## Norma 2120 – Gestión de Riesgos

La actividad de auditoría interna debe evaluar la eficacia y contribuir a la mejora de los procesos de gestión de riesgos.

**Interpretación:**

*Determinar si los procesos de gestión de riesgos son eficaces es un juicio que resulta de la evaluación que efectúa el auditor interno que:*

- *Los objetivos de la organización apoyan a la misión de la organización y están alineados con la misma,*
- *Los riesgos significativos están identificados y evaluados,*
- *Se han seleccionado respuestas apropiadas al riesgo que alinean los riesgos con el apetito de riesgos por parte de la organización, y*
- *Se captura información sobre riesgos relevantes, permitiendo al personal, la Dirección y el Consejo cumplir con sus responsabilidades, y se comunica dicha información oportunamente a través de la organización.*

*La actividad de auditoría interna reúne la información necesaria para soportar esta evaluación mediante múltiples trabajos de auditoría. El resultado de estos trabajos, observado de forma conjunta, proporciona un entendimiento de los procesos de gestión de riesgos de la organización y su efectividad.*

*Los procesos de gestión de riesgos son monitoreados mediante actividades de administración continuas, evaluaciones independientes, o ambas.*

**Introducción**

Para cumplir esta Norma, el Director Ejecutivo de Auditoría (DEA) y los auditores internos comienzan por entender de forma clara el apetito al riesgo, así como la misión y los objetivos del negocio de la organización. También es importante tener un conocimiento completo de las estrategias de negocio de la organización y de los riesgos identificados por la Dirección.

Los riesgos pueden ser financieros, operacionales, legales/regulatorios o estratégicos. Se debería tener en cuenta la definición de gestión de riesgos incluida en el glosario de las Normas Internacionales para la Práctica Profesional de la auditoría interna, además de los marcos de referencia y modelos sobre gestión de riesgos publicados internacionalmente. Además, la Guía de Implementación de la Norma 2100 – Naturaleza del Trabajo, puede ser útil para obtener los argumentos necesarios para implementar la Norma 2120.

Como esta Norma asigna a la actividad de auditoría interna la tarea de evaluar la eficacia de los procesos de gestión de riesgos, los auditores internos generalmente tendrán que conseguir un conocimiento suficiente del entorno actual de gestión de riesgos de la organización y de las acciones correctivas que se han realizado para abordar los riesgos referidos. Es importante saber como la organización identifica, evalúa y supervisa los riesgos, antes de que los auditores internos comiencen a implementar la Norma 2120.

En su evaluación de riesgos, la actividad de auditoría interna debería tener en cuenta el tamaño, la complejidad, el ciclo de vida, la madurez, la estructura de stakeholders o grupos de interés y el entorno legal y competitivo de la organización. Cambios recientes en el entorno de la organización (por ejemplo, nuevas regulaciones, nuevos directivos, nueva estructura organizacional, nuevos procesos y nuevos productos) pueden introducir nuevos riesgos. El DEA puede también valorar la madurez de las prácticas de gestión de riesgos de la organización y determinar hasta que punto la actividad de auditoría interna puede confiar en la evaluación de riesgos de la Dirección.

Finalmente, la actividad de auditoría interna debería contar con un proceso para planificar, auditar e informar sobre problemas relacionados con la gestión de riesgos. Los auditores internos también evaluarán la gestión de riesgos durante las revisiones de aseguramiento y consultoría relacionadas con un área o proceso concreto.



**Consideraciones para la implementación**

En definitiva, con la implementación de la Norma 2120, el DEA y toda la actividad de auditoría interna deben demostrar su comprensión de los procesos de gestión de riesgos de la organización y buscar oportunidades de mejora. En las conversaciones con la alta dirección y con el Consejo, el DEA podrá valorar el apetito al riesgo, la tolerancia al riesgo y la cultura de riesgo de la organización. La actividad de auditoría interna deberá alertar a la Dirección sobre nuevos riesgos, así como sobre riesgos que no han sido adecuadamente mitigados, y proporcionar recomendaciones y planes de acción para una adecuada respuesta a los riesgos (por ejemplo, aceptar, continuar, transferir, mitigar o evitar). Adicionalmente, la actividad de auditoría interna debería obtener suficiente información para evaluar la eficacia de los procesos de gestión de riesgos de la organización.

Al revisar los planes estratégicos de la organización, el plan de negocio y las políticas, y reuniéndose con el Consejo y la alta dirección, el DEA puede obtener un conocimiento profundo para evaluar si los objetivos estratégicos de la organización respaldan y están alineados con su misión, su visión y su apetito

al riesgo. Las entrevistas con los mandos intermedios pueden proporcionar un entendimiento adicional sobre la alineación de la misión, los objetivos y el apetito al riesgo en el nivel de las unidades de negocio.

