NORMA MERCOSUR

NM ISO/TR 31004:2016

Primer edición / *Primeira edição*
2016-08-20

Gestión del riesgo - Guía para la implantación de la ISO 31000 (ISO/TR 31004:2013, IDT)

Gestão de riscos - Guia para a implementação da ISO 31000 (ISO/TR 31004:2013, IDT)

ASOCIACIÓN MERCOSUR DE NORMALIZACIÓN

Número de referencia
NM ISO/TR 31004:2016

Índice

Sumário

Prefacio

La AMN - Asociación MERCOSUR de Normalización - tiene por objeto promover y adoptar las acciones para la armonización y la elaboración de las Normas en el ámbito del Mercado Común del Sur - MERCOSUR, y está integrada por los Organismos Nacionales de Normalización de los países miembros.

La AMN desarrolla su actividad de normalización por medio de los CSM - Comités Sectoriales MERCOSUR - creados para campos de acción claramente definidos.

Las Normas MERCOSUR son elaboradas en acuerdo con las reglas dadas en las Directivas AMN, Parte 2.

Los Proyectos de Norma MERCOSUR, elaborados en el ámbito de los CSM, circulan para votación nacional por intermedio de los Organismos Nacionales de Normalización de los países miembros.

La homologación como Norma MERCOSUR por parte de la Asociación MERCOSUR de Normalización requiere la aprobación por consenso de sus miembros.

Esta Norma fue elaborada por el Comisión Especial MERCOSUR CE 90:06 - Gestión de Riesgos.

El texto base del Proyecto de Norma de la ISO/TR 31004 fue elaborado por Uruguay y tuvo su origen (traducción) en la norma ISO/TR 31004:2013 *Risk management - Guidance for the implementation of ISO 31000*.

Se solicita atención a la posibilidad de que algunos elementos de este documento puedan ser objeto de derechos de patente. La AMN no es responsable por la identificación de cualquier o tales derechos de patente.

Prefácio

A AMN - Asociación MERCOSUR de Normalización - tem por objetivo promover e adotar as ações para a harmonização e a elaboração das normas no âmbito do Mercado Comum do Sul - MERCOSUL, e é integrada pelos Organismos Nacionais de Normalização dos países membros.

A AMN desenvolve sua atividade de normalização por meio dos CSM - Comitês Setoriais MERCOSUL - criados para campos de ação claramente definidos.

Normas MERCOSUL são elaboradas de acordo com as regras dadas nas Diretivas AMN, Parte 2.

Os Projetos de Norma MERCOSUL, elaborados no âmbito dos CSM, circulam para votação nacional por intermédio dos Organismos Nacionais de Normalização dos países membros.

A homologação como Norma MERCOSUL por parte da Asociación MERCOSUR de Normalización requer a aprovação por consenso de seus membros.

Esta Norma foi elaborada pela Comissão Especial MERCOSUL CE 90:06 - Gestão de Riscos.

O texto-base do Projeto de Norma da ISO/TR 31004 foi elaborado pelo Brasil e teve origem (tradução) na ISO/TR 31004:2013 *Risk management - Guidance for the implementation of ISO 31000*.

Solicita-se atenção para a possibilidade de que alguns elementos deste documento possam ser objetos de direitos de patente. A AMN não é responsável pela identificação de qualquer ou tais direitos de patente.

Prefacio ISO

La Organización Internacional de Normalización (ISO) es una federación mundial de organismos nacionales de normalización (organismos miembros de ISO). El desarrollo de normas internacionales generalmente se realiza a través de comités técnicos. Cada organismo miembro que esté interesado en un tema en particular para el cual se haya establecido un comité técnico tiene derecho de estar representado en ese comité. Organizaciones internacionales, gubernamentales y no gubernamentales, en colaboración con ISO, también toman parte en el trabajo. En el campo de la normalización electrotécnica, ISO colabora con la Comisión de Electrotecnia Internacional (IEC).

Las normas internacionales se elaboran de acuerdo a las reglas dadas en la Directiva ISO/IEC, parte 2.

La tarea principal de los comités técnicos es la de preparar normas internacionales. Los proyectos de normas internacionales adoptadas por los comités técnicos son circulados a los organismos nacionales y sometidos a votación. La publicación como norma internacional requiere la aprobación de al menos el 75% de los organismos nacionales.

Es importante señalar la posibilidad de que algunos elementos de esta norma internacional pueden estar sujetos a derechos de patente. ISO no es responsable de la identificación de alguno o todos esos derechos de patentes.

La ISO/TR 31004 fue preparada por el Comité de Gestión Técnica de ISO responsable por la gestión del Grupo de Trabajo sobre Gestión de riesgos.

Prefácio ISO

A ISO (Organização Internacional para Normalização) é uma federação mundial de organismos nacionais de normalização (membros da ISO). O trabalho de preparação de Normas Internacionais é normalmente realizado pelos comitês técnicos da ISO. Cada organismo membro interessado num assunto, para o qual um comitê técnico tenha sido estabelecido, tem o direito de estar representado no comitê em questão. Organizações internacionais que mantenham ligações com a ISO, sejam elas governamentais ou não governamentais, também participam do trabalho. A ISO tem como colaboradora próxima a Comissão Eletrotécnica Internacional (IEC) a respeito de toda a normalização eletrotécnica.

As normas internacionais são elaboradas de acordo com as regras estabelecidas na ISO/IEC Diretiva, Parte 2.

A tarefa principal dos comitês técnicos é elaborar Normas Internacionais. Os projetos de Normas Internacionais adotados pelos comitês técnicos são distribuídos aos organismos membros para votação. A publicação como Norma Internacional requer aprovação de pelo menos 75% dos organismos membros com direito a voto.

Atenção para a possibilidade de que alguns dos elementos deste documento podem ser objeto de direitos de patente. A ISO não deve ser considerada responsável pela identificação de quaisquer direitos de patente.

A ISO/TR 31004 foi elaborada pela Comissão Técnica ISO responsável pela gestão do Grupo de Trabalho sobre gestão de riscos.

Introducción

0.1 Generalidades

Las organizaciones utilizan varios métodos para gestionar el efecto de la incertidumbre en el logro de sus objetivos, por ejemplo la gestión del riesgo, identificando y comprendiendo los riesgos, y tratándolos cuando sea necesario.

La intención de este Informe Técnico es asistir a las organizaciones en la mejora de la eficacia de los esfuerzos empleados en la gestión del riesgo alineándola con la ISO 31000:2009. La ISO 31000 provee de un enfoque genérico de la gestión del riesgo que puede ser aplicado por todas las organizaciones para ayudarlas a alcanzar sus objetivos.

La intención de este Informe Técnico es que sea utilizado en las organizaciones por aquellos que toman las decisiones que impactan en el logro de los objetivos, incluyendo aquellos responsables de la gobernanza y aquellos que proveen de asesoramiento y servicio de soporte para la gestión del riesgo. Es intención de este Informe Técnico que sea utilizado por cualquier persona interesada en los riesgos y su gestión, incluyendo los profesores, estudiantes, legisladores y reguladores.

La intención de este Informe Técnico es que sea leído conjuntamente con la ISO 31000 siendo el mismo aplicable a las organizaciones de cualquier tipo y tamaño. Los conceptos y definiciones básicas que son centrales para la comprensión de la ISO 31000 se explican en el Anexo A.

El Capítulo 3 provee una metodología genérica para ayudar a las organizaciones en la transición de los mecanismos de gestión del riesgo para que se alinee con la ISO 31000, de una forma planificada y estructurada. También provee de un ajuste dinámico tal como los cambios que ocurren en el contexto interno y externo de la organización.

En los Anexos adicionales se provee de guías, ejemplos y explicaciones sobre la implantación de algunos aspectos seleccionados de la ISO 31000, de forma de asistir a los lectores de acuerdo a sus habilidades y necesidades.

Los ejemplos provistos en este Informe Técnico podrían ser o no directamente aplicables a situaciones u organizaciones particulares, y son dados sólo con fines ilustrativos.

Introdução

0.1 Geral

Organizações usam vários métodos para gerenciar o efeito da incerteza nos seus objetivos, isto é, para gerenciar riscos, pela detecção e compreensão do risco, e modificando-o onde necessário.

Este Relatório Técnico destina-se a assistir as organizações a aumentar a eficácia dos seus esforços de gestão de riscos, pelo alinhamento com a ISO 31000:2009. A ISO 31000 fornece uma abordagem de gestão de riscos genérica que pode ser aplicada a todas as organizações para ajudar a atingir os seus objetivos.

Este Relatório Técnico destina-se a ser utilizado por aqueles que, dentro das organizações, tomam decisões que impactam no alcance de seus objetivos, incluindo aqueles responsáveis pela governança e aqueles que fornecem às organizações, serviços de aconselhamento e suporte em gestão de riscos. Este Relatório Técnico também se destina a ser utilizado por qualquer pessoa interessada em riscos e em sua gestão, incluindo professores, estudantes, legisladores e reguladores.

Este Relatório Técnico destina-se a ser lido em conjunto com a ISO 31000 e é aplicável a todos os tipos e tamanhos de organização. Os conceitos centrais e definições que são fundamentais para a compreensão ISO 31000 são explicados no Anexo A.

A Seção 3 fornece uma metodologia genérica para ajudar a transição dos arranjos de gestão de riscos existentes nas organizações para alinhamento com a ISO 31000, de forma planejada e estruturada. Ela também fornece ajustes dinâmicos à medida que mudanças ocorrem no ambiente interno e externo da organização.

Anexos adicionais fornecem aconselhamento, exemplos e explicações relacionadas à implementação de determinados aspectos da ISO 31000, a fim de auxiliar os leitores de acordo com os seus conhecimentos e necessidades individuais.

Exemplos fornecidos neste Relatório Técnico podem ou não ser diretamente aplicáveis a situações ou organizações específicas, e são apenas para fins ilustrativos.

0.2 Conceptos y principios fundamentales

Ciertas palabras y conceptos son fundamentales para comprender la ISO 31000 y este Informe Técnico, y los mismos se explican en la ISO 31000:2009, Capítulo 2, y en el Anexo A.

La ISO 31000 establece una lista de once principios para la gestión eficaz del riesgo. La función de los principios es de informar y guiar en todos los aspectos del enfoque de la organización para la gestión del riesgo. Los principios describen las características de una gestión del riesgo eficaz.

Más que simplemente implementar los principios, es importante que la organización los refleje en todos los aspectos de su gestión. Los mismos sirven como indicadores del desempeño de la gestión del riesgo y fortalecen el valor para la organización de una gestión eficaz del riesgo. Ellos también tienen influencia en todos los elementos del proceso de transición descritos en este Informe Técnico, y los temas técnicos en sus Anexos. En el Anexo B se dan más detalles.

En este Informe Técnico se utilizan las expresiones “alta dirección” y “órgano de supervisión”. La alta dirección se refiere a la persona o grupo de personas que dirigen y controlan la organización al más alto nivel, mientras que el organismo de supervisión se refiere a la persona o grupo de personas que gobiernan una organización, establecen las directivas, y rinden cuentas a la alta dirección.

NOTA En algunas organizaciones, el órgano de supervisión podría ser llamado consejo de directores, junta directiva, consejo supervisor.

0.2 Conceitos e princípios básicos

Determinadas palavras e conceitos são fundamentais para a compreensão tanto da ISO 31000 quanto deste Relatório Técnico, e são explicados na Seção 2 da ISO 31000:2009 e no Anexo A.

A ISO 31000 lista onze princípios para a gestão de riscos eficaz. O papel dos princípios é informar e orientar sobre todos os aspectos da abordagem da organização para gestão de riscos. Os princípios descrevem as características de uma gestão de riscos eficaz.

Em vez de simplesmente implementar os princípios, é importante que a organização os reflita em todos os aspectos da gestão. Estes princípios servem como indicadores de desempenho da gestão de riscos e reforçam o valor para a organização de gerenciar riscos eficazmente. Eles também influenciam todos os elementos do processo de transição descritos neste Relatório Técnico, e as questões técnicas que são tratadas nos anexos. Mais informações são dadas no Anexo B.

Neste Relatório Técnico, as expressões “Alta Direção” e ”organismo de supervisão” são ambas utilizadas: “Alta Direção” refere-se à pessoa ou grupo de pessoas que dirige e controla uma organização no mais alto nível, enquanto “organismo de supervisão” refere-se à pessoa ou grupo de pessoas que governa uma organização, define direções, e a quem a Alta Direção presta contas.

NOTA Em muitas organizações, o organismo de supervisão pode ser chamado de conselho diretor, conselho de curadores, conselho de supervisão etc.

Gestión del riesgo - Guía para la implantación de la ISO 31000 (ISO/TR 31004:2013, IDT)

Gestão de riscos - Guia para a implementação da ISO 31000 (ISO/TR 31004:2013, IDT)

1 Objeto

Este Informe Técnico provee a las organizaciones de una guía para la gestión del riesgo eficaz implantando la ISO 31000. Provee de:

- un enfoque estructurado para la transición en las organizaciones de sus mecanismos de gestión del riesgo para que sean consistentes con la ISO 31000, de una forma adaptada a las características de la organización;

- una explicación de los conceptos fundamentales de la ISO 31000;

- una guía sobre los aspectos de los principios y el marco de la gestión del riesgo, que son descritos en la ISO 31000.

Este Informe Técnico puede ser utilizado por cualquier organización pública, privada, comunitaria, una asociación, un grupo o en forma individual.

NOTA Por conveniencia todos los usuarios de este Informe Técnico son incluidos en el término general de “organización”.

Este Informe Técnico no es específico para ninguna industria o sector, o para un tipo particular de riesgo, y puede ser aplicado a cualquier tipo de actividad y a todas las partes de la organización.

2 Referencias normativas

Los documentos indicados a continuación son indispensables para la aplicación de este documento. Para las referencias fechadas, se aplican solamente las ediciones citadas. Para las referencias sin fecha, se aplican las ediciones más recientes del documento normativo citado (incluyendo cualquier modificación).

NM ISO 31000:2014, Gestión del riesgo - Principios y directrices (ISO 31000:2009, IDT)

3 Implantación de la ISO 31000

3.1 Generalidades

Este Capítulo provee de una guía para aquellas organizaciones que desean alinear su enfoque y sus prácticas de gestión del riesgo con la ISO 31000 y para mantener estas prácticas alineadas de manera continua.

1 Escopo

Este Relatório Técnico fornece orientações para que as organizações gerenciem riscos de forma eficaz por meio da implementação da ISO 31000:2009. Este Relatório Técnico fornece:

- uma abordagem estruturada para as organizações na transição de seus arranjos de gestão de riscos de forma a serem consistentes com a ISO 31000, de uma maneira ajustada às características da organização;

- uma explicação sobre os conceitos básicos da ISO 31000;

- orientações sobre os aspectos dos princípios e da estrutura para gerenciar riscos descritos na ISO 31000.

Este Relatório Técnico pode ser usado por qualquer empresa pública, privada ou comunitária, associação, grupo ou indivíduo.

NOTA Por conveniência, todos os diferentes usuários deste Relatório Técnico são referidos pelo termo geral “organização”.

Este Relatório Técnico não é específico para qualquer indústria ou setor, ou para qualquer tipo de risco específico, e pode ser aplicado a todas as atividades e a todas as partes das organizações.

2 Referências normativas

Os documentos relacionados a seguir são indispensáveis à aplicação deste documento. Para referências datadas, aplicam-se somente as edições citadas. Para referências não datadas, aplicam-se as edições mais recentes do referido documento (incluindo emendas).

NM ISO 31000:2014 - Gestão de riscos - Princípios e diretrizes (ISO 31000:2009, IDT)

3 Implantação da ISO 31000

3.1 Geral

Esta Seção fornece orientações para organizações que buscam alinhar sua abordagem e práticas de gestão de riscos com a ISO 31000 e manter essas práticas alinhadas de forma contínua.

Provee de una metodología general que es adecuada para ser aplicada, de una forma planificada, por cualquier organización independientemente de la naturaleza de sus disposiciones vigentes de gestión del riesgo. Esta metodología implica lo siguiente:

- la comparación de la práctica existente con la descrita en la ISO 31000;

- la identificación de los cambios necesarios, la preparación y la implantación de un plan para realizarlos;

- el mantenimiento del seguimiento y control continuo y la revisión para asegurar la mejora presente y continua.

Esto le permite obtener a las organizaciones una comprensión de sus riesgos presentes, y asegurarse que esos riesgos son consistentes con sus actitudes frente al riesgo y sus criterios de riesgo.

Más allá de los motivos de implantar la ISO 31000, se espera que la organización sea capaz de gestionar mejor el riesgo, apoyando a sus objetivos. Todas las organizaciones gestionan los riesgos de alguna forma. Se recomienda que la estrategia para implantar la ISO 31000, reconozca como la organización ya está gestionando el riesgo.

El proceso de implantación, como se describe en 3.2, evalúa las disposiciones vigentes y, si es necesario, realiza adaptaciones y modificaciones para alinearlas con la ISO 31000.

La ISO 31000 identifica varios elementos de un marco de gestión del riesgo. Existen muchas ventajas que pueden surgir cuando los elementos del marco de gestión del riesgo se integra con la gobernanza, las funciones y los procesos de la organización. Estos se relacionan con la eficacia de la organización, la toma de decisiones y la eficiencia.

a) El marco de gestión del riesgo debería realizarse integrando sus elementos con el sistema de gestión global de la organización y la toma de decisiones, indistintamente si el sistema es formal o informal, los procesos de gestión pueden ser mejorados al referirlos a la ISO 31000.

b) La comprensión y gestión de la incertidumbre se convierte en un elemento integral en el(los) sistema(s) de gestión, estableciendo un enfoque común en la organización.

c) La implantación de un processo de gestión del riesgo puede ser proporcionalmente adaptado al tamaño y los requisitos de la organización.

Fornece uma metodologia geral que é adequada para aplicação, de maneira planejada, por qualquer organização, independente da natureza de seus atuais arranjos de gestão de riscos. Esta metodologia envolve o seguinte:

- comparar a prática atual com a descrita na ISO 31000;

- identificar o que necessita ser mudado e preparar e implementar um plano para tal;

- manter o monitoramento e análise crítica permanentes para assegurar a atualização e melhoria contínua.

Isto habilitará a organização a obter uma compreensão atualizada e abrangente de seus riscos, e assegurar que esses riscos sejam consistentes com a sua atitude perante o risco e os seus crité- rios de risco.

Independentemente do motivo para a implementação da ISO 31000, ao fazê-la, espera-se possibilitar a uma organização gerenciar melhor seus riscos, em apoio aos seus objetivos. Todas as organizações gerenciam riscos em alguma extensão. Convém que a estratégia para a implementação da ISO 31000 reconheça como uma organização já está gerenciando riscos.

O processo de implementação, conforme descrito em 3.2, irá avaliar os arranjos existentes e, se necessário, adaptá-los e modificá-los para alinhá-los com a ISO 31000.

A ISO 31000 identifica vários elementos de uma estrutura para gerenciar riscos. Há diversas vantagens que podem surgir quando os elementos desta estrutura são integrados na governança, funções e processos de uma organização. Estas relacionam-se com a eficácia organizacional, sólida tomada de decisões e eficiência.

a) Convém que a estrutura para gerenciar riscos seja realizada pela integração de seus componentes dentro do sistema global de gestão e tomada de decisões da organização, não importando se o sistema é formal ou informal; os processos de gestão existentes podem ser melhorados pela referência à ISO 31000.

b) A compreensão e a gestão da incerteza tornam-se um componente integral no(s) sistema(s) de gestão, estabelecendo uma abordagem comum para a organização.

c) A implementação do processo de gestão de riscos pode ser proporcionalmente ajustada ao tamanho e aos requisitos da organização.

d) La gobernanza (por ejemplo dirección y supervisión) de la política de gestión del riesgo, el marco de gestión del riesgo y el(los) proceso(s) pueden ser integrados en las disposiciones de la gobernanza existentes en la organización.

e) Los informes de gestión del riesgo están integrados con otros informes de gestión.

f) El desempeño de la gestión del riesgo es una parte integral del enfoque global de la gestión.

g) La integración y la conexión entre los muy frecuentemente separados campos de la gestión del riesgo de una organización (ejemplo gestión del riesgo empresarial, gestión del riesgo financiero, gestión del riesgo de proyectos, gestión del riesgo de seguridad, gestión de la continuidad del negocio, gestión de los seguros) se puede asegurar o mejorar, ya que la atención estará principalmente enfocada en el establecimiento y el logro de los objetivos de la organización, tomando en cuenta los riesgos.

h) Se mejora la comunicación de la incertidumbre y los riesgos entre los equipos de gestión y los niveles de gestión.

i) Las áreas de actividad de gestión del riesgo se centralizan en un foco común para el logro de los objetivos de la organización. Es posible que haya beneficios sociales indirectos ya que las partes interesadas externas de la organización pueden motivarse para mejorar sus respectivas actividades de gestión del riesgo.

j) El tratamiento y control de los riesgos pueden ser una parte integral de las operaciones diarias.

3.2 Cómo implantar la ISO 31000

A pesar que la ISO 31000 explica como gestionar el riesgo eficazmente, no explica como integrar la gestión del riesgo en los procesos de gestión de la organización. Aunque las organizaciones son diferentes y sus puntos de partida pueden ser diferentes, se puede aplicar en todos los casos un enfoque genérico y sistemático para la implantación.

Es conveniente que la organización determine los cambios que son necesarios en su marco de trabajo existente para la gestión del riesgo, antes de planificar e implantar esos cambios, y luego realizar el seguimiento de la eficacia del marco modificado. Esto le permitirá a la organización:

- alinear sus actividades de gestión del riesgo con los principios de eficacia de gestión del riesgo descritos en el Capítulo 3 de la ISO 31000;

- aplicar el proceso de gestión del riesgo descrito en la ISO 31000:2009, Capitulo 5;

d) A governança (isto é, direção e supervisão) da política, estrutura e processo(s) de gestão de riscos podem ser integrados nos atuais arranjos da governança organizacional.

e) O reporte da gestão de riscos é integrado com outros reportes de gestão.

f) O desempenho da gestão de riscos torna-se uma parte integral da abordagem de desempenho geral.

g) A interação e a conexão entre os frequentemente separados campos da gestão de riscos de uma organização (por exemplo, gestão de riscos corporativos, gestão de riscos financeiros, gestão de riscos em projetos, gestão da segurança, gestão da continuidade de negócios, gestão de seguros) podem ser asseguradas ou melhoradas, já que a atenção será agora prioritariamente focada na definição e no atingimento dos objetivos da organização, levando-se em conta os riscos.

h) A comunicação sobre incerteza e risco entre as equipes de gestão e os níveis gerenciais é melhorada.

i) Silos de atividades de gestão de riscos dentro da organização centram-se em atingir os objetivos organizacionais como um foco comum. Pode haver benefícios indiretos à sociedade, uma vez que as partes interessadas externas à organização podem estar motivadas a melhorar suas respectivas atividades de gestão de riscos.

j) O tratamento de riscos e os controles podem tornar-se parte integral das operações diárias.

3.2 Como implementar a ISO 31000

Embora a ISO 31000 explique como gerenciar riscos de forma eficaz, ela não explica como integrar a gestão de riscos nos processos de gestão da organização. Mesmo que as organizações sejam diferentes e os seus pontos de partida possam ser diferentes, uma abordagem de implementação genérica e sistemática é aplicável em todos os casos.

Convém que a organização determine se são necessárias mudanças na estrutura existente para gerenciar riscos antes de planejar e implementar essas mudanças, e então monitorar a eficácia contínua da estrutura alterada. Isso permitirá à organização:

- alinhar suas atividades de gestão de riscos com os princípios para gestão de riscos eficaz descritos na ISO 31000:2009, Seção 3;

- aplicar o processo de gestão de riscos descrito na ISO 31000:2009, Seção 5;

- satisfacer los atributos de una gestión del riesgo fortalecida en la ISO 31000:2009, Capítulo A.3;

- así de este modo lograr los resultados claves de la Norma ISO 31000:2009, Capítulo A.2.

Este enfoque también se aplica a las organizaciones que ya son consistentes con la ISO 31000, pero que quieren continuar con la mejora de su marco de gestión del riesgo y el proceso de gestión del riesgo como se recomienda en la ISO 31000:2009, Apartados 4.6 y 5.6.

La experiencia de otras organizaciones que gestionan tipos de riesgos similares o han pasado por procesos similares puede ayudar a todos los aspectos de la transición.

3.3 Integración de la ISO 31000 en los procesos de gestión de la organización

3.3.1 Generalidades

La ISO 31000 proporciona un marco y un proceso genérico para la gestión del riesgo en toda o parte de cualquier tipo de organización. Este Apartado provee de una guía para la integración de los elementos de la ISO 31000 en el enfoque de gestión de la organización, incluyendo sus actividades, procesos y funciones. Las organizaciones pueden elegir la integración de los conceptos con sus procesos existentes, o pueden elegir el diseño y establecimiento de un nuevo enfoque basado en la ISO 31000. Este Apartado describe los elementos claves del marco y proceso, y las acciones necesarias para una integración exitosa de estos elementos para alcanzar los objetivos de la organización. Existen muchas formas para integrar la ISO 31000 en la organización. La elección y el orden de los elementos deberían adaptarse según las necesidades de la organización y sus partes interesadas. Se debería aplicar esta guía para asegurar esta integración de apoyo a la estrategia global de gestión del negocio. Esto conduce los esfuerzos al logro de los objetivos de la organización de proteger y crear valor. Este enfoque también necesita la consideración de la cultura de la organización, así como las metodologías de gestión de proyectos y de los cambios.

Este Apartado describe los elementos claves del marco y del proceso, y las acciones necesarias para la integración exitosa de estos elementos para lograr los objetivos de la organización.

La implantación de la ISO 31000 es un proceso dinámico e iterativo. Además la implantación del marco de trabajo está interconectada con el

- satisfazer aos atributos de uma gestão de riscos avançada na ISO 31000:2009, Seção A.3;

- assim, atingir os resultados-chave da ISO 31000:2009, Seção A.2.

Essa abordagem também é aplicável a organizações que já são consistentes com a ISO 31000, mas que desejam melhorar continuamente sua estrutura e o processo para gerenciar riscos, como recomendado na ISO 31000:2009, 4.6 e 5.6.

Todos os aspectos da transição podem ser auxiliados pelo uso da experiência de outras organizações que gerenciam tipos semelhantes de riscos ou que tenham passado por um processo semelhante.

3.3 Integração da ISO 31000 nos processos de gestão da organização

3.3.1 Geral

A ISO 31000 fornece uma estrutura e um processo genérico para gerenciar riscos em toda ou em parte de qualquer tipo de organização. Esta Subseção fornece diretrizes para integrar os elementos da ISO 31000 na abordagem gerencial de uma organização, incluindo suas atividades, processos e funções. As organizações podem escolher integrar os conceitos da ISO 31000 aos seus processos existentes ou podem escolher conceber e estabelecer uma nova abordagem baseada na ISO 31000. Esta Subseção descreve os elementos centrais para a estrutura e processo, e as ações necessárias para uma integração bem-sucedida destes elementos de modo a atender aos objetivos organizacionais. Existem várias maneiras de integrar a ISO 31000 em uma organização. Convém que a escolha e a ordem dos elementos sejam ajustadas às necessidades da organização e suas partes interessadas. Convém que se tome cuidado ao aplicar estas diretrizes para assegurar que a integração suporte a estratégia global de gestão do negócio. Isto direciona o esforço para que se atenda aos objetivos da organização de proteger e criar valor. A abordagem também precisa considerar a cultura da organização, bem como as metodologias de gestão de projeto e de mudança.

