TRIBUNAL SUPREMO DE ELECCIONES
AUDITORÍA INTERNA

METODOLOGÍA PARA EVALUACIÓN DEL RIESGO TECNOLOGÍAS DE INFORMACIÓN

Introducción

Los procesos de evaluación de riesgos propuestos por la Contraloría General de la República por medio de metodologías, formulas o modelos de evaluación, son los que se aplican para cualquier auditoría de este tipo.

Con la planeación de la Auditoría en el programa de trabajo se debe realizar un proceso de análisis de riesgos, segundo paso en el proceso de administración proactiva de riesgos.

Este proceso se realiza por medio de la conversión de los datos de un riesgo de información para la toma de decisiones respectiva. El análisis minucioso se corrobora con la solicitud de información como insumo para el programa de auditoría formulado previo a la necesidad de ejecutar la fiscalización.

Esta se realiza por medio de los siguientes artefactos de fiscalización AF:

- entrevistas estructuradas con expertos en el área de interés;
- utilización de grupos multidisciplinarios de expertos;
- evaluaciones individuales utilizando cuestionarios;
- análisis FODA;
- uso de modelos de computador u otros; y
- uso de árboles de fallas y árboles de eventos.

COMPONENTES DE LAS MATRIZ DE DECISIÓN ESTRATÉGICA (MADE)

GRADO DE EXISTENCIA

Mediante la generación de la evidencia pertinente se valorará en tres factores el grado de existencia del proceso requerido a fiscalizar.

Por lo tanto se debe tomar en cuenta los siguientes rubros:

- Si el proceso existe el valor es = 0
- Si existen parcialmente el valor será = 0.5
- Si no existe del todo es grado será = 1
- Si no se aplica ningún criterio de fiscalización el valor será = NA

Se debe sacar un porcentaje de dicho grado de existencia, el cual dependerá del total de puntos o procesos a fiscalizar, los cuales han sido contestados por el auditado utilizando los diferentes artefactos de evaluación para la generación de evidencia.

De esta forma el mismo auditado proporcionara los elementos de evaluación en el análisis de cumplimiento de los diferentes procesos a evaluar y fiscalizar. De aquí sale el rubro del grado de existencia, el cual será el dato base para evaluar el riesgo.

IMPACTO DE UN RIESGO 25%.

El impacto de un riesgo mide la severidad de los efectos adversos, o la magnitud de una pérdida, si el riesgo llega a suceder. La decisión de cómo medir las pérdidas sostenidas no es un asunto trivial.

Si el riesgo tiene un impacto financiero, el valor monetario es la forma preferible para cuantificar la magnitud de una pérdida. El impacto financiero podrían ser costos a largo plazo en la operación y el apoyo, una pérdida en la participación en el mercado, costos a corto plazo por el trabajo adicional, o pérdida en el costo de oportunidad. Pero este es producto de la multiplicación porcentual del grado de cumplimiento, entonces:

Sea GE = Grado de Existencia, I = impacto y valor porcentual del impacto = 0.25

Entonces:

I = GE * 0.25

Otros riesgos pueden tener un nivel de impacto en donde es más conveniente una escala subjetiva del 1 al 10. Básicamente se califica la viabilidad del éxito del proyecto. Los valores altos indican una pérdida seria para el proyecto. Los valores medianos señalan una pérdida en partes del proyecto o una disminución de la eficiencia.

Si: GE = Grado de Existencia, I = impacto y VS valor subjetivo porcentual del impacto = de 0.01 a 0.10

Entonces:

I = GE * VS

MATERIALIDAD Y EL RIESGO DE LA AUDITORÍA 15%

El auditor tomará en cuenta la materialidad como el límite máximo de error que está dispuesto a aceptar para emitir un dictamen sin salvedades. En la determinación de la materialidad los auditores utilizarán su juicio profesional a efecto de emitir un informe confiable. Esto significa que al determinar la materialidad el auditor deberá tener presente quienes son los usuarios primarios y secundarios de los resultados de la auditoría, que uso darán probablemente a estos y el grado de precisión que se deberá tener para que los usuarios fundamenten sus decisiones en ellos.

DETERMINACIÓN DE LA MATERIALIDAD

La materialidad está relacionada con el monto máximo de errores posibles y no con los errores más probables o conocidos. El monto máximo de errores posibles incluye todo tipo de errores, errores "graves", errores "leves", fraudes e incumplimientos. Los errores pueden ser por inobservancia de la normatividad, desviaciones de la realidad, determinación inadecuada de las estimaciones, fallas en los procedimientos de control interno, incumplimientos de convenios, contratos, leyes y otras regulaciones aplicables y la omisión de información necesaria, que tengan un efecto directo y significativo .

