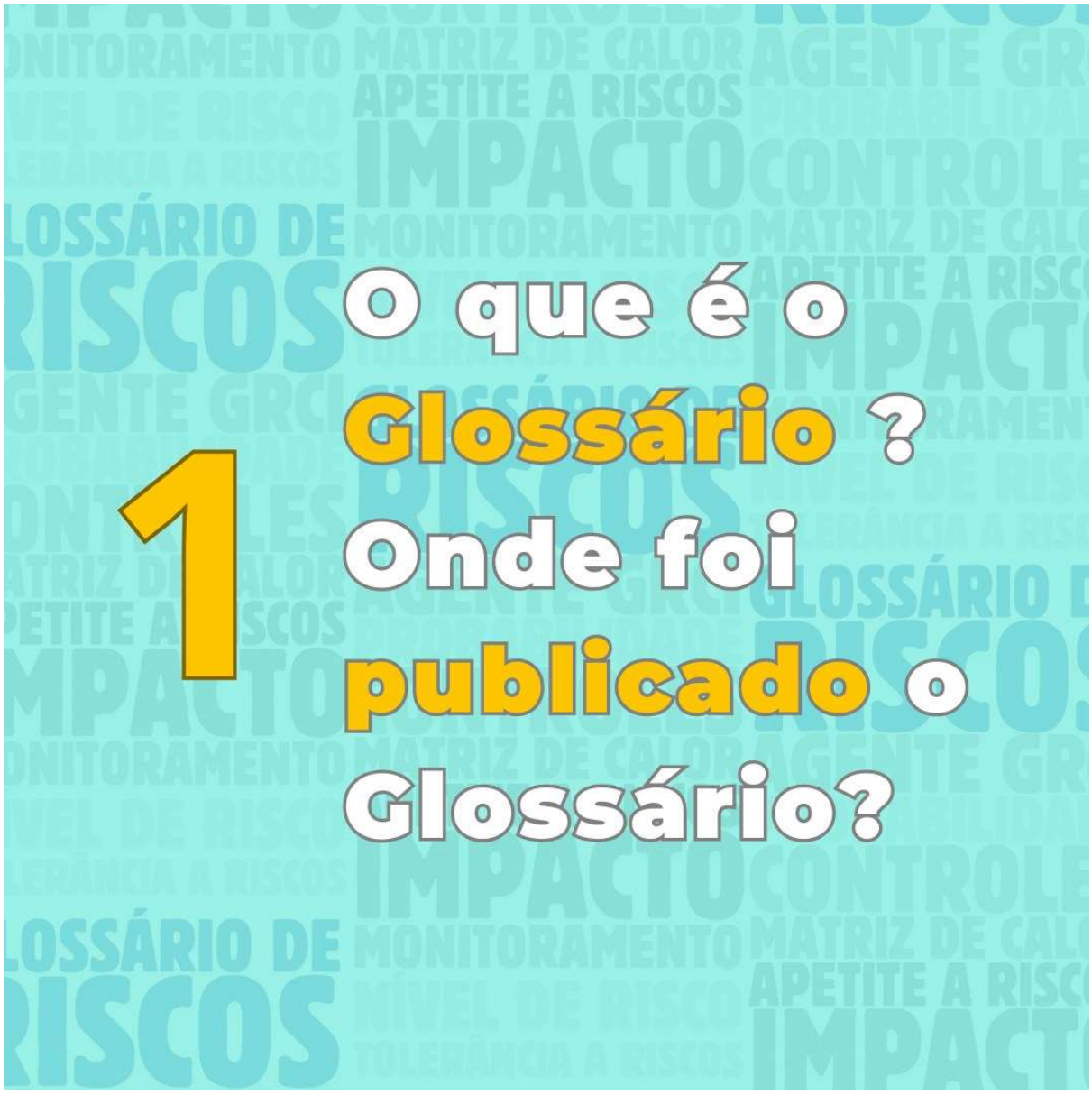
Glossário de Gestão de Riscos e Controles do SERPRO

Sobre o RiskHub

É um espaço que promove a **conexão** de um **tema** aos **conceitos da** Gestão de Riscos. Nesta edição abordaremos: **Glossário de Gestão de Riscos e Controles do SERPRO**

- O que é **Glossário**? Onde foi **publicado** o Glossário?
- Os **verbetes do Glossário** da Gestão de Riscos e Controles no SERPRO
- **Saiba mais...**

