DECISÃO DIRETIVA

GR-007/2025

Data Início: 03/01/2025

Data Fim:

CÓDIGO DE CLASSIFICAÇÃO ARQUIVÍSTICA: 010.01 **CLASSIFICAÇÃO DA INFORMAÇÃO:** Ostensivo

TÍTULO: METODOLOGIA DE GESTÃO DE RISCOS E CONTROLES

PALAVRAS – CHAVE: Metodologia, riscos, controles, gestão de riscos

ANEXO:

1 – Metodologia de Gestão de Riscos e Controles;
1A – Orientação Técnica para Tipologia de Riscos à Integridade;
1B – Orientação para definição de Indicadores Chave de Riscos (KRI;
1C – Método de Gestão de Riscos de Segurança da Informação (GRSI);
1D - Contingencia e Continuidade de Negócios na Gestão de Riscos.

PROCESSO: 12.01 - Gerir Riscos Empresariais e Controles; 12.05 – Gerenciar Continuidade de Negócios

1.0 FINALIDADE

Atualizar a Metodologia de Gestão de Riscos e Controles Internos, conforme Anexo 1, visando a padronização do processo de identificação, tratamento e monitoramento de riscos sobre processos corporativos, projetos estratégicos e planejamento estratégico da empresa. Esta atualização tem como objetivo: revisão da tipologia Financeiro; inclusão de Glossário; revisão de Tolerância a Riscos; inclusão de seção específica sobre Atendimento a Objetivos; mudança no fluxo do cancelamento de risco; e inclusão do conteúdo de contingência e continuidade de negócios na gestão de riscos.

2.0 ÂMBITO DE APLICAÇÃO

Todos os órgãos da empresa.

3.0 DETERMINAÇÕES

3.1 A Metodologia de Gestão de Riscos e Controles deve ser utilizada por todas as Unidades Organizacionais, cabendo-as fazer a gestão dos riscos e controles sob sua responsabilidade.
3.2 As avaliações dos riscos e dos controles previstos devem ser periódicas de forma que empresa identifique e trate continuamente os riscos de modo a possibilitar o alcance dos objetivos corporativos.
3.3 A Superintendência de Controles, Riscos e Conformidade – SUPCR é a Unidade Organizacional responsável pela gestão, implementação e manutenção da metodologia.

4.0 DISPOSIÇÃO FINAL

4.1 Este documento substituirá a Decisão Diretiva GR-026/2024, de 23 de fevereiro de 2024.
4.2 Ficam convalidados os atos praticados desde o dia 1º de janeiro de 2025 até o início da vigência do presente documento.

Diretor-Presidente

ÓRGÃO/REDATOR: DIJUG/SUPCR/CRGRC

METODOLOGIA DE GESTÃO DE RISCOS E CONTROLES

SUMÁRIO

GLOSSÁRIO

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 do apetite definido pela 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, apoiando gestores e disseminando práticas de gerenciamento de riscos. Equivalente a: **Agentes GRCI**.

Agentes GRCI: Ver **Agentes de Riscos e Controles**.

Ameaças: Ver **Riscos Negativos**.

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**.

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. Equivalente a: **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.**

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 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**.

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. Equivalente a: **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.

1. INTRODUÇÃO

Esta metodologia estabelece as diretrizes para a gestão integrada de riscos e controles, promovendo a identificação, avaliação e tratamento de riscos que possam impactar os objetivos organizacionais. Baseia-se nos princípios da ISO 31000:2018 e no modelo COSO ERM, integrando os diferentes tipos de risco à governança corporativa.

Conforme descrito na Norma ABNT ISO 31000:2018, as organizações enfrentam influências de fatores internos e externos que tornam incerto o alcance de seus objetivos. O efeito que essa incerteza tem sobre os objetivos da organização é chamado de "risco". "Um efeito é um desvio em relação ao esperado. Pode ser positivo, negativo ou ambos, e pode abordar, criar ou resultar em oportunidades e ameaças".

A gestão de riscos corresponde às atividades coordenadas para dirigir e controlar uma organização no que se refere aos riscos. Ao ser implementada e mantida, possibilita:

a) Assegurar que os responsáveis pela tomada de decisão, em todos os níveis, tenham acesso tempestivo a informações suficientes sobre quais são os riscos aos quais a organização está exposta, possibilitando uma abordagem proativa em relação a ameaças e oportunidades.

b) Contribuir para aumentar a probabilidade de alcance dos objetivos da organização, por meio do tratamento dos riscos a níveis aceitáveis pelos gestores e demais partes interessadas, o que é fundamental para garantir o sucesso e a sustentabilidade das operações.

c) Agregar valor à organização por meio do tratamento adequado dos riscos e dos impactos decorrentes de sua materialização, fortalecendo a resiliência e a capacidade de adaptação.

d) Atuar de forma integrada com o planejamento estratégico, processos e projetos corporativos, garantindo que a gestão de riscos esteja alinhada com as metas e objetivos estratégicos da organização.

e) Alinhar o Apetite a Riscos com a estratégia empresarial, assegurando que a postura frente aos riscos esteja em sintonia com a visão de longo prazo e os valores da empresa.

f) Dar transparência de que os riscos empresariais são conhecidos e gerenciados, o que constrói a confiança de partes interessadas, como colaboradores, clientes e reguladores.

g) Alinhar a gestão de riscos com a governança corporativa, gestão de segurança da informação, gestão de continuidade de negócios, gestão financeira, gestão da integridade organizacional, gestão de tecnologia da informação e gestão da privacidade e proteção de dados. Isso promove uma abordagem holística para a gestão de riscos, integrando-a em todos os aspectos da organização.

h) A vinculação da gestão de riscos com os Objetivos de Desenvolvimento Sustentável (ODS) ajudando a organização a evitar problemas que possam atrapalhar os ODS e a aproveitar oportunidades que os apoiem. Isso é crucial para promover a sustentabilidade e alinhar as atividades empresariais com as metas globais de desenvolvimento sustentável da agenda ESG (Environmental, Social & Governance – Ambiental, Social e Governança), um conjunto de padrões e boas práticas que visa definir se uma empresa é socialmente consciente, sustentável e corretamente gerenciada.

A Metodologia de Gestão de Riscos e Controles do Serpro padroniza a implementação, manutenção e monitoramento do processo de Gestão de Riscos e Controles. A Metodologia deve ser aplicada para identificação dos riscos da Empresa, visando o estabelecimento de matrizes de riscos, de controles para seu tratamento e de indicadores de evolução. A Metodologia abrange o levantamento e tratamento dos riscos empresariais[1], no qual fazem parte os riscos operacionais do Serpro, cuja principal fonte são os processos organizacionais, os riscos estratégicos, associados ao planejamento estratégico, os Riscos ao Negócio, que afetam os componentes estratégicos da empresa e os riscos dos projetos estratégicos.

Riscos Empresariais = Riscos Operacionais **+** Riscos Estratégicos **+** Riscos ao Negócio + Riscos de Projetos Estratégicos

[1] Entende-se como riscos empresariais a consolidação das seguintes dimensões de riscos: Riscos Estratégicos, Riscos ao Negócio, Riscos de Projetos Estratégicos e Riscos Operacionais. Riscos Empresariais também são referenciados como riscos corporativos.

2. FUNDAMENTOS

A implantação e o aprimoramento da gestão de riscos em uma organização constituem um processo de aprendizado constante, que começa com o desenvolvimento de consciência sobre a importância de gerenciar Riscos e Controles e avança com a implementação e amadurecimento de práticas, políticas, processos e estruturas.

Para elaboração desta metodologia, o Serpro utilizou documentos normativos do Governo Federal Brasileiro e referenciais teóricos de gestão de riscos reconhecidos pelo mercado como *frameworks*. No âmbito do Poder Executivo Federal, o marco regulatório que orienta os órgãos e as entidades públicas sobre as medidas para a sistematização de práticas relacionadas à gestão de riscos e aos controles é a Instrução Normativa Conjunta MP/CGU nº. 01, de 10 de maio de 2016, complementada pela Resolução CGPAR/ME nº. 33, de 4 de agosto de 2022, pelo Decreto 8945/2016 e pela Lei 13.303/2016.

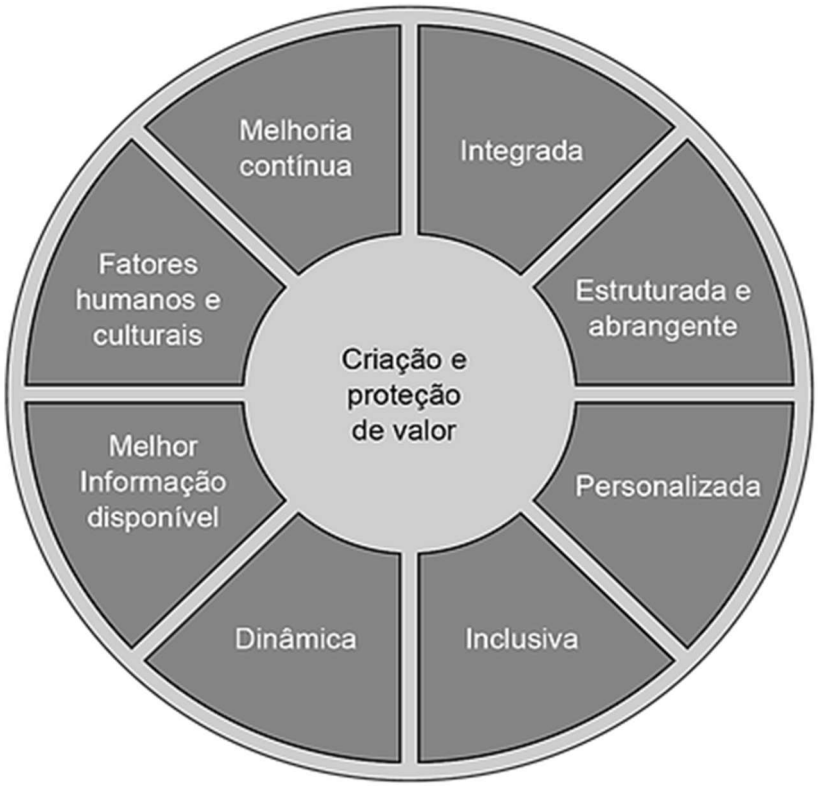
Em relação aos principais referenciais de mercado, os adotados para a construção desta metodologia foram a norma ISO 31000:2018, atualizada com a nova versão, que define um enfoque mais simplificado e estratégico que a versão anterior, de 2009, e o *Committee of Sponsoring Organizations of the Treadway Commission* (COSO).

O COSO publicou, em 2017, seu segundo referencial (COSO II), intitulado Gerenciamento dos Riscos Corporativos – Integrado com a Estratégia e Performance (*Enterprise Risk Management*). Este referencial ressalta a importância de se considerar o risco tanto no processo de definição das estratégias como na melhoria da performance e destaca o valor do gerenciamento de riscos corporativos ao estabelecer e executar uma estratégia.

A gestão de riscos e os controles são mecanismos de governança corporativa e partes integrantes das atividades organizacionais. Seu propósito é a proteção de valor da organização, ao contribuir para a melhoria do desempenho e apoiar o alcance dos objetivos e a tomada de decisões.

Esta metodologia adota, com adaptações, os princípios definidos na norma ISO 31000:2018 que oferecem suporte ao gerenciamento dos riscos e auxiliam a criação de uma estrutura de gestão de riscos, cujas características são apresentadas na Figura 1 e descritas a seguir.

Figura 1 *– Princípios da Gestão de Riscos e Controles*



Fonte*: ABNT/CEE-063 – NBR ISO 31000:2018 – fev.2018*

a) Integrada: A gestão de riscos é parte integrante de todas as atividades organizacionais.

b) Estruturada e abrangente: A execução da gestão de riscos é realizada de forma sistemática, estruturada e oportuna, alinhada ao interesse público.

c) Personalizada: A estrutura e o processo de gestão de riscos são personalizados e proporcionais aos contextos externo e interno da organização, relacionados aos seus objetivos.

d) Inclusiva: Todos os empregados e gestores são responsáveis pela Gestão de Riscos e Controles em suas atividades e processos de trabalho.

e) Dinâmica: Alguns riscos podem surgir, desaparecer ou mudar. A intenção é responder aos ambientes internos e externos de forma dinâmica, apropriada e oportuna.

f) Melhor informação disponível: A Gestão de Riscos e Controles utiliza informações históricas e atuais, bem como expectativas futuras. Limitações, incertezas e divergências associadas a essas informações são levadas em consideração e afetam o resultado da gestão de riscos.

g) Fatores humanos e culturais: Fatores humanos e culturais influenciam significativamente a gestão de riscos.

h) Melhoria contínua: O aprendizado e a internalização da cultura de Gestão de Riscos e Controles permitem ciclos de melhoria contínua.

Tais princípios visam estimular a mudança, melhorando os processos e propondo novos desafios fomentando a inovação e ação empreendedora, responsáveis. Para garantir a adoção dos princípios descritos, a Gestão de Riscos e Controles deve ser apoiada e monitorada pelos administradores da empresa.

3. ESTRUTURA

Segundo a norma ISO 31000:2018, a estrutura de Gestão de Riscos de uma organização é o conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria contínua da Gestão de Riscos e Controles por toda a organização.

Figura 2 *– Linhas da Gestão de Riscos e Controles*

Fonte*: Modelo das Três Linhas – IIA (The Institute of Internal Auditors), 2020*

A estrutura de Gestão de Riscos e Controles do Serpro utiliza o Modelo das Três Linhas (2020), propagado pelo Instituto de Auditores Internos dos Estados Unidos, representado na Figura 2. O Modelo permite que a 2ª. Linha apoie a 1ª. Linha, de forma a subsidiá-la na implementação do processo de Gestão de Riscos e Controles, para que disponham de informações consistentes, relevantes e tempestivas, para que sejam utilizadas como ferramenta auxiliar na tomada de decisão, além de se tornar um insumo cada vez mais relevante para a 3ª. Linha, visto que no Serpro a Auditoria Baseada em Riscos (ABR) já é uma realidade.

A **1ª. Linha** é exercida por todas as Unidades Organizacionais por meio dos empregados e gestores, responsáveis pela gestão dos riscos e dos controles em suas áreas

de atuação. Devem identificar, avaliar, controlar e reduzir as incertezas que possam interferir no alcance dos objetivos organizacionais. Ainda de acordo com o Instituto dos Auditores Internos (IIA), a responsabilidade pela verificação da eficácia dos controles é atribuída também à primeira linha.

A **2ª. Linha** é exercida por diversas unidades organizacionais que possuem sob sua gestão uma pluralidade de competências orientadas pela adoção de boas práticas e metodologias aplicadas às funções abaixo.

a) Controle Financeiro: preservar o valor da empresa, ou seja, acompanhar se os mecanismos adotados pelos gestores são efetivos de forma a evitar perdas econômico-financeiras; monitorar aspectos do reporte financeiro.

b) Segurança: supervisionar a efetiva aplicação da política e do processo de segurança corporativos em todas as áreas da empresa.

c) Qualidade: primar pela contínua qualidade de forma sistemática quanto a avaliação, controle, e comunicação para a qualidade do processo em todo o seu ciclo de vida.

d) Gerenciamento de riscos: avaliar e monitorar, de forma contínua, os controles para mitigação de riscos.

e) Conformidade: orientar na execução dos processos de conformidade, estimular a cultura de conformidade da empresa junto a administradores, gestores, empregados, colaboradores, fornecedores, prestadores de serviço e demais parceiros de negócio, realizar avaliações de conformidade de acordo com o planejamento estabelecido, e apoiar na identificação e monitoramento de eventuais não conformidades.

f) Integridade[2]: atuar na promoção da integridade no Serpro por meio da estruturação, execução e monitoramento do Programa de Integridade, de modo a assegurar uma atuação pautada nos princípios de integridade, transparência e ética.

g) Privacidade e Proteção de Dados: atuar na implementação e manutenção das práticas corporativas de privacidade e proteção de dados no Serpro, em alinhamento com os requisitos de negócio e em consonância com os princípios estabelecidos no Art. 6º. da Lei Geral de Proteção de Dados Pessoais – LGPD.

As diferentes unidades organizacionais são responsáveis, nas respectivas áreas de atuação, pelo suporte e monitoramento das funções da 1ª. Linha, de forma a assegurar que as suas atividades sejam desenvolvidas e executadas de forma apropriada.

A área de Gestão de Riscos e Controles do Serpro, como 2ª. Linha, é responsável pela definição e implementação de políticas, procedimentos e diretrizes relacionados à Gestão de Riscos e Controles, além de prover a orientação e supervisão necessárias à 1ª. Linha e

[2] Os Riscos à Integridade devem ser tratados conforme orientação técnica “Riscos à Integridade” no Anexo 1A.

submeter informações consolidadas ao Comitê Estratégico de Governança, Riscos, Controles e Segurança da Informação (COGRS), à Diretoria Executiva (DIREX), ao Comitê de Auditoria (COAUD), ao Conselho de Administração (CA) e ao Conselho Fiscal (CF).

A **3ª. Linha** é exercida pela Auditoria Interna, responsável por aferir a adequação do controle interno, a efetividade do gerenciamento dos riscos e dos processos de governança.

Na seção 4 desta metodologia estão detalhadas as responsabilidades dos envolvidos no Processo de Gestão de Riscos e Controles.

A gestão de riscos empresariais do Serpro é dividida nas dimensões abaixo descritas, que serão tratados de forma particularizada por esta metodologia.

a) Riscos Operacionais – trata, de forma geral, os riscos associados aos processos organizacionais. Ressalta-se que os processos são definidos por meio da Arquitetura de processos / cadeia de valor do Serpro. O objetivo do processo é o principal insumo para a identificação dos riscos operacionais, embora não seja a única fonte. A única condição que poderia isentar a unidade organizacional da responsabilidade de identificar e gerenciar riscos seria a ausência de qualquer objetivo. Quantitativamente, a dimensão dos Riscos Operacionais é o maior grupo de riscos da organização, uma vez que permeia toda a empresa. A metodologia para gestão dos riscos operacionais será apresentada na seção 7 deste documento.

b) Riscos de Projetos Estratégicos – Inclui os riscos associados aos programas e projetos estratégicos da empresa, definidos e geridos pela área de Projetos, sendo os objetivos específicos de cada projeto os principais direcionadores para a identificação e avaliação de riscos. A área de Riscos e Controles realiza o monitoramento dos Riscos e Controles dos projetos estratégicos priorizados pela Diretoria Executiva, conforme estabelecido no Plano Anual de Riscos e Controles. Estes riscos são tratados na seção 8 deste documento. Ressalta-se que, independentemente de estarem incluídos no Plano Anual de Riscos e Controles, todos os projetos estratégicos devem ter seus riscos identificados e gerenciados de acordo com o processo descrito nesta metodologia.

c) Riscos Estratégicos – referem-se aos riscos associados à estratégia da empresa. O foco encontra-se no acompanhamento de fatores que podem afetar o alcance dos objetivos estratégicos ou pelo menos um dos componentes estratégicos. Caso afetem os componentes estratégicos da empresa, ou seja, a sua missão, visão ou os valores, são descritos como Riscos ao Negócio. Estes são perenes, intrínsecos à organização e podem ser constituídos independente dos objetivos estratégicos definidos. Na gestão estratégica do risco, o foco está na inserção do risco na esfera de temas prioritários de gestão e, conforme definido no Estatuto Social, são aprovados pelo Conselho de Administração (CA) até a última reunião ordinária de cada ano. O item 9 deste documento apresenta a metodologia para gestão dos riscos estratégicos.

4. ATORES, PAPÉIS E RESPONSABILIDADES

O Modelo das Três Linhas e a estrutura de Gestão de Riscos e Controles do Serpro, baseada nas melhores práticas e referenciais teóricos, estabelecem o compartilhamento de responsabilidades para o adequado funcionamento da Gestão de Riscos e Controles na empresa.

A Política Corporativa de Gestão de Riscos e Controles e outros normativos internos também estabelecem responsabilidades relacionadas à gestão de riscos e aos controles.

Todos os **empregados e gestores,** atores da 1ª. Linha**,** são responsáveis pela Gestão de Riscos e Controles em sua Unidade Organizacional e cada risco mapeado e avaliado deve estar associado a um responsável formalmente definido como Gestor de Riscos.

Além desta responsabilidade individual, os órgãos estatutários possuem responsabilidades associadas à gestão de riscos e aos controles, definidas no Estatuto Social e relacionadas, de forma sintética, a seguir:

a) o **Conselho de Administração (CA)** é responsável por aprovar a Política Corporativa de Gestão de Riscos, aprovar e acompanhar o plano de gestão de riscos empresariais, supervisionar os sistemas de gerenciamento de riscos e de controles. Compete ainda, ao Conselho de Administração, a aprovação dos Riscos Estratégicos e ao Negócio e da Declaração de Apetite a Riscos (*Risk Appetite Statement* – RAS). O RAS é o documento pelo qual o Serpro sinaliza aos órgãos reguladores, ao mercado, aos colaboradores e às demais contrapartes quais os níveis de aceitação de riscos que serão admitidos na realização de seus negócios e objetivos.

b) o **Comitê de Auditoria (COAUD)** é responsável por assessorar o Conselho de Administração no monitoramento do gerenciamento de Riscos e Controles, por supervisionar as atividades desenvolvidas nas áreas de Gestão de Riscos e Controles e monitorar a qualidade e a integridade dos mecanismos de Gestão de Riscos e Controles;

c) o **Conselho Fiscal (CF)** se configura como parte integrante do Sistema da governança corporativa, responsável, principalmente, por fiscalizar os atos dos administradores e verificar os cumprimentos dos seus deveres legais e estatutários;

d) a **Diretoria Executiva (DIREX)** é responsável por validar o Apetite a Riscos e os Riscos Estratégicos e ao Negócio. À DIREX cabe ainda monitorar as medidas de tratamento dos riscos estratégicos, acompanhar e submeter à aprovação do Conselho de Administração o plano de gestão de riscos empresariais e os relatórios periódicos do gerenciamento dos Riscos e Controles;

e) o **Diretor-Presidente (DP)** deve manter, sob sua supervisão direta, o gerenciamento de riscos de controles e de conformidade;

f) os **Diretores**, por meio dos seus superintendentes, nos Comitês Táticos, devem ser agentes de proposição de assuntos relevantes relativos à Gestão de Riscos e Controles do Serpro afetos à sua Diretoria e à empresa;

g) o **Comitê Estratégico de Governança, Riscos, Controles e Segurança da Informação (COGRS)** é o órgão colegiado responsável por assessorar a Diretoria Executiva em aspectos relacionados à governança corporativa, Gestão de Riscos e Controles e quanto a supervisão dos aspectos de segurança da informação, gestão de continuidade de negócios, privacidade, proteção e governança de dados;
Cabe ao Comitê a criação, atualização e proteção da Política Corporativa de Gestão de Riscos e Controles. Também é de responsabilidade do Comitê Estratégico dirimir temas transversais que permeiam Diretorias distintas;

h) os **Comitês Táticos de Gestão de Riscos e Controles das Diretorias (COGRC)** são responsáveis por apoiar a institucionalização da Gestão de Riscos e Controles das unidades organizacionais, pelo monitoramento dos planos de tratamento de Riscos e Controles, por dirimir temas transversais que permeiam Superintendências distintas dentro da mesma Diretoria e por prover informações consolidadas para serem submetidas ao Comitê Estratégico;

i) a **Área de Gestão de Riscos e Controles** é responsável por gerenciar a Política de Gestão de Riscos e Controles, por elaborar o Plano Anual de Gestão de Riscos e Controles, por disseminar, apoiar, realizar consultoria, monitorar e supervisionar a implementação e atualização desta metodologia, por definir e atualizar o Processo de Gestão de Riscos e Controles, por avaliar os Controles e por elaborar relatórios periódicos consolidados de gerenciamento de Riscos e Controles aos órgãos colegiados.

Esta metodologia define também papéis que terão responsabilidades específicas na implementação das ações de Gestão de Riscos e Controles:

a) Gestor de Riscos e Controles;

b) Agente de Riscos e Controles (Agente GRCI);

c) Responsável pelos Controles;

d) Agente Corporativo de Riscos e Controles;

e) Aprovador de Riscos;

f) Partes Interessadas; e

g) Especialista da tipologia[3].

[3] As tipologias serão descritas em detalhes na seção 7.2.1 desta Metodologia.

O **Gestor de Riscos e Controles** é o responsável pelo risco e deve estar formalmente identificado em cada unidade. Deve ter alçada suficiente para orientar e acompanhar as ações de gerenciamento de riscos.

São responsabilidades do Gestor de Riscos e Controles:

a) Identificar e registrar os riscos Operacionais, dos Projetos Estratégicos e Riscos Estratégicos e ao Negócio sob sua responsabilidade, na Unidade Organizacional;

b) Assegurar que o risco seja gerenciado de acordo com os normativos de Gestão de Riscos e Controles do Serpro;

c) Monitorar o risco frequentemente de forma a garantir que as respostas adotadas (controles) resultem na manutenção do risco em níveis adequados e de forma tempestiva;

d) Garantir que as informações adequadas sobre o risco e controles estejam disponíveis para todos os níveis da organização;

e) Registrar a materialização do risco e respectivo tratamento;

f) Realizar revisão frequente dos riscos identificados e dos controles;

g) Acompanhar a implementação dos controles propostos;

h) Avaliar a eficácia dos controles; e

i) Envolver os gestores e/ou Agentes de Riscos (Agentes GRCI) de outras unidades, sempre que houver essa necessidade, para o adequado tratamento de riscos transversais, cujo tema principal está sob sua responsabilidade.

Os **Agentes de Riscos e Controles** (Agentes GRCI) são os empregados indicados pelos Superintendentes em cada unidade organizacional. São suas responsabilidades:

a) Orientar suas atividades de acordo com o Plano de Gestão de Riscos e Controles;

b) Atuar como disseminadores do processo de Gestão de Riscos e Controles e como facilitadores da aplicação desta metodologia e auxiliar os responsáveis pelos processos;

c) Apoiar os Gestores de Riscos e Controles de suas unidades;

d) Realizar e registrar, tempestivamente, o monitoramento dos riscos e o acompanhamento dos controles associados aos riscos na ferramenta corporativa;

e) Atuar como facilitador em monitoramento dos riscos e seus controles, sempre que for necessário;

f) Dar ciência ao superintendente da unidade e à segunda linha sobre o monitoramento;

g) Apoiar a elaboração dos relatórios de riscos;

h) Dar suporte à implementação dos controles propostos;

i) Auxiliar na divulgação do processo de Gestão de Riscos e Controles; e

j) Auxiliar a Unidade na identificação e gestão de riscos.

Os Agentes de Riscos e Controles das unidades organizacionais (primeira linha – Agentes GRCI) serão capacitados pelos Agentes Corporativos de Riscos e Controles (2ª linha) em conhecimentos de Gestão de Riscos e Controles, visando apoiar as atividades do processo em suas unidades. As Unidades Organizacionais devem indicar pelo menos dois Agentes de Riscos e Controles (Agentes GRCI).

Os **Responsáveis pelos Controles** são aqueles designados para acompanhar e/ou implementar melhorias em controles existentes ou novos controles, quando necessário, bem como manter em execução controles redutores, para riscos negativos, ou controles alavancadores, para riscos positivos, dos níveis de probabilidade e do impacto do risco, conforme preconizado por meio do processo de gestão dos Riscos e Controles. O detalhamento sobre riscos negativos e riscos positivos, bem como os controles relacionados, será apresentado adiante, neste documento.

Os responsáveis pelos controles, não necessariamente estão alocados na mesma unidade organizacional responsável pelo risco.

Os **Agentes Corporativos de Riscos e Controles** são empregados da área de Gestão de Riscos e Controles (2ª linha) responsáveis pela supervisão da implementação das atividades de gestão de riscos e verificação da presença e funcionamento dos controles nas unidades do Serpro. A área de Gestão de Riscos e Controles deve manter pelo menos um agente corporativo de riscos e controles indicado para atender a cada Diretoria.

São responsabilidades dos Agentes Corporativos de Riscos e Controles:

a) Prover treinamento da Metodologia de Gestão de Riscos e Controles;

b) Realizar análise crítica do desempenho da Gestão de Riscos e Controles da Diretoria objetivando a sua melhoria contínua;

c) Promover a análise crítica sobre os Riscos e Controles mapeados pelas Unidades Organizacionais;

d) Supervisionar o monitoramento da evolução dos níveis de Riscos e Controles e a verificação da presença e do funcionamento dos controles implementadas;

e) Dar suporte à identificação, análise e avaliação dos riscos empresariais selecionados para a implementação da gestão de riscos (implantação assistida); e

f) Realizar análise crítica do desempenho da Gestão de Riscos Empresariais objetivando a sua melhoria contínua, formalizando o resultado por meio de **Relatório consolidado de Riscos e Controles**. O relatório deve ser submetido ao Comitê Estratégico (COGRS), à Diretoria Executiva (DIREX), ao Comitê de Auditoria (COAUD), ao Conselho Fiscal (CF) e ao Conselho de Administração (CA) e/ ou quando à Diretoria Executiva julgar pertinente.

Os **Aprovadores de Riscos** são responsáveis pela aprovação dos riscos identificados pelos Gestores e Agentes de Riscos das unidades (Agentes GRCI), função que pode ser exercida por Diretores das Unidades Organizacionais, Superintendentes ou Gerentes de grupo II designados. Além disso, cabe a eles avaliarem e decidir sobre a necessidade de aprovar o cancelamento de riscos previamente aprovados, quando solicitado.