Esta Subseção descreve os elementos centrais da estrutura e processo, e as ações necessárias para uma integração bem-sucedida destes elementos de modo a atender aos objetivos organizacionais.

A implementação da ISO 31000 é um processo contínuo, dinâmico e iterativo. Além disso, a implementação da estrutura é interconectada com

proceso de gestión del riesgo descrito en la Norma ISO 31000:2009, Capítulo 5. El éxito se mide tanto en términos de la integración del marco de trabajo como en términos de la mejora continua de la gestión del riesgo en toda la organización.

La integración se realiza en un contexto dinámico. La organización debería realizar el seguimiento a los cambios que se dan en el proceso de implantación y en su contexto interno y externo. Esto podría incluir la necesidad de cambios a sus criterios de riesgo.

3.3.2 Mandato y compromiso

Cualquier actividad de gestión del negocio comienza con un análisis racional y de las etapas del proceso, y un análisis de costo-beneficio. Esto es seguido por la decisión de la alta dirección y el órgano de supervisión de implantar y proveer del compromiso y los recursos necesarios.

Comúnmente, el proceso de implantación incluye lo siguiente:

a) adquisición del mandato y compromiso, si es necesario;

b) un análisis de la brecha;

c) un ajuste hecho a medida basado en las necesidades de la organización, la cultura y la creación y protección del valor;

d) la evaluación de los riesgos asociados con la transición;

e) el desarrollo de un plan de negocio:

- establecimiento de los objetivos, prioridades y métricas;

- establecimiento del caso de estudio, incluyendo la alineación con los objetivos de la organización;

- determinación del alcance, las responsabilidades de rendir cuentas, el cronograma y los recursos;

f) la identificación del contexto de la implantación, incluyendo la comunicación con las partes interesadas.

3.3.3 Diseño del marco de gestión del riesgo

3.3.3.1 Se debería evaluar los enfoques existentes de la organización para la gestión del riesgo, incluyendo el contexto y la cultura.

o processo de gestão de riscos descrito na ISO 31000:2009, Seção 5. O sucesso é medido tanto em termos da integração da estrutura, quanto em termos da melhoria contínua da gestão de riscos ao longo de toda organização.

A integração ocorre em um contexto dinâmico. Convém que a organização monitore tanto as mudanças que são causadas pelo processo de implementação quanto as mudanças nos seus contextos interno e externo. Isto pode incluir a necessidade de mudança dos seus critérios de risco.

3.3.2 Mandato e comprometimento

Qualquer atividade de gestão de negócio se inicia com uma análise da fundamentação e etapas dos processos e uma análise de custo-benefício. Isto é seguido por uma decisão da Alta Direção e do organismo de supervisão para implementar e fornecer o comprometimento e os recursos necessários.

Tipicamente, o processo de implementação inclui o seguinte:

a) estabelecimento de mandato e comprometimento, se necessário;

b) análise de deficiências (*gap analysis*);

c) adaptação e escalonamento baseados nas necessidades organizacionais, cultura e criação e proteção de valor;

d) avaliação dos riscos associada à transição;

e) desenvolvimento de um plano de negócios:

- estabelecendo objetivos, prioridades e métricas;

- estabelecendo o caso de negócios, incluindo o alinhamento aos objetivos organizacionais;

- determinando o escopo, responsabilizações, prazo e recursos;

f) identificação do contexto da implementação, incluindo comunicação com as partes interessadas.

3.3.3 Concebendo a estrutura

3.3.3.1 Convém que as abordagens existentes para a gestão de riscos na organização sejam avaliadas incluindo contexto e cultura.

a) Es importante considerar cualquier obligación legal, reglamentarias o con el cliente y los requisitos de certificación que surgen de cualquier sistema de gestión y de las normas que la organización ha elegido adoptar. La finalidad de esta etapa es permitir un diseño cuidadoso y adecuado del marco de gestión del riesgo, y del plan de implantación en sí mismo, y permite la alineación con la estructura, la cultura y el sistema de gestión general de la organización.

b) Es importante considerar tanto el proceso de gestión del riesgo utilizado como los aspectos del marco de gestión del riesgo existentes que permiten que este proceso se aplique.

c) Se recomienda establecer criterios de riesgo adecuados. Es necesario que los criterios de riesgo sean consistentes con los objetivos de la organización y estén alineados con su actitud ante el riesgo. Si se cambian los objetivos, se necesita ajustar adecuadamente los criterios de riesgo. Para una gestión del riesgo eficaz, es importante que se desarrolle los criterios de riesgo reflejando la actitud de la organización ante el riesgo y los objetivos.

Para el diseño del nuevo marco de gestión del riesgo, específicamente se debería evaluar lo siguiente:

- los principios y atributos, de acuerdo a la Norma ISO 31000;

- el marco de gestión del riesgo anterior, la evaluación debería comparar particularmente las prácticas vigentes con los requisitos de los apartados siguientes de la Norma ISO 31000:2009:

  - 4.3.2 (establecimiento de la política de gestión del riesgo);

  - 4.3.3 (responsabilidad de rendir cuentas);

  - 4.3.4 (integración con los procesos de la organización);

  - 4.3.5 (recursos);

  - 4.3.6 y 4.3.7 (establecimiento de mecanismos de comunicación y presentación de informes internos y externos)

- el proceso, la evaluación del mismo debería comparar los elementos existentes con los indicados en la Norma ISO 31000:2009, Capítulo 5, así como también los principios que conducen y proveen la racionalidad al proceso, con los principios de la Norma ISO 31000:2009, Capítulo 3 (ejemplo, cuando este proceso está siendo aplicado realmente en la toma de decisiones en todos los niveles de la organización);

a) É importante considerar quaisquer obrigações legais, regulatórias ou de clientes e requisitos de certificação que surjam de quaisquer sistemas de gestão e normas que a organização escolheu adotar. A finalidade desta etapa é permitir uma adaptação cuidadosa da concepção da estrutura para gerenciar riscos e do próprio plano de implementação, e permitir o alinhamento com a estrutura, a cultura e o sistema geral de gestão da organização.

b) É importante considerar tanto o processo para gerenciar riscos quanto os aspectos da estrutura existente para gerenciar riscos, que possibilitam que esse processo seja aplicado.

c) Convém que os critérios de risco apropriados sejam estabelecidos. Os critérios de risco precisam ser consistentes com os objetivos da organização e alinhados à sua atitude perante o risco. Se os objetivos mudam, os critérios de risco precisam ser ajustados de acordo. É importante para uma gestão de riscos eficaz que os critérios de risco sejam desenvolvidos de modo a refletir a atitude perante o risco e os objetivos da organização.

Convém que, ao conceber a nova estrutura, especificamente, seja avaliado o seguinte:

- princípios e atributos, como descrito na ISO 31000;

- a estrutura anterior, em cuja avaliação convém que se compare em particular as práticas correntes com os requisitos das seguintes subseções da ISO 31000:2009:

  - 4.3.2 (política de gestão de riscos);

  - 4.3.3 (responsabilização);

  - 4.3.4 (integração aos processos organizacionais);

  - 4.3.5 (recursos);

  - 4.3.6 e 4.3.7 (comunicação interna e externa e mecanismos de reporte);

- o processo, em cuja avaliação convém que se comparem os elementos dos processos existentes com aqueles da ISO 31000:2009, Seção 5, assim como os princípios subjacentes que direcionam e fornecem a fundamentação do processo com os princípios estabelecidos na ISO 31000:2009, Seção 3 (por exemplo, se este processo é de fato aplicado à tomada de decisões em todos os níveis):

- evaluar si los procesos existentes proveen a los que toman decisiones, de la información de riesgo que necesitan para realizar decisiones de calidad y lograr o exceder los objetivos;

- evaluar si los enfoques existentes para la gestión del riesgo logran atender de manera suficiente los riesgos interrelacionados y los riesgos que ocurren en las múltiples localidades.

3.3.3.2 Los requisitos del diseño del marco deberían ser identificados.

Sobre la base de la evaluación descrita en 3.3.3.1, la organización debería decidir sobre cuáles aspectos del enfoque de la gestión del riesgo actual:

a) podrían ser utilizados en un futuro (posible extensión a otros tipos de toma de decisiones);

b) necesitan modificación o mejora;

c) no agregan valor y es conveniente discontinuarlos.

La organización debería desarrollar, documentar y comunicar como va a gestionar el riesgo. La escala y el contenido de las normas, guías y modelos internos de la organización relacionados con el riesgo, deberían reflejar la cultura y el contexto de la organización.

Los documentos pueden establecer que:

- el riesgo se gestiona en toda la organización utilizando enfoques consistentes;

- existen diferentes niveles de responsabilidad de rendir cuentas por la gestión del riesgo;

- están claramente definidas las competencias y obligaciones de todas las personas con respecto a la responsabilidad de rendir cuentas por la gestión del riesgo;

- las partes interesadas internas y externas están involucradas, adecuadamente, a través de la comunicación y la consulta;

- se registra la información de los riesgos y de los resultados de todas las aplicaciones del proceso de gestión del riesgo, de una forma consistente y segura, con el acceso apropiado.

Se debería establecer una frecuencia para la revisión periódica de los requisitos de la organización, las herramientas, la formación y los recursos para la gestión del riesgo, si existen cambios en la organización y su contexto, o si se

- avaliar se o processo corrente fornece aos tomadores de decisão a informação de risco de que eles necessitam para tomar decisões de qualidade e atender ou superar os objetivos;

- avaliar se as abordagens existentes para gerenciar o risco abrangem suficientemente os riscos inter-relacionados e os riscos que ocorrem em múltiplos lugares.

3.3.3.2 Convém que os requisitos de concepção da estrutura sejam identificados.

Com base nas avaliações descritas em 3.3.3.1, convém que a organização decida quais aspectos da abordagem de gestão de riscos corrente:

a) poderiam continuar a ser usados no futuro (possivelmente os estendendo para outros tipos de tomada de decisões);

b) precisam de correção ou aperfeiçoamento;

c) não mais agregam valor e convém que sejam descontinuados.

Convém que a organização desenvolva, documente e comunique como irá gerenciar os riscos. Convém que o conteúdo e a escala das normas internas, diretrizes e modelos da organização relacionados à gestão de riscos reflitam a cultura e o contexto organizacional.

Os documentos podem especificar que:

- riscos são gerenciados por toda a organização usando abordagens consistentes;

- existem diferentes níveis de responsabilização para a gestão de riscos;

- as competências e deveres de todas as pessoas com responsabilização na gestão de riscos são claramente definidos;

- tanto as partes interessadas internas quanto externas são envolvidas, como apropriado, por meio de uma comunicação e consulta abrangentes;

- a informação sobre riscos e a saída de todas as aplicações do processo de gestão de riscos são registradas de maneira consistente e segura, com acesso apropriado.

Convém que também seja feita provisão para análise crítica periódica dos requisitos organizacionais, ferramentas, treinamento e recursos para gerenciar riscos, se houver mudanças subsequentes na organização e no seu

identifican ineficiencias o debilidades en el seguimiento y la revisión.

3.3.3.3 Para la fase de implantación, se debería definir el alcance, los objetivos, las metas, los recursos, los indicadores de éxito, el seguimiento y revisión de los criterios.

3.3.3.4 Se debería establecer los mecanismos de comunicación y presentación de informes internos y externos.

3.3.4 Implantación de la gestión del riesgo

Es necesario un plan detallado de implantación para asegurar que los cambios necesarios son realizados en un orden coherente y que los recursos necesarios pueden ser provistos y aplicados.

El plan se debería apoyar con los recursos necesarios para su implantación, lo que puede requerir asignaciones específicas de presupuesto, que es conveniente que sean parte del proceso de planificación.

El plan en sí mismo debería ser sujeto a la evaluación del riesgo de acuerdo a la Norma ISO 31000:2009, 5.4; y que se tomaran las acciones necesarias para el tratamiento del riesgo.

El plan debería requerir y permitir realizar el seguimiento del avance y la realización de informes a la alta dirección y al órgano de supervisión. Debería establecerse una frecuencia periódica para la revisión del plan.

Por lo tanto el plan debería:

- detallar las acciones específicas a realizar, su secuencia, responsables, y el plazo para su finalización: éstas incluirán modificaciones de las normas y guías internas, las explicaciones y la capacitación para lograr las competencias, y los ajustes en las responsabilidades de rendir cuentas;

- identificar cualquier acción que sea implementada como parte de acciones mayores asociadas con el desarrollo organizacional , o que estén relacionadas (por ejemplo: el desarrollo de material de formación y los facilitadores);

- definir los responsables de la implantación;

- incorporar mecanismos para el informe de finalización, el progreso y los problemas;

- identificar y registrar los criterios que desencadenan la revisión del plan.

contexto ou se o monitoramento e a análise crítica contínuos identificarem fraquezas ou ineficiências.

3.3.3.3 Convém que o escopo, os objetivos, as metas, os recursos, as medidas para o sucesso e os critérios para o monitoramento e análise crítica na fase de implementação sejam definidos.

3.3.3.4 Convém que a comunicação interna e externa e os mecanismos de reporte sejam estabelecidos.

3.3.4 Implementação da gestão de riscos

Um plano detalhado de implementação é necessário para assegurar que as alterações necessárias ocorram em uma ordem coerente e que os recursos necessários possam ser fornecidos e aplicados.

Convém que o plano seja suportado pelos recursos necessários para sua implementação, o que pode demandar alocações orçamentárias específicas, cujo desenvolvimento conviria que fosse parte do processo de planejamento.

Convém que o próprio plano seja submetido a uma avaliação de riscos de acordo com a ISO 31000:2009, 5.4, e quaisquer ações necessárias de tratamento de riscos, implementadas.

Convém que o plano tanto requeira quanto permita que o progresso seja rastreado e reportado para a Alta Direção e o organismo de supervisão, e convém que sejam feitas provisões para análises críticas periódicas do plano.

Convém, portanto, que o plano:

- detalhe ações específicas a serem tomadas, sua sequência, por quem e o prazo para sua conclusão: isso incluirá alteração de guias e normas internas, explicação e treinamento para construir competência e realizar ajustes nas responsabilizações;

- identifique quaisquer ações que serão implementadas como parte de algumas ações mais amplas, associadas ao desenvolvimento organizacional, ou que estejam de outra forma ligadas a ele (por exemplo, desenvolvimento de material de treinamento e engajamento de instrutores);

- defina as responsabilidades pela implementação;

- incorpore um mecanismo para reportar a conclusão, progresso e problemas;

- identifique e registre quaisquer critérios que dispararão a análise crítica do plano.

La implantación puede llevar algún tiempo para su culminación y puede realizarse en etapas. Se debería adoptar la práctica común de dar prioridad de acuerdo a las posibilidades, a aquellas acciones que tienen mayor impacto en el logro del fin propuesto. La implantación puede darse en varias etapas de madurez de la organización y de la estructura. También podría ser más efectiva para integrar la implantación con otros programas de cambios.

3.3.5 Seguimiento y revisión

Se debería realizar el seguimiento, los análisis e informes para la alta dirección sobre el avance del plan en una base de tiempo (mensualmente, trimestral, etc.).

Los informes de avance con respecto al plan, y el desempeño con respecto a los indicadores, se deberían validar periódicamente en un proceso imparcial de revisión de los objetivos. La revisión debería incluir el análisis del marco de gestión del riesgo, los procesos, los riesgos en sí mismos y el cambio en el entorno.

Se debería realizar una revisión periódica de la estrategia para la implantación, y una medición del avance, en cuanto a la consistencia y las desviaciones con respecto al plan. Las revisiones también pueden realizarse si se cumplieron los criterios establecidos para la revisión del plan.

Se debería evaluar el desempeño de acuerdo a la eficacia de los cambios y la gestión del riesgo, así como la identificación de las lecciones aprendidas y las oportunidades de mejora.

Se debería informar sobre los temas significativos del seguimiento a aquellos que son responsables de rendir cuentas.

Los resultados de esta etapa serán retroalimentados al contexto y otras funciones, tal que los nuevos riesgos se puedan identificar, así como los cambios en los riesgos existentes y el estado de ejecución del marco de gestión del riesgo y éstos puedan registrarse para la mejora (ver ISO 31000:2009, 4.6 y 5.7).

3.4 Mejora continua

El marco de gestión del riesgo y el proceso de gestión del riesgo se deberían revisar para evaluar si el diseño es adecuado y, su implantación agrega valor a la organización de acuerdo a lo previsto. Si el resultado de la revisión es que se pueden realizar mejoras, las mismas se deberían realizar tan pronto como sea posible.

A implementação pode levar algum tempo para ser concluída e pode ser feita em estágios. Convém que se adote a prática comum de dar prioridade sempre que possível às mudanças que tenham o maior impacto no atingimento do propósito final. Essa implementação pode ocorrer em vários estágios da maturidade e estrutura organizacionais. Também pode ser mais eficaz integrar a implementação com outros programas de mudança.

3.3.5 Monitoramento e análise crítica

Convém que o progresso em relação ao plano seja identificado, analisado e reportado para a Alta Direção periodicamente (mensalmente, trimestralmente etc.).

Convém que sejam validados periodicamente os reportes de progresso, em relação ao plano, e de desempenho, em relação aos indicadores, por meio de um processo de análise crítica objetivo e imparcial. Convém que as análises críticas incluam o exame da estrutura, processos e os próprios riscos assim como mudanças no ambiente.

Convém que haja uma análise crítica periódica da estratégia de implementação, e medição de progresso, da consistência e desvio em relação ao plano de gestão de riscos. Análises críticas também podem ocorrer se os critérios para a análise crítica estabelecidos no plano forem atendidos.

Convém que o desempenho seja avaliado com relação à eficácia da mudança e gestão de riscos, bem como para identificar lições aprendidas e oportunidades de melhoria.

Convém que as questões significativas resultantes do monitoramento sejam reportadas para aqueles que são responsabilizáveis.

Os resultados desta etapa serão retroalimentados no contexto e em outras funções, de forma que novos riscos possam ser identificados, mudanças em riscos existentes possam ser descobertas e que o estado da estrutura possa ser registrado para melhoria (ver ISO 31000:2009, 4.6 e 5.7).

3.4 Melhoria contínua

Convém que tanto a estrutura para gerenciar riscos e o processo de gestão de riscos sejam analisados criticamente para avaliar se a sua concepção está apropriada e se sua implementação está agregando valor para a organização conforme pretendido. Se os resultados do monitoramento e da análise crítica demonstrarem que as melhorias podem ser feitas, convém que estas sejam implementadas tão logo quanto possível.

En aquellas organizaciones que han transitado con la ISO 31000, debería existir una concientización constante y se deberían tomar las oportunidades de mejora. Las mismas etapas transitadas en el proceso de transición son también útiles para realizar las verificaciones periódicas por si existieron desviaciones en el proceso.

Existen varios desencadenantes del proceso de mejora continua, incluyendo los siguientes:

- el seguimiento rutinario y la revisión del marco y del proceso de gestión del riesgo, los cuales identifican oportunidades de mejora;

- nuevos conocimientos disponibles;

un cambio sustantivo en el contexto interno y externo de la organización.

Para as organizações que tenham migrado para a ISO 31000, convém que haja atenção constante e aproveitamento da oportunidade para melhoria. As mesmas etapas utilizadas no processo de transição também são úteis para fazer verificações periódicas para identificar se tem havido desvios neste processo.

Há vários disparadores para a melhoria contínua, incluindo os seguintes:

- monitoramento de rotina e análise crítica da estrutura para gerenciar riscos e do processo de gestão de riscos, que identifiquem oportunidades para melhoria;

- novos conhecimentos se tornarem disponíveis;

- uma mudança substancial nos contextos interno e externo da organização.

Anexo A
(informativo)

Principios y conceptos principales

Conceitos e princípios subjacentes

A.1 Generalidades

Este Anexo explica ciertos términos y conceptos (por ejemplo: riesgo) que son usados comúnmente y pueden tener varios significados, pero que tienen una definición particular en la Norma ISO 31000 y en este Informe Técnico.

La Norma ISO 31000 define riesgo como el “efecto de la incertidumbre en los objetivos”.

NOTA Se recomienda que los lectores se familiaricen con los términos y definiciones presentados en este Anexo.

A.2 Riesgo y objetivos

Las organizaciones de todo tipo enfrentan factores internos y externos e influencias que hacen incierto si ellas lograrán o excederán sus objetivos, y cuándo y en qué medida.

Los objetivos contemplados en la Norma ISO 31000 y en este Informe Técnico son los resultados que la organización está buscando. Por lo general, se trata de la más alta expresión de su intención y propósito, y generalmente reflejan sus objetivos explícitos e implícitos, valores e imperativos, incluida la consideración de sus obligaciones sociales y legales y los requisitos reglamentarios. En general, la gestión del riesgo se facilita si los objetivos se expresan en términos mensurables. Sin embargo a menudo hay múltiples objetivos, y la inconsistencia entre los objetivos puede ser una fuente de riesgo.

La probabilidad no es sólo de la ocurrencia de un evento, sino que es la probabilidad global de experimentar las consecuencias que se derivan del evento y la magnitud de las mismas, ya sean positivas o negativas. Usualmente, puede haber una gama de posibles consecuencias que pueden derivarse de un evento, y cada una tendrá su propia probabilidad. El nivel de riesgo puede ser expresado como la probabilidad de que cada consecuencia particular sea experimentada (incluyendo la magnitud). Las consecuencias se relacionan directamente con los objetivos y surgen cuando algo ocurre o no.

A.1 Geral

Este Anexo explica determinados conceitos e palavras (por exemplo, “risco”) que são de uso cotidiano e podem ter vários significados, mas que têm um significado particular na ISO 31000 e neste Relatório Técnico.

A ISO 31000 define risco como o “efeito da incerteza nos objetivos”.

NOTA É recomendável que os leitores se familiarizem com os termos e definições neste Anexo.

A.2 Objetivos e riscos

Organizações de todos os tipos enfrentam fatores e influências internos e externos que tornam incerto se, quando e em que extensão elas atingirão ou excederão os seus objetivos. O efeito que essa incerteza tem nos objetivos da organização é o risco.

Os objetivos referidos na ISO 31000 e neste Relatório Técnico são os resultados que a organização busca. Tipicamente, esses são a mais elevada expressão da intenção e propósito, e tipicamente refletem os seus valores, metas e imperativos implícitos e explícitos, incluindo a consideração de obrigações sociais e requisitos legais e regulatórios. Em geral, a gestão de riscos é facilitada se os objetivos são expressos em termos mensuráveis. Há frequentemente múltiplos objetivos, entretanto, uma inconsistência entre objetivos pode ser uma fonte de risco.

Probabilidade (*likelihood*), neste contexto, não é somente aquela da ocorrência de um evento, mas a probabilidade global de se experimentar as consequências que advêm de um evento, e a magnitude da consequência, tanto em temos positivos quanto negativos. Tipicamente, pode existir uma gama de consequências possíveis que advêm de um evento, e cada uma terá a sua própria probabilidade. O nível de risco pode ser expresso como a probabilidade de que consequências específicas sejam experimentadas (incluindo magnitude). Consequências relacionam-se diretamente a objetivos e surgem quando alguma coisa acontece ou não acontece.

El riesgo es el efecto de la incertidumbre en los objetivos, independientemente del dominio o las circunstancias, por lo tanto, un evento o un peligro (o cualquier otra fuente de riesgo) no debería describirse como un riesgo. El riesgo debería describirse como la combinación de la probabilidad de un evento (o peligro o fuente de riesgo) y su consecuencia.

La comprensión de que el riesgo puede tener consecuencias positivas o negativas es un concepto central y vital para ser entendido por la dirección. El riesgo puede exponer a la organización tanto a una oportunidad, como a una amenaza o ambas.

El riesgo se crea o modifica cuando se toman decisiones. Debido a que casi siempre hay cierta incertidumbre asociada con las decisiones y la toma de decisiones, casi siempre hay riesgo. Los responsables del logro de los objetivos deberían tener en cuenta que el riesgo es una parte inevitable de las actividades de la organización, que por lo general se crea o modifica cuando se toman las decisiones. Los riesgos asociados con una decisión deberían entenderse en el momento de tomar la decisión, y por lo tanto la toma de riesgos es intencional. La aplicación del proceso de gestión del riesgo descrito en la Norma ISO 31000 lo hace posible.

A.3 Incertidumbre

La incertidumbre que, junto con los objetivos, da lugar al riesgo se origina en el entorno interno y externo en el que opera la organización. Ésta incertidumbre puede ser:

- una consecuencia de factores sociológicos, psicológicos y culturales subyacentes asociados con el comportamiento humano;

- producida por procesos naturales que se caracterizan por la variabilidad inherente, por ejemplo, en el tiempo, la variación entre las observaciones en una población;

- de una información incompleta o inexacta, por ejemplo, debido a la falta de datos, que éstos son mal interpretados, pocos fiables, internamente contradictorios o inaccesibles;

- cambios a lo largo del tiempo, por ejemplo, debido a la competencia, las tendencias, información nueva, cambios en los factores subyacentes;

- producida por la percepción de la incertidumbre que puede variar dentro de las partes de la organización y sus partes interesadas.

Risco é o efeito da incerteza nos objetivos, independentemente do domínio ou circunstâncias, portanto convém que um evento ou um perigo (ou qualquer outra fonte de risco) não seja descrito como um risco. Convém que risco seja descrito como a combinação da probabilidade de um evento (ou perigo ou fonte de risco) e a sua consequência.

O entendimento de que risco pode ter consequências positivas ou negativas é um conceito central e vital a ser compreendido pela direção. O risco pode expor a organização tanto a uma oportunidade quanto a uma ameaça ou a ambos.

O risco é criado ou alterado quando decisões são tomadas. Porque há quase sempre alguma incerteza associada a decisões e na tomada de decisões existe quase sempre risco. Aqueles responsáveis por atingir objetivos precisam compreender que o risco é uma parte inevitável das atividades da organização que é tipicamente criado ou alterado quando decisões são tomadas. Convém que os riscos associados a uma decisão sejam compreendidos no momento em que a decisão é tomada e a assunção do risco é portanto intencional. Usar o processo de gestão de riscos descrito na ISO 31000 torna isto possível.

A.3 Incerteza

A incerteza que, juntamente com os objetivos, gera o risco origina-se no ambiente interno e externo em que a organização opera. Esta incerteza pode:

- ser uma consequência de fatores sociológicos, psicológicos e culturais subjacentes associados ao comportamento humano;

- ser produzida por processos naturais que são caracterizados por variabilidade inerente, por exemplo, na meteorologia, variação entre observações em uma população;

- surgir de informação incompleta ou imprecisa, por exemplo, devido a dados ausentes, mal interpretados, não confiáveis, internamente contraditórios ou inacessíveis;

- mudar ao longo do tempo, por exemplo, devido à competição, tendências, novas informações, mudanças nos fatores subjacentes;

- ser produzida pela percepção de incerteza que pode variar entre partes da organização e as suas partes interessadas.

A.4 Tratamiento y control del riesgo

Los controles son medidas implementadas por las organizaciones para modificar el riesgo tal que permitan el logro de los objetivos. Los controles pueden modificar el riesgo al cambiar cualquier fuente de incertidumbre (por ejemplo, por lo que es más o menos probable que algo ocurra) o cambiando el rango de las posibles consecuencias y donde pueden producirse.

El tratamiento del riesgo, tal como se define en la Norma ISO 31000, es el proceso por el cual se pretende cambiar o crear controles e incluye la retención del riesgo.