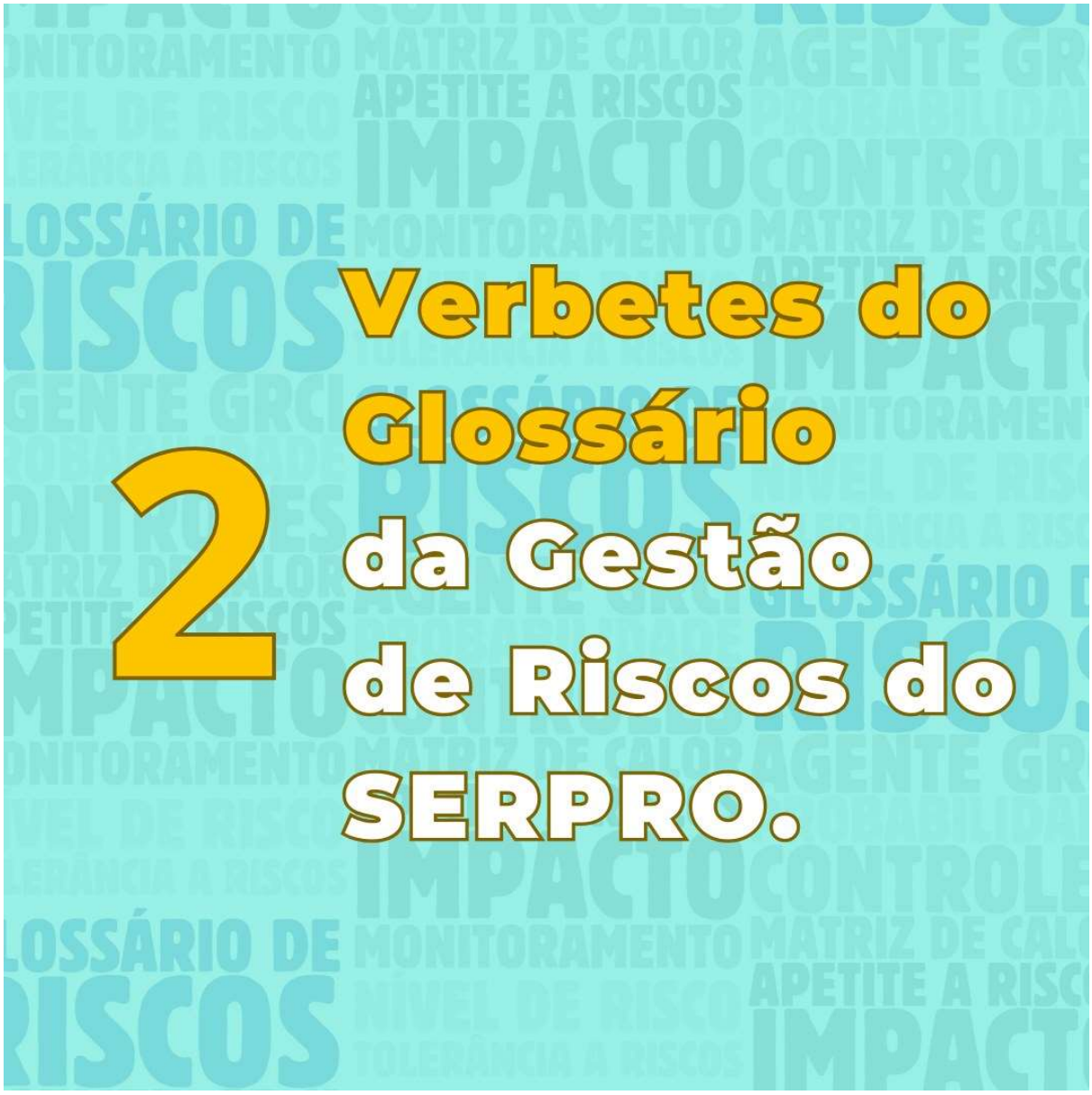


- O que é **Glossário**?

Este Glossário é a reunião dos principais verbetes relacionados à Gestão de Riscos e Controles do SERPRO. Ele fornece uma **explicação concisa e clara dos termos** que constam na Metodologia, possibilitando aos leitores compreenderem o seu **significado e contexto** em que são empregues.

- Onde foi **publicado** o Glossário?

Este material foi compilado e **é parte integrante** da versão vigente da Metodologia de Gestão de Riscos e Controles (GR-007/2025) *(Nas páginas: **04 até 11** da Metodologia. E ainda, nas **imagens dos verbetes compilados neste material**)*


2
Verbetes do Glossário da Gestão de Riscos do SERPRO.

Ameaças:

Ver : Riscos Negativos

Aceitar Risco:

Decisão de não tomar nenhuma ação específica para alterar a probabilidade ou o impacto de um risco identificado. É aplicável quando o risco está dentro dos limites aceitáveis de apetite a risco da organização ou quando o custo ou o esforço para tratar o risco supera os benefícios esperados, com as devidas justificativas. No caso de riscos positivos, aceitar o risco significa estar disposto a aproveitar as oportunidades que ele pode trazer.

Ver também: Respostas a riscos.

Agentes de Riscos e Controles:

Empregados indicados em cada unidade organizacional para atuar como facilitadores na aplicação da metodologia de gestão de riscos e controles internos, apoiando gestores e disseminando práticas de gerenciamento de riscos.

Equivalente a: Agentes GRCI.