Los auditores internos deberían analizar en profundidad como la organización identifica y gestiona los riesgos, y como determina que riesgos son aceptables. La actividad de auditoría interna habitualmente evaluará las responsabilidades y los procesos relacionados con el riesgo del Consejo y de aquellos que tengan funciones clave en la gestión de riesgos. Para cumplir esto, los auditores internos pueden revisar evaluaciones de riesgos que se hayan finalizado recientemente e informes relacionados emitidos por la alta dirección, los auditores externos, reguladores y otras posibles fuentes.

Adicionalmente, la actividad de auditoría interna normalmente realizará sus propias evaluaciones de riesgo. las conversaciones con la Dirección y con el Consejo y la revisión de las políticas de la organización y de las actas de las reuniones, generalmente permitirá deducir el apetito de riesgo de la organización permitiéndole al DEA y a la actividad de auditoría interna alinear las respuestas a los riesgos recomendadas. La actividad de auditoría interna puede utilizar un marco de referencia sobre gestión de riesgos o sobre control interno ya existente (por ejemplo, el marco del Committee of Sponsoring Organizations of the Treadway Commission –COSO– o la Norma ISO 31000) para guiar su identificación de riesgos. Para mantenerse actualizada en lo referente a exposiciones a riesgos potenciales y oportunidades relacionadas con éstos, la actividad de auditoría interna puede también investigar sobre nuevos desarrollos y tendencias relacionadas con el sector de la organización, y también sobre procesos que puedan ser empleados para supervisar, evaluar y responder a los referidos riesgos y oportunidades.

Si siguen estos pasos, los auditores internos pueden desarrollar de forma independientes análisis de deficiencias para determinar si los riesgos significativos están siendo identificados y evaluados adecuadamente. De esta forma, la actividad de auditoría interna estará posicionada para evaluar el proceso de evaluación de riesgos de la Dirección. Al revisar el proceso de gestión de riesgos, es importante que los auditores internos identifiquen y debatan sobre los riesgos y las respuestas correspondientes que hayan sido elegidas. Por ejemplo, la Dirección puede elegir aceptar un riesgo, y el DEA necesitará determinar si la decisión es apropiada de acuerdo con el apetito al riesgo de la organización o la estrategia de gestión de riesgos. Si el DEA concluye que la Dirección ha aceptado un nivel de riesgos que puede ser inaceptable para la organización, el DEA debe discutir este asunto con la alta dirección y puede necesitar comunicar el tema al Consejo,

de acuerdo con la Norma 2600 – Comunicación de la Aceptación de los Riesgos. En los casos en los que la Dirección elige emplear una estrategia de mitigación en respuesta a los riesgos identificados, la actividad de auditoría interna puede evaluar, si es necesario, si las acciones correctivas son adecuadas y se han tomado en el momento oportuno. Esto se puede lograr revisando el diseño del control y probando los controles y supervisando los procedimientos.

Para evaluar si la información sobre riesgos relevantes ha sido capturada y comunicada a tiempo a toda la organización, los auditores internos pueden entrevistar a distintos niveles de la organización y determinar si los objetivos, los riesgos significativos y el apetito al riesgo constan por escrito suficientemente y son comprendidos en toda la organización. Habitualmente, la actividad de auditoría interna también evalúa lo adecuado y la oportunidad en el tiempo de los informes de la Dirección sobre los resultados de la gestión de riesgos. La actividad de auditoría interna puede revisar las actas del Consejo para determinar si los riesgos más significativos han sido comunicados a tiempo al Consejo y si éste está actuando para asegurar que la administración está respondiendo adecuadamente.

Finalmente, la actividad de auditoría interna debería dar los pasos necesarios para asegurar que está gestionando sus propios riesgos, como el riesgo de falla en las auditorías, falso aseguramiento y riesgos reputacionales. Asimismo, todas las acciones correctivas deberían ser monitoreadas.



**Consideraciones para demostrar conformidad**

Los documentos que pueden demostrar conformidad con la Norma 2120 incluyen el Estatuto de auditoría interna, que documenta las funciones y responsabilidades de la actividad de auditoría interna relacionadas con la gestión de riesgos, y el plan de auditoría interna. Adicionalmente, la conformidad puede ser evidenciada con actas de reuniones en las que se hayan discutido los elementos de la Norma, como las recomendaciones sobre gestión de riesgos realizadas por la actividad de auditoría interna, entre el DEA, el Consejo y la alta dirección, o reuniones entre la actividad de auditoría interna y los comités relevantes, equipos especiales y directivos clave.

Las evaluaciones de riesgos desarrolladas por la actividad de auditoría Interna y los planes de acción para mejorar la gestión de riesgos demuestran generalmente tanto la evaluación como la mejora de los procesos de gestión de riesgos, respectivamente.