AUDIdeas

Publicacion Mensual con ideas para el Mejoramiento en Gestion de Riesgos, Seguridad y Auditoría

Bogotá D.C., Febrero de 2020 **Año 10 No. 2** Pag. 1

TEMA: EVALUACION DE LA GESTION DE RIESGOS EN LAS AUDITORIAS BASADAS EN RIESGOS

Contenido

TEMA: EVALUACION DE LA GESTION DE RIESGOS EN LAS AUDITORIAS BASADAS EN RIESGOS

EVALUACION DE LA GESTION DE RIESGOS EN LAS AUDITORIAS BASADAS EN RIESGOS

INTRODUCCION.

La **Auditoría Basada en Riesgos,** *"es una forma de conducir la auditorías,* ***por procesos****,* ***con enfoque preventivo y proactivo,*** *basando su planeación y desarrollo en* ***una muestra de eventos de riesgo inherente*** *que pudieran ocurrir en el proceso y causar impacto negativo significativo a la Empresa, con el propósito de confirmar si el manejo de las operaciones y de la información del proceso se realizan de conformidad con las buenas y mejores prácticas de control interno y seguridad, las reglas del negocio y las normas leyes y regulaciones aplicables".*

Por realizarse **Basadas en Riesgos,** las Auditorías Internas y de Sistemas deberían revisar y evaluar la información de las matrices de riesgo de los procesos y sistemas disponibles en la Empresa, las cuales normalmente se elaboran bajo la dirección del Area de Gestión de Riesgos. *No solo para apoyarse en los conocimientos e indicadores de gestión que proveen éstas matrices para fines de planear la auditoría y evaluar el control interno existente, sino principalmente para* ***asegurar*** *la calidad, confiabilidad y valor de la información de las matrices de riesgo, opinar sobre la forma como se conduce la gestión de riesgos y recomendar acciones para mejorar la Gestión de Riesgos de la organización.*

1. LOS ENTREGABLES DE UNA AUDITORIA INTERNA POR PROCESOS BASADA EN RIESGOS.

Por cada *Auditoria Interna por Procesos Basada en Riesgos, el informe con los resultados de la Auditoría para* la Administración de la Empresa, debería contener:

1) Los resultados de revisar y criticar constructivamente *"el análisis y valoración de riesgos*" del proceso objeto de auditoría, de una muestra de riesgos inherentes seleccionados de la matriz de riesgos del proceso para desarrollar la auditoría "Basada en Riesgos" (entre 10 y 30 eventos de riesgo). Se entregan los siguientes resultados: a) La opinión de la auditoría sobre la confiabilidad del proceso de análisis y valoración de riesgos utilizado por la administración y sobre la calidad de la información producida por la matriz de riesgos del proceso; b) comparativos

entre los resultados de la auditoría y los de la matriz de riesgos; c) hallazgos de la auditoría y d) recomendaciones para mejorar el análisis y valoración de riesgos por parte de los responsables de elaborar y actualizar la matriz de riesgos del proceso.

2) Los resultados de revisar y criticar constructivamente *"el diseño y la efectividad de los controles establecidos por la administración"* para gestionar cada uno de los eventos de riesgo inherente de la muestra de riesgos seleccionada para el desarrollo de la auditoría. Por cada proceso objeto de auditoría, se entrega un informe de Evaluación del Control Interno, que contiene: a) La opinión de la auditoría sobre los procedimientos de diseño de los controles y de evaluación de la efectividad de los controles empleados en la matriz de riesgos del proceso; b) comparativos entre los resultados de evaluación de controles efectuada por la auditoría y los obtenidos por la matriz de riesgos por cada evento de riesgo; c) hallazgos de la auditoría y d) recomendaciones para mejorar las actividades de diseño y efectividad de los controles por parte de los responsables de elaborar y actualizar la matriz de riesgos.

3) Los resultados de verificar en los sitios de operación del proceso, *"el cumplimiento de los controles"* establecidos por la administración para los eventos de riesgo inherente de la muestra de riesgos seleccionados por la auditoría que presentaron resultados "satisfactorios" en la *evaluación del diseño y la efectividad de los controles por riesgo,* es decir, para los riesgos que tienen diseño y efectividad de los controles *"Apropiada*". Por cada sitio de operación se entrega un informe con: a) La opinión de la auditoría sobre el cumplimiento de los controles establecidos; b) el porcentaje de cumplimiento de los controles por cada riesgo inherente según pruebas; c) comparativos de efectividad de los controles antes y después de pruebas de cumplimiento; d) comparativos del riesgo residual antes y después de pruebas de cumplimiento; d) hallazgos de la auditoría para eventos con riesgo residual "No satisfactorio" después de pruebas de cumplimiento; e) motivos de incumplimiento de los controles y f) recomendaciones para mejorar la gestión del riesgos por parte de los responsables de ejecutar los controles y de elaborar y actualizar la matriz de riesgos del proceso. También se genera un informe consolidado con los resultados de la auditoria en todos los sitios de operación verificados.

