Após a leitura do curso, solicite o certificado de conclusão em PDF em nosso site: www.administrabrasil.com.br

Ideal para processos seletivos, pontuação em concursos e horas na faculdade.

Os certificados são enviados em **5 minutos** para o seu e-mail.

Carga horária no certificado: 180 horas

A norma **ABNT NBR ISO 31000**, que fornece diretrizes para a **gestão de riscos**, nasceu de uma demanda global por uma abordagem unificada e coerente para lidar com a **incerteza** no ambiente organizacional. Antes de sua publicação, diversas indústrias e setores desenvolviam métodos próprios para gerenciar riscos, o que frequentemente resultava em **abordagens fragmentadas** e **inconsistentes**. Essa falta de padronização dificultava a comparação de desempenho e a implementação de práticas eficazes em diferentes contextos.

O **propósito inicial** da **ISO 31000**, em sua primeira edição de 2009, foi precisamente o de estabelecer um **conjunto harmonizado de princípios e diretrizes** que pudessem ser aplicados por **qualquer tipo de organização**, independentemente de seu tamanho, setor ou complexidade. A norma foi concebida como um **guia** para auxiliar as organizações a **integrar a gestão de riscos** em todas as suas atividades e processos de tomada de decisão, e não como um padrão de sistema de gestão passível de certificação. A versão brasileira, **ABNT NBR ISO 31000**, reflete fielmente o conteúdo técnico da norma internacional, adaptado para uso no Brasil.

A evolução da norma, culminando na edição de 2018 (ABNT NBR ISO 31000:2018), fortaleceu o foco na **integração da gestão de riscos** com a **governança** e a **cultura organizacional**. A revisão enfatizou o papel crucial da **liderança** e do **comprometimento da alta direção** para o sucesso da gestão de riscos. A norma de 2018 reforça que a gestão de riscos deve ser uma **parte integrante** de todas as funções e atividades da organização, sendo **fundamental para a maneira como a organização é gerenciada** em todos os níveis. O objetivo primordial da **ISO 31000**, conforme redefinido e reforçado na versão de 2018, é a **criação e proteção de valor** para a organização, promovendo a **melhoria do desempenho**, incentivando a **inovação** e apoiando o **alcance dos objetivos estratégicos e operacionais**.

A Necessidade de um Guia Universal para Gerenciar a Incerteza

O cenário global de negócios é cada vez mais caracterizado por **volatilidade**, **complexidade** e **interconexão**. As organizações operam em ambientes dinâmicos, onde a **incerteza** pode afetar significativamente sua capacidade de atingir metas. Sem um **referencial comum** para a **gestão de riscos**, as organizações enfrentavam desafios na identificação, análise e tratamento de riscos de forma consistente e eficaz.

A **ISO 31000** preencheu essa lacuna ao oferecer um **modelo conceitual genérico**, aplicável a **qualquer contexto**, desde os riscos financeiros em uma instituição bancária até os riscos de segurança operacional em uma fábrica ou os riscos de projeto em uma empresa de engenharia. O guia permite que organizações de diferentes portes e setores desenvolvam e implementem suas próprias abordagens de gestão de riscos de maneira estruturada. Por exemplo, uma organização não governamental (ONG) que trabalha em projetos sociais em diferentes regiões pode usar as diretrizes da **ISO 31000** para identificar e gerenciar riscos como instabilidade política local, segurança da equipe em campo, captação de recursos e conformidade com leis e regulamentações específicas de cada país. A norma fornece a estrutura para pensar sobre esses riscos de forma sistemática, mesmo que a natureza dos riscos seja muito diferente daquela enfrentada por uma empresa privada.

Como estabelecer o escopo, o contexto e os critérios para a gestão de riscos conforme a ISO 31000?

O processo de **gestão de riscos** conforme a **ISO 31000** inicia-se de forma prática com a etapa fundamental de estabelecer o **escopo**, o **contexto** e os **critérios**. Esta fase é crucial porque personaliza o processo de **gestão de riscos** para a realidade específica da organização e da atividade em questão, garantindo que os esforços futuros na identificação, análise e tratamento de riscos sejam relevantes e eficazes. É aqui que se define "o quê", "onde", "quando" e "por que" a **gestão de riscos** será aplicada, e quais parâmetros serão usados para avaliar a importância dos riscos identificados. Sem uma definição clara desses elementos, a **gestão de riscos** pode se tornar genérica, desalinhada com os objetivos organizacionais e, consequentemente, pouco útil na tomada de decisão.

Definindo o Escopo da Gestão de Riscos

Definir o **escopo** na **gestão de riscos** significa determinar o alcance e os limites das atividades que serão sujeitas ao processo. A **ISO 31000** permite que a gestão de riscos seja aplicada em diferentes **níveis** dentro da organização, como o **nível estratégico** (relacionado aos objetivos de longo prazo da organização), o **nível operacional**

(relacionado às atividades do dia a dia), ou em **programas** e **projetos específicos**. Ao definir o escopo, é vital ser claro sobre os **objetivos** que se busca alcançar com a gestão de riscos, as **decisões** que precisam ser apoiadas por ela, os **resultados esperados** das etapas do processo, e os **recursos** disponíveis (tempo, pessoal, ferramentas). Também é importante considerar as **inclusões e exclusões específicas** da análise de riscos. Por exemplo, ao aplicar a **ISO 31000** para gerenciar os riscos de um novo projeto de lançamento de produto, o escopo pode ser definido para cobrir apenas as atividades de desenvolvimento, marketing e vendas associadas a esse produto específico, excluindo riscos relacionados à produção em massa ou distribuição logística inicial, que podem ser gerenciados em outros processos. Outro exemplo: uma prefeitura pode definir o escopo da **gestão de riscos** para um projeto de revitalização de uma área urbana, focando nos riscos de cronograma, orçamento, aceitação pública e impacto ambiental dentro da área delimitada do projeto, mas excluindo riscos sistêmicos da economia municipal. A clareza no escopo assegura que os esforços de gestão de riscos sejam direcionados para onde são mais necessários e relevantes.

