las reglas			X	
9	Hago amigos con facilidad	X			

TEST PSICOLÓGICO

¿Cuál es tu nombre? José Parrales

¿Qué edad tienes? 32 años

¿Cuál es tu grado de estudio? Bachiller

¿Cuál es tu sexo? **(**X**) Hombre** **( ) Mujer**

1. **Su relación con su familia es:**

a) Buena b) Depende c) Mala

2. **¿Ha tenido alguna vez problemas en la escuela cuando era niño?**

a) Mucho b) Poco c) A veces d) Nunca

3. **¿Alguna vez se ha mirado en el espejo y no se ha reconocido en él?**

a) Si b) No se c) No

4. **¿Alguna vez ha sentido las ganas de golpear a alguien sin motivo aparente?**

a) Si b) No se c) No

5. **Sus relaciones con sus profesores eran:**

a) Excelente b) Regular c) Malas

TEST DE APTITUD

¿Cuál es tu nombre? José Parrales

¿Qué edad tienes? 32 años

¿Cuál es tu grado de estudio? Bachiller

¿Cuál es tu sexo? **(X) Hombre** **( ) Mujer**

- **Ordena de mayor a menor los siguientes números:**

4,3 43 0,43 44,3

Respuesta: 44,3 | 43 | 4,3 | 0,43

- **Completa los espacios en blanco para que resulte una igualdad:**

37 x 0,01 = 0,37

204 + 104 = 308

15.000: 300 = 50

15 x 30 = 450

- **Escribe una fracción cuyo numerador sea cuatro unidades mayor que el denominador.**

Respuesta: 4/1

- **¿Cuál es el valor de la cifra 4 en el número 140.895?**

Respuesta: 8

Riesgo 1.- Poca seguridad física de los Equipos (Servidor)

CONDICIÓN	CRITERIO	CAUSA	EFECTO	RECOMENDACIÓN
• **Existe libre acceso al servidor ya que se encuentra cerca de un lugar transitable.**	• El acceso al sistema debe ser restringido físicamente y a través de claves de usuario para evitar alteraciones.	**1.** No se ha establecido un espacio físico para el Servidor de la empresa por mala distribución de áreas. **2.** No se ha establecido seguridades físicas en el área de sistemas. **3.** La Directiva no tomó la decisión de establecer un área específica para el servidor.	**1.** Cualquier persona ajena o no a la empresa puede hacer uso del servidor en forma inadecuada o malintencionada. **2.** Presentarse fallas en el sistema por el mal manejo del mismo. **3.** Pérdida y destrucción de información importante para la entidad.	• El Servidor de datos requiere de un lugar apropiado y único para él, pues al estar mal ubicado puede ocasionar ya sea pérdida de información o destrucción de datos causados por algún agente.

Riesgo 2.- Ausencia de seguridades de la Información

CONDICIÓN	CRITERIO	CAUSA	EFECTO	RECOMENDACIÓN
• **Falta de revisiones preventivas a la red de comunicaciones.**	• Las revisiones preventivas a la red son de importancia alta para un mejor proceso del sistema.	**1.** No existen disposiciones escritas por la empresa en donde establezcan los mantenimientos de los equipos. **2.** Los equipos de comunicaciones se mantienen en habitaciones cerradas. **3.** No existe el personal capacitado para realizar las revisiones a la red	**1.** Los equipos pueden colapsar cuando no existe una adecuada ventilación en el lugar donde estén ubicados. **2.** El sistema puede tener errores a cada momento por no tener revisiones oportunas a través de personal capacitado.	• Se debe realizar el mantenimiento oportuno a los equipos de cómputo en forma preventiva que correctiva por lo menos trimestralmente para que no arrojen fallas en el sistema, caso contrario siempre existirá pérdidas indeseables.

Riesgo 3.- No existen normas y políticas sobre los respaldos de las Bases de Datos (Clientes y Proveedores)

CONDICIÓN	CRITERIO	CAUSA	EFECTO	RECOMENDACIÓN
• **No existen políticas y/o normas para regular el uso de la base de datos.**	• Al no tener un buen uso de la red, la empresa podría tener una pérdida de información importante.	**1.** No se ha realizado creación alguna de las políticas y/o normas para el manejo de la base de datos. **2.** No existen disposiciones escritas por la empresa en donde señalen normas para el uso de la base de datos.	**1.** El personal desconoce del buen manejo y uso que se debe dar a la base de datos. **2.** Los usuarios pueden hacer una mala manipulación o una mal intención que derive a la pérdida del material o de los archivos que manejen. **3.** El personal desconoce el funcionamiento correcto de la base de datos.	• La base de información de la empresa debe ser resguardada por un Jefe directo del área, ya que está a disposición de los trabajadores y ellos a su vez pueden hacer plagio de información a través de CD, memorias USB o cualquier otro dispositivo.

Riesgo 4.- Inexistencia de Planes de Contingencia

CONDICIÓN	CRITERIO	CAUSA	EFECTO	RECOMENDACIÓN
• **No existe un plan de contingencia ante cualquier eventualidad.**	• Toda organización debe tener su plan de contingencia en caso de algún suceso.	**1.** La Gerencia no se ha percatado de crear un plan de contingencia con los procedimientos necesarios para permitir un buen funcionamiento en caso de daño o accidente. **2.** La falta de conocimiento por parte de los Jefes Departamentales no se ha podido establecer un plan de contingencia. **3.** La ausencia de un grupo de control de riesgos no ha permitido tener un plan de contingencia.	**1.** Exponerse a cualquier riesgo que pueda suceder dentro de ella y sin un plan de contingencia no se sabrá cómo actuar ante ese evento.	• Establecer un plan de contingencia que permita asegurar la capacidad de supervivencia de la organización ante eventos que ponga en peligro su existencia. • Los Planes de Contingencia se deben hacer de forma clara para futuros acontecimientos.

4.3. Medidas Preventivas

PROGRAMA DE AUDITORÍA PARA MEDIDAS PREVENTIVAS

CLIENTE **:** SUPERMERCADO DE COMPUTADORAS
FECHA AUDITADO **:** 01 de Enero al 31 de Diciembre de 2009
FECHA DE ELABORACIÓN **:** 07 de Mayo de 2010

1. ALCANCE

Todas las áreas administrativas y operativas de la entidad, que realicen cualquier actividad en los locales o matriz.

2. OBJETIVO GENERAL:

El objetivo general del presente documento, es establecer las medidas preventivas que deberán cumplir los trabajadores de la empresa cuando realicen sus actividades con el fin de garantizar la seguridad en las instalaciones.

3. OBJETIVOS ESPECÍFICOS:

3.1 Definir un mejor control administrativo en un ambiente de Procesamiento de Datos.
3.2 Asegurar una mayor integridad, confidencialidad y confiabilidad de la información mediante la recomendación de seguridades y controles.
3.3 Determinar el nivel de confianza de los resultados de Estados Financieros en el uso de Tecnología de información.
3.4 Identificar las debilidades del Proceso en los Sistemas de Información

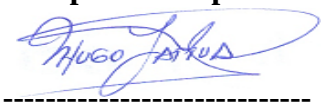
FECHA	Nº	PROCEDIMIENTOS	REF.	RESPONSABLE	OBS.
	1	Realice la evaluación del control interno de la empresa, utilizando para el efecto el cuestionario incluido en este programa y realice pruebas de cumplimiento de los procedimientos descritos.	B – 2	Carolina Leroux	
	2	Realizar inspecciones de seguridad a través de listas de chequeo para identificar los riesgos en el Proceso de Sistemas de Información.	B – 3	Carolina Leroux	
	3	Identificar las debilidades del Proceso de Sistemas de Información.	B – 3	Carolina Leroux	
	4	Realice observaciones de seguridad a través de listas de chequeo para verificar que las tareas se están desarrollando según los procedimientos vigentes y verificar la conducta y actitud de los trabajadores hacia la seguridad.	B – 4	Carolina Leroux	
	5	Identificar las medidas de control con que cuenta la empresa para prevenir y controlar los daños de la información en caso de accidente.	B – 4	Carolina Leroux	
	6	Prepare una hoja en la que se muestre un detalle de los hallazgos encontrados: la hoja deberá contener las siguientes columnas: • Condición	B – 5	Carolina Leroux	

FECHA	Nº	PROCEDIMIENTOS	REF.	RESPONSABLE	OBS.
		• Causa • Criterio • Efecto • Recomendación			

Elaborado por:

Fecha: 17/01/2011

Supervisado por:



Fecha: 17/01/2011

CUESTIONARIO DE CONTROL INTERNO

1. **¿Qué piensa de la seguridad en el manejo de la información en el Departamento de Sistemas?**

1.- Nula ( ) 2.- Riesgosa (X) 3.- Satisfactoria ( ) 4.- Excelente ( )

2. **¿Quién(es) tiene(n) acceso a las Bases de Datos?**

Los técnicos del Departamento de Sistemas que son: Ing. Darwin Ochoa, Ing. Consuelo Moreno, Ing. Sara Ojeda

3. **¿Existe un registro de anomalías de los Programas?**

No existe un registro de anomalías, únicamente se archiva en una carpeta los informes explicativos de los problemas que surjan.

