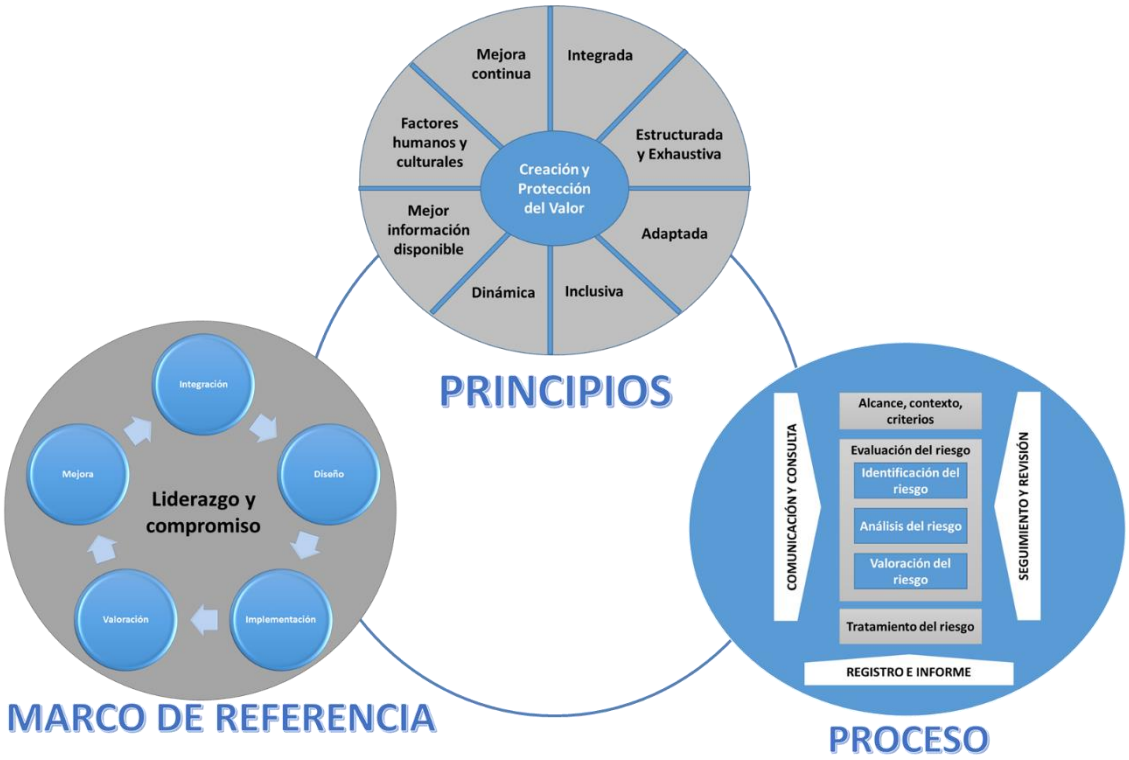
DIRECTRICES PARA LA GESTIÓN DE RIESGOS - ISO 31000:2018

PROPÓSITO DE LA GESTIÓN DE RIESGOS:

Creación y protección del valor. Mejora del desempeño, fomenta la innovación y contribuye al logro de los objetivos.



INTRODUCCIÓN:

La gestión de riesgos está dirigida a las personas que crean y protegen el valor de las organizaciones gestionando riesgos, tomando decisiones, estableciendo y logrando objetivos y mejorando el desempeño.

Las organizaciones se enfrentan a cambios producidos por factores internos y externos que hacen incierto el logro de sus objetivos.

La gestión de riesgos es una herramienta clave para la toma de decisiones que permite apalancar el cumplimiento de los objetivos asociados con la estrategia. Asiste a las organizaciones a establecer su estrategia, lograr sus objetivos y tomar decisiones informadas.

La gestión de riesgos es parte de la gobernanza y rl liderazgo y es fundamental en la manera en que se gestiona la organización en todos sus niveles, es parte de todas las actividades asociadas e incluye la interacción con las partes interesadas.

Se considera los contextos externo e interno de la organización, incluido el comportamiento humano y los factores culturales.

La gestión de riesgos está basada en los principios, el marco de referencia y el proceso.

OBJETO Y CAMPO DE APLICACIÓN:

La ISO 31000 proporciona directrices para gestionar el riesgo al que se enfrentan las organizaciones, puede adaptarse a cualquier organización y a su contexto.