Compreendendo os Contextos Externo e Interno

A **gestão de riscos** não ocorre no vácuo; ela é profundamente influenciada pelos **contextos externo e interno** nos quais a organização opera. A **ISO 31000** enfatiza a necessidade de examinar e compreender esses contextos para personalizar a estrutura e o processo de gestão de riscos. O **contexto externo** abrange o ambiente no qual a organização busca alcançar seus objetivos e pode incluir **fatores sociais, culturais, políticos, jurídicos, regulatórios, financeiros, tecnológicos, econômicos e ambientais**. Compreender as tendências de mercado, as mudanças na legislação, as expectativas dos stakeholders externos (clientes, fornecedores, reguladores) e as condições econômicas são exemplos de análise do contexto externo. Por exemplo, uma empresa de energia pode analisar o contexto externo considerando novas regulamentações sobre emissões de carbono, a volatilidade dos preços internacionais do petróleo e gás, e as preocupações da comunidade local sobre o impacto ambiental de suas operações, tudo isso para identificar riscos que afetam seus objetivos de negócio e conformidade.

O **contexto interno** refere-se ao ambiente dentro da própria organização. Isso inclui sua **visão, missão e valores**, a **cultura organizacional**, a **estrutura de governança**, as **políticas e objetivos**, as **capacidades** em termos de recursos (humanos, financeiros, tecnológicos), os **sistemas de informação** e os **relacionamentos com partes interessadas internas** (funcionários, acionistas). Compreender a cultura, por exemplo, é crucial, pois ela influencia a forma como os riscos são percebidos e tratados dentro da organização. Uma cultura avessa ao risco reagirá de forma diferente a uma mesma situação de risco do que uma cultura que incentiva a experimentação (controlada). Por exemplo, uma empresa de desenvolvimento de software, ao analisar seu contexto interno para aplicar a **ISO 31000**, consideraria sua estrutura organizacional (equipes ágeis vs. tradicionais), sua cultura de compartilhamento de conhecimento, a experiência e competência de seus desenvolvedores, a qualidade de seus processos de desenvolvimento e teste, e a capacidade de seus sistemas de TI, a fim de identificar riscos internos como falhas de comunicação entre equipes, falta de habilidades técnicas para novas tecnologias ou vulnerabilidades de segurança em seus próprios sistemas. A análise conjunta dos contextos externo e interno fornece uma base sólida para a identificação e avaliação relevantes dos riscos.

Estabelecendo Critérios de Risco para Tomada de Decisão

Uma vez definidos o escopo e o contexto, o passo seguinte é estabelecer os **critérios de risco**. Estes critérios são os parâmetros utilizados para avaliar a **significância do risco** e para **apoiar as decisões** sobre como os riscos serão tratados. A **ISO 31000** orienta que os critérios de risco devem ser **alinhados com a estrutura de gestão de riscos** e **personalizados para o propósito e escopo** da atividade em consideração. Os critérios devem refletir os **valores da organização**, seus **objetivos** e **recursos disponíveis**, e serem **consistentes com as políticas de gestão de riscos**. Ao definir critérios, a organização especifica a **quantidade e o tipo de risco** que está disposta a assumir (seu apetite ao risco) em relação aos seus objetivos. Isto envolve definir como as **consequências** (impactos positivos ou negativos) e as **probabilidades** (chance de algo acontecer) serão definidas e medidas (qualitativa ou quantitativamente), e como o **nível de risco** será determinado (geralmente uma combinação da probabilidade e da consequência).

É importante também considerar como as **combinações de múltiplos riscos** serão levadas em conta. Os critérios de risco devem ser estabelecidos levando em consideração as **obrigações da organização** (legais, contratuais, etc.) e os **pontos de vista das partes interessadas**. Por exemplo, uma empresa de alimentos pode definir critérios de risco para a segurança de seus produtos. Para riscos de contaminação bacteriana (consequência alta), a probabilidade aceitável (nível de risco) será extremamente baixa, exigindo controles muito rigorosos. Já para um risco de reclamação estética no produto (consequência baixa), a probabilidade aceitável pode ser maior.

Os critérios devem ser claros: uma consequência pode ser definida em termos de impacto financeiro (perda de receita), impacto na reputação, impacto na segurança das pessoas, impacto ambiental, etc. A probabilidade pode ser expressa em termos de frequência (uma vez por ano, uma vez a cada 10 anos) ou likelihood (rara, improvável, possível, provável, quase certa). O **nível de risco** pode ser classificado em uma matriz de risco (risco baixo, médio, alto, extremo) com base na combinação da probabilidade e da consequência, e os critérios definirão qual nível de risco é aceitável sem tratamento adicional e qual exige ação imediata. Embora estabelecidos no início, os critérios de risco pela **ISO 31000** devem ser **continuamente analisados criticamente** e ajustados conforme necessário, pois o contexto e os objetivos da organização podem mudar.

Quais métodos práticos podem ser utilizados para identificar riscos em alinhamento com a ISO 31000?

