UNIVERSIDAD DE EL SALVADOR

Facultad de Ciencias Económicas

Escuela de Contaduría Pública

"El auditor interno ante la evaluación de la administración de riesgos en tecnología de información en las cadenas de supermercados de El Salvador"

Trabajo de investigación presentado por:

Escalante Rodríguez, Carlos Geovani

Guzmán, Clara Emperatriz

Cerna Cruz, Deysi Doredith

Para optar al grado de

LICENCIADO EN CONTADURÍA PUBLICA

Febrero 2005

San Salvador El Salvador Centro América

AUTORIDADES UNIVERSITARIAS

Rector (a) : Dra. María Isabel Rodríguez

Secretario General : Licda. Alicia Margarita Rivas de Recinos

Facultad de Ciencias Económicas

Decano : Lic. Emilio Recinos Fuentes

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

Coordinador de Seminario

de Graduación : Lic. Alvaro Edgardo Calero Rodas

Asesor : Msc. Sergio Rodríguez Murcia

Tribunal Examinador

Docente Director : Msc. Sergio Rodríguez Murcia

Docente Coordinador : Lic. Alvaro Edgardo Calero Rodas

Febrero 2005

San Salvador El Salvador, Centro América

AGRADECIMIENTOS

A Dios Todopoderoso: Diré yo a Jehová: ¡Que el júbilo que hoy me invade, sea para Ti una plegaria de Alabanza!; porque cada día me regalas una familia, amor, vida, salud, trabajo, inteligencia e infinidad de tus bondades inmerecidas.

A mis Padres: Carlos Antonio Escalante y María Julia Rodríguez, porque este triunfo les pertenece mas a ustedes que a mi; es el fruto de su invaluable sacrificio y dedicación para educar a sus hijos, día tras día.

A mi Esposa: María del Carmen, por su apoyo incondicional, comprensión y compartir conmigo la senda de la vida.

A mis Hermanos y Sobrinos: Maybelline y José; Brandon e Ismael, por su amor fraternal; porque esta alegría también les pertenece.

A mis Amigos y Compañeros: A mis amigos que sin interés alguno me apoyaron, incluso sin saberlo; mi grupo de investigación, por su paciencia; mis compañeros por su respaldo sincero y para todos aquellos que merecen especial agradecimiento, mis disculpas porque al nombrarlos, podría omitir injustamente a alguno.

CARLOS GEOVANI ESCALANTE RODRIGUEZ

A Dios Todopoderoso y la Virgen Santísima: Por su expresión de Amor Divino y Misericordia infinita hacia mí.
Por concederme vida, salud y fortaleza para culminar la meta anhelada.

A mi Madre: María del Carmen Guzmán, por su amor y apoyo incondicional en cada momento de mi existencia, por sus valiosos consejos para guiarme cada día y sobre todo por ser el motivo principal de mi lucha constante en la vida.

A mis Primos y Tía: Que me han brindado su apoyo en los momentos que los he necesitado y por contribuir a iniciar esta etapa profesional de mi vida.

A mis compañeros de Grupo: Deysi y Geovani, que sin su ayuda, colaboración y buena disposición este documento no sería una realidad, gracias por su comprensión en cada momento. Agradezco también la ayuda brindada por Carmencita esposa de nuestro compañero, que su cariño, amistad y atenciones nos acogió cada día de reunión en su hogar

A mis Amigos: A todos aquellos que sinceramente me han brindado su amistad, ayuda, consejos y alegrías y se han mantenido constantes a lo largo de mi carrera.

CLARA EMPERATRIZ GUZMAN

A Dios Todopoderoso: Por la vida, la sabiduría y la fortaleza que en su infinito amor me ha brindado para alcanzar la meta propuesta, la cual sin su misericordia esto no hubiera sido posible.

A mis Padres: Paula de Jesús Cruz y Santos Cerna que con su amor, sacrificios, consejos y apoyo incondicional, inspiraron en mi la confianza y la perseverancia para culminar mis estudios.

A mis Hermanos y Sobrinita: Por estar conmigo en todo momento de mi vida y por el amor que siempre he recibido de ellos.

A mis compañeros de Grupo: Clara y Geovani por su amistad, paciencia, comprensión y apoyo incondicional. Agradezco a Carmencita por recibirnos en su casa y brindarnos su amistad, atención y comprensión.

A mis familiares y Amigos: Que siempre me brindaron su apoyo y amistad.

DEYSI DOREDITH CERNA CRUZ

INDICE

CAPITULO III

RESUMEN

En el cada vez mas competitivo y rápidamente cambiante ambiente actual, se requieren servicios de información oportunos para una adecuada administración; sin embargo, la información requiere de una base tecnológica que le de soporte.

Esta tecnología de información, posee una gran incidencia en las organizaciones, desde la plataforma del usuario hasta las redes locales, servidores y equipos principales.

Por lo tanto, la administración está obligada a considerar, reconocer y entender los riesgos y limitantes del empleo de dicha tecnología, así como comprender y administrar dichos riesgos, para proporcionar una dirección efectiva y controles adecuados.

Las cadenas de supermercados, como cualquier organización moderna deben cumplir con requerimientos de calidad y seguridad, tanto para su información como para sus activos. En consecuencia, se debe obtener un balance adecuado entre riesgos e inversión, así como en el uso de los recursos de personal y tecnológicos.

En ese sentido, uno de los apoyos para la Administración Superior, debieran ser las Unidades de Auditoria Interna, las cuales deben evolucionar y aplicar en su plan de trabajo un enfoque de riesgos de negocios.

Actualmente, las Unidades de Auditoria Interna de las Cadenas de Supermercados de El Salvador, no disponen de herramientas, que les sirvan de guía para la evaluación de la administración de riesgos, derivados del uso de tecnología de información; que permitan minimizar los riesgos asociados al uso de dicha tecnología.

En consecuencia, el presente trabajo está enfocado en el diseño de Lineamientos para las Unidades de Auditoria Interna, que les permitan contribuir de manera efectiva en la gestión de riesgos de la organización.

INTRODUCCIÓN

“La profesión contable hacia la nueva visión de negocios”, fue el lema de la XXV Conferencia Interamericana de Contabilidad, celebrado en Panamá en Septiembre de 2003, el cual fue adoptado para el Seminario de Graduación del año lectivo 2004.

El tema abordaba los nuevos retos para el profesional de la Contaduría Pública, en el contexto actual de la economía.

Un rasgo típico de esta nueva economía, es la reestructuración de las organizaciones a fin de modernizar sus operaciones y aprovechar los avances en tecnologías de información para mejorar su posición competitiva.

Algunas de estas tecnologías son: la alta velocidad en el procesamiento de datos, intercambio electrónico de datos, la comunicación en Internet, comercio electrónico, entre otros.
Esto hace que la información y los datos en los cuales se apoyan sean cada vez mas importantes y representen activos de gran valor. Sin embargo, no se pueden ignorar los riesgos inherentes a la implementación de estas tecnologías.

Por lo tanto, el auditor interno debe desempeñar una importante función en la organización y contribuir a la adecuada gestión de éstos riesgos asociados.

La investigación efectuada con las Unidades de Auditoria Interna de las Cadenas de Supermercado de El Salvador, tuvo como resultado el diseño de Lineamientos, que les permitan participar activamente en la gestión de estos riesgos empresariales.

La estructura del documento es la siguiente:

El Capítulo I, que contiene el Marco Teórico hace un bosquejo de los componentes principales de esta investigación. Se comenta sobre el desarrollo histórico de las cadenas de supermercados en El Salvador, sus antecedentes y rasgos principales. Se enfoca la incidencia de las tecnologías de información en el quehacer de estas organizaciones y su importancia en el procesamiento de datos. Posteriormente, se enfatiza la necesidad e importancia de que las organizaciones posean un sistema de administración de riesgos, los cuales surgen de manera inherente a la implementación de estas tecnologías. Por último, se presenta a los Auditores Internos y su incidencia en la evaluación de la administración de riesgos, como una parte importante en la estructura de control de la organización.

El Capítulo II, que contiene la Metodología de Investigación revela el tipo de estudio aplicado, la determinación de la población y muestra, las unidades sujetas de análisis. También define el proceso de recolección de información, la técnica utilizada. Al final del estudio, se presenta un análisis de las respuestas obtenidas de los encuestados y el correspondiente diagnóstico, con el cual se confirma la razón de ser, de la investigación.

El Capítulo III, demuestra el aporte elaborado en respuesta a la necesidad planteada en la investigación. Este aporte adopta la forma de Lineamientos, los cuales van dirigidos a los Auditores Internos , como una herramienta que les provea y exponga las nociones mas importantes en un trabajo de evaluación de riesgos en tecnología de información.

El Capítulo IV, expone las conclusiones obtenidas por el grupo de investigación, también se efectúan algunas recomendaciones con el fin de contribuir en el desarrollo cualitativo de los Auditores Internos, y en general de los profesionales de la Contaduría Pública.

CAPITULO I

MARCO TEORICO

1.1 Los supermercados en El Salvador

1.1.1 Creación de los primeros supermercados

La necesidad de satisfacer el gusto más exigente del consumidor; disparó en El Salvador un ambiente de ventas de productos alimenticios a bajos costos y competitivos a nivel nacional, estableciéndose un solo lugar accesible de compra-venta para proporcionarle al cliente la libertad de poder escoger a su propia conveniencia el producto más idóneo entre una variedad de artículos.

Al mismo tiempo se pretendía eliminar la costumbre que el cliente tenía que consultar al vendedor de un establecimiento lo que deseaba, es decir los productos se exhibían o eran colocados sobre mostradores detrás de un dependiente lo cual impedía el acceso directo de apreciar el producto que la persona necesitaba.

Además la visión empresarial requería sentar las bases en el desarrollo de impulsar las ventas masivas de productos de

primera necesidad y abarrotes ya sea como unidad al detalle o al mayoreo y estableciéndose un sistema de pagos en efectivo, comenzándose así a impulsar los títulos de: “oferta del día”, “al dos por uno”, “a mitad de precio”, “especiales de la semana”. Estableciéndose así como filosofía principal en la creación de los supermercados la satisfacción de las necesidades de valor, variedad y servicio al consumidor

1.1.2 Precursores del concepto de supermercados

Pioneros como Don Daniel Callejas, fueron los primeros visionarios en introducir al mercado salvadoreño, la idea de concentrar en un solo lugar, una variedad completa de artículos, para satisfacer las necesidades de los consumidores.

Los primeros supermercados de los cuales se tienen datos; surgen a principios de la década de 50´s, algunos son SUMESA, Abarrotería El Cochinito y Tienda Carmela. Desde aquella época, la publicidad era el medio utilizado, para forzar el cambio en las costumbres de los consumidores y hacer más amigable la transición en el modo de comprar los abastecimientos; pues en esos tiempos, más del 95% del mercado era sector informal, un porcentaje sumamente importante.

1.1.3 Algunos impactos económicos y sociales del surgimiento de los supermercados

Entre los impactos económicos y sociales que se dieron por el surgimiento de los supermercados en El Salvador se pueden mencionar los siguientes:

- Generación de empleos directos e indirectos.
- Es un medio utilizado por los productores para realizar mayores ventas de sus productos, estableciéndose como puntos fijos de comercialización.
- Satisfacción de las necesidades de los consumidores.
- Disminución del índice de desempleo del país.
- Mayor incorporación laboral del sexo femenino.
- Mayor inserción de jóvenes a la población económicamente activa.
- Reducción de los niveles delincuenciales.
- Disminución de epidemias debido a la implementación de higiene en cada uno de los productos que se comercializa.

1.1.4 Los supermercados en la época actual

1.1.4.1 Ámbito nacional de los supermercados

Hace más de cincuenta años, cuando surgen los primeros supermercados en El Salvador, el sector informal era dominante, esta situación ha cambiado y la tendencia de compra de los salvadoreños, está inclinada hacia estos lugares, que ofrecen bienes y servicios para absoluta satisfacción de los clientes. Actualmente los supermercados ofrecen servicios bancarios, comida rápida, diversión, belleza y otros más.

Uno de los principales estandartes para el éxito del negocio, es la ubicación y cobertura geográfica, partiendo de esto es fácil deducir porque se ubican en lugares estratégicos y populosos; municipios importantes, ciudades en desarrollo, entre otros.

El recurso humano, es uno de los factores más importantes para éstos negocios; pues constituyen el primer contacto con el cliente, por lo cual, las cadenas de supermercados procurar ofrecer buena atención y servicio al cliente, promoviendo el trabajo en equipo como filosofía de trabajo, para acercarse mas al cliente y buscar su fidelidad.

El disponer de un gran surtido de productos, exige que la base tecnológica para manejarlos sea adecuada. Según el tamaño de diversidad de las cadenas de supermercado, pueden sobrepasar fácilmente los cincuenta mil artículos. Ante esta situación, la

dependencia de tecnología de información es abrumadora; para registrar, recopilar, procesar y analizar los resultados de sus operaciones.

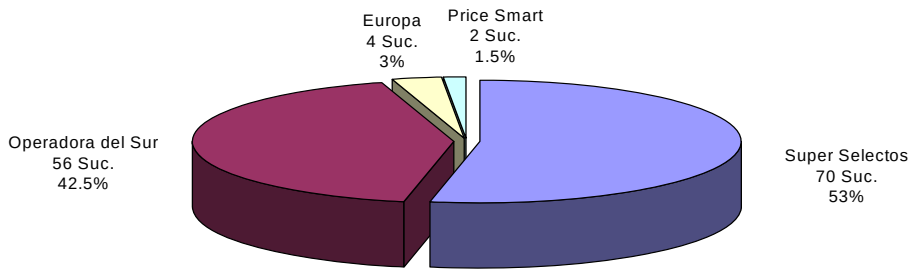
Uno de los usos mas sobresalientes de la tecnología es la aplicación de los códigos de barra, que identifican a un producto de manera precisa (tamaño, peso, color, precio). El código es “leído” por un escaner y procesado en ordenadores, bajo el formato de punto de venta (POS Point of sale).