Agentes GRCI:

Ver : Agentes de Risco
de Risco e Controles

Análise Crítica:

Processo contínuo de revisão e ajuste da Gestão de Riscos e Controles para assegurar que estejam alinhados com os objetivos estratégicos e operacionais da organização. Inclui a validação dos resultados das etapas anteriores e a avaliação da eficácia, presença e funcionamento dos controles.

Apetite a Riscos:

Nível de risco que uma organização está disposta a aceitar para atingir seus objetivos estratégicos e operacionais. O apetite a riscos é estabelecido com base nos objetivos, valores e cultura organizacional e pode variar conforme o tipo de risco (negativo ou positivo).

Aprovadores de Riscos:

São responsáveis pela aprovação formal dos riscos mapeados nas unidades organizacionais, bem como pelo cancelamento desses riscos quando solicitado. Geralmente, essa função é desempenhada por diretores, superintendentes ou gerentes designados, que possuem a autoridade para deliberar sobre o tratamento dos riscos.

Controle Contingencial:

Medida ou plano previamente desenvolvido para ser acionado em resposta à materialização de um risco, tanto negativo quanto positivo. Para riscos negativos (ameaças), o controle contingencial visa mitigar os danos e minimizar os impactos adversos, garantindo que a organização tenha uma resposta preparada para situações emergenciais. Já para riscos positivos (oportunidades), o controle contingencial é utilizado para garantir que a organização maximize os benefícios e consiga capitalizar sobre a oportunidade de maneira eficaz, caso ela se concretize.

Controle Preventivo:

Medida ou ação tomada de forma proativa para reduzir a probabilidade de ocorrência de eventos de risco e seus impactos, tanto negativos quanto positivos. No caso de riscos negativos, os controles preventivos são usados para evitar ou mitigar danos ou perdas. Já para riscos positivos (oportunidades), os controles preventivos buscam aumentar a probabilidade de que os eventos benéficos ocorram ou maximizem seus impactos favoráveis, assegurando que a organização esteja preparada para aproveitar essas oportunidades.

Controles:

Processos, políticas e procedimentos implementados para tratar riscos. Os controles podem ser preventivos (para evitar a ocorrência de riscos negativos) ou fortalecer a probabilidade de ocorrência de riscos positivos); ou contingenciais (para reduzir o impacto de riscos que se concretizam ou reforçar riscos positivos materializados). Exemplos incluem planos de contingência, treinamentos e políticas de conformidade.

Controles Internos:

Ver : Controles

Criticidade do Risco:

É uma medida que combina impacto e probabilidade para avaliar o potencial de um risco em afetar os objetivos estratégicos. Esse conceito permite priorizar riscos e estruturar respostas de maneira proporcional, apoiando a organização a gerenciar seus riscos de forma mais eficaz e alinhada com sua estratégia. A criticidade do risco é essencial para a priorização e alocação de recursos na gestão de riscos.

Equivalente a: Gravidade do risco.

Declaração de Apetite a Riscos (RAS):

Documento que formaliza os níveis de risco que a organização está disposta a aceitar no cumprimento de seus objetivos e metas.
A RAS (Risk Appetite Statement) é utilizada como referência para decisões estratégicas e é revisada periodicamente para refletir mudanças no ambiente interno e externo.

Equivalente a: RAS.

Evento:

Ocorrência ou situação que pode influenciar os objetivos de uma organização, resultando em impactos positivos ou negativos.
Os eventos podem ser previstos ou inesperados, e seu efeito dependerá de como são geridos no contexto organizacional.

Evitar Risco:

Ação de eliminar a possibilidade de ocorrência de um risco, alterando planos ou objetivos que possam ser impactados por esse risco.
Para riscos negativos, isso significa evitar atividades que possam resultar em prejuízos. Para riscos positivos, evitar o risco pode significar abdicar de oportunidades que, apesar de promissoras, estão fora do apetite a risco da organização.

Ver também: Respostas a riscos.


GLOSSÁRIO DE RISCOS
G

Gerenciamento de Riscos:

Abrange a governança, cultura e práticas organizacionais para assegurar que os riscos sejam identificados, avaliados e tratados de maneira alinhada aos objetivos.

Gestão de Crises:

Conjunto de ações coordenadas destinadas a responder de forma estruturada e eficiente a eventos críticos que impactem significativamente os objetivos organizacionais.
A gestão de crises envolve o planejamento e a execução de medidas preventivas, de mitigação e de recuperação, frequentemente articuladas com os Planos de Continuidade de Negócios e a gestão de riscos, para proteger ativos, preservar a reputação e assegurar a retomada das operações.

Gestão de Riscos:

Conjunto de atividades coordenadas, envolvendo princípios, estrutura organizacional, processos estruturados e ferramentas aplicáveis, para identificar, analisar, avaliar, tratar, monitorar e comunicar riscos, abrangendo tanto ameaças quanto oportunidades.
Essa abordagem visa assegurar a integridade, a continuidade dos negócios e o alcance dos objetivos organizacionais, integrando a gestão de riscos em todos os níveis e decisões da organização.