4. **¿La solicitud de modificaciones a los programas se hacen en forma?**

1.- Oral (X) 2.- Escrita ( )

5. **¿Se hace un reporte diario, semanal o mensual de las actividades del Departamento a la Gerencia?**

1.- SI () 2.- NO (X)

6. **¿Se tienen respaldos de las Bases?**

1.- SI ( ) 2.- NO (X) Sólo al que está en la empresa

7. **¿Se cuenta con respaldos actualizados de las bases en lugar distinto al de las computadoras?**

1.- SI ( ) 2.- NO (X)

8. ¿Existen procedimientos de actualización de las copias que se encuentran fuera de la empresa?

1.- SI ( ) 2.- NO (X)

9. ¿Se tiene inventario actualizado de los equipos y terminales con su localización?

1.- SI (X) 2.- NO ( )

10. ¿Se tienen seguros sobre todos los equipos?

1.- SI (X) 2.- NO ( )

11. ¿Se han adoptado medidas de seguridad en el departamento de sistemas?

1.- SI ( ) 2.- NO (X)

12. ¿Existen una persona responsable de la seguridad?

1.- SI ( ) 2.- NO (X)

13. ¿Existe vigilancia en el departamento durante las horas laborales?

1.- SI ( ) 2.- NO (X)

LISTA DE CHEQUEO PARA INSPECCIONES DE SEGURIDAD

DISPOSICIONES MÍNIMAS GENERALES DE SEGURIDAD				
Seguridad informática	**SI**	**NO**	**N/A**	**OBSERVACIONES**
Existe seguridad física de los Equipos (Servidor)		X		
Existe de seguridades de la Información		X		
Existen normas y políticas sobre los respaldos de las Bases de Datos (Clientes y Proveedores)		X		
Existencia de Planes de Contingencia		X		
Existencia de Manuales de Funciones		X		
Seguridad estructural	**SI**	**NO**	**N/A**	**OBSERVACIONES**
Los edificios y los locales de los lugares de trabajo poseen la estructura y solidez apropiada.	✓			
Todos los elementos estructurales y de servicio, incluido escaleras y escalas, soportan el peso.	✓			
Todos los elementos estructurales tanto escaleras y escalones, disponen de un sistema de armado, de apoyo que asegure su estabilidad.	✓			
Condiciones de protección contra incendios	**SI**	**NO**	**N/A**	**OBSERVACIONES**
Los lugares de trabajo están equipadas con dispositivos adecuados para combatir los incendios y, si fuere necesario, con detectores contra incendios y sistemas de alarma.	✓			

Condiciones de protección contra incendios	SI	NO	N/A	OBSERVACIONES
Los dispositivos no automáticos de lucha contra los incendios son de fácil acceso y manipulación y están señalizados.	✓			
Sustancias y materiales inflamables	**SI**	**NO**	**N/A**	**OBSERVACIONES**
El local está compartimentado para que un incendio no se propague libremente.	✓			
Se limpian periódicamente los espacios utilizados para la carga y embalaje de productos.	✓			
La limpieza se realiza con productos no inflamables, en ambientes ventilados.	✓			
Detección y alarma	**SI**	**NO**	**N/A**	**OBSERVACIONES**
Un incendio producido en cualquier zona del local se detectaría rápidamente a cualquier hora, y se transmitiría a los equipos de intervención.	✓			
Se dispone de detectores automáticos adecuados a la clase de fuego previsible en el interior del local (si éste es de alto riesgo)	✓			
Extintores de incendio	**SI**	**NO**	**N/A**	**OBSERVACIONES**
Hay en el local extintores portátiles en cada área de trabajo.	✓			
La parte superior del extintor está como máximo a 1,7 m sobre el suelo.	✓			
Se controla el buen funcionamiento de los extintores (presión, revisión anual).	✓			

Extintores de incendio	SI	NO	N/A	OBSERVACIONES
Hay personas formadas y adiestradas en el manejo de los medios de lucha contra incendios.	✓			
Se dispone de planos del edificio o instalaciones.	✓			
Material de primeros auxilios	**SI**	**NO**	**N/A**	**OBSERVACIONES**
Los lugares de trabajo disponen de material para primeros auxilios en caso de accidente, adecuado en cuanto a su cantidad y características, al número de trabajadores, a los riesgos a que están expuestos y a las facilidades de acceso al centro de asistencia médica más próximo.	✓			Existe un solo botiquín en toda la empresa.
El material de primeros auxilios se adapta a las atribuciones profesionales del personal habilitado para su prestación.	✓			

Simbología a utilizar:

✓ Se cumple
X No se cumple
NA No requiere aplicación
NE Cuando la compañía no ha definido ningún procedimiento

Revisado por: _____ **Fecha de revisión:** 21/01/2011

LISTA DE CHEQUEO PARA OBSERVACIONES DE SEGURIDAD

DISPOSICIONES MÍNIMAS DE SEGURIDAD PARA LA UTILIZACIÓN POR LOS TRABAJADORES DE LOS EQUIPOS DE TRABAJO				
Herramientas manuales de trabajo	**SI**	**NO**	**N/A**	**OBSERVACIONES**
Las herramientas que se usan están concebidas y son específicas para el trabajo a realizar.	✓			
Son fáciles de manejar y son adecuadas al operario.	✓			
Son de buena calidad.	✓			
Se conservan los manuales de manejo de herramientas a disposición de los operarios.		X		
Los operarios están adiestrados en el manejo de las herramientas.	✓			
Se encuentran en buen estado de limpieza y conservación.	✓			
Son periódicamente limpiadas y calibradas para asegurar su uso correcto.	✓			
Hay un número suficiente de herramientas.	✓			
Existen lugares y/o medios idóneos para la ubicación ordenada de las herramientas.	✓			
Se observan hábitos correctos de trabajo.	✓			
Se conoce el posible origen de los accidentes relacionados con herramientas.	✓			

Transporte y conducción	SI	NO	N/A	OBSERVACIONES
La visibilidad desde el puesto de conducción permite al conductor maniobrar con toda seguridad para sí mismo y para las personas expuestas.	✓			
En caso de utilización en lugares oscuros, el vehículo dispone de alumbrado satisfactorio.	✓			
Si el vehículo precisa de cabina, está diseñada y fabricada para proteger de los peligros de vuelco y caída de objetos.	✓			
Existen dispositivos de alarma sonora y/o luminosa.	✓			
Está señalizada la carga máxima de utilización.	✓			
Pantalla	**SI**	**NO**	**N/A**	**OBSERVACIONES**
Los caracteres son claros, definidos y de dimensión suficiente.	✓			
La imagen es estable, sin destellos o centelleos.	✓			
La pantalla es orientable e inclinable.	✓			
No hay reflejos ni reverberaciones	✓			
Teclado	**SI**	**NO**	**N/A**	**OBSERVACIONES**
Es inclinable e independiente de la pantalla.	✓			
Hay espacio antes del teclado para poder apoyar las manos y los brazos.	✓			
La superficie del teclado es mate para evitar reflejos.	✓			

Teclado	SI	NO	N/A	OBSERVACIONES
Las teclas son legibles.	✓			
Mesa	**SI**	**NO**	**N/A**	**OBSERVACIONES**
Es poco reflectante, suficientemente grande para una colocación flexible de los elementos.	✓			
El soporte de los documentos es estable y regulable.	✓			
Asiento	**SI**	**NO**	**N/A**	**OBSERVACIONES**
Es estable y permite libertad de movimientos en una postura confortable.	✓			
La altura es regulable.	✓			
El respaldo es reclinable.	✓			

Simbología a utilizar:

✓ Se cumple
X No se cumple
NA No requiere aplicación
NE Cuando la compañía no ha definido ningún procedimiento

Revisado por: _____ **Fecha de revisión:** 21/01/2011

Riesgo 1.- Inexistencia de Manuales de Funciones

CONDICIÓN	CRITERIO	CAUSA	EFECTO	RECOMENDACIÓN
• **No se conservan los manuales de manejo de herramientas a disposición de los operarios.**	• Para un mejor manejo y buen uso de los instrumentos y herramientas de trabajo se debe conservar y consultar los manuales de manejo y funciones.	**1.** El personal trabaja bajo su conocimiento y experiencia y no por manuales de funciones para el buen uso de los procedimientos laborales. **2.** La Gerencia no ha tomado la decisión de establecer manuales de funciones para el buen uso de los procedimientos laborales. **3.** El personal trabaja por mucho tiempo en la empresa y por su experiencia opinan que no requieren de manuales.	**1.** Por no seguir instructivos y procedimientos de funciones se puede realizar un mal trabajo y ocasionar fallas operarias. **2.** Al no poseer manuales de funciones la Gerencia salta los procedimientos correctos que deberían hacerse bajo una responsabilidad laboral. **3.** Los trabajadores no trabajan según un procedimiento sino según la rutina laboral.	• Un manual de funciones permite establecer normas, procedimientos y responsabilidades que deben ser llevadas con mucha rectitud por todos los empleados.