Proporciona un enfoque común para gestionar cualquier tipo de riesgo y nos es específico de una industria o sector.

Puede utilizarse a lo largo de la vida de la organización y puede aplicarse a cualquier actividad, incluyendo la toma de decisiones a todos los niveles.

REFERENCIAS NORMATIVAS

No contiene

TÉRMINOS Y DEFINICIONES:

Riesgo:

Efecto de la incertidumbre sobre los objetivos.

- Un efecto es una desviación con respecto a lo previsto. Puede ser positivo, negativo o ambos, y puede abordar, crear o resultar en oportunidades y amenazas.
- Los objetivos pueden tener diferentes aspectos y categorías, y se pueden aplicar a diferentes niveles
- Con frecuencia el riesgo se expresa en términos de fuentes de riesgo, eventos potenciales, sus consecuencias y probabilidades.

Gestión del riesgo

Actividades coordinadas para dirigir y controlar la organización con relación al riesgo.

Parte interesada:

Persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad.

Fuente de riesgo:

Elemento que, por sí solo o en combinación con otros, tiene el potencial de generar riesgo.

Evento:

Ocurrencia o cambio de un conjunto particular de circunstancias

- Un evento puede tener una o más ocurrencias y puede tener varias causas y consecuencias
- Un evento puede ser algo previsto que no llega a ocurrir, o algo previsto que ocurre.
- Un evento puede ser una fuente de riesgo.

Consecuencia:

Resultado de un evento que afecta a los objetivos

- Una consecuencia puede ser cierta o incierta y puede tener efectos positivos o negativos, directo o indirecto sobre los objetivos.
- Las consecuencias se pueden expresar de manera cualitativa o cuantitativa
- Cualquier consecuencia puede incrementarse por efecto cascada o acumulativo

Probabilidad:

Posibilidad de que algo suceda, esté definida, medida o determinada objetiva o subjetivamente, cualitativa o cuantitativamente, y descrita en términos generales o matemáticos

Control:

Medida que mantiene y/o modifica un riesgo

- Los controles incluyen, pero no se limitan a cualquier proceso, política, dispositivo, práctica u otras condiciones y/o acciones que mantengan y/o modifiquen un riesgo.
- Los controles no siempre pueden proporcionar el efecto de modificación previsto o asumido.

4. PRINCIPIOS

Proporcionan orientación sobre las características de una gestión del riesgo eficaz y eficiente, comunicando su valor y explicando su propósito.

Principios – Fundamento de la gestión del riesgo:

1. **Integrada:** es parte integral de todas las actividades de la organización.
2. **Estructurada y exhaustiva:** este enfoque contribuye a resultados coherentes y comparables.
3. **Adaptada:** El marco de referencia y el proceso de la gestión del riesgo se adaptan y son proporcionales a los contextos externo e interno de la organización relacionados con sus objetivos.
4. **Inclusiva:** La participación apropiada y oportuna de las partes interesadas permite que se consideren su conocimiento, puntos de vista y percepciones. Esto resulta en una mayor toma de conciencia y una gestión de riesgo informada.
5. **Dinámica:** Los riesgos pueden aparecer, cambiar o desaparecer con los cambios del contexto. La gestión del riesgo anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna.
6. **Mejor información disponible:** Las entradas a la gestión del riesgo se basan en información histórica y actualizada, así como en expectativas futuras, se tiene en cuenta cualquier limitación e incertidumbre asociada con tal información y expectativas. La información debería ser oportuna, clara y disponible para las partes interesadas.
7. **Factores humanos y culturales:** influyen considerablemente en todos los aspectos de la gestión del riesgo en todos los niveles y etapas.

8. **Mejora continua:** proceso recurrente de optimización mediante aprendizaje y experiencia.

5. MARCO DE REFERENCIA:

5.1 Generalidades

El propósito del marco de referencia es asistir a la organización a integrar la gestión del riesgo en todas sus actividades y funciones significativas.

La eficacia dependerá de su integración en la gobernanza de la organización, incluyendo la toma de decisiones. Esto requiere el apoyo de las partes interesadas, particularmente la alta dirección.

Implica: integrar, diseñar, implementar, valorar y mejorar la gestión del riesgo a lo largo de toda la organización.