A fase de **identificação de riscos** é um dos pilares do **processo de avaliação de riscos** delineado pela **ISO 31000**. Seu propósito fundamental é encontrar, reconhecer e descrever as incertezas que podem influenciar a capacidade da organização de alcançar seus objetivos. Uma identificação eficaz depende crucialmente de informações **pertinentes**, **apropriadas** e **atualizadas**. Não se trata apenas de listar eventos negativos potenciais, mas também de reconhecer **oportunidades** que podem surgir da incerteza. A **identificação de riscos** deve ser abrangente, cobrindo todas as áreas relevantes dentro do escopo definido, e envolver as pessoas certas para

garantir que diferentes perspectivas sejam consideradas. A **ISO 31000** sugere a utilização de uma **variedade de técnicas** para realizar esta tarefa de forma eficaz.

Técnicas e Abordagens para Identificação Prática

Para identificar riscos de forma prática em alinhamento com a **ISO 31000**, as organizações podem empregar diversas técnicas. A escolha da técnica ou combinação de técnicas dependerá do escopo, do contexto, dos recursos disponíveis e da natureza dos riscos a serem identificados.

Algumas **técnicas de identificação** comuns e eficazes incluem:

1. **Brainstorming e Workshops:** Reuniões facilitadas com participantes de diversas áreas e níveis da organização para gerar uma lista abrangente de riscos potenciais. A diversidade de pensamento ajuda a cobrir diferentes ângulos.
2. **Checklists e Questionários:** Utilização de listas pré-definidas de riscos comuns em um determinado setor ou tipo de atividade, ou questionários estruturados para coletar informações sobre riscos em processos específicos. Embora úteis, exigem adaptação ao contexto para não limitar a identificação apenas a riscos conhecidos.
3. **Entrevistas Estruturadas e Semi-estruturadas:** Conversas individuais ou em grupo com pessoas-chave que possuem conhecimento profundo de processos, projetos ou áreas específicas, para extrair informações sobre riscos que podem não ser óbvios em discussões em grupo.
4. **Análise de Dados Históricos:** Revisão de incidentes passados, quase-acidentes, auditorias, reclamações de clientes, relatórios de não conformidade e outras fontes de dados internos e externos para identificar riscos que já se materializaram ou estiveram perto de se materializar.
5. **Análise SWOT (Strengths, Weaknesses, Opportunities, Threats):** Embora seja uma ferramenta estratégica mais ampla, a análise das Ameaças (Threats) e Oportunidades (Opportunities) pode ser focada para identificar riscos no

contexto da ISO 31000, ligando incertezas a fatores internos (fraquezas) e externos (ameaças e oportunidades).

6. **Julgamento de Especialistas:** Consultoria com indivíduos que possuem conhecimento técnico ou experiência significativa em uma área específica para obter insights sobre riscos potenciais.

Por exemplo, uma equipe responsável por um projeto de construção de um novo prédio comercial, ao aplicar a **ISO 31000**, poderia usar um **workshop de brainstorming** com engenheiros, arquitetos, gerentes de obra e empreiteiros para identificar riscos como atrasos na entrega de materiais, condições climáticas extremas, problemas com a mão de obra ou falhas no projeto estrutural. Simultaneamente, poderiam usar **checklists** de segurança do trabalho para identificar riscos operacionais no canteiro de obras e analisar **dados históricos** de projetos anteriores para verificar quais riscos foram mais frequentes ou impactantes no passado. A combinação dessas técnicas tende a resultar em uma lista de riscos mais completa e relevante para o projeto.

Considerando Fontes de Risco, Causas e Eventos

A **identificação de riscos** eficaz, conforme a **ISO 31000**, vai além de apenas nomear um evento adverso potencial. Ela envolve a compreensão dos elementos que compõem o risco: suas **fontes**, suas **causas** e os **eventos** que podem ocorrer, levando a **consequências** que afetam os objetivos. A norma sugere considerar uma série de fatores inter-relacionados para uma identificação abrangente, incluindo:

1. **Fontes tangíveis e intangíveis de risco:** Onde a incerteza se origina (por exemplo, um equipamento defeituoso é uma fonte tangível; uma mudança na confiança do consumidor é uma fonte intangível).

2. **Causas e eventos:** O que pode levar a um evento de risco (causa) e a ocorrência em si (evento) (por exemplo, a causa pode ser a falta de manutenção, o evento pode ser a quebra do equipamento).

3. **Ameaças e oportunidades:** Incidências que podem impedir (ameaças) ou auxiliar (oportunidades) o alcance dos objetivos.

4. **Vulnerabilidades e capacidades:** Pontos fracos (vulnerabilidades) que podem aumentar a chance ou impacto de um risco, e pontos fortes (capacidades) que podem mitigá-lo ou aproveitar oportunidades.
5. **Mudanças nos contextos externo e interno:** Novas leis, tecnologias, concorrentes (externo); mudanças na liderança, estrutura, processos (interno) que podem gerar novos riscos.
6. **Indicadores de riscos emergentes:** Sinais precoces de que um novo risco pode estar surgindo.
7. **Natureza e valor dos ativos e recursos:** Identificar o que está em risco (ativos físicos, informação, reputação, pessoas).
8. **Consequências e seus impactos nos objetivos:** Quais seriam os resultados se o risco se materializasse e como afetariam as metas.
9. **Limitações de conhecimento e de confiabilidade da informação:** Reconhecer as incertezas sobre o próprio conhecimento dos riscos.
10. **Fatores temporais:** Quando o risco pode ocorrer, sua duração e urgência.
11. **Vieses, hipóteses e crenças dos envolvidos:** Reconhecer que a percepção de risco pode ser subjetiva.

