

ADMINISTRACIÓN DEL RIESGO: UNA PRIORIDAD EN COLOMBIA

Jorge Edison Ramírez Torres
Especialización en Seguridad Informática
Universidad Piloto de Colombia
wizardedi@gmail.com
wizardedi@hotmail.com

Abstract ---In this inspection of the Standard Model of Internal Control (MECI) and subsequent analysis of risk management, described in detail the evolution of policy and conceptual type that has had the concept of risk at the enterprise level and its direct relationship with the State also shown parallel comparison with the different concepts of risk analysis at international level, this in order to show that Colombia is on par with these processes, policies and concepts, reflecting it a country that is at the forefront of what risk management needs, is why it is highly important to cover this topic in an explicit and concrete way to reach conclusions of changes that lead to new sources of development and highlight the conceptual frameworks Models of the country.

Index terms : risk management, risk, risk treatment, policy development, risk communication, risk context.

Resumen ---En esta inspección del Modelo Estándar de Control Interno (MECI) y el posterior análisis de la administración del riesgo, se ha descrito a detalle la evolución de tipo normativo y conceptual que ha tenido la concepción de riesgo a nivel de empresa y su relación directa con el Estado, además, se muestra de forma paralela una comparación con los distintos conceptos de análisis de riesgos a nivel internacional, esto con el fin de evidenciar que Colombia se encuentra a la par con dichos procesos, políticas y conceptos, lo muestra como un país que está a la vanguardia de lo que necesita la administración de riesgos, es por esto que es de gran

importancia abarcar este tema de manera explícita y concreta para llegar a conclusiones de cambios que lleven a nuevas fuentes de desarrollo y a destacar los marcos conceptuales de los Modelos en el país.

Índice de términos: Gestión de riesgo, riesgo, tratamiento del riesgo, políticas, desarrollo, comunicación del riesgo, contexto del riesgo.

I. INTRODUCCIÓN

La administración del riesgo es un tema prioritario en el mundo en el que se vive actualmente, ya que los riesgos sean esperados o no esperados se presentan en todo tipo de organizaciones convirtiéndose esto en una filosofía de gestión de riesgos tal como lo expresa el Modelo COSO [4], generando así dificultades en todos los campos de acción de la entidad y disminuyendo la eficacia y efectividad de todos los grupos laborales, lo cual, no es ajeno para el Estado colombiano quien a través del Departamento Administrativo de la Función Pública vio este tema como una prioridad para el cumplimiento de objetivos de las instituciones y quiso implementar medidas específicas que sirvieran como una orientación y en sí como una herramienta básica para detectar y detener este tipo de riesgos, es por esto que se implementó el Decreto 1599 del 20 de mayo del 2005 donde se establece un Modelo Estándar de Control Interno que tiene como base modelos internacionales tales, como el ISO/IEC y AS/NZS ISO 31000:2009, los cuales abarcan de manera integral la administración de riesgos mostrando los diferentes factores que intervienen

en este y partiendo de esto Colombia y su modelo tomaron estos conceptos y los implementaron en la norma colombiana. Por tal motivo para entender este mecanismo complejo el siguiente escrito desglosará los distintos parámetros que participan en este modelo, intentando así mostrar una mirada profunda y específica de los avances presentados con este tipo de administración en cuanto a nuevas problemáticas a resolver.[1] Las principales características de la metodología de gestión de riesgos son las siguientes:

- La gestión de riesgos es lo más importante para cada proceso, proyecto o producto y se considera como la base o estructura de la planeación, ya que con base a ella se realiza la creación de los controles que se van a aplicar en las actividades las cuales se irán cumpliendo una a una para obtener los resultados esperados.
- La gestión de riesgos es muy estricta en el manejo de la normatividad y de la afectación que esta pueda llegar a generar en los involucrados en este proceso de gestión.