5.2 Liderazgo y compromiso:

La alta dirección y los órganos de supervisión, deberían asegurar que la gestión del riesgo esté integrada en todas las actividades de la organización y deberían demostrar liderazgo y compromiso:

- Adaptando e implementando los componentes del marco de referencia
- Publicando una declaración o una política que establezca un enfoque, un plan o línea de acción para la gestión del riesgo
- Asegurando los recursos necesarios
- Asignando autoridad, responsabilidad y obligación de rendir cuentas en los niveles apropiados de la organización

Esto ayudará a:

Alinear la gestión del riesgo con sus objetivos, estrategia y cultura

Reconocer y abordar todas las obligaciones, así como los compromisos voluntarios

Establecer la magnitud y el tipo de riesgo que puede o no ser tomado para guiar el desarrollo de los criterios del riesgo.

Comunicar el valor de la gestión del riesgo

Promover el seguimiento sistemático de los riesgos

Asegurarse de que el marco de referencia permanezca apropiado al contexto de la organización

La alta dirección rinde cuentas por gestionar el riesgo

Los órganos de supervisión rinden cuentas por la supervisión de los riesgos, se espera o se requiere que:

- Se aseguren que los riesgos se consideran apropiadamente cuando se establezcan los objetivos
- Comprendan los riesgos a los que hace frente la organización en la búsqueda de sus objetivos

- Se aseguren que los sistemas para gestionar los riesgos se implementan y operan eficazmente
- Se aseguren que los riesgos son apropiados en el contexto de los objetivos de la organización
- Se aseguren de que la información sobre estos riesgos y gestión se comunique de manera apropiada

5.3 Integración

La integración de la gestión del riesgo depende de la comprensión de las estructuras y el contexto de la organización. Las estructuras difieren dependiendo del propósito, las metas y la complejidad de la organización. El riesgo se gestiona en cada parte de la estructura. Todos los miembros de la organización tienen la responsabilidad de gestionar el riesgo.

La gobernanza guía el curso de la organización, sus relaciones externas e internas y las reglas, los procesos y prácticas para alcanzar el propósito. La estructura convierte la orientación de la gobernanza en la estrategia y los objetivos asociados. La determinación de los roles para la rendición de cuentas y la supervisión de la gestión del riesgo dentro de la organización son partes integrales de la gobernanza de la organización

La integración de la gestión del riesgo es un proceso dinámico y se debería adaptar a las necesidades y cultura de la organización. Debería ser parte del propósito, gobernanza, liderazgo, estrategia, objetivos y operaciones.

5.4 Diseño

5.4.1 Comprensión de la organización y su contexto

La organización debería analizar y comprender sus contextos externo e interno cuando diseñe el marco de referencia para gestionar el riesgo

El análisis del contexto externo puede incluir:

- Factores sociales, culturales, políticos, legales, reglamentarios, financieros, tecnológicos, económicos y ambientales, ya sea a nivel internacional, nacional, regional o local.
- Impulsores y tendencias que afectan los objetivos de la organización
- Las relaciones, percepciones, valores, necesidades y expectativas de las partes interesadas externas
- Las relaciones contractuales y los compromisos
- La complejidad de las redes y dependencias

El análisis del contexto interno puede incluir:

- Visión, misión y valores
- Gobernanza, estructura, roles y rendición de cuentas
- Estrategia, objetivos y políticas
- Cultura de la organización
- Normas, directrices y modelos adoptados por la organización

- Las capacidades en términos de recursos y conocimientos (capital, tiempo, personas, propiedad intelectual, procesos, sistemas y tecnologías)
- Los datos, sistemas de información, flujos de información
- Relaciones con partes interesadas internas, teniendo en cuenta sus percepciones y valores
- Relaciones contractuales y compromisos
- Interdependencias e interconexiones

5.4.2 Articulación del compromiso con la gestión del riesgo

La alta dirección y los organismos de supervisión deberían articular y demostrar su compromiso continuo con la gestión del riesgo mediante una política, el compromiso debería incluir:

- El propósito de la organización para gestionar el riesgo y los vínculos con sus objetivos
- La necesidad de integrar la gestión del riesgo en la cultura de la organización
- El liderazgo en la integración de la gestión del riesgo en las actividades y toma de decisiones de la organización
- Las autoridades, responsabilidades y la obligación de rendir cuentas
- La disponibilidad de los recursos necesarios
- La manera de manejar los objetivos en conflicto
- Medición e informe como parte de los indicadores de desempeño de la organización
- La revisión y mejora