Gestor de Riscos:

Profissional responsável por supervisionar os riscos em uma unidade organizacional específica, assegurando que sejam gerenciados conforme as políticas internas.
Suas responsabilidades incluem monitorar frequentemente os riscos, coordenar ações para tratá-los e comunicar informações relevantes sobre os riscos a todos os níveis da organização.

Gravidade do Risco:

Ver Criticidade do risco.

Identificação de Riscos:

Processo sistemático de busca, reconhecimento e descrição de riscos que podem afetar os objetivos organizacionais.
Envolve a análise de fontes de risco, eventos, suas causas e consequências potenciais, considerando o contexto interno e externo da organização.
Este processo pode incluir a utilização de dados históricos, análises teóricas, opiniões de especialistas e necessidades das partes interessadas, conforme descrito na ISO 31000:2018.

Indicador Chave de Desempenho (KPI):

Métrica utilizada para monitorar e avaliar o desempenho de ações, processos ou atividades específicas em relação a metas estabelecidas.
KPIs ajudam a medir a eficiência e a eficácia de esforços realizados, destacando áreas que precisam de melhorias e suportando a tomada de decisões estratégicas e operacionais.
Eles diferem de indicadores de resultado, pois focam em métricas intermediárias ou operacionais diretamente relacionadas à execução.

Equivalente a: KPI

Indicador Chave de Objetivo (KPO):

Métrica que mede o progresso em direção a um objetivo específico dentro de uma organização.
Diferente dos KPIs, que se concentram no desempenho contínuo e operacional, os KPOs são focados em resultados estratégicos de longo prazo, fornecendo uma visão clara sobre o quão perto a organização está de alcançar seus objetivos principais.

Equivalente a: KPO

Indicador Chave de Risco (KRI):

Métrica usada para monitorar sinais de que um risco pode se materializar, ajudando a prever e mitigar eventos adversos que podem impactar negativamente os objetivos da organização.
KRIs oferecem alertas precoces sobre mudanças no perfil de risco, permitindo ações preventivas.

Equivalente a: KRI

Índices de Risco:

Medidas quantitativas atribuídas aos riscos para representar sua probabilidade e impacto.
Os índices de risco são utilizados para criar matrizes de risco que ajudam a priorizar as ações de mitigação e o tratamento dos riscos.
Seus valores vão de 1 a 25 na matriz de riscos.


KPI:
Ver Indicador Chave de Desempenho (KPI)


KPO:
Ver Indicador Chave de Objetivo (KPO)


KRI:
Ver Indicador Chave de Risco (KRI)

Materialização de Risco:

Processo pelo qual um risco previamente identificado deixa de ser apenas uma possibilidade e se torna um evento concreto, gerando impactos tangíveis na organização.

Quando o risco se materializa, ele pode resultar em consequências negativas (perdas financeiras, interrupções operacionais, etc.) ou, em alguns casos, positivas (oportunidades ou ganhos).

A materialização de um risco exige que as medidas de resposta ao risco previamente planejadas sejam executadas.

Ver também: Risco materializado

Matriz de Calor:

Ver Matriz de riscos

Matriz de Riscos:

Ferramenta visual utilizada para avaliar e priorizar riscos com base em duas dimensões principais: a probabilidade de um evento ocorrer e o impacto que esse evento terá se ocorrer.
A matriz é frequentemente organizada em uma grade onde a probabilidade é representada em um eixo e o impacto no outro, permitindo categorizar os riscos em diferentes níveis (muito baixo, baixo, médio, alto, muito alto).
Essa matriz auxilia na tomada de decisões sobre como gerenciar e tratar os riscos identificados.

Equivalente a: Matriz de Calor

Medidas de Contingência:

Ações previamente planejadas que devem ser executadas caso um ou mais riscos se concretizem.

Ver também: Controle contingencial

Modelo das Três Linhas:

Estrutura de governança utilizada para dividir responsabilidades na Gestão de Riscos e Controles.
A Primeira Linha é composta pelas unidades operacionais que identificam e gerenciam riscos diretamente; a Segunda Linha é formada por funções de supervisão (como gestão de riscos e conformidade) que monitoram e apoiam a Primeira Linha; e a Terceira Linha é representada pela Auditoria Interna, que avalia de forma independente a eficácia dos controles e do gerenciamento de riscos.

Monitoramento:

Processo contínuo de acompanhamento e revisão dos riscos e controles para assegurar a eficácia das respostas implementadas e identificar mudanças no ambiente ou nos riscos.

Nível de Risco:

Determinado pela combinação da probabilidade de ocorrência de um evento de risco e o impacto potencial que esse evento pode ter sobre os objetivos da organização.
O nível de risco é utilizado para categorizar riscos como baixo, médio, alto, etc.