Los métodos para realizar un análisis de riesgo [7]:

A. Método cualitativo de análisis

- Análisis de histórico de riesgos.
- Listas de chequeo.
- Análisis de fallas y eventos.
- Análisis causas y consecuencias.

B. Método cuantitativo de análisis

- Análisis cuantitativo de fallas.
- Análisis cuantitativo de eventos.
- Análisis costo ciclo de vida.
- Análisis estadístico y numérico.

II. COLOMBIA Y EL PANORAMA EN GESTIÓN DE RIESGOS

III.

A. Aspecto normativo.

En Colombia, en cuanto a la administración de riesgos las leyes han ido desarrollándose desde hace 20 años, tomando como base la ley 87/93 que complementada por el decreto 1537/01 acerca de las normas del Control

interno, pasando por la ley 489/89 para la organización de la administración pública y un decreto y una directiva presidencial en 1999 que abarcan políticas del control interno y de la lucha contra la corrupción, han hecho que se llegue a una norma integral y de amplio entendimiento tal como lo es el Decreto 1599 de 2005 que adoptó el Modelo Estándar de Control Interno (MECI) [1].

B. El MECI

Es un Modelo que tiene como propósito llevar a las entidades a cumplir objetivos y fines del Estado por medio de:

- Control al Cumplimiento (Legalidad)
- Control Estratégico (Planeación)
- Control de Ejecución (Operación)
- Control de Evaluación (Verificación)
- Control de Información (Comunicación)

Además, toma como principios la autorregulación, la autogestión y el autocontrol [2].

C. Administración del riesgo

En si el riesgo se establece como una incertidumbre de que ocurra un acontecimiento que afecte la capacidad de lograr objetivos y este se mide en términos de consecuencias y probabilidad [4], dicho esto la administración de riesgos juega un papel esencial en el manejo integral de dichos eventos adversos, para este fin se deben tener en cuenta los siguientes pasos:

- Conformación de un equipo MECI.
- Capacitación en la metodología.
- Compromiso alta y media dirección.

En el siguiente cuadro se esquematiza de manera clara los elementos principales que llevan a un óptimo manejo de la administración de riesgos, desarrollando los pasos anteriormente mencionados:

FIGURA I
PROCESO DE GESTIÓN DE RIESGO



Fuente: [7], NTC 5254 GESTIÓN DEL RIESGO.

1) *Establecimiento del contexto*: se basa en definir parámetros básicos desde tres contextos el estratégico, el organizacional y el de la gestión determinando con esto las interacciones entre los distintos factores, para llegar a definir marcos de evaluación, el contexto define los parámetros básicos por los cuales se deben gestionar los riesgos y estos establecen alcances para el resto de un proceso de gestión de riesgos, para realizar una buena visibilidad del contexto tendremos que observar el ambiente interno y externo de la organización.

2) *Identificación de riesgos*: se hace por medio de herramientas que den una global de la serie de eventos, causas y factores asociados, tomar en cuenta los componentes para realizar una identificación del riesgo como, una fuente, un evento o incidente, una consecuencia, una causa, controles y cuándo y dónde puede ocurrir.

3) *Análisis de riesgos*: consiste en clasificar dichos riesgos según su importancia y por ende verificar medidas de control y de manejo, el análisis del riesgo también incluye tomar en cuenta las fuentes del riesgo, las consecuencias que pueden ser de carácter positivo o negativo y realizar una revisión de la probabilidad de que esas consecuencias puedan llegar a ocurrir. Todo esto es necesario para realizar análisis de la información y su propósito para lo cual se podrían realizar diferentes tipos de análisis como cualitativos, semicuantitativos y cuantitativos.

4) *Evaluación de riesgos*: esta medida se basa en una comparación entre el nivel de riesgo y las medidas que se llevan a cabo, como resultado de esto se logrará una lista de decisiones a tomar, donde se podría llegar a generar la preparación e implementación de los planes de tratamiento, valoración de las opciones para tratar el riesgo, identificación de riesgos de rasgos positivos e identificación de riesgos de rasgos negativos y por ultimo realizar un análisis de costo beneficio.