El compromiso se debería comunicar dentro de la organización y a las partes interesadas de manera apropiada

5.4.3 Asignación de roles, autoridades, responsabilidades y obligación de rendir cuentas en la organización

Se debería asegurar que se asignen y comuniquen a todos los niveles de la organización y deberían:

- enfatizar que la gestión del riesgo es una responsabilidad principal
- identificar a las personas que tienen asignada la obligación de rendir cuentas y la autoridad para gestionar el riesgo (dueños del riesgo)

5.4.4 Asignación de recursos

Deberían asegurar la asignación de los recursos apropiados para la gestión de riesgo:

- Las personas, habilidades, experiencia y competencias
- Procesos, métodos y herramientas
- Procesos y procedimientos documentados
- Sistemas de gestión de la información y del conocimiento
- El desarrollo profesional y las necesidades de formación

La organización debería considerar las competencias y limitaciones de los recursos existentes

5.4.5 Establecimiento de la comunicación y consulta

La organización debería establecer un enfoque aprobado con relación a la comunicación y consulta, para apoyar el marco de referencia y facilitar la aplicación eficaz.

La comunicación implica compartir información con el público objetivo

La consulta implica que los participantes proporcionen retroalimentación.

Deberían ser oportunas y asegurar que se recopile, consolide y comparta la información pertinente, cuando sea apropiado, y que se proporcione retroalimentación y se lleven a cabo las mejoras

5.5 Implementación

La organización debería implementar el marco de referencia de la gestión del riesgo mediante:

- El desarrollo de un plan apropiado incluyendo plazos y recursos
- La identificación de dónde, cuándo, cómo y quién toma diferentes tipos de decisiones en toda la organización
- La modificación de los procesos aplicables para la toma de decisiones
- El aseguramiento de que las disposiciones de la organización para gestionar el riesgo son claramente comprendidas y puestas en práctica

La implementación con éxito requiere el compromiso y toma de conciencia de las partes interesadas.

5.6 Valoración

Para valorar la eficacia del marco de referencia de la gestión del riesgo, la organización debería

- Medir periódicamente el desempeño del marco de referencia con relación a su propósito, sus planes, sus indicadores y el comportamiento esperado
- Determinar si permanece idóneo para apoyar el logro de los objetivos de la organización

5.7 Mejora

5.7.1 Adaptación

Realizar seguimiento continuo y adaptar el marco de referencia en función a los cambios externos e internos.

5.7.2 Mejora continua

La organización debería mejorar continuamente la idoneidad, adecuación y eficacia del marco de referencia de la gestión del riesgo. Cuando se identifiquen brechas u oportunidades de mejora, se deberían desarrollar planes y tareas para contribuir al fortalecimiento de la gestión del riesgo.

6 PROCESO

6.1 Generalidades

Implica la aplicación sistemática de políticas, procedimientos y practicas a las actividades de comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registro e informe del riesgo.

El proceso de gestión del riesgo debería ser una parte integral de la gestión y de la toma de decisiones. Puede aplicarse a nivel estratégico, operacional, de programa o de proyecto.

6.2 Comunicación y consulta

El propósito es asistir a las partes interesadas pertinentes a comprender el riesgo, las bases con las que se toman decisiones y las razones por las que son necesarias acciones específicas. La comunicación busca promover la toma de conciencia y la comprensión del riesgo, mientras que la consulta implica obtener retroalimentación e información para apoyar la toma de decisiones.

La comunicación y consulta con las partes interesadas apropiadas, externas e internas, se debería realizar en todas las etapas del proceso de la gestión del riesgo

Pretende:

- Reunir diferentes áreas de experiencia para cada etapa del proceso
- Considerar de manera apropiada los diferentes puntos de vista cuando se definen los criterios del riesgo y cuando se valoran
- Proporcionar suficiente información para facilitar la supervisión del riesgo y la toma de decisiones
- Construir un sentido de inclusión y propiedad entre las personas afectadas por el riesgo

6.3 Alcance, contexto y criterios

6.3.1 Generalidades

El propósito es adaptar el proceso de la gestión del riesgo, para permitir una evaluación del riesgo eficaz y un tratamiento apropiado del riesgo.