As **Partes Interessadas** são as pessoas ou Unidades Organizacionais que podem afetar, ser afetadas, ou perceber-se afetadas por uma decisão ou atividade, ou pelo próprio risco.

O **Especialista da tipologia**[4] é o responsável, na 2ª. Linha, por auxiliar na definição do Apetite a Risco da tipologia, na declaração de níveis de impacto e na análise dos riscos tipificados na tipologia. Além disso, o especialista presta suporte técnico no processo de gestão de riscos, contribuindo com recomendações e sugestões relacionadas aos registros e controles associados.

4.1. Colaboração entre Gestão de Riscos, Continuidade de Negócios e Auditoria

A integração entre as áreas de gestão de riscos, continuidade de negócios e auditoria é fundamental para assegurar uma abordagem coordenada e eficaz na mitigação de riscos e na garantia de resiliência organizacional. Essa colaboração inclui as seguintes diretrizes e responsabilidades:

1. Designação de Representantes:

Cada área deve indicar representantes responsáveis por participar de fóruns e reuniões regulares voltados à discussão e alinhamento de estratégias e ações conjuntas. Esses representantes atuarão como pontos focais, facilitando a comunicação e a execução de iniciativas integradas.

2. Fóruns de Integração:

- Reuniões organizadas pelo Comitê Estratégico de Governança, Riscos, Controles e Segurança da Informação (COGRS) da Diretoria em questão, para discussão de temas transversais relacionados a riscos, continuidade de negócios e auditoria.
- Compartilhamento de informações relevantes, como análises de riscos críticos, atualizações de planos de continuidade de negócios e resultados de auditorias.

3. Sinergia na Resposta a Riscos Críticos:

- Em cenários de materialização de riscos críticos, as áreas envolvidas deverão trabalhar de forma integrada para coordenar planos de ação e garantir a continuidade das operações críticas da organização.

[4] As tipologias serão descritas em detalhes na seção 7.2.1 desta Metodologia.

- A auditoria desempenhará um papel de supervisão e avaliação independente, garantindo a eficácia das respostas implementadas.

4. Capacitação e Alinhamento:

- Programas de capacitação conjunta para os agentes das áreas envolvidas, promovendo a compreensão mútua de metodologias, ferramentas e objetivos.
- Criação de protocolos documentados que formalizem os fluxos de comunicação e as responsabilidades compartilhadas.

Esta integração garante que as respostas a riscos críticos sejam ágeis, consistentes e alinhadas aos objetivos estratégicos da organização, fortalecendo a governança corporativa como um todo.

O anexo 1D – Contingência e Continuidade de Negócios na Gestão de Riscos, integra conceitos e práticas de continuidade de negócios de forma alinhada à esta Metodologia.

5. PLANO DE GESTÃO DE RISCOS E CONTROLES

É competência da área de Gestão de Riscos e Controles elaborar, acompanhar e submeter à apreciação da DIREX e à aprovação do CA o planejamento da gestão dos riscos empresariais e controles.

A área de Gestão de Riscos e Controles é responsável pela implementação da Política de Gestão de Riscos no Serpro e, conforme determina o Art. 45 do seu Estatuto Social, deve coordenar os processos de identificação, classificação e avaliação dos riscos a que a empresa está sujeita.

O Plano de Gestão de Riscos e Controles busca em suas ações o fortalecimento da cultura de gestão de riscos e de controles em todas as áreas da empresa, destacando a sua relevância como instrumento de governança, gestão e de criação e manutenção de valor para a organização. O plano é anual, estabelece as metas e descreve como o gerenciamento de Riscos e Controles será conduzido, executado e monitorado.

6. APETITE E TOLERÂNCIA A RISCOS

6.1. Apetite a Riscos

Segundo definido pelo Tribunal de Contas da União – TCU, Apetite a Riscos indica a "expressão ampla de quanto risco uma organização está disposta a enfrentar para implementar sua estratégia, atingir seus objetivos e agregar valor para as partes interessadas, no cumprimento de sua missão".

Portanto, o Apetite a Riscos nada mais é que o nível máximo em que é possível aceitar o risco. O Apetite a Riscos reflete toda a filosofia administrativa da organização e, por sua vez, influencia a cultura e o estilo operacional.

Todas as melhores práticas, COSO ERM, COSO ICIF, ISO 31.000 sugerem que os gestores devem avaliar e definir o Apetite a Riscos da organização e analisar as estratégias, definindo os objetivos relacionados e desenvolver mecanismos para gerenciar os respectivos riscos. A gestão de riscos torna-se uma função estratégica, pois ajuda a organização a criar valor em suas operações assumindo certos riscos. Isso é parte inerente de qualquer tipo de negócio.

O Apetite a Riscos pode mudar com o tempo, conforme contexto interno e externo, e deve observar os objetivos estratégicos e a própria estratégia empresarial. Por esses motivos a avaliação periódica é necessária. A razão de se explicitar o Apetite a Riscos é para que seja possível subsidiar a organização no estabelecimento do compromisso de gerenciar o risco proativamente, como fonte para auxiliar na tomada de decisão.

O Apetite a Riscos está relacionado ao conservadorismo ou inclinação à aceitação ao risco como estratégia no atingimento dos objetivos. O ideal para a organização é encontrar o "equilíbrio na balança", no que se refere ao Apetite a Riscos, o que significa saber até onde se pode ir com a certeza de que o gerenciamento do risco será efetivo, sem que haja um excesso de controles para reduzir riscos negativos ou ampliar riscos positivos. O excesso de controles torna o processo oneroso (tempo e custos), diminuindo o poder de competitividade da organização ou mesmo sua capacidade de inovação.

A área de Gestão de Riscos e Controles do Serpro conduz o processo de definição e acompanhamento contínuo sobre o estabelecimento do Apetite a Riscos, tanto para riscos negativos quanto para riscos positivos. Tal definição é realizada por meio de atividade específica definida e detalhada como parte da cadeia de valor da empresa, com vistas a desenvolver o documento denominado **Declaração de Apetite a Risco – RAS** – do inglês *Risk Appetite Statement*, aprovado pelo CA, publicado e divulgado para toda a empresa. O RAS é, portanto, um insumo primordial para a condução da gestão de todos os riscos da empresa uma vez que nele são declarados quais valores são considerados razoáveis a assumir na execução de sua estratégia de negócio.

Os **riscos operacionais e de projetos estratégicos** devem ter seus **apetites associados às suas tipologias**[5]. Os **riscos estratégicos e de negócios** devem ter seus **próprios apetites**, de acordo com as características de cada risco.

A revisão do apetite deve ser dinâmica, permitindo aos dirigentes configurarem o esforço de gestão de riscos empregado nos processos, planejamento estratégico e projetos estratégicos.

6.1.1. Apetite para riscos negativos

A definição deste parâmetro visa evitar que a organização assuma ameaças além do que pode absorver ou adote uma estratégia muito conservadora que dificulte situações de inovação ou destine esforços não coerentes com o nível do risco.

De modo geral, quanto mais a organização tem a perder, menos ela pretende arriscar, isto é, quanto maior o nível do risco negativo, maior a tendência de o Apetite a Riscos ser mais baixo.

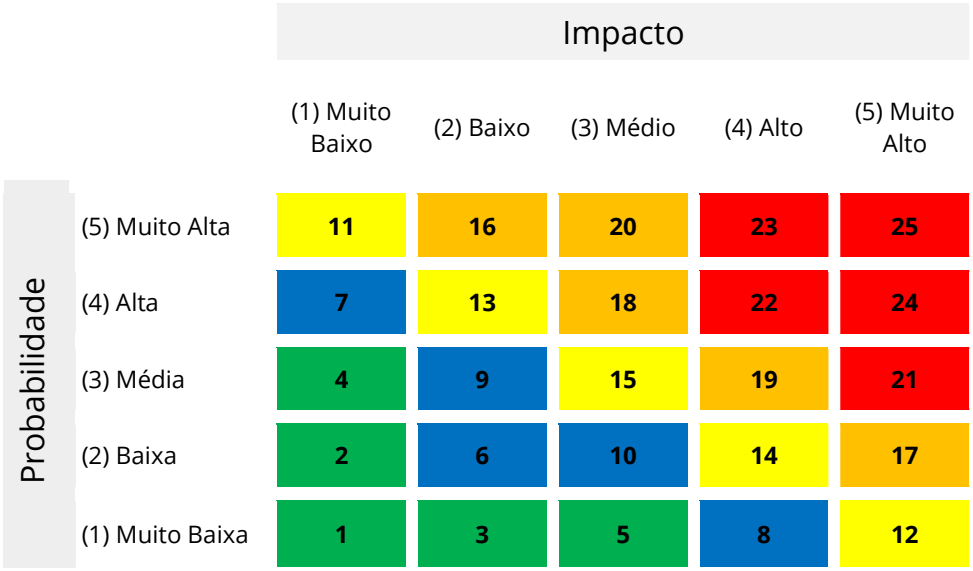
No Serpro, o apetite para riscos negativos é definido por meio de 5 níveis, coincidentes com os níveis de risco, destacados pelas diferentes cores das células da matriz da Figura 3, correlacionados aos Índices de Risco apresentados na Tabela 1

Tabela 1 *– Relação entre níveis de apetite, risco e índices de risco negativo*

Cor	Nível de Apetite ou de Risco	Índices de Risco correlacionados
Verde	Muito Baixo (1)	1 a 5
Azul	Baixo (2)	6 a 10
Amarelo	Médio (3)	11 a 15
Laranja	Alto (4)	16 a 20
Vermelho	Multo Alto (5)	21 a 25

[5] As tipologias serão descritas em detalhes na seção 7.2.1 desta Metodologia.

***Figura 3** – Apetite, níveis e índices de risco para riscos negativos*



Os numerais apresentados nas células representam os Índices de Risco, que serão mais detalhados no item 7.3.3 desta Metodologia.

6.1.2. Apetite para riscos positivos

A definição do apetite para riscos positivos deve considerar o nível ao qual a organização está disposta a investir em iniciativas para aproveitamento das oportunidades.

Assim como nos riscos negativos, o apetite para riscos positivos é definido por meio de 5 níveis, coincidentes com os níveis de risco, destacadas pelas diferentes cores das células da matriz da Figura 4, considerando os Índices de Risco apresentados na Tabela 2.

***Tabela 2** – Relação entre níveis de apetite, risco e índices de risco positivo*

Cor	Nível de Apetite / Nível de Risco	Índices de Risco correlacionados
Vermelho	Muito Baixo (1)	1 a 5
Laranja	Baixo (2)	6 a 10
Amarelo	Médio (3)	11 a 15
Azul	Alto (4)	16 a 20
Verde	Multo Alto (5)	21 a 25

Pode ser observado que os níveis de apetite para riscos positivos se comportam de forma inversa à matriz de apetite para riscos negativos. Assim, de modo geral, quanto menor o nível do risco positivo, maior a tendência de o Apetite a Riscos ser mais alto.

***Figura 4** – Apetite, níveis e índices de risco para riscos positivos*

Probabilidade	Impacto: (1) Muito Baixo	(2) Baixo	(3) Médio	(4) Alto	(5) Muito Alto
(5) Muito Alta	11	16	20	23	25
(4) Alta	7	13	18	22	24
(3) Média	4	9	15	19	21
(2) Baixa	2	6	10	14	17
(1) Muito Baixa	1	3	5	8	12

Os numerais apresentados nas células representam os Índices de Risco, que serão mais detalhados no item 7.3.3 desta Metodologia.

6.2. Tolerância a Riscos

Somente o apetite ao risco pode ser uma medida muito ampla e genérica, sem considerar as flutuações naturais ou inesperadas que podem ocorrer no ambiente de negócios.

Conforme descrito na NBR ISO 31073:2022, a tolerância ao risco é a disposição da organização ou da parte interessada em suportar o risco residual.[6]

Já segundo o Tribunal de Contas da União – TCU, tolerância a risco se refere ao "nível de variação aceitável no desempenho em relação à meta para o cumprimento de um objetivo específico, em nível tático ou operacional".

Enquanto o apetite ao risco define a direção estratégica e o nível aceitável de risco, a tolerância ao risco proporciona a capacidade de controlar, monitorar e reagir às variações no nível de risco, mantendo a organização dentro de limites seguros e alinhados aos seus objetivos.

A tolerância ao risco deve ser avaliada principalmente com base no Nível de Risco Atual (NRa). No entanto, o Nível de Risco Projetado (NRp) também deve ser considerado para garantir que as decisões atuais não comprometam a conformidade futura com o apetite ao risco. Em ambos os casos, é essencial que qualquer operação dentro das margens de tolerância seja monitorada rigorosamente, e que qualquer desvio seja rapidamente corrigido para alinhar-se com os níveis de apetite de risco estabelecidos.

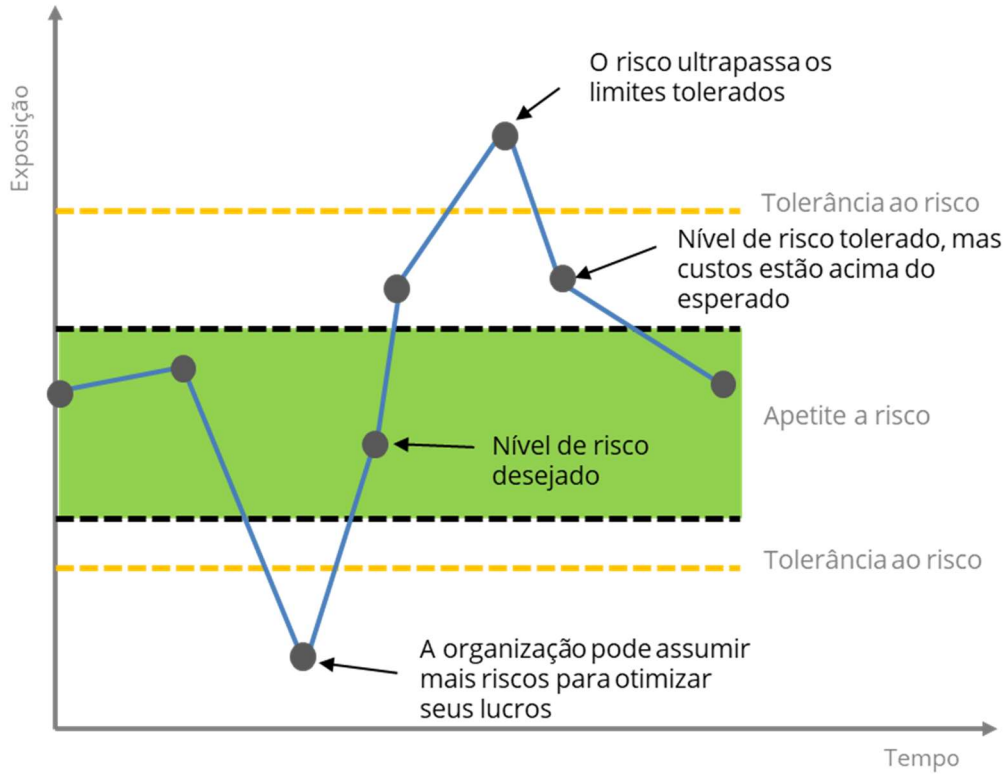
[6] No Serpro, o risco "residual" é referenciado por risco "atual", ou seja, o nível de risco obtido após o tratamento efetuado com os controles implementados.

A comparação do Nível de Risco Atual (NRA) com as faixas de tolerância e apetite de risco estabelece ações claras e responsabilidades para três diferentes situações:

- Quando o NRA está no **nível inaceitável** (fora da faixa de tolerância), devem ser tomadas ações corretivas imediatas e intensificar o monitoramento.
- No **nível tolerável** (dentro da faixa de tolerância), o risco requer monitoramento regular e possível tratamento adicional para evitar que ultrapasse os limites aceitáveis.
- Já no **nível aceitável** (dentro da faixa de apetite), os gestores de risco devem manter o monitoramento padrão e assegurar que os controles permanecem eficazes, garantindo que o risco continue alinhado com os objetivos estratégicos da organização.

A figura a seguir apresenta uma visão gráfica dos conceitos de apetite e tolerância ao risco negativo, em relação à exposição ao risco ao longo do tempo.

Figura 5 *– Apetite e tolerância ao risco em relação à exposição ao risco negativo*



- **Apetite ao Risco:** Representado pela área verde no gráfico, o apetite ao risco corresponde ao nível de exposição a riscos que a organização está disposta a aceitar para atingir seus objetivos.
- **Tolerância ao Risco:** As linhas pontilhadas acima e abaixo do apetite ao risco representam os limites de tolerância. A tolerância ao risco define os níveis máximo e mínimo de exposição que a organização pode suportar antes que sejam necessárias ações corretivas.

- **Exposição ao Risco:** A linha azul demonstra a exposição ao risco real da organização ao longo do tempo. Ela indica as variações nos níveis de risco enfrentados e mostra como esses valores podem oscilar dentro e fora do apetite e tolerância definidos.

A figura destaca a importância de monitorar e gerenciar a exposição ao risco para que ela permaneça dentro dos limites de apetite e tolerância, alinhando a exposição aos objetivos e à capacidade da organização de lidar com riscos.

Essa abordagem estruturada assegura uma gestão proativa e eficaz dos riscos em todos os níveis.

A tabela a seguir detalha as responsabilidades e ações recomendadas para cada situação, facilitando a visualização das medidas necessárias para gerenciar o Nível de Risco Atual (NRa) de acordo com as faixas de tolerância e apetite ao risco estabelecidas pela organização.

Situação	Descrição	Envolvidos	Ações recomendadas
Aceitável: NRA dentro da Faixa de Apetite	O Nível de Risco Atual (NRA) está **dentro da faixa de apetite**, o que significa que o risco está em um nível considerado aceitável e alinhado com os objetivos estratégicos da organização. Nenhuma ação imediata necessária, exceto para monitoramento de rotina.	Gestores, agentes de risco e responsáveis pelos controles.	1. **Monitoramento Padrão:** A 1ª linha deve continuar o monitoramento padrão do risco para assegurar que ele permaneça dentro da faixa de apetite, envolvendo os responsáveis pelos controles. 2. **Manutenção de Controles:** A 1ª linha deve garantir que os controles existentes sejam mantidos e revisados periodicamente para manter sua eficácia, com supervisão da 2ª linha. 3. **Relatórios de Conformidade:** A 2ª linha deve preparar relatórios periódicos para a alta administração, confirmando que os riscos permanecem dentro do apetite e que não são necessárias ações adicionais. 4. **Revisão e Planejamento Estratégico:** Revisar ocasionalmente o apetite ao risco e utilizar a análise de risco projetado para alinhar a estratégia de gestão de riscos com os objetivos de longo prazo.
Tolerável: NRA na Faixa de Tolerância	O Nível de Risco Atual (NRA) está **dentro da faixa de tolerância**, o que significa que, embora o risco seja aceitável temporariamente, ele requer monitoramento contínuo e potencial ação corretiva. Investigar (para verificar e compreender as causas	Alta Administração, Gestores, Agentes de Risco e Responsáveis pelos Controles, com supervisão da 2ª linha (Agentes Corporativos).	1. **Monitoramento Regular:** Os gestores e agentes da 1ª linha devem monitorar regularmente o risco, garantindo que ele não ultrapasse a faixa de tolerância, com supervisão da 2ª linha. 2. **Justificativa e Documentação:** Operações dentro da faixa de tolerância devem ser temporárias e justificadas formalmente, incluindo análise de impacto e plano de mitigação. 3. **Plano de Contingência:** Os gestores e agentes da 1ª linha devem desenvolver ou revisar planos de contingência para ações imediatas, caso o risco aumente.

	subjacentes) e considerar formas de mitigar/evitar dentro de um período especificado		4. **Relatório de Status:** A 1ª e a 2ª linhas devem fornecer atualizações periódicas à alta administração sobre a condição do risco e a eficácia dos controles em vigor.
Inaceitável: NRA Fora da Faixa de Tolerância	O Nível de Risco Atual (NRA) **excede a faixa de tolerância** estabelecida, o que significa que o risco está fora do considerado como aceitável. Tome medidas imediatas para mitigar ou evitar	Alta Administração, Gestores e Agentes de risco, Responsáveis pelos Controles, com supervisão da 2ª linha (Agentes Corporativos). Riscos críticos devem ser levados ao conhecimento dos Conselheiros da organização.	1. **Imediata Revisão e Ação Corretiva:** Os gestores e agentes da 1ª linha, juntamente com a 2ª linha, devem revisar o risco e determinar ações corretivas imediatas. até que ele retorne à faixa de tolerância aceitável. 2. **Revisão de Controles:** A eficácia dos controles existentes deve ser avaliada. É fundamental propor reforços ou novos controles com a participação ativa dos responsáveis por sua implementação. 3. **Justificativa formal:** Os gestores de risco devem justificar e documentar a operação fora da faixa de tolerância, incluindo os motivos da excedência, análise de impacto e plano de ação. 4. **Revisão e Ação Corretiva:** A alta administração deve revisar o risco e determinar ações corretivas imediatas. 5. **Comunicação:** Os Conselhos devem ser informados sobre a situação referente aos riscos críticos, pelo Diretor da área responsável pelo risco.

A **tolerância a riscos** é uma abordagem que se **aplica tanto a riscos negativos** (ameaças), **quanto a positivos** (oportunidades).

A definição das margens de tolerância a riscos é fundamental para o gerenciamento eficaz de risco, permitindo que sejam estabelecidos limites claros para variações aceitáveis. Essas margens refletem o grau de disposição da organização em aceitar desvios em relação aos níveis de apetite a riscos, sejam eles negativos ou positivos. A seguir, são descritas as margens de tolerância para cada nível de apetite, definindo as variações máximas permitidas em cada caso.

6.2.1. Tolerância para riscos negativos

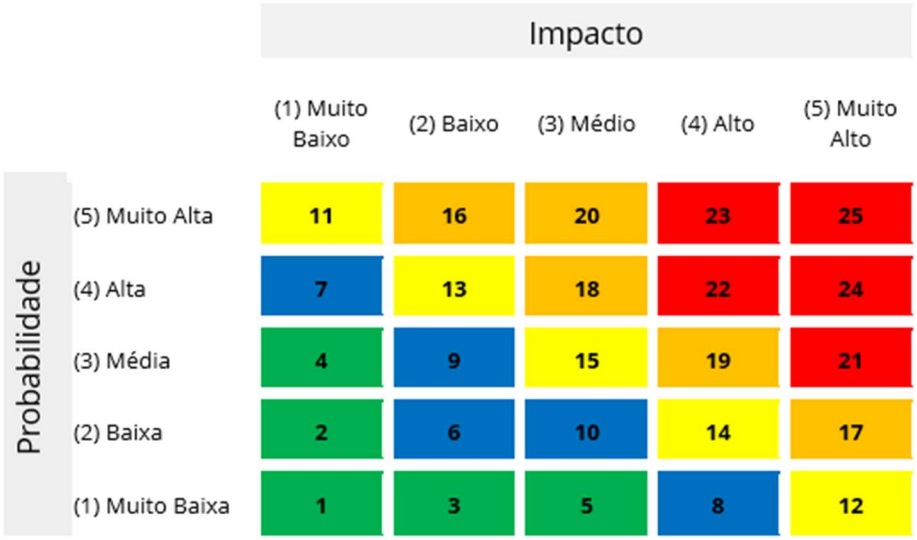
As margens de tolerância a riscos definidas para riscos negativos, em relação ao apetite, são as seguintes:

- Apetite Muito Baixo (Índices 1 a 5)
  - Tolerância: Índices 1 a 6 (variação aceitável de -0 a +1)
- Apetite Baixo (Índices 6 a 10)
  - Tolerância: Índices 4 a 12 (variação aceitável de -2 a +2)
- Apetite Médio (Índices 11 a 15)
  - Tolerância: Índices 9 a 17 (variação aceitável de -2 a +2)
- Apetite Alto (Índices 16 a 20)
  - Tolerância: Índices 13 a 23 (variação aceitável de -3 a +3)
- Apetite Muito Alto (Índices 21 a 25)
  - Tolerância: Índices 18 a 25 (variação aceitável de -3 a +0)

6.2.1.1 Implementação da tolerância para riscos negativos na matriz de riscos

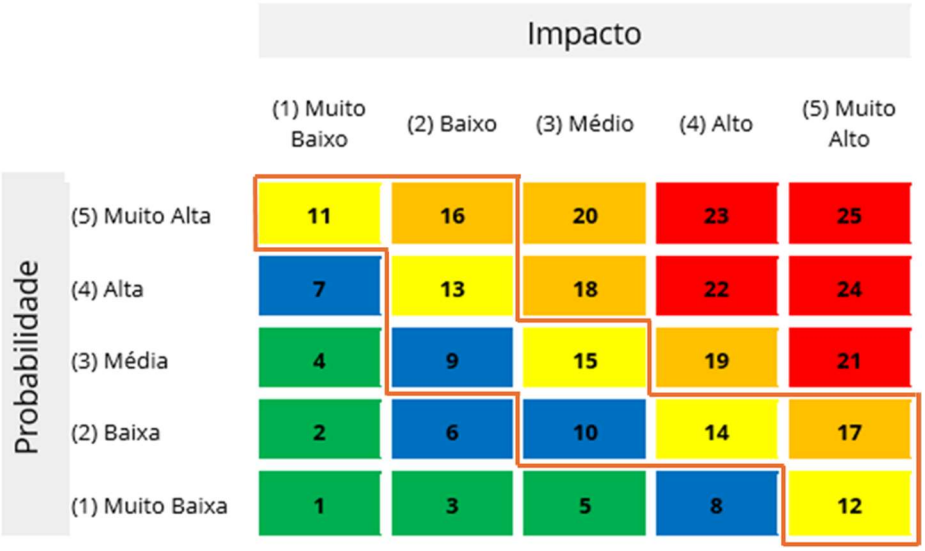
Para cada célula da matriz 5x5, apresentada na figura a seguir, aplica-se a margem de tolerância correspondente ao nível de apetite ao risco, conforme demonstrado anteriormente. Isso cria um intervalo claro para cada faixa de apetite ao risco.

***Figura 6** – Apetite, níveis e índices de risco para riscos negativos*



Como exemplo, o intervalo da tolerância a riscos para apetite médio seria a faixa destacada na figura a seguir, com índices variando entre 9 e 17.

***Figura 7** – Tolerância para riscos negativos – destaque no nível médio*



6.2.2. Tolerância para riscos positivos

Para descrever a tolerância a riscos positivos, adotamos uma abordagem inversa à estabelecida para riscos negativos, aplicando uma matriz de risco que contemple intervalos de tolerância para oportunidades ou riscos positivos.

As margens de tolerância a riscos definidas para riscos positivos, em relação ao apetite, são as seguintes:

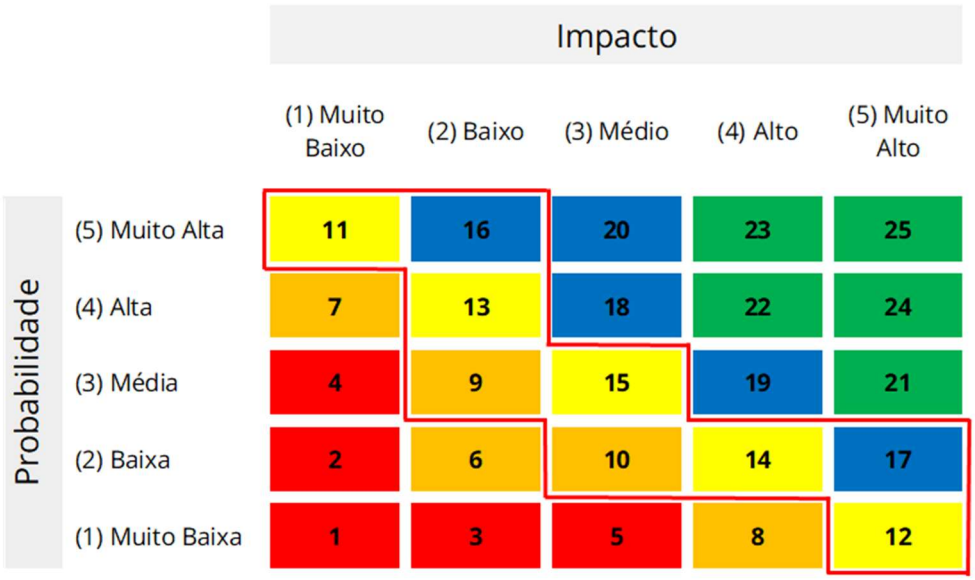
- Apetite Muito Alto (Índices 21 a 25)
  - Tolerância: Índices 21 a 25 (variação aceitável de -1 a -0)
- Apetite Alto (Índices 16 a 20)
  - Tolerância: Índices 14 a 22 (variação aceitável de -2 a +2)
- Apetite Médio (Índices 11 a 15)
  - Tolerância: Índices 9 a 17 (variação aceitável de -2 a +2)
- Apetite Baixo (Índices 6 a 10)
  - Tolerância: Índices 3 a 14 (variação aceitável de -3 a +3)
- Apetite Muito Baixo (Índices 1 a 5)
  - Tolerância: Índices 1 a 8 (variação aceitável de -0 a +3)

6.2.2.1 Implementação da tolerância para riscos positivos na matriz de riscos

Assim como ocorre com os riscos negativos, a matriz 5x5 de riscos também deve contemplar uma faixa de tolerância para os riscos positivos, ajustando-se aos níveis de apetite por oportunidades.