Según el diseño del sistema POS, éste puede ofrecer datos importantes, tales como: cantidad de artículos vendidos, venta percápita, línea de productos con mayor venta, franja horaria con mayor visita de clientes, uso de servicios de colectores (pagos a favor de terceros) y más. La tecnología no solo facilita la gestión de ventas, sino todo el proceso de aprovisionamiento de productos y gestión con los proveedores.

1.1.4.2 Participación en el Mercado

A continuación se presenta el grado de participación de los supermercados, en el mercado de consumo salvadoreño. (al mes de Agosto 2004). Considerando como factor de participación, el número de sucursales.

No.	Cadena de supermercados	Número de sucursales	Participación en el Mercado
1	Super Selectos	70	53%
2	Operadora del Sur	56	42.5%
3	Europa	4	3%
4	Price Smart	2	1.5%
TOTAL		**132**	**100%**



1.2 Tecnología de Información utilizada por los supermercados en El Salvador

Las soluciones tecnológicas permiten una mayor integración debido a la capacidad de respuesta que tienen ante los proveedores, clientes, competidores y prospectos logrando de esta manera un desarrollo empresarial.

1.2.1 Aporte de las tecnologías de información a los supermercados

El valor que aportan las Tecnologías de información a las empresas es la eficacia, porque les permite lograr rentabilidad, exactitud y rapidez en la toma de decisiones.

Entre los resultados que aporta la Eficacia de las tecnologías de información está el ahorro ya que les permite realizar todas sus operaciones con la minimización de gastos operativos, administrativos y productivos para una mayor rentabilidad y convertir a la empresa en un organismo altamente competitivo.

Toda compañía que se encuentra inmersa en la nueva economía de la cual es participe El Salvador, debe implementar un ambiente estructurado de gestión empresarial, para poder hacerle frente al mercado competitivo y globalizado que existe.

Para el caso se puede precisar que en el país actualmente; el sector de los supermercados se encuentra sumamente desarrollado, ya que tienen implantado tecnologías de información de punta en cada uno de los diferentes procesos que se realizan, creando así un adecuado fortalecimiento del sector.

Estas Tecnologías de Información les han brindado a los diferentes establecimientos una serie de aportes para el buen funcionamiento de todas sus operaciones, constituyendo una herramienta valiosa de innovación y de proyección hacia el futuro; por lo que se hace mención de lo siguiente:

- Estas compañías cuentan con una información adecuada, puntual, fácil y de oportuno acceso cuando es requerido, con una coordinación y colaboración basadas en las nuevas Tecnologías.

- Las Tecnologías de Información brindan y crean un medio accesible para llegar al consumidor final, siendo un componente fundamental de la razón de ser de estos negocios.

- Han permitido la optimización de los procesos administrativos: velocidad de procesamiento, grandes capacidades de almacenamiento y un adecuado intercambio de información, ya que todos estos sistemas están enfocados a todas y cada una de las áreas de la empresa (Financiera, Administrativa, Mercadeo, etc.).

- Existe una mejora de los medios de comunicación y un adecuado control de las variables externas referentes a los niveles de competencia en el mercado, aumentándose así el crecimiento del negocio a nivel nacional.

- Se ha efectuado una conexión explícita del plan de negocios de estos supermercados con el propio plan que poseen cada uno de las tecnologías de información, lo cual genera un mejor soporte a los objetivos y metas que estas organizaciones persiguen.

- Contribuyen a realizar comercio entre los supermercados y proveedores de una manera rápida y eficaz evitándose la utilización de los voluminosos documentos, los cuales para llegar a cada uno de los destinos se toma su respectivo tiempo, beneficiándose así la relación de los negocios entre ellos.

- La implantación de esta variedad de procesos tecnológicos les ha permitido a estas cadenas mantener en constante renovación los productos comerciales moviendo miles y miles de artículos cada día, ampliando también los servicios a ofrecerse e incrementando la calidad y cantidad de dichos bienes.

- Se han creado mensajes estándares y estructurados para que la información contenida en ellos se interprete de una forma homogénea por parte de las cadenas participantes en la transacción; como ejemplo de estos mensajes pueden ser: ordenes de compra, avisos de mercadería despachada como de recibida, ordenes de pago y/o cualquier otro documento necesario para hacer valida una operación (supermercados – proveedores).

1.2.2 Intercambio Electrónico de Datos (EDI)

1.2.2.1 Definición

Constituye un conjunto lógico y ordenado de datos y/o procesos, que se encuentran configurados de acuerdo a normas de mensajes preestablecidos, para la adecuada comunicación entre sistemas de información, a través de medios electrónicos, elaborados en un lenguaje capaz de ser interpretado y procesado automáticamente por un ordenador

1.2.2.2 Importancia del EDI en los supermercados

La incorporación de un adecuado intercambio de datos en las miles y miles de operaciones que realizan los supermercados es

de vital utilidad ya que es parte integrante del desarrollo comercial que se impulsan constantemente en la satisfacción de los exigentes gustos de los consumidores.

También es importante por la visión que manejan las cadenas de supermercados procurando llevar a la realidad las cifras de tener: “el 20% de los proveedores, trabajando a través de EDI, y que suponga el 80% de las ventas.”[1]

Permite ejercer un adecuado control de todos los cambios de factores internos y externos del entorno competitivo en los cuales se desenvuelven estas compañías, impulsando eficiencia y eficacia en todas sus operaciones, logrando mantenerse sólidos y firmes en el tiempo y con una cobertura de mercado nacional como factor importante para el fortalecimiento del sector comercio en El Salvador.

1.2.2.3 Ventajas del Intercambio Electrónico de Datos.

La adecuada implantación y utilización del Intercambio Electrónico de Datos crea de innumerables beneficios a los supermercados haciéndose mención de lo siguiente:

[1] “Economía y Negocios” Alberto Labadía, octubre de 1999.

- Ahorro de tiempo y dinero, la información viaja por redes de comunicación.
- Se producen menos errores, ya que el proceso esta completamente automatizado y los ordenadores se equivocan menos.
- Sustituye el soporte de papel de los documentos comerciales mas habituales por transacciones electrónicas con formato normalizados y acordados previamente entre los usuarios del servicio.
- Mejora de la competitividad de la empresa que lo adopta.
- Se consigue mayor control de calidad en las operaciones.
- La relación entre socios comerciales se fortalece creando mayores transacciones y utilidades entre ellos.
- Disminución de Stocks, debido a la facilidad de aplicación de técnicas “Justo a Tiempo”.
- Se relacionan aplicaciones informáticas que residen en las computadoras de las distintas empresas.

1.3 Administración de Riesgos en Tecnología de Información

Es el desarrollo de un ambiente de decisiones y la determinación de acciones para valorar la posibilidad de fallas o pérdidas que se puedan generar en el uso de las tecnologías de información

con el objetivo de determinar los riesgos más importantes y las estrategias que se deben utilizar para controlarlos.

1.3.1 Importancia de la administración de riesgos en Tecnología de información

Conocer de una manera anticipada las posibles pérdidas en la información generada por las tecnologías para poder implementar los procedimientos adecuados que minimicen los daños y los costos causados por los riesgos informáticos y de esta manera garantizar el mejor uso de los recursos y un buen funcionamiento de la organización.

1.3.2 Clasificación de los riesgos en tecnología de información

A continuación se presentan los principales riesgos en tecnología de información que pueden afectar a las cadenas de supermercados.

1.3.2.1 Riesgos de Integridad

Este tipo de riesgos abarca directamente los relacionados con la autorización y exactitud de la entrada de información la cual se

dá dentro del procesamiento de datos y los reportes de la información generados por los sistemas. La integridad de los sistemas puede perderse debido a las siguientes causas:

a) **Errores de programación:** Estos se dan cuando la información se introduce de manera correcta pero es procesada de diferentes formas debido a que los programas utilizados fueron mal construidos generando así una mala información que puede causar grandes pérdidas a la empresa.

b) **Procesamiento de errores:** Este tipo de riesgos ocurren cuando la información que se introduce a los sistemas se efectúa de manera incorrecta ya que las personas encargadas de procesar la información cometen errores al introducirla.

c) **Administración y procesamiento de errores:** Estas situaciones de riesgos ocurren cuando el mantenimiento que se le efectúa a de los sistemas se da de manera inapropiada lo que puede generar daños graves a los sistemas y un incremento en los costos para poder mantenerlos funcionando adecuadamente.

1.3.2.2 Riesgos de relación

Se refieren al uso oportuno que se le puede dar a la información generada por los sistemas para una toma de decisiones adecuadas

dentro de la organización porque de éstas depende el futuro y el buen funcionamiento de la entidad.

1.3.2.3 Riesgos de acceso

Se generan cuando se ingresa de manera inapropiada a los sistemas lo que puede causar daños a la información, a los datos y a los mismos programas utilizados debido a que personas ajenas a la entidad pueden accesar a información confidencial y esto le causaría grandes daños y pérdidas. Entre las causas que pueden originar estos riesgos están:

- Segregación inapropiada de funciones.
- Mala integridad de la información de los sistemas.
- Poca Confidencialidad de la información, etc.

1.3.2.4 Riesgos de utilidad

Estos riesgos se enfocan en tres diferentes niveles los cuales son:

a) Pueden ser enfrentados de manera preventiva de acuerdo a la dirección que se le dé a los sistemas para poder determinar los problemas antes que ocurran y de esta manera poder controlarlos.

b) Uso de Técnicas de recuperación para poder reducir el daño de los sistemas o de la información generada y de esta manera poder garantizar un adecuado funcionamiento y una reducción de los costos.

c) La implementación de planes de contingencias para controlar los desastres en el procesamiento de la información y la creación de backups para su protección.

1.3.2.5 Riesgos en la infraestructura

Estos ocurren cuando en las organizaciones no existe una estructura tecnológica efectiva que pueda adecuarse a las necesidades presentes y futuras con el propósito de cumplir de manera eficaz el proceso de la información tecnológica en la que se definen, desarrollan, mantienen y operan un entorno del procesamiento de la información.

1.3.2.6 Riesgos de seguridad general

Son estándares que proporcionan requisitos para lograr una seguridad general y así disminuir los riesgos tales como:

- Choques eléctricos.
- Incendios de los sistemas.

- Niveles inadecuados de energía eléctrica.
- Riesgos mecánicos, etc.

1.3.3 Técnicas de procedimientos para administrar riesgos

Estas técnicas de procedimientos las utilizan las organizaciones porque sirven de base para realizar la administración de riesgos con el propósito de minimizar los costos en el caso que las amenazas de riesgos se hagan efectivas. A continuación se presentan las diferentes técnicas de procedimientos que se pueden utilizar para la administración de riesgos en tecnología de información

1.3.3.1 Evitar riesgos

Un riesgo es evitado cuando en la organización no se acepta. Esta técnica de procedimientos en muchas ocasiones puede ser más negativa que positiva ya que si la empresa la usa excesivamente sería privada de muchas oportunidades de ganancia por miedo a arriesgarse y probablemente no alcanzaría sus objetivos.

1.3.3.2 Reducción de riesgos

Al utilizar esta técnica las empresas para reducir los riesgos deben de recurrir a programas de seguridad, guardias de seguridad, alarmas y a la estimación de futuras pérdidas con la asesoría de personas expertas.

1.3.3.3 Conservación de riesgos

Esta técnica de procedimientos es la más utilizada para enfrentar los riesgos, pues muchas veces una acción positiva no es transferirlo o reducir su acción sino que la organización debe decidir cuales riesgos se retienen, o se transfieren basándose en la creación de una reserva para contingencias con el objeto de poder soportar la pérdida en un determinado momento.

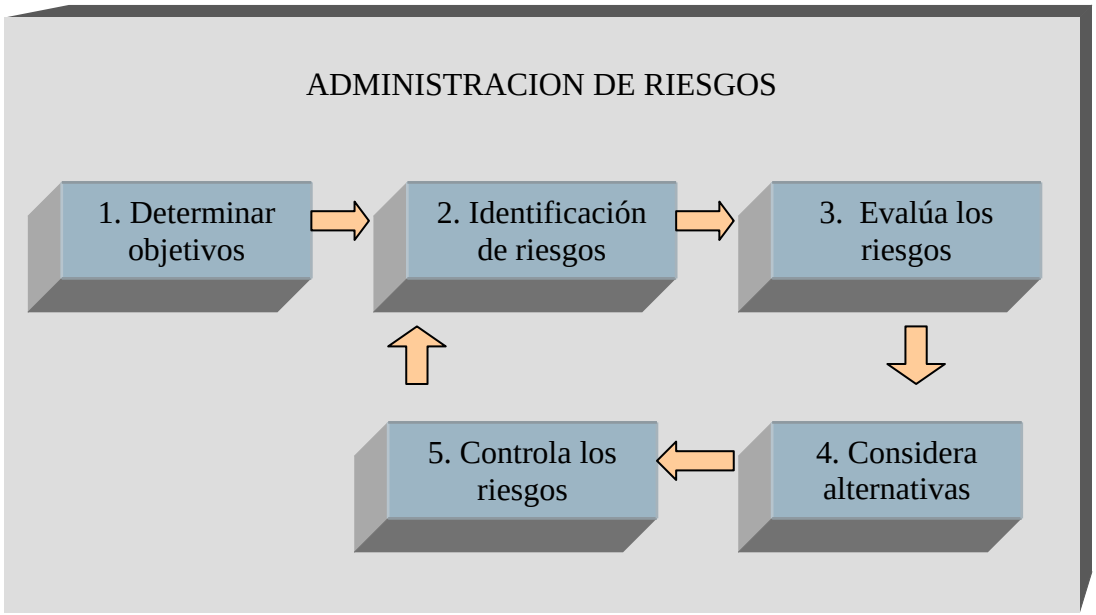
1.3.3.4 Compartir riesgos

Esta técnica se utiliza cuando la posibilidad de pérdida es transferida a otra organización el ejemplo más común son las Aseguradoras ya que la empresa determina que no puede soportar el costo de la pérdida sola, por esa razón decide compartir un

porcentaje de esta y en caso que suceda la organización no carga con todos los costos sino solamente con una parte de estos.

1.3.4 Proceso de la administración de riesgos

El Proceso de la administración de riesgos se puede esquematizar de la siguiente manera:



1.3.4.1 Determinar los objetivos

Es el primer paso que hay que efectuar porque es aquí en donde se desarrolla el programa y los planes de administración de riesgos que se utilizarán para obtener un máximo beneficio y

para garantizar la estabilidad de la entidad con la minimización de los costos relacionados con los riesgos.