Por exemplo, uma instituição financeira ao identificar riscos de segurança da informação sob a ótica da **ISO 31000** consideraria como **fontes de risco** tanto hackers externos (intangível) quanto falhas de software (tangível); analisariam as **causas** (por exemplo, falta de treinamento de funcionários para ataques de phishing) e os **eventos** (por exemplo, acesso não autorizado a dados de clientes); considerariam a **vulnerabilidade** de seus sistemas legados e a **capacidade** de sua equipe de resposta a incidentes; olhariam para as **mudanças no contexto externo** (novos tipos de malware emergindo) e **interno** (implementação de um novo sistema sem testes adequados). Identificariam **indicadores emergentes**, como tentativas de login suspeitas frequentes e; avaliariam as **consequências** na **natureza e valor de seus ativos** (perda de dados confidenciais, danos à reputação) e o **impacto nos objetivos** (perda de confiança do cliente, multas regulatórias).

A Importância da Abordagem Sistemática e Inclusiva

A **ISO 31000** preconiza que o processo de **identificação de riscos** deve ser **sistemático**, **iterativo** e **colaborativo**. Sistemático significa seguir um plano ou metodologia definida. Iterativo implica que a identificação de riscos não é um evento único, mas um processo contínuo que se repete. Colaborativo significa envolver as **partes interessadas** relevantes. Envolver pessoas com diferentes experiências e perspectivas (operadores de linha de frente, gerentes, especialistas, clientes, fornecedores) enriquece significativamente a identificação de riscos.

Por exemplo, ao identificar riscos em uma cadeia de suprimentos, uma abordagem sistemática envolveria mapear todas as etapas do processo, desde a aquisição da matéria-prima até a entrega ao cliente final. A abordagem seria **iterativa** porque novos riscos podem surgir devido a mudanças no mercado ou em fornecedores. E seria **colaborativa** ao envolver compradores, gerentes de logística, pessoal de estoque, equipe de vendas e até mesmo fornecedores-chave e grandes clientes. Esta inclusão garante que riscos como interrupção no fornecimento de um componente crítico (perspectiva do comprador), atrasos no transporte (perspectiva da logística), ou mudanças inesperadas na demanda do cliente (perspectiva de vendas e clientes) sejam identificados. A **ISO 31000** reconhece que a **gestão de riscos** é mais eficaz quando o **conhecimento e os pontos de vista das partes interessadas** são ativamente buscados e considerados durante todo o processo, começando pela identificação.

Quais são as estratégias acionáveis para o tratamento de riscos baseadas na orientação da ISO 31000?

Após identificar, analisar e avaliar os riscos, o **processo de gestão de riscos** conforme a **ISO 31000** avança para a etapa de **tratamento de riscos**. O propósito fundamental do **tratamento de riscos** é selecionar e implementar **opções** para **abordar riscos** considerados inaceitáveis ou que a organização deseja modificar por algum motivo. A **ISO 31000** descreve o tratamento de riscos como um **processo iterativo** que envolve formular opções, planejar a implementação, avaliar a eficácia do tratamento, decidir se o **risco remanescente** é aceitável e, se necessário, realizar **tratamento adicional**. Não se trata apenas de eliminar riscos, o que nem sempre é

possível ou desejável, mas sim de modificá-los para que se tornem aceitáveis ou para aproveitar oportunidades associadas a eles.

Formulando e Selecionando Opções de Tratamento

A formulação e seleção das opções de **tratamento de riscos** é uma atividade prática que exige cuidadosa consideração. A **ISO 31000** orienta que a escolha da(s) opção(ões) mais apropriada(s) envolve **balancear os benefícios potenciais** derivados em relação ao alcance dos objetivos da organização, confrontando-os com os **custos, o esforço ou as desvantagens** da implementação. As opções para tratar o risco não são mutuamente exclusivas e podem ser usadas em combinação.

A norma **ISO 31000** lista diversas opções acionáveis para tratar riscos:

1. **Evitar o risco:** Decidir não iniciar ou descontinuar a atividade que dá origem ao risco. Esta é uma opção radical, usada quando o risco é inerentemente muito alto e não pode ser efetivamente modificado de outra forma.
2. **Assumir ou aumentar o risco:** Decidir conscientemente aceitar um risco para perseguir uma oportunidade. Isto ocorre após uma avaliação informada e alinhada ao apetite ao risco da organização.
3. **Remover a fonte de risco:** Eliminar a causa primária do risco.
4. Mudar a probabilidade: Implementar controles para reduzir a chance de o evento de risco ocorrer.
5. **Mudar as consequências:** Implementar controles para reduzir o impacto se o evento de risco ocorrer.
6. **Compartilhar o risco:** Transferir parte do risco para outra parte, por exemplo, através de contratos, seguros, parcerias ou joint ventures.
7. **Reter o risco:** Decidir por decisão fundamentada aceitar o risco remanescente após o tratamento, ou mesmo o risco original se nenhuma outra opção for viável ou justificável.

Por exemplo, uma empresa de tecnologia desenvolvendo um novo software pode identificar o risco de segurança de dados confidenciais dos usuários. Para tratar este

risco de acordo com a **ISO 31000**, a empresa poderia considerar várias opções. Poderia **mudar a probabilidade** implementando criptografia forte e firewalls para dificultar o acesso não autorizado; poderia **mudar as consequências** criando backups frequentes dos dados para permitir a recuperação rápida em caso de violação; poderia **compartilhar o risco** adquirindo um seguro cibernético que cubra parte dos custos associados a uma violação de dados; poderia **remover a fonte de risco** decidindo não coletar determinados tipos de dados sensíveis, se isso for viável para o negócio.

A decisão sobre qual opção ou combinação de opções utilizar dependerá da análise de custos versus benefícios, da eficácia esperada de cada tratamento e do alinhamento com os **critérios de risco** e o apetite ao risco estabelecido pela organização. A justificação para o tratamento vai além de apenas considerações financeiras, devendo levar em conta obrigações e os pontos de vista das **partes interessadas**.