Riesgo 2.- Falta de un sistema contra incendios y capacitación al personal para su uso

CONDICIÓN	CRITERIO	CAUSA	EFECTO	RECOMENDACIÓN
• **No existe un sistema contra incendios en caso de algún accidente y el personal no ha recibido una capacitación dirigido a la seguridad y al uso de equipos contra incendio.**	• Es necesario contar con un sistema contra incendios para salvaguardar toda la documentación e información de la empresa en caso de alguna eventualidad.	**1.** La Gerencia no ha establecido la normativa de sistemas contra incendios y capacitación al personal para el uso de los mismos. **2.** Falta de prevención por parte de la Administración para prevenir y evitar los incendios. **3.** Falta de presupuesto para la ejecución de un plan de contingencia, ya que este debe ser flexible y suficiente para el cumplimiento de las metas.	**1.** Toda la documentación física, la misma que por tratarse de papeles y folios constituyen un material altamente inflamable, lo que puede incentivar a un incendio. **2.** Por la falta de capacitación del personal exista una mala manipulación de insumos o almacenamiento de papeles o instalaciones eléctricas mal terminadas lo que provocaría un incendio. **3.** En un posible incendio, el personal no pueda actuar ante situaciones de alto riesgo y como resultado de la pérdida de capital humano e información invaluable.	• Todas las empresas, cualquiera que sea su tamaño o actividad, deben contar con un sistema contra incendios, no solo porque proteger la salud de los trabajadores que es un deber moral, sino también, porque constituye una obligación de la empresa.

Riesgo 3.- Inexistencia de UPS[15]

CONDICIÓN	CRITERIO	CAUSA	EFECTO	RECOMENDACIÓN
• **No existe un UPS que permita guardar la información en caso de pérdida de energía eléctrica.**	• La empresa debe contar con un con un UPS para poder respaldar la información en caso de que exista un corte de luz o un problema con el servidor.	**1.** La Directiva no ha tomado las debidas precauciones al adquirir los activos adecuados para respaldar la información. **2.** No ha existido la debida asesoría por parte del departamento de sistemas para resguardar la información. **3.** Falta de presupuesto para la compra de activos adecuados para la institución.	**1.** La pérdida de toda la información importante para la empresa ante un corto circuito de energía eléctrica. **2.** La posibilidad del daño del equipo de cómputo y su servidor. **3.** El riesgo de no tener el tiempo suficiente para guardar la información y el trabajo antes de una falla eléctrica.	• Se sugiere tener un UPS conectado al servidor de la empresa. Con esto usted logra salvar la funcionalidad de un PC en caso de pérdida de energía eléctrica.

[15] Un UPS es una fuente de suministro eléctrico que posee una batería con el fin de seguir dando energía a un dispositivo en el caso de interrupción eléctrica. Los UPS son llamados en español SAI (Sistema de alimentación ininterrumpida). UPS significa en inglés Uninterruptible Power Supply.

Riesgo 4.- Plagio de información por parte de los Empleados

CONDICIÓN	CRITERIO	CAUSA	EFECTO	RECOMENDACIÓN
• **La base de información se encuentra a disposición de los Empleados en dispositivos de almacenamiento.**	• La empresa debe contar con un código de seguridad manejado por la Gerencia General.	**1.** La Gerencia General no ha puesto hincapié en dictar una normativa para que el robo de información no esté al alcance del empleado. **2.** La Directiva no ha tomado las debidas precauciones para evitar este abuso. **3.** Falta de presupuesto para poseer un área específica para el sistema informático central.	**1.** La pérdida de información valiosa que únicamente sirve a la empresa. **2.** La pérdida de datos, de propaganda, de modelos de mercadería, exclusivos de la empresa. **3.** El hurto de información puede llegar a manos de la competencia y así provocar un déficit en ventas.	• Se recomienda que la Gerencia General dicte las necesarias normativas para que la información esté en manos de personal capacitado y de confianza y de ésta manera se evitará que todo el sistema informático sea plagiado por personas inescrupulosas.

4.4. Informe Final

El programa de auditoría para esta fase se presenta a continuación:

PROGRAMA DE AUDITORÍA PARA LA ELABORACIÓN DEL INFORME FINAL SOBRE LOS RESULTADOS DEL ANÁLISIS DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN DE LA EMPRESA SUPERMERCADO DE COMPUTADORAS COMOPUBUSSINES CÍA. LTDA.

FECHA AUDITADO **:** 01 de Enero al 31 de Diciembre de 2009
FECHA DE ELABORACIÓN **:** 17 de Mayo de 2010

1. ALCANCE

Todas las áreas administrativas y operativas de la entidad, que realicen cualquier actividad en los locales o matriz.

2. OBJETIVO GENERAL:

El objetivo general del presente documento, es rendir una opinión acerca de la razonabilidad en la presentación de los Estados Financieros y asegurar la confiabilidad sobre los mismos.

3. OBJETIVOS ESPECÍFICOS:

5.1 Realizar los comentarios respecto a los resultados obtenidos.
5.2 Dar recomendaciones a la gerencia sobre los resultados.
5.3 Presentar los cambios que podrían realizarse para mejorar los procesos de los sistemas de información.
5.4 Explicar los cambios que podrían realizarse para mejorar los procesos de los sistemas de información.
5.5 Identificar las debilidades del Proceso en los Sistemas de Información

FECHA	Nº	PROCEDIMIENTOS	REF.	RESPONSABLE	OBS.
	1	Unifique todos los hallazgos obtenidos en los etapas anteriores	C – 2	Carolina Leroux	
	2	Unifique todos los hallazgos que hable sobre el mismo tema.	C – 3	Carolina Leroux	
	3	Elimine todos los hallazgos que no tengan que ver con errores importantes.	C – 4	Carolina Leroux	
	4	Prepare el borrador del informe de la auditoría.	C – 5	Carolina Leroux	
	5	Organice una reunión para discutir el borrador del informe con el personal directivo, prepare una minuta.	C – 6	Carolina Leroux	
	6	Prepare el informe definitivo y entregue al personal clave.	C – 7	Carolina Leroux	

Elaborado por:

Fecha: 25/03/2011

Supervisado por:

Fecha: 25/03/2011

Riesgo 1.- Poca seguridad física de los Equipos (Servidor)

CONDICIÓN	CRITERIO	CAUSA	EFECTO	RECOMENDACIÓN
• **Existe libre acceso al servidor ya que se encuentra cerca de un lugar transitable.**	• El acceso al sistema debe ser restringido físicamente y a través de claves de usuario para evitar alteraciones.	**1.** No se ha establecido un espacio físico para el Servidor de la empresa por mala distribución de áreas. **2.** No se ha establecido seguridades físicas en el área de sistemas. **3.** La Directiva no tomó la decisión de establecer un área específica para el servidor.	**1.** Cualquier persona ajena o no a la empresa puede hacer uso del servidor en forma inadecuada o malintencionada. **2.** Presentarse fallas en el sistema por el mal manejo del mismo. **3.** Pérdida y destrucción de información importante para la entidad.	• El Servidor de datos requiere de un lugar apropiado y único para él, pues al estar mal ubicado puede ocasionar ya sea pérdida de información o destrucción de datos causados por algún agente.

Riesgo 2.- Ausencia de seguridades de la Información

CONDICIÓN	CRITERIO	CAUSA	EFECTO	RECOMENDACIÓN
• **Falta de revisiones preventivas a la red de comunicaciones.**	• Las revisiones preventivas a la red son de importancia alta para un mejor proceso del sistema.	**1.** No existen disposiciones escritas por la empresa en donde establezcan los mantenimientos de los equipos. **2.** Los equipos de comunicaciones se mantienen en habitaciones cerradas **3.** No existe el personal capacitado para realizar las revisiones a la red	**1.** Los equipos pueden colapsar cuando no existe una adecuada ventilación en el lugar donde estén ubicados. **2.** El sistema puede tener errores a cada momento por no tener revisiones oportunas a través de personal capacitado.	• Se debe realizar el mantenimiento oportuno a los equipos de cómputo en forma preventiva que correctiva por lo menos trimestralmente para que no arrojen fallas en el sistema, caso contrario siempre existirá pérdidas indeseables.