Dentro de los objetivos que tiene la administración de riesgos se pueden mencionar los siguientes:

- Garantizar el mejor manejo de los recursos.
- Minimizar los costos causados por los riesgos.
- Seguridad de los sistemas y de la información generada por estos.
- Eliminar preocupaciones posteriores, etc.

1.3.4.2 Identificación de los riesgos

Proporciona la información de los indicios que le permiten ubicar los riesgos principales antes que estos afecten los sistemas, por lo que es una tarea difícil ya que nuevas amenazas están surgiendo constantemente, siendo necesarias metodologías, técnicas y herramientas que ayuden a la identificación de los riesgos.

1.3.4.2.1 Metodologías de identificación de riesgos

Estas metodologías son desarrolladas como parte de la prevención de pérdidas y esfuerzos de control como las que se mencionan a continuación:

a) Identificación basada en pérdidas pasadas

Se hacen inspecciones para acumular información acerca de sucesos pasados y con base a las experiencias anteriores se puedan predecir pérdidas futuras y tomar las medidas necesarias para controlar dichos riesgos, esta regla de identificación es muy importante porque requiere de conocimientos pasados para prevenir pérdidas o daños futuros.

b) Técnicas de sistemas de seguridad

Son técnicas lógicas que ayudan a la detección y corrección de amenazas de riesgos a través de un sistema de seguridad bien detallado para la prevención de pérdidas o causas de accidentes antes que estos ocurran.

1.3.4.2.2 Herramientas de Identificación de riesgos

Son documentos que proveen guías para organizar e interpretar la información acumulada por la organización a través de las técnicas utilizadas, estas herramientas son diseñadas para facilitar el proceso de la identificación de riesgos y entre las cuales se mencionan:

1.3.4.2.2.1 Cuestionarios de análisis de riesgos

Están diseñados para descubrir amenazas a través de una serie de preguntas con el propósito de orientar a la organización sobre los riesgos a los cuales está expuesta ya que es una herramienta que acumula información de documentos, entrevistas e inspecciones para guiar a las personas encargadas de la administración de riesgos a identificar las exposiciones a riesgos a través de un modelo lógico y consistente.

1.3.4.2.2.2 Lista de chequeos de exposiciones a riesgos

Es una herramienta utilizada con frecuencia para la identificación de riesgos ya que consiste en enumerar las amenazas más importantes a las cuales la entidad está expuesta con el propósito de identificarlos fácilmente antes que ocurran y tomar las medidas necesarias para disminuir el grado de ocurrencia y la pérdida de información.

1.3.4.2.2.3 Lista de chequeos de políticas de seguridad

Es un catálogo de políticas de seguridad diseñado por la administración para la aplicación de medidas correctivas y de prevención ante el surgimiento de riesgos que puedan ocasionar daños a los sistemas y a la información generada por estos.

1.3.4.2.3 Técnicas de identificación de riesgos

1.3.4.2.3.1 Orientación

Es importante el conocimiento que se tenga de la organización y de las operaciones que esta realiza para que la toma de decisiones sobre la identificación de los riesgos sea efectiva ya que a través de estos conocimientos se puede determinar las ventajas y desventajas que tiene la entidad para afrontar los riesgos que puedan surgir durante este proceso y de esta manera se puedan estimar los costos que tendrían si se llegaran a presentar.

1.3.4.2.3.2 Análisis de documentos

Las actividades que realiza la organización así como la historia de ésta son archivadas en diferentes clases de registros que representan una fuente importante de información requerida para el análisis de los riesgos y entre estos podemos mencionar:

a) Informes de análisis financieros

Los balances y los Estados de resultados son fuente de información básica que ayudan a la identificación de riesgos ya que a través del balance se puede determinar los tipos de activos que posee la institución para determinar las pérdidas a las cuales están expuestas. En cuanto al Estado de Resultados este indica la cantidad de dinero o capital que esta disponible para poder solventar cualquier daño que se pueda generar.

b) Diagramas de flujo y organigramas

A través del análisis de los diagramas de flujos se puede determinar las operaciones inusuales de la organización ya que revela el tipo de actividades y la secuencia que estas tienen y de este modo descubrir todas las contingencias que puedan interrumpir el proceso de las operaciones para poder determinar las medidas adecuadas de corrección y prevención.

En cuanto a los organigramas estos documentos proveen al identificador de riesgos conocimientos de la naturaleza de la entidad y del campo de acción de las actividades que se realizan.

c) Políticas y reportes de pérdidas

Las políticas son importantes para evaluar el alcance que tendrán la identificación de riesgos dentro de la organización. En cuanto a los reportes de pérdidas esta información ayuda en el proceso de identificación porque indican las clases de daños ocurridos para poder estimar el grado de riesgos que tienen ciertas actividades u operaciones de la organización.

d) Entrevistas

Ayudan en la identificación de riesgos porque alguna información no es registrada en documentos sino solamente existe en la mente de las personas por lo que se hace necesario entrevistar al personal y a través de la información brindada determinar medidas que ayuden a la administración de riesgos.

e) Inspecciones

Es la técnica más usada en la identificación de los riesgos porque ayuda a obtener un buen conocimiento de las operaciones de la organización, indica las posibles áreas de protección

que tienen los sistemas y revela las posibles pérdidas que puedan ocurrir.

1.3.4.3 Evaluación de riesgos

Una vez que los riesgos han sido identificados deben de ser evaluados, lo que implica la medición cuantificable de la magnitud de una pérdida o la probabilidad que ésta ocurra, para ser clasificados por orden de prioridades, el impacto financiero que estos daños podrían tener son: costos a largo o corto plazo o una pérdida de la participación en el mercado que se desenvuelve.

A continuación se presentan la clasificación de los riesgos fundamentadas en su magnitud

a) Riesgos críticos

Son todas las exposiciones a pérdida en las cuales la gravedad alcanza el hundimiento o fracaso total de la organización.

b) Riesgos importantes

Exposiciones a pérdida que no logran la quiebra de la empresa, pero requiere de acciones significativas por parte de la

organización para poder continuar con el funcionamiento normal de sus operaciones.

c) Riesgos no importantes

Presentación de riesgos que no causan un gran impacto financiero a la organización por lo cual pueden continuar con el desempeño de sus actividades.

1.3.4.4 Consideración de alternativas y selección de mecanismos de tratamiento de riesgos.

Luego de la evaluación de los riesgos se procede a la aplicación de las técnicas que sean necesarias para tratar los riesgos, lo que incluye: evitar los riesgos, retención, transparencia y reducción de las pérdidas.

1.3.4.5 Control de los riesgos

La prevención de los riesgos es muy importante dentro de la organización para lo cual se deben diseñar programas que por lo menos abarque las siguientes áreas:

- Seguridad personal.
- Seguridad de bienes.
- Control de responsabilidades de pérdidas.

- Protección de propiedades.
- Seguridad física.

1.4 El auditor interno ante la evaluación de la administración de riesgos en tecnología de información

1.4.1 Marco técnico para la práctica profesional de la auditoría interna.

El Instituto de Auditores Internos (IIA por sus siglas en inglés, Institute of Internal Auditors), es una Asociación Internacional dedicada al desarrollo profesional continuado del auditor interno y de la profesión de auditoria interna.

En Junio de 1999, el Consejo de Administración del IIA, aprobó el Marco para la Práctica Profesional de la Auditoria Interna, el cual contempla una Definición de Auditoria Interna, el Código de Ética, las Normas y los Consejos para la Práctica de la Profesión.

1.4.1.1 Reglas de conducta (Código de ética) que describen las normas de comportamiento que se espera sean observadas por los auditores internos.

El Código de Ética define la Auditoria Interna, como ‘una actividad independiente y objetiva de aseguramiento y consulta concebida para agregar valor y mejorar las operaciones de una organización,..., ayudando a cumplir sus objetivos, aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno.’

La función principal de este código es proveer orientación a los auditores internos, proporcionando dos componentes esenciales: Principios y reglas de conducta, los cuales guían la conducta ética de los mismos.

1.4.1.1.1 Integridad

Este principio debe ser la base del comportamiento del auditor y es la razón para que se deposite confianza en el trabajo que realiza.

Las reglas de conducta requieren que el auditor sea honesto, diligente, responsable, respetuoso de las leyes y objetivos de

la organización, evitando cualquier acto en detrimento de la profesión y de la institución a la que presta sus servicios.

1.4.1.1.2 Objetividad

Los resultados obtenidos en la ejecución del trabajo del auditor, deben ser expuestos e informados de manera equilibrada, sin tendencias a favorecer los intereses propios o de terceros. Es decir, debe ser imparcial en sus juicios.

1.4.1.1.3 Confidencialidad

La información es un activo que pertenece a la organización, por lo tanto, el auditor no divulgará datos que no le pertenezcan, o que en razón de su trabajo haya conocido; sin la debida autorización o salvo exigencia de una autoridad competente.

1.4.1.1.4 Competencia

Los auditores están obligados a utilizar el cúmulo de conocimientos, capacidades y experiencias, para desempeñar los servicios de auditoria de la mejor forma posible.

1.4.1.2 Aplicación de normas para el ejercicio profesional de la auditoria interna

Debido a la diversidad de las organizaciones, la práctica de la auditoria interna es susceptible de adoptar distintos rasgos, que afecten de manera importante la profesión.

Por esa razón, se hace imprescindible la existencia y aplicación de Normas que regulen el ejercicio de la profesión.

1.4.1.2.1 Normas sobre atributos

En general, proveen un marco de características generales de las organizaciones y de quienes desarrollan la auditoria interna. Considerando aspectos sobre la autoridad y responsabilidad del auditor, independencia, objetividad, pericia y cuidado profesional, calidad y cumplimiento de normas, entre otras.

1.4.1.2.2 Normas sobre desempeño

Este grupo de normas describen la naturaleza de las funciones del auditor y constituyen parámetros de calidad, para medir su trabajo. Algunas de estas se refieren a la administración de la auditoria, adecuada comunicación de planes y aprobación de

requerimientos de recursos, diseño de políticas y procedimientos de auditoria, así como la naturaleza del trabajo.

1.4.1.2.3 Normas de implantación

Consisten en una extensión a las normas de atributos y desempeño, están diseñadas para desarrollar la aplicación de éstos dos grandes grupos. Asimismo, pueden ser específicas y orientadas a trabajos de consultoría, inclusive.

1.4.1.3 Lineamientos para la práctica normativa de la auditoria interna

Es un conjunto de Consejos, guías o recomendaciones para la practica de la profesión; debido a su naturaleza no constituyen una norma de aplicación obligatoria, el uso es opcional.

1.4.2 La aplicación de las normas de desempeño en la evaluación de la administración de riesgos

1.4.2.1 Norma 2100 Naturaleza del trabajo

La función de auditoria interna evalúa y colabora con la mejora permanente de los sistemas de administración de riesgos, control y gobierno de la organización.

El uso de sistemas de información y la tecnología, incorporan riesgos para cualquier institución que hace uso de éstos recursos; los cuales deben ser supervisados y evaluados por el auditor interno, tal como lo prescribe la Norma 2110 Gestión de Riesgos.

Específicamente, la sección A2 de esta norma hace énfasis en la evaluación de aquellas exposiciones a riesgos derivadas de los sistemas de información y requiere que se evalúen como mínimo los siguientes aspectos:

- ✓ Confiabilidad e integridad de la información, ya sea financiera u operativa.
- ✓ Eficacia y eficiencia de las operaciones.
- ✓ Protección de activos.
- ✓ Cumplimiento de leyes, regulaciones y contratos.

Los pasos mínimos a seguir para alcanzar la gestión de riesgos, incluyen la identificación, análisis y control de los mismos.

1.4.3 Administración del riesgo bajo el enfoque del COSO

El Committe of Sponsoring Organizations of the Treadway Commission, emitió el Internal Control – Integrated Framework (Control Interno – Estructura Conceptual), provee una nueva

visión y definición del control interno, como un proceso que busca dar seguridad sobre la consecución de los objetivos de operación, información financiera y de cumplimiento de leyes y regulaciones de una organización.

Las circunstancias que impiden alcanzar los objetivos antes detallados, pueden tener diferente origen y se denominan Riesgos.

Bajo el enfoque del Informe COSO, la administración de riesgos es una actividad crítica, en cualquier sistema de control interno que busque ser efectivo; este proceso incluye lo siguiente:

1.4.3.1 Identificación de riesgos

Los riesgos pueden tener origen externo e interno de la organización, por lo tanto, deben diseñarse los procesos que permitan alertar sobre la exposición a éstos; debe considerarse además, que pueden estar a nivel de la entidad y de las actividades que esta desempeña.

Algunos ejemplos de riesgos externos son: las cambiantes necesidades y expectativas de los clientes, afectando los

productos y servicios que se ofrecen así como los términos de venta; el accionar de la competencia, la legislación y nuevas regulaciones, catástrofes naturales, cambios económicos y políticos, entre otros.

De origen interno son los siguientes riesgos: las rupturas en el procesamiento de datos, el personal y su lealtad, cambios internos y la participación de órganos internos de fiscalización.

Los riesgos a nivel de actividad se relacionan con los problemas que imposibiliten el normal de sus labores productivas, el aprovisionamiento de materias primas, en tiempo, cantidades y precios.

1.4.3.2 Análisis de riesgos

Esto incluye hacer una estimación del significado de un riesgo, es decir, medir el posible efecto o impacto y la probabilidad de ocurrencia, cuanto mas sea el impacto y posea un alto grado de ocurrencia, exigirá atención inmediata y considerable.

Posteriormente, la administración del riesgo conlleva la toma de decisiones respecto de las Actividades de Control, las cuales

parten de un análisis de costo – beneficio, que permitan reducir o eliminar el efecto.

No obstante, esto no es suficiente pues debe garantizarse un monitoreo efectivo sobre la implementación y efectividad de las acciones tomadas al respecto.