6.3.2 Definición del alcance

Definir el alcance de sus actividades de gestión del riesgo

Como el proceso de gestión de riesgos puede aplicarse a niveles distintos (por ejemplo: estratégico, operacional, de programa, de proyecto u otras actividades) es importante tener claro el alcance considerado, los objetivos pertinentes a considerar y su alineamiento con los objetivos de la organización.

En la planificación del enfoque se incluyen las siguientes consideraciones:

Objetivos y decisiones que se necesitan tomar

Los resultados esperados de las etapas a ejecutar en el proceso

El tiempo, la ubicación, inclusiones y exclusiones específicas

Herramientas y técnicas apropiadas de evaluación del riesgo

Recursos requeridos, responsabilidades y registros a conservar

Las relaciones con otros proyectos, procesos y actividades

6.3.3 Contextos externo e interno

Entorno en el cual la organización busca definir y lograr sus objetivos.

Comprender el contexto y reflejar el entorno especifico de la actividad en la cual se va a aplicar el proceso de gestión del riesgo

6.3.4 Definición de los criterios del riesgo

La organización debería precisar la cantidad y el tipo de riesgo que puede o no tomar, con relación a los objetivos.

Definir los criterios para valorar la importancia del riesgo y para apoyar los procesos de toma de decisiones.

Los criterios se deberían definir considerando las obligaciones de la organización y los puntos de vista de las partes interesadas

Los criterios son dinámicos y deben revisarse continuamente y si fuese necesario, modificarse

- Se debería considerar
  La naturaleza y los tipos de las incertidumbre que pueden afectar a los resultados y objetivos (tanto tangibles como intangibles)
- Cómo se van a definir y medir las consecuencias (tanto positivas como negativas) y la probabilidad
- Los factores relacionados con el tiempo
- La coherencia en el uso de las mediciones
- Cómo se va a determinar el nivel de riesgo
- Cómo se tendrán en cuenta las combinaciones y las secuencias de múltiples riesgos
- La capacidad de la organización

6.4 Evaluación del riesgo

6.4.1 Generalidades

Proceso global de identificación, análisis y valoración del riesgo.
La evaluación del riesgo se debería llevar a cabo de manera sistemática, iterativa y colaborativa, basándose en el conocimiento, puntos de vista de las partes interesadas. Se debería utilizar la mejor información disponible, complementada por investigación adicional si fuese necesario

6.4.2 Identificación del riesgo

El propósito es encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a una organización lograr sus objetivos

Para la identificación de los riesgos es importante contar con información pertinente, apropiada y actualizada

La organización puede utilizar un rango de técnicas para identificar incertidumbres que puedan afectar los objetivos. Se deberían considerar los siguientes factores:

Fuentes de riesgo tangibles e intangibles

Causas y eventos

Amenazas y oportunidades

Vulnerabilidades y capacidades

Cambios de contexto

Indicadores de riesgos emergentes

La naturaleza y el valor de los activos y los recursos

Consecuencias e impactos en los objetivos

Limitaciones de conocimiento y confiabilidad de la información

Factores relacionados con el tiempo

Sesgos, creencias y supuestos de las personas involucradas

La organización debería identificar los riesgos, tanto si sus fuentes están o no bajo su control.

6.4.3 Análisis del riesgo

Comprender la naturaleza del riesgo y sus características incluyendo, cuando sea apropiado, el nivel del riesgo. Implica una consideración detallada de incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su eficacia. Un evento puede tener múltiples causas y consecuencias y puede afectar múltiples objetivos.

El análisis del riesgo se puede realizar con diferentes grados de detalle y complejidad, dependiendo del propósito del análisis, la disponibilidad y confiabilidad de la información y recursos disponibles.

Las técnicas de análisis pueden ser cualitativas, cuantitativas o una combinación de éstas.

Debería considerar:

Probabilidad de los eventos y consecuencias

Naturaleza y magnitud de las consecuencias

La complejidad y la interconexión

La eficacia de los controles existentes

Niveles de sensibilidad y de confianza

El análisis del riesgo puede estar influenciado por cualquier divergencia de opiniones, sesgos, percepciones y juicios. Las influencias adicionales son la calidad de la información utilizada, los supuestos y las exclusiones.