Preparando e Implementando Planos de Tratamento

Uma vez selecionadas as opções de tratamento, a próxima etapa prática na **ISO 31000** é preparar e implementar **planos de tratamento de riscos**. O propósito destes planos é especificar detalhadamente como as opções escolhidas serão colocadas em prática, assegurando que todos os envolvidos compreendam suas responsabilidades e que o progresso possa ser monitorado.

Conforme a **ISO 31000**, um plano de tratamento deve identificar claramente a ordem em que as ações serão implementadas e ser integrado nos planos e processos de gestão da organização, em consulta com as **partes interessadas** apropriadas. As informações contidas em um plano de tratamento geralmente incluem:

1. A **justificativa** para a seleção das opções de tratamento, incluindo os **benefícios esperados**.
2. Quem é **responsável** pela aprovação e implementação do plano.
3. As **ações propostas** e a ordem de implementação.
4. Os **recursos requeridos**, incluindo contingências.

5. As **medidas de desempenho** para avaliar a eficácia do tratamento.
6. As **restrições**
7. Os requisitos de **relatos e monitoramento**.
8. Os **prazos** para a conclusão das ações.

Por exemplo, um plano de tratamento para o risco de atraso na entrega de mercadorias (mencionado anteriormente) poderia especificar as **ações propostas**: instalar sistemas de GPS em todos os veículos, treinar motoristas em rotas alternativas e estabelecer um protocolo de comunicação de emergência. A **justificativa** seria a redução dos custos associados a atrasos e a melhoria da satisfação do cliente. O plano indicaria **quem é responsável** (por exemplo, gerente de logística), os **recursos requeridos** (custo dos equipamentos GPS, horas de treinamento), as **medidas de desempenho** (redução percentual no número de entregas atrasadas), as **restrições** (orçamento limitado para novos equipamentos), e os requisitos de **relatos** (relatórios mensais sobre o desempenho das entregas). Definir **prazos** claros para a instalação dos sistemas e a conclusão do treinamento é fundamental para a implementação eficaz.

Monitoramento e Análise Crítica do Tratamento

A implementação do plano de tratamento não encerra o processo de **tratamento de riscos**. A **ISO 31000** enfatiza a necessidade de **monitoramento contínuo e análise crítica** da **eficácia** do tratamento. É possível que o tratamento implementado não produza os resultados esperados, ou até mesmo introduza novos riscos que precisem ser gerenciados. Portanto, após a implementação das ações de tratamento, é crucial **avaliar a eficácia** delas. Se o **risco remanescente** após o tratamento ainda não for aceitável de acordo com os **critérios de risco** da organização, a **ISO 31000** indica a necessidade de realizar **tratamento adicional**.

Os tomadores de decisão e as **partes interessadas** devem estar conscientes da natureza e extensão do risco que permanece mesmo após as ações de tratamento. O **monitoramento e a análise crítica** garantem que os controles e ações de tratamento permaneçam eficazes ao longo do tempo e que a organização reaja a quaisquer mudanças que possam afetar a adequação do tratamento implementado.

Como a estrutura da ISO 31000 pode ser efetivamente integrada às operações diárias de um profissional?

A **ABNT NBR ISO 31000:2018** enfatiza que a **gestão de riscos** deve ser uma **parte integrante** de todas as atividades organizacionais, e não um processo separado ou adicional. A estrutura da **ISO 31000** é projetada justamente para apoiar essa **integração** em todas as funções e níveis da organização. Para um profissional, integrar a estrutura da **ISO 31000** em suas operações diárias significa incorporar a consideração de riscos em suas rotinas, decisões e interações, tornando-a uma parte natural de como o trabalho é feito. A eficácia dessa integração depende, em grande parte, do **apoio da liderança** e do **comprometimento** em todos os níveis, conforme destacado na norma.

O Papel da Liderança e Comprometimento na Integração

A **ISO 31000** salienta a necessidade de a **alta direção** e os órgãos de supervisão demonstrarem **liderança e comprometimento** para assegurar que a **gestão de riscos** esteja integrada. Isso se traduz em ações práticas que facilitam a incorporação da gestão de riscos no dia a dia do profissional. A liderança pode, por exemplo, **emitir uma declaração ou política** que estabeleça a importância da gestão de riscos e a expectativa de que todos os funcionários a considerem em suas atividades. Podem também **assegurar que os recursos necessários sejam alocados** para a gestão de riscos e **atribuir autoridades e responsabilidades** claras. Para o profissional, isso cria um ambiente onde a consideração de riscos não é apenas permitida, mas ativamente encorajada e suportada. Por exemplo, quando um líder, ao aprovar um novo projeto, questiona explicitamente a equipe sobre os principais riscos identificados e os planos para tratá-los, ele está reforçando a expectativa de que a gestão de riscos, seguindo as diretrizes da **ISO 31000**, faz parte do processo decisório normal. Quando recursos são liberados para um treinamento em ferramentas de identificação de riscos ou para a aquisição de software de gestão de riscos, isso demonstra um comprometimento tangível com a integração da **ISO 31000**.

Integrando a Gestão de Riscos nos Processos Existentes

A integração prática da **ISO 31000** nas operações diárias significa que a **gestão de riscos** deve se tornar uma parte inerente dos **processos existentes** da organização. A norma (Seção 5.3) afirma que **gerenciar riscos** é parte, e não separado, do propósito organizacional, governança, liderança, estratégia, objetivos e operações. Na prática, isso implica em modificar os processos de tomada de decisão aplicáveis e garantir que os arranjos para gerenciar riscos sejam compreendidos e praticados (Seção 5.5). Para um profissional, isso pode significar:

1. Incorporar a **identificação de riscos** como uma etapa padrão no início de qualquer novo projeto ou iniciativa, utilizando técnicas como brainstorming ou checklists adaptados ao contexto (conforme Módulo 3). Por exemplo, um gerente de marketing, ao planejar uma nova campanha, incluiria uma reunião com a equipe para identificar riscos como feedback negativo inesperado nas redes sociais, falhas na entrega de materiais promocionais ou resposta baixa do público-alvo, antes mesmo de finalizar o plano.