Riesgo 3.- No existen normas y políticas sobre los respaldos de las Bases de Datos (Clientes y Proveedores)

CONDICIÓN	CRITERIO	CAUSA	EFECTO	RECOMENDACIÓN
• **No existen políticas y/o normas para regular el uso de la red.**	• Al no tener un buen uso de la red, la empresa podría tener una pérdida de información importante.	**1.** No se ha realizado creación alguna de las políticas y/o normas para el manejo de la base de datos. **2.** No existen disposiciones escritas por la empresa en donde señalen normas para el uso de la base de datos.	**1.** El personal desconoce del buen manejo y uso que se debe dar a la base de datos. **2.** El personal desconoce del buen manejo y uso que se debe dar a la base de datos. **3.** Los usuarios pueden hacer una mala manipulación o una mal intención que derive a la pérdida del material o de los archivos que manejen. **4.** El personal desconoce el funcionamiento correcto de la base de datos.	• La base de información de la empresa debe ser resguardada por un Jefe directo del área, ya que está a disposición de los trabajadores y ellos a su vez pueden hacer plagio de información a través de CD, memorias USB o cualquier otro dispositivo.

Riesgo 4.- Inexistencia de Planes de Contingencia

CONDICIÓN	CRITERIO	CAUSA	EFECTO	RECOMENDACIÓN
• **No existe un plan de contingencia ante cualquier eventualidad.**	• Toda organización debe tener su plan de contingencia en caso de algún suceso.	**1.** La Gerencia no se ha percatado de crear un plan de contingencia con los procedimientos necesarios para permitir un buen funcionamiento en caso de daño o accidente. **2.** La falta de conocimiento por parte de los Jefes Departamentales no se ha podido establecer un plan de contingencia **3.** La ausencia de un grupo de control de riesgos no ha permitido tener un plan de contingencia	**1.** Exponerse a cualquier riesgo que pueda suceder dentro de ella y sin un plan de contingencia no se sabrá cómo actuar ante ese evento.	• Establecer un plan de contingencia que permita asegurar la capacidad de supervivencia de la organización ante eventos que ponga en peligro su existencia. • Los Planes de Contingencia se deben hacer de forma clara para futuros acontecimientos.

Riesgo 5.- Inexistencia de Manuales de Funciones

CONDICIÓN	CRITERIO	CAUSA	EFECTO	RECOMENDACIÓN
• **No se conservan los manuales de manejo de herramientas a disposición de los operarios.**	• Para un mejor manejo y buen uso de los instrumentos y herramientas de trabajo se debe conservar y consultar los manuales de manejo y funciones.	**1.** El personal trabaja bajo su conocimiento y experiencia y no por manuales de funciones para el buen uso de los procedimientos laborales. **2.** La Gerencia no ha tomado la decisión de establecer manuales de funciones para el buen uso de los procedimientos laborales. **3.** El personal trabaja por mucho tiempo en la empresa y por su experiencia opinan que no requieren de manuales	**1.** Por no seguir instructivos y procedimientos de funciones se puede realizar un mal trabajo y ocasionar fallas operarias. **2.** Al no poseer manuales de funciones la Gerencia salta los procedimientos correctos que deberían hacerse bajo una responsabilidad laboral **3.** Los trabajadores no trabajan según un procedimiento sino según la rutina laboral.	• Un manual de funciones permite establecer normas, procedimientos y responsabilidades que deben ser llevadas con mucha rectitud por todos los empleados

Riesgo 6.- Falta de un sistema contra incendios y capacitación al personal para su uso

CONDICIÓN	CRITERIO	CAUSA	EFECTO	RECOMENDACIÓN
• **No existe un sistema contra incendios en caso de algún accidente y el personal no ha recibido una capacitación dirigido a la seguridad y al uso de equipos contra incendio.**	• Es necesario contar con un sistema contra incendios para salvaguardar toda la documentación e información de la empresa en caso de alguna eventualidad.	**1.** La Gerencia no ha establecido la normativa de sistemas contra incendios y capacitación al personal para el uso de los mismos. **2.** Falta de prevención por parte de la Administración para prevenir y evitar los incendios. **3.** Falta de presupuesto para la ejecución de un plan de contingencia, ya que este debe ser flexible y suficiente para el cumplimiento de las metas.	**1.** Toda la documentación física, la misma que por tratarse de papeles y folios constituyen un material altamente inflamable, lo que puede incentivar a un incendio. **2.** Por la falta de capacitación del personal exista una mala manipulación de insumos o almacenamiento de papeles o instalaciones eléctricas mal terminadas lo que provocaría un incendio. **3.** En un posible incendio, el personal no pueda actuar ante situaciones de alto riesgo y como resultado de la pérdida de capital humano e información invaluable.	• Todas las empresas, cualquiera que sea su tamaño o actividad, deben contar con un sistema contra incendios, no solo porque proteger la salud de los trabajadores que es un deber moral, sino también, porque constituye una obligación de la empresa.

Riesgo 7.- Inexistencia de UPS[16]

CONDICIÓN	CRITERIO	CAUSA	EFECTO	RECOMENDACIÓN
• **No existe un UPS que permita guardar la información en caso de pérdida de energía eléctrica.**	• La empresa debe contar con un con un UPS para poder respaldar la información en caso de que exista un corte de luz o un problema con el servidor.	**1.** La Directiva no ha tomado las debidas precauciones al adquirir los activos adecuados para respaldar la información. **2.** No ha existido la debida asesoría por parte del departamento de sistemas para resguardar la información. **3.** Falta de presupuesto para la compra de activos adecuados para la institución.	**1.** La pérdida de toda la información importante para la empresa ante un corto circuito de energía eléctrica. **2.** La posibilidad del daño del equipo de cómputo y su servidor. **3.** El riesgo de no tener el tiempo suficiente para guardar la información y el trabajo antes de una falla eléctrica.	• Se sugiere tener un UPS conectado al servidor de la empresa. Con esto usted logra salvar la funcionalidad de un PC en caso de pérdida de energía eléctrica.

[16] Un UPS es una fuente de suministro eléctrico que posee una batería con el fin de seguir dando energía a un dispositivo en el caso de interrupción eléctrica. Los UPS son llamados en español SAI (Sistema de alimentación ininterrumpida). UPS significa en inglés Uninterruptible Power Supply.

Riesgo 8.- Plagio de información por parte de los Empleados

CONDICIÓN	CRITERIO	CAUSA	EFECTO	RECOMENDACIÓN
• **La base de información se encuentra a disposición de los Empleados en dispositivos de almacenamiento.**	• La empresa debe contar con un código de seguridad manejado por la Gerencia General.	**1.** La Gerencia General no ha puesto hincapié en dictar una normativa para que el robo de información no esté al alcance del empleado. **2.** La Directiva no ha tomado las debidas precauciones para evitar este abuso. **3.** Falta de presupuesto para poseer un área específica para el sistema informático central.	**1.** La pérdida de información valiosa que únicamente sirve a la empresa. **2.** La pérdida de datos, de propaganda, de modelos de mercadería, exclusivos de la empresa. **3.** El hurto de información puede llegar a manos de la competencia y así provocar un déficit en ventas.	• Se recomienda que la Gerencia General dicte las necesarias normativas para que la información esté en manos de personal capacitado y de confianza y de ésta manera se evitará que todo el sistema informático sea plagiado por personas inescrupulosas.

Riesgo 2 y 3.- Ausencia de seguridades de la información e inexistencia de normas y políticas sobre los respaldos de bases de datos

CONDICIÓN	CRITERIO	CAUSA	EFECTO	RECOMENDACIÓN
• **No se realiza revisiones preventivas a la red de comunicaciones.**	• Las revisiones preventivas a la red son de importancia alta para un mejor proceso del sistema.	**1.** No existen disposiciones escritas por la empresa en donde establezcan los mantenimientos de los equipos. **2.** Los equipos de comunicaciones se mantienen en habitaciones cerradas **3.** No existe el personal capacitado para realizar las revisiones a la red	**1.** A los equipos deben darles mantenimiento oportuno para que no arrojen fallas en el sistema, caso contrario siempre existirá pérdidas indeseables. **2.** Los equipos pueden colapsar cuando no existe una adecuada ventilación en el lugar donde estén ubicados. **3.** El sistema puede tener errores a cada momento por no tener revisiones oportunas a través de personal capacitado	• Se debe realizar el mantenimiento de equipos de cómputo en proporción preventiva que correctiva por lo menos trimestralmente.