Como exemplo, o intervalo da tolerância a riscos positivos, para apetite médio seria a faixa destacada na figura a seguir, com índices variando entre 9 e 17. Neste caso, coincidente com os níveis de apetite para riscos negativos.

Figura 8 *– Tolerância para riscos positivos – destaque no nível médio*



6.2.3. Integração com a Continuidade de Negócios e Contingência

Na prática, a aplicação da tolerância a riscos está diretamente conectada à articulação entre Planos de Continuidade de Negócios (PCNs) e Planos de Contingência. Os Planos de Contingência oferecem respostas imediatas e específicas para mitigar os impactos de eventos materializados, enquanto os PCNs garantem a manutenção ou retomada das operações críticas de forma estratégica e abrangente. Essa relação operacional reforça a necessidade de respostas alinhadas aos limites de tolerância estabelecidos, assegurando eficácia e resiliência em situações adversas.

6.3. Alinhando Apetite, Tolerância e Estratégia Organizacional

As margens de tolerância oferecem uma faixa aceitável de variação nos níveis de risco, permitindo que a organização aproveite oportunidades e minimize ameaças dentro dos limites seguros. No entanto, é imperativo que a atenção principal esteja sempre voltada para os apetites de risco previamente definidos.

Os níveis de apetite de risco estabelecidos pela organização representam o grau de exposição ao risco que a alta administração está disposta a aceitar em busca de seus objetivos. Esses níveis foram definidos para equilibrar oportunidades e ameaças, garantindo que a organização opere dentro de parâmetros seguros e controlados. Portanto, o tratamento do risco deve sempre buscar manter os níveis de risco dentro dos limites do apetite definido, garantindo uma abordagem consistente e alinhada com a estratégia organizacional.

Embora as faixas de tolerância permitam certa flexibilidade, qualquer decisão de operar fora dos níveis de apetite de risco deve ser justificada e documentada pelo gestor do risco. As variações dentro das margens de tolerância são aceitáveis apenas como exceções, e não devem ser vistas como uma prática comum. A justificativa deve incluir:

a) Motivo da excedência: Razões específicas que levaram à necessidade de operar fora do apetite de risco definido.

b) Análise de impacto: Avaliação detalhada do impacto potencial no alcance dos objetivos estratégicos e operacionais da organização.

c) Plano de ação: Medidas corretivas ou de mitigação a serem implementadas para retornar aos níveis aceitáveis de apetite de risco o mais rápido possível.

Os gestores e agentes de risco, na 1ª linha, são responsáveis por monitorar continuamente os níveis de risco e garantir que estejam alinhados com os apetites definidos. Eles devem ser proativos em identificar qualquer desvio e tomar as ações necessárias para tratar os riscos, envolvendo os responsáveis pelos controles. Qualquer operação dentro das margens de tolerância deve ser temporária e justificada com base em uma análise criteriosa e documentação adequada.

Assim, práticas específicas devem ser adotadas ao aplicar a tolerância ao risco no processo de gestão de riscos, considerando tanto os riscos positivos quanto os negativos:

- **Monitoramento contínuo:** Avaliar continuamente o risco atual para garantir que ele esteja dentro dos limites de tolerância definidos, com vistas a atingir os níveis de apetite.
- **Ações corretivas:** Implementar melhorias ou novos controles se o risco atual exceder a tolerância ao risco.
- **Planejamento estratégico:** Utilizar a análise de risco projetado para planejar melhorias futuras e alinhar a estratégia de gestão de riscos com os objetivos de longo prazo da organização.

6.4. Necessidade de Alinhamento dos Riscos aos Objetivos Organizacionais

Conforme abordado na introdução desta metodologia, na gestão de riscos, é fundamental que os riscos sejam claramente associados aos objetivos da organização. Tradicionalmente, os riscos estratégicos e de negócio estão vinculados aos objetivos e componentes estratégicos, os riscos de projetos estão relacionados aos objetivos dos projetos estratégicos, enquanto os riscos operacionais refletem os objetivos dos processos organizacionais.

No entanto, a organização deve reconhecer que uma variedade de objetivos — além dos objetivos estratégicos, operacionais, de projeto e de negócios — pode ser afetada tanto por riscos positivos quanto negativos. Além disso, objetivos mais amplos e de relevância global, como os Objetivos de Desenvolvimento Sustentável (ODS), precisam ser integrados ao escopo de gestão de riscos, dado seu valor crescente no contexto organizacional e de sustentabilidade.

Com a crescente preocupação global com as questões relacionadas ao meio ambiente, à equidade social e à transparência nas operações corporativas, a gestão de riscos ESG emerge como uma necessidade fundamental também para as empresas de TI como o Serpro. Vincular riscos, a serem identificados, aos Objetivos de Desenvolvimento Sustentável (ODS) é crucial para uma gestão eficaz, conectando desafios organizacionais a metas globais. Esta abordagem não apenas fortalece a resiliência interna, mas também demonstra comprometimento com a sustentabilidade global. Reconhecendo que riscos derivam tanto do **ambiente interno quanto externo**, essa associação permite uma visão holística, integrando práticas sustentáveis na tomada de decisões e contribuindo para um impacto positivo mais amplo.

Os 17 Objetivos de Desenvolvimento Sustentável – ODS são apresentados na figura a seguir.

Figura 9 – Os 17 Objetivos de Desenvolvimento Sustentável (ODS)

Essa abordagem facilita uma visão coerente e alinhada, permitindo que a gestão de riscos contribua diretamente para o alcance dos objetivos organizacionais, incluindo aqueles que apoiam a responsabilidade social e a sustentabilidade.

A orientação sobre a necessidade de vínculo dos ODS à cada tipo de risco (estratégico, de negócio, de projeto ou operacional) deve ser conduzida em consonância com as diretrizes estratégicas definidas pela empresa, reforçada pelas definições do Plano de Gestão de Riscos e Controles, apresentado no item 5 desta Metodologia. Isso deve ser observado durante a fase de Definição do Escopo e Contexto do processo de identificação dos riscos, de acordo com o tipo de risco. Esta fase será apresentada nas próximas seções desta metodologia.

7. METODOLOGIA PARA GESTÃO DE RISCOS OPERACIONAIS

A Metodologia de Gestão de Riscos Operacionais e Controles do Serpro propõe-se a estabelecer e estruturar as etapas necessárias para a gestão de riscos operacionais, tendo como principal insumo os processos definidos por meio da Cadeia de Valor e/ou Arquitetura de Processos do Serpro.

Deverá ser aplicada para identificação dos riscos operacionais, de forma a permitir a elaboração de matrizes de riscos, planos de ação para tratamento de riscos e indicadores de sua evolução. Estes resultados permitirão aos gestores visualizarem, de forma estruturada, o apetite aos riscos e diretrizes gerais para o gerenciamento de riscos e controles.

Em conformidade com a ISO 31000:2018, o Processo de Gestão de Riscos e Controles é definido por meio das seguintes etapas, a saber:

a) definição de escopo e contexto;

b) identificação e análise dos riscos;

c) avaliação dos riscos e verificação dos controles;

d) priorização dos riscos;

e) definição dos controles de respostas aos riscos;

f) validação dos resultados;

g) registro, relato e contingência;

h) comunicação e consulta; e

i) análise crítica e monitoramento.

Figura 10 *– Processo de Gestão de Riscos Operacionais*

Fonte: *NBR ISO 31000 – fev.2018 (adaptado)*

A aplicação da metodologia de gestão de riscos operacionais e controles do Serpro é **descentralizada**, ou seja, as Unidades Organizacionais devem executar o processo de gerenciamento de riscos na Unidade Organizacional sob sua responsabilidade, com base nas diretrizes e orientações apresentadas neste documento.

A área de Gestão de Riscos e Controles está apta a prestar o apoio às Unidades Organizacionais, durante todas as etapas do processo, apoiando e orientando quanto à correta aplicação deste processo.

7.1. Definição de escopo e contexto

O escopo dos riscos operacionais diz respeito a todos os processos componentes da Cadeia de Valor do Serpro, considerando objetivos pertinentes às unidades e o alinhamento aos objetivos organizacionais.

A aplicação desta metodologia ao processo organizacional de cada Superintendência será conduzida pela própria Unidade Organizacional, com auxílio do Agente de Riscos (Agentes GRCI) capacitado pela área de Gestão de Riscos e Controles.

A construção da percepção do ambiente externo da organização envolve analisar as ameaças e oportunidades para a organização, ou seja, na fase de definição de escopo e

contexto, devem ser definidos os critérios de riscos a serem identificados, analisados e tratados nas etapas seguintes.

7.1.1. Critérios de riscos

As mesmas fontes de incertezas, causadoras de novas ameaças e destruidoras de valor, são também geradoras de uma vasta gama de oportunidades potenciais e opções de inovação para as organizações.

a) Riscos negativos: Na gestão de riscos negativos, a organização analisa suas fontes de risco de forma a identificar eventos que caracterizem ameaças com consequências negativas (perdas) sobre os resultados da organização.

Nesta versão da Metodologia, a gestão de **riscos negativos** deve ser considerada no escopo de **Riscos Operacionais, Riscos de Projetos Estratégicos, Riscos Estratégicos e Riscos ao Negócio.**

b) Riscos positivos: Na gestão de riscos positivos devem ser avaliados os fatores de riscos de forma a identificar eventos que podem alavancar as oportunidades e quais serão as consequências positivas (ganhos) para a organização.

Nesta versão da Metodologia, a **gestão de riscos positivos** deve ser considerada apenas no escopo de **Riscos Estratégicos e Riscos ao Negócio.**

O **contexto externo** inclui, mas não está limitado a:

a) Fatores sociais, culturais, políticos, jurídicos, regulatórios, financeiros, tecnológicos, econômicos e ambientais, em âmbito internacional, nacional, regional ou local;

b) Direcionadores-chave e tendências que afetam os objetivos da organização;

c) Relacionamentos, percepções, valores, necessidades e expectativas das partes interessadas externas;

d) Relações e compromissos contratuais; e

e) Complexidade das redes de relacionamento e dependências.

O **contexto interno** é composto pelos elementos da própria organização como visão, missão, valores, governança, estrutura organizacional, papéis e responsabilidades, cultura organizacional, normas, estratégia, políticas e capacidades em termos de recursos e conhecimento. Os fatores internos podem influenciar nos critérios de riscos (riscos negativos e/ou riscos positivos) a serem tratados pela organização. O contexto interno, para os riscos operacionais, deve ser orientado pelos objetivos da organização e da própria Unidade Organizacional, pelos processos e seus objetivos, além do Apetite a Riscos, **por tipologia**[7], declarado no RAS.

[7] As tipologias serão descritas em detalhes na seção 7.2.1 desta Metodologia.

7.2. Identificação e análise dos riscos

Um evento é uma ocorrência ou mudança em um conjunto específico de circunstâncias. A identificação dos riscos é o processo de encontrar, reconhecer e registrar eventos que podem interferir no alcance dos objetivos, seja do processo (riscos operacionais), do projeto (riscos de projetos estratégicos) ou da organização (riscos estratégicos).

A definição de um objetivo claro é premissa para uma adequada identificação de riscos. Ressalta-se o foco na qualidade da informação, tendo como propósito que a matéria prima gerada deve subsidiar a tomada de decisão e/ou proteger o valor da empresa.

Atenção! A Gestão de Riscos e Controles não é um fim em si mesma. Tenha claro o escopo e o propósito das informações geradas, não a deixe pesada ao ponto de se tornar não gerenciável. Riscos devem ser **poucos**, **bons** e **gerenciáveis**.

Os principais objetivos apontados na etapa anterior são parâmetros para a identificação e classificação dos riscos. Portanto, os eventos que impactem a consecução de um determinado objetivo deverão ser identificados como risco.

A ausência da formalização do processo não inviabiliza a identificação e Gestão de Riscos e Controles operacionais, pois risco é o efeito da incerteza sobre o **objetivo.**

Os riscos podem ser identificados a partir de perguntas, como: “quais eventos podem prejudicar (ou atrasar, ou impedir) o atingimento de um ou mais objetivos?

O risco será descrito nos termos abaixo:

a) Causa: fato gerador responsável pela ocorrência do risco;

b) Risco: evento de risco associado ao objetivo geral ou específico;

c) Consequência: possível impacto nos objetivos definidos, caso o risco se materialize.

Figura 11 *– Relação entre Causa, Evento e Consequência do Risco*

Os riscos identificados são monitorados, priorizando aqueles com maior Nível de Risco, considerando o Apetite a Risco, para os quais são elaborados planos de ação para seu tratamento. Ou seja, o monitoramento (e consequente tratamento) dos riscos deve se dar dos que possuem níveis de risco mais altos para os mais baixos. Tais pontos serão vistos adiante neste documento.

Os riscos operacionais identificados pelo Serpro podem ser classificados das seguintes formas:

7.2.1. Quanto à tipologia

Para cada risco, deve ser definida uma tipologia que mais se relaciona ao risco. A definição da tipologia deve ser associada às causas do risco, para saber a que se relacionam de forma a identificar a tipologia mais adequada". As principais causas de riscos representam os fatores fundamentais que podem desencadear ou contribuir para a manifestação de eventos indesejados (riscos negativos) ou desejados (riscos positivos). Ao associar essas causas às tipologias de riscos, a organização estabelece uma estrutura que reflete a realidade operacional e estratégica em que está inserida.

A estrutura apresentada a seguir, agrupa as tipologias em categorias amplas (financeiros, de operação, legais e/ou conformidade, governança e gestão, etc.) e, em seguida, são desdobradas em subcategorias mais específicas, por exemplo, crédito, investimento, liquidez e mercado, associadas à categoria de riscos financeiros. Essa hierarquia ajuda a organizar os riscos em um formato lógico e compreensível.

- **Riscos financeiros:**
  - **Atuarial:** Risco relacionado à não concretização de premissas atuariais utilizadas, seja pela Entidade Fechada de Previdência Complementar, podendo gerar déficits com impactos no Serpro, como patrocinadora, seja pela própria empresa, no tocante ao Plano de Assistência à Saúde, podendo gerar insuficiência de contribuições para sustentabilidade do benefício.
  - **Crédito**: risco relacionado à adimplência ou inadimplência de clientes ou contrapartes, que pode resultar em ganhos ou perdas financeiras e afetar o balanço patrimonial da empresa de forma positiva ou negativa.
  - **Investimento (aplicações financeiras)**: risco relacionado às decisões de investimento ou à volatilidade dos mercados, podendo resultar em perdas ou ganhos financeiros significativos.
  - **Investimento (despesas de capital):** risco relacionado às decisões de investimento ou à volatilidade dos mercados, podendo resultar em perdas ou ganhos financeiros significativos.
  - **Liquidez**: risco relacionado ao capital disponível para cumprir obrigações financeiras, podendo afetar, positivamente ou negativamente, a capacidade da empresa em honrar pagamentos e suas operações diárias, em decorrência da materialização dos demais riscos listados nos riscos financeiros e nas demais categorias. O risco de liquidez está associado a eventos de curto prazo, ou seja, quando os ativos precisam ser altamente líquidos para garantir a operação e manutenção (fornecedores, tributos, salários, etc) da empresa, ou longo prazo, quando se espera que os passivos de longo prazo (passivos judiciais, benefícios pós emprego) sejam cobertos pelos ativos totais, inclusive os ilíquidos.

- **Mercado**: risco relacionado às flutuações nos preços de ativos financeiros, taxas de juros, câmbio, entre outros, que possa afetar os investimentos e a rentabilidade da empresa, de forma positiva ou negativa.

- **Riscos de operação:**
  - **Aquisições e Contratações:** risco relacionado às relações com fornecedores, que possam beneficiar ou prejudicar a disponibilidade de matéria-prima, produtos ou serviços essenciais para as operações da empresa.
  - **Infraestrutura predial**: risco relacionado a falhas ou melhoria nas instalações prediais da empresa, podendo impactar de forma negativa ou positiva nas atividades operacionais ou de serviços essenciais para a continuidade do negócio.
  - **Pessoas**: risco negativo ou positivo relacionado a questões trabalhistas, força de trabalho, composição do quadro de pessoas, saúde e segurança no trabalho, recompensar pessoas, política de remuneração, programa de qualidade de vida no trabalho, jornada e frequência, responsabilidade social, clima e cultura organizacional, serviços de apoio a gestão de pessoas, greves, desempenho de empregados, falta de habilidades ou recursos humanos insuficientes no corpo funcional, que podem afetar a produtividade, a satisfação dos funcionários e a capacidade de atrair e reter talentos.
  - **Privacidade e proteção de dados pessoais:** risco negativo ou positivo relacionado à violação ou proteção de dados pessoais, à conformidade no tratamento de dados pessoais, à implementação eficaz de *privacy by design* nos processos internos ou soluções desenvolvidas pelo Serpro, ao gerenciamento de dados pessoais, ao cumprimento pelos colaboradores de suas responsabilidades em relação aos tratamentos de dados pessoais, ao cumprimento de regulamentações de privacidade e proteção de dados pessoais, e ao atendimento de direitos dos titulares.
  - **Processos**: risco relacionado a falhas/ineficiências ou melhorias/eficiência nos processos internos da empresa, o que pode afetar na produtividade ou qualidade empresarial.
  - **Segurança – GRSI:** tem por objetivo agrupar, exclusivamente, os riscos decorrentes da aplicação da Gestão de Riscos Simplificada (GRS), coordenada pela Área de Segurança da Informação. O anexo 1C apresenta o Método específico para a Gestão de Risco de Segurança – GRSI, alinhado com esta Metodologia.
  - **Segurança da informação:** risco relacionado a falhas ou melhorias na proteção de infraestrutura de nuvem, servidores, sistemas, redes e dados

contra ameaças cibernéticas, incluindo ataques de *hackers*, *malware*, *phishing*, acesso não autorizado a dados e interrupções de serviços.

- **Riscos legais e/ou conformidade:** risco positivo ou negativo relacionado a eventos derivados do cumprimento ou descumprimento de leis, regulamentos ou normas aplicáveis que impactam as atividades da empresa, oportunizando melhorias ou novos negócios para o Serpro ou sujeitando-o a multas, penalidades, ações judiciais, perda de licenças, dentre outros.
- **Riscos de governança e gestão:**
  - **Capacidade gerencial:** risco relacionado às habilidades, competências ou experiências adequadas nos gestores da empresa. Pode estar relacionado ao planejamento e preparação para a sucessão de cargos-chave na organização, incluindo cargos de liderança, o que pode impactar positivamente ou negativamente a eficiência operacional, a tomada de decisões, a continuidade dos negócios e a estabilidade organizacional.
  - **Concorrência**: refere-se à dinâmica do mercado, incluindo a intensificação da competição, a entrada de novos concorrentes e as mudanças na participação de mercado. Isso pode exigir adaptações estratégicas para manter ou melhorar a competitividade da organização, representando tanto oportunidades para crescimento quanto desafios que podem impactar a posição no mercado.
  - **Estratégia**: risco positivo ou negativo relacionado a decisões estratégicas ou de planejamento, podendo resultar em vantagens competitivas ou desvantagens para a empresa.
  - **Imagem/reputação:** eventos que podem afetar positiva ou negativamente a confiança da sociedade, parceiros, clientes ou fornecedores em relação à capacidade do órgão ou da entidade em cumprir sua missão institucional.
  - **Inovação**: Risco relacionado à atividade de pesquisa, desenvolvimento e inovação, envolvendo a criação de novos produtos, serviços ou processos. Em situações positivas, a inovação pode impulsionar a competitividade, abrir novos mercados e fortalecer a posição da empresa. No entanto, em cenários negativos, desafios durante o processo de inovação, como atrasos ou custos inesperados, podem impactar negativamente os resultados.
  - **Tecnologia**: Risco positivo ou negativo relacionado ao direcionamento tecnológico, criação e ciclo de vida de produtos, bem como à melhoria, aquisição ou criação de novas tecnologias, que podem resultar em vantagens competitivas, crescimento, eficiência ou desafios para a organização.
- **Riscos à integridade:** ações, omissões ou vulnerabilidades que possam favorecer ou dificultar a ocorrência de práticas de corrupção, fraude,

irregularidade, desvio ético e/ou de conduta, impactando tanto positiva quanto negativamente a consecução dos objetivos organizacionais. O anexo 1A apresenta o Método específico para a Gestão de Riscos à Integridade, alinhado com esta Metodologia.

- **Casos fortuitos ou de força maior:**
  - **Desastres não naturais:** risco relacionado a atos terroristas, guerras, invasões, incêndios ou outros eventos não naturais, que podem ter impactos negativos ou positivos nas operações da empresa, dependendo das medidas de prevenção, segurança e resiliência implementadas.
  - **Desastres naturais:** risco relacionado a inundação, ventania, desabamento, sismo, tempestade elétrica, incêndio ou outros eventos de causas naturais, que podem impactar negativa ou positivamente as operações da empresa, dependendo das medidas de preparação e resiliência implementadas.

Vale lembrar que, não raro, um risco pode estar relacionado a mais de uma tipologia, contudo sempre existirá uma que é mais dominante em relação às demais.

7.2.2. Quanto aos controles

a) Risco inerente: refere-se ao cenário inicial. Demonstra o Nível de Risco a que a organização está exposta no momento de mapeamento dos riscos, sem considerar os controles existentes ou propostos.

b) Risco atual (residual): refere-se ao cenário atual (“onde estamos”). Demonstra o Nível de Risco a que a organização está exposta considerando-se a implementação dos controles existentes no momento da avaliação do risco. As informações são dinâmicas e os níveis se alteram conforme tratamento das causas (controles preventivos / redução da probabilidade de ocorrência do risco negativo / aumento da probabilidade de ocorrência do risco positivo) ou tratamento das possíveis consequências (controles contingenciais / redução do impacto do risco negativo / ampliação do impacto do risco positivo).

Nota de esclarecimento: Por ser uma empresa criada em **1964**, inserida em um contexto maduro de processos internos, com atividades executadas há décadas, a **maioria dos riscos nascem residuais**, exceto os vinculados a projetos e a novos processos.

c)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. Caso não seja necessário o tratamento do risco, ou seja, a estratégia adotada seja "aceitar", o risco projetado terá os mesmos níveis de probabilidade e impacto do risco atual.

7.2.3. Quanto à abrangência

a) Riscos Transversais: Quando mais de uma área tiver atuação relevante no gerenciamento do risco ou controle interno recomenda-se que o gestor de risco seja da área mais intimamente ligada às causas ou consequências do risco. Assim, o gestor do risco ou executor do controle interno pode estar em área diferente do gestor do processo/projeto/estratégia, porém é imprescindível uma comunicação entre gestor do risco e executor dos controles, deixando claro os papéis e as responsabilidades que cada um desempenhará para reduzir o Nível de Risco. Caso esse gestor não tenha influência decisória sobre as demais áreas envolvidas ou enfrente dificuldades no tratamento transversal, as decisões poderão ser tomadas de forma colegiada, por meio dos comitês táticos (COGRC) quando envolverem superintendências dentro da mesma Diretoria, ou por meio do Comitê Estratégico (COGRS) quando envolver Superintendências de Diretorias distintas. Em ambos os casos, as Unidades Organizacionais podem contar com apoio da Área de Gestão de Riscos e Controles.

b) Riscos Funcionais: a área entende, trata e gerencia apenas os riscos relativos às atividades que lhe são inerentes e, portanto, somente ela tem atuação sobre o risco.

7.2.4. Quanto ao critério

a) Riscos negativos: Na gestão de riscos negativos, a organização analisa suas fontes de risco de forma a identificar eventos (ameaças) com consequências negativas (perdas) sobre os resultados da organização. O foco encontra-se no acompanhamento de fatores que podem tornar vulnerável o alcance dos objetivos (do processo, do projeto ou da estratégia da organização).

Nesta versão da Metodologia, a gestão de **riscos negativos** deve ser considerada no escopo de **Riscos Operacionais, Riscos de Projetos Estratégicos e Riscos Estratégicos.**

b) Riscos positivos: A gestão de riscos positivos utilizará a mesma metodologia para mapeamento dos riscos negativos. Somente haverá a mudança de ótica. O gestor terá que pensar sempre em fatores de riscos que podem alavancar as oportunidades e quais serão as consequências positivas para o Serpro, em termos de imagem, financeiro, legal, operacional *etc*. Neste sentido, com o interesse em atuar de maneira proativa nas suas fontes de incerteza, alavancando, rapidamente, oportunidades lucrativas para a organização, é necessário responder à seguinte pergunta: *quais são as deficiências e vulnerabilidades em termos de pessoas, processos e sistemas que impedem que os ganhos de uma oportunidade potencial sejam explorados no limite?* Materializando esta ideia, pode-se pensar nos métodos e ferramentas que a gestão de riscos positivos deve aplicar para orientar a

organização a identificar e mitigar suas principais deficiências e vulnerabilidades no que tange a sua capacidade de aproveitar "oportunidades".
Para reforçar o entendimento do risco positivo é necessário que se entenda o que não é risco positivo:

- eventos completamente inesperados que geram ganhos para a organização sem que haja um planejamento prévio (ganho por acaso);
- não se deve confundir a excelência da gestão de riscos negativos com a gestão de riscos positivos;
- uma gestão de riscos positivos ineficiente pode parecer uma gestão de riscos negativos;
- apenas ter sorte não significa gerir riscos positivos.

Nesta versão da Metodologia, a gestão de **riscos positivos** deve ser considerada apenas para os **Riscos Estratégicos e Riscos ao Negócio.**

7.3. Avaliação dos riscos e verificação dos controles

O entendimento dos riscos, causas, consequências, Nível de Risco Atual, cenários, controles existentes e sua eficácia fornecem informações para as decisões sobre o tratamento de riscos. Durante esta etapa, o risco é mensurado em termos de probabilidade e impacto.

7.3.1. Controles

Controles são as medidas que mantêm e/ou modificam o risco. Eles são criados para levar o Nível de Risco Atual (NRA) ao Nível de Risco Projetado (NRP) buscando, sempre que possível, atingir o Nível de Apetite associado ao risco. Controles incluem, mas não estão limitados a processo, norma, política, dispositivo, prática, ou outras condições e/ou ações que mantêm ou modificam riscos.

Os controles podem ser do tipo:

a) Preventivo: atua sobre as possíveis causas do risco, com o objetivo de prevenir a sua ocorrência, no caso de riscos negativos, ou reforçá-la nos riscos positivos. Exemplos de controles preventivos: requisitos ou *checklist* definidos para o processo, capacitação dos empregados; ou

b) Contingencial: é um controle previamente definido para ser executado quando ocorrer a materialização do risco, com o intuito de diminuir o impacto de suas consequências para os riscos negativos ou aproveitar ao máximo a oportunidade identificada, no caso de riscos positivos. Exemplos de controles de atenuação e recuperação: plano de contingência, tomada de contas especiais e procedimento apuratório. Exemplos de controles de adaptação positiva: capacitação adicional da equipe, diversificar parcerias estratégicas.

Alguns controles podem servir tanto como **controles preventivos quanto contingenciais.** A **distinção** está relacionada ao **momento** em que esses controles são **utilizados**.

Além disso, quanto à implementação, pode ser:

a) Existente: o controle foi implementado/concluído por meio de uma atividade em funcionamento ou artefato vigente;

b) Em melhoria: controle pré-existente, mas que necessita de melhoria. Importante destacar que o controle existente atua no Nível de Risco Atual enquanto o controle melhorado deve ser considerado no Nível de Risco Projetado; Após a sua implementação, passa a ser um controle existente, substituindo o anterior; ou

c) Proposto: é um novo controle que deve ser implementado para alterar o Nível de Risco, buscando atingir o Nível de Risco Projetado.

A descrição dos controles existentes consiste no detalhamento dos controles utilizados para tratar o risco. Os controles a serem melhorados ou novos controles propostos devem ter responsáveis definidos e data inicial e final previstas.

Os controles podem nem sempre exercer o efeito modificador pretendido, e por isso, poderão ser objeto de verificação de controle (testes de *walkthrough*, no caso de riscos estratégicos e ao negócio), pela 1ª. e 2ª. Linha ou testes de controle, pela 3ª. Linha.

Não há dúvidas de que o conceito do propósito ou intenção da gestão de riscos é de caráter subjetivo na diferenciação entre oportunidades ou ameaças. Contudo, é inquestionável afirmar que a maneira como o gestor entende e descreve o evento incerto irá afetar significativamente o conjunto de controles propostos para seu tratamento e natureza dos ganhos resultantes.

7.3.2. Visão integrada sobre riscos positivos, negativos e seus controles

A Figura 12 demonstra um diagrama de comparação entre risco positivo e negativo, consolidando todos os elementos até aqui apresentados.

Figura 12 *– Estrutura de Gestão de Riscos Estratégicos Positivos e Negativos*

Fonte*: Gestão de riscos positivos – André Macieira, Daniel Karrer, Leandro Jesus, Rafael Clemente / Editora Sicurezza*

Para melhor entendimento dos elementos da figura acima, a tabela a seguir destaca a correspondência de cada elemento, seja para risco positivo ou negativo. Diferenças que reforçam o entendimento de que a Gestão de riscos negativos e positivos reside e destaca-se fortemente no foco da aplicação realizada pela organização.