1.4.3.3 Manejo de cambios

Bajo la premisa, de que ‘lo único constante es el cambio’; en el proceso de identificar y gestionar los riesgos, debe existir la conciencia de que el entorno exige un conjunto de condiciones renovado, para mantener su efectividad.

Es conocido que las circunstancias detalladas a continuación llevan implícitos cambios que conllevan nuevos riesgos: personal contratado recientemente, cambios en la plataforma tecnológica, nueva tecnología, incremento de la competencia, nuevas líneas de productos, reestructura corporativa, operaciones en el extranjero, crecimiento rápido, entre otros.

1.4.3.4 Actividades de control para la valoración de riesgos

La administración debe identificar y ejecutar políticas y procedimientos que contribuyan al manejo adecuado de los riesgos, sobre todo que permitan verificar la aplicación de acciones adecuadas y oportunas, en la identificación y gestión de riesgos.

1.4.3.5 Control sobre los sistemas de información

Estos cada vez son más necesarios, debido que existe mayor dependencia al uso de la tecnología para el procesamiento de la información, por lo cual se deben de tener revisiones que garanticen un buen funcionamiento de los sistemas que se están utilizando. A continuación se detallan los controles siguientes:

1.4.3.5.1 Controles generales

El objetivo principal de estos controles, consiste en asegurar la continuidad y operación adecuada del centro de datos, software de sistema, de administración de accesos y aplicaciones del sistema.

1.4.3.5.2 Controles de aplicación

Estos se refieren al control de las aplicaciones en proceso, asegurando que el procesamientos de los datos, se realice de

manera completa y exacta. Es decir, aquellas tareas que están diseñadas para ser ejecutadas automáticamente por un proceso computarizado.

1.5 Evaluación de la administración de riesgos en Tecnología de información

Con el progreso económico y la complejidad de los negocios, las responsabilidades de la Administración Superior, con relación a los riesgos y controles son mas vitales para el éxito de la organización.

En ese sentido, la función de auditoria interna, adquiere mayor importancia, pues constituye uno de los apoyos principales de la Administración, para alcanzar los objetivos de la Organización, evaluando y mejorando la eficacia de los procesos de gestión, control y gobierno.

En la evaluación de tecnologías de información, existen dos metodologías muy identificadas: la Auditoria Informática y el Análisis de Riesgos. La primera identifica el nivel de exposición por la falta de controles y la segunda facilita la evaluación de los riesgos y recomienda acciones correctivas.

Ambas metodologías hacen uso de los conceptos siguientes:

- Amenazas: posibles fuentes de peligro o catástrofes. Vulnerabilidad: situación creada con la que la amenaza pudiera acaecer y dañar la tecnología de información.
- Riesgo: probabilidad de ocurrencia de una amenaza por la existencia de una vulnerabilidad.
- Impacto: la medición del efecto del riesgo en la organización.

Las metodologías pueden tener carácter Cuantitativo o Cualitativo, el primero basado en modelos matemáticos y el segundo, en el criterio, razonamiento y experiencia humana.

El proceso de evaluación ejecutado por auditoria interna debe incluir, al menos los siguiente pasos:

- ✓ Evaluar los objetivos y las políticas de la administración de riesgos: esto implica la medición de programas con estándares y los objetivos del programa representan los primeros estándares lógicos. Esta evaluación puede incluir una revisión de las finanzas de la organización y su habilidad de soportar pérdidas.

- ✓ Identificar y evaluar las exposiciones a riesgos existentes en la organización, mediante el análisis de actividades y operaciones utilizadas por la administración para determinar las distintas exposiciones a pérdida.

- ✓ Evaluar las decisiones relacionadas a pérdida, este paso incluye una revisión de la extensión de los riesgos.

- ✓ Evaluar las medidas de la administración de riesgos que han sido implementadas. Este paso evalúa las decisiones pasadas, verificando que la decisión fue propiamente implementada, incluyendo una revisión de medidas de control y pérdidas financieras.

- ✓ Recomendar cambios para el beneficio del sistema de gestión utilizado por la organización.

1.5.1 Alcance de la auditoria

Las principales áreas que deben ser auditadas de manera periódica son:

- ✓ Políticas de administración de riesgos: este aspecto está enfocado en los objetivos del programa, la responsabilidad

y autoridad del administrador de riesgos y la consistencia de las políticas con los objetivos.

- ✓ Control de riesgos: la naturaleza especializada de la prevención de pérdidas y control para diversos tipos de riesgos hacen necesario realizar auditorías especializadas que pueden incluir:
  - Auditoria de protección.
  - Auditoria de seguridad.
  - Auditoria ambiental.
  - Auditoria de seguridad informática.
  - Auditoria de control de pérdida de propiedades.

De conformidad, con las Normas de auditoria, si el profesional de auditoria interna, no posee la capacidad técnica para llevar a cabo estas funciones; está obligado por principios de ética a divulgarlo, a fin de actuar en concordancia con los objetivos de la organización; propiciando la contratación de servicios externos.

- ✓ Función de seguridad: Esta función puede ser conducida en dos niveles, el primero es la evaluación del rol del auditor en el todo del programa de la administración de riesgos, el segundo es una revisión mas detallada del programa de seguridad, sobre todo del alcance, mediante un detallado análisis.

CAPITULO II

METODOLOGÍA DE LA INVESTIGACIÓN

2.1 Tipos de estudio

El tipo de estudio aplicado determinó la estrategia de la investigación, el diseño, los datos y su forma de recolección y otros componentes del proceso de investigación.

2.1.1 Hipotético Deductivo

La investigación se realizó considerándola Hipotética porque inició de la formulación de un problema el cual se delimitó, justificó y se procedió a la enunciación de Hipótesis con lo que se confirmó la existencia de la problemática planteada, así mismo se concluyó sobre la respuesta al problema de investigación. Y fue deductivo porque generó una síntesis global de los aspectos y vinculaciones esenciales entre todos ellos con el propósito de pasar de afirmaciones de carácter normal a hechos particulares los cuales fueron comparados con la realidad en torno a todas las unidades de auditoria interna de las cadenas de supermercados de la zona metropolitana de San Salvador conclusiones de los planteamientos usuales (Hipótesis).

2.1.2 Analítico Descriptivo[2]

La información obtenida por parte de las compañías investigadas, se relacionó con los elementos generales (teóricos - prácticos) del tema de estudio, fueron examinados en un sentido lógico, obteniéndose de esta forma los elementos específicos que ayudarán al análisis y establecimiento de una síntesis amplia y profunda de la investigación, interrelacionándolos con los factores mínimos de conocimientos y lineamientos que debe poseer el auditor interno ante las diferentes evaluaciones que son consideradas necesarias en una buena administración integral de riesgos a las cuales las cadenas de supermercados se enfrentan en el uso y manejo diario de las operaciones a través de las tecnologías de información.

2.2 Población y Muestra

La población utilizada para esta investigación estuvo conformada por las cuatro cadenas de supermercados que se encuentran operando en el país, bajo la legislación vigente.

La muestra estuvo compuesta por el cien por ciento de las unidades de observación, permitiendo una representatividad total

[2] Rojas Soriano, Raúl. El proceso de la investigación científica.

en la investigación de campo, por lo que, no fue necesario la utilización de fórmulas estadísticas debido a que el universo de investigación es muy reducido.

2.3 Unidades de análisis

Las unidades de análisis sobre las cuales se dirigió la investigación fueron las Unidades de Auditoria Interna, de las cadenas de supermercados de El Salvador, debido a que es en este contexto en donde se desarrolla la problemática planteada.

2.4 Métodos de recolección de información (Técnicas / instrumentos)

El método de recolección de datos, implicó la ejecución de tres actividades secuenciales, éstas fueron:

1 La selección del Cuestionario como instrumento de medición.

2 La aplicación del instrumento, es decir, obtener la información de la población sujeta de estudio.

3 El análisis de los datos obtenidos.

2.4.1 Técnicas

2.4.1.1 Investigación documental

Consistió en la obtención y revisión de literatura, relacionadas con aspectos generales de la investigación utilizando: libros, tesis, leyes, trabajos presentados en conferencias o seminarios, artículos publicadas en Internet, revistas y boletines científicos virtuales, testimonios de expertos y diccionarios.

2.4.1.2 Investigación de campo

En la investigación de campo se utilizó básicamente el cuestionario para la recolección de la información: El cual fue el medio que permitió la realización de un diagnostico del auditor interno ante la evaluación de la administración de los riesgos en tecnología de información.

2.4.2 Instrumento utilizado para la recolección de datos.

2.4.2.1 Cuestionario

El cuestionario se elaboró con preguntas abiertas, cerradas y de opción múltiple. Las primeras con el objeto de obtener

diferentes puntos de vistas por parte de los encuestados y las siguientes se formularon de tal forma que tuvieran opciones específicas para responder o abstenerse. Este instrumento fue dirigido a los auditores internos de las cadenas de supermercados de El Salvador

2.4.2.1.1 Tabulación y análisis de los resultados de la investigación

Los datos recolectados en la investigación, fueron organizados de acuerdo al orden de las preguntas,.para lo cual fueron registradas utilizando tablas de doble o múltiples entradas que permitieron analizar e interpretar la información.

Además se tabuló y analizó cada pregunta por separado, identificando el objetivo de las mismas y las respuestas obtenidas de la población, a fin de describir el comportamiento de los resultados.

OBJETIVO

Conocer el ambiente de control y de administración de riesgos de tecnología de información existente, en las cadenas de supermercados de El Salvador, así como el desarrollo técnico

alcanzado por las unidades de auditoría interna, para la ejecución de su plan de trabajo

Pregunta 1

Como parte de su experiencia profesional en auditoria interna, ¿Ha ejecutado evaluaciones de la administración de riesgos?

Resultado

Descripción	Frecuencia	
	Absoluta No.	Relativa %
SI	3	75
NO	1	25
TOTAL	**4**	**100**

Análisis

Los resultados obtenidos confirman que la mayoría de las unidades de auditoria interna de las cadenas de supermercados de El Salvador si han efectuado en algún momento del proceso de ejecución de su trabajo evaluaciones de la Administración de Riesgos pero enfatizado en términos generales y no aplicado al área de Tecnología de Información.

Pregunta 2

Considera que para evaluar la administración de riesgos en tecnología de información el auditor interno necesita de conocimientos técnicos adicionales a la formación académica?

Resultado

Descripción	Frecuencia	
	Absoluta No.	**Relativa %**
SI	4	100
NO	0	0
TOTAL	**4**	**100**

Análisis

La adquisición de conocimientos técnicos enfocados al área de Tecnología de Información para poder efectuar el trabajo de auditoria con un enfoque especial es considerado por la totalidad de la población como un factor determinante y esencial en esta clase de evaluaciones.

Pregunta 3

A. Existe por parte de la compañía un programa de capacitación continua para el personal de auditoria interna sobre aspectos relacionados a la evaluación de riesgos ó tecnologías de información?

Resultado

Descripción	Frecuencia	
	Absoluta No.	**Relativa %**
SI	2	50
NO	2	50
TOTAL	**4**	**100**

Análisis

La poca existencia de entrenamiento técnico dentro de las cadenas de supermercados de El Salvador constituye un limitante para las unidades de auditoria interna, ya que no se desarrolla el trabajo con efectividad y eficiencia y así obtener los mejores resultados en una evaluación enfocada a la Administración de Riesgos en Tecnología de Información.

B. Si su respuesta es negativa ¿Qué factores dificultan la existencia de un programa de capacitación?

Resultado

Descripción	Frecuencia	
	Absoluta No.	**Relativa %**
Falta de Recursos	0	0
Limitaciones de Tiempo	0	0
No se consideran necesarios	2	100
TOTAL	**2**	**100**

Análisis

El factor principal expresado por la mitad de la población que no reciben ninguna capacitación continua sobre los temas consultados es, que no es considerado necesario por parte de la entidad y aunado a la falta de interés, constituyen un factor decisivo el cual repercute directamente en el resultado del trabajo del auditor y en la adecuada operatividad de la compañía.

Pregunta 4

¿Tiene conocimiento si en su compañía, el departamento de informática realiza la actividad de administración de riesgos en tecnología de información, ya sea de una manera formal o informal?

Resultado

Descripción	**Frecuencia**	
	Absoluta No.	**Relativa %**
SI	2	50
NO	2	50
TOTAL	**4**	**100**

Análisis

De los datos obtenidos de los resultados se determinó que en la mitad de las unidades de auditoria interna es el departamento de

informática el encargado de administrar los riesgos este es un resultado negativo ya que dentro de las empresas debería de existir un departamento establecido únicamente para realizar esta actividad.

Pregunta 5

A. Si la compañía no tiene implementado dentro de sus operaciones la evaluación de la administración de riesgos en tecnología de información, ¿Incluiría usted dentro de su plan de trabajo el efectuar este tipo de evaluaciones?

Resultado

Descripción	Frecuencia	
	Absoluta No.	**Relativa %**
SI	3	75
NO	1	25
TOTAL	**4**	**100**

Análisis

De los resultados obtenidos la mayor parte de las unidades de auditoria interna expresó que si incluirían dentro de su plan de trabajo la evaluación de la Administración de Riesgos en Tecnología de Información, lo que indica la importancia que tiene para los auditores internos y las empresas realizar este

tipo de evaluaciones ya que la adecuada administración de riesgos conlleva a prevenir pérdidas que puedan causar grandes daños a la organización.

B. Si su respuesta a la pregunta anterior fue negativa señale los motivos, del porqué no incluiría este tipo de evaluaciones en su trabajo.

Resultado

Descripción	**Frecuencia**	
	Absoluta No.	**Relativa %**
Desconocimiento del Tema	1	100
Falta de Personal	0	0
Limitaciones de Tiempo	0	0
TOTAL	**1**	**100**

Análisis

Hay que tomar en cuenta que un menor porcentaje de los encuestados expresó que no incluirían dentro de su plan de trabajo este exámen por desconocer del tema. Una situación negativa para las unidades de auditoria interna por no contar con las herramientas y los conocimientos necesarios, provocando

así mayores costos para las empresas al no realizar la evaluación de la administración de riesgos.

Pregunta 6

Al realizar la evaluación de la administración de riesgos en tecnología de información, ¿Incluiría usted como parte de su trabajo las tres fases de la auditoria como lo requieren las Normas para le ejercicio profesional de la auditoria interna?.