CONDICIÓN	CRITERIO	CAUSA	EFECTO	RECOMENDACIÓN
• **No existen políticas y/o normas para regular el uso de la red.**	• Al no tener un buen uso de la red, la empresa podría tener una pérdida de información importante.	**1.** No se ha realizado creación alguna de las políticas y/o normas para el manejo de la base de datos. **2.** No existen disposiciones escritas por la empresa en donde señalen normas para el uso de la red. **3.** El personal no está capacitado para el buen manejo de la red	**1.** La base de información debe ser resguardada por un Jefe directo del área ya que está a disposición de los trabajadores y ellos a su vez pueden hacer plagio de información a través de CD, memorias USB o cualquier otro dispositivo. **2.** La base de datos debe estar guardada a través de claves de seguridad por una sola persona designada por la Gerencia **3.** El personal debe hacer buen uso de sus capacidades para evitar daños a la red	• La empresa debe tener políticas establecidas para manejar y almacenar en forma adecuada la base de información del servidor.

Quito, 16 de Mayo de 2011

Ingeniera
Cristina Orellana
Gerente Administrativa Financiera
SUPERMERCADO DE COMPUTADORAS
Ciudad.-

Analizado cada uno de los hallazgos realizados en el examen de sistemas de información de la empresa, se determinó que cada uno de ellos es importante por lo que se toma la decisión de no eliminar ninguno.

Atentamente,

Carolina Leroux

Quito, 03 de Junio de 2011

Señores.
SUPERMERCADO DE COMPUTADORAS
Presente.

De nuestra consideración:

Hemos realizado nuestro proceso de auditoría con el fin de expresar nuestro informe sobre los niveles de seguridad de los procesos en el sistema de información.

Hemos observado un aspecto de los procesos de sistemas de información y de su operación que consideramos es una condición reportable bajo las Normas de Auditoría Informática Generalmente Aceptadas. Las condiciones reportables comprenden aspectos que llaman nuestra atención, relacionados con deficiencias significativas en el diseño u operación de los procesos de sistemas de información que, a nuestro juicio, podrían afectar adversamente la capacidad de la organización de registrar, procesar, resumir y reportar información financiera consistente con las afirmaciones de la gerencia en los estados financieros.

Es importante mencionar que no es fácil medir con exactitud los beneficios de los procesos de sistemas de información que estimule el cumplimiento de las directrices de la administración, resulta difícil determinar los procesos que se incurre para establecer muchos procesos de sistemas de información, es necesario utilizar un criterio subjetivo para tomar decisiones sobre cuáles procesos de sistemas de información son deseables para un mejor funcionamiento de la organización.

- ***Acceso al Servidor***

Nuestra auditoría reveló que existe libre acceso al servidor ya que se encuentra cerca de un lugar transitable.

Esto puede ocurrir cuando no se ha establecido un espacio físico para el Servidor de la empresa por mala distribución de áreas, cuando no se ha establecido seguridades físicas en el área de sistemas, ó porque la Directiva no tomó la decisión de establecer un área específica para el servidor.

Los principales peligros que pueden presentarse son que cualquier persona ajena o no a la empresa puede hacer uso del servidor en forma inadecuada o malintencionada; presentarse fallas en el sistema por el mal manejo del mismo, ó pérdida y destrucción de información importante para la entidad.

Recomendamos que el Servidor de datos requiere de un lugar apropiado y único para él, pues al estar mal ubicado puede ocasionar ya sea pérdida de información o destrucción de datos causados por algún agente; además no deje el sistema, las unidades de cinta, las terminales o las estaciones de trabajo sin vigilancia durante largos períodos de tiempo; conviene establecer algunas restricciones de acceso en los lugares donde se encuentren estos dispositivos.

- ***Seguridad en la Información***

Nuestra auditoría reveló la falta de revisiones preventivas a la red de comunicaciones. Las revisiones preventivas a la red son de importancia alta para un mejor proceso del sistema.

Esto puede ocurrir cuando no existen disposiciones escritas por la empresa en donde establezcan los mantenimientos de los equipos; ó ya sea que a los equipos de comunicaciones se les mantienen en habitaciones cerradas, ó no existe el personal capacitado para realizar las revisiones a la red.

Los principales peligros que presenta la empresa son que los equipos pueden colapsar cuando no existe una adecuada ventilación en el lugar donde estén ubicados; el sistema puede tener errores a cada momento por no tener revisiones oportunas a través de personal capacitado.

Recomendamos que se deba dar mantenimiento oportuno a los equipos de cómputo en forma preventiva que correctiva por lo menos trimestralmente para que no arrojen fallas en el sistema, caso contrario siempre existirá pérdidas indeseables.

- ***Respaldo de la Base de Datos***

Nuestra auditoría reveló que no existen políticas y/o normas para regular el uso de la base de datos. Al no tener un buen uso de la base de datos, la empresa podría tener una pérdida de información importante.

Esto puede ocurrir cuándo no se ha realizado creación alguna de las políticas y/o normas para el manejo de la base de datos. No existen disposiciones escritas por la empresa en donde señalen normas para el buen uso de la base de datos.

Los principales peligros que presenta la empresa son que el personal desconoce del buen manejo y uso que se debe dar a la base de datos; los usuarios pueden hacer una mala manipulación o una mal intención que derive a la pérdida del material o de los archivos que manejen; y por último no saben cómo es el funcionamiento correcto de la base de datos.

Recomendamos que la base de información de la empresa debe ser resguardada por un Jefe directo del área, ya que está a disposición de los trabajadores y ellos a su vez pueden hacer plagio de información a través de CD, memorias USB o cualquier otro dispositivo; se debe establecer políticas para manejar y almacenar en forma adecuada la base de información del servidor. La base de datos debe estar guardada a través de claves de seguridad por una sola persona designada por la Gerencia. El personal debe hacer buen uso de sus capacidades para evitar daños a la base de datos.

- ***Plan de Contingencia***

Nuestra auditoría reveló que no existe un plan de contingencia ante cualquier eventualidad. Toda organización debe tener su plan de contingencia en caso de algún suceso.

Esto puede ocurrir cuándo la Gerencia no se ha percatado de crear un plan de contingencia con los procedimientos necesarios para permitir un buen funcionamiento en caso de daño o accidente. La falta de conocimiento por parte de los Jefes Departamentales no se ha podido establecer un plan de contingencia. La ausencia de un grupo de control de riesgos no ha permitido tener un plan de contingencia

Los principales peligros que podría presentar la empresa es exponerse a cualquier riesgo que pueda suceder dentro de ella y sin un plan de contingencia no se sabrá cómo actuar ante ese evento.

Recomendamos establecer un plan de contingencia que permita asegurar la capacidad de supervivencia de la organización ante eventos que pongan en peligro su existencia. Los Planes de Contingencia se deben hacer de forma clara para futuros acontecimientos, los cuales hace falta estar preparado.

- ***Manual de Funcionamiento***

Nuestra auditoría reveló que no se conservan los manuales de manejo de herramientas a disposición de los operarios.

Para un mejor manejo y buen uso de los instrumentos y herramientas de trabajo se debe conservar y consultar los manuales de manejo y funciones.

Esto puede ocurrir cuándo el personal trabaja bajo su conocimiento y experiencia y no por manuales de trabajo. La Gerencia no ha tomado la decisión de establecer manuales de funciones para el buen uso de los procedimientos laborales. El personal

trabaja por mucho tiempo en la empresa y por su experiencia opinan que no requieren de manuales.

Los principales peligros que presenta la empresa por no seguir instructivos y procedimientos de funciones se puede realizar un mal trabajo y ocasionar fallas operarias. Al no poseer manuales de funciones la Gerencia salta los procedimientos correctos que deberían hacerse bajo una responsabilidad laboral. Los trabajadores no trabajan según un procedimiento sino según la rutina laboral.

Recomendamos un manual de funciones permite establecer normas, procedimientos y responsabilidades que deben ser llevadas con mucha rectitud por todos los empleados.

- ***Sistema contra incendios***

Nuestra auditoría reveló que no existe un sistema contra incendios en caso de algún accidente y el personal no ha recibido una capacitación dirigido a la seguridad y al uso de equipos contra incendio. Es necesario contar con un sistema contra incendios para salvaguardar toda la documentación e información de la empresa en caso de alguna eventualidad.

Esto puede ocurrir cuando la Gerencia no ha establecido la normativa de sistemas contra incendios y capacitación al personal para el uso de los mismos; por falta de prevención por parte de la Administración para advertir y evitar los incendios y además por falta de presupuesto para la ejecución de un plan de contingencia, ya que éste debe ser flexible y suficiente para el cumplimiento de las metas.

Los principales peligros que pueden presentarse es que toda la documentación física, la misma que por tratarse de papeles y folios constituye un material altamente inflamable, lo que puede incentivar a un incendio; ó por la falta de capacitación del personal exista una mala manipulación de insumos o almacenamiento de papeles o instalaciones eléctricas mal terminadas lo que provocaría un incendio y en un posible incendio, el personal no pueda actuar ante situaciones de alto riesgo y como resultado de la pérdida de capital humano e información invaluable.

Recomendamos que todas las empresas, cualquiera que sea su tamaño o actividad, deben contar con un sistema contra incendios, no solo porque proteger la salud de los trabajadores que es un deber moral, sino también, porque constituye una obligación de la empresa.