2. Incluir a **análise e avaliação de riscos** como parte das revisões periódicas de desempenho ou das análises pós-projeto. Por exemplo, uma equipe de TI, após a implementação de uma nova ferramenta, revisaria os riscos de segurança e usabilidade que foram identificados e analisaria se o **nível de risco remanescente** é aceitável, documentando as lições aprendidas para projetos futuros em alinhamento com a **ISO 31000**.

3. Utilizar os **critérios de risco** estabelecidos pela organização (conforme Módulo 2) ao tomar decisões diárias. Por exemplo, um comprador, ao escolher entre dois fornecedores, consideraria não apenas o preço e o prazo, mas também os riscos associados a cada um (como histórico de confiabilidade, saúde financeira), comparando esses riscos com os critérios definidos pela organização para riscos da cadeia de suprimentos.

4. Considerar as opções de **tratamento de riscos** (conforme Módulo 5) ao desenvolver planos de ação ou ao resolver problemas operacionais. Por exemplo, um supervisor de produção, ao identificar o risco de falha de um equipamento crítico, consultaria o plano de tratamento de riscos relacionado a esse equipamento, que pode incluir ações como manutenção preventiva

reforçada (mudar a probabilidade) ou ter um fornecedor de peças sobressalentes de prontidão (mudar as consequências).

5. Incluir a **comunicação e consulta** sobre riscos com as **partes interessadas** relevantes em suas atividades diárias. Por exemplo, um gerente de vendas, ao negociar um grande contrato, consultaria as equipes jurídica e financeira para entender os riscos contratuais e de crédito associados à **ISO 31000**, e comunicaria os riscos potenciais ao cliente de forma transparente.

A integração da **ISO 31000** nas operações diárias transforma a **gestão de riscos** de uma função especializada em uma competência generalizada, onde cada profissional, dentro de sua alçada e responsabilidade, contribui para a gestão eficaz das incertezas que podem afetar o alcance dos objetivos organizacionais.

A Cultura e o Comportamento Humano na Integração

A **cultura organizacional** e o **comportamento humano** exercem uma influência significativa em todos os aspectos da **gestão de riscos**, incluindo sua integração no dia a dia. Uma cultura que valoriza a transparência, a comunicação aberta e o aprendizado com erros facilita a discussão e a gestão dos riscos. Se a cultura pune a identificação de riscos ou desencoraja a comunicação de problemas, a integração da **ISO 31000** será muito mais difícil. A **ISO 31000** reconhece explicitamente a importância dos **fatores humanos e culturais** como um de seus princípios fundamentais.

Para promover a integração através da cultura, é importante fomentar um ambiente onde os profissionais se sintam seguros para levantar preocupações de risco, discutir incertezas e propor soluções. A comunicação e a consulta (Seção 5.4.5, 6.2) desempenham um papel vital nisso, garantindo que as informações sobre riscos fluam livremente e que as opiniões das **partes interessadas** sejam consideradas. Por exemplo, se uma empresa promove "cafés de risco" informais onde funcionários de diferentes departamentos podem compartilhar preocupações sobre incertezas em seus processos, isso contribui para uma cultura que integra a **gestão de riscos** no diálogo diário. Da mesma forma, reconhecer e recompensar equipes que

proativamente identificaram e gerenciaram um risco importante reforça o comportamento desejado em linha com a **ISO 31000**.

Ferramentas e Recursos para Apoiar a Integração Diária

Para que a integração da **ISO 31000** seja prática no dia a dia, os profissionais precisam ter acesso às **ferramentas** e **recursos** apropriados. A **ISO 31000** destaca a necessidade de alocar recursos como **pessoas com as habilidades e competências** necessárias, **processos, métodos e ferramentas** para a gestão de riscos, **documentação** clara, **sistemas de informação e conhecimento** e **treinamento e desenvolvimento profissional** (Seção 5.4.4).

Na prática, isso pode significar fornecer aos profissionais acesso a um software de gestão de riscos centralizado onde podem registrar riscos identificados e planos de tratamento, ou disponibilizar modelos e guias simples para a realização de análises de risco básicas. Treinamentos práticos sobre como usar uma matriz de risco ou realizar uma análise de causa raiz capacitam os profissionais a aplicar as diretrizes da **ISO 31000** em suas tarefas. Ter acesso fácil a documentação sobre a política de gestão de riscos da organização e os critérios de risco estabelecidos ajuda os profissionais a tomar decisões alinhadas com a abordagem da **ISO 31000**. Por exemplo, um engenheiro de projetos que recebe treinamento sobre a ferramenta de análise de risco da empresa e tem acesso a uma base de dados de lições aprendidas de projetos anteriores está mais bem equipado para identificar e gerenciar riscos em seu próprio projeto, integrando assim a **ISO 31000** em sua rotina de trabalho.

Perceba que a disponibilidade e a facilidade de uso desses recursos são essenciais para tornar a **gestão de riscos** uma parte fluida e eficaz das operações diárias.

Como implementar atividades práticas de monitoramento, análise crítica, registro e comunicação dentro de um sistema baseado na ISO 31000?