A.5 Marco de gestión del riesgo

El marco de gestión de riesgo se refiere a los acuerdos (incluidos las prácticas, los procesos, los sistemas, los recursos y la cultura) dentro del sistema de gestión de la organización que permiten que el riesgo sea gestionado. En última instancia las características del marco, y el grado en que está integrado con el sistema de gestión de la organización, determinan la eficacia de la gestión del riesgo.

El marco incluye declaraciones claras de la alta dirección sobre la intención de la organización con respecto a la gestión del riesgo (que se describe en la Norma ISO 31000 como el mandato y el compromiso) y de la capacidad necesaria (recursos y capacidades) para lograr este propósito.

Esta capacidad no existe como un sistema o entidad únicos. Esta capacidad comprende numerosos elementos integrados en los procesos de la gestión global de la organización. O bien pueden ser únicos para la tarea de la gestión del riesgo (por ejemplo, un sistema de información especializado), o ser aspectos del sistema de gestión de la organización (por ejemplo, las prácticas de recursos humanos).

A.6 Criterios de riesgo

Los criterios de riesgo son los términos de referencia establecidos por la organización para que pueda proceder a describir los riesgos y tomar decisiones acerca de la relevancia del riesgo, teniendo en cuenta la actitud frente al riesgo de la organización. Estas decisiones permiten evaluar y seleccionar el tratamiento del riesgo.

A.7 Gestión, gestión del riesgo y gestionar el riesgo

La gestión implica actividades coordinadas para dirigir y controlar una organización en la consecución de sus objetivos.

A.4 Controle e tratamento de risco

Controles são medidas implementadas pelas organizações para modificar o risco, possibilitando o alcance dos objetivos. Controles podem modificar riscos pela mudança de qualquer fonte de incerteza (por exemplo, ao tornar mais ou menos provável que algo aconteça) ou pela mudança da série de possíveis consequências e onde podem ocorrer.

Tratamento de risco, como definido na ISO 31000, é o processo que se destina a alterar ou criar controles, e inclui a retenção de risco.

A.5 Estrutura para gerenciar riscos

A estrutura para gerenciar riscos refere-se aos arranjos (incluindo práticas, processos, sistemas, recursos e cultura) no sistema de gestão da organização, que possibilitam que o risco seja gerenciado. As características de uma estrutura, e a extensão em que é integrada no sistema de gestão da organização, determinarão por fim o quão efetivamente o risco será gerenciado.

A estrutura inclui declarações claras pela Alta Direção sobre as intenções da organização em relação à gestão de riscos (descrita na ISO 31000 como mandato e comprometimento) e a capacidade necessária (recursos e competências) para atingir este intento.

Esta capacidade não existe como um sistema único ou entidade. Esta capacidade abrange numerosos elementos integrados nos processos globais de gestão da organização. Podem ser aplicados unicamente para a tarefa de gerenciar risco (por exemplo, um sistema de informação especializado), ou serem aspectos do sistema de gestão da organização (por exemplo, as suas práticas de recursos humanos).

A.6 Critérios de risco

Critérios de risco são parâmetros estabelecidos pela organização que a possibilitem descrever o risco e tomar decisões sobre a significância do risco, levando em consideração a atitude da organização perante o risco. Estas decisões possibilitam que o risco seja avaliado e o tratamento selecionado.

A.7 Gestão, gestão de riscos e gerenciar riscos

A gestão envolve atividades coordenadas que dirigem e controlam uma organização para o atingimento de seus objetivos.

La gestión del riesgo es un componente integral de la gestión, ya que implica la coordinación de actividades relacionadas con el efecto de la incertidumbre en dichos objetivos. Es por ello que, con el fin de ser eficaz, es importante que la gestión del riesgo esté completamente integrada en el sistema de gestión de la organización y los procesos.

En este Informe Técnico, como en Norma la ISO 31000, la expresión "gestión del riesgo" por lo general se refiere a la arquitectura que las organizaciones utilizan (principios, el marco y el proceso) para gestionar el riesgo de manera eficaz, y "gestionar el riesgo" se refiere a la aplicación de la arquitectura en las decisiones particulares, las actividades y los riesgos.

A gestão de riscos é um componente integral da gestão, uma vez que envolve atividades coordenadas relacionadas com o efeito da incerteza nesses objetivos. É por isso que, para ser eficaz, é importante que a gestão de riscos seja completamente integrada aos processos e sistema de gestão da organização.

Neste Relatório Técnico, assim como na ISO 31000, a expressão “gestão de riscos” refere-se, em termos gerais, à arquitetura que as organizações usam (princípios, estrutura e processo) para gerenciar riscos efetivamente (com eficácia) e “gerenciando riscos” refere-se à aplicação da arquitetura a decisões, atividades e riscos em particular.

Anexo B
(informativo)

Aplicación de los principios de la norma ISO 31000

Aplicação dos princípios da ISO 31000

B.1 Generalidades

Si bien todas las organizaciones gestionan el riesgo en cierta medida, la Norma ISO 31000:2009 establece once principios que tienen que ser satisfechos para la gestión eficaz del riesgo.

Los principios ofrecen orientación sobre lo siguiente:

a) la razón fundamental para la gestión del riesgo de manera eficaz (por ejemplo, la gestión de riesgos protege y crea valor);

b) las características de la gestión del riesgo que permiten que la gestión del riesgo sea eficaz, por ejemplo, principio b), que específica que la gestión de riesgos es una parte integral de todos los procesos de la organización.

En la Norma ISO 31000, cada principio se resume con su título en pocas palabras, con el texto de apoyo que proporciona la explicación y el detalle.

Los once principios deberían ser considerados en el diseño de los objetivos de la gestión del riesgo de la organización, sin embargo, la importancia de los principios individuales puede variar de acuerdo con la parte del marco en consideración y la adaptación a su aplicación específica.

La implementación exitosa de estos principios permite determinar la eficacia y la eficiencia de la gestión del riesgo en la organización.

Los once principios deberían tenerse en cuenta en todo momento, incluso aunque la importancia de los principios individuales puede variar de acuerdo con la parte del marco en consideración.

Aunque los principios se expresan de manera sucinta, las implicancias de cada uno necesitan ser cuidadosamente entendidas con el fin de llevarlas a la práctica sobre una base continua.

Posteriormente, los resultados de este tipo de análisis se deberían reflejar en el diseño o mejora del marco (por ejemplo, en la asignación de responsabilidades, la provisión de capacitación, la comunicación con las partes interesadas y el

B.1 Geral

Considerando-se que todas as organizações gerenciam riscos em algum grau, a ISO 31000:2009 estabelece onze princípios que precisam ser atendidos para tornar a gestão de riscos efetiva.

Os princípios fornecem orientações sobre o seguinte:

a) a fundamentação para gerenciar riscos efetivamente (por exemplo, a gestão de riscos cria e protege valor);

b) as características de gestão de riscos que tornam a gestão de riscos eficaz, por exemplo, princípio b), que especifica que a gestão de riscos é parte integrante de todos os processos organizacionais.

Na ISO 31000, cada princípio está resumido em poucas palavras por seu título, com o texto de apoio fornecendo explicações e detalhes.

Convém que todos os onze princípios sejam considerados na concepção dos objetivos para a gestão de riscos da organização, no entanto, a importância de princípios individuais pode variar de acordo com a parte da estrutura considerada e ajustada para a sua aplicação específica.

A implementação bem-sucedida desses princípios determinará a eficácia e eficiência da gestão de riscos na organização.

Convém que todos os onze princípios sejam mantidos em mente o tempo todo, mesmo que a importância dos princípios individuais possa variar de acordo com a parte da estrutura em questão.

Embora os princípios sejam expressos de forma sucinta, as implicações de cada um deles precisam ser completamente compreendidas, a fim de dar-lhes efeito de forma contínua.

Posteriormente, convém que os resultados deste tipo de análise sejam refletidos na concepção ou no aprimoramento da estrutura (por exemplo, na alocação de responsabilidades, na provisão de treinamento, na comunicação com as partes

diseño de un seguimiento continuo y revisión del desempeño de la gestión del riesgo).

En este Anexo se ofrece orientación sobre cómo aplicar cada principio y, además para algunos principios se dan también ayuda práctica.

B.2 Los principios

B.2.1 La gestión del riesgo protege y crea valor

B.2.1.1 Principio

a) La gestión de riesgos protege y crea valor.
La gestión del riesgo contribuye al logro de los objetivos y en la mejora demostrable del desempeño, por ejemplo, la salud humana y la seguridad, el cumplimiento legal y reglamentario, la aceptación pública, la protección del ambiente, la calidad del producto, la gestión de proyectos, la eficiencia en las operaciones, la gobernanza y la reputación.

B.2.1.2 Cómo aplicar el principio

Este principio explica que el propósito de la gestión del riesgo es proteger y crear valor ayudando a una organización a alcanzar sus objetivos. Para ello, ayuda a la organización a identificar y abordar los factores, tanto internos como externos a la organización, que dan lugar a la incertidumbre asociada a sus objetivos.

Se debería demostrar claramente y comunicar el vínculo entre la eficacia de la gestión del riesgo y cómo contribuye al éxito de la organización. El principio aclara que el riesgo no se debería manejar por su propio bien, sino para que se logren los objetivos y se mejore el desempeño.

Algunos atributos y valores no se pueden medir fácilmente en forma directa (por ejemplo, en términos de dinero), pero también contribuyen en gran medida al desempeño, la reputación y el cumplimiento legal. Los valores humanos, sociales y ecológicos son de particular importancia en la gestión de la seguridad, y los riesgos relacionados con el cumplimiento, así como los relacionados con los activos intangibles, por eso es posible que se exprese la creación de valor mediante descriptores cualitativos en vez de medidas cuantitativas.

B.2.2 La gestión del riesgo es una parte integral de todos los procesos de la organización

B.2.2.1 Principio

interessadas e na concepção de monitoramento e análise crítica contínuos do desempenho da gestão de riscos).

Este Anexo fornece orientação sobre como aplicar cada princípio e, além disso, para alguns princípios há também caixas de ajuda prática.

B.2 Os princípios

B.2.1 A gestão de riscos cria e protege valor

B.2.1.1 Princípio

a) A gestão de riscos cria e protege valor.
A gestão de riscos contribui para a realização demonstrável dos objetivos e melhoria de desempenho em, por exemplo, saúde e proteção humana, segurança, conformidade legal e regulatória, aceitação pública, proteção ambiental, qualidade de produto, gerenciamento de projetos, eficiência das operações, governança e reputação.

B.2.1.2 Como aplicar o princípio

Este princípio explica que o objetivo da gestão de riscos é criar e proteger valor quando ajuda uma organização a atingir seus objetivos. Isso é realizado, ajudando a organização a identificar e lidar com os fatores, internos ou externos à organização, que dão origem à incerteza associada com os seus objetivos.

Convém que a ligação entre a eficácia da gestão de riscos e como ela contribui para o sucesso da organização seja claramente demonstrada e comunicada. O princípio esclarece que não convém que o risco seja gerenciado por si só, mas para que os objetivos sejam atingidos e o desempenho aprimorado.

Alguns atributos e valores não podem ser medidos diretamente de forma fácil (por exemplo, em termos financeiros), no entanto, contribuem fortemente para o desempenho, reputação e conformidade legal. Os valores humanos, sociais e ecológicos são particularmente importantes na gestão dos riscos relativos à segurança e conformidade, assim como aqueles associados com os ativos intangíveis, portanto, a criação de valor pode precisar ser expressa utilizando descrição qualitativa em vez de medidas quantitativas.

B.2.2 A gestão de riscos é parte integrante de todos os processos organizacionais

B.2.2.1 Princípio

b) La gestión del riesgo es una parte integral de todos los procesos de la organización.
La gestión del riesgo no es una actividad aislada que está separada de las principales actividades y procesos de la organización. La gestión del riesgo es parte de las responsabilidades de la dirección y una parte integral de todos los procesos de la organización, incluida la planificación estratégica y todos los proyectos y procesos de gestión del cambio.

B.2.2.2 Cómo aplicar el principio

Las actividades de una organización, incluida la toma de decisiones, dan lugar a riesgo.

Los cambios en el contexto externo que están más allá del control y la influencia de la organización también pueden dar lugar a nuevos riesgos.

Todas las actividades y los procesos de la organización se llevan a cabo en un entorno interno y externo, en los que hay incertidumbre. De ello se desprende que:

a) el marco para la gestión del riesgo debería realizarse mediante la integración de sus elementos en el sistema de gestión general de la organización y la toma de decisiones, los procesos de gestión existentes pueden mejorarse mediante la referencia a la Norma ISO 31000 independientemente que el sistema sea formal o informal;

b) el proceso de gestión del riesgo debería ser una parte integral de las actividades que generan los riesgos; de lo contrario, la organización encontrará la necesidad de modificar las decisiones más tarde, cuando los riesgos asociados son comprendidos posteriormente;

c) cuando no exista un sistema de gestión formal, el marco de gestión del riesgo puede servir para este propósito.

Si la gestión del riesgo no está integrada con otras actividades y procesos de gestión, se puede percibir como una tarea administrativa adicional, o ser vista como un ejercicio burocrático que no protege ni crea valor.

Los dos métodos principales para aplicar el principio son los siguientes:

- en el desarrollo (incluido el mantenimiento y mejora) del marco de gestión del riesgo;

- en la aplicación del proceso de gestión del riesgo para la toma de decisiones y las actividades relacionadas.

El método de expresión de la intención de la

b) A gestão de riscos é parte integrante de todos os processos organizacionais.
A gestão de riscos não é uma atividade autônoma, separada das principais atividades e processos da organização. A gestão de riscos é parte das responsabilidades da direção e uma parte integrante de todos os processos organizacionais, incluindo planejamento estratégico e todos os projetos e processos de gestão de mudanças.

B.2.2.2 Como aplicar o princípio

As atividades de uma organização, incluindo as tomadas de decisões, dão origem a riscos.

As mudanças no contexto externo que estão fora do controle e influência da organização também podem dar origem a novos riscos.

Todas as atividades e processos da organização ocorrem em ambientes interno e externo, nos quais há incerteza. Segue-se que:

a) convém que a estrutura para gerenciar riscos seja compreendida pela integração de seus componentes ao sistema global de gestão e tomada de decisões da organização, independentemente do sistema ser formal ou informal; processos de gestão existentes podem ser melhorados referindo-se à ISO 31000;

b) convém que o processo de gestão de riscos seja parte integrante das atividades que geram risco; caso contrário, a organização perceberá que é preciso modificar as decisões mais tarde, quando os riscos associados são posteriormente compreendidos;

c) se um sistema formal de gestão não existe, é possível que uma estrutura para gerenciar riscos sirva a esse propósito.

Se a gestão de riscos não está integrada a outras atividades e processos de gestão, esta pode ser percebida como uma tarefa administrativa adicional, ou vista como um exercício burocrático que não cria ou protege valor.

Os dois principais métodos de aplicação do princípio são os seguintes:

- no desenvolvimento (incluindo a manutenção e melhoria) da estrutura para gerenciar riscos;

- na aplicação do processo de gestão de riscos para a tomada de decisões e atividades relacionadas.

Convém que o método de expressar a intenção da

organización (es decir, el mandato y el compromiso) sobre la gestión del riesgo debería ser similar a la forma en que expresa sus otras intenciones (ver Anexo C). Cuando sea posible, los demás elementos del marco de gestión de riesgos deberían estar embebidos en los elementos de los sistemas de gestión existentes (más detalle se establece en el Anexo E y en la Norma ISO 31000).

También los órganos de auditoria pueden desempeñar un papel importante, al cuestionar cómo se ha llegado a una decisión y comprobar si implicó una aplicación adecuada del proceso de gestión del riesgo.

B.2.3 La gestión del riesgo es parte de la toma de decisiones

B.2.3.1 Principio

c) La gestión del riesgo es parte de la toma de decisiones.
La gestión del riesgo ayuda a quienes toman las decisiones a tomar decisiones informadas, priorizar acciones y distinguir entre cursos alternativos de acción.

B.2.3.2 Cómo aplicar el principio

Este principio establece que la gestión del riesgo proporciona la base para la toma de decisiones informadas.

La gestión del riesgo debería integrarse en las actividades de apoyo a la consecución de los objetivos y al proceso de toma de decisiones. El proceso de toma de decisiones debería evaluar de forma consistente y, cuando fuera necesario, tratar el riesgo. Tomar o no tomar decisiones implica un riesgo, y en ambas situaciones es importante tener una comprensión de los riesgos asociados.

La gestión del riesgo debería aplicarse como parte de una decisión, y en el momento de tomar la decisión (es decir, proactiva), y no después de haber tomado la decisión (es decir, de forma reactiva), por ejemplo de la forma siguiente:

- las decisiones sobre cuestiones estratégicas deberían tener en cuenta las incertidumbres que pesan sobre los cambios en los factores del entorno, así como los cambios en los recursos de la organización;

- el proceso de innovación debería tener en cuenta no sólo la incertidumbre que determina el éxito de la innovación, sino también los riesgos de la innovación relativos a los aspectos de los derechos humanos, sociales, de seguridad y del entorno, y los requisitos legales (por ejemplo, la seguridad del producto);

organização (ou seja, mandato e comprometimento) sobre a gestão de riscos seja semelhante à maneira que são expressas suas outras intenções (ver Anexo C). Sempre que possível, convém que outros componentes da estrutura para gerenciar riscos sejam incorporados a componentes de sistemas de gestão existentes (mais recomendações são fornecidas no Anexo E e na ISO 31000).

Organismos de auditoria também estão aptos a desempenhar um papel importante, ao questionar como a direção chegou a uma decisão e verificar se essa envolveu uma aplicação adequada do processo de gestão de riscos.

B.2.3 A gestão de riscos é parte da tomada de decisões

B.2.3.1 Princípio

c) A gestão de riscos é parte da tomada de decisões.
A gestão de riscos ajuda os tomadores de decisão a fazerem escolhas informadas, priorizarem ações e distinguirem entre cursos alternativos de ação.

B.2.3.2 Como aplicar o princípio

Este princípio estabelece que a gestão de riscos fornece a base para a tomada de decisões informadas.

Convém que a gestão de riscos seja integrada a atividades de apoio à realização dos objetivos e ao processo de tomada de decisões. Convém que o processo de tomada de decisões avalie consistentemente e, se necessário, trate o risco. Tomar ou não tomar decisões envolve riscos, e é importante ter uma compreensão dos riscos associados em ambas as situações.

Convém que a gestão de riscos seja aplicada como parte de uma decisão, no momento em que é tomada a decisão (ou seja, de forma proativa), e não após a decisão ser tomada (ou seja, de forma reativa), por exemplo, do seguinte modo:

- convém que as decisões sobre questões estratégicas levem em consideração as incertezas sobre as mudanças nos fatores ambientais, bem como mudanças nos recursos da organização;

- convém que o processo de inovação leve em consideração não apenas a incerteza que determina o sucesso da inovação, mas também os riscos relativos aos aspectos humanos, sociais, ambientais e de segurança da inovação, e tratados de acordo com os requisitos legais (por exemplo, a segurança de produtos);

- en los planes con grandes inversiones se debería especificar los hitos de decisión en los cuales se realizará la evaluación del riesgo.

La política de la organización acerca de la gestión del riesgo, así como la forma en que se comunica debería reflejar este principio.

Las otras partes del marco deberían tener en cuenta la forma en que se toman las decisiones, para que el proceso se aplique de una manera eficaz y consistente en toda toma de decisiones, por ejemplo, gestión de proyectos, evaluación de la inversión, la contratación.

Los responsables de la toma de decisiones en toda la organización deberían comprender la política de gestión del riesgo y tener las competencias para aplicar el proceso de gestión del riesgo para la toma de decisiones. Esto requiere una clara asignación de responsabilidades, con el apoyo de capacitación y evaluación del desempeño.

Ayuda práctica

Para dar cumplimiento al principio, se debería considerar cuidadosamente las siguientes preguntas desde el inicio:

- ¿Cómo puede ayudar a proteger y crear valor? [Principio a)]

- ¿Cómo y en qué parte de la organización se toman las decisiones?

- ¿Quién está involucrado en la toma de decisiones?

- ¿Qué conocimiento y habilidades requieren aquellos que toman decisiones para que la gestión del riesgo sea una parte en su proceso de toma de decisión?

- ¿Cómo los que toman decisiones van adquirir los conocimientos y habilidades que necesitan?

- ¿Qué dirección y apoyo se necesita para el personal existente?

- ¿Cómo será inducido el personal en este método de toma de decisiones en el futuro?

- ¿Cómo se verán afectadas las partes interesadas externas?

- ¿Qué procesos de toma de decisión tendrían que cambiar en la organización?

- ¿Cómo sería el seguimiento del progreso en la aplicación de este principio?

- convém que os planos para grandes investimentos especifiquem os marcos de decisão em que ocorrerão a avaliação dos riscos.

Convém que a política da organização sobre a gestão de riscos e a forma como ela é comunicada reflita este princípio.

Convém que as outras partes da estrutura levem em conta a forma como as decisões são tomadas, de modo que o processo seja aplicado de forma eficaz e de modo consistente em todas as tomadas de decisões, por exemplo, gerenciamento de projetos, avaliação de investimentos, aquisições.

Convém que os responsáveis pela tomada de decisões em toda a organização compreendam a política de gestão de riscos da organização e convém que seja especificamente requerido que tenham competências para aplicar o processo de gestão de riscos para a tomada de decisões. Isso vai exigir atribuição clara de responsabilidade, apoiada por formação de competências e análise crítica de desempenho.

Ajuda prática

- Para dar efeito ao princípio, convém que as seguintes perguntas sejam consideradas com cuidado desde o início:

- Como isso pode ajudar a criar e proteger valor? [Princípio a)]

- Como e onde na organização são tomadas as decisões?

- Quem está envolvido na tomada de decisões?

- Quais conhecimentos e habilidades são necessários para aqueles que tomam decisões para tornar a gestão de riscos parte da sua tomada de decisões?

- Como os tomadores de decisões adquirem os conhecimentos e habilidades necessários?

- Que direção e apoio são necessários para a equipe existente?

- Como a equipe futura será introduzida a este método de tomada de decisões?

- Como as partes interessadas externas serão afetadas?

- Que processos de tomada de decisões da organização precisariam mudar?

- Como o progresso na aplicação deste princípio seria monitorado?

B.2.4 La gestión del riesgo aborda explícitamente la incertidumbre

B.2.4.1 Principio

d) La gestión de riesgos aborda explícitamente la incertidumbre.
La gestión del riesgo tiene en cuenta explícitamente la incertidumbre, la naturaleza de esa incertidumbre, y cómo se puede abordar.

B.2.4.2 Cómo aplicar el principio

Lo que hace única a la gestión del riesgo entre otros tipos de gestión es que aborda específicamente el efecto de la incertidumbre en los objetivos. El riesgo sólo se puede evaluar o tratar de manera eficaz si se entienden la naturaleza y la fuente de incertidumbre.

Se requiere la consideración de todo tipo de incertidumbre, y es necesario tener cuidado de no sobrestimar o subestimar.

También es importante centrarse en la incertidumbre al seleccionar los tratamientos del riesgo teniendo en cuenta el efecto y la fiabilidad de los controles. Del mismo modo, habrá incertidumbres asociadas con las etapas de apoyo al proceso de gestión del riesgo, por ejemplo, si la información se ha transmitido con éxito a las partes interesadas en la comunicación y consulta, o si los intervalos seleccionados para el seguimiento de los procesos son suficientes para detectar un cambio.

Las personas involucradas en la gestión del riesgo deberían tener un buen conocimiento de la importancia de la incertidumbre, y los tipos y fuentes de incertidumbre. El número y los tipos de métodos utilizados para la evaluación del riesgo deberían ser adecuados y pertinentes de acuerdo a la importancia de la decisión: se pueden aplicar métodos múltiples.

Se debería registrar los supuestos cuando se documente el proceso de gestión del riesgo (ISO 31000:2009, 5.7). Generalmente los supuestos reflejan algún tipo de incertidumbre, así como las incertidumbres explícitas que han sido corregidas, en las diversas etapas del proceso.

Cuando se evalúa el riesgo, es importante tener en cuenta la incertidumbre asociada a la estimación de las valoraciones de la probabilidad matemática y las consecuencias. Al analizar los riesgos y proponer tratamientos, debería utilizarse los estudios de sensibilidad para entender la influencia real de esas incertidumbres.

B.2.4 A gestão de riscos aborda explicitamente a incerteza

B.2.4.1 Princípio

d) A gestão de riscos aborda explicitamente a incerteza.
A gestão de riscos leva em conta explicitamente a incerteza, a natureza dessa incerteza, e como ela pode ser abordada.

B.2.4.2 Como aplicar o princípio

O que faz a gestão de riscos tornar-se única entre os outros tipos de gestão é que ela aborda especificamente o efeito da incerteza nos objetivos. O risco só pode ser avaliado ou tratado com sucesso se a natureza e a fonte da incerteza são compreendidas.

Incertezas de todos os tipos devem ser consideradas, e é preciso cuidado para não superestimá-las ou subestimá-las.

Foco na incerteza também é importante na seleção de tratamentos de risco e na consideração do efeito e confiabilidade dos controles. Do mesmo modo, haverá incertezas associadas com as etapas de apoio do processo de gestão de riscos, por exemplo, se a informação foi transmitida com sucesso ao se comunicar e consultar as partes interessadas, ou se os intervalos selecionados para monitoramento de processos são suficientes para detectar mudanças.

Convém que as pessoas envolvidas na gestão de riscos tenham uma boa compreensão da importância da incerteza, e os tipos e fontes de incerteza. Convém que o número e os tipos de métodos de avaliação de risco utilizados para tratar a incerteza sejam adequados e relevantes para a importância da decisão: pode-se justificar o uso de vários métodos.

Registrar suposições durante o registro do processo de gestão de riscos (ISO 31000:2009, 5.7). Suposições geralmente refletem algum tipo de incerteza, bem como quaisquer incertezas explícitas que tenham sido consideradas nas várias etapas do processo.

Quando o risco está sendo avaliado, é importante considerar a incerteza associada com a estimativa das classificações de probabilidade e consequência. Ao analisar o risco e propor tratamentos, convém que estudos de sensibilidade sejam utilizados para compreender a real influência dessas incertezas.

Ayuda práctica

- Los que toman decisiones deberían adoptar la práctica común de preguntarse "¿Cuáles son los supuestos?" ¿Cuáles son las incertidumbres asociadas a dichos supuestos? " .

- Esta práctica no tiene por qué limitarse a las evaluaciones formales del riesgo, por ejemplo, se puede aplicar a todos los pronósticos.

- Al considerar el entorno interno y externo como parte de establecer el contexto, debería establecerse las características que puedan estar asociada con una alta volatilidad. Esta es una fuente de incertidumbre y también informa la manera en la que se realiza el seguimiento, control y revisión del contexto.

- Si la incertidumbre significa que un valor particular es conocido dentro de cierto rango, se recomienda comunicar ese rango.

Ajuda prática

- Convém que os tomadores de decisões adotem a prática de sempre perguntar “Quais são as suposições aqui?” e “Quais são as incertezas associadas a essas suposições?”.

- Esta prática não precisa ser limitada a avaliações de riscos formais, por exemplo, poderia aplicar-se a todas as previsões.

- Quando se considera o ambiente interno e externo como uma parte do estabelecimento do contexto, convém que sejam observadas quaisquer características que possam ser associadas a alta volatilidade. Esta é uma fonte de incerteza e também informa a maneira pela qual o contexto é monitorado e analisado criticamente de modo contínuo.