Resultado

Descripción	**Frecuencia**	
	Absoluta No.	**Relativa %**
SI	4	100
NO	0	0
TOTAL	**4**	**100**

Análisis

El total de la población encuestada opinó que incluirían las tres fases de auditoria en la evaluación de la administración de riesgos. Este resultado es positivo ya que demuestra que las unidades de auditoria interna conocen y aplican las Normas para el ejercicio profesional de la auditoria interna en el desarrollo de su trabajo.

Pregunta 7

¿Qué normas técnicas aplican en el desarrollo de la auditoria interna?

Resultado

Descripción	Frecuencia			
	SI	NO	Absoluta No.	Relativa %
NEPAI´s – IIA	4	0	4	100
SAS – AICPA	2	2	4	50
NIA´s – IFAC	3	1	4	75
Informe COSO	1	3	4	25
Otros[3]	1	3	4	25

Análisis

Con respecto a las normas técnicas que aplican las unidades de auditoria interna el total de la población expresó que aplican las Normas para el ejercicio profesional de la auditoria interna, así mismo otras regulaciones como los son SAS, NIA´s y COSO entre otras, lo que exige al personal de las unidades de auditoria interna un nivel académico y conocimientos teóricos y técnicos actualizados para responder satisfactoriamente en el desarrollo de su trabajo.

[3] Security Exchanges Commisssion y Sarbanes & Oxley

Pregunta 8

En su organización, ¿A qué nivel jerárquico le informa Auditoria Interna?

Resultado

Descripción	Frecuencia			
	SI	NO	Absoluta	Relativa %
Junta Directiva	3	1	4	75
Presidencia	2	2	4	50
Gerencia General	1	3	4	25
D A F	1	3	4	25
Gerencia Financiera	1	3	4	25
Otros[4]	1	3	4	25

Análisis

El nivel jerárquico principal al cual le informa auditoria interna es la Junta Directiva, seguidamente la presidencia, esto con el propósito de discutir los hallazgos y las posibles soluciones para tomar las medidas correctivas necesarias. Este resultado es positivo ya que demuestra que las unidades de auditoria interna de las cadenas de supermercados de El salvador informan al nivel jerárquico adecuado.

Pregunta 9

¿Cuáles procesos de su trabajo son documentados, mediante papeles de trabajo?

Resultado

Descripción	Frecuencia			
	SI	NO	Absoluta	Relativa %
Planificación	3	1	4	75
Estudio Control Interno	4	0	4	100
Procedimientos	3	1	4	75
Obtención de evidencia	4	0	4	100
Revisión	4	0	4	100
Seguimiento	4	0	4	100

Análisis

Los resultados obtenidos denotan que los procesos de la auditoria interna mayor documentados mediante papeles de trabajo son el estudio de control interno, la obtención de evidencia y la planificación entre otros. Este resultado demuestra que las unidades de auditoria interna aplican las disposiciones establecidas en las Normas Internacionales de Auditoria.

[4] Comité de Auditoria

OBJETIVO

Comprobar la realidad bajo la cual operan las Unidades de Auditoría interna, en función de los nuevos riesgos, que producen los progresos tecnológicos y de negocios, que hacen de la información y la tecnología un factor crítico de éxito, para las cadenas de supermercados de El Salvador.

Pregunta 10

En el desarrollo de la auditoria interna, ¿diseñan programas específicos orientados a la evaluación de la administración de riesgos?.

Resultado

Descripción	Frecuencia	
	Absoluta No.	**Relativa %**
SI	3	75
NO	1	25
TOTAL	**4**	**100**

Análisis

La consideración en la auditoria de crear mecanismos para evaluar la administración de riesgos en términos globales sí

existe en la mayoría de las unidades de auditoria interna de las cadenas de supermercados a excepción de que exige dentro de ellas la ausencia de material relacionado a verificar la adecuada implementación de procedimientos que minimicen la ocurrencia de pérdidas informáticas, incidiendo en ello la falta de capacitación profesional que poseen los profesionales en el tema, necesarios para el diseño de esta clase de lineamientos.

Pregunta 11

De las siguientes técnicas de identificación de riesgos, ¿Cuáles se aplican en su organización?

Resultado

Descripción	Frecuencia			
	SI	NO	Absoluta No.	Relativa %
Analíticas	4	0	4	100
Diagramas	3	1	4	75
Organigramas	2	2	4	50
Políticas	4	0	4	100
Pérdidas pasadas	1	3	4	25
Entrevistas	4	0	4	100
Inspecciones	4	0	4	100

Análisis

Se puede apreciar que en la actualidad las cadenas de supermercados de El Salvador se encuentran utilizando las mayores técnicas para identificar los riesgos a los cuales están expuestos en el diario operacional, permitiendo evaluar las incertidumbres y las oportunidades que les generan, estableciendo de esta manera una plataforma que les permite una revisión a todos los eventos inciertos que podrían obstaculizar el logro de los objetivos de la organización.

Pregunta 12

En la ejecución de sus actividades, ¿Cuáles de los siguientes riesgos informáticos ha detectado?

Resultado

Descripción	Frecuencia			
	SI	NO	Absoluta No.	Relativa %
Integridad	2	2	4	50
Relación	1	3	4	25
Accesos	4	0	4	100
Utilidad	1	3	4	25
Infraestructura	1	3	4	25
Seguridad General	1	3	4	25
Otros[5]	1	3	4	25

[5] Sincronización de Sistemas

Análisis

La amplia utilización de los sistemas informáticos ha puesto en evidencia que el riesgo mayor detectado por parte de las unidades de auditoria interna es el de accesos lo cual contribuye a que personas desautorizadas conozcan información confidencial y que puedan utilizarlas para operaciones ilícitas, de igual forma y en un porcentaje medio observado se encuentra el de integridad enfocado a errores de la organización y exactitud de la información dentro del procesamiento de datos y en menor frecuencia de ocurrencia se encuentra la sincronización de sistemas como un nuevo factor de exposición a pérdidas. Estos y otros tipos de riesgos vinculados a la falta de una adecuada evaluación de la administración, contribuyen a que el profesional le de la importancia requerida dentro de su plan de trajo.

Pregunta 13

¿El proceso de auditoria del sistema de administración de riesgos, incluye la verificación respecto si los objetivos y políticas del sistema, cumplen con los criterios siguientes?.

Resultado

Descripción	Frecuencia			
	SI	NO	Absoluta No.	Relativa %
Niveles de exposición a riesgos	3	1	4	75
Relación de políticas con objetivos	4	0	4	100
Responsabilidad y autoridad	3	1	4	75
Eficiencia operativa	3	1	4	75

Análisis

El nivel de revisiones que actualmente mantiene la población encuestada refleja que si existe y en la totalidad de ellas una verificación de la relación de las políticas con los objetivos establecidos por la organización y en un menor nivel comprueban que cumplan con los criterios de exposición a riesgos, responsabilidad , autoridad y eficiencia operativa, lo que demuestra una conducta dinámica encaminada a la apertura de nuevas área de revisión.

Pregunta 14

¿La auditoria del sistema de administración de riesgos verifica, cuáles herramientas de identificación de riesgos se aplican?

Resultado

Descripción	Frecuencia			
	SI	NO	Absoluta No.	Relativa %
Cuestionarios de análisis	2	2	4	50
Listas de chequeo de exposición a riesgos	2	2	4	50
Catálogo de políticas de seguridad	2	2	4	50
Sistemas expertos en riesgos	1	3	4	25
Mapas de riesgos	1	3	4	25
Otros[6]	1	3	4	25

Análisis

La mitad de la población indica que entra las herramientas de mayor frecuencia utilizadas para identificar los riesgos se encuentran los cuestionarios, listas de chequeo de exposición a perdidas y el manejo de catálogos de políticas de seguridad, ya que mediante ellos se obtiene una imagen del nivel de amenazas a la cual esta inmersa la compañía, en tanto se puede notar que únicamente una unidad se encuentra aplicando lo nuevo en normativa de control interno como lo es inventarios de procesos

[6] Inventarios de procesos (COSO)

COSO, constituyendo una limitante la para demás que no se encuentran implantándolas dentro de sus procesos.

Pregunta 15

¿El sistema de administración de riesgos, posee canales de información y comunicación interna, que garantice el aprovisionamiento de información oportuna sobre nuevos riesgos tecnológicos, así como medios de registro históricos y estadísticos de los mismos?

Resultado

Descripción	Frecuencia	
	Absoluta No.	Relativa %
SI	3	75
NO	1	25
TOTAL	**4**	**100**

Análisis

Los canales de información y comunicación oportuna sobre la aparición de nuevos riesgos constituyen un elemento potencial para adoptar medidas preventivas y una habilidad para administrarlos según los resultados obtenidos por la mayoría de las unidades de auditoria interna de las cadenas de supermercados de El Salvador.

Pregunta 16

De los factores siguientes, ¿Cuáles generan riesgos al entorno informático en su organización?

Resultado

Descripción	Frecuencia				
	SI	NO	N/R	Absoluta No.	Relativa %
Presupuestos y revisión gerencial	0	2	2	4	0
Entorno de trabajo inadecuado	2	0	2	4	50
Usuarios finales inexpertos	1	1	2	4	25
Deficiencias del personal	0	2	2	4	0
Procesos de trabajo inadecuados	2	0	2	4	50
Deficiencias de planificación	0	2	2	4	0

Análisis

Se puede identificar claramente que la mitad de la población encuestada coincide en dos diferentes factores causantes de riesgos informáticos: El entorno de trabajo y los procesos inadecuados, los cuales están directamente relacionados a los

tipos de pérdida detectados por parte de las unidades de auditoria interna mencionadas en la pregunta número 12, por lo cual se esta conciente que las operaciones de la compañía están expuestas a tener cambios inestables e inherentes.

Pregunta 17

¿Cómo se ejecuta la estimación de la probabilidad y frecuencia de materialización de riesgos, en su programa de administración de riesgos?

Resultado

Descripción	Frecuencia			
	SI	NO	Absoluta No.	Relativa %
Expertos en informática	2	2	4	50
Técnica Delphi	0	4	4	0
Calibración por adjetivos	0	4	4	0
Otros[7]	2	2	4	50

Análisis

De los resultados obtenidos se comprobó que la mitad de las unidades de auditoria interna desconocen sobre la estimación de

la probabilidad y frecuencia de la materialización de los riesgos lo que indica que no se efectúa una buena administración de riesgos en cambio el resto de los encuestados manifestó que se auxilian de expertos para realizar este procedimiento.

Pregunta 18

¿Qué estrategias suelen utilizarse en el programa de administración de riesgos, para que éstos sean controlados?

Resultado

Descripción	Frecuencia			
	SI	NO	Absoluta No.	Relativa %
Evitar riesgos	0	4	4	0
Reducir riesgos	2	2	4	50
Planificar riesgos	4	0	4	100
Transferir riesgos	3	1	4	75
Otros	0	4	4	0

Análisis

La estrategia con mayor porcentaje de utilización para controlar los riegos es el de planificar riesgos, seguidamente de la

[7] Auditores Externos y Plan Anual de Riesgos Históricos

transferencia de riesgos y el de reducción de los mismos, como una agrupación en tres perspectivas distintas relacionadas al factor inherente de ocurrencia.

Pregunta 19

Debido a la naturaleza especializada del entorno informático y como parte del control de riesgos, ¿con qué frecuencia se contratan auditorias informáticas?.

Resultado

Descripción	Frecuencia			
	SI	NO	Absoluta No.	Relativa %
6 meses – 1 año	0	4	4	0
Más de 1 año – 2 años	3	1	4	75
Más de 2 años	0	4	4	0

Análisis

Dadas las circunstancias y los convenios establecidos entre las cadenas de supermercados de El Salvador y auditores informáticos externos, la mayoría de los encuestados afirmó que únicamente se contratan por un periodo de uno a dos años. Lo anterior

comprueba que las unidades de auditoria interna actualmente no tienen ninguna participación en esta clase de evaluaciones.

Pregunta 20

¿Existe un proceso de monitoreo o seguimiento, respecto de la incorporación oportuna de controles y medidas correctivas, como parte de la gestión de riesgos?.

Resultado

Descripción	Frecuencia	
	Absoluta No.	**Relativa %**
SI	4	100
NO	0	0
TOTAL	**4**	**100**

Análisis

El total de la población coincidió que dentro de la gestión de riesgos existen controles y medidas correctivas enfocadas a la minimización de pérdidas, las cuales son monitoreadas constantemente, lo cual indica que si existen los métodos idóneos para evaluar la operatividad de todas las operaciones informáticas.

Pregunta 21

¿Cuáles de los siguientes aspectos de la evaluación de la administración de riesgos considera necesarios para el desarrollo de su trabajo?

Resultado

Descripción	Frecuencia			
	SI	NO	Absoluta No.	Relativa %
Correlación de objetivos y políticas de riesgos	2	2	4	50
Identificación y evaluación de exposiciones a riesgos	3	1	4	75
Decisiones sobre pérdidas	1	3	4	25
Evaluación de medidas de gestión de riesgos implementadas	2	2	4	50
Recomendaciones y cambios en la gestión de riesgos	2	2	4	50

Análisis

La evaluación de la Administración de riesgos requiere que se consideren elementos esenciales para efectuarla, de los resultados obtenidos se observa que el factor de Identificación y evaluación de exposiciones a riesgo es el más útil para la

mayoría de las unidades de auditoria interna y en importancia de orden se menciona la correlación de objetivos y políticas de riesgos las cuales concuerdan con la medición, recomendación y cambios a toda la gestión de pérdidas.

Pregunta 22

¿Qué tipo de evidencia forma parte de sus papeles de trabajo relacionados con la evaluación de la administración de riesgos en tecnología de información?

Resultado

Descripción	Frecuencia			
	SI	NO	Absoluta No.	Relativa %
Papel	4	0	4	100
Cintas magnéticas	2	2	4	50
Discos compactos	4	0	4	100
Disquetes	3	1	4	75
Diapositivas	0	4	4	0
Películas	0	4	4	0

Otros: Correos electrónicos

Análisis

Se puede determinar mediante los resultados obtenidos que la totalidad de la población utilizan como tipo de evidencia el

papel y los discos compactos seguido de los disquetes y quedando en un menor rango las cintas magnéticas, todo ello con el propósito de sustentar el trabajo de auditoria desarrollado.