4) Los resultados de verificar en las áreas de operación del proceso, *"la exactitud (integridad) de la información (datos) del proceso, que pudiera presentar errores o irregularidades"* a causa de las debilidades o deficiencias de control identificadas en la *evaluación del diseño y efectividad de controles por riesgo,* es decir, para los riesgos inherentes que presentaron resultados "No Satisfactorios" en la evaluación de controles. Por cada sitio de operación se entrega un informe con: a) La opinión

de la auditoría sobre la exactitud de la información del proceso; b) por cada evento de riesgo inherente con debilidades de control, el porcentaje de exactitud de los datos verificados según pruebas sustantivas; c) comparativos de efectividad de los controles antes y después de pruebas de cumplimiento; d) comparativos del riesgo residual antes y después de pruebas sustantivas; e) hallazgos de la auditoría para eventos de la muestra de auditoria con riesgo residual "No satisfactorio" después de pruebas sustantivas; f) motivos de las inexactitudes identificadas en la información y g) recomendaciones para mejorar la gestión del riesgos por parte de los responsables de ejecutar los controles y de elaborar y actualizar la matriz de riesgos del proceso.

5) Los resultados de medir (estimar) la satisfacción de siete (7) criterios que debe satisfacer la información de negocios generada por el proceso objeto de la auditoría. Estos son: eficacia, eficiencia, integridad, disponibilidad, confidencialidad, confiabilidad y cumplimiento con normas y regulaciones. Para el proceso, se genera una informe con: a) La opinión de la auditoría sobre la satisfacción de cada criterio de evaluación; b) el porcentaje de satisfacción de los criterios evaluados; c) hallazgos de la auditoría para criterios con resultados "No satisfactorios" (con satisfacción menor del 80%) y d) recomendaciones para mejorar la gestión del riesgos por parte de los responsables de ejecutar los controles y de elaborar y actualizar la matriz de riesgos del proceso.

2. INFORMACION VALIOSA QUE PROVEEN LAS MATRICES DE RIESGO PARA LA AUDITORIA INTERNA.

Las matrices de riesgo proveen información valiosa para desarrollar las fases de Planeación Especifica y Ejecución de las Auditorías Basadas en Riesgos, como se describe a continuación.

2.1 Para la Fase de Planeación de las Auditorías de Procesos Basadas en Riesgos.

En la fase de planeación de las auditorias Basadas en Riesgos, la Auditoría debe seleccionar y analizar en profundidad una muestra de riesgos inherentes para los cuales se evaluará el control interno existente y se ejecutarán pruebas de auditoría (de cumplimiento y/o sustantivas).

TEMA: EVALUACION DE LA GESTION DE RIESGOS EN LAS AUDITORIAS BASADAS EN RIESGOS

Para esta fase de la Auditoría, las matrices de riesgo proveen los siguientes datos:

Por cada proceso.

1) Enunciados o descripción o al menos una lista de los eventos de riesgo inherente negativos que podrían presentarse en cada proceso.

2) Documentación del análisis realizado a cada uno de los eventos de riesgos que podrían presentarse en cada proceso, ANTES DE CONTROLES. Como mínimo, por cada evento de riesgo, los siguientes resultados: a) Lista o descripción de los activos impactados (tangibles e intangibles) y su valor monetario estimado; lista o descripción de los agentes generadores del riesgo; descripción de las causas del riesgo (vulnerabilidades o debilidades de control o ausencia de controles que podrían ser explotadas por los agentes generadores del riesgo); Porcentaje del Factor de Exposición al Riesgo (FE); Frecuencia Anual de Ocurrencia (FAO) estimada; Valor estimado de las pérdidas por cada ocurrencia (PS: pérdida simple); Pérdida Anual Estimada (PAE); fuentes del riesgo (actividades del proceso y áreas de la empresa o terceros en donde puede originarse el riesgo), dueño del riesgo.

3) Evaluación o calificación de la ***Severidad*** de cada uno de los eventos de riesgo inherente identificados para el proceso (**E**: Extremo; **A**: Alto; **M**: Moderado ó **B**: Bajo), ANTES DE CONTROLES, según su ubicación en las celdas de la ***matriz de riesgos inherentes*** . Normalmente es una matriz de 5x5; en el eje horizontal se colocan cinco (5) valores cualitativos del impacto estimado de los riesgos para el horizonte de tiempo de un año; en el eje vertical se colocan cinco (5) valores cualitativos de la probabilidad de ocurrencia del riesgo. Las celdas de la matriz tienen colores asociados a cada nivel de severidad de los riesgos, así: Extrema (E), color rojo; Alta (A), color naranja; Moderada (M), color amarillo; y Baja (B), color verde. Finalmente, dentro de las celdas de la matriz, se colocan números arábigos separados por comas, los cuales identifican a los riesgos del proceso.