- Se a incerteza significa que um determinado valor é conhecido apenas por existir dentro de um determinado intervalo, convém que esse intervalo seja comunicado.

B.2.5 La gestión del riesgo es sistemática, estructurada y oportuna

B.2.5.1 Principio

e) La gestión del riesgo es sistemática, estructurada y oportuna.
Un enfoque sistemático, estructurado y oportuno para la gestión del riesgo contribuye a la eficiencia y a resultados consistentes, comparables y fiables.

B.2.5.2 Cómo aplicar el principio

Un enfoque coherente de la gestión del riesgo en el momento de la toma de decisiones logrará eficiencias en una organización, y puede proporcionar resultados que promuevan la confianza y el éxito. Esto requiere de prácticas organizacionales que consideren los riesgos asociados a todas las decisiones, y el uso de criterios de riesgo consistentes que se relacionan con los objetivos de la organización y el alcance de sus actividades.

Un enfoque oportuno significa que el proceso de gestión del riesgo se aplica en el momento óptimo en el proceso de toma de decisiones. En parte, esto depende del diseño del marco, al que también se aplica este principio. Si las consideraciones sobre el riesgo se hacen demasiado pronto o demasiado tarde, o bien se podrían perder oportunidades o haber costos sustanciales de la revisión de la decisión. Se debería evaluar y entender las dependencias con el tiempo para determinar el enfoque más eficaz en la gestión del riesgo.

B.2.5 A gestão de riscos é sistemática, estruturada e oportuna

B.2.5.1 Princípio

e) A gestão de riscos é sistemática, estruturada e oportuna.
Uma abordagem sistemática, oportuna e estruturada para a gestão de riscos contribui para a eficiência e resultados consistentes, confiáveis e comparáveis.

B.2.5.2 Como aplicar o princípio

Uma abordagem consistente para gerir riscos no momento da tomada de decisões tornará a organização mais eficiente, e pode fornecer resultados que criam confiança e sucesso. Isto requer práticas organizacionais que considerem os riscos associados a todas as decisões, bem como a utilização de critérios de risco consistentes que se relacionam com os objetivos das organizações e o escopo de suas atividades.

Uma abordagem oportuna significa que o processo de gestão de riscos é aplicado no ponto ideal no processo de tomada de decisões. Em parte, isso depende da concepção da estrutura, para a qual este princípio também se aplica. Se as considerações de risco forem feitas muito cedo ou tarde demais, tanto as oportunidades podem ser perdidas como poderia haver custos substanciais para revisar a decisão. Convém que o efeito do tempo seja avaliado e compreendido para determinar a abordagem de gestão de riscos mais eficaz.

Un enfoque estructurado significa la aplicación del proceso de gestión del riesgo en la forma descrita en la Norma ISO 31000:2009, Capítulo 5, incluyendo las preparaciones adecuadas para estas actividades. Dependiendo de las necesidades, el método debería ser consistente, ya sea con un enfoque descendente o ascendente, con el fin de abordar el nivel apropiado de la gestión.

B.2.6 La gestión del riesgo se basa en la mejor información disponible

B.2.6.1 Principio

f) La gestión del riesgo se basa en la mejor información disponible.
Los elementos de entrada al proceso de gestión del riesgo se basan en las fuentes de información, tales como los datos históricos, la experiencia, la retroalimentación de las partes interesadas, las observaciones, los pronósticos y las opiniones de expertos. Sin embargo, quienes toman las decisiones deberían informarse, y tener en cuenta, cualquier limitación de los datos o de los modelos utilizados o la posibilidad de divergencia entre los expertos.

B.2.6.2 Cómo aplicar el principio

Es importante obtener la mejor información disponible con el fin de tener una comprensión correcta de cualquier riesgo. En consecuencia, los mecanismos de gestión del riesgo deberían incluir los métodos de investigación (por ejemplo investigación) para recoger o generar la información. Sin embargo, a pesar de los esfuerzos, a veces la información disponible puede ser limitada, por ejemplo, la anticipación de lo que sucederá en el futuro puede estar limitada a la utilización de proyecciones estadísticas.

Se debería comprender la sensibilidad de las decisiones a cualquier incertidumbre en la información. La fiabilidad de la evaluación del riesgo dependerá, en parte, de la claridad y precisión de los criterios de riesgo. La recopilación de datos relacionados con los riesgos (por ejemplo, la ocurrencia de incidentes y otra información basada en la experiencia) pueden ayudar a las predicciones estadísticas.

Aunque la toma de decisiones basada en la evidencia es el objetivo final, esto no siempre es posible en el tiempo o con los recursos disponibles. En tales situaciones, se debería utilizar la opinión de expertos, en combinación con la información que esté disponible. Sin embargo, al aplicar tal opinión es necesario tener cuidado para evitar el sesgo de grupo. Además, la evidencia del pasado podría no predecir con exactitud el futuro. En situaciones en las que

Uma abordagem estruturada significa aplicação do processo de gestão de riscos na forma descrita na ISO 31000:2009, Seção 5, incluindo os preparativos adequados para essas atividades. Dependendo das necessidades, convém que o método esteja consistente tanto com uma abordagem de cima para baixo ou de baixo para cima, a fim de abordar o nível adequado de gestão.

B.2.6 A gestão de riscos baseia-se nas melhores informações disponíveis

B.2.6.1 Princípio

f) A gestão de riscos baseia-se nas melhores informações disponíveis.
As entradas para o processo de gestão de riscos baseiam-se em fontes de informação, como dados históricos, experiência, retorno das partes interessadas, observações, previsões e pareceres de especialistas. No entanto, convém que os tomadores de decisões se informem, e convém que levem em consideração quaisquer limitações de dados ou de modelagem utilizados, ou a possibilidade de divergência entre os especialistas.

B.2.6.2 Como aplicar o princípio

É importante obter a melhor informação disponível, a fim de se ter uma compreensão correta de qualquer risco. Consequentemente, convém que arranjos de gestão de riscos incluam métodos (por exemplo, de pesquisa) para coletar ou gerar informações. No entanto, apesar dos melhores esforços, a informação disponível pode às vezes ser limitada, por exemplo, antecipar o que vai acontecer no futuro pode ser limitado ao uso de projeções estatísticas.

Convém que a sensibilidade das decisões a quaisquer incertezas na informação seja entendida. A confiabilidade da avaliação de risco dependerá, em parte, da clareza e precisão dos critérios de risco. A coleta de dados relacionados a riscos (por exemplo, a ocorrência de incidentes e outras informações baseadas na experiência) pode ajudar em predições estatísticas.

Embora a tomada de decisões baseada em evidências seja o objetivo final, isso pode não ser sempre possível com o tempo ou os recursos disponíveis. Em tais situações, convém que o julgamento de especialistas seja usado, em combinação com a informação disponível. No entanto, é necessário cuidado para evitar julgamento enviesado. Além disso, as evidências do passado podem não prever com precisão o futuro. Em situações que envolvam o potencial

existe un potencial de eventos de muy alta consecuencia, la ausencia de información podría desencadenar en una acción si hay evidencia de daño potencial, más que una prueba definitiva de daño.

Este principio también es aplicable al diseño (o mejora) del marco de gestión del riesgo, ya que habrá aspectos del marco (por ejemplo, los que proporcionan la capacidad de investigar, reunir, analizar, actualizar y poner a disposición la información para apoyar la aplicación del proceso) que determinará qué tan bien se aplica este principio.

Se debería evaluar periódicamente la fiabilidad y la exactitud de la información para determinar su pertinencia, oportunidad y fiabilidad, con supuestos documentados. El marco debería establecer una revisión periódica para las actualizaciones o correcciones.

Ayuda práctica

- Primero debería considerarse en forma cuidadosa cómo la información de los incidentes podría ayudar en la toma de decisiones para diseñar cómo serán informados, es decir, por ejemplo quiénes son los actuales y futuros usuarios finales, y cómo puede ser necesario ordenar la información, cómo se puede mejorar su integridad, y cómo se puede acceder a ella. Una vez que esto se ha hecho, se puede diseñar la forma de los informes, teniendo en cuenta que la calidad suministrada puede ser afectada por el tiempo necesario para su ingreso.

- Se debería incluir una descripción del contexto (incluyendo la fecha en que fue realizada) como parte del detalle y documentar las descripciones de los principales riesgos que enfrentan (por ejemplo, registros de riesgos). Esto permite que los usuarios del registro tengan en cuenta cualquier cambio en el contexto que pudo haber ocurrido, posteriormente, con los cambios en el riesgo resultante.

- Cuando se hayan hecho suposiciones en una evaluación, se debería registrar claramente y comprender la justificación de esos supuestos, incluyendo cualquier limitación.

- En el diseño de los tratamientos del riesgo debería considerarse cómo se realizará el seguimiento del desempeño de los controles resultantes y cómo se pondrán a disposición de los que a futuro tomaran las decisiones, quienes podrían confiar en esos controles.

B.2.7 La gestión del riesgo está hecha a medida

B.2.7.1 Principio

para eventos de consequência elevada, a ausência de informações pode levar à ação imediata se houver evidência de dano potencial, em vez de uma prova definitiva de dano.

Este princípio também é aplicável à concepção (ou melhoria) da estrutura para gerenciar os riscos, porque haverá aspectos da estrutura (por exemplo, aqueles que fornecem capacidade de investigação ou que coletam, analisam, atualizam e disponibilizam informações para apoiar a aplicação do processo) que determinarão a melhor maneira de se aplicar este princípio.

Convém que a confiabilidade e a precisão das informações sejam regularmente avaliadas quanto à sua relevância, oportunidade e confiabilidade, com os pressupostos documentados. Convém que a estrutura preveja análises críticas periódicas, bem como atualizações ou correções.

Ajuda prática

- Ao conceber como os incidentes são reportados, convém que primeiro se considere cuidadosamente quais decisões esta informação poderia ajudar, ou seja, quem são os atuais e futuros usuários finais, como pode ser necessário ordenar a informação, como a sua integridade pode ser melhorada, e como ela pode ser acessada. Uma vez que isto tenha sido realizado, o formulário de reporte pode ser concebido, tendo em conta que a qualidade fornecida pode ser influenciada pelo tempo necessário para a sua entrada.

- Convém que a descrição do contexto (incluindo a data em que foi escrito) seja incluída como parte das descrições detalhadas e documentadas dos riscos-chave encarados (por exemplo, registro de risco). Isto permite aos usuários do registro levar em conta quaisquer mudanças no contexto que possam ter ocorrido subsequentemente, com as alterações resultantes no risco.

- Onde tiverem sido feitas suposições em uma avaliação, convém que a justificativa para essas suposições, incluindo quaisquer limitações, seja claramente registrada e compreendida.

- Ao conceber tratamentos de risco, convém considerar como o desempenho dos controles resultantes será monitorado e disponibilizado para os futuros tomadores de decisão, que podem estar apoiados nesses controles.

B.2.7 A gestão de riscos é feita sob medida

B.2.7.1 Princípio

g) La gestión del riesgo está hecha a medida
La gestión del riesgo está alineada con el contexto interno y externo de la organización, y con su perfil de riesgo.

B.2.7.2 Cómo aplicar el principio

La Norma ISO 31000 proporciona un enfoque genérico para la gestión del riesgo, que es aplicable a todo tipo de organización y de riesgo. Todas las organizaciones tienen su propia cultura y sus características, criterios de riesgo y contextos de operación. La gestión del riesgo debería adaptarse para satisfacer las necesidades de cada organización.

No hay una sola manera, correcta para diseñar e implementar el marco y los procesos de gestión del riesgo, ya que requieren flexibilidad y adaptación en cada una de las organizaciones. El diseño puede ser determinado por muchos aspectos, como el tamaño de la organización, la cultura, el sector, la configuración y el estilo de gestión.

Las diferentes áreas de riesgo pueden requerir diferentes procesos a la medida dentro de la misma organización. Mientras que todos los procesos sean consistentes con la Norma ISO 31000, igualmente habrá diferencias en los sistemas, en los modelos y nivel de juicio implicado; por ejemplo entre los que participan en la evaluación de la información sobre los riesgos relacionados a la tecnología, los riesgos de tesorería y de inversión, o los riesgos de la competencia. Cada proceso debería adaptarse a su propósito específico.

Dado que el objetivo del marco es asegurar que el proceso de gestión del riesgo se aplique en las decisiones de una forma eficaz y que refleje la política, el diseño del marco debería reflejar dónde y cómo se toman las decisiones, y que tenga en cuenta las obligaciones con las cuales se compromete la organización ya sean legales o externas de otro tipo.

Es importante tener en cuenta que la adaptación no implica que cualquiera de los elementos del marco (como se describe en la Norma ISO 31000:2009, Capitulo 4) o los pasos del proceso (ver la Norma ISO 31000:2009, Capítulo 5) se modifiquen. Todos son esenciales para la gestión eficaz del riesgo.

Este principio es importante en el diseño y la mejora del marco de gestión del riesgo, pero también es pertinente en la forma en que se estructuran los aspectos del proceso.

g) A gestão de riscos é feita sob medida.
A gestão de riscos está alinhada com o contexto interno e externo da organização e com o perfil do risco.

B.2.7.2 Como aplicar o princípio

A ISO 31000 oferece uma abordagem genérica para a gestão de riscos que é aplicável a todos os tipos de organizações e todos os tipos de risco. Todas as organizações têm sua própria cultura e características, critérios de risco e contextos de operação. Convém que a gestão de riscos seja ajustada para atender às necessidades de cada organização.

Não há uma maneira única correta para conceber e implementar a estrutura e os processos de gestão de riscos, uma vez que exigem flexibilidade e adaptação em cada organização. A concepção pode ser determinada por vários aspectos, incluindo o tamanho da organização, cultura, setor, configuração e estilo de gestão.

Diferentes áreas de risco podem requerer diferentes processos sob medida dentro de uma mesma organização. Enquanto convém que todos os processos sejam consistentes com a ISO 31000, haverá diferenças nos sistemas, modelos e nível de julgamento envolvidos, por exemplo, entre aqueles envolvidos na avaliação de riscos relacionados à tecnologia da informação, riscos de tesouraria e investimento, ou riscos dos concorrentes. Convém que cada processo seja ajustados ao seu propósito específico.

Como o objetivo da estrutura é assegurar que o processo de gestão de riscos será aplicado para a tomada de decisões de uma forma que seja eficaz e reflita a política, convém que a concepção da estrutura reflita onde e como as decisões são tomadas, e convém que leve em conta quaisquer obrigações legislativas ou outras externas com as quais a organização esteja comprometida.

É importante ter em mente que fazer sob medida não implica que os elementos da estrutura (como descrito na ISO 31000:2009, Seção 4) ou as etapas do processo (ver ISO 31000:2009, Seção 5) devam ser variados. Todos são essenciais para a gestão eficaz dos riscos.

Este princípio é importante durante a concepção e melhoria da estrutura de gerenciamento de risco, mas também será pertinente à forma em que esses aspectos do processo são estruturados.

Este principio también puede significar que la organización tenga en cuenta las cuestiones internas, por ejemplo la rotación del personal (que, si es muy alta, puede requerir ajustes apropiados en el ámbito de la formación inicial, con el fin de asegurar que todos los nuevos empleados son capaces de cumplir lo que se requiere de ellos en relación con la gestión del riesgo).

La adaptación del marco es necesaria para lograr la integración con los procesos de toma de decisiones de la organización, También es posible que los procesos de toma de decisiones necesiten ser modificados para adaptarse a un marco estructurado de gestión del riesgo.

Ayuda práctica

- El diseño del marco de gestión del riesgo incluye la consideración de las opiniones de los que van a participar en su aplicación.

- La construcción de una comprensión más profunda de los conceptos fundamentales de la Norma ISO 31000 ayuda a asegurar el marco que se adapta y que el proceso alcanzará los atributos de una gestión del riesgo eficaz, como se indica en la Norma ISO 31000:2009, Anexo A. Por el contrario, esto no se logrará marcando casillas simplemente.

B.2.8 La gestión del riesgo tiene en cuenta factores humanos y culturales

B.2.8.1 Principio

h) La gestión del riesgo tiene en cuenta factores humanos y culturales

La gestión de riesgos reconoce las capacidades, percepciones e intenciones de las personas internas y externas que pueden facilitar o dificultar el logro de los objetivos de la organización.

B.2.8.2 Cómo aplicar el principio

Este principio consiste en obtener las opiniones de las partes interesadas, así como la comprensión de que esos puntos de vista pueden ser influidos por las características humanas y culturales. Los factores a considerar son el social, político y cultural, así como el concepto de tiempo.

Los tipos comunes de error incluyen lo siguiente:

a) el fracaso para detectar y responder a las alertas tempranas;

b) la indiferencia ante las opiniones de los demás o la falta de conocimiento;

c) el sesgo debido a la simplificación de las

Este princípio também pode significar que a organização precisa considerar questões internas, por exemplo, rotatividade de pessoal (que, se bastante elevada, pode requerer ajustes apropriados no treinamento inicial, a fim de assegurar que todos os novos funcionários são capazes de cumprir o que lhes é requerido em relação à gestão de riscos).

Ajustar a estrutura é necessário para atingir a integração com os processos de tomada de decisão da organização. Também é possível que esses processos de tomada de decisão precisem ser modificados para se encaixar a uma estrutura de gestão de riscos.

Ajuda prática

- Convém que a concepção da estrutura para gestão de riscos inclua buscar e levar em conta os pontos de vista daqueles que serão envolvidos na sua implementação.

- Construir uma compreensão mais aprofundada dos conceitos subjacentes da ISO 31000 ajudará a assegurar que o ajuste tanto da estrutura quanto do processo atingirá os atributos de uma gestão de riscos eficaz, como referido na ISO 31000:2009, Anexo A. Por outro lado, apenas “assinalar caixinhas” não alcançará isto.

B.2.8 A gestão de riscos considera fatores humanos e culturais

B.2.8.1 Princípio

h) A gestão de riscos considera fatores humanos e culturais.

A gestão de riscos reconhece as capacidades, percepções e intenções de pessoas externas e internas que podem facilitar ou dificultar o atingimento dos objetivos da organização.

B.2.8.2 Como aplicar o princípio

Este princípio envolve a obtenção das visões das partes interessadas, bem como a compreensão de que essas visões podem ser influenciadas por características humanas e culturais. Fatores a serem considerados incluem os sociais, políticos e culturais, bem como conceitos de tempo.

Os tipos comuns de erro incluem os seguintes:

a) falha em detectar e responder a alertas precoces;

b) indiferença em relação às opiniões de outros, ou a uma falta de conhecimento;

c) viés devido a estratégias simplificadas de

estrategias de tratamiento de la información para abordar cuestiones complejas;

d) la falta de reconocimiento de la complejidad.

En el diseño de la estructura y en la aplicación de todos los aspectos del proceso de gestión del riesgo, es necesario adoptar medidas específicas con el fin de comprender y aplicar los factores humanos y culturales.

El diseño de la estructura y la comunicación sobre el riesgo deberían tener en cuenta las características culturales y los niveles de conocimiento de la audiencia.

Ayuda práctica

- Los gerentes deberían actuar de forma de promover y apoyar el respeto y la comprensión de las diferencias individuales.

- Las personas aprecian que se les pregunte por su opinión.

- Como regla general, las organizaciones premian lo que valoran. Si la selección de los empleados, la promoción y la remuneración no están abiertamente vinculadas con el desempeño real de gestión del riesgo, es poco probable que la actuación cumpla con el nivel esperado. Se debería reconocer adecuadamente los esfuerzos de las personas.

- Como regla general, no es recomendable confiar en un único control humano - dependiente para hacer una gran modificación en el riesgo.

- Las organizaciones transnacionales son sabias para reconocer la importancia de la cultura en la determinación del comportamiento de las personas.

Ayuda práctica

- Los siguientes son ejemplos de preguntas de utilidad acerca de los factores humanos y organizacionales:

- ¿La estructura de la organización es adecuada a las necesidades de la organización?

- ¿Están claramente identificadas las responsabilidades formales de las personas?

- ¿Todas las descripciones de cargo contienen especificaciones claras de los niveles de autoridad y responsabilidad individuales?

- ¿Son todos los canales de comunicación claros y eficaces?

- ¿De vez en cuando se verifica si la comunicación es comprendida e interpretada correctamente en todos los niveles de la organización?

processamento de informação para tratar de questões complexas;

d) falha em reconhecer complexidades.

Ao conceber a estrutura e ao aplicar todos os aspectos do processo de gestão de riscos, ações específicas são necessárias, a fim de compreender e aplicar esses fatores humanos e culturais.

Convém que a concepção da estrutura e a comunicação sobre o risco leve em conta as características culturais e níveis de conhecimento da audiência.

Ajuda prática

- Convém que os gestores ajam de modo a mostrar que promovem e apoiam o respeito e a compreensão das diferenças individuais.

- As pessoas gostam de ser perguntadas sobre a sua opinião.

- Como regra geral, as organizações premiam aquilo que valorizam. Se a seleção, promoção e remuneração de funcionários não estão abertamente ligadas ao real desempenho da gestão de riscos, é improvável que esse desempenho atinja o nível esperado. Convém que os esforços individuais sejam reconhecidos de forma apropriada.

- Como regra geral, não é prudente confiar em um único controle humano-dependente para fazer uma grande modificação ao risco.

- As organizações transnacionais serão sensatas ao reconhecer a importância da cultura na determinação do modo como as pessoas se comportam.

Ajuda prática

- Exemplos de perguntas úteis a fazer sobre fatores humanos e organizacionais incluem os seguintes:

- A estrutura organizacional é adequada às necessidades da organização?

- Os indivíduos com responsabilidades formais são claramente identificados?

- Todas as descrições de trabalho contêm especificações claras de autoridades e responsabilidades do indivíduo?

- Todos os canais de comunicação são claros e eficazes?

- É ocasionalmente verificado se a comunicação é corretamente entendida e interpretada em todos os níveis da organização?

- ¿Se controla el nivel moral en la organización?

- ¿Se revisan las interfaces de opinión entre los equipos?

- ¿Existen mecanismos para reconocer y responder a los rumores dentro de la organización antes de que impacten de manera negativa?

- ¿Existen políticas claras de contratación, remuneración y promoción?

- Si las políticas son problemáticas, ¿hay un proceso de revisión?

- ¿Se respetan las políticas y los procedimientos? Si no es así, ¿hay una investigación? ¿Se promueven?

- ¿Los auditores internos y externos buscan conductas inseguras o poco éticas de la organización?

B. 2.9 La gestión del riesgo es transparente e inclusiva

B.2.9.1 Principio

i) La gestión del riesgo es transparente e inclusiva.
La participación, de las partes interesadas, adecuada y oportuna en todos los niveles de la organización, en particular de los que toman decisiones, asegura que la gestión del riesgo siga siendo pertinente y actualizada. La participación también permite que las partes interesadas estén representadas adecuadamente y que sus opiniones sean tenidas en cuenta en la determinación de los criterios de riesgo.

B.2.9.2 Cómo aplicar el principio

Este principio puede tener efecto en múltiples niveles. Esto puede reflejarse en la organización, en la política de gestión del riesgo (por ejemplo "Vamos a informar y consultar a las partes interesadas siempre que sea posible con el fin de que entiendan nuestros objetivos y puedan contribuir con sus conocimientos y puntos de vista ayudando en nuestra toma de decisiones").

La consulta con las partes interesadas como parte de la aplicación del proceso de gestión del riesgo requiere una planificación cuidadosa. Es aquí que la confianza se puede construir o destruir. Para ser eficaz y reforzar la confianza en los resultados, es conveniente que las partes interesadas pertinentes participen en todos los aspectos del proceso de gestión del riesgo, incluyendo el diseño del proceso de comunicación y consulta.

- O nível de moralidade na organização é monitorado?

- As interfaces são analisadas criticamente entre as equipes?

- Existem mecanismos para reconhecer e responder a rumores dentro da organização antes que gerem um impacto negativo?

- Existem políticas de recrutamento, remuneração e promoção claras?

- Se as políticas são problemáticas, há um processo de análise crítica?

- Há adesão às políticas e procedimentos? Se não, há uma investigação? Elas são aplicadas?

- Auditores internos e externos procuram observar comportamento inseguro ou antiético na organização?

B.2.9 A gestão de riscos é transparente e inclusiva

B.2.9.1 Princípio

i) A gestão de riscos é transparente e inclusiva.
O envolvimento apropriado e oportuno das partes interessadas e, em particular, dos tomadores de decisão em todos os níveis da organização, assegura que a gestão de riscos permaneça relevante e atualizada. O envolvimento também permite que as partes interessadas sejam devidamente representadas e tenham suas opiniões levadas em conta na determinação dos critérios de risco.

B.2.9.2 Como aplicar o princípio

Este princípio pode ser aplicado em vários níveis. Pode ser refletido na política de gestão de riscos, da organização (por exemplo, “Vamos informar e consultar as partes interessadas, sempre que possível, a fim de que compreendam os nossos objetivos e possam contribuir com seus conhecimentos e pontos de vista para ajudar na nossa tomada de decisão”).

Consulta às partes interessadas, como parte da aplicação do processo de gestão de riscos, necessita de um planejamento cuidadoso. É aqui que a confiança pode ser construída ou destruída. Para ser eficiente e reforçar a confiança nos resultados, convém que as partes interessadas pertinentes sejam envolvidas em todos os aspectos do processo de gestão de riscos, incluindo a concepção do processo de comunicação e consulta.

Es conveniente que la aplicación de este principio considere los aspectos de confidencialidad, la seguridad y la privacidad, por ejemplo, esto puede requerir que la información en los registros de riesgos sea segregada de forma que el acceso a cierta información sea restringido.

Ayuda práctica

- El juego de roles debería incluirse en relación con la comunicación y la consulta en la formación en gestión del riesgo.

- Debería realizarse una evaluación de la forma en que se percibirá la recepción de la información.

- Debería proporcionarse la retroalimentación periódica para demostrar que lo que se prometió o proyectó efectivamente se realizó en la práctica.

- Debería promoverse los puntos de vista no solicitados, y que sean reconocidos y apreciados, y siempre que sea posible, realizar la retroalimentación a los comentarios recibidos.

B.2.10 La gestión del riesgo es dinámica, iterativa y capaz de reaccionar ante los cambios.

B.2.10.1 Principio

j) La gestión del riesgo es dinámica, iterativa y capaz de reaccionar ante los cambios.

La gestión del riesgo detecta y responde a los cambios continuamente. Cuando se producen los acontecimientos externos e internos, el contexto y el conocimiento cambia, da lugar al control y la revisión de los riesgos, surgen nuevos riesgos, algunos cambian, y otros desaparecen.

B.2.10.2 Cómo aplicar el principio

Cualquier cambio en la organización, los objetivos, o cualquier aspecto de las circunstancias internas o externas, cambiará inevitablemente el riesgo (por ejemplo, una reestructuración interna, un nuevo proveedor principal, o un cambio en una ley pertinente). Del mismo modo, los cambios en el contexto de la organización (por ejemplo, la adquisición de otra empresa, o conseguir un nuevo contrato importante) pueden requerir cambios en el marco (por ejemplo, en formación, especialistas en riesgo). Es conveniente que los procesos de gestión del riesgo sean diseñados para reflejar la dinámica de la organización (por ejemplo, velocidad de cambio).

La Norma ISO 31000 contiene dos regímenes de seguimiento y control (para el marco y el proceso). Cada uno es específico a su propósito, y cada uno requiere planificación y ejecución.