OBJETIVO

Justificar la utilidad de una guía de lineamientos que ayude a las Unidades de auditoría interna a entender y evaluar la administración de riesgos asociados con la tecnología de información.

Pregunta 23

¿Considera que es importante y útil, elaborar una guía que ayude a las unidades de auditoria interna de las cadenas de supermercado; a evaluar la administración de riesgos en tecnología de información?

Resultado

Descripción	**Frecuencia**	
	Absoluta No.	**Relativa %**
SI	4	100
NO	0	0
TOTAL	**4**	**100**

Análisis

La totalidad de las unidades de auditoria interna confirman que la existencia de una guía que contenga lineamientos orientados al adecuado desarrollo de la evaluación de la administración de riesgos en tecnología de información contribuirá a que el trabajo ejecutado este enfocado al fortalecimiento del control interno, a la solución de problemas y a la minimización de la ocurrencia de pérdidas informáticas, generándoles de esta manera eficiencia y calidad a sus actividades.

2.5 Diagnóstico de la investigación

Para muchas organizaciones, la información y la base tecnológica que la soporta, representa sus activos más valiosos.
Estas reconocen los beneficios potenciales que la tecnología proporciona, sin embargo, las organizaciones exitosas también deben comprender y administrar los riesgos asociados con la implementación de estos nuevos recursos.

Por lo tanto el profesional de la contaduría pública y en particular el que ejerce la auditoria interna, tiene ante sí la necesidad de contar con una guía que le provea de lineamientos para que sea capaz de evaluar la administración de riesgos en tecnología de información.

De acuerdo al análisis de los resultados obtenidos, las unidades de auditoria interna si poseen experiencia el la evaluación de riesgos de auditoria y reconocen que la planificación sobre riesgos es la mejor técnica contra posibles daños; esto mismo hace que la mayoría demuestren disposición en conocer e incluir en su plan de trabajo la revisión de la administración de riesgos en tecnología de información, reconociendo que no existe dentro de estas compañías capacitaciones continuas sobre aspectos relacionados a la temática planteada, lo cual contribuye al desconocimiento e incide en el desempeño de sus labores, creando estancamiento en el alcance y naturaleza de sus revisiones.

Los factores antes mencionados presentan limitaciones y a la vez un desafío para las unidades de auditoria interna; limitantes por lo que el resultado y calidad del trabajo hasta hoy desarrollado podría no estarse obteniendo de la mejor manera y desafío por que se convierte en una buena oportunidad y estimulo para que se mejoren sus competencias y se evalúe objetivamente la necesidad de implementar las medidas, políticas y estrategias necesarias para desempeñar con calidad y eficacia la actividad de auditoria interna consistentes con las metas y objetivos de la organización.

La aplicación de la normativa técnica por parte de las unidades de auditoria interna, actualmente se encuentra basada en las Normas para el ejercicio profesional de la auditoria interna (NEPAI´s), no obstante se reconoce la poca utilización del modelo internacional del Control Integral (COSO) el cuál provee un estándar fundamental para la evaluación del control interno e identificación de las mejores prácticas aplicables.

La adecuada verificación del cumplimiento de las políticas y objetivos del sistema de administración de pérdidas, la expectativa en la identificación de nuevos riesgos de control y amenazas externas, mediante la utilización de las diferentes herramientas y la adecuada canalización de la información y comunicación oportuna sobre la aparición de nuevos riesgos, proporciona un grado razonable de seguridad fomentado mediante el monitoreo y seguimiento de medidas correctivas y el desempeño de nuevas estrategias, estableciendo de esta manera una nueva plataforma de enfoque operacional.

Actualmente dentro de las cadenas de supermercados de El Salvador los riesgos informáticos resultan de deficiencias en el control sobre los accesos, incrementando de esta manera el potencial a la realización de actividades fraudulentas o a errores en aplicaciones específicas, lo cual ha sido de fácil

identificación por parte de las unidades de auditoria interna, pero mostrando poca habilidad para especificar los factores internos que agravan la existencia de riesgos en tecnología de Información.

La necesidad de contratación de personal experto y especializado en sistemas informáticos al momento de estimar los riesgos y su probabilidad de ocurrencia, es muy evidente el las Cadenas de Supermercados; constituyéndose este factor en un fuerte reto para los auditores internos en adquirir adiestramiento y en tomar la iniciativa en la realización de este tipo de evaluaciones, minimizándoles a las entidades la dependencia de esas fuentes.

Un aspecto que sobresale de lo anterior, es el surgimiento de una brecha importante, entre el trabajo de los auditores internos y los responsables de informática; ya que en muchos casos los primeros únicamente son usuarios limitados de los recursos tecnológicos, lo que indica una incertidumbre sobre la adecuada administración de riesgos en tecnología de información.

La vinculación entre la periodicidad de contratación de auditoria informáticas, con la implementación de opciones para el tratamiento de riesgos, representa costos adicionales para

las cadenas de supermercados, por lo que es de resaltar en este punto que para minimizar estas erogaciones se podría recurrir a los recursos internos que se poseen, ampliando el enfoque al trabajo del auditor interno, ya que su labor esta orientado al fortalecimiento de la estructura del control interno y a la reducción de riesgos informáticos.

Considerando lo anterior, la totalidad de las unidades en auditoria interna de las cadenas de supermercados de E Salvador consideran conveniente que exista una guía que sea utilizada para efectuar adecuadamente la evaluación de la administración de riesgos en Tecnología de Información, lo que debería plasmar los procedimientos generales y específicos a seguir, los cuales vendrían a ampliar y fortalecer los procedimientos que actualmente se utilizan.

CAPITULO III

3.1 Consideraciones Generales

En el marco del desarrollo mundial del comercio, la importancia de la información y la tecnología que la soporta es ampliamente aceptada, incluso han pasado a representar sus activos mas valiosos.

Las organizaciones se están reestructurando a fin de modernizar sus operaciones y aprovechar los avances en tecnologías de información (TI), a fin de mejorar su posición competitiva.

La alta velocidad con la cual se procesan las transacciones, el comercio electrónico, los sistemas de información, las redes de telecomunicaciones, el procesamiento e intercambio de datos, el Internet y en general, el Ciberespacio, donde la información viaja sin restricciones de tiempo, distancia y velocidad, son aspectos característicos de las TI.

Sin embargo, la Administración Superior, debe apreciar y entender que las TI, no solo generan beneficios y oportunidades, traen aparejados riesgos y limitantes, que deben ser conocidos y

administrados, para proporcionar una dirección efectiva, controles adecuados y un entorno de TI seguro.

La tecnología que utilizan las cadenas de supermercados en El Salvador, para el tratamiento de la información, ha generado la necesidad que se Evalúe la Administración de Riesgos en TI.

Por ese motivo, se ha elaborado una guía que sirva de base a los auditores internos a desarrollar esta evaluación, cumpliendo así su propósito Ayudar a la Organización a cumplir sus objetivos, midiendo los procesos de gestión de riesgos, control y gobierno.

3.2 Introducción de la Propuesta

El diseño de la propuesta está desarrollado según le enfoque convencional de la Auditoria, de acuerdo con las Normas para el Ejercicio Profesional de la Auditoria Interna, con la diferencia que no es un examen sobre la corrección de cuentas contables; se enfoca en el trabajo de las Unidades de Auditoria Interna de las Cadenas de Supermercado de El Salvador, en la Evaluación de la Administración de Riesgos en Tecnología de Información.

La primera etapa consiste en describir la planeación, estableciéndose los objetivos, alcance, naturaleza y componentes

sujetos de revisión a riesgos; derivando el diseño de lineamientos encaminados a verificar la acertada Administración de Riesgos.

La segunda etapa detalla los lineamientos aportados para la ejecución de la auditoria, con la aplicación de tales lineamientos, se obtendrá evidencia suficiente para respaldar sus conclusiones y resultados, sobre la Administración de Riesgos aplicada por la Organización.

En la tercera etapa se comenta sobre la comunicación de los resultados a través del informe, detallando los hallazgos sobre situaciones que afectan e impiden a la Organización alcanzar sus objetivos y presentando las recomendaciones pertinentes.

Se considera que el documento es en conjunto, una base adecuada para la ejecución de este tipo de trabajos.

3.3 Propuesta de lineamientos para la evaluación de la administración de riesgos en tecnología de información por parte de las unidades de auditoria interna de las cadenas de supermercados de el salvador.

Un proceso de evaluación de tecnología de información que integre las necesidades de las cadenas de supermercados en El Salvador, conlleva a los auditores internos a aplicar lineamientos de auditoria y la incorporación de los elementos funcionales del proceso de administración de riesgos.

3.3.1 Planeación de la evaluación de la administración de riesgos en tecnología de información.

Los riesgos de la incorporación de tecnología de información, en las operaciones normales de las cadenas de supermercados en El Salvador, se incrementa principalmente porque no se han implementado las medidas que ayuden a minimizarlos; por lo que, una adecuada planeación por parte de las unidades de auditoria interna para examinar esta área requiere del establecimiento de objetivos, del alcance y de la identificación de las áreas a examinar. Es decir, el diseño de instrucciones específicas para la ejecución del trabajo.

3.3.1.1 Establecimiento de los Objetivos de la Evaluación, Alcance y Naturaleza del trabajo a efectuar.

Dada la importancia de las operaciones y la administración efectiva de la información generada a través del uso de las Tecnologías de Información, la función de las unidades de Auditoria Interna de las Cadenas de Supermercados de El Salvador establecen como objetivos para la evaluación los siguientes:

Objetivo General

Valorar si las fases de determinación de objetivos, identificación, evaluación, decisión (minimización, retención y transferencia) y control de los riesgos a los cuales se expone la organización, son ejecutadas por la administración; evitando la materialización de riesgos y amenazas, que pongan en peligro los objetivos, la marcha y existencia del negocio.

Objetivos Específicos

- Evaluar si la estructura organizacional está formalmente definida (si posee organigrama, objetivos, políticas, manuales de procedimientos, descripción de puestos, presupuesto), también, si los procesos de selección, capacitación y

promoción de personal, están en consonancia con las necesidades de la función de administración de riesgos.

- Determinar si los procedimientos, técnicas o herramientas aplicadas para la identificación de riesgos, son efectivos, eficaces y económicos.

- Establecer si los procedimientos, técnicas o herramientas aplicadas para la evaluación de riesgos, permiten medir o cuantificar la magnitud de las pérdidas o la probabilidad de que ocurran, de manera efectiva.

- Comprobar si los procedimientos, técnicas o herramientas aplicadas para las distintas opciones de control de riesgos, incorporan los factores de costo, servicio y protección para la organización.

- Verificar si los procedimientos, técnicas o herramientas aplicadas para el control de riesgos, son efectivas.

3.3.1.2 Alcance y Naturaleza de la evaluación

El alcance de la evaluación por parte de las Unidades de Auditoria Interna de las Cadenas de Supermercados de El Salvador

está de acuerdo con las Normas para el ejercicio Profesional de la auditoria interna; evaluando los controles implementados para administrar los riesgos tecnológicos, el proceso funcional de la Administración de riesgos y el grado de seguridad que genera el sistema, para poder emitir el informe requerido, que expresará los diferentes resultados obtenidos de la evaluación.

Durante la etapa de Planificación del Trabajo, las normas requieren que documenten los procedimientos de auditoria a aplicar. Así como establecer el alcance y grado de las pruebas. También, deben fijarse los requisitos del trabajo, los periodos a cubrir y fechas estimadas de terminación.

Con relación a la evaluación de riesgos en tecnología de información, el auditor interno debe fijar en su plan de trabajo, los periodos o fechas en los cuales incorporará los lineamientos sugeridos. Cabe mencionar, que procedimientos relativos a evaluación de riesgos tecnológicos, pueden ser aplicados varias veces al año; debido a que cada vez surgen nuevos riesgos, de manera inherente al avance de la tecnología.

No se evalúa el cumplimiento de leyes, códigos y/o reglamentos aplicables, ya que en la actualidad en El Salvador no existe ninguna normativa legal, que regule la implantación del proceso

de la administración de riesgos en tecnología de información, para este tipo de compañías.

El alcance del trabajo de Auditoria Interna, que se describe a continuación, sirve de base para la evaluación del control, el proceso funcional, la seguridad, la elaboración de los lineamientos de auditoría para el desempeño del trabajo de campo, la supervisión y la elaboración del informe, en todo momento y durante la realización de este trabajo se observa la objetividad y el debido cuidado profesional.

El alcance de la Evaluación contiene como mínimo el trabajo siguiente:

- Entendimiento de las diferentes etapas de la Administración de riesgos
- Evaluación de los controles internos implementados para que el sistema detecte las exposiciones a riesgos en el uso de las tecnologías de información.
- Pruebas de cumplimiento del proceso de la Administración de riesgos en tecnología de información.
- Análisis de los mayores riesgos potenciales identificados que afectan las operaciones de la compañía.
- Selección de procesos que requieren mayor atención por parte de la Junta Directiva de la entidad evaluada.

- Concientización a la Organización de la importancia de las evaluaciones periódicas a los riesgos informáticos.
- Determinación de los principales impactos en las operaciones financieras de la compañía.
- Diseño de lineamientos de auditoría para la evaluación de la Administración de riesgos en tecnología de información.
- Documentación del trabajo desarrollado dejando evidencia suficiente, confiable, relevante y útil de la auditoría.
- Presentación de observaciones de auditoría.
- Documentación de las acciones tomadas por la entidad para superar las observaciones informadas por la unidad de auditoría interna.

La Naturaleza del trabajo de las unidades de auditoría interna está en evaluar y contribuir a la mejora de los procesos de la Administración de Riesgos en tecnología de información, asistiendo a la Organización en la identificación y evaluación de las exposiciones significativas a los riesgos, supervisando y evaluando la eficacia del sistema.

