ADMINISTRACIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN DE UNA EMPRESA DEL SECTOR INFORMÁTICO

AUTORES:

Jennifer Dennise Maxitana Cevallos[1], Bertha Alice Naranjo Sánchez[2].

- [1]Auditor en Control de Gestión 2005; email: jmaxitana@ubbi.com.

- [2]Directora de Tesis, Ingeniera en Computación, Escuela Superior Politécnica del Litoral, 1994, Postgrado Ecuador, Escuela de Postgrado de Administración de Empresas ESPAE, 1997. Profesora de la ESPOL desde 1996., email: anaranjo2408@ubbi.com

RESUMEN

El presente trabajo muestra una alternativa de Administración de Riesgos, en una empresa del sector informático, cuyo objetivo principal es satisfacer las necesidades de sus clientes dando garantía de su trabajo.

En el primer capítulo se revisa un poco la historia de la Tecnología de Información (TI) en lo que respecta a la Administración de Riesgos y a los avances de la Tecnología de Información. En la segunda parte se presenta el marco teórico, dejando claro los conceptos y procesos para la iniciación del proyecto. En el tercer capítulo, se muestra las normas y estándares internacionales sobre los cuales tiene que regirse la elaboración de este trabajo. En la cuarta parte se lleva a cabo el desarrollo de la Administración de Riesgos, detectándose las falencias durante el análisis y determinando las soluciones respectivas puestas a consideración de la Gerencia de la empresa. En la quinta y última parte, se muestran las conclusiones y recomendaciones correspondientes.

ABSTRACT

The present work shows an Administration Risk alternative in a company of the information sector, whose principal objetive is satisfay the necesities of their customers, give them the guaranty of their job.

In the first chaper, you can review a little bit the history of the Technology of Information (TI) in relation with the Administration Risk and the Technology of Information advances. In the second part, it presents the theoretical aspect

and it leaves the definitions and process clear for the project initiation. In the third chaper, it shows the international norms and standards in which, the elaboration of these job must be rule. In the fourth chaper, you can find the Administration Risk development, and it detects the debilities during the analysis and it determines the respective solutions and put them to the management consideration. In the fifth and last part, it shows the conclusions and recomendations of the present work.

INTRODUCCIÓN

La Tecnología de Información (TI) se ha convertido en el corazón de las operaciones de cualquier organización, desde los sistemas transaccionales hasta las aplicaciones enfocadas a la alta gerencia que ayudan tanto a las operaciones transaccionales diarias como a definir el rumbo que tiene que seguir una organización.
Una de las situaciones que se está presentando con mayor relevancia en las organizaciones, es el outsourcing de procesos que están en la cadena de valor de una organización pero que los directivos deciden colocarla a cargo de un tercero, esta es una situación que se documenta en el presente trabajo.
Por otro lado las operaciones de una organización tienen que seguir ciertos estándares y lineamientos y a su vez ésto puede provocar cambios en la manera de realizar las cosas, todos estos criterios se detallan en este documento.

Importancia de Tecnología de Información

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

Actualmente, las organizaciones dependen en su totalidad de tener la información exacta en el momento preciso, las compañías que no son capaces de alcanzar esto, están en peligro de extinción porque con el paso de los años, la información se ha convertido en el arma más potente para la toma decisiones, y es aquí donde radica la prioridad de desarrollar nuevas tecnologías que permitan tener la información requerida y lista para ser utilizada. Sin embargo, la mayoría de las organizaciones han fallado al no aprovechar el ambiente existente e implementar ideas innovadoras para mejorar el papel que juegan los sistemas de información dentro de sus organizaciones, algunos de estos errores son:

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

La Administración y los Riesgos

Se debe decidir cual es la inversión razonable en seguridad y en control de TI y cómo lograr un balance entre riesgos e inversiones en el enfoque de control en un ambiente de Tecnología de Información, frecuentemente impredecible. Mientras la seguridad y los controles en los sistemas de información ayudan a administrar los riesgos sin eliminarlos, surge la necesidad de administrar esos riesgos, puesto que el exacto nivel de riesgo nunca puede ser conocido ya que siempre existe un grado de incertidumbre.