Convém que a implementação deste princípio considere questões de confidencialidade, segurança e privacidade, por exemplo, isso pode requerer que as informações em registros de riscos sejam segregadas para que o acesso a alguma informação possa ser restringido.

Ajuda prática

- Convém que simulação de papéis seja incluída em relação à comunicação e consulta, na formação em gestão de riscos.

- Convém que uma avaliação seja feita sobre a forma como aqueles que recebem a informação a percebem.

- Convém que uma retroalimentação periódica seja efetuada para demonstrar o quão bem o que foi prometido ou concebido realmente funcionou na prática.

- Convém que visões não solicitadas sejam encorajadas, reconhecidas e apreciadas, e sempre que possível, convém que uma retroalimentação sobre elas seja fornecida.

B.2.10 A gestão de riscos é dinâmica, iterativa e capaz de reagir a mudanças

B.2.10.1 Princípio

j) A gestão de riscos é dinâmica, iterativa e capaz de reagir a mudanças.

A gestão de riscos percebe continuamente a mudança e responde a mesma. Como ocorrem eventos externos e internos, o contexto e o conhecimento mudam, acompanhamento e revisão dos riscos ocorrem, novos riscos surgem, alguns mudam e outros desaparecem.

B.2.10.2 Como aplicar o princípio

Qualquer alteração nos objetivos da organização, ou qualquer aspecto das circunstâncias internas ou externas, modificará inevitavelmente o risco (por exemplo, uma reestruturação interna, um novo grande fornecedor, ou uma mudança na legislação pertinente). Da mesma forma, mudanças no contexto organizacional (por exemplo, a aquisição de outra empresa, ou conseguir um novo grande contrato) podem requerer mudanças na estrutura (por exemplo, em treinamento, especialistas de risco). Convém que processos de gestão de riscos sejam concebidos para refletir a dinâmica da organização (por exemplo, velocidade de mudança).

A ISO 31000 contém dois regimes de monitoramento e análise crítica (para a estrutura e o processo). Cada um é específico para o seu propósito, e cada um requer reflexão e implementação.

Se debería realizar seguimiento y control y revisión al marco para asegurar que puede continuar dando cumplimiento a estos principios de gestión del riesgo de forma eficaz, poner en práctica la política de gestión del riesgo de la organización, y apoyar la aplicación del proceso de toma de decisiones en toda la organización.

El seguimiento y control y revisión deberían incorporarse en cada uno de los pasos fundamentales del proceso de gestión del riesgo.

También se deberían revisar los controles sean revisados para asegurar su eficacia en respuesta a los cambios. Por ejemplo, los controles que dependen del desempeño particular de las personas no pueden ser tan eficaces si hay cambios en el personal.

El seguimiento, el control y la revisión deberían adaptarse cuidadosamente, en particular, para que puedan ser sensibles a los factores de cambio que pueden tener efectos más profundos. En el seguimiento, el control y la revisión debería evaluarse la importancia continua de los indicadores y, en caso de ser necesario, los indicadores tendrían que adaptarse a las circunstancias cambiantes o emergentes.

El seguimiento, el control y la revisión son actividades distintas, como se explica en la Norma ISO 31000:2009, 4.5 y 5.6. El seguimiento y control se refiere a la observación continua de los parámetros claves para determinar si se están realizando según lo previsto o como se supone. La revisión ocurre de vez en cuando, se estructura en cuanto a su propósito y está destinada en general para determinar si los supuestos sobre los que se toman las decisiones (por ejemplo, el diseño del marco) se mantienen al día, y por lo tanto si las decisiones resultantes necesitan revisión. La revisión también debería tener en cuenta los nuevos conocimientos y las tecnologías.

Ayuda práctica

- Al aplicar el proceso de gestión del riesgo y el desarrollo de la declaración de contexto, se deberían identificar los elementos (por ejemplo, las características del entorno externo) que tienen más probabilidades de cambio y se les debería realizar el seguimiento y control de cerca para identificar los cambios. Cualquier cambio podría requerir una reevaluación de todos o algunos de los riesgos documentados.

- Las personas deberían ser alentadas a informar acerca de la situación actual (incluidos los denunciantes).

- Incluso las organizaciones pequeñas deberían tener en cuenta los cambios globales, por ejemplo,

Convém que a estrutura seja monitorada e analisada criticamente para assegurar que possa continuar a pôr em prática estes princípios da gestão de riscos eficaz, por em prática a política de gestão de risco da organização e apoiar a aplicação do processo na tomada de decisão em toda a organização.

Convém que o monitoramento e a análise crítica sejam incorporados em cada uma das etapas centrais do processo de gestão de riscos.

Convém que controles também sejam analisados criticamente para assegurar a sua contínua eficácia em resposta à mudança. Por exemplo, controles que são dependentes do desempenho de pessoas em particular podem não ser tão eficazes caso haja mudanças no pessoal.

Convém que monitoramento e análise crítica sejam cuidadosamente ajustados, em particular de modo a serem sensíveis aos fatores de mudança que podem ter os efeitos mais profundos. Convém que o monitoramento e a análise crítica avaliem a contínua significância dos indicadores monitorados e, se necessário, os indicadores necessitarão ser adaptados às circunstâncias em mudança ou emergentes.

Monitoramento e análise crítica são atividades distintas, como explicado na ISO 31000:2009, 4.5 e 5.6. O monitoramento diz respeito à observação contínua de parâmetros-chave para determinar se estão desempenhando como pretendido ou assumido. A análise crítica ocorre de tempos em tempos, é estruturada de acordo com o seu propósito e geralmente destina-se a determinar se as suposições com base nas quais as decisões foram tomadas (por exemplo, a concepção da estrutura) permanecem atuais e, portanto, se as decisões resultantes precisam ser analisadas criticamente. Convém que a análise crítica também leve em consideração novos conhecimentos e tecnologias.

Ajuda prática

- Ao aplicar o processo de gestão de riscos e desenvolvimento da declaração do contexto, convém que os componentes (por exemplo, características do ambiente externo) que têm maior probabilidade de mudar sejam identificados, e convém que eles sejam cuidadosamente monitorizados para a mudança. Qualquer alteração pode exigir uma reavaliação de todos ou de alguns dos riscos documentados.

- Convém que as pessoas sejam encorajadas a reportar preocupações com o *status quo* (incluindo delatores).

- Convém que mesmo as pequenas empresas tenham em mente as mudanças globais, por

la crisis financiera mundial de 2008 tuvo un profundo impacto en algunos pequeños proveedores cuyos principales clientes eran organizaciones afectadas directa o indirectamente por los fracasos de los bancos. Este tipo de acontecimientos externos o circunstancias emergentes pueden requerir cambios proactivos para el marco de gestión del riesgo.

exemplo, a crise financeira global de 2008 teve impactos profundos sobre alguns pequenos fornecedores cujos principais clientes eram organizações impactadas direta ou indiretamente por falências bancárias. Tais eventos externos ou circunstâncias emergentes podem exigir mudanças proativas para a estrutura de gerenciamento de risco.

B.2.11 La gestión del riesgo permite la mejora continua de la organización

B.2.11 A gestão de riscos facilita a melhoria contínua da organização

B.2.11.1 Principio

B.2.11.1 Princípio

k) La gestión del riesgo permite la mejora continua de la organización,
Es conveniente que las organizaciones desarrollen y apliquen estrategias para mejorar su grado de madurez de gestión del riesgo junto con todos los demás aspectos de su organización.

k) A gestão de riscos facilita a melhoria contínua da organização.
Convém que as organizações desenvolvam e implementem estratégias para melhorar a sua maturidade na gestão de riscos juntamente com todos os demais aspectos de sua organização.

B.2.11.2 Cómo aplicar el principio

B.2.11.2 Como aplicar o princípio

La mejora continua del desempeño de la organización está interrelacionada con la mejora continua del desempeño de la gestión del riesgo. La mejora de la gestión del riesgo, sobre la base de la toma de decisiones basada en el riesgo, puede reducir la incertidumbre en el logro de los objetivos, minimizar la volatilidad y aumentar la agilidad. Sin embargo, se debería tener cuidado de no complicar el desempeño de la gestión del riesgo hasta el punto de ahogar la búsqueda de oportunidades y la flexibilidad de la respuesta.

A melhoria contínua do desempenho organizacional está inter-relacionada à melhoria contínua do desempenho da gestão de riscos. Uma gestão de riscos melhorada, de acordo com a tomada de decisão baseada no risco, pode reduzir a incerteza no atingimento dos objetivos, minimizar a volatilidade e aumentar a agilidade. No entanto, convém que se tome cuidado para não complicar demasiadamente o desempenho de gestão de riscos, a ponto de sufocar a busca de oportunidades e a flexibilidade de resposta.

En su lugar, la importancia de este principio radica en que las organizaciones estén atentas a nuevas oportunidades de mejora. Tales oportunidades pueden surgir internamente (por ejemplo, al aprender de los incidentes notificados) o externamente (por ejemplo, la disponibilidad de nuevas herramientas y los conocimientos que puedan mejorar la gestión del riesgo).

Em vez disso, a importância deste princípio reside nas organizações permanecerem alertas a novas oportunidades de melhoria. Essas oportunidades podem surgir internamente (por exemplo, a aprendizagem a partir de incidentes reportados) ou externamente (por exemplo, por meio da disponibilidade de novas ferramentas e conhecimentos que possam melhorar a gestão de riscos).

Este principio también es pertinente en la búsqueda continua de mejoras en la eficiencia de la gestión del riesgo, por ejemplo, la implementación de nuevas tecnologías que conecten mejor a los que toman decisiones con la información.

Este princípio também é pertinente para a busca contínua de melhorias na eficiência da gestão de riscos, por exemplo, a implantação de novas tecnologias que melhor conectam os tomadores de decisão à informação.

El objetivo de la mejora continua debería quedar claro en la política de gestión del riesgo de la organización, y debería ser comunicada continuamente tanto de formas formales como informales.

Convém que o objetivo de melhoria contínua fique claro na política de gestão de riscos da organização e convém que ele seja continuamente comunicado em ambos os sentidos formal e informal.

La mejora continua puede incluir lo siguiente:

A melhoria contínua pode incluir o seguinte:

- mejora en el grado de integración de la actividad de gestión del riesgo con la actividad general;

- melhorar o grau de integração da atividade de gestão de riscos à atividade geral;

- mejora en la calidad de la evaluación del riesgo;

- mejora en el marco, por ejemplo, la calidad y el acceso a la información;

- mejora en la velocidad de la toma de decisiones.

La mejora continua se basa en indicadores cualitativos y cuantitativos de avance. Las organizaciones que utilizan los enfoques graduales y los modelos de madurez deberían diseñarlo como impulsores de la mejora continua en función de los recursos y la cultura de la organización. Se debería reconocer que las conductas humanas exitosas generan éxitos. El propósito de la gestión del riesgo eficaz recae exclusivamente en el aumento de la probabilidad de que una organización logre sus objetivos en su totalidad. Cuanto más rápidamente una organización puede lograr una gestión eficaz del riesgo, logrará sus objetivos de forma más eficiente.

En términos puramente prácticos, puede tardar tiempo para lograr algunas mejoras, por ejemplo, algunas pueden requerir la asignación de un presupuesto, o una cuidadosa planificación y puesta en marcha. Los planes de mejora deberían considerar las prioridades y los beneficios relativos y permitir el seguimiento de los avances.

Ayuda práctica

- Utilizando los elementos de seguimiento y control y revisión del marco debería realizarse una revisión anual de la actuación en comparación con los principios de gestión del riesgo y mejora en el diseño.

- Se debería evaluar y revisar la adecuación, idoneidad y eficiencia del marco de gestión del riesgo.

- Debería utilizarse un sistema de notificación de incidentes para llevar a cabo el análisis de causa raíz, buscando no sólo las causas proximales de los hechos, sino también las características del marco de gestión del riesgo que hicieron posible que el incidente se produzca.

- Debería controlarse el éxito (por ejemplo, un proyecto a tiempo y cumpliendo el presupuesto) a fin de entender qué características del marco de gestión del riesgo han facilitado el éxito, y esto debería comunicarse para reforzar el valor.

- melhorar a qualidade da avaliação de riscos;

- melhorar a estrutura, por exemplo, a qualidade e o acesso à informação;

- melhorar a velocidade da tomada de decisão.

A melhoria contínua é baseada em indicadores de progresso qualitativos e quantitativos. Convém que as organizações que usam abordagens por fases e modelos de maturidade os concebam como impulsionadores de melhoria contínua, com base nos recursos e na cultura da organização. Convém que reconheçam que em muitos empreendimentos humanos sucesso gera sucesso. O propósito de gerenciar riscos com eficácia reside somente em aumentar a probabilidade de que uma organização atinja os seus objetivos na íntegra. Quanto mais rapidamente uma organização puder atingir uma gestão de riscos eficaz, mais eficientemente alcançará seus objetivos.

Em termos puramente práticos, algumas melhorias podem levar algum tempo para serem atingidas, por exemplo, algumas podem requerer alocação de recursos, ou um planejamento cuidadoso e respectiva implantação. Convém que planos de melhoria considerem as prioridades e benefícios relativos, e que permitam o monitoramento dos progressos.

Ajuda prática

- Usando os elementos de monitoramento e análise crítica da estrutura, convém que seja conduzida uma análise crítica anual do desempenho em relação a estes princípios de gestão de riscos e melhorias na concepção.

- Convém que a adequação e a eficiência da estrutura para a gestão de riscos sejam avaliadas e analisadas criticamente.

- Convém que o sistema de reporte de incidentes seja utilizado para conduzir análises de causa-raiz, em busca não só das causas do incidente, mas também das características da estrutura para gestão de riscos que tornaram possível a ocorrência do incidente.

- Convém que o sucesso (por exemplo, um projeto realizado dentro do tempo e orçamento previstos) seja monitorado de forma a permitir o entendimento daquelas características da estrutura para gerenciar riscos que mais facilitaram o sucesso, e convém que isso seja comunicado para reforçar o valor.

Anexo C
(informativo)

¿Cómo expresar el mandato y el compromiso?

Como expressar mandato e comprometimento?

C.1 Generalidades

En este Anexo se ofrecen orientaciones y estrategias sobre cómo la organización puede expresar y comunicar el mandato y el compromiso.

Para ser eficaz es conveniente que por mandato y compromiso, la alta dirección y el órgano de supervisión de la organización expresen claramente a las partes interesadas el enfoque de la gestión del riesgo y documenten y comuniquen esto, según el caso. El mandato para la gestión del riesgo suele implicar cambios en el comportamiento, la cultura, la política, los procesos y el desempeño esperado en la gestión del riesgo que se reflejarán en el marco de gestión del riesgo. El mandato y el compromiso podría ser una declaración de política de corto plazo, que es comunicada ampliamente.

El desarrollo del mandato implica decidir el curso de acción requerido, así como autorizar que se realice. Invariablemente, en las organizaciones existentes, esto implicará necesariamente la autoridad para lograr un cambio. No tendría mucho sentido identificar el curso de acción preferido a menos que, al mismo tiempo, exista un compromiso adecuado para lograrlo.

El mandato y el compromiso es una parte fundamental del marco de gestión del riesgo. Debería ser parte de las estructuras de la organización, de gestión y de gobierno e influir en el diseño de ambos.

El mandato y el compromiso deberían reflejar los once principios establecidos en la Norma ISO 31000:2009, Capítulo 3.

En la práctica, el mandato de la organización, y su compromiso son expresados, y se perciben tanto de forma explícita como implícita. Las expresiones implícitas (por ejemplo, las acciones del día a día de la alta dirección y del órgano de supervisión dentro de la cultura organizacional predominante) suelen proporcionar un estímulo más poderoso que las expresiones explícitas (por ejemplo, una política de gestión del riesgo por escrito).

C.1 Geral

Este Anexo fornece diretrizes e estratégias sobre como o mandato e o comprometimento podem ser expressos e comunicados por uma organização.

Para que o mandato e o comprometimento sejam efetivos, convém que a Alta Direção e o organismo de supervisão da organização expressem claramente às partes interessadas a abordagem para gerenciar riscos e a documentem e comuniquem conforme apropriado. O mandato para a gestão de riscos tipicamente envolve mudanças no comportamento, cultura, política, processos, e o desempenho esperado na gestão de riscos que se refletirão na estrutura para a gestão de riscos. O mandato e o comprometimento poderiam ser uma curta declaração de política que é amplamente comunicada.

O desenvolvimento do mandato envolve a tomada de decisão sobre o modo de ação requerido, assim como a autorização para que ocorra. Invariavelmente, em organizações existentes, isto necessariamente envolverá uma autoridade para suscitar mudanças. Não haveria muito sentido em identificar a linha de ação preferida, salvo se houvesse, concomitantemente, um comprometimento correspondente para que ocorra.

Mandato e comprometimento são uma parte fundamental da estrutura para gerenciar riscos. Convém que sejam parte das estruturas de gestão e de governança da organização e que influenciem a concepção de ambas.

Convém que o mandato e o comprometimento reflitam os onze princípios estabelecidos na ISO 31000:2009, Seção 3.

Na prática, o mandato da organização e seu comprometimento para com ele são expressos e percebidos tanto de maneira explícita quanto implícita. As expressões implícitas (por exemplo, as ações do dia a dia da Alta Direção e do organismo de supervisão dentro da cultura organizacional prevalecente) tipicamente fornecem um estímulo mais poderoso do que as expressões explícitas (por exemplo, uma política escrita de gestão de riscos).

C.2 Métodos para expresar el mandato y el compromiso

C.2.1 Principales características

La expresión del mandato y el compromiso deberían cumplir con los siguientes criterios:

a) ser compatibles con la organización, su plan estratégico, los objetivos, las políticas, los estilos de comunicación y el sistema de gestión;

b) ser compatibles con los criterios de riesgo determinados por el organismo de supervisión;

c) cumplir con los principios de la Norma ISO 31000, así como buscar la excelencia en la gestión del riesgo como se indica en la Norma ISO 31000:2009, Anexo A;

d) ser fácil de comunicar y evaluar su comprensión dentro y fuera de la organización;

e) tener expectativas razonables de ser implementada con éxito;

f) atender a las responsabilidades de los dueños de los riesgos.

Si el compromiso del mandato de gestión de riesgos existente y el compromiso de la organización aún no cumple con estos criterios, los aspectos explícitos e implícitos de los mismos tendrán que ser modificados.

EJEMPLO Si el órgano de supervisión o la alta dirección han tomado decisiones que no han sido objeto de una evaluación exhaustiva del riesgo, esta es una clara indicación de que la organización no se compromete con la comprensión de sus riesgos.

Una parte esencial de la adopción de un mandato revisado es el desarrollo de un plan para cambiar la comprensión de lo que se requiere. El objetivo de este plan será el de asegurar que tanto el mandato y sus beneficios son ampliamente comprendidos y se cree en ellos, y que la organización se ha comprometido consistentemente con el mandato y se comporta en consecuencia. Será el comportamiento de la organización, y cómo esto se compara con las declaraciones explícitas sobre el mandato que tendrán el mayor efecto sobre si el mandato es aceptado por las diversas partes interesadas.

C.2.2 Establecer y comunicar la política de gestión del riesgo y el compromiso

Una forma de expresión y comunicación del mandato de manera explícita es a través de la creación y luego la comunicación de política de gestión del riesgo. La Norma ISO 31000:2009,

C.2 Métodos para expressar o mandato e o comprometimento

C.2.1 Características-chave

Convém que a expressão do mandato e do comprometimento atenda aos seguintes critérios:

a) seja compatível com o planejamento estratégico da organização, seus objetivos, políticas, estilos de comunicação e sistema de gestão;

b) seja compatível com os critérios de risco determinados pelo organismo de supervisão;

c) atenda aos princípios da ISO 31000, assim como que se empenhe pela excelência na gestão de riscos como delineado na ISO 31000: 2009, Anexo A;

d) seja de fácil comunicação e que a sua compreensão seja testada dentro e fora da organização;

e) haja expectativas razoáveis de ser implementada com sucesso;

f) aborde as responsabilidades dos proprietários do risco.

Caso o mandato de gestão de riscos existente e o comprometimento da organização com a gestão de riscos ainda não atendam a estes critérios, ambos os aspectos explícitos e implícitos dos mesmos necessitarão ser mudados.

EXEMPLO Caso o organismo de supervisão ou a Alta Direção tenha tomado decisões as quais não tenham sido objeto de minucioso processo de avaliação de riscos, isto é uma clara indicação de que a organização não está comprometida com a compreensão dos seus riscos.

Uma parte essencial da adoção de um mandato revisado é o desenvolvimento de um plano para mudar a compreensão do que é requerido. O objetivo deste plano será assegurar que tanto o mandato quanto seus benefícios sejam amplamente compreendidos e aceitos, e que a organização esteja comprometida de forma consistente com o mandato e comporte-se de acordo. Será o comportamento da organização e como este se compara às declarações explícitas sobre o mandato que terá o maior efeito em se o mandatado é aceito pelas várias partes interessadas.

C.2.2 Estabelecendo e comunicando a política de gestão de riscos e o comprometimento

Um modo de expressar e comunicar o mandato de uma maneira explicita é por meio do estabelecimento e subsequente comunicação da politica de gestão de riscos. A ISO 31000:2009,

4.3.2, especifica que la organización no sólo debería elaborar una política clara sobre la gestión del riesgo, perusino que también debería ser comunicada, tanto dentro como fuera de la organización. La Norma ISO 31000:2009, 4.3.2, también identifica temas específicos que normalmente se recomienda reflejar en la política.

Teniendo en cuenta el principio g) (es decir, la gestión de riesgos está hecha a medida), la expresión de la política debería ser adecuada, y coherente con la forma general en el que opera la organización. De lo contrario, no puede ser considerado como pertinente para, y parte de la totalidad del sistema en el que opera la organización.

Para las grandes organizaciones, el establecimiento de una política normalmente significa el desarrollo de una declaración formal sobre el mandato para la gestión del riesgo que formará parte de su grupo global de las políticas. En consecuencia, será firmada por el órgano de supervisión y luego comunicada y reforzada a través del sistema de gestión.

Ayuda práctica

El compromiso de la alta dirección y el órgano de supervisión es clave para el éxito de cualquier programa de gestión del riesgo. Es conveniente que la organización considere las siguientes preguntas al establecer su mandato y compromiso con la gestión del riesgo:

- ¿Cuáles son los objetivos estratégicos de la organización? ¿Son claros? ¿Qué es explícito e implícito en esos objetivos?

- ¿Es clara la naturaleza y el alcance de los riesgos significativos en el logro de los objetivos estratégicos que la alta dirección está dispuesta a asumir y las oportunidades que está dispuesta a seguir?

- ¿Es necesario que la alta dirección establezca una gobernanza más clara sobre la actitud ante el riesgo de la organización?

- ¿Qué medidas ha adoptado la alta dirección para aegurar el seguimiento y control de la gestión del riesgo?

- ¿Los que toman decisiones comprenden el grado en que a ellos (individualmente) se les permite exponer a la organización a las consecuencias de un evento o situación? Cualquier actitud ante el riesgo tiene que ser práctica, siendo una guía para la toma de decisiones basadas en el riesgo.

- ¿Los ejecutivos comprenden su nivel agregado e interrelacionado de riesgo para que puedan determinar si es aceptable o no?

4.3.2, especifica que convém que a organização não apenas torne sua politica de gestão de riscos clara, mas também que a comunique, tanto dentro quanto fora da organização. A ISO 31000:2009, 4.3.2, também identifica questões específicas as quais convém que sejam tipicamente refletidas na política.

Tendo em mente o Princípio g) (isto é, a gestão de riscos é feita sob medida), convém que a expressão da política seja apropriada, e consistente, com a maneira geral em que a organização opera. Caso contrário, pode não ser vista nem como pertinente, nem como parte do sistema geral pelo qual a organização opera.

Para organizações maiores, o estabelecimento de uma política normalmente significará o desenvolvimento de uma declaração formal sobre o mandato para a gestão de riscos que será uma parte de seu conjunto global de políticas. Em consonância, essa declaração será aprovada pelo organismo de governança e então comunicada e reforçada por meio do sistema de gestão.

Ajuda prática

O envolvimento e comprometimento da Alta Direção e do organismo de supervisão são chaves para o sucesso de qualquer programa de gestão de riscos. Convém que a organização considere as seguintes questões ao estabelecer seu mandato e comprometimento com a gestão de riscos:

- Quais são os objetivos estratégicos da organização? São claros? O que está explícito e o que está implícito nesses objetivos?

- A Alta Direção tem clareza quanto à natureza e extensão dos riscos significativos que está disposta a assumir e às oportunidades que está disposta a perseguir para atingir seus objetivos estratégicos?

- A Alta Direção necessita estabelecer uma governança mais clara sobre a atitude perante o risco da organização?

- Que passos a Alta Direção tem tomado para assegurar a supervisão da gestão de riscos?

- Os gestores que tomam decisões compreendem o grau em que (individualmente) lhes é permitido expor a organização às consequências de um evento ou situação? Qualquer atitude perante o risco necessita ser prática, orientando os gestores a tomarem decisões com base em risco.

- Os executivos compreendem seu nível de risco agregado e interligado de forma a poderem determinar se este é aceitável ou não?

- ¿La alta dirección y el líder ejecutivo comprenden el nivel agregado e interrelacionado de riesgo para la organización en su conjunto?

- ¿Tienen claro los directivos y ejecutivos que la actitud frente al riesgo no es constante? Se puede cambiar a medida que las condiciones del entorno y el negocio cambian. Todo lo aprobado por la alta dirección tiene que tener cierta flexibilidad en su construcción.

- ¿Se realizan las decisiones de riesgo con plena consideración de las consecuencias? El marco de gestión del riesgo tiene que ayudar a los gerentes y ejecutivos a tomar un nivel adecuado de riesgo, dado el potencial de recompensa.

- ¿Cuáles son los riesgos significativos que la alta dirección está dispuesta a asumir y las oportunidades que está dispuesta a seguir? ¿Cuáles son los riesgos significativos que la alta dirección no está dispuesta a asumir? Cualquiera que sea la forma de la política sobre la gestión del riesgo, debería establecerse junto con las otras políticas que dirigen la forma en que opera la organización.

- A Alta Direção e a liderança executiva compreendem o nível de risco agregado e interligado da organização como um todo?

- Tanto os gestores quanto os executivos têm clareza que a atitude perante o risco não é constante? Isto pode mudar conforme as condições do ambiente e de negócios mudam. Qualquer coisa aprovada pela Alta Direção necessita possuir certo grau de flexibilidade.

- As decisões relativas aos riscos são tomadas com total consideração das consequências? A estrutura a para gestão de riscos necessita auxiliar gestores e executivos a assumir um nível apropriado de risco para o negócio, em função do potencial de recompensa.

- Quais são os riscos significativos que a Alta Direção está disposta a assumir e as oportunidades que ela está disposta a perseguir? Quais são os riscos significativos que a Alta Direção não está disposta a assumir? Qualquer que seja a forma de política sobre a gestão de riscos, convém que ela esteja alinhada às demais políticas que direcionam o modo como a organização opera.

Convém que a política seja apoiada tanto de maneira explícita quanto implícita e que seja refletida de acordo, e convém que atenda aos seis critérios descritos em C.2.1.