As etapas finais do **processo de gestão de riscos** conforme a **ISO 31000** são o **monitoramento**, a **análise crítica**, o **registro** e o **relato**. Embora frequentemente apresentadas no final do ciclo do processo, essas atividades são contínuas e cruciais para garantir que a **gestão de riscos** permaneça eficaz, relevante e que as

informações sobre riscos estejam disponíveis para apoiar a tomada de decisão em todos os níveis da organização. A implementação prática dessas atividades é essencial para a melhoria contínua do sistema de gestão de riscos.

Monitoramento Contínuo e Análise Crítica Periódica

O **monitoramento** e a **análise crítica** são atividades gêmeas cujo propósito é assegurar e melhorar a **qualidade e eficácia** da concepção, implementação e resultados do processo de **gestão de riscos**. A **ISO 31000** especifica que o **monitoramento contínuo** e a **análise crítica periódica** devem ser uma **parte planejada** do processo de gestão de riscos, com **responsabilidades claramente estabelecidas** (Seção 6.6). O monitoramento acompanha a **eficácia** dos controles e tratamentos de riscos implementados, bem como a identificação de novos riscos que possam surgir devido a mudanças nos contextos interno ou externo. A análise crítica, por sua vez, avalia a adequação do próprio processo de gestão de riscos e da estrutura que o suporta.

Essas atividades ocorrem em **todos os estágios do processo de gestão de riscos**, desde a definição do escopo até o tratamento de riscos. Na prática, o monitoramento pode envolver a coleta regular de dados de desempenho, como o número de incidentes reportados relacionados a um risco específico, o tempo de resposta a eventos de risco ou a conclusão de ações de tratamento planejadas. A análise crítica pode ser realizada através de reuniões periódicas da equipe de gestão de riscos, auditorias internas ou revisões pela alta direção. Por exemplo, uma empresa de manufatura que identificou o risco de falha de equipamento crítico e implementou um plano de manutenção preventiva (tratamento) monitoraria continuamente a frequência de falhas, os resultados das inspeções de manutenção e os custos associados à manutenção. A cada seis meses, a equipe de gestão de riscos realizaria uma **análise crítica** para avaliar se o plano de manutenção está sendo eficaz na redução das falhas, se o **risco remanescente** é aceitável e se o processo de identificação e tratamento de riscos para equipamentos precisa ser ajustado com base nas lições aprendidas. A **ISO 31000** ressalta que os resultados do monitoramento e análise crítica devem ser incorporados nas atividades de gestão de desempenho da organização.

Registro: Documentando o Processo e Resultados

O **registro** na **gestão de riscos** refere-se à **documentação** sistemática do processo e de seus resultados. A **ISO 31000** (Seção 6.7) estabelece que o processo de gestão de riscos e seus resultados devem ser documentados através de mecanismos apropriados. O **registro** serve a múltiplos propósitos práticos:

1. **Comunicar** as atividades de gestão de riscos e seus resultados em toda a organização.
2. Fornecer **informações para a tomada de decisão**, tanto para decisões relacionadas a riscos quanto para outras decisões estratégicas e operacionais.
3. **Melhorar as atividades de gestão de riscos** ao longo do tempo, fornecendo uma base para aprendizado e ajuste.
4. Auxiliar a **interação com as partes interessadas**, fornecendo um registro transparente do processo.

Na prática, o **registro** envolve a criação e manutenção de diversos tipos de documentos. Por exemplo, um **registro de riscos** centralizado é um documento comum onde os riscos identificados são detalhados, incluindo sua descrição, fontes, causas, consequências, **nível de risco** avaliado e os tratamentos planejados ou implementados. Outros registros importantes podem incluir **relatórios de incidentes** relacionados a riscos, **planos de tratamento de riscos** detalhados, **atas de reuniões** de análise crítica de riscos, e **registros de comunicação e consulta** com as **partes interessadas**. A **ISO 31000** sugere que as decisões sobre a criação, retenção e manuseio da informação documentada levem em consideração seu uso, a sensibilidade da informação e os contextos externo e interno. Manter registros precisos e acessíveis é fundamental para a rastreabilidade do processo de **gestão de riscos** e para demonstrar conformidade com as diretrizes da **ISO 31000**.

Relato: Comunicando Informações de Risco

O **relato** na **gestão de riscos** diz respeito à comunicação das informações de risco para as diferentes **partes interessadas**. Conforme a **ISO 31000** (Seção 6.7), o **relato**

tem como objetivo principal **comunicar atividades e resultados de gestão de riscos** e fornecer **informações para a tomada de decisão**. É uma parte integrante da **governança** e apoia a **alta direção** e os órgãos de supervisão a cumprirem suas responsabilidades.

Ao planejar o **relato**, é essencial considerar as **diferentes partes interessadas** e suas necessidades específicas de informação. O que é relevante para a alta direção pode ser diferente do que é relevante para um gerente de projeto ou para um funcionário da linha de frente. Outros fatores a considerar incluem o **custo**, a **frequência** e a **pontualidade** do relato, o **método de relato** (relatórios escritos, apresentações, dashboards interativos) e a **pertinência da informação** para os objetivos organizacionais e para a tomada de decisão.