- ***Inexistencia de UPS***

Nuestra auditoría reveló que no existe un UPS que permita guardar la información en caso de pérdida de energía eléctrica. La empresa debe contar con un UPS para poder respaldar la información en caso de que exista un corte de luz o un problema con el servidor.

Esto puede ocurrir cuando la Directiva no ha tomado las debidas precauciones al adquirir los activos adecuados para respaldar la información.; ó cuando no ha existido la debida asesoría por parte del departamento de sistemas para resguardar la información y también por falta de presupuesto para la compra de activos adecuados para la institución.

Los principales peligros que pueden presentarse son la pérdida de toda la información importante para la empresa ante un corto circuito de energía eléctrica; la posibilidad del daño del equipo de cómputo y su servidor y el riesgo de no tener el tiempo suficiente para guardar la información y el trabajo antes de una falla eléctrica.

Recomendamos tener un UPS conectado al servidor de la empresa. Con esto la empresa logra salvar la funcionalidad de un PC en caso de pérdida de energía eléctrica.

- ***Plagio de información***

Nuestra auditoría reveló que la base de información se encuentra a disposición de los Empleados en dispositivos de almacenamiento.

Esto puede ocurrir cuando la Gerencia General no ha puesto hincapié en dictar una normativa para que el robo de información no esté al alcance del empleado; ó la Directiva no ha tomado las debidas precauciones para evitar este abuso y también por falta de presupuesto para poseer un área específica para el sistema informático central.

Los principales peligros que pueden presentarse es la pérdida de información valiosa que únicamente sirve a la empresa; la pérdida de datos, de propaganda, de modelos de mercadería, exclusivos de la compañía y el hurto de información que puede llegar a manos de la competencia y así provocar un déficit en ventas.

Recomendamos que la Gerencia General dicte las necesarias normativas para que la información esté en manos de personal capacitado y de confianza y de ésta manera se evitará que todo el sistema informático sea plagiado por personas inescrupulosas.

La empresa debe contar con un código de seguridad manejado por la Gerencia General.

Atentamente,

Carolina Leroux

Minuta de Reunión

Fecha: Quito, 10 de Junio de 2011
Lugar: Empresa Supermercado de Computadoras
Minuta: Nº 1

Participantes:

- Ing. Cristina Orellana — Gerente Administrativa Financiera
- Sra. Carolina Leroux — Auditora

Agenda:

1. Discusión sobre hallazgos encontrados en auditoría realizada, período 1 de Enero a 31 de Diciembre 2009

Puntos Tratados:

1. La Sra. Carolina Leroux realizó la presentación de un informe detallado del proceso de auditoría realizado, abordando aspectos vinculados a su funcionamiento y procesos que maneja la organización. Informó que hasta el momento se han detectado 5 hallazgos sobre los procesos de sistemas de información de la empresa.

Intercambio de Opinión:

- La Ing. Cristina Orellana manifestó la conformidad de los hallazgos encontrados por lo que indicó que considerarán la necesidad de fortalecer y educar en los conocimientos a todo el personal que se involucre en el proceso de sistemas de información contable.

Quito, 03 de Junio de 2011

Señores.
SUPERMERCADO DE COMPUTADORAS
Presente.

De nuestra consideración:

Hemos realizado nuestro proceso de auditoría con el fin de expresar nuestro informe sobre los niveles de seguridad de los procesos en el sistema de información.

Hemos observado un aspecto de los procesos de sistemas de información y de su operación que consideramos es una condición reportable bajo las Normas de Auditoría Informática Generalmente Aceptadas. Las condiciones reportables comprenden aspectos que llaman nuestra atención, relacionados con deficiencias significativas en el diseño u operación de los procesos de sistemas de información que, a nuestro juicio, podrían afectar adversamente la capacidad de la organización de registrar, procesar, resumir y reportar información financiera consistente con las afirmaciones de la gerencia en los estados financieros.

Es importante mencionar que no es fácil medir con exactitud los beneficios de los procesos de sistemas de información que estimule el cumplimiento de las directrices de la administración, resulta difícil determinar los procesos que se incurre para establecer muchos procesos de sistemas de información, es necesario utilizar un criterio subjetivo para tomar decisiones sobre cuáles procesos de sistemas de información son deseables para un mejor funcionamiento de la organización.

- ***Acceso al Servidor***

Nuestra auditoría reveló que existe libre acceso al servidor ya que se encuentra cerca de un lugar transitable.

Esto puede ocurrir cuando no se ha establecido un espacio físico para el Servidor de la empresa por mala distribución de áreas, cuando no se ha establecido seguridades físicas en el área de sistemas, ó porque la Directiva no tomó la decisión de establecer un área específica para el servidor.

Los principales peligros que pueden presentarse son que cualquier persona ajena o no a la empresa puede hacer uso del servidor en forma inadecuada o malintencionada; presentarse fallas en el sistema por el mal manejo del mismo, ó pérdida y destrucción de información importante para la entidad.

Recomendamos que el Servidor de datos requiere de un lugar apropiado y único para él, pues al estar mal ubicado puede ocasionar ya sea pérdida de información o destrucción de datos causados por algún agente; además no deje el sistema, las unidades de cinta, las terminales o las estaciones de trabajo sin vigilancia durante largos períodos de tiempo; conviene establecer algunas restricciones de acceso en los lugares donde se encuentren estos dispositivos.

COMENTARIO ING. CRISTINA ORELLANA:

Se va a tomar en cuenta la recomendación de establecer un lugar único para el servidor de la empresa y así poder evitar posibles pérdidas de información.

- ***Seguridad en la Información***

Nuestra auditoría reveló la falta de revisiones preventivas a la red de comunicaciones. Las revisiones preventivas a la red son de importancia alta para un mejor proceso del sistema.

Esto puede ocurrir cuando no existen disposiciones escritas por la empresa en donde establezcan los mantenimientos de los equipos; ó ya sea que a los equipos de comunicaciones se les mantienen en habitaciones cerradas, ó no existe el personal capacitado para realizar las revisiones a la red.

Los principales peligros que presenta la empresa son que los equipos pueden colapsar cuando no existe una adecuada ventilación en el lugar donde estén ubicados; el sistema puede tener errores a cada momento por no tener revisiones oportunas a través de personal capacitado.

Recomendamos que se deba dar mantenimiento oportuno a los equipos de cómputo en forma preventiva que correctiva por lo menos trimestralmente para que no arrojen fallas en el sistema, caso contrario siempre existirá pérdidas indeseables.

COMENTARIO ING. CRISTINA ORELLANA:

La Directiva establecerá mantenimientos de la red en forma preventiva cada tres meses o cuándo lo amerite.

- ***Respaldo de la Base de Datos***

Nuestra auditoría reveló que no existen políticas y/o normas para regular el uso de la base de datos. Al no tener un buen uso de la base de datos, la empresa podría tener una pérdida de información importante.

Esto puede ocurrir cuándo no se ha realizado creación alguna de las políticas y/o normas para el manejo de la base de datos. No existen disposiciones escritas por la empresa en donde señalen normas para el buen uso de la base de datos.

Los principales peligros que presenta la empresa son que el personal desconoce del buen manejo y uso que se debe dar a la base de datos; los usuarios pueden hacer una mala manipulación o una mal intención que derive a la pérdida del material o de los archivos que manejen; y por último no saben cómo es el funcionamiento correcto de la base de datos.

Recomendamos que la base de información de la empresa debe ser resguardada por un Jefe directo del área, ya que está a disposición de los trabajadores y ellos a su vez pueden hacer plagio de información a través de CD, memorias USB o cualquier otro dispositivo; se debe establecer políticas para manejar y almacenar en forma adecuada la base de información del servidor. La base de datos debe estar guardada a través de claves de seguridad por una sola persona designada por la Gerencia. El personal debe hacer buen uso de sus capacidades para evitar daños a la base de datos.

COMENTARIO ING. CRISTINA ORELLANA:

Cada Jefe de área tendrá un respaldo del trabajo que se lleva a diario para evitar pérdida de información, siempre y cuando no se duplique la misma.

- ***Plan de Contingencia***

Nuestra auditoría reveló que no existe un plan de contingencia ante cualquier eventualidad. Toda organización debe tener su plan de contingencia en caso de algún suceso.

Esto puede ocurrir cuándo la Gerencia no se ha percatado de crear un plan de contingencia con los procedimientos necesarios para permitir un buen funcionamiento en caso de daño o accidente. La falta de conocimiento por parte de los Jefes Departamentales no se ha podido establecer un plan de contingencia. La ausencia de un grupo de control de riesgos no ha permitido tener un plan de contingencia

Los principales peligros que podría presentar la empresa es exponerse a cualquier riesgo que pueda suceder dentro de ella y sin un plan de contingencia no se sabrá cómo actuar ante ese evento.

