**ISO 31000**

**Liderazgo y compromiso**

1. **Compromiso de la alta dirección**: La gestión del riesgo debe ser liderada por la alta dirección, asegurando su integración en todos los niveles organizacionales y la toma de decisiones.
2. **Asignación de roles y responsabilidades**: Debe existir una clara asignación de responsabilidades en la gestión del riesgo, con un enfoque que involucre a todas las partes interesadas de la organización.

**Integración en la estructura organizativa**

1. La gestión del riesgo debe ser parte integral de los procesos de la organización, no solo un proceso aislado. Debe ser integrada dentro de la estrategia y los objetivos de la organización, y debe ser abordada a todos los niveles de gestión.

**Establecimiento del contexto**

1. **Análisis del contexto interno y externo**: Antes de gestionar los riesgos, es esencial comprender tanto el contexto interno (factores culturales, recursos disponibles, capacidades) como el contexto externo (entorno de mercado, regulaciones, competencia).
2. **Definición de los criterios de riesgo**: La organización debe establecer los criterios que determinarán lo que se considera un riesgo aceptable, estableciendo una base para la evaluación.

**Proceso de evaluación del riesgo**

1. **Identificación de riesgos**: Los riesgos deben ser identificados en todos los niveles de la organización, utilizando métodos adecuados que incluyan la consulta con las partes interesadas.
2. **Evaluación de riesgos**: Los riesgos identificados deben ser evaluados en función de su probabilidad y su impacto potencial. La evaluación debe incluir un análisis cualitativo y cuantitativo, si es posible.
3. **Evaluación del control existente**: Evaluar los controles actuales que la organización tiene para mitigar los riesgos y determinar su efectividad.

**Tratamiento del riesgo**

1. **Opciones de tratamiento**: La organización debe definir cómo va a tratar cada riesgo, utilizando diversas estrategias:

* **Evitar**: Cambiar el plan o proceso para eliminar el riesgo.
* **Reducir**: Implementar medidas para disminuir la probabilidad o impacto del riesgo.
* **Transferir**: Asumir que el riesgo será gestionado por otra entidad (por ejemplo, seguros).
* **Aceptar**: Aceptar el riesgo si los beneficios superan el coste de mitigarlo o si es improbable que ocurra.

1. **Selección de la estrategia**: Las decisiones sobre cómo tratar cada riesgo deben estar alineadas con los objetivos organizacionales y con los recursos disponibles.

**Monitoreo y revisión**

1. **Seguimiento continuo**: La eficacia del proceso de gestión del riesgo debe ser monitoreada continuamente para asegurar que los riesgos sean gestionados de forma adecuada y que las estrategias implementadas sigan siendo efectivas.
2. **Revisión periódica**: El sistema de gestión de riesgos debe ser revisado regularmente para asegurar que se adapten a los cambios en el contexto y que sigan siendo relevantes y efectivos.
3. **Mejora continua**: Debe haber un proceso de mejora continua para asegurar que el enfoque de gestión de riesgos se ajuste con el tiempo a medida que surgen nuevos riesgos o cambian las circunstancias.

**Comunicación y consulta**

1. **Comunicación interna y externa**: La gestión del riesgo debe ser comunicada de forma clara y efectiva dentro de la organización, y también a las partes interesadas externas cuando sea relevante.
2. **Consulta con las partes interesadas**: La consulta con las partes interesadas clave (empleados, clientes, accionistas, etc.) es fundamental para garantizar que los riesgos sean entendidos de manera integral y se gestionen adecuadamente.

**Documentación y evidencia**

1. **Documentación del proceso**: Debe haber registros documentados que respalden todo el proceso de gestión del riesgo, incluidos los análisis de riesgos, las decisiones tomadas, las estrategias de mitigación aplicadas y las revisiones periódicas.
2. **Transparencia y trazabilidad**: La organización debe ser capaz de demostrar que su enfoque para gestionar el riesgo es coherente con la norma ISO 31000, y debe tener registros que demuestren que se han seguido todos los pasos adecuados del proceso.

**Mejora continua**

1. La norma establece la necesidad de evaluar y ajustar constantemente el sistema de gestión del riesgo para adaptarse a los cambios y mejorar su efectividad en la gestión de riesgos.