5) *Tratamiento de riesgo*: esta etapa abarca las decisiones a tomar en las cuales es prioritario evitar reducir, transferir y retener el riesgo.

6) *Monitoreo y revisión*: se realiza para identificar nuevos riesgos y verificar el cumplimiento de las medidas control, ya que es parte esencial en el crecimiento de las empresas para monitorear la eficacia y la eficiencia de las estrategias para la implementación de los tratamientos de riesgos.

7) *Comunicación y consulta*: abarca procesos de gestión y flujo de información entre las partes interesadas para llegar a acuerdos y normas de control. [3] Tomar en cuenta los objetivos de la comunicación, los participantes, las perspectivas de los participantes, los métodos de comunicación a usar y un proceso de evaluación.

IV. ÁMBITO INTERNACIONAL

Este aspecto la nueva Norma Internacional ISO/IEC 27005:2011 Tecnología de la información- técnicas de seguridad- gestión del riesgo de la seguridad de la información refuerza la implementación de ISO/IEC 27001, que es la norma del sistema de gestión de seguridad de la información que se basa en un enfoque de gestión de riesgos. Cabe resaltar que el tener pleno conocimiento de estos conceptos ayuda a comprender de manera amplia la Norma Internacional (5), en la cual está también basada la Norma Colombiana con los mismos parámetros para la administración de riesgos, esto deja ver como el sistema colombiano está a la vanguardia en sistemas internacionales tanto como el ISO/IEC y AS/NZS ISO 31000:2009 Risk management que es la norma basada en AS / NZS 4360:2004 esta fue creada por un comité establecido por la Organización Internacional de Normalización (ISO), creando cambios

para la Norma de 2009 ya que realiza un mayor énfasis en la implementación e integración a instituciones de las normas, además de anexos para resaltar gestiones y admitir que no todas las gestiones pueden ser óptimas, además esta norma describe en detalle el proceso sistemático y lógico(6), mostrando que el sistema colombiano se encuentra a la par de la aplicación de dichas normas dadas por los dos documentos internacionales, esto lo posiciona como un país interesado en la seguridad general de la información mediante la prevención y control de posibles riesgos.

V. RIESGO

El objetivo de la seguridad de la información es encontrar una metodología que permita detectar, analizar y controlar el riesgo o en su defecto mitigar la posibilidad que este ocurra en las organizaciones. La norma técnica Colombiana NTC 5254 esta guía es la que las empresas colombianas deben establecer e implementar para realizar un proceso de administración de riesgos para que estas puedan realizar pasos como identificación, análisis, evaluación, tratamiento, comunicación y monitoreo.

La Administrar del riesgo con lleva realizar una valoración del riesgo, para lo cual es importante realizar unos procesos los cuales son muy importantes a la hora de identificar los posibles riesgos las definiciones a tener en cuenta son [10]:

- **Análisis del riesgo.** Proceso sistemático para entender la naturaleza del riesgo y deducir el nivel del riesgo.
- **Consecuencia.** Resultado o impacto de un evento.
- **Control.** Proceso, política, dispositivo, práctica u otra acción existente que actúa para minimizar el riesgo negativo o potenciar oportunidades positivas.
- **Evaluación del control.** Revisión sistemática de los riesgos para garantizar que los controles aún son eficaces y adecuados.
- **Evento.** Ocurrencia de un conjunto particular de circunstancias.
- **Frecuencia.** Medición del número de ocurrencias por unidad de tiempo.