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

Existe una creciente necesidad entre los usuarios de los servicios de Tecnología de Información, de estar protegidos a través de la acreditación y la auditoría de servicios de Tecnología de Información proporcionados internamente o por terceras partes, que aseguren la existencia de controles y seguridades adecuadas. Actualmente, sin embargo, es confusa la implementación de buenos controles de Tecnología de Información en sistemas de negocios por parte de entidades comerciales, entidades sin fines de lucro o entidades gubernamentales. Esta confusión proviene de los diferentes métodos de evaluación, como las evaluaciones ISO9000, nuevas evaluaciones de control interno COSO, COBIT, entre otras.

Frecuentemente, los auditores han tomado el liderazgo en estos esfuerzos internacionales de estandarización, debido a que ellos enfrentan continuamente la necesidad de sustentar y apoyar su opinión acerca de los controles internos frente a la Gerencia. Es por esta razón para mí, un tema de importancia en mi perfil profesional por lo cual considero necesario estudiarlo.

Presentación del Problema

Este trabajo identifica los principales controles y seguridades que deben implementarse en el departamento de sistemas de una empresa del sector informático.

En el campo informático, el trabajo destaca la importancia de definir acertadas políticas ligadas de forma inseparable a los objetivos de la organización, planteados en su estrategia empresarial, en su misión y visión.

Debido a la trascendencia de los controles y seguridades de los sistemas de procesamiento de información que ameritan ser implementados, se debe enfatizar y relevar la importancia y la significación de la Administración de Riesgos de TI.

Entonces, se hace necesario revisar, evaluar y actualizar aspectos relacionados a un control efectivo de la Administración de Riesgos de TI.

CONTENIDO

Para el desarrollo de esta investigación es necesario dejar en claro ciertas definiciones que son consideradas como relevantes para un mejor entendimiento del trabajo.

Definiciones:

1.- Riesgo: Según Fernando Izquierdo Duarte: "El Riesgo es un incidente o situación, que ocurre en un sitio concreto durante un intervalo de tiempo determinado, con consecuencias positivas o negativas que podrían afectar el cumplimiento de los objetivos".

2.- Riesgos de Tecnología de Información: El concepto de riesgo de TI puede definirse como el efecto de una causa multiplicado por la frecuencia probable de ocurrencia dentro del entorno de TI. Surge así, entonces la necesidad del control que actúe sobre la causa del riesgo para minimizar sus efectos. Cuando se dice que los controles minimizan los riesgos, lo que en verdad hacen es actuar sobre las causas de los riesgos, para minimizar sus efectos.

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

4.- Determinación del Nivel del Riesgo: La determinación del nivel de riesgo es el resultado de confrontar el impacto y la probabilidad con los controles existentes al interior de los diferentes procesos y procedimientos que se realizan. Para adelantar esta etapa se deben tener muy claros los puntos de control existentes en los diferentes procesos, los cuales permiten obtener información para efectos de tomar decisiones, estos niveles de riesgo pueden ser: Alto, Medio y Bajo.

5.- Matriz de Riesgos: Utilidad del Método Matricial para el análisis de Riesgos: Este método utiliza una matriz para mostrar gráficamente tanto las amenazas a que están expuestos los sistemas computarizados como los objetos que comprenden el sistema. Dentro de cada celda se muestran los controles que atacan a las amenazas.

6.- Administración de Riesgos: Es un proceso interactivo e iterativo basado en el conocimiento, evaluación y manejo de los riesgos y sus impactos, con el propósito de mejorar la toma de decisiones organizacionales. Es aplicable a cualquier situación donde un resultado no deseado o inesperado pueda ser significativo o donde se identifiquen oportunidades de mejora.

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

8.- Metodología: Según el Diccionario, Método es el “modo de decir o hacer con orden una cosa”. Asimismo define el diccionario la palabra Metodología como “conjunto de métodos que se siguen en una investigación científica”. Esto significa que cualquier proceso cinético debe estar sujeto a una disciplina de proceso defina con anterioridad que llamaremos Metodología.

Una vez revisadas las definiciones conceptuales, iniciaremos el desarrollo del proceso de administración de riesgo.