Un error o el conjunto de errores existentes se consideran importantes si a la luz de las circunstancias, es probable que las decisiones tomadas con base en dichos errores deba ser modificada.

Para determinar la materialidad en la fase de la planeación deben consideran sólo factores cuantitativos y el auditor deberá considerar siempre el punto de vista del usuario como producto de los artefactos de fiscalización.

Entonces:

Sea GE = Grado de Existencia, M = Materialidad

Entonces:

$M = GE * 0.15$

POSIBILIDAD DE CAMBIO 20%

La magnitud de las consecuencias de un evento, si el mismo ocurriera, y la probabilidad del evento y sus consecuencias asociadas, se evalúan en el contexto de los controles existentes. En las posibilidades de cambio la ocurrencia y la probabilidad se combinan para producir un nivel de riesgo.

Se pueden determinar las consecuencias y probabilidades utilizando análisis y cálculos estadísticos o los artefactos de fiscalización.

Alternativamente cuando no se dispone de datos anteriores, se pueden realizar estimaciones subjetivas que reflejan el grado de convicción de un individuo o grupo de que podrá ocurrir un evento o resultado particular para generar una posibilidad de cambio.

Para evitar prejuicios subjetivos cuando se analizan consecuencias y probabilidades, deberían utilizarse las mejores técnicas y fuentes de información disponibles.

Se pueden incluir las siguientes fuentes de información:

a) Registros anteriores;
b) Experiencia relevante;
c) Prácticas y experiencia de la industria;
d) Literatura relevante publicada;
e) Comprobaciones de *marketing* e investigaciones de mercado;
f) Experimentos y prototipos;
g) Modelos económicos, de ingeniería u otros;
h) Opiniones y juicios de especialistas y expertos.

Para efectos darle un porcentaje se tomará en cuenta el uso de los AF en cuanto a la posibilidad de cambio que ha demostrado el auditado. Entonces:

Si PC = posibilidad de cambio
El valor de PC depende del análisis (AC) que es de 0.01 entre 0.10

Entonces:

PC = (AC * 0.20) * 100

Siempre que sea posible, debería incluirse el nivel de confianza asignado a las estimaciones de los niveles de riesgo.

NIVEL DE EXPOSICIÓN AL RIESGO 25%

Un riesgo se compone de dos factores: su probabilidad y su impacto. La probabilidad de un riesgo es la posibilidad de que un evento suceda en realidad. Para clasificar los riesgos es recomendable la asignación de un valor numérico a la probabilidad. La probabilidad de un riesgo debe ser mayor que cero o el riesgo no representa una amenaza para el proyecto. Asimismo, la probabilidad debe ser menor que 100% o el riesgo es una certeza, en otras palabras, es un problema identificado.

GRAVEDAD DE LOS DAÑOS

- **I: Muy grave 4 a 5**
- **II: Grave 2 a 3**
- **III: Leve = 1**

Por lo tanto sea:

ER = Exposición al riesgo, GV = grado de gravedad valor determinado por el análisis 0 a 5

ER = GV * 0.25

FACTIBILIDAD DE FISCALIZACION 15%

Es responsabilidad de las auditorías internas velar por el cumplimiento de la normativa legal vigente por lo tanto se ha establecido este rubro como una oportunidad de analizar y someter a consideración del superior jerárquico o del auditado, la pertinencia y factibilidad de establecer, derogar y modificar disposiciones, procedimientos, métodos, y sistemas de contabilidad y archivo, entre otros elementos normativos, que permitan la práctica idónea de las auditorías y revisiones a priori.

De Igual manera este rubro se produce por medio de los AF, Si:

FF = Factibilidad de Fiscalización

AF = al análisis de Factibilidad de Fiscalización valor de 0.1 a 0.10

FF = AF * 0.15

Calificación total obtenida 100%

Crítico: De 75% y màs
Alto: De 50% a 75%
Moderado: De 25% a 50%
Bajo: Hasta un 25%

El paso final de evaluación es sumar todos los procesos y rubros porcentuales y se obtendrá un porcentaje que dará un nivel de riesgo de acuerdo con la tabla coloreada.

Este será el insumo para el proceso de generación de hallazgos, fiscalizaciones y recomendaciones finales.

25 de noviembre del 2005

LIC. ALLAN ACEVEDO RODRIGUEZ

AUDITOR EN TI