El área de dirección para el diseño de los procedimientos de evaluación diseñados por el auditor interno para evaluar la administración de riesgos en tecnología de información, se limita únicamente a la parte externa del computador y no a la

parte lógica de los sistemas ya que para ello se necesita la ayuda de un experto con habilidades especializadas, de acuerdo con la sección 620 de las Normas Internacionales de Auditoria. Sin embargo, el auditor interno debería evaluar lo apropiado del trabajo del experto.

3.3.1.3 Identificación de las áreas de evaluación.

3.3.1.3.1 Controles para administrar riesgos tecnológicos.

El adoptar una estructura de Administración de riesgos tecnológicos dentro de las cadenas de supermercados de El Salvador representa un cambio completo en la cultura y estructura de la Organización, por lo que las unidades de auditoria interna evalúan:

1. El Compromiso de la Junta Directiva

Verificar el acuerdo de la máxima autoridad y el apoyo a través del compromiso de sus recursos tanto económicos como humanos y especialmente a través de la transmisión de mensajes hacia toda la organización.

2. El cambio en el proceso Administrativo

Comprobar que exista un plan de implementación del proceso que facilite el cambio de la condición actual a la condición deseada en el futuro.

3. Asignación de Responsabilidades.

Determinar si la máxima autoridad de la compañía posee la política y estructura de asignar en el desarrollo de trabajos especiales aquellas personas que en su conjunto posean los conocimientos, las experiencias y disciplina necesarias para conducir apropiadamente la auditoria.

3.3.1.3.2 Proceso funcional de la administración de riesgos.

Es la ejecución de los lineamientos planteados dentro de la planificación de la auditoria, para verificar que las operaciones dentro del sistema de información, se están desarrollando de acuerdo a lo establecido.

3.3.1.3.3 Evaluación de la Seguridad de la administración de riesgos en tecnología de información

Una adecuada Administración de riesgos, otorga un nivel de seguridad aceptable para la prestación de servicios d4e información; por lo que las unidades de auditoria interna, como elemento del fortalecimiento de la estructura de control interno efectúan revisiones del proceso de protección y preservación de la información relacionándolos con la calidad y eficacia del conjunto de acciones y medidas adoptadas para controlar los peligros informáticos, por lo que las unidades:

- Verifican si el nivel de la aplicación del proceso de la Administración de riesgos adecuado.
- Detectan cualquier desviación de las actividades a realizar y determinan las posibles deficiencias o carencias de toda la gestión de pérdidas.
- Mantienen un adecuado monitoreo de los riesgos identificados, controlados y transferidos.

3.3.1.4 Educación Bibliográfica continuada

El auditor interno se auxilia de toda información posible que le sirve de apoyo para cumplir con los objetivos del trabajo.

3.3.1.5 Duración de la evaluación y asignación de recursos

Dentro de la planeación el auditor interno estima el tiempo que llevará la realización del exámen de la administración de riesgos para lo cual programa el número de horas y asigna el personal idóneo que participará en la revisión determina los recursos materiales y tecnológicos (software) de los cuales de auxilia el auditor en el desarrollo de este trabajo.

3.3.1.6 Diseño de Lineamientos

Este trabajo considera que un Sistema de Administración de Riesgos, posee cinco etapas: Determinación de Objetivos, Identificación, Evaluación, Decisión (Alternativas y Tratamiento) y Control de Riesgos.

Los lineamientos que aplicará el auditor interno, están agrupados en las cinco etapas mencionadas anteriormente:

3.3.1.6.1 Determinación de objetivos organizacionales

1. Comprobar mediante examen documental, la existencia de un Manual de Administración de Riesgos. Cerciorarse que posee

Objetivos, Políticas de Seguridad y Procedimientos Formales y por Escrito.

2. Investigar sobre los cambios mas recientes en la Organización, sus Operaciones y Sistemas de Información. Así como determinar cuales son sus activos de información más relevantes.

3. Verificar las características de la Estructura Organizativa, Organigramas y Descripciones de Puestos, los cuales debe estar Actualizados, con una imprescindible delimitación de responsabilidades y atribuciones específicas, tanto para Propietarios, Depositarios y Usuarios de los recursos de Tecnología de Información.

4. Revisar los planes de entrenamiento y capacitación de usuarios, sean programados y ejecutados regularmente, también si fueron supervisados oportunamente. Investigar incentivos y compensaciones por buen desempeño.

5. Determinar si los presupuestos de la Organización, incluyen erogaciones relacionadas, con la administración de riesgos; tales como: primas de seguro para el equipo informático, contratación de servicios informáticos, contratación de

especialistas, compras de software antivirus, licencias de programas, entre otros.

6. Inspeccionar los registros auditables (listas de control, bitácoras, secuencias de acontecimientos) que poseen los sistemas de información, con relación a: Intentos de accesos a recursos TI, Violaciones de Acceso, Alertas de Virus y Códigos Malignos (Gusanos, Caballos de Troya, Bombas Lógicas, Cáncer de Rutinas), Hackers, entre otros.

El éxito en la aplicación de éstos lineamientos dependerá de la adecuada aplicación de las técnicas de auditoria, ya sea: Observación, Inspección física, Investigación, Examen documental, Certificaciones o Confirmaciones.

3.3.1.6.2 Identificación de riesgos

1. Compruebe mediante la existencia de políticas, procedimientos, chequeos e instrucciones específicas, si la organización ha identificado riesgos en los procesos siguientes:

    - Conexiones a Internet y uso de Web Site
    - Conexiones a Redes Virtuales Privadas
    - Uso de Tecnología Inalámbrica

- Acceso Público
- Transferencia de Activos – E-Mail
- Intercambio Electrónico de Datos
- Procesamiento y Almacenamiento de Datos
- Desarrollo de Aplicaciones y Hosting para E-Commerce
- Servicios de respaldo y recuperación de información.

2. Investigar los hallazgos derivados de revisiones efectuadas por Consultores, Auditores de Calidad y otras surgidas por Investigaciones Específicas de la Gerencia, mediante los cuales se hayan identificado Riesgos en Tecnología de Información.

3. Verificar si la Gerencia ha efectuado, por lo menos una vez al año, un Diagnóstico de Seguridad Informática, revisar el Informe de Resultados y detallar las características de éste trabajo:

    - Según el ámbito de la revisión puede ser por Función o Total (a toda la organización)
    - Según el alcance y equipo revisor, puede ser Auto Evaluación, Revisión (puede ser externo) o Auditoria (expertos ajenos a la empresa).

4. Determinar si la Gerencia ha levantado un Inventario de Aplicaciones por Función (por lo menos una vez al año) y ha Clasificado sus Activos de Información (Uso interno, confidencial, secreto o reservado); identificándolos con sus correspondientes Riesgos de divulgación y renovando las medidas de protección y uso de la información.

5. Efectuar lectura crítica de Contratos por Servicios de Tecnología de Información Proveídos por Terceros (desarrollo de aplicaciones, mantenimiento, hosting; tarjetas de crédito, centros de llamadas, Outsourcing) y verificar (según la naturaleza del servicio) que se hayan establecido de manera clara y precisa, los aspectos siguientes:
   - Responsabilidad de los datos, aplicaciones y confidencialidad de la información.
   - Responsabilidad del soporte técnico, control de accesos y sistemas operativos.
   - Monitoreo de activos de información y datos.
   - Especificación sobre la propiedad de la información.
   - Cláusula que garantice el derecho a efectuar auditorias de cumplimiento de contratos y el correspondiente acceso.
   - Proceso de negociación, revisión, cambios y finiquito de contrato.

6. Elaborar extracto de Pólizas de Seguro, enfatizando la cobertura de los riesgos asegurados e identificados por la Gerencia, tales como:

   - Servidores, Mainframe, Terminales
   - Equipos portátiles y equipos auxiliares (UPS)
   - Activos de información almacenados centros alternativos
   - Lucro cesante por interrupción de operaciones

3.3.1.6.3 Evaluación de riesgos

1. Cerciorarse que los sistemas operativos y software son chequeados regularmente por los fabricantes o proveedores, ejecutándose las actualizaciones disponibles.
2. Comprobar que los software de antivirus instalados en los puestos de trabajo, están siendo actualizados mediante suscripción con las compañías proveedoras.

3. Verificar que los medios de resguardo (Back up), son programados para su ejecución de manera regular, en los servidores, equipos principales y terminales; revisar el almacenamiento de las copias de seguridad en locales propios, centros alternativos y complementarios.

4. Chequear si la Gerencia ha obtenido Certificaciones de Seguridad de sus Conexiones Externas y/o Recertificaciones Anuales.

5. Revisar los informes de los equipos revisores, cuando la organización haya sufrido suspensiones temporales o definitivas de sus conexiones externas e investigar la gestión para su reactivación.

6. Inquirir a la Gerencia sobre la existencia de factores de riesgo y su monitoreo, tales como:

   - Insatisfacción / descontento de empleados.
   - Despidos potenciales por reestructuración.
   - Existencia de activos fácilmente susceptibles de apropiación o malversación.
   - Actitud hostil (desleal) de la competencia.
   - Sofisticación y complejidad técnica de los sistemas de información.

7. Indagar si se aplican procesos de comparación por puntos de referencia (Benchmarking), con algunas compañías internacionales de similar naturaleza, respecto del uso y

explotación de tecnología informática, para asegurar que se alcanzan los objetivos organizacionales.

8. Verificar la ejecución de pruebas de integridad de sistemas, mediante expertos o especialistas; por lo menos una vez al año.

3.3.1.6.4 Decisión (alternativas y tratamiento) de riesgos

1. Corroborar que las decisiones de la Gerencia para la administración de riesgos, estén basadas en la aplicación de procedimientos de selección del software del sistema, de instalación, de mantenimiento, seguridad y control que conlleven a alcanzar los objetivos de la organización.
2. Evaluar si las decisiones de la Gerencia, evidencian la aplicación de las técnicas de administración de riesgos siguientes:

   - Evitar
   - Reducir
   - Conservar o Asumir
   - Transferir o Diversificar

3. Valorar la aplicación del principio de segregación de deberes y tareas incompatibles, y la revisión de la gerencia a las técnicas de control.

3.3.1.6.5 Control de riesgos

1. Revise el Plan de Contingencia y Recuperación de Desastres de la Organización y verifique su contenido con relación a:

    - Identificaciones preliminares, aplicaciones y activos críticos, sistemas esenciales y/o prioritarios, centros alternativos y revisiones periódicas.
    - Almacenamiento en centro alternativo, propio y complementario de las copias de respaldo de los datos
    - Ejecución de pruebas de continuidad y recuperación del centro siniestrado.

2. Verificar la aplicación de medidas de seguridad y protección lógicas a los activos de información, tales como:

    - Perfil e Identificación de Usuarios
    - Autentificación de Usuarios
    - Contraseñas

- Firmas electrónicas
- Cifrado de Información
- Sistemas de filtro de paquetes (Cortafuegos)

3. Completar el examen de las medidas de seguridad y protección lógicas a los activos de información, con los aspectos siguientes:

    - Disposición adecuada de dispositivos de salida fuera de uso.
    - Acceso de los empleados a la información, en función de su puesto de trabajo.
    - Eliminación oportuna de usuarios inactivos o retirados; revalidación periódica de usuarios.
    - Los accesos otorgados para la recepción de servicios de mantenimiento y soporte deben ser registrados y monitoreados oportunamente.
    - Registros de accesos a sistemas en horarios inusuales.

4. Inspeccionar la aplicación de medidas de seguridad y protección física a los activos de información, tales como:

    - Uso de cerrojos y llaves.

- Fichas o tarjetas inteligentes.
- Dispositivos biométricos (huellas dactilares, patrones de voz, firmas digitales, escáner de retinas).

5. Evaluar la seguridad y protección física, mediante los parámetros siguientes:

   - Distribución de Áreas de Acceso Limitado y Acceso Restringido.
   - Sistemas de extinción de incendios.
   - Condición física de los suministros auxiliares, energía eléctrica y aire acondicionado.

6. Comprobar si el programa de control, incorpora los componentes siguientes:

   - Soporte de Especialistas en Informática.
   - Auditorias Informáticas.
   - Consultoría para la gestión de riesgos.
   - Aplicación de Sistemas Expertos.

7. Revisar si la organización aplica Intercambio electrónico de datos, entre sus sistemas de información, para ejecutar transacciones comerciales y verificar:

    - Acuerdos contractuales, que establezcan derechos y obligaciones específicas a los participantes y definan los requisitos documentales de las transacciones
    - Definición de los medios técnicos que intervendrán
    - Criterios de aceptación o rechazo de transacciones
    - Medios de protección de mensajes, cifrado de contenido, comprobantes de alteración, firmas digitales, autenticación e incluso intervención de terceros para certificar el origen.

3.3.2 Ejecución de la evaluación de la administración de riesgos en tecnología de información.

Para la realización de la ejecución de la auditoría el auditor interno deberá de dejar constancia de todos los procedimientos efectuados en el exámen de la administración de riesgos en tecnología de información a través de los papeles de trabajo

como lo son: Cédulas, Matriz de riesgos, Cuestionarios de Control Interno, etc.

3.3.3 Comunicación de los resultados por parte del auditor interno en la Evaluación de la Administración de riesgos en Tecnología de Información.

La comunicación de los resultados es el producto final del examen realizado y frecuentemente es lo único que conocen los altos funcionarios de la compañía, respecto al trabajo desempeñado por el auditor; considerando reportar los asuntos y/o condiciones que podrían afectar de forma negativa, la capacidad de la entidad para: identificar, evaluar y controlar los riesgos informáticos antes que estos afecten los sistemas.