Proceso de Administración de Riesgos de TI:

A continuación se describen las principales etapas definidas para el Proceso de Administración de Riesgos de TI.

- Establecimiento de la Metodología de TI
- Identificación de Riesgos de TI
- Análisis del Riesgo de TI

- Evaluación y Priorización de Riesgos de TI
- Tratamiento de Riesgos de TI (Controles Definitivos)
- Monitoreo y Revisión

1.- Establecer Metodología.- Luego de una evaluación de las diferentes metodologías que existen para analizar y administrar el Riesgo de Tecnología de Información, la decisión se inclinó por considerar la del criterio de los expertos, que es la metodología Delphi, que consiste en reunir un grupo de personas que conozcan del negocio y tengan noción mínima de los riesgos.

La directiva de la empresa se inclinó por esta metodología ya que consideraron que para poder establecer soluciones en la empresa era imprescindible que se considere la opinión de las personas que colaboran en la organización, en este caso, los expertos del departamento de Sistemas, que son cuatro personas conjuntamente con el jefe del departamento de sistemas, las que participan en el desarrollo de la metodología.

2.- Identificar Riesgos de TI.- Una vez definidos los objetivos y el alcance del trabajo a realizar, se desarrollaron criterios de evaluación de riesgos de TI, que es el aspecto en el que se va a centrar esta evaluación, para el Área de Informática.

Para la identificación de los riesgos, se entrevistó a cada uno de los expertos, donde analizando los problemas que afectan al departamento, se estableció la Matriz de Ponderaciones y se determinaron los riesgos más relevantes.

3.- Análisis del Riesgo de TI.-

3.1. Valorar el Riesgo Inherente: Para la valoración de los riesgos que se analizan, se definió una escala de valoración Cualitativa, que es la asignación de las características Alto, Medio y Bajo a los diferentes riesgos encontrados.

3.2. Determinar Controles Existentes: El Departamento tiene ciertos controles, pero carece de otros controles que son necesarios ya sea para prevenir, detectar o corregir la materialización de los Riesgos.

3.3. Identificar Nivel de Exposición: Cabe recalcar que el Nivel de Exposición es igual a decir Riesgo Inherente menos Controles. Teniendo en cuenta esta definición, se puede decir que la empresa tiene un nivel de exposición medio-alto, ya que no tiene los suficientes controles necesarios para restarle a los riesgos inherentes.

4. Evaluación y Priorización de los Riesgos: Método Matricial para el Análisis de Riesgos: Este método utiliza una matriz que muestra gráficamente tanto las amenazas a que están expuestos los sistemas computarizados y la información del departamento, como los objetos que comprenden el departamento de Sistemas.

Se describe a continuación los pasos para el desarrollo del método:

- Crear la matriz de amenazas (causas de riesgo) y de objetos del sistema a analizar.
- Categorizar los riesgos.

4.1. Crear la matriz de amenazas y de objetos: Luego de ponderar los riesgos existentes dentro del Departamento, trabajo realizado por el grupo de experto, se determinaron los que compondrán la Matriz de Control de Riesgos (Amenazas y Objetos).

4.2. Categorización de Riesgos: Se categorizan las amenazas por niveles de riesgo, de mayor a menor en orden de importancia, como haya sido determinado por el grupo Delphi.

Luego los cinco expertos proceden a votar. La votación se realiza de manera vertical y horizontal. Después se suman los votos derechos de las columnas y los votos izquierdos de las filas; y para la cifra total se suman los resultados antes obtenidos.

Paso a seguir, se procede a categorizar la sensibilidad de los objetos. Proceso que se inicia pasando los objetos que registra la matriz de control de riesgos en una hoja de comparación de categorías de riesgos. Para categorizar la sensibilidad de los objetos se utiliza como criterio la percepción que tenga cada uno de los miembros del equipo Delphi sobre objetos que puedan causar mayor pérdida económica si se daña o causa demoras en el procesamiento.
A seguir, se procede a la votación del grupo de igual manera como se realizó con la categorización de las amenazas. De igual manera se procede a sumar de la misma manera que se realizó con las amenazas.