Equivalente a: NR


NR:
Ver Nível de Risco


GLOSSÁRIO DE RISCOS
MATRIZ DE CALOR
APETITE A RISCOS
IMPACTO
CONTROLES
MONITORAMENTO
AGENTE GRC
NÍVEL DE RISCO
TOLERÂNCIA A RISCOS

Objetivos:

Resultados específicos que uma organização pretende alcançar, servindo como referência para a identificação e avaliação dos riscos.
Na gestão de riscos, os objetivos podem ser estratégicos, operacionais ou de conformidade, e devem ser claros e mensuráveis para facilitar a análise de riscos.
Qualquer desvio em relação ao esperado pode representar um risco que precisa ser gerido.

Objetivos de Desenvolvimento Sustentável (ODS):

Conjunto de metas globais da ONU para promover o desenvolvimento sustentável, abrangendo áreas como erradicação da pobreza, igualdade, proteção ambiental e prosperidade até 2030.

Objetivos Estratégicos:

Metas de longo prazo que orientam uma organização em direção à sua visão, estabelecendo prioridades e direcionando recursos para alcançar vantagens competitivas e cumprir sua missão.

ODS:

Ver Objetivos de Desenvolvimento Sustentável (ODS)

Oportunidades:

Ver Riscos Positivos

Parte Interessada:

Pessoa ou organização que pode afetar, ser afetada, ou perceber-se afetada por uma decisão ou atividade da organização (ABNT, 2009).

Equivalente a: Stakeholder

PCN:

Ver Plano de Continuidade de Negócios (PCN)

Plano de Contingência:

Conjunto de ações específicas e imediatas para responder a eventos de interrupção pontuais, mitigando impactos enquanto as condições normais não são restabelecidas.
É um componente operacional dentro do escopo do PCN.

Plano de Continuidade de Negócios (PCN):

Documento estratégico que descreve as estratégias, ações e recursos necessários para assegurar a continuidade das operações críticas da organização em situações de interrupção ou crise, integrando-se ao processo de gestão de riscos.

Equivalente a: PCN

Plano de Continuidade de Negócios (PCN):

Documento estratégico que descreve as estratégias, ações e recursos necessários para assegurar a continuidade das operações críticas da organização em situações de interrupção ou crise, integrando-se ao processo de gestão de riscos.

Equivalente a: PCN

Plano de Gestão de Riscos:

Ver Plano de Gestão de Riscos e Controles

Plano de Gestão de Riscos e Controles:

Documento elaborado pela área de Gestão de Riscos e Controles que estabelece as metas e descreve como o gerenciamento de Riscos e Controles será conduzido, executado e monitorado dentro da organização. Este plano é atualizado anualmente e submetido para aprovação da alta administração.

Equivalente a: Plano de Gestão de Riscos

Política de Gestão de Riscos:

Documento que contém a declaração das intenções e diretrizes gerais relacionadas à gestão de riscos e estabelece claramente os objetivos e o comprometimento da organização em relação à gestão de riscos.
Não se trata de uma declaração de propósitos genérica, mas de um documento que, além de declarar os princípios, explica porque a gestão de riscos é adotada, o que se pretende com ela, onde, como e quando ela é aplicada, quem são os responsáveis em todos os níveis, dentre outros aspectos (ABNT, 2009).

Princípios da Gestão de Riscos:

Diretrizes fundamentais que orientam e direcionam as ações de gestão de riscos para alcançar os objetivos organizacionais. Segundo a ISO 31000:2018, os principais princípios incluem: integração, estrutura e abrangência, personalização, inclusão, dinamismo, melhor informação disponível, fatores humanos e culturais, e melhoria contínua.
Esses princípios servem como guias para a tomada de decisão, ajudando a alinhar as práticas de gestão de riscos com a estratégia organizacional, garantindo que a gestão de riscos contribua para a criação e proteção de valor.

Processo:

Conjunto de atividades inter-relacionadas ou interativas que transformam insumos (entradas) em produtos/serviços (saídas) com valor agregado. Processos são geralmente planejados e realizados de maneira contínua para agregar valor na geração de produtos e serviços.
Processos podem ser agrupados em macroprocessos e subdivididos em subprocessos (BRASIL, 2011).