Tabela 3 *– Correspondência dos elementos da Gestão de Riscos Estratégicos Positivos e Negativos*

Elementos	Risco negativo	Risco positivo
Eventos	Ameaças	Oportunidades
Fontes de Riscos	Fontes de Riscos (causas)	Fontes de Riscos (causas)
Consequências	Negativas (perdas)	Positivas (ganhos)
Controle	Diminuir a probabilidade de concretização das ameaças	Tirar o máximo proveito das oportunidades identificadas
Incerteza	Fonte de Perda	Fonte de ganhos
Objetivo	Reduzir suas consequências indesejáveis	Elevar (alavancar) tanto a probabilidade de ocorrência quanto a magnitude de suas consequências.

Nota-se que controles podem ser utilizados tanto para diminuir a probabilidade ou impacto das ameaças quanto para alavancar a probabilidade ou impacto das oportunidades.

A avaliação da probabilidade e do impacto de cada risco, deve ser considerada com base nos critérios definidos nas tabelas apresentadas a seguir. A classificação com o olhar sistêmico/corporativo é importante para que a matriz de riscos não tenha uma visão distorcida quanto a prioridade do tratamento.

7.3.3. Definição do Nível de Risco (NR)

Os eventos que podem interferir na consecução dos objetivos do processo são analisados em termos de probabilidade e impacto, que serão utilizados na definição do Nível de Risco (NR), conforme descrição a seguir.

A **Probabilidade** é a chance de o evento de risco acontecer, ou seja, é o quanto um evento de risco está sujeito a algum tipo de ameaça, dentro de determinado período. Deve ser pontuado em valores inteiros de 1 a 5, conforme descrições da Tabela 4, considerando-se o período de um ano.

Tabela 4 *– Probabilidade do Risco – descrição e valores*

Probabilidade/ Valor atribuído	Descrição
Muito Baixa (MB=1)	Raro. Em situações excepcionais, o evento poderá se efetivar, mas nada nas circunstâncias indica essa possibilidade, uma vez que políticas e procedimentos para controles preventivos são bem projetados, em caso de riscos negativos ou inexistentes em caso de riscos positivos.
Baixa (B=2)	Pouco provável. A efetivação do evento parece difícil, pois as circunstâncias pouco indicam essa possibilidade, uma vez que políticas e procedimentos para controles preventivos estão completos, em caso de riscos negativos ou são insuficientemente implementados, em caso de riscos positivos.
Média (M=3)	Provável. De alguma forma, o evento poderá se efetivar, pois as circunstâncias indicam moderadamente essa possibilidade, uma vez que políticas e procedimentos para controles preventivos são mais prováveis do que não completos, tanto para o caso de riscos negativos quanto riscos positivos.
Alta (A=4)	Muito Provável. De forma até esperada, o evento poderá se efetivar, pois as circunstâncias indicam fortemente essa possibilidade, uma vez que políticas e procedimentos para controles preventivos são insuficientemente implementados em caso de riscos negativos ou bem projetados, em caso de riscos positivos.
Muito Alta (MA=5)	Praticamente certo. De forma inequívoca, o evento poderá se efetivar, pois as circunstâncias indicam claramente essa possibilidade, uma vez que políticas e procedimentos para controles preventivos são inexistentes em caso de riscos negativos ou bem projetados em caso de riscos positivos.

Fonte*: Gestão de Riscos – Avaliação da Maturidade (TCU, 2018) – Adaptada*

A **probabilidade** está associada às causas fontes do risco.

O **impacto** está relacionado ao resultado de um evento que afeta, positivamente ou negativamente, os objetivos da empresa, caso o evento ocorra, ou seja, caso o risco (negativo ou positivo) se materialize. Deve ser pontuado em valores inteiros de 1 a 5, conforme referenciais descritos nas Tabelas 5 a 10, utilizando a tipologia majoritariamente relacionada às consequências do risco. As tabelas são válidas tanto para riscos positivos (no caso de riscos estratégicos e Riscos ao Negócio), quanto para riscos negativos, exceto quando houver ressalvas explicitas

Tabela 5 *– Categoria: Riscos Financeiros – Impacto do Risco por tipologia – descrição e valores*

Impacto	Tipologia / Descrição do impacto nos objetivos (Consequências)					
	Crédito	**Investimento (aplicações financeiras)**	**Investimento (despesas de capital)**	**Liquidez**	**Mercado**	**Atuarial**
Muito Baixo (MB=1)	Significa que o risco de crédito resulta em um impacto mínimo no alcance dos objetivos do processo ou das atividades, não afetando substancialmente a capacidade de alcançar a maioria dos objetivos/resultados de crédito. Pode gerar impacto financeiro insignificante: < 1% sobre a receita do Serpro.	Sugere que os investimentos têm um impacto mínimo no alcance dos objetivos do processo ou das atividades, não afetando substancialmente a capacidade de alcançar a maioria dos objetivos/resultados de investimento Pode gerar impacto financeiro insignificante: < 1% sobre a receita do Serpro.	Sugere que os investimentos têm um impacto mínimo no alcance dos objetivos do processo ou das atividades, não afetando substancialmente a capacidade de alcançar a maioria dos objetivos/resultados de investimento Pode gerar impacto financeiro insignificante: < 1% sobre a receita do Serpro.	O impacto na liquidez é mínimo no alcance dos objetivos do processo ou das atividades, não afetando substancialmente a capacidade de alcançar a maioria dos objetivos/resultados. Pode gerar impacto financeiro insignificante: < 1% sobre a receita do Serpro.	Sugere que as flutuações no mercado têm um impacto mínimo no alcance dos objetivos do processo ou das atividades de mercado, não afetando substancialmente a capacidade de alcançar a maioria dos objetivos/resultados. Pode gerar impacto financeiro insignificante: < 1% sobre a receita do Serpro.	Sugere que o passivo atuarial tem impacto mínimo no alcance dos objetivos, não afetando substancialmente a capacidade de alcançar a maioria dos objetivos/resultado. Pode gerar impacto econômico-financeiro insignificante: < 1% sobre a receita do Serpro
Baixo (B=2)	Indica que há alguma preocupação com o risco de crédito, mas isso não afeta significativamente a capacidade da organização de atingir a maioria de seus objetivos. Pode haver um impacto leve no alcance dos objetivos de crédito, mas	Indica que os investimentos têm alguma influência, mas não são impactantes. Pode haver um impacto leve no alcance dos objetivos do investimento, do processo ou das atividades de investimento, mas não se espera que seja substancial e não impacta a	Indica que os investimentos têm alguma influência, mas não são impactantes. Pode haver um impacto leve no alcance dos objetivos do investimento, do processo ou das atividades de investimento, mas não se espera que seja substancial e não impacta a	Sugere que o impacto na liquidez é de pequena magnitude. Isso resulta em um impacto que afeta em alguma medida o alcance dos objetivos do processo ou das atividades, mas não coloca em risco a possibilidade de alcançar a maioria dos	indica que as flutuações de mercado têm alguma influência, mas não são benéficos ou prejudiciais. Pode haver um impacto leve no alcance dos objetivos do processo ou das atividades de mercado, mas não se espera que seja substancial e não afeta a realização da maioria	Indica que o passivo atuarial tem influência, mas gera baixo impacto. Pode haver impacto no alcance dos objetivos relativos ao nível de endividamento, ao processo e às atividades, mas não se espera que seja substancial e não afeta a maioria dos objetivos e resultados. Pode

Impacto	Tipologia / Descrição do impacto nos objetivos (Consequências)					
	Crédito	**Investimento (aplicações financeiras)**	**Investimento (despesas de capital)**	**Liquidez**	**Mercado**	**Atuarial**
	não se espera que seja substancial. Isso pode gerar um impacto financeiro pequeno, equivalente a ≥1% e < 3% sobre a receita do Serpro.	realização da maioria dos objetivos. Pode gerar impacto financeiro pequeno: ≥1% < 3% sobre a receita do Serpro.	realização da maioria dos objetivos. Pode gerar impacto financeiro pequeno: ≥1% < 3% sobre a receita do Serpro.	objetivos/resultados. Pode gerar impacto financeiro pequeno: ≥1% < 3% sobre a receita do Serpro.	dos objetivos. Pode gerar impacto financeiro pequeno: ≥1% < 3% sobre a receita do Serpro.	gerar impacto econômico-financeiro pequeno: ≥1% < 3% sobre a receita do Serpro.
Médio (M=3)	Reflete uma preocupação moderada com o risco de crédito. Isso resulta em um impacto significativo no alcance dos objetivos do processo ou das atividades. Pode gerar impacto financeiro moderado, equivalente a ≥ 3% e < 10% sobre a receita do Serpro.	Reflete que os investimentos têm um impacto significativo. Isso resulta em um impacto significativo no alcance dos objetivos do investimento, do processo ou das atividades. Pode gerar impacto financeiro moderado: ≥ 3% < 10% sobre a receita do Serpro.	Reflete que os investimentos têm um impacto significativo. Isso resulta em um impacto significativo no alcance dos objetivos do investimento, do processo ou das atividades. Pode gerar impacto financeiro moderado: ≥ 3% < 10% sobre a receita do Serpro.	Reflete um impacto de magnitude moderada na liquidez. Isso resulta em um impacto significativo no alcance dos objetivos do processo ou das atividades. Pode gerar impacto financeiro moderado: ≥ 3% < 10% sobre a receita do Serpro.	Reflete que as flutuações do mercado têm um impacto significativo. Isso resulta em um impacto significativo no alcance dos objetivos do processo ou das atividades. Pode gerar impacto financeiro moderado: ≥ 3% < 10% sobre a receita do Serpro	Reflete um impacto moderado do passivo atuarial, resultando em um impacto relevante no alcance dos objetivos relativos ao nível de endividamento, ao processo e às atividades, com impacto médio na maioria dos objetivos e resultados. Pode gerar impacto econômico-financeiro moderado: ≥3% < 10% sobre a receita do Serpro.
Alto (A=4)	Indica que a preocupação com o risco de crédito é considerável. Isso resulta em um impacto alto no alcance dos objetivos do	Indica que os investimentos têm um impacto substancial. Isso resulta em um impacto alto no alcance dos	Indica que os investimentos têm um impacto substancial. Isso resulta em um impacto alto no alcance dos	Indica que o impacto na liquidez é considerável. Isso resulta em um impacto alto no alcance dos objetivos do processo ou das	Indica que as flutuações do mercado têm um impacto substancial. Isso resulta em um impacto alto no alcance dos objetivos	Indica que o passivo atuarial tem impacto substancial. Isso resulta em um alto impacto no alcance dos objetivos relativos ao nível de

Impacto	Tipologia / Descrição do impacto nos objetivos (Consequências)					
	Crédito	**Investimento (aplicações financeiras)**	**Investimento (despesas de capital)**	**Liquidez**	**Mercado**	**Atuarial**
	processo ou das atividades. Pode gerar impacto financeiro grande, equivalente a ≥ 10% e < 25% sobre a receita do Serpro.	objetivos do investimento, do processo ou das atividades. Pode gerar impacto financeiro grande: ≥ 10% < 25% sobre a receita do Serpro.	objetivos do investimento, do processo ou das atividades. Pode gerar impacto financeiro grande: ≥ 10% < 25% sobre a receita do Serpro.	atividades. Pode gerar impacto financeiro grande: ≥ 10% < 25% sobre a receita do Serpro.	do processo ou das atividades. Pode gerar impacto financeiro grande: ≥ 10% < 25% sobre a receita do Serpro.	endividamento, ao processo e às atividades. Pode gerar impacto econômico-financeiro grande: ≥10% < 25% sobre a receita do Serpro.
Muito Alto (MA=5)	Sugere uma preocupação extrema com o risco de crédito. Isso resulta em um impacto muito alto no alcance dos objetivos do processo ou das atividades de crédito, com a possibilidade de afetar diversos aspectos, incluindo processos, sistemas, aspectos comerciais e financeiros, e até mesmo a continuidade das operações. Pode gerar impacto financeiro que modifica significativamente a continuidade das	Sugere que os investimentos têm um impacto extremamente significativo. Isso resulta em um impacto muito alto no alcance dos objetivos do processo ou das atividades de investimento e a possibilidade de afetar diversos aspectos, incluindo processos, sistemas, aspectos comerciais e financeiros, e até mesmo a continuidade das operações. Pode gerar impacto financeiro que modifica significativamente a	Sugere que os investimentos têm um impacto extremamente significativo. Isso resulta em um impacto muito alto no alcance dos objetivos do processo ou das atividades de investimento e a possibilidade de afetar diversos aspectos, incluindo processos, sistemas, aspectos comerciais e financeiros, e até mesmo a continuidade das operações. Pode gerar impacto financeiro que modifica significativamente a	Sugere que o impacto na liquidez é de magnitude extrema. Isso resulta em um impacto muito alto no alcance dos objetivos do processo ou das atividades e a possibilidade de afetar diversos aspectos, incluindo processos, sistemas, aspectos comerciais e financeiros, e até mesmo a continuidade das operações. Pode gerar impacto financeiro que modifica significativamente a continuidade das operações do Serpro: ≥ 25% sobre a receita.	Sugere que as flutuações do mercado têm um impacto extremamente significativo. Isso resulta em um impacto muito alto no alcance dos objetivos do processo ou das atividades e a possibilidade de afetar diversos aspectos, incluindo processos, sistemas, aspectos comerciais e financeiros, e até mesmo a continuidade das operações. Pode gerar impacto financeiro que modifica significativamente a continuidade das operações do Serpro: ≥ 25% sobre a receita.	Sugere que o impacto no passivo atuarial é de magnitude extrema. Isso resulta em um impacto muito alto no alcance dos objetivos relacionados ao nível de endividamento, ao processo ou às atividades e a possibilidade de afetar diversos aspectos, incluindo processos, sistemas, aspectos comerciais e financeiros, e até mesmo a continuidade das operações. Pode gerar impacto econômico-financeiro que modifica significativamente a continuidade das operações do Serpro:

Impacto	Tipologia / Descrição do impacto nos objetivos (Consequências)					
	Crédito	**Investimento (aplicações financeiras)**	**Investimento (despesas de capital)**	**Liquidez**	**Mercado**	**Atuarial**
	operações do Serpro, representando ≥ 25% sobre a receita.	continuidade das operações do Serpro: ≥ 25% sobre a receita.	continuidade das operações do Serpro: ≥ 25% sobre a receita.			≥ 25% sobre a receita.

Tabela 6 *– Categoria: Riscos de Operação – Impacto do Risco por tipologia – descrição e valores*

Impacto	Tipologia / Descrição do impacto nos objetivos (Consequências)			
	Aquisições e Contratações	**Infraestrutura predial**	**Pessoas**	**Privacidade e Proteção de Dados Pessoais**
Muito Baixo (MB=1)	Sugere que as aquisições e contratações têm um impacto mínimo. Isso resulta em um impacto mínimo no alcance dos objetivos do processo ou das atividades de aquisições e contratações, não afetando substancialmente a capacidade de alcançar a maioria dos objetivos/resultados nessa área.	Sugere que os riscos nessa área têm um impacto mínimo. Isso resulta em um impacto mínimo no alcance dos objetivos do processo ou das atividades relacionadas à infraestrutura predial, não afetando substancialmente a capacidade de alcançar a maioria dos objetivos/resultados nessa área.	Impacto circunscrito a um profissional ou percentual reduzido de pessoas/equipes (até 20%) atuantes no processo/área.	Sob a ótica da organização, não envolve tratamento crítico de dados pessoais [8] e há possibilidade de impacto insignificante para a organização (financeira, imagem/reputação, segurança da informação, outras). Sob a ótica do titular de dado pessoal [9], os titulares de dados pessoais não serão afetados.
Baixo (B=2)	Indica que as aquisições e contratações têm alguma influência, mas não são prejudiciais. Pode haver um impacto leve no alcance dos objetivos do processo ou das atividades de aquisições e contratações, mas não se espera que seja substancial e não impede a realização da maioria dos objetivos.	Indica que os riscos nessa área têm alguma influência, mas não são prejudiciais. Pode haver um impacto leve no alcance dos objetivos do processo ou das atividades relacionadas à infraestrutura predial, mas não se espera que seja substancial e não impede a realização da maioria dos objetivos.	Impacto percentual reduzido de pessoas/equipes (de 20% a 40%) atuantes no processo/área.	Sob a ótica da organização, não envolve tratamento crítico de dados pessoais (*) e há possibilidade de baixo impacto para a organização (financeira, imagem/reputação, segurança da informação, outras). Sob a ótica do titular de dado pessoal (**), os titulares de dados pessoais poderão encontrar alguns inconvenientes, os quais serão superados sem nenhum problema (tempo gasto reinserindo informações, aborrecimentos, irritações, dentre outros.), no caso de riscos negativos.
Médio	Reflete que as aquisições e contratações	Reflete que os riscos nessa área têm um	Moderado impacto no	Sob a ótica da organização, não envolve tratamento crítico

[8] (*) Tratamento crítico de dados pessoais é considerado sempre que um tratamento envolver dados sensíveis ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, ou tiver o potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade. Da mesma forma, deve-se considerar o volume de dados envolvido, o quantitativo de indivíduos afetados, a boa-fé e as intenções dos terceiros que terão acesso aos dados após o incidente e a facilidade de identificação dos titulares por terceiros não autorizados. Ou seja, é considerado um tratamento crítico de dados pessoais quando há possibilidade de risco ou dano relevante para seus titulares.

[9] (**) Riscos oriundos do RIPD (Relatório de Impacto à Proteção de Dados Pessoais) devem ter seu nível de impacto avaliado sob a ótica do titular de dado pessoal.

Impacto	Tipologia / Descrição do impacto nos objetivos (Consequências)			
	Aquisições e Contratações	**Infraestrutura predial**	**Pessoas**	**Privacidade e Proteção de Dados Pessoais**
(M=3)	têm um impacto significativo. Isso resulta em um impacto significativo no alcance dos objetivos do processo ou das atividades de aquisições e contratações, com reflexos na imagem, mas sem impactos pecuniários significativos.	impacto significativo. Isso resulta em um impacto significativo no alcance dos objetivos do processo ou das atividades relacionadas à infraestrutura predial, com reflexos na imagem, mas sem impactos pecuniários significativos.	capital humano, atingindo percentual moderado de pessoas/equipes (de 40% a 60%) atuantes no processo/área.	de dados pessoais (*) e há possibilidade de impacto moderado para a organização (financeira, imagem/reputação, segurança da informação, outras). Sob a ótica do titular de dado pessoal (**), os titulares de dados pessoais podem encontrar inconvenientes significativos, que eles serão capazes de superar, apesar de algumas dificuldades (custos extras, negação de acesso a serviços de negócios, medo, falta de entendimento, estresse, pequenas doenças físicas, dentre outras.), no caso de riscos negativos.
Alto (A=4)	Indica que as aquisições e contratações têm um impacto substancial. Isso resulta em um impacto alto no alcance dos objetivos do processo ou das atividades de aquisições e contratações, com reflexos na imagem/reputação e pode ter consequências econômicas e financeiras.	Indica que os riscos nessa área têm um impacto substancial. Isso resulta em um impacto alto no alcance dos objetivos do processo ou das atividades relacionadas à infraestrutura predial, com reflexos na imagem/reputação e pode ter consequências econômicas e financeiras. Os prejuízos/ benefícios exigem ação estratégica para mitigar/ampliar os efeitos sobre a imagem e reputação do Serpro.	Impacto significativo no capital humano, atingindo grande percentual de pessoas/equipes (de 60% a 80%) atuantes no processo/área.	Sob a ótica da organização, envolve tratamento crítico de dados pessoais (*) e há possibilidade de impacto alto para a organização (financeira, imagem/reputação, segurança da informação, outras). Sob a ótica do titular de dado pessoal (**), os titulares de dados pessoais podem encontrar consequências significativas, que convém que sejam capazes de superar, embora com sérias dificuldades (apropriação indevida de fundos, lista negra de bancos, danos à propriedade, perda de emprego, intimação, piora do estado de saúde, dentre outras.), no caso de riscos negativos.
Muito Alto (MA=5)	Sugere que as aquisições e contratações têm um impacto extremamente significativo. Isso resulta em um impacto muito alto no alcance dos objetivos do processo ou das atividades de aquisições e contratações,	Sugere que os riscos nessa área têm um impacto extremamente significativo. Isso resulta em um impacto muito alto no alcance dos objetivos do processo ou das atividades relacionadas à infraestrutura predial, com reflexos significativos na	Impacto significativo no capital humano, atingindo percentual crítico de pessoas/equipes (de 80% a 100%) atuantes	Sob a ótica da organização, envolve tratamento crítico de dados pessoais (*) e há possibilidade de impacto significativo para a organização (financeira, imagem/reputação, segurança da informação, outras). Sob a ótica do titular de dado pessoal (**), os titulares de Dados Pessoais podem encontrar consequências

Impacto	Tipologia / Descrição do impacto nos objetivos (Consequências)			
	Aquisições e Contratações	**Infraestrutura predial**	**Pessoas**	**Privacidade e Proteção de Dados Pessoais**
	com reflexos significativos na imagem/reputação e a possibilidade de afetar diversos aspectos, incluindo processos, sistemas, aspectos comerciais e financeiros, e até mesmo a continuidade das operações.	imagem/reputação e a possibilidade de afetar diversos aspectos, incluindo processos, sistemas, aspectos comerciais e financeiros, e até mesmo a continuidade das operações.	no processo/área e/ou profissionais de mercado com potencial perspectiva de ingresso no quadro do Serpro.	significativas, ou mesmo irreversíveis, que não podem superar (dificuldades financeiras, como dívidas não prestáveis ou incapacidade de trabalhar, doenças físicas ou psicológicas a longo prazo, morte, dentre outras.), no caso de riscos negativos.

Tabela 6 (continuação) *– Categoria: Riscos de Operação – Impacto do Risco por tipologia – descrição e valores*

Impacto	Tipologia / Descrição do impacto nos objetivos (Consequências)		
	Processos	**Segurança – GRSI**	**Segurança da Informação**
Muito Baixo (MB=1)	Impactos irrelevantes na eficiência ou nos resultados do processo. Não há interferência em processos de outras áreas.	A materialização do risco pode afetar de forma insignificante os recursos, processos e/ou sistemas envolvidos.	A materialização do risco pode afetar de forma insignificante os recursos, processos e/ou sistemas envolvidos.
Baixo (B=2)	Impactos mínimos na eficiência ou nos resultados do processo. Não há interferência em processos de outras áreas.	A materialização do risco pode afetar os recursos, processos e/ou sistemas envolvidos, mas a implementação de controles é simples.	A materialização do risco pode afetar os recursos, processos e/ou sistemas envolvidos, mas a implementação de controles é simples.
Médio (M=3)	Alguns resultados podem ser afetados, causando impacto na eficiência do processo ou nas entregas para outros processos.	A materialização do risco causa pequeno impacto nos recursos, processos e/ou sistemas envolvidos, mas a implementação de controles é viável.	A materialização do risco causa pequeno impacto nos recursos, processos e/ou sistemas envolvidos, mas a implementação de controles é viável.
Alto (A=4)	Alto impacto na eficiência ou resultados do processo. Há interferência na execução de outros processos de negócio, demonstrada pelo indicador do processo (quando disponível).	A materialização do risco causa impacto significativo em vários recursos, processos e/ou sistemas e a implementação de controles é complexa.	A materialização do risco causa impacto significativo em vários recursos, processos e/ou sistemas e a implementação de controles é complexa.
Muito Alto (MA=5)	Altíssimo impacto na eficiência ou resultados do processo ou outros processos críticos, podendo ocasionar prejuízos/benefícios em serviços ou sistemas críticos do Serpro, demonstrada pelo indicador do processo (quando disponível).	A materialização do risco causa impactos significativos para os recursos, processos e/ou sistemas. A implementação de controles é complexa e acarreta impactos ao negócio.	A materialização do risco causa impactos significativos para os recursos, processos e/ou sistemas. A implementação de controles é complexa e acarreta impactos ao negócio.

Tabela 7 *– Categoria: Riscos Legais e de conformidade – Impacto do Risco por tipologia – descrição e valores*

Impacto	Tipologia / Descrição do impacto nos objetivos (Consequências)
	Legais e/ou Conformidade
Muito Baixo (MB=1)	Os efeitos da materialização do risco são meramente formais e podem ser absorvidos pelas atividades, com pouco ou nenhum impacto no alcance de objetivos ou cumprimento de atividades operacionais, e sem repercussões significativas na atuação da gestão do risco.
Baixo (B=2)	Os efeitos da materialização do risco ainda podem ser absorvidos pelas atividades, com baixo impacto no alcance de objetivos ou cumprimento de atividades operacionais, e requerem ações de caráter orientativo pela gestão do risco.
Médio (M=3)	Os efeitos da materialização do risco são significativos, porém ainda podem ser tratados em condições normais de operação. Acarretam impactos consideráveis no alcance de objetivos e/ou cumprimento de atividades operacionais. Tais efeitos demandam ações de caráter corretivo/potencializador pela gestão do risco, porém sem impactos pecuniários significativos.
Alto (A=4)	Os efeitos da materialização do risco são muito significativos. Acarretam impactos no alcance de objetivos da Unidade. Tais efeitos demandam ações de caráter corretivo/potencializador pela gestão do risco, com repercussões pecuniárias relevantes ao Serpro e possível responsabilização de gestores e empregados em caso de impactos negativos.
Muito Alto (MA=5)	Os efeitos da materialização do risco são de alto impacto e podem interromper/potencializar a execução de serviços. Demandam intervenção imediata da gestão e/ou Direção. Acarretam impactos relevantes no alcance de objetivos da Unidade e/ou no cumprimento da missão do Serpro, com repercussões pecuniárias relevantes e responsabilização de gestores em caso de impactos negativos.

***Tabela 8** – Categoria: Riscos de governança e gestão – Impacto do Risco por tipologia – descrição e valores*

Tipologia	Tipologia / Descrição do impacto nos objetivos (Consequências)		
	Capacidade gerencial	**Concorrência**	**Estratégia**
Muito Baixo (MB=1)	Sugere que os riscos nessa área têm um impacto mínimo no alcance dos objetivos do processo ou das atividades relacionadas à capacidade gerencial, não afetando substancialmente a capacidade de alcançar a maioria dos objetivos/resultados nessa área.	Sugere que os riscos nessa área têm um impacto mínimo no alcance dos objetivos do processo ou das atividades relacionadas à concorrência, não afetando substancialmente a capacidade de competir no mercado.	Resulta em um impacto mínimo no alcance dos objetivos estratégicos da organização, não afetando substancialmente a capacidade de atingir a maioria dos objetivos/resultados estratégicos.
Baixo (B=2)	Pode haver um impacto leve no alcance dos objetivos do processo ou das atividades relacionadas à capacidade gerencial, mas não se espera que seja substancial e não impede a realização da maioria dos objetivos.	Pode haver um impacto leve no alcance dos objetivos do processo ou das atividades relacionadas à concorrência, mas não se espera que seja substancial em relação ao mercado.	Pode haver um impacto leve no alcance dos objetivos estratégicos da organização, mas não se espera que seja substancial, mantendo a trajetória estratégica.
Médio (M=3)	Reflete que os riscos nessa área têm um impacto significativo no alcance dos objetivos do processo ou das atividades relacionadas à capacidade gerencial, com reflexos na imagem, mas sem impactos pecuniários significativos.	Reflete que os riscos nessa área não apresentam impactos significativos, positivos ou negativos. Isso implica que não há grande influência nas atividades relacionadas à concorrência, mantendo um equilíbrio competitivo no mercado.	Implica que não há grande influência nas atividades estratégicas da organização, mantendo uma trajetória estável.
Alto (A=4)	Indica que os riscos nessa área têm um impacto substancial Isso resulta em um impacto alto no alcance dos objetivos do processo ou das atividades relacionadas à capacidade gerencial, com reflexos na imagem/reputação e pode ter consequências econômicas e financeiras.	Indica que os riscos nessa área têm um impacto substancial, seja positivo ou negativo. Isso resulta em um impacto alto no alcance dos objetivos do processo ou das atividades relacionadas à concorrência, podendo afetar substancialmente a posição competitiva da organização.	Indica que os riscos nessa área têm um impacto substancial, seja positivo ou negativo. Isso resulta em um impacto alto no alcance dos objetivos estratégicos da organização, podendo afetar substancialmente a direção estratégica ou o desempenho.
Muito Alto	Sugere que os riscos nessa área têm um impacto	Sugere que os riscos nessa área têm um impacto	Sugere que os riscos nessa área têm um impacto

Tipologia	Tipologia / Descrição do impacto nos objetivos (Consequências)		
	Capacidade gerencial	**Concorrência**	**Estratégia**
(MA=5)	extremamente significativo no alcance dos objetivos do processo ou das atividades relacionadas à capacidade gerencial, com reflexos significativos na imagem/reputação e a possibilidade de afetar diversos aspectos, incluindo processos, sistemas, aspectos comerciais e financeiros, e até mesmo a continuidade das operações.	extremamente significativo, positivo ou negativo. Isso pode resultar em um impacto muito alto no alcance dos objetivos do processo ou das atividades relacionadas à concorrência, podendo causar mudanças substanciais na dinâmica do mercado, inviabilizando ou tornando a empresa líder entre os competidores.	extremamente significativo, positivo ou negativo, superando fortemente ou inviabilizando as metas traçadas. Isso pode resultar em um impacto muito alto no alcance dos objetivos estratégicos da organização, com reflexos significativos na imagem/reputação e a possibilidade de afetar diversos aspectos, incluindo processos, sistemas, aspectos comerciais e financeiros, e até mesmo a continuidade das operações.