Recomendamos establecer un plan de contingencia que permita asegurar la capacidad de supervivencia de la organización ante eventos que ponga en peligro su existencia. Los Planes de Contingencia se deben hacer de forma clara para futuros acontecimientos, los cuales hace falta estar preparado.

COMENTARIO ING. CRISTINA ORELLANA:

Los planes de contingencia son buenos siempre y cuándo se los aplique, en éste caso pondremos énfasis tener a mano uno en cada de que existe algún peligro laboral.

- ***Manual de Funcionamiento***

Nuestra auditoría reveló que no se conservan los manuales de manejo de herramientas a disposición de los operarios.

Para un mejor manejo y buen uso de los instrumentos y herramientas de trabajo se debe conservar y consultar los manuales de manejo y funciones.

Esto puede ocurrir cuándo el personal trabaja bajo su conocimiento y experiencia y no por manuales de trabajo. La Gerencia no ha tomado la decisión de establecer manuales de funciones para el buen uso de los procedimientos laborales. El personal trabaja por mucho tiempo en la empresa y por su experiencia opinan que no requieren de manuales.

Los principales peligros que presenta la empresa por no definir y seguir instructivos y procedimientos de funciones, se refiere a que se puede realizar un mal trabajo y ocasionar fallas operarias. Al no poseer manuales de funciones la Gerencia “salta” los procedimientos correctos que deberían hacerse bajo una responsabilidad laboral. Los trabajadores no trabajan según un procedimiento sino según la rutina laboral.

Recomendamos un manual de funciones que permita establecer normas, procedimientos y responsabilidades que deben ser llevadas con mucha rectitud por todos los empleados.

COMENTARIO ING. CRISTINA ORELLANA:

Se empezará con la elaboración de manuales de funciones para llevar un mejor desenvolvimiento en cada uno de los procesos que realizan los empleados.

- ***Sistema contra incendios***

Nuestra auditoría reveló que no existe un sistema contra incendios en caso de algún accidente y el personal no ha recibido una capacitación dirigido a la seguridad y al uso de equipos contra incendio. Es necesario contar con un sistema contra incendios para salvaguardar toda la documentación e información de la empresa en caso de alguna eventualidad.

Esto puede ocurrir cuando la Gerencia no ha establecido la normativa de sistemas contra incendios y capacitación al personal para el uso de los mismos; por falta de prevención por parte de la Administración para advertir y evitar los incendios y además por falta de presupuesto para la ejecución de un plan de contingencia, ya que éste debe ser flexible y suficiente para el cumplimiento de las metas.

Los principales peligros que pueden presentarse es que toda la documentación física, la misma que por tratarse de papeles y folios constituye un material altamente inflamable, lo que puede incentivar a un incendio; ó por la falta de capacitación del personal exista una mala manipulación de insumos o almacenamiento de papeles o instalaciones eléctricas mal terminadas, lo cual provocaría el siniestro. En un posible incendio, el personal no puede actuar ante situaciones de alto riesgo y como resultado existe la posibilidad de la pérdida de capital humano e información invaluable de la compañía.

Recomendamos que todas las empresas, cualquiera que sea su tamaño o actividad, deben contar con un sistema contra incendios, no solo porque proteger la salud de los trabajadores que es un deber moral, sino también, porque constituye una obligación de la empresa.

COMENTARIO ING. CRISTINA ORELLANA:

La Gerencia elaborará un pequeño manual con procedimientos en caso de que ocurra algún accidente de incendio, para poder salvaguardar tanto las vidas de los empleados como también la información y activos que posea la empresa.

- ***Inexistencia de UPS***

Nuestra auditoría reveló que no existe un UPS que permita guardar la información en caso de pérdida de energía eléctrica. La empresa debe contar con un UPS para poder respaldar la información en caso de que exista un corte de luz o un problema con el servidor.

Esto puede ocurrir cuando la Directiva no ha tomado las debidas precauciones al adquirir los activos adecuados para respaldar la información.; ó cuando no ha existido la debida asesoría por parte del departamento de sistemas para resguardar la información y también por falta de presupuesto para la compra de activos adecuados para la institución.

Los principales peligros que pueden presentarse son la pérdida de toda la información importante para la empresa ante un corto circuito de energía eléctrica; la posibilidad del daño del equipo de cómputo y su servidor y el riesgo de no tener el tiempo suficiente para guardar la información y el trabajo antes de una falla eléctrica.

Recomendamos tener un UPS conectado al servidor de la empresa. Con esto la empresa logra salvar la funcionalidad de un PC en caso de pérdida de energía eléctrica.

COMENTARIO ING. CRISTINA ORELLANA:

Se va a implementar un UPS para cada computador de la empresa y así poder evitar pérdidas de información.

- ***Plagio de información***

Nuestra auditoría reveló que la base de información se encuentra a disposición de los Empleados en dispositivos de almacenamiento.

Esto puede ocurrir cuando la Gerencia General no ha puesto hincapié en dictar una normativa para que el robo de información no esté al alcance del empleado; ó la

Directiva no ha tomado las debidas precauciones para evitar este abuso y también por falta de presupuesto para poseer un área específica para el sistema informático central.

Los principales peligros que pueden presentarse es la pérdida de información valiosa que únicamente sirve a la empresa; la pérdida de datos, de propaganda, de modelos de mercadería, exclusivos de la compañía y el hurto de información que puede llegar a manos de la competencia y así provocar un déficit en ventas.

Recomendamos que la Gerencia General dicte las necesarias normativas para que la información esté en manos de personal capacitado y de confianza y de ésta manera se evitará que todo el sistema informático sea plagiado por personas inescrupulosas.

La empresa debe contar con un código de seguridad manejado por la Gerencia General.

COMENTARIO ING. CRISTINA ORELLANA:

Personalmente me haré cargo de un disco duro externo para guardar la información a diario de todo lo que realiza el personal en cada día de trabajo.

Atentamente,

Carolina Leroux

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

1. Este trabajo tiene como una de sus metas primordiales el orientar a las generaciones futuras, sobre los aspectos importantes que se deben considerar en la Administración de Riesgos de Tecnología de Información de las empresas del sector privado comercial. Éste tema es importante por su aproximación científica en el comportamiento de los riesgos, anticipando las posibles pérdidas accidentales con el diseño e implementación de procedimientos que minimicen la ocurrencia de pérdidas o el impacto financiero que se pueda ocurrir.

2. El principal objetivo de la Administración de Riesgos de TI, tiene como primera ley garantizar la supervivencia de la organización, minimizando los costos asociados con los riesgos. Muchos de los defectos en la administración de riesgos radican en la ausencia de objetivos claros.

3. Se debe enfatizar y relevar la importancia y la significación de la Administración de Riesgos de TI, debido a la trascendencia de los controles y seguridades de los procesos de sistemas de información que ameritan ser implementados en toda la organización.

4. La Administración de Riesgos de TI, dentro de la empresa, es una herramienta muy útil para el mejor desarrollo de las actividades de un departamento o de todos los departamentos de la organización.

5. La Administración de Riesgos de Tecnología de Información, nos muestra los principales controles y seguridades que deben implementarse en los departamentos de la Empresa Supermercado de Computadoras Compubussines Cía. Ltda., como es el caso en el área contable y de sistemas. El análisis de riesgos de TI, desarrollado en la empresa, ha contribuido a ampliar aún más los conocimientos sobre los problemas significativos de las áreas anteriormente mencionadas y sobre las múltiples soluciones que se pueden aplicar.

5.2. Recomendaciones

1. La Empresa Supermercado de Computadoras Compubussines Cía. Ltda., debería designar un grupo de personas que se encarguen de implementar un plan de contingencia ante cualquier eventualidad, de ésta manera se salvaguardará la información contable de todo el sistema.

2. La Empresa Supermercado de Computadoras Compubussines Cía. Ltda., debería implementar un manual de funciones donde estén los objetivos y normativas para garantizar la supervivencia de la organización.

3. Con el crecimiento de la Empresa Supermercado de Computadoras Compubussines Cía. Ltda., aparecen nuevos riesgos, por lo que la Gerencia en conjunto con los Departamentos deberían organizar el Análisis de Riesgos cada cierto tiempo sea trimestral o semestral.

4. Todos los departamentos de una empresa deben poseer un sistema de análisis de riesgos de TI, con ello dará soluciones a los posibles riesgos que se puedan presentar en dicha empresa.

5. Es necesario que el grupo humano que conforman los diversos departamentos de la Empresa Supermercado de Computadoras Compubussines Cía. Ltda., posean el conocimiento tanto para la elaboración del análisis como para la revisión y monitoreo del trabajo una vez implementado. Es necesario que todos los profesionales se encuentren actualizados con los conocimientos de la metodología de TI y de esta manera la Empresa Supermercado de Computadoras Compubussines Cía. Ltda., crecerá en el ámbito general.