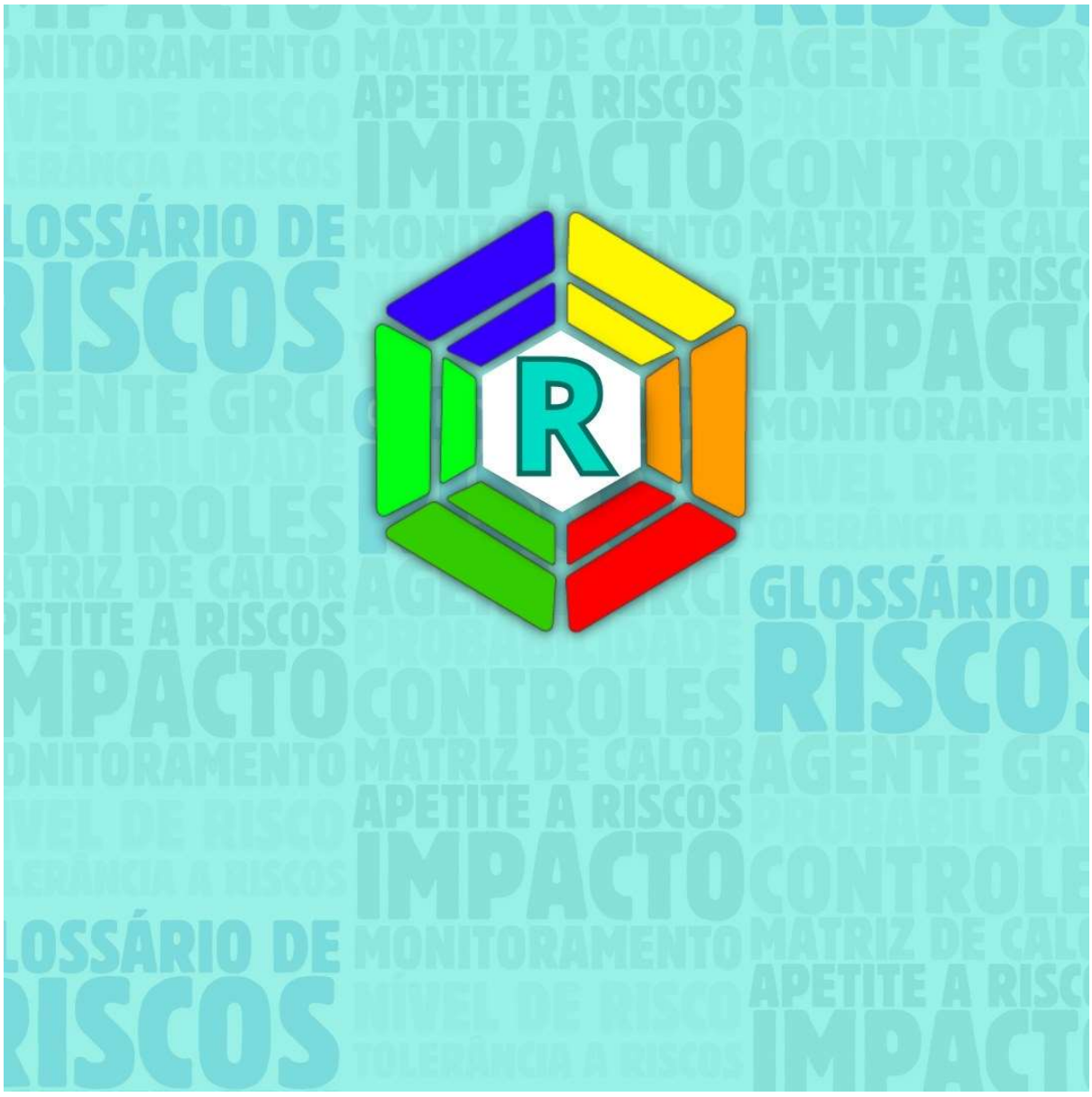
Processo de avaliação de riscos:

Processo global representado pelo conjunto de métodos e técnicas que possibilitam a identificação de riscos, a análise de riscos e a avaliação de riscos que possam impactar os objetivos de organizações, programas, projetos e atividades.
Envolve a identificação das fontes de risco, dos eventos e de sua probabilidade de ocorrência, de suas causas e suas consequências potenciais, das áreas de impacto, das circunstâncias envolvidas, inclusive aquelas relativas a cenários alternativos (ABNT, 2009, adaptado).

Processo de Gestão de Riscos:

Aplicação sistemática de políticas, procedimentos e práticas de gestão em atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica de riscos (ABNT, 2009).

Equivalente a: Gerenciamento de riscos


R

RAS (Risk Appetite Statement):

Ver Declaração de Apetite a Riscos

Responsável por Controles:

Profissional responsável por implementar e supervisionar os controles em uma unidade organizacional específica, garantindo que estejam alinhados às políticas internas e sejam eficazes na mitigação de riscos.
Também deve monitorar frequentemente os controles, avaliar sua eficácia e reportar informações sobre sua operação e resultados.

Respostas a riscos:

Opções e ações gerenciais para tratamento de riscos.
Inclui evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem ao risco porque o risco está além do apetite a risco da organização e outra resposta não é aplicável; transferir o risco com outra parte; aceitar o risco por uma escolha consciente; ou tratar o risco diminuindo sua probabilidade de ocorrência ou minimizando suas consequências (INTOSAI, 2007).

Risco:

Possibilidade de um evento ocorrer e afetar adversamente a realização de objetivos (COSO GRC, 2004); possibilidade de algo acontecer e ter impacto nos objetivos, sendo medido em termos de consequências e probabilidades (BRASIL, 2010c); efeito da incerteza nos objetivos (ABNT, 2009).
Pode ser Positivo ou Negativo.