C.2.3 Fortalecimiento

La alta dirección y el órgano de supervisión deberían demostrar y fortalecer a la organización con su compromiso y con el mandato a través de una combinación de acciones explícitas e implícitas, incluyendo:

- dejar en claro que los objetivos de gestión del riesgo están vinculados y no se separan de otros objetivos de gestión;

- dejar en claro que la gestión del riesgo es sobre la entrega eficaz de los objetivos de la organización;

- asegurar qué tipo de actividades de gestión del riesgo que requiere el mandato se integran en los procesos de gobernanza y de gestión existentes, y en los procesos estratégicos, operativos y de proyectos;

- requerir un seguimiento regular de información sobre el marco de gestión del riesgo de la organización, y los procesos para asegurar que sigan siendo adecuados y eficaces;

- seguir y controlar que la organización tenga una comprensión actualizada y completa de sus

C.2.3 Reforço

Convém que a Alta Direção e o organismo de supervisão demonstrem e reforcem o comprometimento da organização com o mandato por meio de uma combinação de ações explícitas e implícitas incluindo:

- tornar claro que os objetivos da gestão de riscos estão ligados e não separados de outros objetivos de gestão;

- tornar claro que a gestão de riscos trata da entrega efetiva dos objetivos da organização;

- assegurar que o tipo de atividades de gestão de riscos requerido pelo mandato está integrado aos processos de gestão e governança existentes e nos processos estratégico, operacional e de projeto;

- requerer monitoramento e reporte da estrutura para gestão de riscos e dos processos da gestão de riscos da organização para assegurar que permaneçam apropriados e eficazes;

- monitorar que a organização tenha um entendimento atual e abrangente de seus riscos,

riesgos y esos riesgos se encuentran dentro de los criterios de riesgo determinados y tomar medidas correctivas cuando no se cumplan estos criterios;

- predicar con el ejemplo en lo que respecta a sus propias actividades;

- renovar el compromiso con el mandato en el tiempo, eventos y cambio de gestión superior.

La implementación de la Norma ISO 31000 puede tener lugar a través de una organización como un todo, o se puede lograr parte por parte, por ejemplo, dentro de las empresas subsidiarias.

C.3 Orientación sobre el desarrollo del mandato y el compromiso

El establecimiento del mandato para la gestión del riesgo requiere una cuidadosa reflexión, una perspectiva estratégica y consulta entre el órgano de supervisión y la alta dirección. Esto ayudará a asegurar que, una vez adoptado el mandato, la organización lo cumplirá.

La expresión del mandato y el compromiso deberían considerarse tanto en los niveles tácticos como en los estratégicos. La organización debería definir y evaluar las competencias para cumplir con sus objetivos y cultivar las habilidades y los conocimientos necesarios para alcanzarlos.

Las implicancias de los cambios requeridos por un mandato tendrán una consideración cuidadosa. Esto incluye quién dirigiría el cambio y que apoyo u orientación necesitaría. A veces los cambios pueden ser muy radicales en su alcance (por ejemplo, cambios en las especificaciones del trabajo, el seguimiento del desempeño y los procesos de gestión) y así absorberá parte de la capacidad de cambio de la organización. Esto tendrá que ser considerado en el contexto de otros cambios que están en marcha y si puede ser integrado.

Las personas que se verán afectadas de manera significativa por los cambios deberían ser consultadas, en particular los custodios de gestión del riesgo en los silos de la organización, de modo que todas las implicancias del cambio se puedan comprender dentro de la organización (por ejemplo, la salud y la seguridad, la gestión de la seguridad).

El mandato debería articularse con una declaración de política que demuestre el compromiso de la organización con la misma.

que esses riscos estejam dentro de determinados critérios de risco e que ações corretivas sejam tomadas quando estes critérios não forem atendidos;

- liderar dando exemplo com respeito às suas próprias atividades;

- renovar o comprometimento com o mandato sempre que o tempo, eventos e a Alta Direção mudarem.

A implementação da ISO 31000 pode ocorrer através da organização como um todo, ou ser alcançada, em partes, por exemplo, nas subsidiárias.

C.3 Diretrizes para o desenvolvimento do mandato e do comprometimento

Estabelecer o mandato para a gestão de riscos requer um pensamento cauteloso, uma perspectiva estratégica e uma consulta entre o organismo de supervisão e a Alta Direção. Isto ajudará a assegurar que uma vez adotado, a organização seguirá o mandato.

Convém que a expressão do mandato e do comprometimento seja considerada em ambos os níveis tático e estratégico. Convém que a organização defina e avalie as competências para atingir seus objetivos e cultive as habilidades e competências necessárias para atingi-los.

As implicações das mudanças requeridas por um mandato necessitarão de consideração cautelosa. Isto inclui quem lideraria a mudança e quem necessitaria de orientação e suporte. Algumas vezes as mudanças podem ser bastante radicais no escopo (por exemplo, mudanças nas especificações de trabalho, monitoramento do desempenho e gerenciamento de processos) e assim absorverão parte da capacidade de mudança da organização. Isto necessitará ser considerado no contexto de outras mudanças que estejam em curso e se poderá haver integração.

Convém que as pessoas que serão significativamente afetadas pelas mudanças sejam consultadas, em particular, os depositários de qualquer silo de gestão de riscos dentro da organização (por exemplo, gestão da saúde e segurança), de modo que todas as implicações da mudança possam ser compreendidas.

Convém que o mandato seja articulado em uma declaração de política que demonstrará o comprometimento da organização para com ele.

Ayuda práctica

Las siguientes son algunas formas de como ésto se puede lograr:

- teniendo en cuenta cómo se explica el mandato en la organización y cómo se refuerza esas explicaciones por las acciones en curso;

- teniendo en cuenta el plazo para hacer efectivo el mandato (es conveniente que éste se respete e integre con otros imperativos de la organización, al menos hasta que el marco se complete no se tomará conciencia de sus beneficios y la gestión del riesgo no será tan eficaz como podría ser);

- identificando los roles claves para lograr el cambio necesario en el enfoque de la gestión del riesgo y para dirigir y liderar las actividades de gestión del riesgo;

- especificando cuáles son los aspectos del marco y las actividades de gestión del riesgo para los cuales la alta dirección, los niveles de gestión y los comités realizarán el seguimiento, control y las modalidades de cómo será recogida y presentada dicha información;

- incluyendo los resultados de la gestión del riesgo como un tema regular de la agenda en todas las reuniones claves de supervisión y de la alta dirección;

- desarrollando métodos eficaces para comunicar sobre el desempeño de gestión del riesgo (por ejemplo, la publicación de un boletín de noticias para el personal en el estilo de un informe de gestión del riesgo);

- teniendo en cuenta los desencadenantes de la revisión del mandato.

Ajuda prática

Alguns dos meios pelos quais isto pode ser atingido incluem o seguinte:

- considerar como o mandato será explicado à organização e como essas explicações serão reforçadas pelas ações em curso;

- considerar o prazo para que o mandato tenha efeito (convém que isto respeite e seja integrado aos outros imperativos da organização, já que até a estrutura estar completa, seus plenos benefícios não serão percebidos e a gestão de riscos não será tão efetiva como poderia ser);

- identificar os papéis-chave para promover as mudanças necessárias na abordagem da gestão de riscos e para dirigir e liderar as atividades de gestão de riscos;

- especificar quais aspectos das atividades e da estrutura para gestão de riscos serão monitorados nos níveis da alta direção, gestão e comitês e como tal informação será coletada e apresentada;

- incluir o desempenho da gestão de riscos como um item de agenda regular em todas as reuniões-chave de supervisão e da alta direção;

- desenvolver métodos eficazes para a comunicação sobre o desempenho da gestão de riscos (por exemplo, publicação de um boletim informativo para os funcionários no estilo de um relatório de gestão de riscos);

- convém considerar quais são os gatilhos para a análise crítica do mandato.

Anexo D
(informativo)

Seguimiento, control y revisión

Monitoramento e análise crítica

D.1 Antecedentes

D.1.1 Generalidades

Este Anexo proporciona orientaciones sobre el seguimiento y control, y la revisión del marco de gestión del riesgo y los procesos de acuerdo con la Norma ISO 31000:2009, 4.5, 4.6 y 5.6.

El seguimiento y control, y la revisión son dos actividades distintas destinadas a determinar si las premisas y decisiones siguen siendo válidas. Las técnicas se utilizan tanto en el mantenimiento de un marco eficaz de gestión del riesgo y en cada una de las etapas del proceso de gestión del riesgo.

- El seguimiento y control implica la vigilancia de rutina del desempeño real y su comparación con el desempeño esperado o requerido. Se trata de la verificación continua o investigar, supervisar, observar críticamente, o determinar la situación con el fin de identificar el cambio desde el nivel de desempeño requerido o esperado, así como los cambios en el contexto.

- La revisión implica la verificación periódica o improvisada de la situación actual, los cambios en el entorno, las prácticas de la industria, o las prácticas de la organización. Se trata de una actividad llevada a cabo para determinar la conveniencia, adecuación y eficacia de los marcos y procesos para alcanzar los objetivos establecidos. En las revisiones se consideran los resultados de las actividades de seguimiento y control.

- Una auditoría es un proceso basado en la evidencia, la revisión sistemática con criterios predeterminados. Mientras que cada auditoría es una revisión, no todas las revisiones son una auditoría.

En conjunto, el seguimiento y control y la revisión proveen del aseguramiento de que el desempeño de la gestión del riesgo es el esperado, ya que puede ser mejorado; o si se ha dado un cambio que requiera adaptación o revisión del marco o de algún aspecto del proceso.

El objetivo del seguimiento y control y revisión es proporcionar un aseguramiento razonable de que los riesgos se gestionan adecuadamente, para

D.1 Antecedentes

D.1.1 Geral

Este Anexo fornece orientações sobre monitoramento e análise crítica da estrutura para a gestão de riscos e processos de gestão de riscos de acordo com a ISO 31000:2009, 4.5, 4.6 e 5.6.

- O monitoramento e a análise crítica são duas atividades distintas destinadas a determinar se suposições e decisões continuam válidas. As técnicas são utilizadas tanto na manutenção de estrutura para a gestão de riscos eficaz quanto em cada uma das etapas do processo de gestão de riscos.

- O monitoramento envolve a vigilância de rotina do desempenho real e sua comparação com o desempenho esperado ou requerido. Envolve a verificação ou investigação contínua, supervisão, observação crítica, ou determinação do estado, a fim de identificar mudança no nível de desempenho exigido ou esperado, assim como mudanças no contexto.

- A análise crítica envolve verificação, periódica ou improvisada, da situação atual, para mudanças no ambiente, práticas da indústria, ou práticas organizacionais. É uma atividade realizada para determinar a adequação e eficácia da estrutura e do processo para atingir os objetivos estabelecidos. Convém que as análises críticas considerem os resultados das atividades de monitoramento.

- Uma auditoria é um processo de análise crítica sistemática baseado em evidências, contra critérios pré-determinados. Enquanto cada auditoria é uma análise crítica, nem toda análise crítica é uma auditoria.

Juntos, o monitoramento e a análise crítica fornecem garantias de que o desempenho da gestão de riscos está como esperado, se pode ser melhorado e se mudanças ocorreram requerendo ajuste ou revisão da estrutura ou de algum aspecto do processo.

O monitoramento e análise crítica têm por objetivo assegurar razoavelmente que os riscos estão adequadamente gerenciados, para identificar

identificar deficiencias en la gestión del riesgo, y para identificar oportunidades de mejora para la gestión del riesgo. Ambos son necesarios con el fin de asegurar que la organización mantiene una comprensión actual de los riesgos en relación con sus criterios de riesgo, en consonancia con su actitud ante el riesgo. Ambos requieren un enfoque sistemático integral a los sistemas generales de gestión de la organización.

Las actividades de seguimiento y control y de revisión y de las medidas adoptadas en respuesta a las conclusiones a menudo se caracteriza por ser un sistema de aseguramiento, ya que tienen el potencial de detectar y remediar las debilidades antes de que ocurran efectos adversos o de proporcionar la confianza que los riesgos están todavía dentro de los criterios de la organización. Estas actividades también se pueden utilizar para proporcionar, a las partes interesadas internas y externas, del aseguramiento razonable de que el riesgo se gestiona con eficacia.

A medida que cambien los factores en el contexto interno y externo, también lo hará el riesgo. Del mismo modo, el seguimiento del contexto externo puede alertar a la organización de los cambios que pueden presentar una oportunidad para mejorar el desempeño o una nueva actividad. Al permanecer atentos a dichos cambios; de desempeño, no conformidades e incidentes, la organización será capaz de identificar las oportunidades de mejora del marco de gestión del riesgo y del desempeño general de la organización.

Debería existir un programa integral para el seguimiento y control, y el registro de los indicadores de desempeño de riesgo que se alinean con los indicadores de desempeño de la organización.

El programa debería brindar una alerta temprana de las tendencias adversas que puedan requerir acciones preventivas y de intervención.

Una sola actividad de seguimiento y control, o revisión puede estar dirigida a un riesgo individual o una serie de riesgos relacionados. Puede centrarse en los riesgos o en los controles de los mismos.

D.1.2 Responsabilidad de rendir cuentas del seguimiento y control y revisión

La responsabilidad general de las actividades de seguimiento y control y revisión recae en el órgano de supervisión y en la alta dirección, y no en los proveedores de aseguramiento, por ejemplo de auditoría interna. Las funciones de aseguramiento de calidad, de revisión independiente y de seguimiento regulatorio son complementos útiles para el proceso de presentación de informes de

deficiências na gestão de riscos e identificar oportunidades para melhorar a gestão de riscos. Ambos são necessários a fim de assegurar que a organização mantenha um entendimento atual de seus riscos em relação aos seus critérios de risco, consistente com a sua atitude perante o risco. Ambos requerem uma abordagem sistemática integral dos sistemas gerais de gestão da organização.

As atividades de monitoramento e análise crítica e as ações tomadas em resposta às constatações são muitas vezes caracterizadas como um sistema de garantia porque têm o potencial de detectar e remediar as fraquezas antes da ocorrência de efeitos adversos ou para fornecer a confiança de que os riscos ainda estão dentro dos critérios da organização. Essas atividades também podem ser usadas para assegurar razoavelmente às partes interessadas internas e externas de que o risco está gerenciado de forma eficaz.

Como os fatores no contexto interno e externo mudam, assim também o risco. Da mesma forma, o monitoramento do contexto externo pode alertar a organização para mudanças que possam apresentar uma oportunidade para melhorar o desempenho ou uma nova atividade. Ao permanecer alerta para tais mudanças, desempenho, não conformidades e quase acidentes, a organização será capaz de identificar oportunidades de melhoria da estrutura de gestão de riscos e desempenho global da organização.

Convém que exista um programa abrangente implementado para monitorar e registrar indicadores de desempenho de risco que estejam alinhados com os indicadores de desempenho da organização.

Convém que o programa forneça alertas precoces sobre tendências adversas que possam requerer ações preventivas e intervenção.

Uma única atividade de monitoramento ou análise crítica pode ser dirigida a um risco individual ou uma série de riscos relacionados. Isto pode ser focado nos riscos ou sobre os controles a eles endereçados.

D.1.2 Responsabilização pelo monitoramento e análise crítica

A responsabilidade global para as atividades de monitoramento e análise crítica encontra-se com o organismo de supervisão e Alta Direção, e não com os fornecedores de garantia, por exemplo, auditoria interna. Funções de garantia de qualidade, funções de análise crítica independente e monitoramento regulatório são auxiliares úteis para o processo de reporte de gestão de linha porque

gestión de la línea debido a que estas actividades ofrecen una visión alternativa.

Las actividades de seguimiento y control y revisión pueden ser considerados en términos de una jerarquía, con la práctica regular en el nivel superior: si se diseñan adecuadamente, esto proporciona el nivel más potente de aseguramiento. Sin embargo, el programa de seguimiento y control y revisión debería incluir los tres elementos.

El programa de seguimiento y control y revisión debería verificar que la política de gestión del riesgo es a la vez implementada y eficaz. La forma en que la alta dirección reacciona a los resultados del programa de seguimiento y control puede afectar el comportamiento del personal, y es importante que la alta dirección actúe como modelo a seguir.

D.1.3 Revisiones independientes

La independencia está dada por la relación del revisor/auditor con la parte que contrata, ya sea que se lleve a cabo por partes internas o externas a la organización.

La independencia es la base de la imparcialidad de la revisión y la objetividad de las conclusiones de la revisión. Los revisores y auditores deberían ser independientes de la actividad que se revisa /audita siempre que sea posible, y en todo caso deberían actuar de una manera que sea libre de sesgos y de conflicto de intereses.

Para las auditorías internas, los auditores deberían ser independientes de los gerentes operativos de la función que está siendo auditada. Los revisores y auditores deberían mantener la objetividad en todo el proceso de revisión de auditoría para asegurar que los resultados y las conclusiones se basan únicamente en la evidencia.

Para las organizaciones pequeñas, puede no ser posible que los revisores y auditores sean totalmente independientes de la actividad objeto de revisión/auditoría, pero se debería hacer todo lo posible para eliminar los sesgos y fomentar la objetividad.

La independencia de los revisores y auditores ayuda a hacer de las revisiones y auditorías herramientas eficaces y fiables en apoyo de las políticas y los controles de gestión del riesgo, al proporcionar información sobre la cual una organización puede actuar con el fin de mejorar su desempeño.

essas atividades proporcionam uma visão alternativa.

As atividades de monitoramento e análise crítica podem ser consideradas em termos de uma hierarquia, com prática regular no topo: se concebidas corretamente, fornecem o nível mais poderoso de garantia. No entanto, convém que um programa de monitoramento e análise crítica inclua todos os três elementos.

Convém que o programa de monitoramento e análise crítica verifique tanto se a política de gestão de riscos está implementada quanto se é eficaz. A maneira em que a Alta Direção reage aos resultados do programa de monitoramento pode afetar o comportamento dos funcionários, e é importante que a Alta Direção atue como um modelo a ser seguido.

D.1.3 Análises críticas independentes

Seja conduzida por partes internas ou externas, a independência vem da relação do analista/auditor com a parte engajada.

A independência é a base para a imparcialidade e objetividade das conclusões da análise crítica. Convém que os analistas e auditores sejam independentes da atividade a ser analisada criticamente/ auditada tanto quanto possível, e convém que, em todos os casos, atuem de uma forma que seja livre de viés e conflitos de interesse.

Para auditorias internas, convém que os auditores sejam independentes em relação aos gerentes operacionais da função que está sendo auditada. Convém que os analistas e auditores mantenham a objetividade durante o processo de análise crítica da auditoria para assegurar que as constatações e as conclusões sejam baseadas apenas em evidências.

Para empresas pequenas, pode não ser possível que os analistas e auditores sejam totalmente independentes da atividade que está sendo analisada criticamente/auditada, mas convém que se façam todos os esforços para eliminar vieses e incentivar a objetividade.

A independência dos analistas e auditores ajuda a fazer das análises críticas e auditorias uma ferramenta eficaz e confiável de apoio às políticas de gestão de riscos e controles, fornecendo informações sobre as quais uma organização pode agir para melhorar seu desempenho.

La revisión podrá centrarse en el cumplimiento de las normas (internas o externas), procedimientos o requisitos legales. A menudo, también consideran la idoneidad, la eficacia y eficiencia de los controles, por ejemplo, pueden considerar si las actividades de gestión del riesgo siguen los valores expresados en los principios de la Norma ISO 31000.

Muchas organizaciones cuentan con revisión por la dirección y funciones de asesoramiento (tales como asesores de gestión del riesgo, los inspectores de cumplimiento, y gerentes de control de calidad) que realizan revisiones de rutina; auditoría interna suele informar al órgano de supervisión y de la alta dirección. El objetivo de estas revisiones es proporcionar confianza al organismo de supervisión y la alta dirección de la organización que:

- sus criterios de riesgo son coherentes con los objetivos y el contexto en el que opera;

- se ha utilizado un proceso adecuado y sistemático para identificar, valorar y tratar los riesgos y hay confianza en que este proceso va a continuar operando;

- los riesgos no tolerables están siendo tratados adecuadamente;

- los controles que se cree que modifican los riesgos que de otro modo serían no tolerables, son a la vez adecuados y eficaces;

- se está avanzando adecuadamente con los planes de tratamiento del riesgo.

Las actividades de un proceso de revisión independiente no liberan a la gestión de la línea de sus responsabilidades de seguimiento y control y revisión.

D.1.4 Obtención de información adecuada

Al igual que otros aspectos de la gestión del riesgo, el seguimiento y control y la revisión requieren el uso de la mejor información disponible [ver Principio f)]. Para ser adecuada al propósito, la información debería ser pertinente para los usuarios y debería representar fielmente lo que pretende representar. La utilidad de la información se ve reforzada si es comparable, verificable, oportuna y comprensible. La información puede obtenerse a partir de dos tipos de fuentes:

a) fuentes directas: las observaciones y mediciones de las operaciones reales del proceso o sus resultados;

b) fuentes indirectas: las medidas que se derivan de los procesos o resultados considerados.

Tais análises críticas podem se concentrar na conformidade com normas (internas ou externas), procedimentos ou requisitos legislativos. Por vezes também consideram a adequação, eficácia e eficiência dos controles, por exemplo, podem considerar se as atividades de gestão de riscos seguem os valores expressos nos princípios da ISO 31000.

Muitas organizações têm funções de análise crítica pela direção e funções de assessoramento (como assessores de gestão de riscos, responsáveis pela conformidade e gerentes de garantia de qualidade) que procedem análises críticas de rotina; a auditoria interna normalmente relata as suas análises críticas ao organismo de supervisão e para a Alta Direção. O objetivo dessas análises críticas é fornecer garantia ao organismo de supervisão e Alta Direção da organização que:

- seus critérios de risco são consistentes com seus objetivos e o contexto em que está operando;

- um processo adequado e sistemático foi utilizado para identificar, avaliar e tratar os riscos e que existe confiança de que este processo vai continuar a operar;

- riscos inaceitáveis são objeto de tratamento de risco adequado;

- controles que se crê que modifiquem riscos de outra maneira inaceitáveis são tanto adequados quanto eficazes;

- está se tendo progresso apropriado com os planos de tratamento de riscos.

As atividades de um processo de análise crítica independente não aliviam a gerência de linha de suas responsabilidades de monitoramento e análise crítica.

D.1.4 Obtenção de informação adequada

Como outros aspectos da gestão de riscos,o monitoramento e a análise crítica requerem o uso da melhor informação disponível [ver Princípio f)]. Para ser adequada ao propósito, a informação tem de ser pertinente para os usuários e representar fielmente o que se pretende representar. A utilidade da informação é reforçada se for comparável, verificável, oportuna e compreensível. A informação pode ser obtida a partir de dois tipos de fontes:

a) fontes diretas: observações e medições de operações do processo real ou seus resultados;

b) fontes indiretas: medições que são derivadas dos processos ou resultados considerados.

Se eligen las combinaciones de las diversas fuentes de las mediciones según la necesidad (según la disponibilidad) o por conveniencia (oportunidad, costo, etc.)

D.1.5 Informar sobre el proceso de revisión

El informe debería proporcionar información al órgano de supervisión, a la alta dirección y a las partes interesadas de la organización, sobre si los riesgos de la organización, se encuentran dentro de sus criterios de riesgo o si tiene planes de tratamiento de riesgos creíbles que en última instancia conducirán a este resultado. Además, puede proporcionar información acerca de los riesgos nuevos y emergentes.

Cualquier colección de información del riesgo (por ejemplo, en un registro de riesgos) debería ser actualizada periódicamente. El tipo y la frecuencia de los informes dependen de la naturaleza, el tamaño y el alcance de la evaluación del riesgo.

La salida de una revisión o de una auditoría será un informe que resume los hallazgos y proporciona las conclusiones de la evaluación de acuerdo a los criterios predeterminados. El informe puede establecer recomendaciones para la mejora del sistema en base a lo que los revisores observaron. De vez en cuando, el revisor hace observaciones más amplias, dirigidas a los propios criterios. La respuesta a cualquier revisión debería centrarse en la mejora del sistema y debería tratarse las causas raíces de los problemas.

D.1.6 Acción correctiva y mejora continua

Se debería establecer procesos para asegurar que las recomendaciones son consideradas activamente en la gestión de la organización y que se ejecutan las respuestas acordadas. Las acciones en respuesta a los comentarios deberían informarse al órgano de supervisión y se debería realizarse el seguimiento y control rutinario hasta ser implementadas.

D.2 Seguimiento y control, y revisión del marco de gestión del riesgo

D.2.1 Generalidades

El propósito del seguimiento y control y la revisión es mantener el marco de gestión del riesgo actualizado y coherente con las intenciones de gestión del riesgo de la organización. El marco se refiere a los elementos y procesos del sistema de gestión dentro de la organización que permiten gestionar el riesgo.

La Norma ISO 31000:2009, Capítulo 4, contiene orientación sobre los elementos necesarios de un marco de gestión del riesgo y señala que es

Combinações de medições das várias fontes são escolhidas por necessidade (dependendo da disponibilidade) ou por conveniência (oportunidade, custo etc.).

D.1.5 Reporte do processo de análise crítica

Convém que os reportes forneçam informações ao organismo de supervisão e à Alta Direção e às partes interessadas da organização sobre se os riscos da organização estão dentro de seus critérios de risco ou se existem planos de tratamento de riscos confiáveis que levarão, em última análise, a este resultado. Além disso, pode fornecer informações sobre riscos novos e emergentes.

Convém que qualquer coleção de informação de risco (por exemplo, em um registro de riscos) seja atualizada periodicamente. O tipo e frequência dos reportes dependerá da natureza, do tamanho e do escopo do processo de avaliação de riscos.

A saída de uma análise crítica ou auditoria será um reporte que resume as constatações e fornece conclusões da avaliação com base em critérios pré-determinados. O reporte pode fornecer recomendações para melhorias do sistema com base no que os analistas observaram. Ocasionalmente, o analista vai fazer sugestões mais amplas, direcionadas aos próprios critérios. Convém que a resposta a qualquer análise crítica seja focada na melhoria do sistema e no tratamento das causas dos problemas.

D.1.6 Ação corretiva e melhoria contínua

Convém que sejam estabelecidos processos para assegurar que as recomendações sejam ativamente consideradas pela gestão organizacional e que as respostas acordadas sejam executadas. Convém que as ações em resposta às análises críticas sejam reportadas ao organismo de supervisão e rotineiramente monitoradas até que estejam implementadas.

D.2 Monitoramento e análise crítica da estrutura

D.2.1 Geral

O objetivo do monitoramento e da análise crítica é manter a estrutura de gestão de riscos atualizada e consistente com as intenções de gestão de riscos da organização. A estrutura refere-se aos componentes e processos dentro do sistema de gestão da organização que possibilitam que o risco seja gerenciado.

A ISO 31000:2009, Seção 4, contém diretrizes sobre os componentes necessários de uma estrutura e assinala que convém que estes levem

recomendable que éstos tengan en cuenta el contexto interno y externo de la organización.

Como se producen cambios en el contexto interno o externo de la organización, puede ser necesario adecuar el marco de gestión del riesgo para asegurar que éste permanece eficaz.

Incluso si no ha habido cambios internos o externos que requieran cambio en el diseño, aún es necesario para asegurarse que en cualquier momento, el marco funciona como se ha diseñado.

Para las organizaciones que realizan la transición para alinearse con la Norma ISO 31000, esto puede implicar la verificación de los elementos del marco de la implementación del plan para asegurarse que se han implementado correctamente. Para las organizaciones que ya han implementado la Norma ISO 31000 implica asegurar que los elementos del marco siguen existiendo y funcionando como estaba previsto.