Tabela 8 (continuação) *– Categoria: Riscos de governança e gestão – Impacto do Risco por tipologia – descrição e valores*

Tipologia	Tipologia / Descrição do impacto nos objetivos (Consequências)		
	Imagem / Reputação	**Tecnologia**	**Inovação**
Muito Baixo (MB=1)	Impactos leves à imagem do Serpro cuja repercussão se dará por pouquíssimo tempo e as ações de reversão/ potencialização se limitam a esforços de comunicação junto ao público envolvido.	Positivo: Pequenas melhorias tecnológicas que trazem benefícios internos, como eficiência operacional marginal ou redução de custos. Negativo: Desafios técnicos menores que são prontamente superados, sem impacto significativo nas operações ou na estratégia da empresa.	Positivo: Pequenas melhorias incrementais que não têm um impacto significativo nos resultados financeiros ou na posição de mercado da empresa. Inovações pouco percebidas pelos clientes. Negativo: Desafios menores durante o processo de inovação que são prontamente superados sem afetar substancialmente os resultados ou prazos.
Baixo (B=2)	Impacto com potencial de repercutir na imagem ou reputação do Serpro, por pouco tempo e baixo alcance. As ações de reversão/potencialização se consolidam de forma coordenada entre diversas áreas da instituição.	Positivo: Adoção bem-sucedida de novas tecnologias que melhoram a eficiência operacional e contribuem para a competitividade. Negativo: Desafios moderados na implementação de tecnologias, resultando em atrasos ou custos adicionais, mas gerenciáveis sem prejudicar substancialmente os objetivos estratégicos.	Positivo: Introdução bem-sucedida de produtos ou serviços inovadores no mercado, resultando em um aumento moderado de participação e visibilidade. Negativo: Desafios moderados durante a inovação que podem causar atrasos ou custos adicionais, mas que são gerenciáveis sem prejudicar gravemente os objetivos estratégicos.
Médio (M=3)	Impacto com potencial de repercutir de forma localizada e moderada na imagem ou reputação do Serpro. Os prejuízos/benefícios exigem ação coordenada entre diversas áreas da instituição para mitigar/ampliar os efeitos sobre a imagem e reputação do Serpro	Positivo: Desenvolvimento de produtos tecnológicos bem-recebidos pelo mercado, aumentando a participação da empresa e gerando receitas adicionais. Negativo: Desafios tecnológicos significativos que podem levar a atrasos substanciais ou custos mais elevados. Requer ajustes nos planos estratégicos, mas a empresa ainda pode se recuperar.	Positivo: Lançamento bem-sucedido de produtos ou serviços inovadores que geram impacto significativo no mercado e na lucratividade. Negativo: Desafios consideráveis durante a inovação, resultando em atrasos substanciais ou custos significativos. Pode exigir ajustes nos planos estratégicos, mas a empresa ainda pode se recuperar.
Alto (A=4)	Impacto com potencial de repercutir de forma substancial na imagem ou reputação do Serpro, em âmbito nacional.	Positivo: Inovações tecnológicas que conferem uma vantagem competitiva significativa no mercado e impulsionam o crescimento.	Positivo: Inovações que transformam significativamente o mercado, proporcionando à empresa uma vantagem competitiva duradoura.

Tipologia	Tipologia / Descrição do impacto nos objetivos (Consequências)		
	Imagem / Reputação	**Tecnologia**	**Inovação**
	Os prejuízos/ benefícios exigem ação estratégica para mitigar/ampliar os efeitos sobre a imagem e reputação do Serpro.	Negativo: Desafios sérios na implementação de tecnologias que podem impactar substancialmente os resultados financeiros e a posição da empresa. Exige uma reavaliação completa das estratégias de tecnologia e pode levar a revisões nos objetivos de curto prazo.	Negativo: Desafios sérios durante a inovação que podem impactar severamente os resultados financeiros e a posição de mercado. Requer uma reavaliação completa das estratégias de inovação e pode levar a revisões nos objetivos de curto prazo.
Muito Alto (MA=5)	Impacto que apresenta altíssimo potencial de repercutir na imagem e reputação do Serpro, cuja alteração é difícil ou improvável a curto ou médio prazo.	Positivo: Desenvolvimento de tecnologias revolucionárias que transformam o setor e solidificam a empresa como líder inovadora. Negativo: Desafios catastróficos na direção tecnológica que têm o potencial de comprometer seriamente a viabilidade a longo prazo da empresa. Necessita de intervenções significativas e uma reavaliação completa das estratégias de tecnologia.	Positivo: Inovações revolucionárias que redefinem completamente o mercado e consolidam a empresa como líder incontestável. Negativo: Desafios catastróficos durante a inovação que têm o potencial de comprometer seriamente a viabilidade a longo prazo da empresa. Necessita de intervenções significativas e uma reavaliação completa das estratégias.

Tabela 9 *– Categoria: Riscos à Integridade – Impacto do Risco por tipologia – descrição e valores*

Impacto	**Tipologia / Descrição do impacto nos objetivos (Consequências)**
	À Integridade
Muito Baixo (MB=1)	Impacta minimamente o alcance dos objetivos do processo ou das atividades.
Baixo (B=2)	Impacta em alguma medida o alcance dos objetivos do processo ou das atividades, mas não altera a possibilidade de alcance da maior parte dos objetivos/resultados.
Médio (M=3)	Impacta significativamente o alcance dos objetivos do processo ou das atividades, com reflexo na imagem do Serpro, porém sem impactos pecuniários significativos.
Alto (A=4)	Impacto alto no alcance dos objetivos do processo ou das atividades, com reflexo na imagem/ reputação do Serpro, com consequências econômico/ financeiras.
Muito Alto (MA=5)	Impacto muito alto no alcance dos objetivos do processo ou das atividades, com reflexo na imagem/ reputação do Serpro. Também pode acarretar consequências nos processos/ sistemas, comercial/ financeiro, ou na continuidade das operações do Serpro.

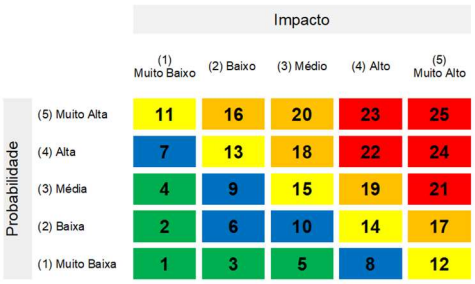
***Tabela 10** – Categoria: Casos fortuitos ou de força maior – Impacto do Risco por tipologia – descrição e valores*

Impacto	Tipologia / Descrição do impacto nos objetivos (Consequências)	
	Desastres não naturais	**Desastres naturais**
Muito Baixo (MB=1)	Impacto muito baixo em riscos de desastres não naturais sugere que a organização possui medidas altamente eficazes de prevenção, segurança e resiliência. Isso resulta em um impacto mínimo no alcance dos objetivos do processo ou das atividades, mantendo a continuidade das operações e a estabilidade organizacional, seja em situações positivas ou negativas.	Impacto muito baixo em riscos de desastres naturais sugere que a organização possui medidas excepcionalmente eficazes de preparação e resiliência. Isso resulta em um impacto mínimo no alcance dos objetivos do processo ou das atividades, mantendo a continuidade das operações e a estabilidade organizacional, seja em situações positivas ou negativas.
Baixo (B=2)	Impacto baixo em riscos de desastres não naturais indica que a organização possui medidas eficazes de prevenção, segurança e resiliência. Pode haver um impacto leve no alcance dos objetivos do processo ou das atividades, mas não se espera que seja substancial, mantendo a continuidade das operações e a estabilidade organizacional, seja em situações positivas ou negativas.	Impacto baixo em riscos de desastres naturais indica que a organização possui medidas eficazes de preparação e resiliência. Pode haver um impacto leve no alcance dos objetivos do processo ou das atividades, mas não se espera que seja substancial, mantendo a continuidade das operações e a estabilidade organizacional, seja em situações positivas ou negativas.
Médio (M=3)	Impacto médio em riscos de desastres não naturais reflete que, apesar das medidas de prevenção, o impacto desses eventos pode ter efeitos significativos. Isso resulta em um impacto que afeta consideravelmente o alcance dos objetivos do processo ou das atividades, exigindo respostas e adaptações mais substanciais, mas ainda mantendo a continuidade e estabilidade em certa medida, seja em situações positivas ou negativas.	Impacto médio em riscos de desastres naturais reflete que, apesar das medidas de preparação, o impacto desses eventos pode ter efeitos significativos. Isso resulta em um impacto que afeta consideravelmente o alcance dos objetivos do processo ou das atividades, exigindo respostas e adaptações mais substanciais, mas ainda mantendo a continuidade e estabilidade em certa medida, seja em situações positivas ou negativas.
Alto (A=4)	Impacto alto em riscos de desastres não naturais indica que, apesar das medidas de prevenção, o impacto desses eventos é substancial. Isso resulta em um impacto que afeta substancialmente o alcance dos objetivos do processo ou das atividades, exigindo respostas e adaptações significativas, com reflexos na imagem/reputação e possíveis consequências econômicas e financeiras, seja em situações positivas ou negativas.	Impacto alto em riscos de desastres naturais indica que, apesar das medidas de preparação, o impacto desses eventos é substancial. Isso resulta em um impacto que afeta substancialmente o alcance dos objetivos do processo ou das atividades, exigindo respostas e adaptações significativas, com reflexos na imagem/reputação e possíveis consequências econômicas e financeiras, seja em situações positivas ou negativas.

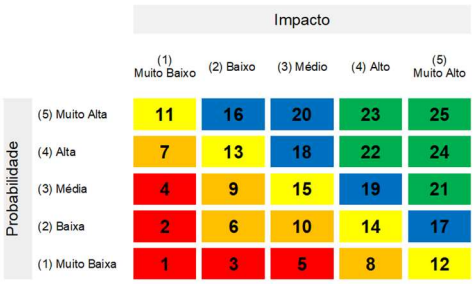
Impacto	Tipologia / Descrição do impacto nos objetivos (Consequências)	
	Desastres não naturais	**Desastres naturais**
Muito Alto (MA=5)	Impacto muito alto em riscos de desastres não naturais sugere que o impacto desses eventos é extremamente significativo, mesmo com medidas de prevenção robustas. Isso resulta em um impacto muito alto no alcance dos objetivos do processo ou das atividades, com reflexos significativos na imagem/reputação e a possibilidade de afetar diversos aspectos, incluindo processos, sistemas, aspectos comerciais e financeiros, e até mesmo a continuidade das operações, seja em situações positivas ou negativas.	Impacto muito alto em riscos de desastres naturais sugere que o impacto desses eventos é extremamente significativo, mesmo com medidas de preparação robustas. Isso resulta em um impacto muito alto no alcance dos objetivos do processo ou das atividades, com reflexos significativos na imagem/reputação e a possibilidade de afetar diversos aspectos, incluindo processos, sistemas, aspectos comerciais e financeiros, e até mesmo a continuidade das operações, seja em situações positivas ou negativas.

Os índices de risco são obtidos pelo cruzamento entre os níveis de probabilidade e de impacto de cada risco. Os índices estão grafados em cada célula das matrizes da Figura 13. Confrontando-se o índice de risco obtido, tomando por base os quadros da Figura 14, obtém-se o Nível de Risco, tanto para riscos negativos quanto positivos.

Figura 13 – *Níveis de risco e índices para riscos negativos e positivos*



Riscos negativos



Riscos positivos

Figura 14 *– Relação entre níveis de apetite, risco e índices de riscos negativos e positivos*

Cor	Nível de Apetite / Nível de Risco	Índices de Risco correlacionados
Verde	Muito Baixo (1)	1 a 5
Azul	Baixo (2)	6 a 10
Amarelo	Médio (3)	11 a 15
Laranja	Alto (4)	16 a 20
Vermelho	Multo Alto (5)	21 a 25

Riscos negativos

Cor	Nível de Apetite / Nível de Risco	Índices de Risco correlacionados
Vermelho	Muito Baixo (1)	1 a 5
Laranja	Baixo (2)	6 a 10
Amarelo	Médio (3)	11 a 15
Azul	Alto (4)	16 a 20
Verde	Multo Alto (5)	21 a 25

Riscos positivos

Como exemplo, para um risco de Probabilidade Baixa (2) e Impacto Médio (3), o seu Índice de Risco possui o valor 10, conforme observamos na Figura 13. Nesse caso, o NR é Baixo (2), uma vez que o índice de risco 10 (dez) se encontra nos intervalos do Nível de Risco azul, para risco negativo, ou laranja, para risco positivo, conforme constatamos na Figura 14.

O NR pode ser definido para três cenários distintos:

a) Nível de Risco Inerente (NRI) é definido para os riscos em sua forma intrínseca, ou seja, sem a atuação de controles. O NRI é gerado pela relação entre a probabilidade inerente e o impacto inerente. O NRI deve ser definido nesta fase do processo de gestão de riscos;

b) Nível de Risco Atual (**NRA**) é definido para os riscos considerando-se os controles já implementados. O NRA é gerado pela relação entre a probabilidade atual e o impacto atual. O NRA deve ser definido durante esta fase do processo de gestão de riscos; e

c) Nível de Risco Projetado (NRP) é definido a partir da projeção ou expectativa de probabilidade e impacto, após a implementação dos controles propostos ou a melhoria dos controles existentes. O NRP é gerado pela relação entre a probabilidade projetada e o impacto projetado. O NRP deve buscar atender ao Nível de Apetite

relacionado ao risco e será abordado em mais detalhes em fase seguinte do processo de gestão de riscos, quando são definidos os controles de resposta aos riscos necessários a reduzir o Nível de Risco negativo ou ampliar o nível de risco positivo.

Para cada risco deve ser adotada uma estratégia de resposta. Após a definição do Nível de Risco Atual, identifica-se e avalia-se a efetividade de políticas, procedimentos, técnicas e ferramentas, ou seja, os controles, que têm por objetivo diminuir ou aumentar o Nível de Risco e, assim, aumentar a probabilidade do alcance dos objetivos organizacionais.

De acordo com o Nível de Risco Atual, o critério do risco (positivo ou negativo), o Apetite a Risco definido e os recursos necessários para implementação do controle (análise custo *versus* benefício), será possível decidir qual a estratégia mais adequada, dentre as opções ilustradas nas Tabelas 11 e 12, para riscos negativos ou positivos, respectivamente:

Tabela 11 *– Opções de estratégia de resposta aos riscos negativos*

Estratégia	Descrição
Evitar	Decisão de não se envolver ou agir de forma a se retirar de uma situação de risco.
Tratar	Um risco negativo normalmente é tratado de forma a ser reduzido quando o seu NRA está acima do Apetite a Riscos definido. O tratamento é realizado por meio dos controles, contingenciais e preventivos, que diminuem, respectivamente, as consequências e as causas dos riscos.
Transferir	Transferir um risco para terceiros, transferindo os impactos e responsabilidades. O risco não é eliminado e, quase sempre, envolve o pagamento de prêmios para a parte que está assumindo o risco. Exemplo: contratação de seguro.
Aceitar	Um risco negativo geralmente é aceito quando o seu NRA está dentro do Apetite a Riscos ou quando não exige ações adicionais, ou seja, quando não há necessidade de novos controles ou melhoria dos existentes. Em certos casos os controles definidos não são suficientes para se atingir o nível de Apetite a Risco desejado. Nesta situação o risco deve ser aceito, com a devida justificativa, desde que acatada pelo Especialista da Tipologia associada ao risco. É importante observar que um risco negativo aceito não deixa de existir e prevalece a necessidade de monitoramento sobre o mesmo.
Tolerar	Um risco pode ser tolerado quando se encontra fora da faixa de apetite, mas dentro da faixa de tolerância. Nessa condição, ele não exige ações imediatas de mitigação, mas requer monitoramento constante e esforço contínuo para que o risco seja levado à faixa de apetite.

A estratégia de tolerar risco negativo aplica-se quando o risco está fora da faixa de apetite, mas dentro da faixa de tolerância. Nessa condição, não são necessárias ações imediatas de mitigação, mas é imprescindível realizar monitoramento constante e manter um esforço contínuo para reduzir o risco ao nível desejado, dentro da faixa de apetite.

Tabela 12 – *Opções de estratégia de resposta aos riscos positivos*

Estratégia	Descrição
Evitar	Decisão de não se envolver com a oportunidade, geralmente nas condições em que NRA do risco positivo está muito distante do apetite, ou não há condições favoráveis para o seu aproveitamento.
Tratar	Buscar que o risco ocorra para a organização aproveitando os impactos positivos, geralmente, quando o NRA do risco está abaixo do apetite, por meio da criação de controles que reforcem a oportunidade.
Transferir	Transferir a oportunidade para terceiros que possam capturar melhor os benefícios da oportunidade.
Aceitar	Um risco positivo geralmente é aceito quando o seu NRA está dentro do Apetite a Riscos ou quando não exige ações adicionais, ou seja, quando não há necessidade de novos controles ou melhoria dos existentes.
Tolerar	Uma oportunidade pode ser tolerada quando se encontra fora da faixa de apetite, mas dentro da faixa de tolerância. Nessa condição, não exige ações imediatas para potencializá-la, mas requer monitoramento constante e esforço contínuo para que a oportunidade seja levada à faixa de apetite.

Fonte*: Gestão de Riscos – Avaliação da Maturidade (TCU, 2018) – Adaptada*

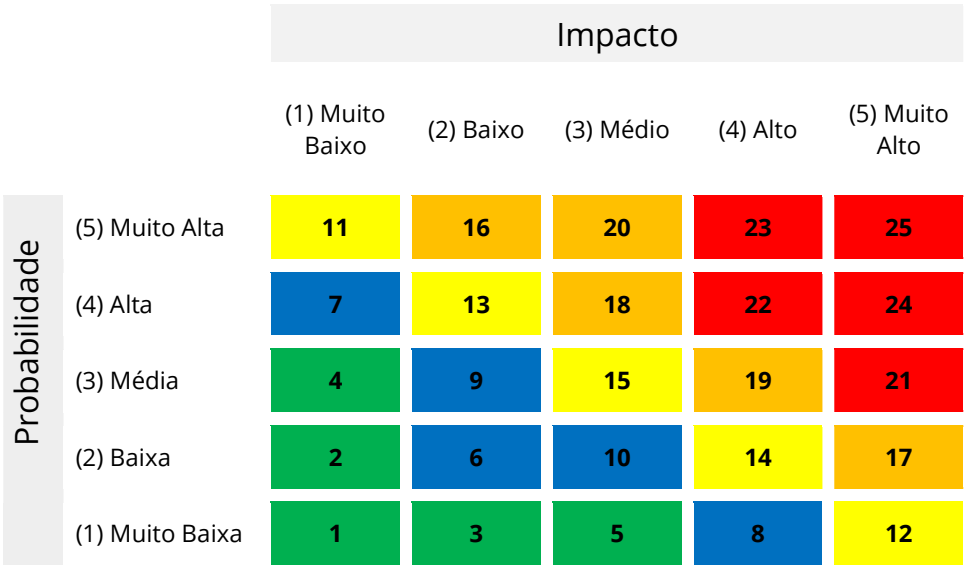
A estratégia de tolerar risco positivo aplica-se quando a oportunidade está fora da faixa de apetite, mas dentro da faixa de tolerância. Nesse caso, não são necessárias ações imediatas para adequação mas é essencial realizar monitoramento constante e manter um esforço contínuo para tratar a oportunidade até que ela esteja dentro da faixa de apetite.

A escolha da estratégia de resposta ao risco dependerá do valor do Nível de Risco Atual em comparação ao valor do Apetite a Riscos relacionado ao risco e ao critério do risco, conforme apresentado a seguir.

7.3.3.1 Influência no tratamento considerando Apetite a Riscos para riscos negativos

Conforme já visto, no Serpro, o apetite para riscos é definido por 5 níveis, destacados por diferentes cores, coincidentes com os níveis de risco e correlacionados a diferentes índices de risco grafados no interior das células da matriz apresentada na figura abaixo.

Figura 15 – *Apetite, níveis e índices para riscos negativos*



A Tabela 13, apresentada a seguir, deve ser utilizada como um referencial inicial que relaciona os mesmos 5 níveis da matriz de apetite com as diretrizes orientadoras para tratamento dos riscos negativos. Neste referencial o Apetite a Riscos a ser aceito pela empresa é equivalente ao nível médio (3-Amarelo) da matriz de riscos.

Tabela 13 – *Referencial de diretrizes para apetite de riscos negativos*

Apetite a Risco Negativo	NRA	Diretriz
Muito abaixo do Apetite	Muito Baixo (1-Verde)	Zona de conforto. Risco deve ser monitorado para acompanhar sua evolução, mas é possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custo x benefício, como diminuir o nível de controles.
Abaixo do Apetite	Baixo (2-Azul)	Nível de Risco abaixo do Apetite a Risco. Condições favoráveis para convivência com o risco, com grande chance de sucesso.
Apetite	Médio (3-Amarelo)	Nível de Risco dentro do Apetite a Risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da gerência (Diretoria responsável pelo risco) na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.
Acima do Apetite	Alto (4-Laranja)	Nível de Risco além do Apetite a Risco. Qualquer risco nesse nível dever ser comunicado a alta administração e ter uma ação tomada em período determinado. Postergação de medidas só com autorização da DIREX.

Apetite a Risco Negativo	NRA	Diretriz
Muito acima do Apetite	Muito Alto (5-Vermelho)	Nível de risco muito além do Apetite a Risco. Qualquer risco nesse nível deve ser comunicado à alta administração e ter sua resposta imediata. Postergação de medidas somente com autorização do CA.

Entretanto, como o Apetite a Risco pode variar de acordo com o declarado no RAS, para o correto uso das diretrizes, deve-se tomar como base o Nível do Apetite a Risco negativo definido para o risco em análise.

Por exemplo, se o risco é relacionado ao Apetite de nível 2 (NR=Baixo), para um risco negativo, teríamos as diretrizes orientadoras conforme a Tabela 14, alinhando o NRA=2 à diretriz adequada para o Apetite a Risco negativo.

Tabela 14 – *Exemplo de diretrizes para apetite de riscos negativos*

Apetite a Risco Negativo	NRA	Diretriz
Abaixo do Apetite	Muito Baixo (1-Verde)	Nível de Risco abaixo do Apetite a Risco. Condições favoráveis para convivência com o risco, com grande chance de sucesso.
Apetite	Baixo (2- Azul)	Nível de Risco dentro do Apetite a Risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da gerência (Diretoria responsável pelo risco) na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.
Acima do Apetite	Médio (3-Amarelo)	Nível de Risco além do Apetite a Risco. Qualquer risco nesse nível dever ser comunicado a alta administração e ter uma ação tomada em período determinado. Postergação de medidas só com autorização da DIREX.
Muito acima do Apetite	Alto (4-Laranja) ou Muito Alto (5-Vermelho)	Nível de risco muito além do Apetite a Risco. Qualquer risco nesse nível deve ser comunicado à alta administração e ter sua resposta imediata. Postergação de medidas somente com autorização do CA.

Conforme o exemplo, o apetite de nível Baixo (2-Azul) se torna o referencial para que os gestores avaliem as necessidades de tratamento ou aceitação do risco, assim:

- Se o NRA = Muito Baixo o risco terá as condições favoráveis para aceite
- Se o NRA = Baixo, portanto, no mesmo Nível do Apetite, há uma certa tranquilidade para decidir ou não pela sua minimização
- Caso o NRA = Médio, o risco deve ser tratado com atenção
- Em caso de NRA = Alto ou Muito Alto, além de tratados devem ter comunicados às instâncias superiores.

Nesta versão da Metodologia, a gestão de **riscos negativos** deve ser considerada no escopo de **Riscos Operacionais, Riscos de Projetos Estratégicos, Riscos Estratégicos e Riscos ao Negócio**.

7.3.3.2 Influência no tratamento considerando Apetite a Riscos para riscos positivos

Assim como nos riscos negativos, a matriz de apetite para riscos positivos possui 5 níveis. Pode se observar que os níveis de apetite se comportam de forma inversa à matriz de apetite para riscos negativos, destacadas por diferentes cores, relacionadas a diferentes índices de risco, conforme visualizado no interior das células da matriz da figura abaixo.

Figura 16 *– Apetite, níveis e índices para riscos positivos*

Probabilidade	Impacto: (1) Muito Baixo	(2) Baixo	(3) Médio	(4) Alto	(5) Muito Alto
(5) Muito Alto	11	16	20	23	25
(4) Alto	7	13	18	22	24
(3) Médio	4	9	15	19	21
(2) Baixo	2	6	10	14	17
(1) Muito Baixo	1	3	5	8	12

A Tabela 15, apresentada a seguir, deve ser utilizada como um referencial inicial que relaciona os mesmos 5 níveis da matriz de apetite com as diretrizes orientadoras para tratamento dos riscos positivos. Neste referencial o Apetite a Risco positivo a ser aceito pela empresa é equivalente ao nível Médio (3-Amarelo) da matriz.

Tabela 15 *– Referencial de diretrizes para apetite de riscos positivos*

Apetite a Risco Positivo	NRA	Diretriz
Muito acima do Apetite	Muito Alto (5-Verde)	Condições extremamente favoráveis para que o risco positivo colabore para se obter êxito no atingimento dos objetivos relacionados.
Acima do Apetite	Alto (4-Azul)	Condições favoráveis para que o risco positivo colabore para se obter êxito no atingimento dos objetivos relacionados.

Apetite	Médio (3-Amarelo)	Nível de Risco dentro do Apetite a Risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da área responsável pelo risco na manutenção de respostas e controles para manter o risco nesse nível, ou ampliá-lo sem custos adicionais.
Abaixo do Apetite	Baixo (2-Laranja)	Condições favoráveis para atingimento do apetite, porém, com chances de insucesso se não tiver métricas claras para gerir o risco. A diretoria responsável pelo risco pode optar pela implementação de controles.
Muito abaixo do Apetite	Muito Baixo (1-Vermelho)	Nível de risco muito abaixo do Apetite a Risco. Qualquer risco nesse nível deve ser rigorosamente avaliado de forma a verificar se o esforço ou custos para se atingir o apetite desejado é muito grande. É desejável o aconselhamento da DIREX.

Entretanto, como o Apetite a Risco pode variar de acordo com o declarado no RAS, para o correto uso das diretrizes, deve-se tomar como base o Nível do Apetite a Risco positivo definido para o risco em análise

Por exemplo, se o risco é relacionado ao Apetite de nível 4 para um risco positivo, teríamos as diretrizes orientadoras conforme a tabela seguinte:

Tabela 16 *– Exemplo de diretrizes para apetite de riscos positivos*

Apetite a Risco Positivo	NRA	Diretriz
Acima do Apetite	Muito Alto (5-Verde)	Condições favoráveis para que o risco positivo colabore para se obter êxito no atingimento dos objetivos relacionados.
Apetite	Alto (4-Azul)	Nível de Risco dentro do Apetite a Risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da área responsável pelo risco na manutenção de respostas e controles para manter o risco nesse nível, ou ampliá-lo sem custos adicionais.
Abaixo do Apetite	Médio (3-Amarelo)	Condições favoráveis para atingimento do apetite, porém, com chances de insucesso se não tiver métricas claras para gerir o risco. A diretoria responsável pelo risco pode optar pela implementação de controles.
Muito abaixo do Apetite	Baixo (2-Laranja) ou Muito Baixo (1-Vermelho)	Nível de risco muito abaixo do Apetite a Risco. Qualquer risco nesse nível deve ser rigorosamente avaliado de forma a verificar se o esforço ou custos para se atingir o apetite desejado é muito grande. É desejável o aconselhamento da DIREX.

Conforme o exemplo, o apetite de nível Alto (4-Azul) se torna o novo referencial para que os gestores possam realizar suas iniciativas para alavancar vantagens competitivas, assim:

- Caso o risco tenha o NRA = Muito Alto, existirão condições favoráveis, com grande chance de sucesso para aproveitamento das oportunidades apresentadas pelo risco positivo.
- Se o NRA = Alto, o risco estará no mesmo nível do apetite do exemplo, cabendo apenas a manutenção dos controles relacionados.

- No caso de o risco apresentar NRA = Médio, o aproveitamento da oportunidade deve ser realizado com cuidado.
- Se o risco apresentar NRA = Baixo ou Muito Baixo, a implementação de controles para se atingir o apetite deve ser rigorosamente avaliada, uma vez que, possivelmente, os custos serão altos para se atingir o apetite firmado."

Nesta versão da Metodologia, a gestão de **riscos positivos** deve ser considerada apenas para os **Risco Estratégicos e Riscos ao Negócio**.

Uma boa prática para apoiar o processo de avaliação de riscos é estabelecer critérios para priorização e tratamento associados aos níveis (criticidade) de risco, conforme descrito para a próxima fase do processo.