El análisis del riesgo proporciona una entrada para la valoración del riesgo, para las decisiones de tratamiento de los riesgos.

6.4.4 Valoración del riesgo

El propósito es apoyar la toma de decisiones, implica comparar los resultados del análisis del riesgo con los criterios del riesgo. Esto puede conducir a una decisión de:

No hacer nada más

Considerar opciones para el tratamiento del riesgo

Realizar un análisis adicional para una mejor comprensión

Mantener los controles existentes

Reconsiderar los objetivos

Las decisiones deberían tener en cuenta un contexto más amplio y las consecuencias reales y percibidas por las partes interesadas

Los resultados de la valoración se deberían registrar, comunicar y luego validar a los niveles apropiados de la organización

6.5 Tratamiento del riesgo

6.5.1 Generalidades

Seleccionar e implementar opciones para abordar el riesgo

Implica un proceso iterativo de:

Formular y seleccionar opciones para el tratamiento del riesgo

Planificar e implementar el tratamiento del riesgo

Evaluar la eficacia de ese tratamiento

Decidir si el riesgo residual es aceptable

Si no es aceptable, efectuar tratamiento adicional.

6.5.2 Selección de las opciones para el tratamiento del riesgo

La selección de las opciones más apropiadas para el tratamiento del riesgo implica hacer un balance entre los beneficios potenciales, derivados del logro de los objetivos contra los costos, esfuerzos o desventajas de la implementación.

Las opciones de tratamiento no necesariamente son mutuamente excluyentes o apropiadas en todas las circunstancias.

Opciones:

Evitar el riesgo decidiendo no iniciar o continuar con la actividad que genera el riesgo

Aceptar o aumentar el riesgo en busca de una oportunidad

Eliminar la fuente del riesgo

Modificar la probabilidad

Modificar las consecuencias

Compartir el riesgo (por ejemplo: contratos, compras de seguros)

Retener el riesgo con base en una decisión informada

La justificación para el tratamiento del riesgo es más amplia que las simples consideraciones económicas y debería tener en cuenta todas las obligaciones de la organización, compromisos y puntos de vista de las partes interesadas.

La selección de las opciones debería realizarse de acuerdo con los objetivos, criterios y recursos disponibles

El seguimiento y la revisión necesitan ser parte integral de la implementación del tratamiento para asegurar la eficacia

Si no hay opciones disponibles para el tratamiento o si el tratamiento no modifica el riesgo, éste se debería registrar y mantener en continua revisión

El riesgo residual se debería documentar y ser objeto de seguimiento, revisión y cuando sea apropiado de tratamiento adicional.

6.5.3 Preparación e implementación de los planes de tratamiento de riesgo

El propósito es especificar la implementación de las opciones elegidas para el tratamiento, de tal manera que los involucrados comprendan las disposiciones y que pueda realizarse el seguimiento del avance respecto de lo planificado.

Los planes de tratamiento deberían integrarse en los planes y procesos de la gestión de la organización, en consulta con las partes interesadas apropiadas

La información proporcionada en el plan de tratamiento debería incluir:

El fundamento de la selección de las opciones para el tratamiento incluyendo los beneficios esperados

Las personas que rinden cuentas y aquellas responsables de la aprobación e implementación del plan

Acciones propuestas

Recursos necesarios

Medidas del desempeño

Restricciones

Informes y seguimientos requeridos

Plazos previstos

6.6 Seguimiento y revisión

Asegurar y mejorar la calidad y la eficacia del diseño, la implementación y los resultados del proceso. Seguimiento continuo y la revisión periódica del proceso de la gestión del riesgo y sus resultados.

El seguimiento y la revisión deberían tener lugar en todas etapas del proceso.

6.7 Registro e informe

El proceso de la gestión del riesgo y sus resultados se deberían documentar e informar a través de los mecanismos apropiados.

El informe es una parte integral de la gobernanza y debería mejorar la calidad del diálogo con las partes interesadas, apoyar a la alta dirección y a los organismos de supervisión a cumplir sus responsabilidades. Los factores a considerar incluyen:

Partes interesadas, necesidades y requisitos específicos de información
Costos, frecuencia y los tiempos del informe
Método del informe
Pertinencia de la información con respecto a los objetivos de la organización y la toma de decisiones