

Template: Matriz de Riscos ISO

Modelo completo para mapeamento, avaliação e tratamento de riscos

Este template é baseado na metodologia ISO 31000:2018 (Gestão de Riscos) e é compatível com os requisitos de gestão de riscos das normas ISO 9001, ISO 14001 e ISO 27001. Use-o para identificar, avaliar, tratar e monitorar os riscos dos seus processos organizacionais.

Como Usar Esta Matriz de Riscos

Siga os passos abaixo para preencher a matriz com eficácia. Envolve os responsáveis de cada processo.

- PASSO 1 — Defina o escopo: quais processos, atividades ou projetos serão analisados
- PASSO 2 — Monte uma equipe multidisciplinar: inclua gestores de processo e especialistas técnicos
- PASSO 3 — Para cada processo, liste os eventos de risco (o que pode dar errado?)
- PASSO 4 — Para cada risco, descreva a causa raiz provável e as consequências potenciais
- PASSO 5 — Avalie a PROBABILIDADE de ocorrência: escala de 1 (muito baixa) a 5 (quase certa)
- PASSO 6 — Avalie o IMPACTO caso o risco se materialize: escala de 1 (insignificante) a 5 (catastrófico)
- PASSO 7 — Calcule o NÍVEL DE RISCO: Probabilidade x Impacto (resultado de 1 a 25)
- PASSO 8 — Defina o tratamento: Mitigar / Aceitar / Transferir (seguro) / Evitar (eliminar atividade)
- PASSO 9 — Para riscos que serão mitigados, defina ação específica, responsável e prazo
- PASSO 10 — Monitore mensalmente o status das ações e reavalie os níveis de risco trimestralmente

Escala de Probabilidade e Impacto

Utilize estas definições para garantir consistência nas avaliações entre diferentes equipes.

- PROBABILIDADE 1 — Muito Baixa: evento pode ocorrer em circunstâncias excepcionais (menos de 1x em 5 anos)
- PROBABILIDADE 2 — Baixa: evento pode ocorrer em algum momento (1x em 2 a 5 anos)
- PROBABILIDADE 3 — Média: evento provavelmente ocorrerá em algum momento (1x por ano)
- PROBABILIDADE 4 — Alta: evento provavelmente ocorrerá com frequência (mais de 1x por ano)
- PROBABILIDADE 5 — Quase Certa: evento é esperado para ocorrer na maioria das circunstâncias (mensal)
- IMPACTO 1 — Insignificante: sem impacto significativo nas operações, financeiro ou reputacional
- IMPACTO 2 — Menor: impacto pequeno, facilmente gerenciado com recursos normais
- IMPACTO 3 — Moderado: impacto significativo mas gerenciável; requer atenção da gestão
- IMPACTO 4 — Grave: impacto severo nas operações, financeiro alto ou dano reputacional significativo
- IMPACTO 5 — Catastrófico: impacto que pode comprometer a continuidade do negócio ou causar dano irreversível

Níveis de Risco e Critérios de Resposta

Com base no resultado de *Probabilidade x Impacto*, adote a resposta adequada ao nível de risco.

- NÍVEL 1-4: BAIXO (verde) — Risco aceitável; monitorar periodicamente (revisão semestral)
- NÍVEL 5-9: MÉDIO (amarelo) — Requer atenção; implementar controles preventivos (revisão trimestral)
- NÍVEL 10-16: ALTO (laranja) — Ação prioritária; plano de mitigação com prazo máximo de 90 dias
- NÍVEL 17-25: CRÍTICO (vermelho) — Ação imediata; escalar para alta direção; prazo máximo 30 dias
- REGRA GERAL — Qualquer risco com impacto 5 (catastrófico) deve ser tratado independentemente da probabilidade
- REGRA GERAL — Riscos legais/regulatórios devem ser tratados como ALTO independentemente do cálculo
- APETITE DE RISCO — Defina com a direção o nível máximo de risco que a organização está disposta a aceitar

Campos da Matriz — Guia de Preenchimento

Descrição detalhada de cada campo da planilha de riscos para garantir preenchimento correto.

- ID: código único (ex: R-OPE-001 = Risco, área Operacional, sequencial 001)
- Processo / Área: nome do processo ou departamento onde o risco existe
- Categoria: Operacional / Estratégico / Financeiro / Legal-Regulatório / Tecnológico / Ambiental / RH
- Descrição do Risco: descreva o evento de risco no formato "risco de [evento] causado por [causa]"
- Causa Raiz: origem principal do risco (falha de processo, falta de recurso, fator externo)
- Consequência: impacto potencial se o risco se materializar (financeiro, operacional, legal, reputacional)
- Controles Existentes: ações/processos já em vigor para reduzir probabilidade ou impacto
- Probabilidade (P): valor de 1 a 5 conforme escala definida
- Impacto (I): valor de 1 a 5 conforme escala definida
- Nível Bruto (P x I): risco sem considerar os controles existentes
- Nível Residual: nível após aplicação dos controles existentes
- Tratamento: Mitigar / Aceitar / Transferir / Evitar
- Ação de Mitigação: ação específica e mensurável para reduzir o risco
- Responsável: nome e cargo da pessoa responsável pela implementação da ação
- Prazo: data limite para implementação da ação de mitigação
- Status: A Fazer / Em Andamento / Concluído / Monitorando

Exemplos Práticos de Riscos por Categoria

Use estes exemplos como ponto de partida para identificar riscos na sua organização.

- OPERACIONAL — Risco de parada de produção por falha de equipamento crítico sem manutenção preventiva (P:3 / I:4 = 12 ALTO)
- OPERACIONAL — Risco de erro no produto por falta de instrução de trabalho atualizada (P:4 / I:3 = 12 ALTO)
- TECNOLÓGICO — Risco de perda de dados por falha de backup sem procedimento de recuperação testado (P:2 / I:5 = 10 ALTO)
- TECNOLÓGICO — Risco de indisponibilidade de sistema crítico por ataque cibernético (P:3 / I:4 = 12 ALTO)
- LEGAL — Risco de multa regulatória por descumprimento de licença ambiental (P:2 / I:4 = 8 MÉDIO)
- RH — Risco de perda de conhecimento crítico por saída de colaborador-chave sem sucessão (P:3 / I:3 = 9 MÉDIO)
- ESTRATÉGICO — Risco de perda de cliente principal por dependência excessiva de fornecedor único (P:2 / I:5 = 10 ALTO)
- FINANCEIRO — Risco de inadimplência por concentração de receita em poucos clientes (P:3 / I:4 = 12 ALTO)