D.2.2 Responsabilidad de rendir cuentas

La gestión es responsable de asegurar que periódicamente se revisa el marco y se realiza el seguimiento y control de los indicadores de desempeño. Es conveniente que como parte de la asignación de responsabilidades para la gestión del riesgo, ya sea una persona (por ejemplo, un alto directivo) o una función de la organización (por ejemplo, la función de apoyo a la gestión del riesgo organizacional) sea custodio del marco de gestión del riesgo, y sea asegurada una responsabilidad clave de que el marco sigue siendo eficaz.

D.2.3 Establecimiento de una línea de base

Se debería establecer una línea de base para la gestión del riesgo en la organización. La línea base puede ser descrita de diversas maneras, pero debería incluir:

a) los elementos del marco de gestión del riesgo (como se describe en la Norma ISO 31000:2009, 4.3) que brindan la capacidad para el logro de la intención que se persiga;

b) el alcance del apoyo proporcionado por el órgano de supervisión y la alta dirección en el mandato y el compromiso para la gestión del riesgo (a menudo se expresa en la forma de una política de gestión del riesgo).

Generalmente la forma y la arquitectura pretendida del marco de gestión del riesgo son documentadas cuando se realiza el diseño, y la información esta disponible tal como se muestra en la Tabla D.1.

em conta o contexto interno e externo da organização.

Como ocorrem mudanças no contexto interno ou externo da organização, pode ser necessário ajustar a estrutura para assegurar que permaneça eficaz.

Mesmo que não tenha havido alterações internas ou externas que requeiram mudança na concepção, ainda é necessário assegurar que a qualquer momento a estrutura está funcionando como concebida.

Para organizações em transição para se alinhar com a ISO 31000, isto pode implicar na verificação dos componentes da estrutura do plano de implementação, para assegurar que estes foram corretamente implementados. Para as organizações que já implementaram a ISO 31000, isto envolverá assegurar que os componentes da estrutura continuem existindo e funcionando como planejado.

D.2.2 Responsabilização

A direção é responsável por assegurar que a estrutura seja periodicamente analisada criticamente e monitorada em relação a indicadores de desempenho. Como parte da alocação de responsabilidades para gestão de riscos, convém que uma pessoa (por exemplo, um gerente sênior) ou uma função organizacional (por exemplo, a função de apoio à gestão de riscos corporativos) seja feita custodiante da estrutura e que uma responsabilidade-chave seja assegurar que a estrutura permaneça eficaz.

D.2.3 Estabelecimento de uma linha de base

Convém que seja estabelecida uma linha de base para a gestão de riscos na organização. A linha de base pode ser descrita de várias maneiras, mas convém que inclua:

a) os componentes da estrutura (como descrito na ISO 31000:2009, 4.3) que fornecem a capacidade que possibilita que esta intenção seja alcançada;

b) a extensão do apoio fornecido pelo organismo de supervisão e pela Alta Direção no mandato e compromisso para a gestão de riscos (muitas vezes expressa na forma de uma política de gestão de riscos).

A forma e arquitetura da estrutura pretendidas, em geral, seria registrada quando concebida, e a informação, como a mostrado na Tabela D.1, estaria disponível. Isso forma uma linha de base

Esto implica una línea de base o punto de referencia para las verificaciones que se realizan durante el seguimiento y control, y revisión.

ou ponto de referência para comparações feitas durante o monitoramento e análise crítica.

Tabla D.1 - / ***Tabela D.1*** **–**
Ejemplo de una tabla para estabelecer los elementos del marco de gestión del riesgo /
Exemplo de uma tabela que lista os componentes de uma estrutura

Elemento / ***Componente***	**Dónde está desplegado /** ***Onde é implantado***	**Objetivo**	**Acciones clave /** ***Açoes-chave***	**Responsabilidad y cronograma /** ***Responsabilidade e cronograma***	**Mediciones de desempeño /** ***Medidas de desempenho***	**Estado de la implementación /** ***Estado da implementação***
Responsabilidad de rendir cuentas / *Responsabilização*	Nivel de la organización / *Em nível organizacional*	Mantener la política de gestión del riesgo de la organización actualizada / *Manter atualizada a política de gestão de riscos da organização*	• Determinar los critérios / *Determinar critérios* • Informes / *Reportar documentos* • Delegar autoridade / *Delegar autoridade*	• Publicar la política / *Publicar política* • Formalizar el esquema de delegaciones / *Formalizar cronograma de delegações* • Próxima revisión / *Próxima análise crítica* xx / xx / xx	…	…
…						
Recursos: Formación / *Recursos: Treinamento*	Nivel de la división / *Em nível de divisão*	Proporcionar los elementos de gestión del riesgo para toda la capacitación de la inducción / *Fornecer componentes de gestão de riscos para todos os treinamentos de iniciação* Hacer un curso disponible de actualización / *Disponibilizar recursos de reciclagem*	• Obtener asesoramiento / *Obter aconselhamento* • Diseñar la formación / *Projetar o treinamento* • Capacitar a los docentes / *Capacitar facilitadores*	• Diseño: gestión del riesgo Corporativa / *Projetar gestão de riscos corporativos* • Despliegue: Gestión Divisional / *Implantação: Gestão Divisional* • Próxima revisión: / *Próxima análise crítica* xx / xx / xx	• Realizado: Los informes mensuales / *Realização: Relatórios mensais* • Calidad:La formación y puesta en común y auditoria / *Qualidade: Reunião e auditoria de treinamento*	

Asimismo, la organización debería establecer los indicadores de desempeño que estén vinculados a los objetivos de la organización para dar una indicación de la eficacia del marco general de la gestión del riesgo. Los indicadores de desempeño, refieren a veces colectivamente como indicadores retrospectivos, incluyendo los siguientes:

- incidentes y accidentes;
- pérdidas reales;
- no alineaciones;
- quejas de los clientes;

Convém que a organização também estabeleça indicadores de desempenho que estão ligados aos objetivos organizacionais para fornecer uma indicação da eficácia da estrutura global para a gestão de riscos. Indicadores de desempenho, algumas vezes denominados coletivamente como indicadores de resultado, incluem o seguinte:

- incidentes, acidentes e quase acidentes;
- perdas reais;
- desalinhamentos;
- reclamações de clientes;

- deuda pendiente;

- disponibilidad del sistema;

- el grado de cumplimiento de los objetivos de la organización;

- el grado de cumplimiento de los objetivos de gestión del riesgo.

D.2.4 Evaluación de si han cambiado las características y el contexto de la organización

Se determina si el contexto interno o externo de la organización ha tenido un cambio sustancial desde que se desarrolló o modificó el marco de gestión del riesgo.

Ayuda práctica
Las características internas que podrían haber cambiado son:

- la estructura;

- las prácticas de gobernanza y los requisitos;

- las políticas, las normas internas y los modelos;

- los requisitos contractuales;

- los sistemas estratégicos y operativos afectados por factores internos o externos (por ejemplo, cambios reglamentarios legales);

- la capacidad y los recursos (por ejemplo, de capital financiero y de reputación, tiempo, personas, procesos, sistemas y tecnologías);

- los conocimientos, las habilidades y la propiedad intelectual;

- los sistemas y flujos de información;

- social, el comportamiento del entorno y cultural;

- otras prioridades de la organización y los imperativos que se pueden percibir que compiten con las intenciones de la organización' para la gestión del riesgo.

Los indicadores prospectivos, que podrían marcar los cambios en el contexto externo, se encuentran con frecuencia en los informes y encuestas que reflejan los cambios y tendencias en la industria en que opera la organización. Citamos a título de ejemplo las siguientes actividades:

- en los precios de los productos básicos, las tasas de interés de los bancos, los rendimientos de los bonos, tipos de cambio, índices bursátiles, el índice de precios al consumidor (tendencia);

- dívida ativa;

- disponibilidade do sistema;

- a extensão em que os objetivos da organização estão sendo alcançados;

- a extensão em que os objetivos da gestão de riscos estão sendo alcançados.

D.2.4 Avaliar se as características e o contexto da organização sofreram modificações

Determinar se o contexto interno ou externo da organização sofreu modificações relevantes desde que a estrutura para gerenciar riscos foi desenvolvida ou modificada.

Ajuda prática
As características internas que podem ter se modificado incluem:

- estrutura;

- práticas de governança e requisitos;

- políticas, normas e modelos internos;

- requisitos contratuais;

- sistemas estratégicos e operacionais afetados por fatores internos ou externos (por exemplo alterações regulatórias legais);

- capacidade e recursos (por exemplo, capital financeiro e reputacional, tempo, pessoas, processos, sistemas e tecnologias);

- conhecimento, habilidades e propriedade intelectual;

- sistemas e fluxos de informação;

- comportamento social, ambiental e cultural;

- outras prioridades e imperativos organizacionais que podem ser percebidos para competir com as intenções da organização para gerenciar riscos.

Indicadores antecedentes, que podem apontar para mudanças no contexto externo, são frequentemente encontrados em relatórios e levantamentos, os quais refletem alterações e tendências no segmento no qual a organização opera. Exemplos incluem:

- preços de *commodities*, taxas de juros bancários, rendimentos de títulos, taxas de câmbio, índices do mercado de ações, índice de preços ao consumidor (tendência);

- índice (tendencia);

- nivel o incidentes de fraude en organizaciones similares;

- el tamaño del mercado y las cifras de crecimiento, y los cambios repentinos en el volumen de pedidos;

- la estabilidad política y social, el descontento social y el activismo.

Si el contexto de la organización ha cambiado desde que se desarrolló el marco de gestión del riesgo, éste debería ser reevaluado y alineado con el fin de dar cuenta de estos cambios. El propósito de esta actividad es para confirmar que el marco y los procesos son adecuados para los fines previstos y de conformidad con los objetivos y prioridades de la organización.

Como consecuencia de esta revisión, la organización puede tener que cambiar su línea de base.

EJEMPLO 1 Un cambio en la estructura de una organización puede requerir alguna revisión de la política de gestión del riesgo y una reasignación de responsabilidades y recursos para permitir que el riesgo siga siendo gestionado con eficacia. Si la organización ha aumentado de tamaño, por ejemplo, debido a una fusión o adquisición, la adecuación permanente de los recursos de gestión del riesgo requiere la consideración, como un cuidadoso análisis de cualquier diferencia entre las organizaciones en el enfoque de la gestión del riesgo. Puede que sea necesario desarrollar un plan de transición para aplicar los cambios derivados del análisis.

EJEMPLO 2 Si se han promulgado nuevas disposiciones legislativas, pueden necesitar modificación o ampliación los aspectos del marco de rendición de cuentas que se refieren a la formación y la obtención de información o informes.

D.2.5 Revisión del marco

Una vez que la evaluación de las características y el contexto externo se ha completado, debería llevarse a cabo un examen más exhaustivo del marco para determinar si:

a) el plan de gestión del riesgo se lleva a cabo según lo previsto;

b) el marco y los procedimientos adoptados están funcionando según lo previsto;

c) el nivel de riesgo está dentro de los criterios;

d) os objetivos básicos de la organización están siendo influidos positivamente por la gestión del riesgo;

e) las partes interesadas reciben suficiente información para que puedan desempeñar sus

- índice (tendência);

- nível ou incidentes de fraude em organizações similares;

- tamanho do mercado, taxas de crescimento e mudanças bruscas de volume de pedidos;

- estabilidade política e social, descontentamento e ativismo social.

Se o contexto organizacional tem mudado desde que a estrutura para gerenciar riscos foi desenvolvida, convém que a estrutura para gerenciar riscos seja reavaliada e alinhada, para levar em conta essas alterações. O objetivo desta atividade é confirmar que a estrutura e os processos são adequados às suas finalidades previstas e consistentes com os objetivos e prioridades da organização.

Como consequência desta análise crítica, a organização pode precisar alterar sua linha de base.

EXEMPLO 1 Uma mudança na estrutura de uma organização pode exigir alguma revisão da política de gestão de riscos e uma realocação de responsabilizações e recursos para permitir que o risco continue a ser gerido de forma eficaz. Se a organização aumentou de tamanho, por exemplo, devido a uma fusão ou aquisição, adequação contínua de recursos para a gestão de riscos requererá consideração, bem como a análise cuidadosa de qualquer diferença entre as organizações em suas abordagens para gestão de riscos. Pode ser necessário o desenvolvimento de um plano de transição para implementar quaisquer alterações decorrentes da análise.

EXEMPLO 2 Se novas exigências legislativas forem promulgadas, os aspectos da estrutura que se referem à responsabilização, treinamento e captura ou reporte de informações podem necessitar de alteração ou ampliação.

D.2.5 Análise crítica da estrutura

Uma vez que a avaliação das características e do contexto externo tenha sido concluída, convém que uma análise crítica mais abrangente da estrutura seja realizada para determinar se:

a) o plano de gestão de riscos está sendo conduzido conforme o planejado;

b) a estrutura e os processos adotados estão operando conforme o planejado;

c) o nível de risco está dentro dos critérios;

d) objetivos centrais da organização estão sendo influenciados positivamente pela gestão de riscos;

e) partes interessadas pertinentes estão recebendo relatórios suficientes que lhes

funciones y responsabilidades en la estructura de la gobernanza;

f) las personas a través de la organización tienen las suficientes habilidades de gestión del riesgo, conocimientos y competencia para llevar a cabo sus responsabilidades como se han identificado;

g) los recursos para la gestión del riesgo son adecuados;

h) las lecciones se han aprendido de los resultados reales que se produjeron, incluidas las pérdidas, los incidentes y las oportunidades;

i) se están logrando los objetivos establecidos para la gestión del riesgo.

Debería existir un programa de revisión periódica de acuerdo, con la capacidad de llevar a cabo revisiones para un propósito específico, por ejemplo si las circunstancias cambian, en donde las consecuencias de los riesgos son repentinos o severos.

Los entregables de dicha revisión deberían incluir:

- un informe general sobre el funcionamiento del marco de gestión del riesgo;

- un informe sobre el avance de la implementación del plan de manejo del riesgo (incluyendo el análisis de cualquier retraso en la ejecución);

- un informe que describa, la posición de madurez de la organización con respecto a las mejores prácticas;

- recomendaciones de cambios que son necesarios para mejorar la gestión del riesgo y su eficacia en la organización;

- los cambios en la política de gestión del riesgo, los objetivos y el plan según sea necesario;

- los cambios a la descripción del contexto en el que opera la organización, según corresponda;

- un informe sobre las tendencias de los indicadores claves del riesgo;

- un plan de acción para hacer frente a los cambios necesarios para cumplir con los objetivos de gestión del riesgo.

D.3 Seguimiento y control y revisión del proceso

D.3.1 Generalidades

possibilitem desempenhar as suas funções e responsabilidades na estrutura de governança;

f) pessoas em toda a organização têm habilidades, conhecimento e competências de gestão de riscos suficientes para levarem a cabo as suas responsabilidades, conforme forem identificadas;

g) os recursos para a gestão de riscos são adequados;

h) lições foram aprendidas com os resultados reais, incluindo perdas, quase acidentes e oportunidades que ocorreram;

i) os objetivos estabelecidos para a gestão de riscos estão sendo alcançados.

Convém que seja acordado um cronograma de análise crítica regular, com a capacidade de realizar análises críticas para um propósito específico se as circunstâncias mudarem, por exemplo, quando as consequências dos riscos são repentinas ou severas.

Convém que os resultados de tal análise crítica incluam:

- um reporte global sobre o desempenho da estrutura para gerenciar riscos;

- um reporte sobre os progressos da implementação do plano de gestão de riscos (incluindo a análise de qualquer atraso na implementação);

- um relatório descrevendo a posição da maturidade da organização em relação às melhores práticas;

- recomendações de mudanças que são necessárias para melhorar a gestão de riscos e sua eficácia na organização;

- atualizações da política, objetivos e plano de gestão de riscos, quando necessário;

- atualizações da descrição do contexto em que a organização opera, conforme o caso;

- um reporte sobre tendências dos indicadores-chave de risco;

- um plano de ação que aborde as mudanças necessárias para cumprir os objetivos da gestão de riscos.

D.3 Monitoramento e análise crítica do processo

D.3.1 Geral

La finalidad del seguimiento y control y revisión del proceso de gestión del riesgo es asegurar que:

- es adecuado para la actividad del negocio;

- se implementa según lo previsto.

Los riesgos, los controles y los tratamientos subyacentes pueden ser modificados con el tiempo, y los responsables de la gestión del riesgo tienen que ser conscientes de las implicancias de estos cambios. Las fallas en los tratamientos del riesgo pueden causar que el riesgo sea no tolerable. Además, los controles que tienen por objeto modificar los riesgos pueden cambiar en función de la adecuación y la eficacia, así que a menos que al riesgo se le realice el seguimiento y control y revisión, puede ser que los riesgos no permanezcan dentro de los criterios aceptables de la organización y puede ser que la organización no tenga una comprensión actual de sus riesgos.

Los resultados del seguimiento y control y revisión serán remitidos en el establecimiento de la fase de contexto, que proporciona la base para la evaluación actualizada del riesgo, el cumplimiento de la naturaleza iterativa y dinámica del proceso de gestión del riesgo y el diseño de la estructura de gestión del riesgo.

D.3.2 Rendición de cuentas

El seguimiento y control debería ser una parte integral de la gestión. Los riesgos y los controles deberían ser asignados a los propietarios, quienes son responsables de su seguimiento. La responsabilidad debería estar documentada en las descripciones de roles o posición.

Las organizaciones deberían considerar la incorporación de indicadores de desempeño de la gestión del riesgo, que reflejen la gama de controles claves de la organización, por ejemplo en la revisión formal de los empleados, así se consideran las partes interesadas, la eficiencia interna financiera y los objetivos de aprendizaje y crecimiento. Los resultados en relación con el mismo conjunto de indicadores se pueden medir a todos los niveles de la organización y luego informar.

Los planes de tratamiento del riesgo también deberían ser vigilados para asegurar que se están logrando avances y que las acciones se completan a tiempo.

D.3.3 Aprender de la experiencia

La organización debería aprender de los resultados reales. Éstos deberían incluir las

O objetivo do monitoramento e da análise crítica do processo de gestão de riscos é assegurar que eles estão:

- adequados para a atividade empresarial da organização;

- funcionando como planejado.

Os riscos, seus controles e tratamentos subjacentes podem ser alterados ao longo do tempo, e os responsáveis pela gestão de riscos precisam estar conscientes das implicações dessas mudanças. Falhas nos tratamentos podem levar os riscos a tornarem-se inaceitáveis. Além disso, os controles cujo objetivo é modificar riscos podem mudar em termos de adequação e eficácia, de modo que, a não ser que o risco seja monitorado e analisado criticamente, os riscos podem não permanecer dentro dos critérios de aceitação de riscos da organização e a organização pode não ter uma compreensão atualizada de seus riscos.

Os resultados do monitoramento e análise crítica irão realimentar a fase de estabelecimento do contexto, fornecendo a base para a avaliação de riscos renovada, atendendo à natureza dinâmica e iterativa do processo de gestão de riscos e da concepção da estrutura para gerenciar riscos.

D.3.2 Responsabilização

Convém que o monitoramento seja uma parte integrante da gestão. Convém que os riscos e controles sejam alocados a proprietários, que são responsáveis por monitorá-los. Convém que essa responsabilidade seja registrada em descrições de funções ou cargos.

Convém que as organizações considerem a incorporação de indicadores de desempenho da gestão de riscos, que reflitam a gama dos direcionadores-chave organizacionais, nas análises críticas formais de empregados, como por exemplo, de modo que o financeiro, partes interessadas, eficiência interna e objetivos de aprendizado e crescimento sejam considerados. O desempenho em relação ao mesmo conjunto de indicadores pode ser medido em todos os níveis da organização e então reportado conforme o caso.
Convém que os planos de tratamento de riscos também sejam monitorados para assegurar que estejam tendo progresso e que ações sejam concluídas a tempo.

D.3.3 Aprendendo com a experiência

Convém que a organização aprenda com os resultados reais. Convém que estes incluam

pérdidas, los incidentes, las no conformidades y oportunidades que se identificaron con antelación, y que sin embargo no se actuó. Los puntos que pueden ser considerados en esta revisión incluyen:

- lo que sucedió;

- cómo y por qué el resultado se produjo;

- si todas las premisas necesitan ser revisadas como consecuencia de los resultados;

- qué medidas se han adoptado (si las hubo) en respuesta;

- la probabilidad que el resultado se repita;

- las respuestas adicionales o pasos a seguir;

- los puntos claves de aprendizaje y a quiénes necesita comunicarse.

D.3.4 Seguimiento y control

D.3.4.1 Los enfoques típicos para el seguimiento y control incluyen los siguientes.

a) Los propietarios del riesgo pueden explorar el entorno para seguir los cambios en el contexto. La frecuencia de esta actividad depende del nivel de riesgo y la dinámica de los cambios en el contexto. En algunos casos, los informes de excepción de indicadores pueden ser suficientes. El propietario del riesgo compara los factores externos o internos pertinentes contra la declaración de contexto para determinar si ha tenido lugar un cambio sustancial.

Esto puede implicar la comunicación periódica y la consulta con las partes interesadas para determinar si sus puntos de vista u objetivos han cambiado.

b) Los propietarios del riesgo deberían realizar también el seguimiento y control a tiempo de los planes de acciones de tratamiento del riesgo y las respuestas a los cambios en el entorno.

c) Los propietarios de control son responsables de supervisar los controles que se les asignen, que pueden implicar la verificación periódica o el seguimiento continuo. Debido a que la gestión del riesgo es más eficaz cuando está totalmente integrada con la toma de decisiones normales y el sistema de gestión de la organización, la organización debería utilizar la gestión del desempeño para realizar el seguimiento y control de los riesgos y la eficacia del proceso de gestión del riesgo.

perdas, quase perdas, não conformidades e oportunidades que foram identificadas com antecedência, ocorridas e ainda para as quais não houve ações. Pontos que podem ser considerados em tal análise crítica incluem:

- o que aconteceu;

- como e por que o resultado surgiu;

- se quaisquer dos pressupostos precisam ser analisados crtiticamente em decorrência do resultado;

- qual ação foi tomada (se houver) em resposta;

- a probabilidade de o resultado acontecer novamente;

- quaisquer respostas ou passos adicionais a serem tomados;

- pontos chave de aprendizagem e para quem precisam ser comunicados.

D.3.4 Monitoramento

D.3.4.1 Abordagens típicas para monitoramento incluem o seguinte.

a) Proprietários do risco podem varrer o ambiente para monitorar as mudanças no contexto. A frequência dessa atividade dependerá do nível de risco e da dinâmica das mudanças no contexto. Em alguns casos, reportes de exceção de indicadores podem ser suficientes. O proprietário do risco compara os fatores pertinentes, externos ou internos, em relação à declaração do contexto para determinar se uma alteração significativa ocorreu.

Isso pode envolver a comunicação e consulta periódicas às partes interessadas para determinar se seus pontos de vista ou objetivos mudaram.

b) Convém que os proprietários de risco também monitorem os planos de tratamento de riscos para ações oportunas e resposta a mudanças no ambiente.

c) Proprietários de controle são responsáveis por monitorar os controles atribuídos a eles, que podem envolver a verificação periódica ou monitoramento contínuo. Como a gestão de riscos é mais eficaz quando é totalmente integrada com a tomada de decisões normal e o sistema de gerenciamento da organização, convém que a gestão de desempenho da organização seja usada para monitorar os riscos e a eficácia do processo de gestão de riscos.

Los indicadores de desempeño deberían reflejar la gama de objetivos de la organización clave definidos cuando se estableció el contexto en el inicio del proceso. También se pueden desarrollar relacionándolos con los riesgos específicos y los controles y la aplicación del proceso de gestión del riesgo.

NOTA Como es el caso de los riesgos, también los controles deberían ser propiedad de una persona quien es responsable de su operación. El propietario u operador de control normalmente será la persona que ejecuta el control sobre una base diaria, y puede ser una persona distinta del dueño del riesgo. Esto no afecta a la responsabilidad general del dueño del riesgo para la modificación adecuada de este riesgo, y para el diseño, la ejecución, aplicación, seguimiento y evaluación de los controles correspondientes.

D.3.4.2 Los indicadores de desempeño pueden medir los resultados (por ejemplo, las pérdidas o ganancias específicas) o procesos (por ejemplo, terminación oportuna de los planes de tratamiento de riesgos). Normalmente se puede utilizar una mezcla de indicadores, pero generalmente los indicadores de resultado aplazan los cambios significativos que dan lugar a los mismos. Como resultado de ello, en un entorno que cambia rápidamente, es probable que sean más útiles los indicadores de proceso (indicadores prospectivos).

En la elección de los indicadores de desempeño, es importante verificar que:

- son medibles;

- su uso es eficiente en términos de demanda de tiempo, esfuerzo y recursos;

- el proceso de medición o vigilancia favorezca o facilite la conducta deseable y no motiva a un comportamiento indeseable (por ejemplo, la fabricación de datos);

- los involucrados comprenden el proceso y los beneficios esperados y tienen la oportunidad de dar su opinión en el establecimiento de los indicadores;

- los resultados son relevados y el desempeño se analiza e informa en una forma que facilite el aprendizaje y la mejora en la organización.

D.3.4.3 En la aplicación de gestión del desempeño para el proceso de gestión del riesgo, se debería tener en cuenta que:

- la medición eficaz del desempeño requiere de recursos, que deberían ser identificados y asignados como parte del desarrollo de los indicadores de desempeño;

Convém que os indicadores de desempenho reflitam a gama dos objetivos organizacionais-chave definidos quando o contexto foi estabelecido no início do processo. Eles também podem ser desenvolvidos de maneira a se relacionar a riscos e controles específicos e à aplicação do processo de gestão de riscos.

NOTA Como é o caso com os riscos, é aconselhável que os controles também sejam de propriedade de alguém que é responsável pela sua operação. O proprietário ou operador do controle seria normalmente a pessoa que executa o controle em uma rotina diária e pode ser alguém que não seja o proprietário do risco. Isso não afeta a responsabilidade global do proprietário do risco para a modificação apropriada desse risco, e para a concepção, implementação, aplicação, monitoramento e avaliação dos controles correspondentes.

D.3.4.2 Os indicadores de desempenho podem medir os resultados (por exemplo, perdas ou ganhos específicos) ou processos (por exemplo, de conclusão oportuna dos planos de tratamento de riscos). Normalmente, uma mistura de indicadores pode ser utilizada, mas indicadores de desempenho de resultados geralmente atrasam significativamente as mudanças que lhes dão origem. Como resultado, em um ambiente em rápida mudança, os indicadores de processo (indicadores antecedentes) são provavelmente mais úteis.

Na escolha de indicadores de desempenho, é importante verificar se:

- eles são mensuráveis;

- a sua utilização é eficiente em termos de exigências de tempo, esforço e recursos;

- o processo de medição ou vigilância favorece ou facilita o comportamento desejável e não motiva o comportamento indesejável (por exemplo, fabricação de dados);

- os envolvidos entendem o processo e os benefícios esperados e têm a oportunidade de contribuir para a definição de indicadores;

- os resultados são capturados e o desempenho analisado e reportado de forma a facilitar a aprendizagem e a melhoria em toda a organização.