6. Finalmente, se puede recomendar que la Empresa Supermercado de Computadoras Compubussines Cía. Ltda., debe salvaguardar su información con la ayuda de CD, memorias USB o cualquier otro dispositivo de medio magnético, con el fin de administrar y almacenar en forma adecuada su información.

GLOSARIO

1. **Administración de riesgos:** Una rama de administración que aborda las consecuencias del riesgo. Consta de dos etapas: 1) El diagnóstico o valoración, mediante Identificación, Análisis y determinación del Nivel, y 2) El manejo o la administración propiamente dicha, en que se elabora, ejecuta y hace seguimiento al Plan de manejo que contiene las Técnicas de Administración del Riesgo propuestas por el grupo de trabajo, evaluadas y aceptadas por la alta dirección.

2. **Análisis de Beneficio-Costo:** Una herramienta de Administración de Riesgos usada para tomar decisiones sobre las técnicas propuestas por el grupo para la administración de los riesgos, en la cual se valoran y comparan los costos, financieros y económicos, de implementar la medida, contra los beneficios generados por la misma. Una medida de administración de riesgos será aceptada siempre que el beneficio valorado supere al costo.

3. **Análisis de riesgos:** Determinar el Impacto y la Probabilidad del riesgo. Dependiendo de la información disponible pueden emplearse desde modelos de simulación, hasta técnicas colaborativas.

4. **Área de Responsabilidad:** Se define como un centro de actividad que desarrolla un conjunto de funciones, al frente de la cual se encuentra un responsable facultado para desplegar acciones de control encaminadas a que las tareas asignadas al área se desarrollen de forma eficiente. El área de responsabilidad constituye la base del esquema de dirección de las empresas, por lo cual deben estar bien definidas en cada entidad. Una premisa básica para la determinación de un área de responsabilidad es que su jefe pueda controlar y accionar sobre los gastos que en la misma se originan y consecuentemente responder por su comportamiento.

5. **Backup:** en tecnología de la información o informática es una copia de seguridad - o el proceso de copia de seguridad - con el fin de que estas copias

adicionales puedan utilizarse para restaurar el original después de una eventual pérdida de datos.

6. **Causa:** Son los medios, circunstancias y agentes que generan los riesgos.

7. **Control:** Es toda acción que tiende a minimizar los riesgos, significa analizar el desempeño de las operaciones, evidenciando posibles desviaciones frente al resultado esperado para la adopción de medidas preventivas. Los controles proporcionan un modelo operacional de seguridad razonable en el logro de los objetivos.

8. **Costo:** Se entiende por costo las erogaciones, directas e indirectas en que incurre la entidad en la producción, prestación de un servicio o manejo de un riesgo.

9. **Factores de riesgo:** Manifestaciones o características medibles u observables de un proceso que indican la presencia de Riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

10. **Identificación de riesgos:** Establecer la estructura del riesgo; fuentes o factores, internos o externos, generadores de riesgos; puede hacerse a cualquier nivel: total entidad, por áreas, por procesos, incluso, bajo el viejo paradigma, por funciones; desde el nivel estratégico hasta el más humilde operativo.

11. **Impacto:** consecuencias que puede ocasionar a la organización la materialización del riesgo.

12. **Indicador:** es la valoración de una o más variables que informa sobre una situación y soporta la toma de decisiones, es un criterio de medición y de evaluación cuantitativa o cualitativa.

13. **Interactivo:** dicho de un programa que permite una interacción a modo de diálogo entre ordenador y usuario.

14. **Iteración:** se refiere a la acción de repetir una serie de pasos un cierto número de veces.

15. **Mapas de riesgos:** herramienta metodológica que permite hacer un inventario de los riesgos ordenada y sistemáticamente, definiéndolos, haciendo la descripción de cada uno de estos y las posibles consecuencias.

16. **Nivel de riesgo (determinación del):** Es el resultado de confrontar el impacto y la probabilidad, con los controles existentes.

17. **Normas ISO 9000 y 14000:** Normas que regulan la calidad de los bienes o de los servicios que venden u ofrecen las empresas, así como los aspectos ambientales implicados en la producción de los mismos. Tanto el comercio como la industria tienden a adoptar normas de producción y comercialización uniformes para todos los países, es decir, tienden a la normalización. Ésta no sólo se traduce en leyes que regulan la producción de bienes o servicios sino que su influencia tiende a dar estabilidad a la economía, ahorrar gastos, evitar el desempleo y garantizar el funcionamiento rentable de las empresas. El organismo internacional de normalización es la ISO. La ISO 9000 es un sistema para asegurar la calidad. La ISO 14000, es un sistema de estándares ambientales administrativos.

18. **Plan de contingencia:** Parte del plan de manejo de riesgos que contiene las acciones a ejecutar en caso de la materialización del riesgo, con el fin de dar continuidad a los objetivos de la entidad.

19. **Plan de manejo de riesgos:** Plan de acción propuesto por el grupo de trabajo, cuya evaluación de beneficio costo resulta positiva y es aprobado por la gerencia.

20. **Plan de mejoramiento:** Parte del plan de manejo que contiene las técnicas de administración del riesgo orientadas a prevenir, evitar, reducir, dispersar, transferir o asumir riesgos.

21. **Probabilidad:** Una medida (expresada como porcentaje o razón) para estimar la posibilidad de que ocurra un incidente o evento. Contando con registros, puede estimarse a partir de su Frecuencia histórica mediante modelos estadísticos de mayor o menor complejidad.

22. **Retroalimentación:** Información sistemática sobre los resultados alcanzados en la ejecución de un plan, que sirven para actualizar y mejorar la planeación futura.

23. **Riesgo:** posibilidad de ocurrencia de toda aquella situación que pueda entorpecer el normal desarrollo de las funciones de la entidad y le impidan el logro de sus objetivos.

24. **Riesgo absoluto:** el máximo riesgo sin los efectos mitigantes de la administración del riesgo.

25. **Riesgo residual:** es el riesgo que queda cuando las técnicas de administración del riesgo han sido aplicadas.

26. **Seguimiento:** Recolección regular y sistemática sobre la ejecución del plan, que sirven para actualizar y mejorar la planeación futura.

27. **Sistema:** Conjunto de cosas o partes coordinadas, ordenadamente relacionadas entre sí, que contribuyen a un determinado objetivo.

28. **Técnicas para manejar el riesgo:** Evitar o prevenir, reducir, dispersar, transferir y asumir riesgos.

29. **TI:** Tecnologías de la Información.

30. **Valoración del riesgo:** Primera fase en la administración de riesgos, diagnóstico que consta de la identificación, análisis y determinación del nivel de riesgo.

BIBLIOGRAFÍA

1. AGUIRRE ORMAECHEA, Juan M. Auditoria III, *Control Interno Áreas Específicas de Implantación, Procedimientos y Control.*

2. BECERRA J., Germán. *Procesamiento Administrativo de Datos PAD y Auditoría de Sistemas*. 1ra Ed., Roesga, Cali, 2000

3. ECHENIQUE GARCÍA, José Antonio. *Auditoría en informática*, Primera Edición, McGraw-Hill, México, México

4. ESTUPIÑÁN GAITÁN, Rodrigo. *Control Interno y Fraude con base en los ciclos transaccionales, Análisis de Informe COSO*, 2da. Ed. Bogotá, Colombia. ECOE Ediciones 2006

5. HELLRIEGEL, Jackson Slocum. *Administración: Un Enfoque Basado en Competencias*, Novena Edición

6. J.W Cook/ G.M. Winkle. *Auditoria*, Tercera Edición.

7. MANTILLA, Samuel Alberto. *Control Interno, Informe COSO*, Cuarta Edición.

8. MC CONNELL Steve, 1996. *Desarrollo y Gestión de Proyectos Informáticos: Gestión de Riesgos*, Primera Edición, McGraw-Hill, España.

9. O. Ray Whittington-Kurt Pany. *Auditoria un Enfoque Integral*

10. PIATTINI Mario y Del Peso Emilio, 2004. *Auditoría Informática: Un Enfoque Práctico*, Segunda Edición, Editorial RA-MA, España, Páginas 45-89, 310-317, 394-401, 570-581, 616

11. SALLENAVE Jean Paul, 1996. *Gerencia y Planeación Estratégica: El Método Delphi*, Segunda Edición, Editorial Norma, Colombia.

12. http://www.deloitte.com.mx/archivos/aseso_fin/fcpa.pdf

13. Autor: Edgar Armando Vega Briceño, Investigación de mercados http://www.gestiopolis.com/Canales/mkt/simparalas.htm

14. Autor: Juan de Dios Bel, Uso de la Evaluación de Riesgos en la Planificación de Auditorías de TI, http://www.iaia.org.ar/elauditorinterno/02/articulo3.html