7.4. Priorização para tratamento dos riscos

O Plano de Gestão de Riscos já define a priorização de tratamento sobre as dimensões Riscos Estratégicos, Riscos ao Negócio e Riscos Críticos Operacionais e de Projetos Estratégicos. Para os riscos vinculados a cada uma dessas dimensões, nesta etapa, devem ser considerados os valores dos Níveis de Risco Atuais (NRA), a fim de identificar quais riscos serão priorizados na implementação.

7.4.1. Riscos negativos

O Gestor do Risco deve verificar quais riscos foram mapeados na fase anterior, em que o NRA esteja acima da classificação do Apetite a Riscos. A tabela a seguir representa os critérios referenciais para priorização e tratamento de riscos negativos no Serpro.

Tabela 17 *– Priorização do tratamento de riscos negativos*

Nível de Risco Atual (NRA)	Critérios para priorização e tratamento de riscos negativos
Muito acima do Apetite	Nível de Risco muito além do Apetite a Risco. Qualquer risco nesse nível deve ser comunicado à alta administração e ter uma resposta imediata. Postergação de medidas só com autorização do dirigente máximo.
Acima do Apetite	Nível de Risco além do Apetite a Risco. Qualquer risco nesse nível deve ser comunicado a alta administração e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do dirigente de área.
Apetite	Nível de Risco dentro do Apetite a Risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da gerência na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.
Abaixo do Apetite	Nível de Risco abaixo do Apetite a Risco indica que nenhuma medida especial é necessária além do monitoramento do risco e controles associados.

Nível de Risco Atual (NRA)	Critérios para priorização e tratamento de riscos negativos
Muito abaixo do Apetite	Nível de Risco muito abaixo do Apetite a Risco. É possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custos x benefícios, como diminuir o nível de controles.

7.4.2. Riscos positivos

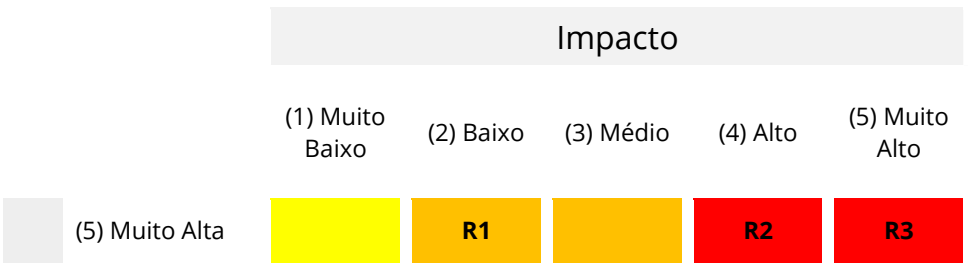
O Gestor do Risco deve verificar quais riscos foram mapeados na fase anterior, em que o NRA esteja acima da classificação do Apetite a Risco e tratá-los conforme os critérios de priorização de riscos positivos. A tabela abaixo representa os critérios referenciais para priorização e tratamento de riscos positivos no Serpro.

***Tabela 18** – Priorização do tratamento de riscos positivos*

Nível de Risco Atual (NRA)	Critérios para priorização e tratamento de riscos positivos
Muito acima do Apetite	Nível de Risco muito além do Apetite a Risco. Qualquer risco nesse nível deve ter uma resposta imediata. As oportunidades devem ser aproveitadas com a maior brevidade. A Postergação de medidas deve ser aprovada pela alta administração.
Acima do Apetite	Nível de Risco além do Apetite a Risco. Qualquer risco nesse nível deve ter as ações tomadas em período determinado pelo dirigente da área e qualquer postergação de medidas deve ter a sua aprovação.
Apetite	Nível de Risco dentro do Apetite a Risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da gerência na manutenção de respostas e controles para manter o risco nesse nível, ou ampliá-lo sem custos adicionais
Abaixo do Apetite	Nível de Risco abaixo do Apetite a Risco indica que medidas especiais devem ser tomadas apenas com a aprovação da DIREX, com menor priorização.
Muito abaixo do Apetite	Nível de Risco muito abaixo do Apetite a Risco indica que nenhuma medida especial é necessária.

Para ambos os casos (riscos positivos e negativos), a partir da definição dos Níveis de Risco Atuais é possível a construção da Matriz de Riscos.

***Figura 17** – Exemplo de priorização de riscos negativos na Matriz de Riscos*



(4) Alta				R4	R5
(3) Média	R6	R7		R8	
(2) Baixa		R9	R10		R11
(1) Muito Baixa					

A matriz apresenta um exemplo de situação na qual os riscos negativos (R1, R2, Rn) estão relacionados a tipologias cujo nível de Apetite a Risco se encontram no nível Baixo (2-Azul). Dessa forma, o risco R3 terá maior priorização para tratamento, seguido pelos riscos R2, R4 e R5, com mesma prioridade e R8, com menor prioridade em relação aos demais. Neste caso, as diretrizes contidas na seção "7.3.2.1. Influência no tratamento considerando Apetite a Riscos para riscos negativos", devem ser consideradas.

A priorização para riscos positivos deve ser realizada da mesma forma, obviamente considerando-se a construção da matriz adequada para riscos positivos bem como as diretrizes definidas para tal.

Nesta versão da Metodologia, a gestão **de riscos positivos** deve ser considerada apenas para os **Riscos Estratégicos e Riscos ao Negócio**.

7.5. Definição dos controles de respostas aos riscos

Pressupõe-se que os controles são capazes de diminuir os níveis de probabilidade e/ou de impacto, para riscos negativos ou ampliar a probabilidade e/ou impacto para riscos positivos, a um nível dentro ou mais próximo possível do nível de Apetite a Riscos. Selecionar a opção mais adequada envolve equilibrar, de um lado, os custos e esforços de implementação e, de outro, os benefícios decorrentes. Assim deve-se considerar os recursos necessários para a implementação dos controles propostos, considerando-se uma análise custo *versus* benefício.

Quando a estratégia adotada é o tratamento, os controles representam a principal ação de resposta ao risco. Os riscos devem ser tratados por meio da criação de novos controles ou melhoria dos controles existentes, de forma a levar o Nível de Risco Projetado para o nível de Apetite a Risco relacionado. O processo de definição dos controles é o mesmo, tanto para riscos negativos quanto positivos, entretanto, o controle deve diminuir a probabilidade (preventivo) ou minimizar o impacto (contingencial) do risco negativo enquanto, para os riscos positivos, o controle pretende ampliar a probabilidade (facilitador) ou aumentar o impacto (reforçador).

Os resultados da avaliação da etapa anterior subsidiam a definição de controles propostos necessários para atingir o Nível de Risco Projetado, normalmente no nível ou abaixo do Nível de Apetite ao Risco. Nesta etapa pode-se utilizar as deficiências dos controles existentes para propor melhorias ou propor novos controles para os riscos.

Durante esta fase, o Gestor do Risco e o Agente de Riscos (Agentes GRCI), assim como os Responsáveis pelos Controles, devem estar atentos aos seguintes pontos:

a) Para a redução da probabilidade da ocorrência do risco, os controles preventivos devem ser definidos e focados nas causas identificadas para o risco;

b) Para a redução do impacto da ocorrência do risco, os controles contingenciais devem ser definidos e focados nas consequências identificadas para o risco;

c) Controles propostos devem apresentar as datas previstas para início e fim de sua implementação e o responsável. Após o início da implementação do controle, o campo "data inicial de implementação" deve ser informado;

d) Controles existentes devem ser informados com sua data de implementação e responsável. Devem ser identificados no momento do mapeamento do risco atual;

e) Deve ser apresentada a justificativa para o cancelamento de controles, sempre que estiverem vinculados a riscos aprovados;

f) Sempre que a estratégia sugerida for "tratar", pelo menos um controle proposto ou uma melhoria em controle existente deve ser definida visando baixar o NRP. Caso os controles não possibilitem a redução do NRP para o nível de Apetite a Riscos, deve ser incluída uma justificativa e o risco deve ser aceito, caso haja a concordância do especialista da tipologia;

g) Se a estratégia sugerida for "tratar" e a estratégia adotada for diferente, deve-se ter justificativa para a estratégia proposta evidenciando a excepcionalidade. O risco deverá passar pela análise do Especialista da Tipologia.

h) Se a estratégia sugerida for "aceitar" e a estratégia adotada for "tratar" a justificativa é opcional.

i) Se a estratégia adotada for "Aceitar", o NRP deve se manter com o mesmo valor do NRA. Isso não impede que sejam definidos controles propostos por decisão do gestor do risco;

j) É possível que, após análise de eficácia dos controles já implementados, verifique-se que não há necessidade de propor novos controles em função do risco estar dentro do parâmetro estabelecido no Apetite a Riscos definido. Neste caso, aceita-se o risco, não necessitando de controles adicionais, porém o risco se mantém e deve ser adequadamente monitorado;

k) Em certos casos os controles definidos não são suficientes para se atingir o nível de Apetite a Risco desejado. Nesta situação o risco deve ser aceito, com a devida justificativa, desde que acatada pelo Especialista da Tipologia associada ao risco.

A implementação do tratamento (controles propostos) envolve a participação da unidade organizacional responsável pelo risco e, eventualmente, de unidades relacionadas como corresponsáveis.

Ao final desta fase, tanto os riscos negativos quanto positivos, acima do nível de Apetite a Riscos, deverão ter a confirmação sobre seu tratamento e, neste caso, devem ter controles de respostas aos riscos definidos, considerando-se as suas devidas priorizações.

Durante esta fase, deverá ser definido o Nível de Risco Projetado (NRP), estimando-se a probabilidade e impacto do risco considerando a melhoria de controles existentes e/ou a implementação de novos controles.

Os riscos operacionais com índices de Nível de Risco Atual entre 21 e 25 são considerados riscos críticos e devem ser analisados com maior atenção, assim como a evidenciação dos controles implementados para os riscos com impacto Alto ou Muito Alto.

Salienta-se que riscos operacionais são importantes insumos para identificação dos riscos estratégicos portanto, dependendo do nível do risco, pertinência do tema ao contexto atual e impacto estratégico, um risco operacional pode ser proposto pelo Superintendente para ser considerado como estratégico. Ressalta-se que, neste caso, é necessário cumprir todo o rito de apreciação pelos órgãos colegiados, inclusive passando pela aprovação do Conselho de Administração.

Além do responsável pelo controle, deve ser informado o cronograma de implantação do controle ou melhoria e, durante o monitoramento de sua implementação, o percentual de conclusividade relacionado.

O acompanhamento sobre a implementação dos controles de respostas aos riscos é descrito na seção 7.10 deste documento.

7.6. Validação dos resultados das etapas anteriores

Os resultados das etapas anteriores do processo de gerenciamento de riscos (entendimento do contexto, identificação e análise dos riscos, avaliação dos riscos, priorização dos riscos e definição de respostas aos riscos) devem passar pela avaliação do especialista da tipologia, pela análise crítica da 2ª. Linha e, após, ser avaliados e aprovados pelo Aprovador definido para o risco.

O envio do risco para análise crítica e para aprovação deve ser realizado pelo Agente de Riscos (Agentes GRCI) ou pelo Gestor de Riscos.

Após a aprovação do risco e respectivos controles, o Gestor de Riscos da unidade deve registrar os resultados alcançados e mensurar se o Nível de Risco Projetado foi alcançado após a implementação ou melhoria dos controles, conforme descrito na seção 7.9, que trata de monitoramento desta metodologia.

Assim como no processo de aprovação de risco, ao solicitar o cancelamento de um risco, o Agente de Riscos (Agente GRCI) ou Gestor do Risco deve submeter a solicitação à avaliação do Especialista da Tipologia e do Agente Corporativo de Riscos e Controles, cuja análise de pertinência é necessária antes do encaminhamento ao Aprovador do Risco.

7.7. Comunicação e consulta

O propósito da comunicação e consulta é auxiliar as partes interessadas pertinentes na compreensão do risco, na base sobre a qual decisões são tomadas e nas razões pelas quais ações específicas são requeridas.

A comunicação busca promover a conscientização e o entendimento do risco, enquanto a consulta envolve obter retorno e informação para auxiliar na tomada de decisão. Convém que uma coordenação estreita entre as duas facilite a troca de informações factuais, oportunas, pertinentes, precisas e compreensíveis, levando em consideração a integridade da informação, bem como os direitos de privacidade dos indivíduos. Convém que ocorram comunicação e consulta com partes interessadas apropriadas externas e internas, no âmbito de cada etapa e ao longo de todo o processo de gestão de riscos.

Durante as etapas do processo de gerenciamento de riscos do Serpro, é importante que a comunicação observe os atores/papéis envolvidos ou unidades apontadas como consultados ou informados na matriz RACI (**R**esponsável, **A**provador, **C**onsultado**, I**nformado), da tabela a seguir.

Tabela 19 *– Matriz RACI com principais atores e papéis na Gestão de Riscos e Controles*

Atividade	Gestor de Riscos	Agente de Riscos (Agentes GRCI) / Corresponsável	Agente Corporativo de Riscos e Controles	Aprovador	Parte Interessada	Responsável pelo controle	Especialista da Tipologia
Cadastrar Risco	R	C	C			C	C
Enviar Risco para Análise da Tipologia	R	C	CI			C	I
Executar Análise da Tipologia	C	C	C				R
Enviar Risco para Análise Crítica	R (quando não houver especialista da tipologia)	I	I				R (quando houver especialista da tipologia)
Executar Análise Crítica de Risco	I	I	R				I
Enviar Risco para Aprovação	R	C	I	I	I		
Aprovar Risco	CI	CI	I	A	I	I	C
Recusar Risco	C	C	I	R	I		
Cancelar Risco	R	CI	I	A	I	I	C
Encerrar Risco	R	I	I	I	I	I	I
Registrar materialização de Risco	R	C	I	I	I		I
Concluir Ocorrência de Materialização do Risco	R	C	I	I	I		I

Atividade	Gestor de Riscos	Agente de Riscos (Agentes GRCI) / Corresponsável	Agente Corporativo de Riscos e Controles	Aprovador	Parte Interessada	Responsável pelo controle	Especialista da Tipologia
Alterar Data Final Prevista de Implementação do Controle	C	C	I			R	
Implementar Controle	I	I	I			R	I
Avaliar Controle	I		R			C	
Cancelar Controle	C	C	I	A		R	I

RACI:

a) **R**esponsável (*Responsible*): é o papel responsável por completar as tarefas e as entregas;

b) **A**provador (*Accountable*): é quem tem a autoridade final sobre a aprovação da atividade;

c) **C**onsultado (*Consulted*): é o papel de quem é consultado, dentro ou fora da empresa, para que possa contribuir para a execução das tarefas. Alguém cuja participação agrega valor e/ou é essencial para a implementação. Neste caso, a comunicação é de duas vias (consulta <=> resposta); e

d) **I**nformado (*Informed*): são *stakeholders* ou quaisquer pessoas que devem ser atualizadas sobre o andamento das atividades. São notificadas de resultados ou ações tomadas, mas não precisam estar envolvidos no processo de tomada de decisão. A comunicação, neste caso, ocorre num sentido.

7.8. Registro, relato e contingência

7.8.1. Registro

O **registro** deve ocorrer em todas as etapas do processo de gestão de riscos e a qualquer tempo, na solução de gerenciamento de riscos adotada pela empresa.

Durante o seu ciclo de vida, um risco pode passar pela necessidade de registro das seguintes situações[10]:

a) **Em Edição**: Situação em que o risco e suas informações associadas estão sendo editados na solução de gerenciamento de riscos, ainda sem validação formal.;

b) **Disponível para Análise pelo Especialista da Tipologia:** Situação em que o risco está pendente de avaliação técnica pelo Especialista da Tipologia, responsável por verificar sua relevância e alinhamento com os critérios de risco definidos para a tipologia;

c) **Disponível para Análise Crítica**: Situação em que o risco aguarda avaliação pelo Agente Corporativo de Riscos e Controles para validar as informações registradas;

[10] O fluxo detalhado está descrito na ferramenta de diagramação de processos.

d) **Análise Crítica Concluída:** Situação em que o risco foi validado pelo Agente Corporativo de Riscos e Controles, com todas as informações registradas consideradas completas e consistentes;

e) **Disponível para Aprovação**: Situação em que o risco aguarda a decisão final do Aprovador de Riscos para inclusão no catálogo ou formalização de alterações;

f) **Disponível para Cancelamento**: Situação em que o risco, após análises do Especialista da Tipologia e do Agente Corporativo de Riscos e Controles, aguarda a decisão final do Aprovador de Riscos sobre o cancelamento;

g) **Recusado**: Situação em que o Aprovador de Riscos determina que as informações registradas, seja para inclusão ou cancelamento, não são pertinentes ou não justificam a solicitação. Antes dessa decisão, o risco deve passar pela análise do Especialista da Tipologia e do Agente Corporativo de Riscos e Controles;

h) **Aprovado**: Situação em que o Aprovador de Riscos valida as informações registradas, seja para inclusão ou cancelamento, considerando-as pertinentes e alinhadas aos critérios estabelecidos. Antes dessa aprovação, o risco deve ter passado pelas análises do Especialista da Tipologia e do Agente Corporativo de Riscos e Controles.;

i) **Cancelado**: Situação indicada quando o risco deixou de existir ou não é mais válido devido a alterações no contexto interno ou externo. Deve-se registrar a justificativa detalhada para o cancelamento. Salvo as situações mencionadas, um risco aprovado não deve ser cancelado, devendo permanecer sob monitoramento contínuo. Antes do cancelamento, o risco deve ser avaliado pelo Especialista da Tipologia, pelo Agente Corporativo e pelo Aprovador de Riscos.[11] Os riscos cancelados poderão ser reativados, pelo Gestor de Risco, voltando à situação de edição e retornando ao ciclo de aprovação;

j) **Encerrado**: Situação utilizada quando ocorreu um registro incorreto do risco. Para ser encerrado, o risco deve ter sido previamente cancelado e considerado definitivamente irrelevante. O risco encerrado não pode ser editado novamente pelo Gestor de Riscos;

k) **Materializado**: Situação em que o risco se concretiza durante o monitoramento. Após o tratamento adequado utilizando controles de contingência, deve-se avaliar a causa da materialização, o impacto causado e a necessidade de revisar controles ou níveis de probabilidade e impacto. Dependendo da gravidade e dos impactos do evento, podem ser acionados Planos de Continuidade de Negócios (PCNs) e/ou procedimentos de Gestão de Crises para assegurar a resiliência organizacional e a mitigação de danos;

[11] O registro de cancelamento de riscos Estratégicos ou ao Negócio só poderá ser efetivado na ferramenta corporativa de gestão de riscos após a aprovação final pelos órgãos colegiados.

l) **Materializado com Ocorrência Concluída**: Situação em que a ocorrência de um risco materializado foi tratada e resolvida por meio de controle(s) contingencial(ais). Dependendo da gravidade e dos impactos enfrentados durante o tratamento, pode ter havido o acionamento de Planos de Continuidade de Negócios (PCNs) e/ou procedimentos de Gestão de Crises. Após a conclusão, é essencial revisar os controles aplicados, analisar as lições aprendidas e verificar a necessidade de ajustes nos níveis de probabilidade e impacto do risco.

O processo de Gestão de Riscos e Controles e seus resultados devem ser documentados e relatados por meio de mecanismos apropriados, entre outros: relatórios periódicos e sistemas informatizados. O registro e o relato visam:

a) comunicar atividades e resultados de Gestão de Riscos e Controles em toda a organização;

b) fornecer informações para a tomada de decisão;

c) melhorar as atividades de Gestão de Riscos e Controles;

d) auxiliar a interação com as partes interessadas, incluindo aquelas com responsabilidade e com responsabilização por atividades de gestão de riscos; e

e) registrar e buscar tratamento das dificuldades para realização da Gestão de Riscos e Controles em cada unidade.

Convém que as decisões relativas ao registro e relato de informações levem em consideração, mas não se limitem ao seu uso, a sensibilidade da informação e os contextos externo e interno.

7.8.2. Relato

O **relato** é parte integrante da governança corporativa e convém que melhore a qualidade do diálogo com as partes interessadas e apoie os tomadores de decisão a cumprirem suas responsabilidades.

Com base nos registros efetuados na solução de gerenciamento de riscos, pela 1ª. Linha, ao final de cada ciclo de monitoramento, descrito na seção 7.9 desta metodologia, o Agente Corporativo elabora o relatório da Diretoria, no mês subsequente ao fechamento do trimestre. Para isso é necessário realizar nova Análise Crítica sobre o risco, considerando todas as informações advindas do monitoramento realizado pela 1ª. Linha (gestores e agentes de riscos (Agentes GRCI) e responsáveis pelos controles) no período.

Com base nos relatórios trimestrais de cada Diretoria, elaborados pela 2ª. Linha, a área de Gestão de Riscos e Controles elabora o relatório de monitoramento semestral consolidado que é reportado aos órgãos colegiado, DIREX e CA.

7.8.3. Contingência

Os **planos de contingência**[12] compõem o conjunto de controles planejados para a recuperação ou atenuação do impacto, quando da materialização de um risco. A Figura 118 descreve a associação entre os controles e as ações de contingência. A superintendência, ao analisar os riscos aos quais a empresa está exposta e o Apetite a Riscos do processo, deve sinalizar quais os riscos que têm necessidade de um plano de contingência, levando em consideração, no mínimo, a relação entre o custo e o benefício, o Apetite a Riscos definido para o processo e o impacto em caso de materialização.

Figura 18 *– Riscos e plano de contingência*

7.9. Análise crítica e monitoramento

Antes do risco ser encaminhado para aprovação pelo Superintendente ou Diretor, deverá ser submetido à análise do especialista da tipologia e pela crítica da 2ª. Linha.

7.9.1. Análise crítica

A etapa de **análise crítica dos riscos** é realizada tanto pelo Agente Corporativo indicado para acompanhar a implementação de gestão de riscos na Diretoria, quanto pelo Especialista da Tipologia. Para tanto, o Gestor de Riscos ou Agente de Riscos da unidade (Agentes GRCI) disponibiliza o risco com todas as informações referentes ao seu tratamento para o Especialista da Tipologia.

Será informado ao Agente de Riscos (Agentes GRCI) e Gestor de Riscos caso o Especialista da Tipologia identifique necessidade de algum ajuste. Caso contrário, o especialista da Tipologia encaminha o risco para análise pelo Agente Corporativo.

[12] Em atendimento à Resolução nº. 18, de 10 de maio de 2016 (CGPAR 18/2016).

Caso o Agente Corporativo de Riscos e Controles verifique necessidade de ajuste, o risco retornará para a 1ª. Linha, com as devidas anotações. Caso não sejam identificadas necessidades de ajustes, o Agente Corporativo de Riscos e Controles informará que a análise crítica foi concluída para que o Agente de Riscos (Agentes GRCI) ou o Gestor do Risco encaminhe para aprovação.

Abaixo seguem detalhes sobre a execução das respectivas análises.

7.9.1.1. Análise crítica pelo Especialista da Tipologia

O Especialista da Tipologia deve promover a análise crítica dos riscos associados à sua área de conhecimento, assegurando que os seguintes aspectos sejam considerados:

a) **Vinculação do Risco à Tipologia Correta**

O **Especialista da Tipologia** deve verificar se o risco está devidamente associado à tipologia correta, apontando eventuais desvios ou inconsistências nos registros.

b) **Avaliação dos Controles**

O especialista deve avaliar se os controles definidos são adequados para modificar o Nível de Risco Atual (NRA) e suficientes para alinhar ao nível de Apetite a Riscos estabelecido.

- Caso os controles não sejam suficientes para possibilitar levar o Nível de Risco Projetado (NRP) ao nível de Apetite, o risco deve conter uma justificativa clara e detalhada. Se a justificativa apresentada for considerada válida, o risco pode ser aceito. Caso contrário, o risco deve ser devolvido para a 1ª Linha com as ressalvas devidamente registradas e recomendações para ajustes.

c) **Responsabilidade pela Qualidade Técnica**

O especialista deve garantir que suas análises agreguem valor ao processo, fornecendo recomendações detalhadas e fundamentadas, de forma a subsidiar decisões informadas. Essa abordagem assegura o alinhamento técnico e estratégico dos riscos aos objetivos organizacionais, preservando a agilidade do processo.

O especialista possui um papel técnico de suporte e análise, mas sua atuação não é obrigatória para que o fluxo de aprovação do risco prossiga. Caso um risco evolua sem a sua análise, dentro do prazo estipulado, será registrado como "análise do especialista não realizada", cabendo esta análise ao Agente Corporativo.

7.9.1.2 Análise crítica pelo Agente Corporativo

Para a realização da análise crítica pelo **Agente Corporativo** devem ser considerados os seguintes pontos:

a) A descrição do risco deve permitir visualizar claramente os eventos que podem evitar, atrasar, prejudicar ou impedir o atingimento de um ou mais objetivos empresariais;

b) O correto preenchimento das causas, consequências e relação ao processo associado;

c) Para a redução da probabilidade da ocorrência do risco, os controles preventivos devem ser definidos e focados nas causas identificadas para o risco;

d) Para a redução do impacto da ocorrência do risco, os controles contingenciais devem ser definidos e focados nas consequências identificadas para o risco;

e) Se mais de um risco possuir causas iguais ou muito parecidas, considerar a possibilidade de fusão desses riscos;

f) Se um risco se materializar, essa ocorrência deve ser registrada pelo agente de risco (Agentes GRCI) ou gestor do risco e deve ser avaliada a possibilidade de se estabelecer novos controles ou melhoria dos existentes, bem como mensuração dos controles contingenciais;

g) O Nível de Risco Projetado (NRP) não pode ser maior que o Nível de Risco Atual (NRA);

h) Controles existentes devem ser informados com sua data de implementação e responsável. Devem ser identificados no momento do mapeamento do risco atual;

i) Controles propostos devem apresentar as datas previstas para início e fim de sua implementação e o responsável. Após o início da implementação do controle, o campo “data inicial de implementação” deve ser informado;

j) Observar se houve mudança no Nível de Risco Atual, se houve reporte da eficácia (atingimento dos objetivos) do(s) controle(s) e mudanças no contexto interno ou externo;

k) Verificar se há compatibilidade entre a evolução da implementação dos controles e a evolução do Nível de Risco Atual, visando alcançar o Nível de Risco Projetado;

l) Deve ser apresentada a justificativa para o cancelamento de controles, sempre que estiverem vinculados a riscos aprovados;

m) Sempre que a estratégia adotada for diferente da estratégia sugerida, deve ser justificada;

n) Se o NRA for maior que o Apetite a Risco do processo, então a estratégia deve ser, preferencialmente, “Tratar”;

o) Sempre que a estratégia adotada for “tratar”, pelo menos um controle proposto ou uma melhoria em controle existente deve ser definida visando baixar o NRP. Caso os controles não possibilitem a redução do NRP para o nível de Apetite a Risco,

deve ser incluída uma justificativa e o risco deve ser aceito, caso haja a concordância do especialista da tipologia;

p) Se a estratégia adotada for "Aceitar", o NRP deve se manter com o mesmo valor do NRA. Isso não impede que sejam definidos controles propostos por decisão do gestor do risco;

q) Em certos casos os controles definidos não são suficientes para se atingir o nível de Apetite a Risco desejado. Nesta situação o risco deve ser aceito, com a devida justificativa, desde que acatada pelo Especialista da Tipologia associada ao risco.

7.9.2. Monitoramento

A etapa de **monitoramento** dos riscos tem como objetivo avaliar de forma sistemática a qualidade do gerenciamento de Riscos e Controles.

Os **Agentes de Riscos da unidade (Agentes GRCI)** devem monitorar:

a) a execução da implementação dos controles propostos nas datas previstas, acompanhando as informações providas pelo responsável pelo controle;

b) a identificação de novos riscos e controles;

c) a materialização dos riscos, o registro de sua ocorrência, assim como a realização do plano de contingência;

d) possíveis falhas das estratégias de tratamento, observando ainda que, mesmo os riscos que estejam dentro ou abaixo do nível de Apetite a Risco não deixam de existir e o seu monitoramento deve ser constante;

e) a eficácia dos controles sobre os riscos;

f) os controles que deixaram de ser considerados para a mitigação do risco e registrar o motivo;

g) a atualização do NRA após verificação da eficácia do(s) controle(s) implementado(s);

Ressalta-se que **um risco não deixa de existir** pelo fato de todos os controles propostos terem sido executados ou melhorados. **Riscos dentro do apetite** definido é uma forma de comunicar a empresa de que não só os conhecemos, como os gerenciamos.

Quando o Nível de Risco Atual (NRA) do risco atingir o Apetite a Risco definido, ele deve ser **mantido como aprovado** e deve-se **manter o monitoramento**, pelos agentes (Agentes GRCI) / gestores do risco, para poder mantê-lo em parâmetro aceitável/controlado.

h) avaliar periodicamente os fatores de causa, consequência, probabilidade e impacto relacionados aos riscos, assim como os controles associados, considerando as mudanças do cenário (Mundo VUCA - sigla em inglês, formada pela primeira letra

das palavras: *Volatility* (volatilidade), *Uncertainty* (incerteza), *Complexity* (complexidade) e *Ambiguity* (ambiguidade).

As alterações observadas durante a monitoração dos riscos devem ser registradas conforme indicado na atividade de Registro na seção 7.8 desta metodologia.

Os **Responsáveis pelos Controles** devem monitorar:

a) A implementação de controles propostos considerando as datas previstas;

b) Mensalmente, atualizar o percentual de conclusividade da implementação;

c) A funcionalidade dos controles;

d) Controles propostos cujo percentual de implementação apresente 100% de conclusividade devem ser evidenciados e considerados como implementados refletindo no Nível de Risco Atual, após a confirmação de sua eficácia de atuação sobre o risco.