D.3.4.3 Na aplicação de gestão de desempenho para o processo de gestão de riscos, convém observar que:

- a medição eficaz do desempenho requer recursos, e é recomendado que estes sejam identificados e alocados como parte do desenvolvimento dos indicadores de desempenho;

- algunas de las actividades de gestión del riesgo pueden ser difíciles de medir, lo que no los hace menos importantes, pero puede ser necesario el uso de indicadores indirectos, por ejemplo, los recursos dedicados a las actividades de gestión del riesgo puede ser un medida sustituta de compromiso con la gestión del riesgo eficaz;

- cualquier variación entre los datos de medición de los indicadores de desempeño y la sensación instintiva es importante y debería ser investigada, por ejemplo, si la dirección le sigue preocupando que los riesgos no se manejan adecuadamente, a pesar de numerosas evaluaciones del riesgo que indican bajos niveles de riesgo, se debería investigar y descartar estas preocupaciones;

- mientras que el deterioro repentino de los indicadores generalmente atraen la atención, el deterioro progresivo puede ser igualmente problemático, y se recomienda se le realice el seguimiento y control de la evolución de los indicadores de desempeño.

D.3.5 Revisión

La gerencia debería revisar periódicamente los procesos, sistemas y actividades para asegurar que:

a) no han surgido nuevos riesgos;

b) los controles y tratamientos del riesgo siguen siendo adecuados y eficaces.

Estas revisiones deberían ser programadas (ver programa y enfoque de auditoría basado en el riesgo y cómo seleccionar los revisores, como se indica en la Norma ISO 19011).

Estas revisiones pueden utilizar las mismas técnicas que el seguimiento continuo, pero pueden proporcionar un análisis más objetivo si se llevan a cabo por alguien que no esté directamente involucrado en la operación de los procesos. La frecuencia de la revisión puede verse afectada por el nivel de riesgo, el ciclo de la planificación empresarial, la dinámica en el entorno/contexto, o una reunión de un órgano de gobernanza que es responsable del seguimiento y control de los riesgos y la gestión del riesgo.

Si se detectan problemas, la organización debería considerar cómo se produjo y por qué no se detectó antes.

Los controles deberían asegurarse a través de las acciones de los gerentes responsables (dueños del riesgo) como parte de sus puestos de trabajo y funciones normales.

- algumas atividades de gestão de riscos podem ser de difícil medição, o que não as torna menos importantes, mas pode ser necessário o uso de indicadores substitutos, como por exemplo, recursos destinados às atividades de gestão de riscos pode ser uma medida substituta do compromisso para a gestão de riscos eficaz;

- qualquer variação entre dados de medição de indicadores de desempenho e a sensação institiva é importante e é recomendado que esta seja investigada, como por exemplo, se a gerência continua preocupada que os riscos não estão sendo bem gerenciados, apesar de as inúmeras avaliações de riscos indicarem baixos níveis de risco, convém que essas preocupações sejam investigadas e não rejeitadas;

- enquanto a súbita degradação de indicadores costuma atrair atenção, a degradação progressiva pode ser igualmente problemática, e é recomendado que as tendências em indicadores de desempenho sejam monitoradas e analisadas.

D.3.5 Análise crítica

Convém que a direção periodicamente analise criticamente os processos, sistemas e atividades para assegurar que:

a) não têm surgido novos riscos;

b) os controles e tratamentos de riscos permanecem adequados e eficazes.

Convém que tais análises críticas sejam programadas (ver programa e abordagem de auditoria baseada no risco e como selecionar analistas, conforme descrito na ISO 19011).

Estas análises críticas podem usar as mesmas técnicas como o monitoramento contínuo, mas se forem conduzidas por alguém que não esteja diretamente envolvido na operação dos processos, podem fornecer uma análise mais objetiva. A frequência de análise crítica pode ser influenciada pelo nível de risco, o ciclo de planejamento de negócios, as dinâmicas no ambiente/contexto, ou uma reunião de um organismo de governança, que é responsável pela supervisão de riscos e pela gestão de riscos.

Se forem encontrados problemas, convém que a organização considere como surgiram e por que não foram detectados antes.

Convém que os controles sejam assegurados por meio das ações dos gestores responsáveis (proprietários do risco), como parte de seu trabalho e funções normais.

La asignación de los controles específicos a los dueños de control les facilita la aplicación de los controles, pero se requiere la formación de los mismos en los procesos de aseguramiento del control con el fin de que sea eficaz.

Cuando se planifican los cambios en la organización, o se detectan cambios externos, puede haber cambios en:

- el entorno externo o interno, o los puntos de vista de las partes interesadas;

- el contexto de la gestión del riesgo, la organización, los objetivos y sus criterios de riesgo;

- los riesgos y niveles de riesgo;

- la necesidad de tratamientos de riesgo;

- el efecto y la eficacia de los controles.

Por esta razón, es esencial que las organizaciones revisen sus riesgos, tratamientos y controles del riesgo en el desarrollo o revisión de los negocios o planes estratégicos. Además, debido a que los planes de negocio y estratégicos pueden crear o modificar los objetivos de una organización, es valioso utilizar el proceso de evaluación del riesgo para destacar los proyectos de planes con el fin de velar que la propuesta o los objetivos son alcanzables, y también para definir en que medida el tratamiento del riesgo es necesario para asegurar resultados exitosos. Quienes llevan a cabo el proceso de gestión del riesgo también deberían revisar periódicamente sus experiencias, productos y resultados para identificar las oportunidades de mejora.

A alocação de controles específicos para controlar proprietários facilita a implementação de controles, mas esses proprietários necessitarão de treinamento em processos de garantia de controle, a fim de serem eficazes.

Quando mudanças organizacionais são planejadas, ou mudanças externas são detectadas, pode haver mudanças em:

- no ambiente externo ou interno ou as partes interessadas e seus pontos de vista;

- no contexto de gestão de riscos, os objetivos da organização e os seus critérios de risco;

- nos riscos e níveis de risco;

- na necessidade de tratamentos de riscos;

- no efeito e a eficácia dos controles.

Por esta razão, é essencial para as organizações a análise crítica de seus riscos, tratamentos e controles de riscos no desenvolvimento ou revisão de planos estratégicos ou de negócios. Adicionalmente, como os planos estratégicos e de negócios permitem criar ou revisar os objetivos de uma organização, é valioso usar o processo de avaliação de riscos para realizar teste de esforço dos esboços dos planos, a fim de assegurar que os objetivos propostos são realizáveis, e também para definir a medida de tratamento de riscos requerida para assegurar resultados bem-sucedidos. Convém também que aqueles que executam o processo de gestão de riscos analisem criticamente de forma regular as suas experiências, saídas e resultados para identificar oportunidades de melhoria.

Anexo E
(informativo)

La integración de la gestión del riesgo con un sistema de gestión

Integrando a gestão de riscos em um sistema de gestão

E.1 Generalidades

La gestión del riesgo es una parte integral del sistema de gestión de una organización. La Norma ISO 31000 recomienda a las organizaciones a desarrollar, implementar y mejorar continuamente un marco cuyo objetivo es integrar la gestión del riesgo en la organización con el sistema de gestión (incluido la gobernanza y la estrategia). Específicamente, la integración debería asegurar que la información sobre el riesgo se utilice como base para la toma de decisiones en todos los niveles de la organización. Las personas y las organizaciones gestionan el riesgo cada día como parte de la forma en que toman las decisiones. La gestión del riesgo ya está integrada de forma natural en lo que todos hacemos antes de decidirnos a hacer algo. Algunos son mejores en esto que otros, pero todos pueden mejorar la calidad de la gestión del riesgo y la toma de decisiones, lo que resulta en una mejora en la consecución de los objetivos y mejora de la confianza. Si el propósito de integrar la gestión del riesgo es agregar valor, lógicamente significa la adopción de formas de influir en lo que ya se lleva a cabo, de intensificar y mejorar, en lugar de reemplazarlo con algo diferente. No puede significar la adición o forzar algo diferente a lo que ya se realiza como una función natural de la toma de decisiones.

La integración no se trata simplemente de introducir herramientas gestión del riesgo establecidas y normalizadas y los procesos en (a) el/los sistema/s de gestión existente/s, requiere la adecuación y modificación de estos instrumentos y procesos para satisfacer las necesidades de los que toman decisiones y los procesos existentes para la toma decisiones.

En este Anexo se presentan algunos ejemplos prácticos de cómo la gestión del riesgo se puede integrar en el/los sistema/s de gestión existente/s.

E.2 ¿Qué es un sistema de gestión?

Todas las organizaciones utilizan algún tipo de sistema de gestión. En los últimos tiempos, se han creado sistemas de gestión formales que consisten en una variedad de requisitos, que proporcionan un marco en el que la organización puede establecer prácticas y procedimientos para dirigir y controlar las actividades de gestión.

E.1 Geral

A gestão de riscos é parte integrante do sistema de gestão de uma organização. A ISO 31000 recomenda que as organizações desenvolvam, implementem e melhorem continuamente uma estrutura cujo objetivo é integrar a gestão de riscos no sistema de gestão da organização (incluindo governança e estratégia). Especificamente, convém que a integração assegure que a informação sobre riscos é usada como base para a tomada de decisão em todos os níveis da organização. As pessoas e as organizações gerem riscos a cada dia como parte da forma como eles tomam decisões. A gestão de risco já está naturalmente integrada em tudo que nós fazemos antes de decidirmos fazer algo. Alguns são melhores nisto do que outros, mas todos podem aperfeiçoar a qualidade da gestão de riscos e da tomada de decisão, resultando na melhoria do alcance dos objetivos e melhorando a confiança. Se a proposta de integrar a gestão de riscos for criar valor, isso logicamente significa adotar meios de influenciar aquilo que já acontece, para melhorá-lo e aperfeiçoá-lo, ao invés de substituí-lo por algo diferente. Isto não pode significar adicionar ou impor algo de diferente naquilo que já ocorre como uma função natural do processo de tomada de decisão.”

Integração não envolve simplesmente a introdução de ferramentas e processos de gestão de riscos estabelecidos e padronizados em (um) sistema(s) de gestão existente(s), isto requer adaptação e alteração dessas ferramentas e processos para atender às necessidades dos tomadores de decisão e seus processos de tomada de decisão existentes.

Este Anexo fornece alguns exemplos práticos de como a gestão de riscos pode ser integrada no(s) sistema(s) de gestão existente(s).

E.2 O que é um sistema de gestão?

Todas as organizações usam algum tipo de sistema de gestão. Recentemente, sistemas de gestão formalizados consistindo de uma variedade de requisitos foram criados, fornecendo uma estrutura em que a organização pode estabelecer práticas e procedimentos de gestão para dirigir e controlar suas atividades. Muitas normas

Muchas de las normas internacionales se ocupan de los sistemas de gestión en general o con respecto a los contenidos específicos.

Un sistema de gestión es un conjunto de elementos interrelacionados o que interactúan de una organización para establecer políticas y objetivos, así como los procesos para alcanzar dichos objetivos. Desde la perspectiva de la gestión empresarial, la eficiencia se gana por tener un sistema integrado de gestión.

Por ejemplo, la gestión de la calidad de la que refiere la Norma ISO 9001 tiene un enfoque amplio orientado hacia la satisfacción del cliente, mientras que la gestión del riesgo trata con los efectos de la incertidumbre sobre el logro de los objetivos que pueden no sólo ser de interés para los clientes, sino también a una variedad de otras partes interesadas. Muchas organizaciones han implementado un sistema de gestión de calidad basado en las Normas ISO 9001 y la gestión de riesgo puede ser integrada en los sistemas de gestión, creando sinergias y evitando la duplicación.

E.3 Sistema de gestión integrado y gestión del riesgo

Además de la integración de la gestión del riesgo en los procesos centrales del negocio, hay una necesidad de crear una interacción entre todos los enfoques de sistemas de gestión, por ejemplo, gestión de calidad, gestión ambiental, gestión de seguridad, cumplimiento, gestión financiera y presentación de informes, e incluso con la administración de seguros tratando con eventos que pueden ser transferidos financieramente a otras organizaciones.

Estos sistemas de gestión individuales deberían formar un sistema integrado de gestión, basado en la política y la estrategia de cualquier organización. Aun cuando una organización cuenta con sistemas individuales de gestión para gestionar los riesgos particulares, el marco de gestión del riesgo debería extenderse e incorporarse a esos sistemas.

Este enfoque de gestión del riesgo de toda la organización puede:

a) aumentar la atención de la alta dirección de la organización en los objetivos estratégicos;

b) permitir que todos los riesgos en el sistema de gestión integrado se manejen de acuerdo con los principios y directrices de la Norma ISO 31000.

Este enfoque puede incluir lo siguiente:

- la aplicación de las técnicas de gestión del riesgo

internacionais lidam com sistemas de gestão em geral ou relativos a um conteúdo especifico.

Um sistema de gestão é um conjunto de elementos inter-relacionados ou interativos de uma organização para estabelecer políticas e objetivos, bem como processos para atingir esses objetivos. Sob a perspectiva da gestão empresarial, a eficiência é ganha quando se tem um sistema de gestão integrado.

Por exemplo, a gestão da qualidade conforme descrita na ISO 9001 tem uma ampla abordagem voltada para a satisfação do cliente, enquanto a gestão de riscos lida com os efeitos da incerteza nos objetivos que podem não apenas ser pertinentes para os clientes, mas também para uma variedade de outras partes interessadas. Muitas organizações implementaram um sistema de gestão da qualidade baseado nos requisitos da ISO 9001, e a gestão de riscos pode ser integrada a esses sistemas de gestão, criando sinergias e evitando duplicação.

E.3 Sistema de gestão integrado e gestão de riscos

Assim como na integração da gestão de riscos aos processos centrais do negócio, é necessário criar uma interação entre todas as abordagens de sistema de gestão, isto é, gestão da qualidade, gestão ambiental, gestão da segurança, gestão financeira, da conformidade e de reporte, e até a gestão de seguros que lida com os eventos que podem ser financeiramente transferidos para outras organizações.

Convém que estes sistemas de gestão individuais formem um sistema de gestão integrado, baseado na politica e estratégia de qualquer organização. Até no caso de uma organização ter um sistema de gestão individual para gerenciar riscos particulares, convém que a estrutura para gerenciar riscos se estenda e incorpore esses sistemas.

Tal abordagem de gestão de riscos interorganizacional pode:

a) aumentar o foco da Alta Direção nos objetivos estratégicos da organização;

b) permitir que todos os riscos no sistema de gestão integrado sejam tratados de acordo com os princípios e diretrizes da ISO 31000.

Esta abordagem pode envolver o seguinte:

- a aplicação no sistema de gestão da qualidade

que se refieren sobre todo a productos y proyectos, en el sistema de gestión de la calidad;

- el tratamiento de las incertidumbres en la gestión ambiental, por ejemplo, los incidentes y accidentes potenciales en locales peligrosos, disposición de materiales y sustancias peligrosas;

- el tratamiento de los riesgos combinados con operaciones como la seguridad en el trabajo;

- el manejo de los riesgos de seguridad, por ejemplo, los actos de violencia en contra de la organización o de sus empleados o clientes;

- el manejo los riesgos de seguridad de la Tecnología de la Información (TI), por ejemplo, el desglose de las operaciones de TI, pérdida de datos, violación de la confidencialidad y asegurar la continuidad del negocio;

- la gestión del riesgo de continuidad de negocio que aseguren la preparación y respuesta rápida ante eventos perturbadores;

- el establecimiento de controles para proteger los activos de la organización, para asegurar una correcta información, el cumplimiento de los requisitos legales, o para gestionar los riesgos asegurables de una manera que minimice las primas.

E.4 La implementación de la gestión del riesgo en un marco de gestión de la calidad

E.4.1 Generalidades

El proceso de gestión del riesgo debería integrarse en los procesos de decisión de la organización, sea cual sea el nivel y la función a la que se toman esas decisiones.

E.4.2 Identificación y concientización de la toma de decisiones

Los siguientes métodos ayudan en el reconocimiento de cuándo y dónde se están tomando las decisiones, alineado con el ciclo Planificar-Hacer-Verificar-Actuar.

a) la identificación de todas las formas de prácticas de toma de decisiones formales que ya existen dentro de la organización. En las grandes organizaciones, es probable que sean numerosos los procedimientos que requieren aprobaciones formales para una amplia gama de decisiones, por ejemplo, la aprobación del plan estratégico anual, los gastos de capital, el empleo de nuevo personal, la modificación de los controles del proceso, los viajes del personal.

de técnicas de gestão de riscos concernentes principalmente à gestão de riscos de produto e projeto;

- lidar com as incertezas da gestão ambiental, por exemplo, incidentes e acidentes potenciais em instalações perigosas, descarte de materiais e substâncias perigosas;

- o tratamento de riscos combinado com operações, como segurança ocupacional;

- lidar com os riscos de segurança, isto é, atos de violência contra a organização ou seus empregados ou clientes;

- lidar com os riscos de segurança da tecnologia da informação (TI), isto é, a queda das operações de TI, perda de dados, violação da confidencialidade e assegurar a continuidade dos negócios;

- gerenciar os riscos de continuidade de negócios que asseguram a preparação para, e a resposta rápida a, eventos disruptivos;

- estabelecer os controles para proteger os ativos da organização, para assegurar o correto reporte e a conformidade aos requisitos legais ou para gerenciar riscos seguráveis de maneira a minimizar os prêmios.

E.4 A implementação da gestão de riscos na estrutura de um sistema de gestão da qualidade

E.4.1 Geral

Convém que o processo de gestão de riscos seja integrado nos processos de tomada de decisão da organização, independentemente do nível e da função nos quais essas decisões são tomadas.

E.4.2 Identificação e conscientização da tomada de decisões

Os seguintes métodos ajudam a reconhecer quando e onde as decisões estão sendo tomadas, alinhadas ao ciclo *Plan* (planejar) - *Do (*fazer) - *Check* (checar) - *Act* (agir) (PDCA).

a) Identificar todas as formas de práticas formais de tomada de decisão, que já existem na organização. Em grandes organizações, é provável que existam numerosos procedimentos que requerem aprovações formais para uma vasta gama de decisões, por exemplo, a aprovação do planejamento estratégico anual, as despesas de capital, a admissão de novos funcionários, a modificação de controles de processos, as viagens de funcionários.

b) el uso de diagramas de flujo, o alguna otra técnica, para mapear las principales prácticas de toma de decisiones y las secuencias que son aplicables tanto a proyectos específicos y todos los aspectos del negocio. Esto se puede considerar en una división o una base de la función, y debería extenderse a la gobernanza, así como a la toma de decisiones de gestión. Si hay actividades que se gestionan a través de la aplicación de un sistema de gestión formalizado (por ejemplo, la gestión de calidad a través de la aplicación de la Norma ISO 9001), los puntos de decisión en este tipo de sistemas deberían formar parte de este análisis. Del mismo modo, si la organización cuenta con algún tipo de autoridad para la toma de decisiones delegada, estas delegaciones deberían ser incluidas en el análisis. El resultado final debería ser una imagen coherente y documentada de donde se toman las decisiones, quién toma esas decisiones y los procesos existentes aplicables a tales decisiones.

Con una combinación de las técnicas mencionadas debería generarse un alto grado de concientización, tanto de la organización como del personal que toma las decisiones.

E.4.3 Evaluación del riesgo

En algunos tipos de decisiones (por ejemplo, el desarrollo y la realización de un nuevo producto, o la planificación y ejecución de un proyecto de gran envergadura), se debería incluir una evaluación formal de los riesgos en las distintas etapas del proyecto. Por ejemplo, la mayoría de los proyectos tienen múltiples puntos de decisión, es decir, de viabilidad, modelo de negocio, presupuesto detallado y la planificación, la ejecución y entrega final. En cada uno de estos puntos, es adecuada una evaluación formal de los riesgos para decidir entre las distintas opciones. Esto aumenta la probabilidad de éxito del proyecto y también mejora la eficiencia.

Para la evaluación del riesgo de las decisiones operativas, se pueden desarrollar formularios normalizados simples del proceso de gestión del riesgo para su uso por parte del personal involucrado.

Estos métodos son especialmente adecuados en situaciones donde las personas trabajan sin supervisión directa. Un elemento clave de estos métodos es la creación de conciencia sobre premisas como insumos para las decisiones. Por definición, las premisas son una fuente de incertidumbre.

Tales procesos normalizados pueden ser específicos para el tipo de toma de decisiones en cuestión, para el grupo particular de personas que realizan una tarea en particular, y para el contexto

b) O uso de fluxograma, ou alguma outra técnica para mapear as práticas principais de tomada de decisão e as sequências que são aplicadas tanto a projetos específicos quanto a todos os aspectos do negócio. Isto pode ser considerado ao nível de divisão ou de função, e convém que seja estendido à governança, bem como à tomada de decisão gerencial. Caso existam atividades que sejam gerenciadas por meio da aplicação de um sistema de gestão formal (por exemplo, gestão da qualidade por meio da aplicação da ISO 9001), convém que os pontos de decisão em tais sistemas formem parte desta análise. Similarmente, caso a organização tenha alguma forma de autoridade delegada para a tomada de decisão, convém que tais delegações sejam incluídas nestas análises. É conveniente que o resultado final seja uma fotografia coerente e documentada de onde as decisões são tomadas, de quem toma essas decisões, e dos processos existentes aplicáveis a tais decisões.

Convém que a combinação das técnicas acima crie um alto nível de conscientização, tanto organizacional quanto pessoal na tomada de decisões.

E.4.3 Processo de avaliação de risco

Em alguns tipos de decisão (por exemplo, desenvolvimento e realização de um novo produto, ou planejamento e implementação de um projeto maior) será apropriado incluir um processo de avaliação de risco formal em vários estágios do projeto. Por exemplo, a maioria dos projetos tem múltiplos pontos de decisão, isto é, a viabilidade, caso de negócio, orçamento e planejamento detalhados, implementação, e entrega. Em cada um destes pontos, um processo de avaliação de risco formal é apropriado para decidir entre opções. Isto aumenta a probabilidade do sucesso do projeto e também melhora a sua eficiência.

Para o processo de gestão de riscos das decisões operacionais, formulários padronizados simples do processo de gestão de riscos podem ser desenvolvidos para o uso pelo pessoal envolvido.

Tais métodos são especialmente adequados em situações onde pessoas trabalham sem supervisão direta. Um componente-chave desses métodos é criar uma conscientização sobre pressupostos como entradas para as decisões. Por definição, os pressupostos são uma fonte de incerteza.

Tais processos padronizados podem ser específicos para o tipo de tomada de decisão envolvida, para o grupo de pessoas em particular que desenvolvem uma tarefa em particular, e para

típico en el que se producen. Los sistemas simples pueden ser codificados en una tarjeta que consiste en una lista de verificación de tamaño de bolsillo y ser llevados por todos los que participan en ese tipo de trabajo.

E.4.4 Implicancias para el marco de gestión de riesgos

La aplicación de las técnicas descritas en el presente apartado requiere del establecimiento de un marco de gestión de riesgos adecuados o cambios en el mismo, por ejemplo,

- la modificación de la política de gestión del riesgo de la organización;

- los ajustes para llevar a cabo la investigación y el mapeo de la práctica de toma de decisiones inicial;

- la realización de enmiendas a los manuales de procedimientos;

- la formación de los directivos y el personal;

- la formación específica de las personas cuyo trabajo se lleva a cabo de acuerdo con un sistema de gestión específico (por ejemplo, los que se ocupan de la gestión de determinados tipos de riesgo);

- los ajustes al sistema de la organización, de la capacidad de seguridad y la información de gestión del riesgo;

- la efectiva comunicación interna y la consulta.

o contexto típico onde ela ocorre. Sistemas simples podem ser codificados em cartões de bolso de instrução de lista de verificação e levados por todos os envolvidos nesse tipo de trabalho.

E.4.4 Modificação na política de gestão de riscos da organização;

A implementação das técnicas descritas nesta Seção irão requerer provisão apropriada ou ajuste da estrutura para gerenciar riscos, por exemplo.

- modificação na política de gestão de risco da organização;

- arranjos para conduzir a investigação inicial e mapeamento da prática de tomada de decisão;

- realizar modificações nos manuais de procedimento;

- treinamento de gerentes e pessoal;

- treinamento específico daqueles cujo trabalho é realizado de acordo com o sistema de gestão específico (por exemplo, aqueles que estão relacionados com a gestão de tipos de risco em particular);

- ajustes no sistema de garantia e capacidade de informação de gestão de riscos da organização;

- comunicação e consultas internas efetivas.

Bibliografía

Bibliografia

[1] NM ISO 9000, Sistemas de gestión de calidad - Fundamentos y vocabulario / *Sistemas de gestão da qualidade - Fundamentos e vocabulário*

[2] NM ISO 9001, Sistemas de gestión de calidad - Requisitos / *Sistemas de gestão da qualidade - Requisitos*

[3] NM ISO 19011, Directrices para la auditoría de sistemas de gestión / *Diretrizes para auditoria de sistemas de gestão*

[4] AMN Guía ISO 73:2013, Gestión del riesgo - Vocabulario (ISO Guía 73:2009, IDT) / *Gestão de riscos - Vocabulário (ISO Guia 73:2009, IDT)*

[5] NM IEC 31010:2014, Gestión del riesgo - Técnicas de evaluación del riesgo (ISO/IEC 31010:2009, IDT) / *Gestão de riscos - Técnicas para o processo de avaliação de riscos (ISO/IEC 31010:2009, IDT)*

ICS 03.100.01
Descriptores: gestión de riesgos; guía
Palavras chave: gestão de riscos; guia
Número de páginas: 58

SINTESIS DE LAS ETAPAS DE ESTUDIO DE LA NORMA MERCOSUR

PNM 90:06-ISO/TR 31004

1. INTRODUCCIÓN

La intención de este Informe Técnico es asistir a las organizaciones en la mejora de la eficacia de los esfuerzos empleados en la gestión del riesgo alineándola con la ISO 31000:2009.

2. COMITÉ ESPECIALIZADO

El texto del Proyecto de Norma MERCOSUR 90:06-ISO/TR 31004 fue elaborado oportunamente por la CE 90:06 – Gestión de riesgos.

El texto base del Proyecto participaron Brasil y Uruguay, y tuvo su origen (traducción) en ISO/TR 31004:2013 *Risk management - Guidance for the implementation of ISO 31000*.

3. MIEMBROS ACTIVOS EN LA ELABORACIÓN DEL PROYECTO

ABNT - Associação Brasileira de Normas Técnicas
UNIT - Instituto Uruguayo de Normas Técnicas

4. MIEMBROS PARTICIPANTES EN EL PROCESO DE VOTACIÓN

ABNT - Associação Brasileira de Normas Técnicas
IRAM - Instituto Argentino de Normalización y Certificación
INTN - Instituto Nacional de Tecnología, Normalización y Metrología
UNIT - Instituto Uruguayo de Normas Técnicas
IBNORCA - Instituto Boliviano de Normalización y Calidad
INN - Instituto Nacional de Normalización [Chile]

5. CONSIDERACIONES

Este proyecto se inició durante el año de 2014, donde Uruguay si quedó a cargo de la Secretaría Técnica de la Comisión Especial MERCOSUR 90:06 de Gestión de Riesgos.
El 24 de febrero de 2016 fue a votación nacional para la consideración de los países miembros del MERCOSUR, por un período de 60 días, finalizando el 25 de abril de 2016. Uruguay aprobó el texto con observaciones editoriales. Argentina y Bolivia aprobaron el texto sin observaciones.
El 04 de mayo de 2016 fue nuevamente a votación final para la consideración de los países miembros del MERCOSUR, por un período de 30 días.
ABNT ha solicitado prórroga del plazo para la votación final de más 45 días.
El documento fue finalmente enviado a AMN, conforme lo determina el reglamento para el estudio de normas MERCOSUR, para impresión y aprobación como norma MERCOSUR (NM).