Na prática, um sistema baseado na **ISO 31000** envolveria diferentes tipos de relatos. Por exemplo, a equipe de **gestão de riscos** pode preparar um **relatório de riscos operacionais** semanal para os gerentes de departamento, destacando novos riscos identificados em suas áreas e o status das ações de tratamento. Para a alta direção, poderia ser preparado um **sumário executivo** mensal dos riscos estratégicos mais significativos, incluindo a **avaliação de riscos** atualizada e os planos de tratamento de alto nível. Um gerente de projeto prepararia **relatórios de riscos de projeto** regulares para a equipe do projeto e para a gerência, detalhando os riscos que podem afetar o cronograma e o orçamento. O **relato** não se limita à comunicação interna; informações sobre riscos relevantes podem precisar ser comunicadas a **partes interessadas** externas, como reguladores, investidores ou a comunidade, dependendo do contexto e das obrigações. O **relato** eficaz, alinhado com a **ISO 31000**, melhora a qualidade do diálogo sobre riscos e contribui para uma cultura de gestão de riscos mais transparente e responsável. Monitoramento, análise crítica, registro e relato, quando bem implementados, fecham o ciclo do **processo de gestão de riscos**, fornecendo o feedback necessário para a melhoria contínua e assegurando que a **ISO 31000** seja uma ferramenta viva e útil na organização.

Quais são as mudanças visíveis dos resultados da ISO 31000 para a empresa?

Encontrar descrições detalhadas das mudanças no dia a dia de cada profissional em empresas que utilizam a **ISO 31000** de forma aberta pode ser um desafio, visto que

muitas divulgações tendem a focar nos benefícios estratégicos e de alto nível da implementação. No entanto, a própria natureza da **ISO 31000**, que preconiza a **integração da gestão de riscos** nas atividades e processos da organização, implica em transformações concretas na forma como o trabalho é realizado no cotidiano. A norma busca incorporar o "pensamento baseado em risco" nas rotinas, tornando a consideração da **incerteza** algo natural e intrínseco às tarefas.

Ao alinhar suas práticas à **ISO 31000**, empresas como a **Tata Power** relataram que a **gestão de riscos corporativos** foi incorporada ao que chamaram de "DNA" da companhia, promovendo uma cultura onde os funcionários agem como guardiões do valor corporativo. Isso se traduz, no dia a dia, em uma maior **conscientização** sobre os riscos associados às suas atividades individuais. Por exemplo, um engenheiro na Tata Power, ao projetar uma nova subestação, não apenas seguiria os códigos técnicos, mas seria proativo em identificar potenciais falhas que poderiam levar a interrupções no fornecimento de energia (um risco operacional), discutindo ativamente com a equipe de manutenção (comunicação e consulta, princípios da **ISO 31000**) para entender as causas mais comuns de falhas em equipamentos existentes e incorporando medidas preventivas no projeto. A gestão de riscos deixa de ser responsabilidade exclusiva de um departamento e passa a ser vista como parte da responsabilidade de cada um na proteção e criação de valor.

Em empresas do setor **Fintech na Indonésia** que utilizam a **ISO 31000**, a melhoria na qualidade dos **relatórios financeiros** tem um impacto direto no cotidiano das equipes de finanças e contabilidade. Profissionais dessas áreas provavelmente passaram a incorporar, em suas rotinas de fechamento mensal e preparação de relatórios, a análise dos riscos financeiros identificados (como risco de crédito ou risco de liquidez), assegurando que as informações reportadas reflitam não apenas os números brutos, mas também as incertezas associadas a eles. Isso envolve, por exemplo, a revisão mais criteriosa das provisões para perdas com base em critérios de risco estabelecidos pela **ISO 31000**, ou a inclusão de notas explicativas nos relatórios que detalham os riscos financeiros relevantes e as ações de tratamento em andamento. Essa atenção aos riscos na própria base da informação financeira leva a relatórios mais precisos e confiáveis.

A melhoria na **saúde ocupacional e segurança** reportada por algumas empresas que adotam a **ISO 31000** impacta diretamente o dia a dia dos trabalhadores em ambientes

operacionais. A implementação prática da **ISO 31000** nesse contexto envolve, por exemplo, a inclusão da **identificação de riscos** de segurança como parte das inspeções rotineiras no local de trabalho. Um supervisor de linha de produção, alinhado com os princípios da norma, passaria a olhar para as atividades diárias não apenas em termos de eficiência, mas também identificando proativamente condições inseguras ou práticas de trabalho arriscadas (identificação de riscos). As equipes de segurança, por sua vez, utilizariam os resultados dessas identificações e a **análise de riscos** (considerando a probabilidade de acidentes e a gravidade das consequências) para desenvolver procedimentos de trabalho mais seguros ou implementar controles de engenharia (tratamento de riscos), o que muda a forma como as tarefas são executadas no chão de fábrica.

Além disso, a ênfase da **ISO 31000** na **comunicação e consulta** com as **partes interessadas** significa que, no dia a dia, os profissionais são mais frequentemente envolvidos em discussões sobre riscos relacionados ao seu trabalho. Isso pode ocorrer em reuniões de equipe, em canais de feedback específicos ou durante o planejamento de atividades. Um gerente de projeto, por exemplo, não apenas criaria o cronograma e o orçamento, mas dedicaria tempo, seguindo as diretrizes da **ISO 31000**, para realizar **workshops** com a equipe do projeto e outros stakeholders (como fornecedores ou clientes) para identificar riscos potenciais que poderiam impactar o sucesso do projeto, mudando a rotina de planejamento para incluir ativamente essa colaboração focada em riscos.

Em suma, a adoção da **ISO 31000** move a **gestão de riscos** de uma função de *compliance* ou especialista para uma responsabilidade compartilhada, integrada aos processos e à cultura. Isso se reflete no dia a dia dos profissionais através de uma maior **consciência sobre incertezas**, a inclusão da consideração de riscos nas **tomadas de decisão rotineiras**, a participação em **discussões e análises de risco**, a contribuição para a **identificação proativa** de problemas e oportunidades, e a utilização de **informações sobre riscos** (registros e relatos) para guiar suas ações. É essa incorporação nas atividades cotidianas que transforma a **ISO 31000** de um documento em uma ferramenta viva para melhorar o desempenho e proteger o valor organizacional.