- **Posibilidad.** Se usa como descripción general de la probabilidad o la frecuencia.
- **Monitorear.** Verificar, supervisar o medir regularmente el progreso de una actividad, acción o sistema para identificar los cambios en el nivel de desempeño requerido.
- **Probabilidad.** Medida de la oportunidad de ocurrencia expresada como un número entre 0 y 3.
- **Riesgo residual.** Riesgo remanente después de la implementación del tratamiento del riesgo.
- **Valoración del riesgo.** Proceso total de identificación, análisis y evaluación del riesgo.
- **Criterios del riesgo.** Términos de referencia mediante los cuáles se evalúa la importancia del riesgo.
- **Reducción del riesgo.** Acciones que se toman para reducir la posibilidad y consecuencias asociadas a un riesgo.

Implementar un sistema de gestión del riesgo es con el fin de que las empresas colombianas puedan tener una mejor forma de identificar amenazas y oportunidades, para lo cual se requiere que al implantar un sistema de gestión de riesgos tengan la información requerida y suficiente para así tomar decisiones y poder estar preparados para todas aquellas incidencias y pérdidas de la información lo cual genera costos y pérdidas para la empresa colombiana.

VI. CONCLUSIONES

- El Modelo Estándar de Control Interno (MECI) es fundamental, ya que brinda las herramientas necesarias para realizar gestión a los riesgos y así controlarlos para mitigar sus consecuencias.
- Es necesario estar en completa comunicación con las partes de la empresa ya que estas deciden el camino de una puesta en marcha óptima enfocada hacia un modelo de control interno de riesgos ejemplar y así estos factores darán una guía para brindar las herramientas y así lograr implementar adecuadamente y mitigar los riesgos en la empresa por medio de una buena comunicación y monitoreo de los posibles riesgos a tratar.

- Es importante resaltar que el desarrollo en Colombia en cuanto a modelos de riesgo se está implementando de una forma muy activa con la implementación de las normas ISO/IEC, logrando así que los niveles de seguridad y mitigación de riesgos sean aún más confiables y certeros en las empresas de hoy en día en el país.
- La integración de la gestión del riesgo en un sistema produce una mejor administración de la continuidad del negocio, aumentando la seguridad.

REFERENCIAS

- [1] Departamento administrativo de la función pública. Cartillas de Administración Pública .7 Guía de Administración del Riesgo. Juan Felipe Rueda. 2009.
- [2] Cartilla Guía. Modelo Estándar De Control Interno MECI 1000:2005. Dr. Álvaro Hernández Gutiérrez.
- [3] Gestión del riesgo: Pautas Generales ofrecidas por la Norma Técnica Colombiana. Revista Apuntes Contables. Universidad Externado De Colombia.2006.
- [4] Gestión de riesgos corporativos (COSO ERM).Dr. Lago José. Ex Presidente de FLAI. Director At Large IIA Board Of Directors.2005.
- [5] <http://www.iso.org/iso/news.htm?refid=Ref1451>
- [6] AS/NZS ISO 31000:2009. Risk management— Principles and guidelines. Australian/New Zealand Standar.2009.
- [7] Icontec. Norma Técnica Colombiana ntc 5254, Gestión del Riesgo, Colombia, 2004.
- [8] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Medical devices -- Application of risk management to medical devices. ISO 14971. Geneva: ISO, 2007. 82 p.
- [9] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Dispositivos Médicos. Sistemas de Gestión de Calidad. Requisitos para propósitos regulatorios. NTC-ISO 13485. Bogotá D.C.: El Instituto, 2006. 67 p.
- [10] ICONTEC, RESUMEN NORMA TECNICA COLOMBIANA NTC 5254. Colombia: ICONTEC 2006. p. 1.
<http://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCEQFjAB&url=http%3A%2F%2Fwww.sarlaf.com%2Fhtml%2FRESUMEM%2520NORMA%2520TECNICA%2520COLOMBIANA%2520NTC%252052541.doc&ei=1FyEVfL9EaqwsATBuZXYCw&usg=AFQjCNHAWxS8LZh9QN8QO9neAepbEBRqfA&sig2=k4ZNBw9szR26V66TmTbLvQ&bvm=bv.96042044,d.cWw>