As alterações observadas sobre os controles, durante o seu monitoramento, devem ser registradas conforme indicado na atividade de Registro na seção 7.8 desta metodologia.

Ao final de cada ciclo de monitoramento, o Agente Corporativo de Riscos e Controles elabora o relatório trimestral da Diretoria, conforme descrito na atividade de Relato na seção 7.8 desta metodologia.

7.10. Implementação dos controles de respostas aos riscos

A implementação dos controles de resposta aos riscos envolve a participação da Unidade Organizacional responsável pelo processo organizacional e das unidades relacionadas como corresponsáveis em cada iniciativa, se previstas. Para a implementação dos controles de resposta aos riscos deve ser definido o principal responsável pela implementação da iniciativa, que também deverá monitorar e reportar a evolução das iniciativas.

Os controles podem assumir 6 estados de implementação:

a) **Não Iniciado:** o controle foi proposto e ainda não foi iniciada a implementação;

b) **Em Implementação:** a implementação do controle foi iniciada;

c) **Implementado**: o controle teve sua implementação finalizada;

d) **Em melhoria**: o controle foi implementado anteriormente, mas necessita melhoria. Neste caso o controle a ser melhorado deve se manter registrado como existente e um novo controle proposto deve ser cadastrado. Após a sua implementação, este deverá substituir o controle original.

e) **Suspenso**: a implementação do controle foi suspensa. Deve ser registrado o motivo e a data da suspensão;

f) **Cancelado**: esta situação é indicada quando: houve registro incorreto do controle, o controle deixou de existir; o controle não é mais válido, contexto interno ou cenário externo foram alterados e o registro não é mais pertinente à situação atual. Quando for observado um registro indevido para o controle (o controle não é válido), ele deve ser cancelado. Neste caso deve ser registrada a justificativa para o cancelamento.

Esta etapa deve ser acompanhada pela ação de monitoramento descrita anteriormente.

Para os controles implementados, periodicamente, deve ser avaliada a eficácia sobre seu efeito no Nível de Risco Atual (NRA), ou seja, a 1ª. Linha deve confirmar a eficácia do controle antes de reduzir o NRA.

A implementação dos controles propostos, para os riscos críticos, deve ser acompanhada, pela 1ª. Linha, registrando-se, tempestivamente, o percentual de conclusividade observado durante este processo.

8. METODOLOGIA PARA GESTÃO DE RISCOS DOS PROJETOS ESTRATÉGICOS

A gestão de projetos no Serpro é regulamentada pela Norma "Gerenciar Portfólio, Programas e Projetos", vinculada ao Processo "Gerenciar Portfólios, Programas e Projetos", e ao Subprocesso "Gerenciar Projetos". Nela, já constam as etapas de identificação e avaliação dos riscos para os projetos da empresa, as quais devem ser realizadas conforme esta metodologia.

Diferente da gestão e medição dos riscos operacionais, a gestão dos riscos dos projetos estratégicos não será executada continuamente, existindo apenas durante o ciclo de vida do projeto, podendo ter riscos que, após a conclusão do projeto, sejam incluídos como riscos contínuos a serem acompanhados e relacionados a um processo operacional correspondente.

O Processo de Gestão de Riscos e Controles para os Projetos Estratégicos deve atender a todas as definições para Processos Operacionais, com exceção das peculiaridades dos projetos, descritas a seguir:

Figura 19 *– Processo de Gestão de Riscos de Projetos Estratégicos*

Fonte*: NBR ISO 31000 – fev.2018 (adaptado)*

8.1. Definição do escopo e contexto

Os Projetos Estratégicos do Serpro possuem alta complexidade de gestão e requerem o comprometimento e participação direta de todos os envolvidos, membros, gerentes e patrocinadores. Os projetos estão alinhados ao planejamento estratégico da empresa.

Projetos estratégicos já ensejam riscos pela própria natureza de exclusividade e complexidade de suas atividades. Portanto, não há dúvidas quanto a necessidade de conhecer e gerenciar, de forma adequada e tempestiva, as incertezas que podem afetar o alcance de seus objetivos. É imprescindível que as informações dos riscos dos projetos estratégicos estejam estruturadas, atualizadas e disponíveis na ferramenta corporativa de GRCI, que além de garantir a transparência aos *stakeholders*, podem ser utilizadas como auxílio na tomada de decisão e na proteção de valor.

O Apetite a Risco de cada projeto estratégico deve ser definido **de acordo com a sua tipologia**, conforme declaração no RAS.

8.2. Identificação e análise dos riscos

Após a análise do contexto do projeto, é iniciada a fase de levantamento e identificação dos riscos do projeto. Nesta etapa, o gestor do projeto contará com o apoio da 2ª. Linha na área de Gestão de Riscos e Controles, disponibilizando um Agente Corporativo de Riscos e Controles para participar, auxiliando na internalização da metodologia em conjunto com a equipe do projeto, em todas as etapas, conforme preconizado na Metodologia para Gestão de Riscos Operacionais, Especificamente em relação à identificação e análise dos riscos, sobre os riscos do projeto, deve ser realizado conforme descrito na seção 7.2.

O encerramento do projeto implica no cancelamento dos riscos a ele atrelados.

8.3. Avaliação dos riscos e verificação dos controles

O Nível de Risco Atual (NRA) deve ser analisado em relação ao momento do mapeamento dos riscos, e não em relação ao início do projeto. O Nível de Risco Projetado (NRP) deverá ser atingido até a conclusão do projeto.

A avaliação dos riscos e verificação dos controles sobre o projeto estratégico, deve ser idêntica à apresentada na seção 7.3 desta metodologia.

8.4. Priorização para tratamento dos riscos

Deverá ser realizada conforme descrito na seção 7.4.

8.5. Definição dos controles de respostas aos riscos

Deverá ser realizada conforme descrito na seção 7.5.

Os riscos de projetos estratégicos com índices de Nível de Risco Atual entre 21 e 25 são considerados riscos críticos e devem ser analisados com maior atenção, assim como a evidenciação dos controles implementados para os riscos com impacto Alto ou Muito Alto.

8.6. Validação dos resultados das etapas anteriores

A gestão dos riscos é realizada pela equipe do projeto, onde o gestor do projeto é obrigatoriamente o gestor dos riscos identificados. A aprovação será do patrocinador do Projeto. Caso exista mais de um, deverá ser realizado pelo Superintendente ou Diretor Supervisor que atua como patrocinador. Essa etapa deve ser realizada como descrito na seção 7.6 desta metodologia.

8.7. Comunicação e consulta

Deverá ser realizada conforme descrito na seção 7.7.

8.8. Registro, relato e contingência

Deverá ser realizada conforme descrito na seção 7.8.

8.9. Análise crítica e monitoramento

O acompanhamento dos riscos dos Projetos Estratégicos será constante, pela 1ª. Linha e periódico, pela 2ª. Linha, em reuniões com a participação da equipe do projeto e do escritório central de projetos do Serpro. A periodicidade do acompanhamento será minimamente a cada trimestre na forma de relatórios de análise crítica de monitoramento para os Comitês Táticos e Estratégico, bem como para Órgãos Colegiados e Diretoria Executiva. A execução desta fase é realizada da mesma forma que a descrita na seção 7.9.

8.10 Implementação dos controles de respostas aos riscos

Conforme descrito na seção 7.10.

9. METODOLOGIA PARA GESTÃO DE RISCOS ESTRATÉGICOS E RISCOS AO NEGÓCIO DO SERPRO

Entende-se como Riscos Estratégicos (RE) aqueles eventos que afetam os objetivos estratégicos da empresa. Riscos ao Negócio do Serpro (RN) afetam a missão, a visão ou o valor da empresa, ou seja, seus componentes estratégicos. Riscos Estratégicos e Riscos ao Negócio serão anualmente revistos e aprovados pelo Conselho de Administração (CA) até a última reunião do ano, conforme determina a Lei 13.303/2016 e o Estatuto Social do Serpro.

Conforme visto no capítulo Introdutório desta metodologia, estes eventos podem ter impactos negativos (riscos) ou positivos (oportunidades). As mesmas fontes de incertezas, causadoras de novas ameaças e destruidoras de valor, são também geradoras de uma vasta gama de oportunidades potenciais e opções de inovação para as organizações. Desta forma, aparentemente, há um desequilíbrio entre a atenção e esforços investidos em gestão de riscos para prevenção de ameaças em detrimento a gestão de riscos para exploração de oportunidades.

Esta seção da metodologia refletirá a forma de tratamento, em ambos os aspectos, para os riscos estratégicos do Serpro.

A percepção dos Riscos Estratégicos pode variar em função de necessidades, conceitos e interesses das partes envolvidas ao identificar aspectos relacionados com o risco propriamente dito, suas causas, suas consequências e as medidas que estão sendo tomadas para tratá-los.

O processo de identificação de riscos estratégicos demanda:

a) conhecimento profundo do negócio da empresa, incluindo o mercado em que atua, ambiente legal, social, político e cultural; e

b) compreensão dos objetivos estratégicos da empresa.

O processo de identificação de um Risco Estratégico culmina na especificação de uma série de riscos que compõem o perfil de risco da empresa.

O modelo utilizado é composto pelas etapas demonstradas na Figura , bastante semelhante ao modelo adotado sobre os Riscos Operacionais. As particularidades existentes sobre os riscos estratégicos, em função da sua natureza diferenciada, assim como a diferenciação sobre o tratamento de riscos negativos e positivos, serão destacadas nesta seção da metodologia.

Figura 20 *– Processo de Gestão de Riscos Estratégicos*

Fonte*: NBR ISO 31000 – fev.2018 (adaptado)*

O trabalho de gestão sobre os Riscos Estratégicos e Riscos ao Negócio do Serpro é dependente da definição do planejamento estratégico, assim como dos objetivos estratégicos, uma vez que os riscos a serem mapeados afetam o atingimento de tais objetivos ou componentes estratégicos. Considerando a necessidade de priorização para tratamento dos riscos, os RE precedem os Riscos Operacionais e de Projeto Estratégico. Todos os RE com resposta definida como "tratar", terão a mesma priorização, ou seja, independente do NRA, cada RE terá o tratamento igualmente priorizado.

Por outro lado, os riscos críticos identificados no ano anterior, considerando os resultados apresentados sobre a evolução no seu tratamento, por meio da implementação dos controles no ano vigente, servem de subsídio para a construção do Planejamento Estratégico. Riscos que tenham controles pendentes na implementação podem se manter ativos para o próximo exercício, conforme decisão dos participantes da construção do Planejamento Estratégico. Assim, tais riscos são insumo, tanto para a construção do Planejamento Estratégico, quanto para a definição dos próprios Riscos Estratégicos a serem tratados no ano seguinte.

Um ponto específico a ser considerado para o levantamento dos riscos estratégicos é a identificação de Riscos ao Negócio da organização. As ameaças e fraquezas (riscos negativos), oportunidades e forças (riscos positivos) inerentes ao ambiente de negócios da empresa relacionadas ao atingimento da visão, missão e ou seus valores, devem ser consideradas. Estes eventos continuamente pressionam as finanças, imagem, sustentabilidade e operações do Serpro.

Tais riscos possuem uma característica perene e tendem a impactar não somente os objetivos estratégicos. Riscos ou causas de riscos relacionados à sustentabilidade econômica, adequação do quadro de pessoal ou obsolescência tecnológica são exemplos de Riscos ao Negócio, uma vez que, independentemente dos objetivos estratégicos traçados, sempre irão impactar a própria existência da empresa. Estes riscos são mapeados (identificados, avaliados e, analisados), tratados e monitorados como Riscos Estratégicos.

As etapas de identificação dos Riscos Estratégicos Negativos estão associadas à construção do Planejamento Estratégico da empresa e não será diferente para os riscos estratégicos positivos que seguirá o mesmo trâmite. Há necessidade de trabalho integrado entre a Área de Gestão da Estratégia Empresarial e a Área de Riscos e Controles dando início ao ciclo de gestão dos Riscos Estratégicos diferenciando a escolha das abordagens a serem seguidas. Atividades específicas, que abordam essa integração, são conduzidas, principalmente, durante as fases de "Definição do escopo e contexto" e "Identificação e análise dos riscos", conforme descrito a seguir:

9.1. Definição do escopo e contexto

Nesta etapa, que deve ocorrer anualmente, em setembro, são alinhadas as ações do Planejamento Estratégico e da Gestão de Riscos do ano vigente. Associadas a esta fase, devem ser conduzidas, pela área de gestão de riscos, as seguintes atividades:

1) **Alinhar ações entre PE e RE para o próximo ano**:

   a) Os riscos críticos identificados no ano anterior, considerando os resultados apresentados sobre a evolução no seu tratamento, devem servir de subsídio para a construção do Planejamento Estratégico. Os Riscos que tenham controles pendentes na implementação podem se manter ativos para o próximo exercício, conforme decisão dos participantes da construção do Planejamento Estratégico e são insumos, tanto para a construção do Planejamento Estratégico, quanto para a definição dos próprios Riscos Estratégicos a serem tratados no ano seguinte;

   b) A matriz SWOT, oriunda do Planejamento Estratégico, fornece as forças, fraquezas, Oportunidades e Ameaças para definir um plano estratégico, com ações e táticas, para o Serpro. A partir das informações de forças e das oportunidades é que utilizaremos insumos para construção dos riscos estratégicos positivos. As fraquezas e ameaças podem se tornar insumo para o levantamento dos riscos estratégicos negativos;

2) **Estabelecer roadmap para identificação de RE do próximo ano:** O plano de ação para formalização dos riscos estratégicos negativos e positivos é estabelecido nessa atividade.

   a) As ações do Planejamento Estratégico devem estar alinhadas com o plano de ação da definição dos riscos estratégicos positivos e negativos. Os Objetivos Estratégicos, definidos no Planejamento Estratégico, são insumo para o levantamento dos riscos

estratégicos, uma vez que estes afetam, negativamente ou positivamente, o atingimento dos objetivos;

b) Deve ser criada apresentação, contendo as informações consolidadas e orientações, para subsidiar a realização das oficinas que irão ocorrer na sequência.

O Apetite a Risco para os riscos estratégicos e de negócio, deverá ser definido de acordo com as características de cada risco, **independentemente de sua tipologia**, na fase de identificação e análise dos riscos.

9.2. Identificação e análise dos riscos

Nesta fase, ainda em setembro, a área de Gestão de Riscos deverá coordenar oficinas de identificação dos efeitos de incerteza para alcance dos Objetivos Estratégicos, candidatos a Riscos Estratégicos, em cada Diretoria.

Além das informações consolidadas na fase de definição do Escopo e Contexto é desejável que, cada diretoria, de acordo com suas atribuições, considere os cenários internos e externos para o levantamento dos RE candidatos.

Para avaliação de **cenários externos,** pode ser considerado, mas não está limitado a:

a) **Cenário regulatório do setor público**: abrange notícias e trabalhos dos órgãos de controle, tais como Tribunal de Contas da União (TCU) e Corregedoria-Geral da União (CGU), bem como relacionados ao órgão supervisor e de orientação das empresas estatais – Ministério da Economia e Secretaria de Coordenação e Governança das Empresas Estatais (SEST). Inclui ainda o acompanhamento de projetos em discussão no Congresso Nacional, e que podem afetar a empresa e seu mercado de atuação. As principais fontes são: veículos de imprensa, acórdãos e decisões dos órgãos de controle, leis, resoluções, portarias e decretos que podem afetar o Serpro;

b) **Cenário econômico do país e perspectivas para o setor público:** análise da conjuntura econômica e financeira para o próximo ano, em especial nos aspectos relacionados ao setor público, como expectativa de crescimento e evolução do orçamento federal, fonte da maior parte da receita do Serpro. As principais fontes de consulta são sites especializados do Banco Central (BACEN), do Tesouro Nacional e do IPEA; e

c) **Cenário de Tecnologia:** evolução do cenário tecnológico voltado para a construção e prestação de soluções digitais, e seus efeitos para as soluções do Serpro. As principais fontes de consulta são *sites* especializados, boletins de fornecedores de *hardware e software* e consultorias independentes, como o *Gartner Group.*

Para avaliação de **cenários internos** pode ser considerado, mas não está limitado a:

a) **Consulta à base corporativa de riscos**;

b) **Anuário de Inteligência**: publicação anual do Serpro elaborada por especialistas da empresa, com avaliações e cenários para as perspectivas usadas no Planejamento Estratégico do ano corrente. Ele abrange tópicos de tecnologia, gestão, pessoas e inovação, com um panorama abrangente de tópicos que podem afetar a estratégia da empresa para os próximos anos;

c) **Indicadores de acompanhamento do Planejamento Estratégico do ano corrente:** permite avaliar os Objetivos e Riscos Estratégicos para o próximo ano com base no comportamento do exercício vigente;

d) **Revisão do PETI** do ano corrente;

e) **Elaboração do PDTI** do ano seguinte; e

f) **Realização dos Painéis Estratégicos**.

Para a identificação dos RE candidatos, são necessárias as seguintes atividades:

1. **Elaborar proposta de RE para o próximo ano no COGRC de cada Diretoria**: A identificação, tanto de riscos estratégicos negativos, quanto de riscos estratégicos positivos, é realizada pelas Superintendências de cada diretoria. A caracterização de um evento incerto como uma oportunidade ou uma ameaça é resultante da intenção dos gestores ao analisar as fontes de incertezas (pessoas, processos, sistemas, eventos externos) e se comprometer financeiramente com uma série de controles para explorá-la ou mitigá-la. Assim, de acordo com a intenção dos gestores devem ser considerados:

   a. **Riscos negativos:** A gestão de riscos negativos vê a incerteza como fonte de perda. Na gestão de riscos negativos a organização analisa suas fontes de risco com o propósito de encontrar "o que pode dar errado". Assim, na gestão de riscos negativos, a organização analisa suas fontes de risco de forma a identificar eventos (ameaças) com consequências negativas (perdas) sobre os resultados da organização em relação aos objetivos estratégicos mapeados no Planejamento Estratégico. Outra boa fonte de análise se encontra nas ameaças descritas na matriz SWOT, desenvolvida durante o Planejamento Estratégico;

   b. **Riscos positivos:** Na gestão de riscos positivos, a intenção é identificar "o que pode dar mais certo do que ocorre hoje". As mesmas fontes de risco deverão ser analisadas, mas, dessa vez, o foco deverá ser a busca de eventos (oportunidades) com consequências positivas (ganhos) que levem a organização a alcançar resultados superiores aos obtidos atualmente, sobre os objetivos estratégicos definidos. Na gestão de riscos positivos, a incerteza é vista como uma fonte de ganhos. Uma boa fonte de análise se encontra nas oportunidades descritas na matriz SWOT, desenvolvida durante o Planejamento Estratégico.

2. **Analisar e Consolidar RE candidatos:** Uma vez identificados os riscos em cada diretoria e seus devidos apetites, esses são consolidados considerando a

especificação da maioria de seus atributos (Descrição do risco, suas causas e consequências, apetite, probabilidade e impactos Inerentes, Atuais e Projetados) e vínculos com os Objetivos Estratégicos para o próximo exercício;

3. **Submeter à revisão dos RE, pelo COGRS:** os RE consolidados são submetidos à apreciação pelo COGRS;
4. **Submeter RE para apreciação da DIREX / Indicar Diretor responsável:** Os RE são apresentados à DIREX para revisão, validação e indicação de responsáveis pelos riscos;
5. **Submeter RE para apreciação do COAUD:** Os RE são apresentados ao COAUD para revisão e validação;
6. **Submeter RE para aprovação pelo CA:** Os RE serão apreciados pelo CA, para a aprovação dos riscos que farão parte do portfólio de Riscos Estratégicos, conforme previsto na legislação.

Os demais detalhes sobre a identificação e análise dos Riscos Estratégicos devem ser considerados conforme descrito na seção 7.2 deste documento.

9.3. Avaliação dos riscos e verificação dos controles

A avaliação dos Riscos Estratégicos é realizada após sua aprovação pelo CA e visa promover o entendimento do Nível de Risco e de sua natureza, auxiliando na definição de prioridades e opções de tratamento aos riscos identificados**.**

Por meio da avaliação, é possível saber qual a chance, a probabilidade de os riscos virem a acontecer e calcular seus respectivos impactos no Serpro, tanto para riscos negativos, quanto positivos. Esta etapa deverá ser realizada conforme descrito na seção 7.3 deste documento, considerando que:

- Para riscos negativos, compara-se o Nível de Risco Atual (NRA) com o apetite do RE ou RN negativo identificado. Se for superior ao apetite, deverá ser tratado (reduzido). Caso seja igual ou inferior, deverá ser aceito.
- Para riscos positivos, compara-se o Nível de Risco Atual (NRA) com o apetite do RE ou RN positivo identificado. Se for inferior ao apetite, deverá ser tratado (potencializado). Caso seja igual ou superior, deverá ser aceito.

Para os Riscos Estratégicos aprovados devem ser definidos os Indicadores Chave de Riscos (KRI) conforme a Orientação Técnica descrita no Anexo 1B deste documento.

9.4. Priorização para tratamento dos riscos

Esta etapa deverá ser realizada conforme descrito na seção 7.4 deste documento.

Todos os RE com resposta definida como “tratar”, terão a mesma priorização, ou seja, independente do NRA, cada RE terá o tratamento igualmente priorizado.

9.5. Definição dos controles de respostas aos riscos

Esta etapa deverá ser realizada conforme descrito na seção 7.5 deste documento. Observar que, para Riscos Estratégicos e Riscos ao Negócio, controles existentes devem ser informados com sua data de implementação e responsável. Devem ser identificados no momento do mapeamento do risco atual. Quando da realização da Análise Crítica pelo Agente Corporativo de Riscos e Controles, os controles existentes que não tenham pelo menos um registro de verificação, serão avaliados;

Todos os riscos estratégicos e ao negócio são considerados riscos críticos e devem ser analisados com maior atenção.

9.6. Validação dos resultados das etapas anteriores

Esta etapa deverá ser realizada conforme descrito na seção 7.6 deste documento.

Conforme definido no estatuto do Serpro, o Conselho de Administração é responsável pela aprovação dos Riscos Estratégicos.

O gestor do Risco Estratégico deve ser o Diretor responsável pelo acompanhamento do risco, podendo ser delegado para superintendente ou ocupante de função GR-II.

9.7. Comunicação e consulta

Estas atividades alcançam mais importância no trabalho com os Riscos Estratégicos, por envolver cenários externos relacionados à tecnologia, economia e regulação, dentre outros.

Deverá ser realizada de acordo com o descrito na seção 7.7 desta metodologia.

9.8. Registro, relato e contingência

Deverá ser realizada conforme descrito na seção 7.8.

Ressalta-se que:

- Os riscos Estratégicos ou ao Negócio, devem passar por processo de aprovação pelos Órgãos Colegiados, antes do seu registro na ferramenta corporativa de gestão de riscos.
- No caso de solicitação de cancelamento de riscos estratégicos ou ao negócio, o processo exige aprovação final pelos órgãos colegiados, precedida por análises sequenciais realizadas pelo Especialista da Tipologia, pelo Agente Corporativo e pelo Aprovador do Risco. A decisão de submeter o cancelamento aos colegiados ocorre somente se todos esses atores considerarem a solicitação pertinente. O registro de cancelamento só poderá ser efetivado na ferramenta corporativa de gestão de riscos após a aprovação final pelos órgãos colegiados.

9.9. Análise crítica e monitoramento

9.9.1. Análise crítica

Para os riscos estratégicos e de negócio devem ser considerados os aspectos abaixo.

No momento da análise crítica, os controles existentes que não tenham pelo menos um registro de verificação, devem ser verificados.

Sempre que um controle passe para o estado "implementado", o Agente Corporativo de Riscos e Controles deve fazer e registrar a sua verificação, atestando, com coleta e registro de evidências da:

a) sua **presença**, pela existência de modelagem de processo descrita e publicada, existência de procedimento operacional descrito e publicado, ou pela aferição de procedimento *ad-hoc*;

b) seu **funcionamento**, pelo acompanhamento do processo e coleta de artefatos intermediários que possam inferir com segurança seu funcionamento.

Para os Riscos Estratégicos e Riscos ao Negócio, a verificação de cada um dos controles relacionados deve ser registrada na ferramenta corporativa de gestão de riscos, juntamente com as evidências coletadas e com a identificação do Agente Corporativo de Riscos e Controles que efetuou a verificação, bem como a evidência do momento que essa verificação foi executada.

9.9.2. Monitoramento

O **monitoramento** deve ser realizado pela 1ª. Linha e documentado por meio de Painel de Indicadores corporativo específico em uso na empresa. A fase de monitoramento envolve duas etapas:

a) A primeira é verificar se o Plano de Ação proposto está sendo executado; e

b) A segunda é analisar a evolução das condições dos riscos identificados, verificar se houve mudanças ou alterações no ambiente interno ou externo que afetam o Nível do Risco.

Com base no Plano de Ação, o responsável pelo Risco Estratégico deve elaborar o registro e o relato sobre a sua execução e submeter a 2ª. Linha, com periodicidade máxima de três meses (janeiro, abril, julho e outubro).

Maiores detalhes sobre a análise crítica e monitoramento podem ser verificadas na seção 7.9 deste documento.

9.10. Implementação dos controles de respostas aos riscos

A implementação dos controles de resposta aos riscos envolve a participação da Unidade Organizacional responsável pelo risco estratégico e das unidades relacionadas como corresponsáveis em cada iniciativa, se previstas.

As atividades relativas à gestão de Riscos Estratégicos e Riscos ao Negócio deverão ser realizadas conforme descrito na seção 7.10 deste documento, tanto para riscos negativos quanto para riscos positivos.

REFERÊNCIAS BIBLIOGRÁFICAS

- Associação Brasileira de Normas Técnicas – ABNT
  NBR ISO 31000 – Gestão de riscos: Diretrizes
  Rio de Janeiro, 2018.
- Associação Brasileira de Normas Técnicas – ABNT
  NBR ISO 31004 Gestão de Riscos – Guia para Implementação da ABNT ISO 31000
  Rio de Janeiro, 2009.
- Brasiliano INTERISK – Inteligência em Riscos
  www.brasiliano.com.br/software-interisk-apetite-riscos
  (último acesso em 05/12/2024)
- Committee of Sponsoring Organizations – COSO
  Gerenciamento de Riscos Corporativos – Estrutura Integrada
  New Jersey, 2007.
- Committee of Sponsoring Organizations – COSO
  Gerenciamento de Riscos Corporativos – Sumário Executivo
  Brasil, 2017.
- Corpo Comum de Conhecimento – CBOK 3.0
  Guia de Orientação para Gestão de Processos de Negócio – BPM
  São Paulo, 2009.
- Elo Group – Handbook para Gestão de Riscos Positivos
  ©Outubro 2007. ELO Group – www.elogroup.com.br
- Gestão de Riscos – Avaliação da Maturidade
  Tribunal de Contas da União, SEGECEX, janeiro de 2018.
  Disponível: https://portal.tcu.gov.br/biblioteca-digital/gestao-de-riscos-avaliacao-da-maturidade.htm
  (último acesso em 05/12/2024)
- Gestão de Riscos – Diretrizes para Implementação da ISO 31000:2018
  Coleção Risk Tecnologia
  São Paulo, 2018.
- Gestão de Riscos Positivos
  André Macieira, Daniel Karrer, Leandro Jesus e Rafel Clemente
  Editora Sicurezza, 1ª. Edição, 2011

- Guia Prático de Gestão de Riscos a Integridade – CGU
  Ministério da Transparência e Controladoria-Geral da União – 2018
  https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/manual-gestao-de-riscos.pdf
  (último acesso em 05/12/2024)
- Instrução Normativa Conjunta Nº. 1, de 10 de maio de 2016, do Ministério do Planejamento, Orçamento e Gestão e Controladoria-Geral da União
  Diário Oficial da União de maio de 2016.
- Metodologia de Gestão de Riscos
  Ministério da Transparência e Controladoria-Geral da União – CGU
  Brasília, abril de 2018.
- Referencial Básico de Gestão de Riscos
  Tribunal de Contas da União, SEGECEX, abril de 2018.
  Disponível: https://portal.tcu.gov.br/planejamento-governanca-e-gestao/gestao-de-riscos
  (último acesso em 05/12/2024)
- Tribunal de Contas da União - Gestão de Riscos: Glossário. Disponível em: https://portal.tcu.gov.br/governanca/governancapublica/gestao-de-riscos/glossario.htm
  (último acesso em 05/12/2024)

FICHA TÉCNICA

Alexandre Goncalves de Amorim
Diretor Presidente – DP

Alexandre Brandao Henriques Maimoni
Diretor Jurídico, de Gestão e Riscos – DIJUG

Ana Flavia Bastos Guedes Resende
Superintendente de Controles, Riscos e Conformidade – DIJUG/SUPCR

Raquel de Carvalho Drummond de Sant Ana
Gerente do Departamento de Gestão de Riscos e Controles – DIJUG/SUPCR/CRGRC

Daniella Freitas Garcia Dupin
Gerente da Divisão de Estratégia de Gestão de Riscos – DIJUG/SUPCR/CRGRC/CRGER

Fernando Cezar Xabregas
Gerente da Divisão de Gestão de Riscos e Controles – DIJUG/SUPCR/CRGRC/CRRIC

Equipe técnica:
Alexandre Vieira Coutinho – DIJUG/SUPCR/CRGRC/CRGER
Amanda Lobato Cunha – DIJUG/SUPCR/CRGRC/CRRIC
Claudia de Moraes Amaral Marques – DIJUG/SUPCR/CRGRC/CRRIC
Claudia Ferreira Giambastiani da Silva – DIJUG/SUPCR/CRGRC/CRRIC
Gerson Augusto Maturana Lage - DIJUG/SUPCR/CRGRC/CRGERG
Gustavo Assis Chaves – DIJUG/SUPCR/CRGRC/CRGER
Nilson Costa da Silva – DIJUG/SUPCR/CRGRC/CRRIC
Patrícia Borges de Sousa Wasowski – DIJUG/SUPCR/CRGRC/CRGER

Anexo 1A

ORIENTAÇÃO TÉCNICA PARA A TIPOLOGIA DE RISCOS À INTEGRIDADE

1. CONTEXTUALIZAÇÃO

Os riscos à integridade derivam de ações, omissões ou vulnerabilidades que possam favorecer ou facilitar a ocorrência de práticas de corrupção, fraude, irregularidade, desvio ético e/ou de conduta, comprometendo a consecução dos objetivos organizacionais.