Ver também: Riscos positivos e Riscos negativos

Risco atual:

Nível de risco que permanece após a implementação dos controles e medidas de mitigação.
O risco atual, ou residual, refere-se ao cenário atual e deve ser monitorado constantemente para assegurar que permaneça dentro dos níveis aceitáveis de apetite a riscos.

Equivalente a: Risco residual

Risco crítico:

Qualquer risco com índices de Nível de Risco Atual entre 21 e 25.
Todo risco estratégico ou de negócio são considerados riscos críticos.

Risco inerente:

Nível de risco presente em um ambiente ou atividade antes da implementação de qualquer medida de controle.
Representa o risco bruto ao qual a organização está exposta naturalmente, sem levar em consideração as ações de mitigação.

Risco Materializado:

Ver Materialização de risco

Risco projetado:

Refere-se ao cenário projetado (“aonde se quer chegar”), após a implementação de todos os controles propostos, ou melhorias em controles existentes, ou seja, após o completo tratamento do risco.

Risco Residual:

Ver Risco atual

Riscos Corporativos:

Ver Riscos Empresariais

Riscos de Negócio:

Riscos que afetam os componentes estratégicos fundamentais de uma organização, como sua missão, visão e valores. Eles são considerados perenes e intrínsecos à organização e podem surgir independentemente dos objetivos estratégicos definidos.

Os riscos de negócio representam uma exposição constante e exigem monitoramento contínuo e gestão criteriosa, pois podem impactar significativamente a continuidade e o sucesso da organização.

A gestão de riscos de negócio é crítica para garantir que os objetivos corporativos sejam alcançados mesmo em um ambiente de incerteza.

Riscos de Projetos Estratégicos:

Riscos associados aos projetos e programas estratégicos de uma organização. São riscos que, se materializados, podem impactar o sucesso ou fracasso de projetos importantes.
A gestão destes riscos envolve a identificação antecipada, monitoramento contínuo e a implementação de controles específicos.

Riscos Empresariais:

Refere-se à consolidação das seguintes dimensões de riscos:

- Riscos Estratégicos,
- Riscos de Negócio,
- Riscos de Projetos Estratégicos e
- Riscos Operacionais.

Ver também: Riscos Corporativos

Riscos Estratégicos:

Riscos que podem afetar diretamente a estratégia de uma organização, incluindo riscos que impactam a missão, visão e valores da empresa.
Estes riscos são gerenciados no nível de alta administração e exigem uma abordagem estratégica para assegurar a sustentabilidade da organização a longo prazo.

Riscos negativos:

Eventos que, se ocorrerem, podem ter impactos adversos para a organização.
A gestão de riscos negativos visa reduzir a probabilidade de ocorrência e o impacto de tais eventos, utilizando controles preventivos e contingenciais.

Ver também: Ameaças

Riscos Operacionais:

Riscos associados a processos organizacionais que podem impactar o desempenho operacional e a continuidade das atividades de uma empresa.
Estes riscos são gerenciados através da identificação de processos críticos, avaliação de controles existentes e desenvolvimento de planos de ação para mitigação.