2.2 Para la Fase de Ejecución de la Auditoría: Evaluación del Control Interno Existente y diseño de pruebas de Auditoria.

La auditoría debe evaluar el control interno existente (diseño y efectividad), como base para determinar la naturaleza y extensión de las pruebas de auditoría requeridas. Para este fin, las matrices de riesgo proveen:

TEMA: EVALUACION DE LA GESTION DE RIESGOS EN LAS AUDITORIAS BASADAS EN RIESGOS

Por cada proceso.

1) La descripción de los controles o al menos una lista de controles implantados y tratamientos en proceso de implantación para cada uno de los riesgos inherentes del proceso. Por cada control la descripción de sus atributos (tipo, clase, efectividad, etc).

2) La evaluación (calificación) del diseño y efectividad de los controles que actúan sobre cada evento de riesgo del proceso.

3) Documentación del análisis realizado a cada uno de los eventos de riesgos que podrían presentarse en cada proceso, DESPUES DE CONTROLES. Como mínimo, por cada evento de riesgo, los siguientes resultados después de aplicar el efecto de los controles: Porcentaje del Factor de Exposición al Riesgo (FE); Frecuencia Anual de Ocurrencia (FAO) estimada; Valor estimado de las pérdidas por cada ocurrencia (PS: pérdida simple); Pérdida Anual Estimada (PAE);

4) Evaluación (calificación) de la severidad de cada uno de los eventos de riesgo inherente DESPUES DE CONTROLES, es decir, la severidad del riesgo residual o remanente (E: Extremo; A: Alto; M: Moderado; ó B: Bajo).

5) El riesgo residual neto del proceso.

TEMA: EVALUACION DE LA GESTION DE RIESGOS EN LAS AUDITORIAS BASADAS EN RIESGOS

3. USO DE LOS DATOS DE LA MATRIZ DE RIESGOS PARA FINES DE AUDITORIA.

Los datos arriba mencionados, suministrados por las matrices de riesgos de los procesos o sistemas de información, pueden utilizarse de las siguientes maneras:

3.1 En la Planeación Especifica de las Auditorias Basadas en Riesgos.

En la Planeación de las Auditorías Basadas en Riesgos, las matrices de riesgos se utilizan como *fuente de información para seleccionar los riesgos inherentes de la muestra de riesgos que serán revisados por la auditoría de los procesos.* Por ejemplo, el tamaño de la muestra de riesgos para la auditoria puede ser de 30 riesgos y de estos, 20 se seleccionan de la matriz de riesgos y 10 son riesgos nuevos adicionados según criterio de la auditoria. La auditoría normalmente, por cada riesgo de la muestra de auditoria, revisa la calidad de los resultados del análisis del riesgo provistos por la matriz de riesgos para determinar la confiabilidad de su análisis y evaluación.

Etapa 2: Comprensión del Contexto del Proceso objeto de la Auditoria.

Los auditores deben comprender el contexto del proceso, como requisito para poder auditarlo. La matriz de riesgos puede proveer información sobre objetivos del proceso, actividades del proceso (ciclo PHVA) y activos que se manejan en el proceso.

Etapa 3: Identificación y Análisis de la Muestra de Riesgos Inherentes seleccionada para la Auditoría.

La auditoría, aplicando sus conocimientos sobre “buenas y mejores prácticas de análisis de riesgos”, debe revisar que los estándares utilizados por la Administración para el análisis de riesgos concuerden con esas buenas prácticas y que se estén aplicando correctamente.

Para los riesgos de la muestra de auditoría, seleccionados de la matriz de riesgos, la auditoría revisa la forma como se analizaron los riesgos y la confiabilidad que ofrecen los resultados documentados en la matriz de riesgos. En caso de encontrar resultados NO SATISFACTORIOS, genera hallazgos de auditoría y

recomienda acciones de mejoramiento a los encargados de la gestión de riesgos empresariales.

Para los riesgos de la muestra de auditoría que no fueron seleccionados de la matriz de riesgos, el auditor realiza el análisis utilizando una metodología similar a la empleada por los diseñadores de la matriz de riesgos u otra que este alineada con las buenas y mejores prácticas de análisis de riesgos. En caso de establecer que los riesgos tienen severidad E: Extrema o A: Alta, debe recomendar que estos riesgos se adicionen a la matriz de riesgos del proceso.

Etapa 4: Cubo de Riesgos de la Auditoria.