Con la categorización tanto de las amenazas como los objetos, se realiza la combinación de las dos categorías, elaborando una matriz de combinaciones, colocando los totales en orden de mayor a menor (de izquierda a derecha y de arriba abajo), en los dos casos.

Después se procede a realizar los cálculos correspondientes, multiplicando los valores de las amenazas con los de los objetos para así poder obtener el nivel de riesgo / sensibilidad de las celdas de acuerdo con el valor del producto. Puede que al terminar este proceso se presenten repeticiones, las cuales no son consideradas para determinar el nivel de riesgos de las celdas. Luego dividimos las celdas en regiones de mayor, menor y mediano riesgo.

Como en este caso no existen repeticiones en los productos, se consideran las 36 celdas para la determinación del nivel de riesgo. Se procede a dividir las 36 celdas para el número de expertos (36 / 5 = 7,2 = 7). La escala de valoración es Semicuantitativa ya que se asignan rangos numéricos a las características Alto, Medio y Bajo. Se toman las siete celdas con los productos más altos para determinarlas con un nivel de riesgo alto, las siete celdas con los productos más bajos para determinarlas con un nivel de riesgo bajo; y las veinte y dos celdas restantes se las determina con un nivel de riesgo medio.

5.- Diseñar los controles definitivos.- Finalmente, con el resultado del trabajo realizado, apoyados en el Método Delphi y en el modelo matricial Riesgo / Sensibilidad, se diseñan y documentan definitivamente los controles a nivel: preventivo, detectivo y correctivo; de acuerdo al área informática del Departamento de Sistemas.

6. Presentar los Resultados.- La Gerencia de la empresa debe de conocer el resultado del análisis de riesgo de manera oportuna, el cual será presentado en un informe detallado. De esta manera la Gerencia podrá tomar las acciones necesarias para su implantación.

CONCLUSIONES

1. La Administración de Riesgos de TI es importante ya que es una aproximación científica del comportamiento de los riesgos, anticipando posibles pérdidas accidentales con el diseño e implementación de procedimientos que minimicen la ocurrencia de pérdidas o el impacto financiero de las pérdidas que puedan ocurrir.

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

3. Se debe enfatizar y relevar la importancia y la significación de la Administración de Riesgos de TI, debido a la trascendencia de los controles y seguridades de los sistemas de procesamiento de información que ameritan ser implementados en toda la organización.

4. La Administración de Riesgos de TI, dentro de la empresa, es una herramienta muy útil para el mejor desarrollo de las actividades de un departamento o de todos los departamentos de la organización.

5. La Administración de Riesgos de Tecnología de Información, nos muestra los principales controles y seguridades que deben implementarse en uno de los departamentos de la empresa como es el caso del departamento de sistemas.

6. El análisis de riesgos de TI, desarrollado en la empresa, ha contribuido a ampliar aún más los conocimientos sobre los problemas significativos que pueda tener el área de sistemas de una empresa y sobre las múltiples ideas de soluciones que se pueden aplicar.

7. Este trabajo tiene como una de sus metas primordiales el orientar a las generaciones futuras, sobre los aspectos importantes que se deben considerar en la administración de riesgos de Tecnología de Información de las empresas del sector informático.

REFERENCIAS

1. J. Maxitana, "Administración de Riesgos de Tecnología de Información de una empresa del sector Informático" (Tesis, Instituto de Ciencias Matemáticas, Escuela Superior Politécnica del Litoral, 2005).

2. G. Cepeda, <u>Auditoría y Control Interno</u> (2da. Edición, Colombia, McGraw-Hill Interamericana S.A., 1997), pp. 208-224, 227-232

3. Mario Piattini y Emilio Del Peso**,** <u>Auditoría Informática: Un Enfoque Práctico</u>, (2da. Edición, España, Editorial RA-MA, 2004), pp. 45-89, 310-317, 394-401, 570-581, 616.

4. Pinilla Forero José Dagoberto, Auditoría Informática - Aplicaciones en Producción: Análisis de Riesgos (1ra. Edición, Colombia, ECOE Ediciones, 1997), pp. 129-141, 165-186.

5. Jean Paul Sallenave, Gerencia y Planeación Estratégica: El Método Delphi (2da. Edición, Colombia, Editorial Norma, 1996).