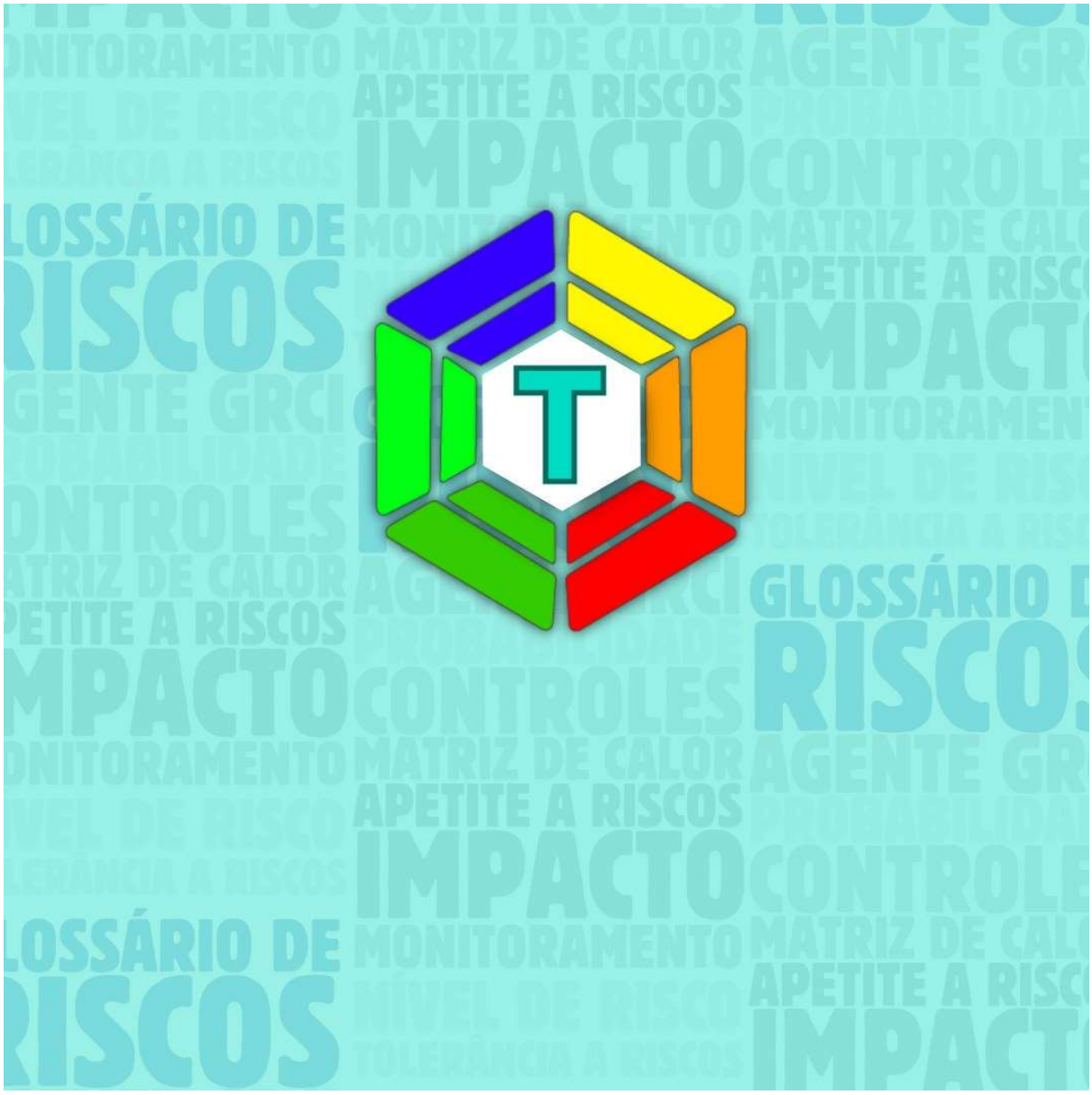
Riscos positivos:

Eventos que, se ocorrerem, podem ter impactos benéficos para a organização.
A gestão de riscos positivos envolve maximizar a probabilidade e o impacto de oportunidades identificadas, transformando incertezas em vantagens competitivas.

Ver também: Oportunidades

Stakeholder:

Ver Parte interessada



Teste de Controle:

Processo de execução prática dos controles para verificar sua eficácia real em mitigar os riscos e atingir os objetivos esperados.

Tipologia:

É a categorização dos riscos com base nas causas fundamentais que os impulsionam, sejam elas negativas ou positivas, permitindo uma estrutura que reflete o contexto operacional e estratégico da organização.

Tolerância a riscos:

Tolerância ao risco representa a variação aceitável em torno do apetite ao risco estabelecido.
É a margem dentro da qual a organização pode operar sem necessidade de ações corretivas imediatas, porém requer monitoramento constante e esforço contínuo para levar o risco ao nível do apetite.
A flexibilidade na definição de tolerância permite adaptação a cenários imprevistos ou mudanças significativas nas condições de negócios.

Transferir risco:

Ação de transferir a responsabilidade pelo risco, total ou parcialmente, para outra parte. Isso pode ser feito por meio de contratos, seguros ou terceirização.
Para riscos negativos, a transferência reduz o impacto financeiro ou operacional na organização.
Para riscos positivos, a transferência pode ocorrer por meio de parcerias ou co-investimentos, compartilhando os benefícios potenciais com outra entidade.

Ver também: Respostas a riscos

Tratar risco:

Processo de planejar e implementar medidas para modificar a probabilidade de ocorrência ou o impacto de um risco.
O tratamento pode incluir ações de mitigação, fortalecimento de controles, transferência, aceitação ou eliminação do risco.
No caso de riscos positivos, o tratamento pode envolver a maximização das chances de sucesso e dos benefícios associados.

Ver também: Respostas a riscos

Verificação de controle:

Avaliação documental e análise dos controles estabelecidos para garantir que estão implementados conforme planejado.


GRATO PELA
AUDIÊNCIA!
Caminhe conosco nessa jornada
rumo à excelência na Gestão de
Riscos do SERPRO!

Acesse o link abaixo *que **CONECTAM*** os conceitos e **complementam** a explicação do **TEMA** abordado neste material.

Documento Relacionado:

Metodologia de Gestão de Riscos e Controles do SERPRO (GR-007/2025)

- ***Link para a Deliberação GR-007/2025 (no Portal da Transparência do Serpro)***


GRATO PELA
AUDIÊNCIA!
Caminhe conosco nessa jornada
rumo à excelência na Gestão de
Riscos do SERPRO!


Glossário
de Riscos
SWAY