La mejor forma de diseñar las comunicaciones dirigidas a la Administración de las cadenas de supermercados en El Salvador, es el de advertir el incumplimiento de establecer un adecuado sistema de administración de riesgos, las medidas que necesitan implementar para superarlos y el adecuado monitoreo en el cumplimiento de esas medidas, por lo tanto, la comunicación de los resultados incluye tres áreas:

a) Objetivos del trabajo desarrollado

- Comunicar a la Junta Directiva los resultados de la evaluación efectuada al sistema de administración de riesgos tecnológicos, implementando controles que cubran aquellas situaciones de mayor riesgos y relevancia.
- Servir de apoyo en la toma de decisiones.

b) Alcance de la auditoria

El alcance de la evaluación viene dado por las etapas de la Administración de riesgos detallada a continuación:

- Determinación de los objetivos organizacionales.
- Identificación de los riesgos.
- Evaluación de los riesgos
- Decisión (Alternativas y Tratamiento)
- Control de riesgos.

c) Análisis de la situación

En esta parte se detalla la situación actual y real de la función de la Administración de riesgos que incluye como mínimo lo siguiente:

- Descripción de la condición o amenaza que se observó, durante la examen efectuado al sistema de administración de riesgos tecnológicos y que necesita ser solventada.
- Las posibles causas que le dieron surgimiento.
- Los efectos que genera el riesgo detectado, detallando el impacto económico que ocasiona.
- La correspondiente solución o recomendación que el auditor interno realiza en base a los criterios técnicos obtenidos durante su evaluación.

Proceso de seguimiento, el cual incluye un monitoreo de los planes de acción implementados para minimizar las amenazas o exposiciones a riegos detectados dentro del proceso de administración de riesgos en tecnología de información.

CAPITULO IV

4 CONCLUSIONES Y RECOMENDACIONES

Como resultado de la investigación de campo y con los datos recopilados y analizados, se obtuvieron las conclusiones concernientes al diseño de lineamientos para la evaluación de la administración de riesgos en tecnología de información, como una herramienta para las Unidades de Auditoria Interna de las Cadenas de Supermercado de El Salvador. Con la finalidad de apoyar el trabajo de los auditores internos, de acuerdo a los avances de los sistemas de información y tecnología relacionada. También se desarrollan las recomendaciones derivadas de la realización de este trabajo y su correspondiente análisis.

4.1 CONCLUSIONES

Las Unidades de Auditoria Interna poseen un grado de desarrollo técnico acorde a sus responsabilidades; no obstante, no han evolucionado hacia un enfoque proactivo en materia de evaluación de riesgos y aún mas específicamente, en tecnología de información.

Las Cadenas de Supermercados cuentan con recursos de tecnología de información, para el manejo de sus operaciones, así como herramientas de comunicación y una estructura organizacional adecuada, que les permite formalizar un plan de administración de riesgos. Le corresponde a las Unidades de Auditoría Interna, modificar el perfil de usuario que hasta la fecha posea y adoptar una actitud que le permita estar en consonancia, con los objetivos de la organización a la que pertenece.

Las Unidades de Auditoria Interna carecen de bases de conocimiento y adiestramiento especializado en tecnología de información y riesgos de negocio, que les permitan mantenerse actualizados con los cambios permanentes en el ambiente económico.

La función de auditoría interna y la de informática, puede ser una excelente combinación de esfuerzos y recursos, para la protección y control de activos de la organización. No obstante, es evidente la falta de trabajo combinado y de entendimientos, lo cual repercute y limita la proyección de beneficios de la tecnología de información, hacia la entidad.

El factor de estimación de riesgos, no constituye un elemento tan importante para la Administración; esto hace que ante la

ocurrencia de daños y pérdidas, se adopte una actitud reactiva, sin considerar que la prevención es la mejor medida para evitar perjuicios que puedan poner en peligro, inclusive la capacidad de subsistir de la organización.

4.2 RECOMENDACIONES

Las Unidades de Auditoria Interna deben en el corto o mediano plazo, reformular su gestión y asumir nuevos desafíos, trabajando para generar valor agregado a la organización, con mejoras y optimizaciones de procesos, con una visión hacia la evaluación de la administración de riesgos en tecnología de información.

La creciente dependencia de la información y los sistemas, la progresiva vulnerabilidad, la amplia gama de amenazas tecnológicas y el costo de las inversiones en tecnología de información; recalcan la necesidad de que los Auditores Internos se mantengan actualizados para entender los cambios y riesgos asociados.

Un documento que contenga lineamientos de auditoria, que sirva de guía a las Unidades de Auditoria Interna, para evaluar la administración de riesgos; contribuirá y apoyará con las

responsabilidades de la Administración Superior, relativas a la protección de uno de los activos mas valiosos y críticos para el éxito de las empresas, la Información y la Tecnología que la soporta.

BIBLIOGRAFIA

AIC Asociación Interamericana de Contabilidad, XXV Conferencia Interamericana de Contabilidad, Panamá 2003. Trabajos Técnicos Interamericanos y Nacionales.

COSO Comité de Organizaciones Auspiciantes de la Comisión Treadway, Estructura Conceptual del Control Interno, traducido por Coopers & Lybrand, 1997.

IIA Instituto de Auditores Internos, Normas para el Ejercicio Profesional de la Auditoria Interna y Consejos para la Práctica, 2002. www.theiia.org

IIA Instituto de Auditores Internos, Sistemas de Aseguramiento y Control SAC, 2002. www.theiia.org/itaudit

ISACA Asociación de Auditoria y Control de Sistemas de Información, Resumen Ejecutivo, Marco Referencial y Objetivos de Control de COBIT Gobierno, Control y Auditoria de la Información y Tecnologías Relacionadas, Segunda Edición, 1998

IT GI Instituto para el Gobierno de Tecnología de Información, Gobierno de Seguridad de Información: Guía para Juntas Directivas y Administradores Ejecutivos, 2001. www.ITgovernance.org

Janet L. Colberty y Paul L. Bowen, Una comparación de Controles Internos: COBIT, SAC, COSO y SAS 55/78.

SEDISI Asociación Española de Empresas de Tecnología de la Información, Guía de Seguridad Informática, 2002. www.sedisi.es

Serrano Cinca C., Riesgos y Seguridad en los Sistemas de Información, 2003. www.5campus.org

ANEXO

ANEXO

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECONOMICAS
ESCUELA DE CONTADURIA PUBLICA

San Salvador, Septiembre de 2004

Atn. Director Ejecutivo de Auditoria Interna
Presente.

Como parte del proceso de formación profesional, ejecutado por la Universidad de El Salvador y su Facultad de Ciencias Económicas; y según Reglamento de Graduación, se exige que los estudiantes egresados en la carrera de Contaduría Pública, presenten un Trabajo de Graduación para optar al grado de licenciatura.

Dicho Trabajo de Graduación, debe cumplir y aportar conocimiento técnico sobre una de las necesidades del sector profesional contable.

En ese sentido, los suscritos preparan su Trabajo de Graduación titulado **"El auditor interno ante la evaluación de la administración de riesgos en tecnología de información en las cadenas de supermercados de El Salvador"**, el cual pretende ofrecer un aporte, en el tema de la Administración de Riesgos Empresariales.

Reconocemos que el Código de Ética del Instituto de Auditores Internos, exige que los profesionales de la auditoria interna, sean prudentes en el uso de la información que adquieren en el transcurso de su trabajo; y que no utilizarán dicha información en detrimento de la organización para la cual prestan sus servicios.

El grupo de trabajo, solicita de ustedes información que entendemos es confidencial; no obstante, queremos garantizar bajo palabra de honor, que la información será manejada con estricta seguridad y únicamente para los fines antes mencionados.

Por su valiosa colaboración y por el tiempo que dedicará al responder objetivamente a las preguntas, le agradecemos sinceramente.

¡Por el engrandecimiento de la profesión contable¡

Atentamente,

Carlos Geovani Escalante Deysi Doredith Cerna
Clara Emperatriz Guzmán

Indicación: Marque con una equis, la opción que estime correcta.

1. Como parte de su experiencia profesional en auditoria interna ¿Ha ejecutado evaluaciones de la administración de riesgos?

   SI NO

2. Considera que para evaluar la administración de riesgos en tecnología de información el auditor interno necesita de conocimientos técnicos adicionales a la formación académica?

   SI NO

Comente,_____

3. Existe por parte de la compañía un programa de capacitación continua para el personal de auditoria interna sobre aspectos relacionados a la evaluación de riesgos ó tecnologías de información?

   SI NO

Si su respuesta es negativa, ¿Qué factores dificultan la existencia de un programa de capacitación?

- Falta de recursos
- Limitaciones de tiempo
- No se consideran necesarios
- Otros, Especifique _____

4. ¿Tiene conocimiento si en su compañía, el departamento de informática realiza la actividad de administración de riesgos en tecnología de información; ya sea de una manera formal o informal?

   SI NO

5. Si la compañía no tiene implementado dentro de sus operaciones la evaluación de la administración de Riesgos en Tecnología de información, ¿Incluiría usted dentro de su plan de trabajo el efectuar este tipo de evaluaciones?

   SI NO

Si su respuesta a la pregunta anterior fue negativa, señale los motivos del porqué no incluiría este tipo de evaluaciones en su trabajo:

- Desconocimiento del tema
- Falta de personal
- Limitaciones de tiempo
- Todas las anteriores
- Otras, especifique._____

6. Al realizar la evaluación de la administración de riesgos en Tecnología de Información, ¿Incluiría usted como parte de su trabajo las tres fases de la auditoria como lo requieren las Normas para el ejercicio profesional de la auditoria interna?

   SI NO

7. ¿Qué normas técnicas aplican en el desarrollo de la auditoria interna?

   - Normas para el ejercicio profesional de la Auditoria Interna
   - Declaraciones sobre Normas de Auditoria (SAS)
   - Normas Internacionales de Auditoria (NIA)
   - Informe COSO
   - Otros, Especifique:_____

8. En su Organización, ¿A qué nivel jerárquico le informa Auditoria Interna?

   - Junta Directiva
   - Presidencia
   - Gerencia General
   - Dirección de Administración y finanzas
   - Gerencia Financiera
   - Otros, Especifique_____

9. ¿Cuáles procesos de su trabajo son documentados, mediante papeles de trabajo?

   - Planificación
   - Examen y evaluación de control interno
   - Procedimientos aplicados
   - Información obtenida y conclusiones alcanzadas
   - La revisión
   - El Seguimiento
   - Todos los anteriores

10. En el desarrollo de la auditoria interna, diseñan programas específicos orientados a la evaluación de la administración de riesgos?

SI NO

11. De las siguientes técnicas de identificación de riesgos, ¿cuáles se aplican en su organización?.

- Análisis de informes financieros
- Diagramas de flujo de operaciones
- Todos los anteriores
- Organigramas
- Políticas
- Reportes de pérdidas pasadas
- Entrevistas
- Inspecciones

12. En la ejecución de sus actividades, ¿Cuáles de los siguientes riesgos informáticos ha detectado?

- Riesgos de Integridad
- Riesgos de Relación
- Riesgos de Accesos
- Riesgos de Utilidad
- Riesgos en la Infraestructura
- Riesgos de Seguridad General
- Todos los anteriores
- Otros, especifique:_____

13. ¿El proceso de auditoria del sistema de administración de riesgos, incluye la verificación respecto si los objetivos y políticas del sistema, cumplen con los criterios siguientes?

- Evaluación de Niveles máximos de exposición a riesgos
- Cumplimiento y consistencia de las políticas con los objetivos del programa
- Delimitación de responsabilidad y autoridad del equipo de administración de riesgos
- Conservación de eficiencia operativa
- Todos los anteriores

14. ¿La auditoria del sistema de administración de riesgos verifica, cuáles herramientas de identificación de riesgos se aplican?

- Cuestionarios de análisis de riesgos
- Listas de chequeo de exposición a riesgos
- Catálogo de políticas de seguridad
- Sistemas expertos en administración de riesgos
- Mapas de riesgos
- Todas las anteriores
- Ninguna de las anteriores
- Otros, comente:_____

15. ¿El sistema de administración de riesgos, posee canales de información y comunicación interna, que garantice el aprovisionamiento de información oportuna sobre nuevos riesgos tecnológicos; así como medios de registro históricos y estadísticos de los mismos?

SI NO

16. De los factores siguientes, ¿cuáles generan riesgos al entorno informático en su organización?

- La organización y gestión: presupuestos bajos, revisión gerencial lenta.
- Entorno de trabajo: espacios inadecuados, curvas de aprendizaje mas largas, falta o mal funcionamiento de herramientas.
- Usuarios finales: falta de participación y problemas de comunicación.
- Personal: falta de motivación, poca calidad, resistencia al trabajo en equipo.
- Procesos: burocracia, no existe control de calidad.
- Planificación: tareas innecesarias, falta de previsión en áreas desconocidas.

17. ¿Cómo se ejecuta la estimación de la probabilidad y frecuencia de materialización de riesgos, en su programa de administración de riesgos?.

- Mediante expertos de informática
- Uso de la técnica Delphi
- Calibración por adjetivos
- Todos los anteriores
- Otros, indique:_____

18. ¿Qué estrategias suelen utilizarse en el programa de administración de riesgos, para que éstos sean controlados?

- Evitar riesgos: Eliminando actividades arriesgadas.

- Reducir riesgos: Diversificando responsabilidades.
- Planificar: Preparar reacción oportuna del entorno informático ante los riesgos.
- Transferir riesgos: Uso de seguros, protección externa
- Otros, señale:_____

19. Debido a la naturaleza especializada del entorno informática y como parte del control de riesgos, ¿con que frecuencia se contratan auditorias informáticas?.

- 6meses – 1 año
- Más de 1 año – 2 años
- Más de 2 años

20. ¿Existe un proceso de monitoreo o seguimiento, respecto de la incorporación oportuna de controles y medidas correctivas, como parte de la gestión de riesgos?.

SI NO

21. ¿Cuáles de los siguientes aspectos de la evaluación de la administración de riesgos considera necesarios para el desarrollo de su trabajo?

- Evaluar los objetivos y las políticas de la administración de riesgos.
- Identificar y evaluar las exposiciones a riesgos existentes en la organización
- Evaluar las decisiones relacionadas a pérdidas.

- Evaluar las medidas de la administración de riesgos que han sido implementadas.
- Recomendar cambios para el beneficio del sistema de gestión utilizado por la organización.
- Todos los anteriores.

22. ¿Qué tipo de evidencia forma parte de sus papeles de trabajo relacionados con la evaluación de la administración de riesgos en tecnología de información?.

- Papel
- Cintas Magnéticas
- Discos Compactos
- Disquetes
- Diapositivas
- Películas

23. ¿Considera que es importante y útil, elaborar una guía que ayude a las unidades de auditoria interna de las cadenas de supermercados; a evaluar la administración de riesgos en tecnología de información?

SI NO