La matriz de riesgos puede provee información sobre los objetivos de control diseñados para cada actividad del proceso sujeto a auditoría. En este caso, la auditoría revisa la consistencia de la asociación de los riesgos inherentes con cada objetivo de control y determina su conformidad o reparos. En caso de encontrar resultados NO SATISFACTORIOS genera hallazgos de auditoría y recomienda acciones de mejoramiento a los encargados de la gestión de riesgos empresariales.

3.2 En la Ejecución de la Auditoría.

En la Evaluación del Control Interno y Diseño de Pruebas de Auditoria, las matrices de riesgo se utilizan como *fuente de información para seleccionar los controles que serán revisados por la auditoria del proceso*. La auditoría normalmente revisa el diseño, la efectividad y el cumplimiento de los controles por cada riesgo inherente de la muestra de riesgos seleccionada para la auditoría. Revisa el diseño de los controles para determinar si los controles son apropiados para neutralizar (bloquear) a los agentes de riesgo y eliminar las causas del riesgo (vulnerabilidades) que pueden ser explotadas por los agentes generadores del riesgo. Revisa la efectividad individual y colectiva de los controles por cada riesgo de la muestra de auditoría con el propósito de determinar si los controles establecidos tienen la capacidad para reducir la probabilidad y/o el impacto de los riesgos como se indica en la matriz de riesgos del proceso. Finalmente, revisa el cumplimiento de los controles por cada evento de riesgo de la muestra de

auditoria, para verificar que los controles se están ejecutando y monitoreando como está previsto en la matriz de riesgos del proceso.

Etapa 5: Evaluar el control Interno Existente.

Para cada uno de los riesgos de la muestra de auditoría, seleccionados de la matriz de riesgos, la auditoría revisa la forma como se evalúan el diseño y la efectividad individual y colectiva de los controles, aplicando criterios similares a los que utilizaron los diseñadores de la matriz de riesgos y compara los resultados obtenidos por la auditoría con los de la matriz de riesgos. En caso de encontrar desviaciones significativas o RESULTADOS NO SATISFACTORIOS, genera hallazgos de auditoría y recomienda acciones de mejoramiento a los encargados de la gestión de riesgos empresariales.

Para los riesgos de la muestra de auditoría que no fueron seleccionados de la matriz de riesgos, el auditor identifica los controles aplicables entre los que están documentados en la matriz de riesgos y luego evalúa su diseño y efectividad. En caso de encontrar que los controles son insuficientes o no son efectivos, genera hallazgos de auditoría y recomienda acciones de mejoramiento a los encargados de la gestión de riesgos empresariales.

Etapa 6: Pruebas de Cumplimiento.

En esta etapa, la auditoría aplica procedimientos y técnicas generalmente aceptados por los estándares de auditoría, para verificar el cumplimiento y operación de los controles que corresponden a los riesgos de la muestra de auditoría que presentaron resultados SATISFACTORIOS en la evaluación del control interno existente. Esta revisión comprende un periodo de tiempo hacia atrás no mayor a 6 meses.

Como resultado de las pruebas realizadas en el campo de trabajo (sitio de prueba), la auditoría mide porcentualmente el cumplimiento de los controles establecidos por cada evento de riesgo de la muestra de auditoría a la que correspondan los controles verificados. Si el porcentaje de cumplimiento es menor o igual al 80%, los resultados de las pruebas son NO SATISFACTORIOS, se generan hallazgos de auditoría y recomendaciones de acciones de mejora para las áreas administrativas a las que corresponda ejercer la acción correctiva o de mejoramiento.

TEMA: EVALUACION DE LA GESTION DE RIESGOS EN LAS AUDITORIAS BASADAS EN RIESGOS

Etapa 7: Pruebas Sustantivas.

En esta etapa, la auditoría aplica procedimientos y técnicas generalmente aceptados por los estándares de auditoría, para verificar la exactitud e integridad de los datos o información que genera el proceso y que pudiera ser impactada por las debilidades o deficiencias de control en los riesgos de la muestra de auditoría que presentaron resultados NO SATISFACTORIOS en la evaluación del control interno existente o en las pruebas de cumplimiento. Esta revisión comprende un periodo de tiempo hacia atrás no mayor a 6 meses.

Como resultado de las pruebas realizadas en el campo de trabajo (sitio de prueba), la auditoría mide porcentualmente el nivel de exactitud de los datos verificados por cada evento de riesgo de la muestra de auditoría que presentaron debilidades de control o resultados no satisfactorios en pruebas de cumplimiento. Si el porcentaje de exactitud de un dato después de las verificaciones de exactitud es menor o igual al 80%, los resultados de las pruebas son NO SATISFACTORIOS, se generan hallazgos de auditoría y recomendaciones de acciones de mejora para las áreas administrativas a las que corresponda ejercer la acción correctiva o de mejoramiento.

PROXIMA ENTREGA (Marzo 2020):