Nesse sentido, é importante pontuar que o favorecimento ou facilitação da ocorrência dessas práticas não deve ser entendido apenas em termos de infração e/ou descumprimento de leis, regulamentos, normativos etc. Essas ações ou omissões, de acordo com a Política de Integridade e Anticorrupção do Serpro, enquadram-se como uma "**quebra de integridade**", assim definida:

> *"Situação caracterizada quase sempre como um ato doloso, praticado por uma pessoa ou grupo de pessoas, e que envolve a afronta aos princípios da administração pública, englobando atos como corrupção, fraude, abuso de poder, conflito de interesses, nepotismo, desvios éticos, dentre outros." (Política de Integridade e Anticorrupção do Serpro, 2024).*

Contudo, esse tipo de favorecimento ou facilitação também deve ser entendido de maneira mais ampla, englobando atos como suborno, desvio de verbas, abuso de poder e/ou influência, nepotismo, conflito de interesses, uso indevido e/ou vazamento de informação sigilosa, práticas antiéticas, dentre outras práticas.

De modo geral, essas condutas compartilham as seguintes características[1]:

a) é um ato quase sempre doloso, à exceção de certas situações envolvendo conflito de interesses, nepotismo etc.;

b) é um ato humano, ou seja, praticado por uma pessoa ou por um grupo de pessoas;

c) envolve uma afronta aos princípios da administração pública, como legalidade, impessoalidade, moralidade, publicidade e eficiência, mas destaca-se mais fortemente como uma quebra à impessoalidade e/ou moralidade; e

d) envolve alguma forma de deturpação, desvio ou negação da finalidade pública ou do serviço público a ser entregue ao cidadão.

---

[1] Guia prático de gestão de riscos para a integridade: Orientações para a administração pública federal direta, autárquica e fundacional. (CGU, 2018).

A partir das características e orientações explicitadas, podemos iniciar a identificação dos riscos à integridade, sendo importante ressaltar que a identificação, a gestão, o monitoramento e o tratamento desses riscos devem seguir a Metodologia de Gestão de Riscos e Controles Internos e, de forma complementar, o disposto nesta Orientação Técnica.

2. COMO IDENTIFICAR UM RISCO À INTEGRIDADE

De forma geral, o risco à integridade se materializa quando um agente público adota uma conduta profissional inadequada e a sua materialização traz sérias consequências para a empresa, como comprometimento da base de dados e/ou fornecimento de informações não fidedignas, prestação de contas não fidedignas, favorecimento da corrupção ativa ou passiva, fraude em processos, prejuízos financeiros, danos à imagem e à reputação da empresa etc.

Algumas áreas e processos são mais sensíveis à ocorrência de riscos à integridade, como áreas de aquisições e contratações, gestão financeira etc. Contudo, os riscos à integridade podem estar presentes em diferentes áreas e processos da empresa, assim como sua ocorrência de forma reiterada também pode variar a depender do caso específico.

Nesse sentido, um risco à integridade pode estar associado a um único processo da cadeia de valor, direta ou indiretamente, ou a vários processos afins. Cabe ao gestor identificar os riscos à integridade dos processos sob sua responsabilidade e, se for o caso, sua correlação e impacto em outros processos da empresa.

Algumas perguntas podem auxiliar na identificação de possíveis riscos à integridade, quais sejam:

a) Há vulnerabilidades vinculadas aos processos sob a minha responsabilidade que podem favorecer ou facilitar a ocorrência de atos de fraude e de corrupção? Quais?

b) Há a possibilidade de utilização de recursos da empresa em favor de interesses privados vinculados aos processos sob a minha responsabilidade?

c) Há vulnerabilidades vinculadas aos processos sob a minha responsabilidade que possibilitem o oferecimento ou a aceitação de qualquer tipo de vantagem indevida? Quais?

d) Há vulnerabilidades vinculadas aos processos sob a minha responsabilidade que possibilitem a ocorrência de conflito de interesses? Quais?

e) Quais fatores relacionados aos processos sob a minha responsabilidade podem favorecer ou facilitar a ocorrência de práticas de corrupção, fraude, irregularidades e/ou desvios éticos e de conduta? São exemplos: descumprimento de leis e/ou

normas internas, ausência de alçada financeira e/ou de gestão compartilhada, processos e controles geridos de forma manual (não automatizada), dentre outros.

A materialização de riscos à integridade pode ser evitada por meio do estabelecimento de controles preventivos, como ações de comunicação e de capacitação para o corpo gerencial e funcional, campanhas de conscientização, estabelecimento de políticas e normas internas, informatização de processos, dentre outros. Por exemplo, no processo de Gestão Financeira, os controles preventivos para mitigar o risco de ocorrer uma transferência de recursos não autorizada, podendo ser a validação pelo gerente de todas as transações realizadas pelo empregado (*double check*) e/ou o estabelecimento de alçadas financeiras compartilhadas conforme valor da transação a ser realizada.

Já os controles contingenciais devem ser estabelecidos com a finalidade de recuperar ou atenuar o impacto quando da materialização de um risco à integridade, visando tratar as consequências e minimizar os impactos para a empresa. Estes podem se dar em forma de sindicâncias, processo administrativo disciplinar, realização de apurações e auditorias, entre outros.

2.1. Importante

O nome do risco deve apontar a irregularidade, exemplo: "Alteração indevida do código fonte com a intenção de manipular dados." Este apontamento caracteriza que é um risco à integridade, pois a alteração do código fonte foi intencional, não tendo sido apenas um erro material.

No Serpro, o **Apetite a Risco** definido para a **Tipologia de Riscos à Integridade** é **"muito baixo"** e, por isso, por menor que seja a sua probabilidade e o seu impacto para a empresa, estes devem ser sempre monitorados pelo gestor. Para tanto, a **estratégia adotada será, preferencialmente, "TRATAR"**, devendo ser estabelecido pelo menos um controle proposto ou uma melhoria em controle existente até que o Nível de Risco atinja o Apetite a Risco definido.

Contudo, se os **controles existentes não forem suficientes para se atingir o nível de Apetite a Risco desejado** ou, **caso o risco se materialize, estes já resguardam em maior parte as suas consequências**, **poderá ser adotada a Estratégia "ACEITAR"**, com a devida justificativa, desde que esta seja acatada pelo Especialista da área de Integridade. É importante ressaltar que um risco à integridade aceito não deixa de existir, ou seja, este não deve ser cancelado, prevalecendo o seu monitoramento contínuo.

A partir das orientações apresentadas, seguem alguns exemplos de riscos à integridade[2]:

[2] Guia prático de gestão de riscos para a integridade: Orientações para a administração pública federal direta, autárquica e fundacional. (CGU, 2018)

a) **abuso de posição ou poder em favor de interesses privados** – conduta contrária ao interesse público, valendo-se da sua condição para atender interesse privado, em benefício próprio ou de terceiros, como concessão de cargos ou vantagens em troca de apoio ou auxílio; esquivar-se do cumprimento de obrigações; falsificação de informação para interesses privados; dentre outras.

b) **Nepotismo** – este pode ser entendido como uma das formas de abuso de posição ou poder em favor de interesses privados, em que se favorecem familiares. O nepotismo pode ser presumido ou requerer apuração específica.

   i. **nepotismo presumido:** contratação de familiares para cargos em comissão e função de confiança; contratação de familiares para vagas de estágio e de atendimento a necessidade temporária de excepcional interesse público; contratação de pessoa jurídica de familiar por agente público responsável por licitação etc.; e

   ii. **apuração específica:** nepotismo cruzado; contratação de familiares para prestação de serviços terceirizados; nomeações, contratações não previstas expressamente no decreto etc.

c) **conflito de interesses** – situação gerada pelo confronto entre interesses públicos e privados, que possa comprometer o interesse coletivo ou influenciar, de maneira imprópria, o desempenho da função pública, como uso de informação privilegiada; relação de negócio com pessoa física ou jurídica que tenha interesse em decisão; atividade privada incompatível com o cargo; atuar como intermediário junto à administração; praticar ato em benefício de pessoa jurídica (em que participe o servidor ou parente); receber presente de quem tenha interesse em decisão; etc.

d) **pressão interna ou externa ilegal ou antiética para influenciar agente público** – pressões explícitas ou implícitas de natureza hierárquica (interna), de colegas de trabalho (organizacional), política ou social (externa), que podem influenciar indevidamente atuação do agente público.

   i. **Formas de pressão interna ilegal ou antiética:** influência sobre empregados subordinados para violar sua conduta devida; e ações de retaliação contra possíveis denunciantes; e

   ii. **Formas de pressão externa ilegal ou antiética:** *lobby* realizado fora dos limites legais ou de forma antiética; e pressões relacionadas a tráfico de influência.

e) **solicitação ou recebimento de vantagem indevida** – caracteriza-se por qualquer tipo de enriquecimento ilícito, seja dinheiro ou outra utilidade, dado que ao agente público não é permitido colher vantagens em virtude do exercício de suas atividades.

Os tipos mencionados acima não exaurem todas as possibilidades de manifestação de riscos à integridade.

Os riscos à integridade são monitorados pela área de Integridade Institucional e apresentados por meio do Relatório de Integridade Institucional para a Diretoria Executiva, o Comitê de Auditoria e os Conselhos de Administração e Fiscal, de modo a permitir o devido acompanhamento das ações de mitigações estabelecidas pelos colegiados.

3. RESPONSABILIDADES

Dentre os principais atores envolvidos no processo de gestão de riscos à integridade destacam-se:

Os empregados e gestores representam a primeira linha e são responsáveis por identificar e avaliar riscos, mitigando-os por meio da implementação de ações preventivas, contingenciais ou corretivas, de forma a resolver possíveis deficiências em processos e controles. Esta linha deve implementar controles internos destinados a garantir que as atividades sejam realizadas de acordo com os objetivos organizacionais e em conformidade com as expectativas legais, regulatórias, estatutárias e éticas.

A área de Integridade Institucional representa a segunda linha e é responsável por apoiar a primeira linha na identificação, supervisão e tratamento dos riscos à integridade.

A área de Gestão de Riscos e Controles Internos também representa a segunda linha, sendo responsável por orientar, coordenar e promover o alinhamento da gestão de risco e dos controles internos com a estratégia empresarial.

Os Administradores são responsáveis:

a) pelo estabelecimento da estratégia empresarial, assim como direcionar e supervisionar os sistemas de gestão de riscos e controles internos; e

b) por estabelecer, manter, monitorar e aprimorar o sistema de gestão de riscos e controles internos com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos à integridade que possam impactar a implementação da estratégia e a consecução dos objetivos organizacionais.

4. CONCLUSÃO

A identificação dos riscos à integridade permite ao gestor conhecer fragilidades que possam favorecer ou facilitar a ocorrência de práticas de corrupção, fraude, irregularidades e/ou desvios éticos relacionados aos processos sob sua responsabilidade e, a partir dessa identificação, gerir e tratar esses riscos a fim de reduzir a sua ocorrência e o seu impacto para a empresa caso se materialize.

Anexo 1B

ORIENTAÇÃO PARA A DEFINIÇÃO DE INDICADORES CHAVE DE RISCOS (KRI)

ORIENTAÇÃO PARA A DEFINIÇÃO DE INDICADORES CHAVE DE RISCOS (KRI)

Na gestão de riscos, o indicador central utilizado é o *Key Risk Indicator* (KRI), uma ferramenta crucial para avaliar e monitorar eventos que podem impactar no atingimento dos objetivos da organização. No entanto, é importante compreender distintamente outros conceitos essenciais, como *Key Performance Indicators* (KPI) e *Objectives and Key Results* (OKR), para garantir uma abordagem abrangente na análise do desempenho e na consecução de metas organizacionais. Esses conceitos serão abordados a seguir, destacando a relevância de cada um na gestão eficaz de riscos, e examina como sua integração contribui para a tomada de decisões informadas e a sustentabilidade do sucesso empresarial.

KPI, **OKR** e **KRI** são termos relacionados à gestão e avaliação de desempenho em organizações, mas cada um tem um significado específico:

KPI (*Key Performance Indicator*): Indicador-Chave de Desempenho

Os KPI são medidas quantificáveis que refletem o desempenho de uma organização em relação a seus objetivos estratégicos. Estão diretamente associados às metas da organização ou de um determinado projeto. Eles fornecem uma maneira mensurável de monitorar o progresso e o sucesso na consecução dos objetivos estabelecidos. Também são conhecidos como metas de resultados.

Por exemplo, em uma empresa, os KPIs podem incluir indicadores como receita líquida, satisfação do cliente, taxa de conversão, entre outros.

OKR (*Objectives and Key Results*): Objetivos e Resultados-Chave.

Os OKR também estão relacionados às metas, mas eles oferecem uma abordagem mais específica e estruturada para definir e alcançar essas metas em momentos específicos. É uma abordagem que visa alinhar e direcionar as atividades da organização para alcançar objetivos estratégicos. Os objetivos são metas amplas e ambiciosas, enquanto os resultados-chave são indicadores mensuráveis e específicos que demonstram o progresso em direção a esses objetivos, criando assim uma estrutura mais tangível para melhorar os KPIs.

KRI (*Key Risk Indicator*): Indicador-Chave de Risco

Os KRI são indicadores utilizados para monitorar e avaliar a probabilidade e o impacto de eventos que podem afetar tanto positiva quanto negativamente uma organização. Eles ajudam a identificar potenciais oportunidades ou ameaças, reforçando a capacidade da organização em atingir seus objetivos relacionados ao risco.

Não há uma regra rígida sobre se os *Key Risk Indicators (*KRI) devem estar relacionados apenas a controles preventivos ou também a controles contingenciais. A escolha dependerá da

estratégia de gestão de riscos da organização, da natureza dos riscos envolvidos e dos objetivos específicos.

- **KRI Relacionados a Controles Preventivos:**
  - Podem medir a eficácia na implementação e manutenção de controles preventivos para evitar a ocorrência de eventos indesejados.
  - Exemplos incluem taxas de conformidade com políticas e procedimentos, eficácia de treinamentos preventivos, entre outros.
- **KRI Relacionados a Controles Contingenciais:**
  - Podem medir a eficácia dos planos e controles de contingência e a prontidão da organização para responder a eventos indesejados.
  - Exemplos incluem o tempo de recuperação após uma interrupção, eficácia de planos de continuidade de negócios, entre outros.

Muitas organizações adotam uma abordagem equilibrada, usando KRI para avaliar tanto a eficácia dos controles preventivos quanto a preparação para responder a eventos contingenciais. A ideia é ter uma visão abrangente dos riscos, desde sua prevenção até a resposta a possíveis incidentes.

Da mesma forma, não é estritamente necessário ter um *Key Risk Indicator* (KRI) para cada controle específico. Os KRI podem ser projetados para avaliar a eficácia combinada de vários controles ou podem estar relacionados a objetivos mais amplos da organização. Algumas abordagens possíveis incluem:

- **KRI Agregados:** Desenvolva KRI que avaliem a eficácia geral de um conjunto de controles em mitigar um risco específico. Isso pode envolver uma análise combinada de vários controles relacionados.
- **KRI por Categoria de Controle:** Agrupe controles semelhantes em categorias e desenvolva KRI que avaliem a eficácia dessas categorias. Isso oferece uma visão mais ampla sem a necessidade de KRI individuais para cada controle.
- **KRI Relacionados a Objetivos de Controle**: Alinhe os KRI aos objetivos gerais dos controles. Se um controle visa mitigar o risco de fraude, o KRI pode focar na detecção eficaz de atividades suspeitas, considerando a combinação de controles relevantes.

Os KRI desempenham um papel fundamental na verificação da eficácia dos controles e na tomada de decisões proativas para gerenciar os riscos de uma organização.

Em resumo, o importante é garantir que os KRI escolhidos forneçam informações valiosas para a tomada de decisões informadas sobre a gestão de riscos e o alcance dos objetivos organizacionais.

É importante alinhar os KRI com os objetivos estratégicos da organização e garantir que forneçam *insights* valiosos para a tomada de decisões informadas sobre a gestão de riscos. Independentemente da abordagem escolhida, a análise contínua e a adaptação dos KRI são essenciais para garantir que estejam alinhados com a dinâmica do ambiente de negócios e os objetivos organizacionais em constante mudança.

Idealmente, indicadores chave de riscos eficazes possuem características, como:

a) **Relevância**: os KRI devem ajudar a identificar, quantificar, monitorar e gerenciar riscos associados aos principais objetivos do negócio, ou seja, à estratégia organizacional.

b) **Mensurável**: como todo indicador, o de riscos precisa ser quantificável (que pode ser traduzido em um número, porcentagem *etc.*)

c) **Preditivo**: é capaz de prever problemas futuros sobre os quais a administração pode agir preventivamente.

d) **Fácil de monitorar**: simples de coletar, analisar e relatar.

e) **Auditável**: fácil de verificar como as informações foram obtidas.

f) **Comparável**: os indicadores chave de riscos devem também possibilitar a comparação tanto no âmbito interno quanto com os padrões da indústria.

Em resumo, enquanto OKR se concentra em estabelecer metas e resultados-chave para impulsionar a realização de objetivos estratégicos, KPIs são medidas de desempenho usadas para avaliar o sucesso em atingir esses objetivos, e KRI são indicadores que alertam sobre possíveis ameaças ou oportunidades que podem impactar a organização no atingimento dos objetivos.

Para clarificar esses conceitos apresentamos a seguir uma situação exemplo.

Pretendo viajar de uma cidade a outra chegando ao destino em 7 horas. Devo considerar que, em todo o trecho da viagem, a velocidade máxima estipulada é de 100Km/h.

Vamos avaliar abaixo o objetivo, as metas, possíveis riscos que envolvem o atingimento do objetivo e das metas associadas, as causas dos riscos, controles que devem ser considerados, bem como descrever os OKR, KPIs e KRI que envolvem essa situação.

Objetivo: Completar a viagem de carro rapidamente e de maneira eficiente.

Metas:

1. **Meta de Tempo (MT):** Chegar ao destino em 7 horas.
2. **Meta de Velocidade (MV):** Não ultrapassar a velocidade de 100 km/h.
3. **Meta de Velocidade Média (MM):** manter velocidade média mínima de 80 Km/h.

Riscos:

1. **Trânsito intenso:**
   - **Causa:** Acidentes, obras na estrada, congestionamentos.
   - **Controle:** Monitoramento em tempo real do tráfego, uso de aplicativos de navegação, utilizar rotas alternativas.
2. **Condições meteorológicas adversas:**
   - **Causa:** Chuva intensa, neblina, tempestades.
   - **Controle:** Verificação de previsões meteorológicas antes da viagem, ajuste do plano conforme as condições.
3. **Problemas mecânicos no veículo:**
   - **Causa:** Falha no motor, pneus furados, problemas na bateria, temperatura do líquido de arrefecimento do motor.
   - **Controle:** Revisão prévia do veículo, monitorar as condições do veículo, transporte de equipamentos de emergência.

OKR:

- **Objetivo (O):** Completar a viagem de carro rapidamente e de maneira eficiente.
- **Resultados-Chave (KR):**
  a) **KR(a)**: Alcançar a Meta de Tempo (MT).
  b) **KR(b):** Não ultrapassar a Meta de Velocidade (MV).
  c) **KR(c):** Manter a Meta de Velocidade Média (MM).

KPI:

a) Tempos medidos durante a viagem.
b) Velocidades média e máxima efetivas durante o percurso.

KRI:

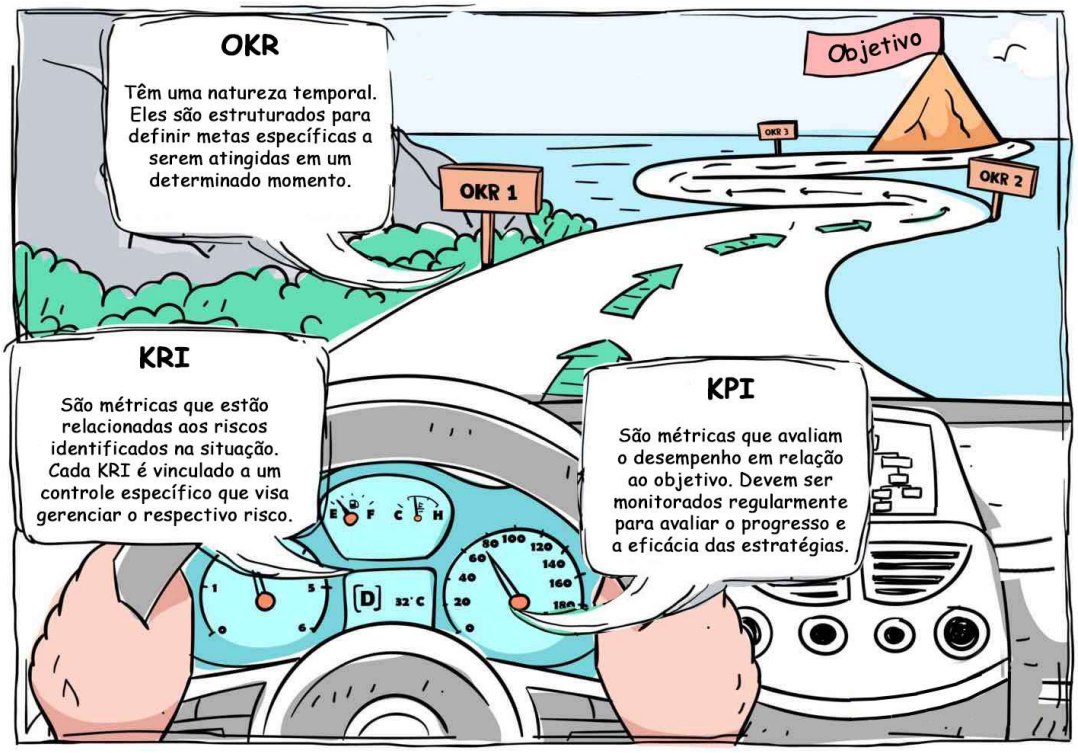
a) Índice de tráfego (indicador de possíveis congestionamentos ou atrasos).

b) Alertas meteorológicos (indicador de condições adversas no percurso).

c) Histórico de manutenção do veículo (indicador de possíveis falhas mecânicas) / Monitoramento das condições do veículo durante a viagem (painel de instrumentos).

A figura a seguir ilustra didaticamente estas medidas.

Figura 17 – OKR, KPI e KRI



Fonte: https://www.perdoo.com/resources/strategy-okrs-and-kpis/

No contexto da situação que discutimos, as metas eram chegar ao destino em 7 horas, manter uma velocidade média de 80 Km/h e não ultrapassar a velocidade de 100 km/h. Os **KPI** associados a essas metas poderiam incluir a verificação do tempo da viagem e a velocidade média e máxima durante o percurso a fim de se verificarem os resultados da viagem. Estes KPIs forneceriam indicadores claros e mensuráveis do desempenho em relação ao objetivo estabelecido, durante o desenrolar da viagem.

Como vimos, os **OKR** são uma ferramenta de gestão que ajuda a traduzir metas em ações específicas e mensuráveis. No contexto da viagem de carro, o objetivo de completá-la de maneira eficiente se desdobram em resultados-chave que podem incluir alcançar o destino em 7 horas, mantendo uma velocidade inferior a 100 km/h. Definir um resultado chave associado à velocidade média também seria importante, uma vez que, quanto maior, menor o tempo da

viagem. Os OKR são o roteiro dinâmico em direção ao destino. À medida que se avança, o terreno pode mudar, obstáculos podem aparecer e as condições podem ficar desfavoráveis. É por isso que os OKR, mudam conforme se avança em direção ao seu objetivo final. Esses resultados-chave tornam o objetivo mais concreto e fornecem critérios claros para avaliar o sucesso, principalmente quando avaliados no decorrer da viagem de nosso exemplo, referenciados como OKR1, OKR2 e OKR3 na Figura 17.

Os **KRI** estão relacionados aos riscos identificados na situação da viagem de carro, e cada KRI é vinculado a um controle específico que visa gerenciar o respectivo risco. É preciso ficar de olho no painel do carro para garantir que o motor não superaqueça e que o combustível não acabe enquanto se avança em relação ao destino. Os KRI são indicadores que ajudam a monitorar e alertar continuamente os fatores de risco durante a viagem, permitindo ações preventivas e ajustes para garantir um percurso seguro e bem-sucedido.

Note que, para se definir os KRI é necessário que as causas e consequências relacionadas ao risco, bem como os controles envolvidos já estejam definidos. Os KRI estão diretamente associados aos controles porque ajudam a avaliar se eles estão operando conforme o esperado e se são suficientes para atuar nos riscos identificados, minimizando riscos negativos ou alavancando riscos positivos. Se um KRI indicar que um determinado risco está se aproximando de um nível inaceitável, isso pode sinalizar a necessidade de revisão ou reforço nos controles existentes.

Note ainda que existe uma relação entre risco e desempenho, e para ilustrar, imagine que o objetivo da viagem seja o de vencer um rali e cruzar a linha de chegada antes de qualquer outro participante. Essa linha de chegada se assemelha ao objetivo final da sua organização (a missão e a visão).

Rapidamente podemos imaginar o surgimento de novos concorrentes. Para se preparar para o rali, você precisa determinar quais recursos seu carro precisa. Você terá que entender a pista de corrida, seus concorrentes *etc*. Essas informações influenciarão o tipo de carro que você precisa, inclusive o seu desempenho para aquela situação específica. Estas decisões críticas são os seus Pilares Estratégicos.

Da mesma forma, nos negócios, trata-se de conhecer seus concorrentes, compreender seus clientes-alvo e avaliar seu mercado. Cada organização é única, com as suas próprias prioridades, circunstâncias e recursos, e essa é a base sobre a qual deve ser construída a estratégia. Assim, essa empresa pode ter um KRI para monitorar os riscos de perda de participação no mercado, relacionados à diminuição da carteira de clientes e ao aumento da concorrência.

Como um motorista atento ao painel durante uma viagem, os KRI nas organizações desempenham um papel estratégico, possibilitando ajustes contínuos para garantir um percurso seguro em direção aos objetivos, assim como a linha de chegada em uma corrida de rali. A relação entre risco e desempenho demanda compreensão do cenário competitivo,

adaptação estratégica de recursos e decisões fundamentadas. Os KRI, atuando como faróis estratégicos, alertam tanto para ameaças quanto para oportunidades, orientando decisões que preservam a participação de mercado e impulsionam o sucesso empresarial.

Anexo 1C

MÉTODO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO (GRSI)

1. INTRODUÇÃO

A Gestão de Riscos de Segurança da Informação (GRSI) tem como foco a atuação nos riscos que impactam a confidencialidade, disponibilidade, integridade e autenticidade, abrangendo as informações, serviços, processos, sistemas de informação e recursos gerenciados e sob guarda do Serpro. Esses riscos estão associados com o potencial de ameaças que possam explorar vulnerabilidades de um ativo de informação, causando danos à organização e que serão objetos de tratamento.

Para tanto, adota o Método de Gestão de Riscos para Segurança da Informação (GRSI) de acordo com as orientações da Política Corporativa de Segurança da Informação (PCSI), com o modelo de gestão da segurança adotado pelo Programa de Segurança do Serpro (PSS), e alinhado com a Metodologia de Gestão de Riscos e Controles.

2. FINALIDADE

Alinhar as orientações gerais da gestão de riscos de segurança da informação – método GRSI (Gestão de Riscos de Segurança da Informação) com a metodologia de gestão de risco e controles. O Método GRSI deve ser aplicado na entrada em produção de novos serviços e nas situações de alteração de arquitetura dos serviços.

3. APRESENTAÇÃO DO GRSI

A gestão de Risco de Segurança da Informação (GRSI) descreve as etapas de Risco de Projeto, Escopo e Contexto, Identificação e Análise, Avaliação dos riscos e verificação dos Controles, Priorização e Tratamento de riscos. Utiliza a ferramenta de gerenciamento de riscos adotada pela empresa, na qual os riscos estão identificados sob a Tipologia de Gestão de Riscos de Segurança (GRSI).

As informações do GRSI são categorizadas como sigilosas em consonância com a Norma que trata sobre a Classificação dos Ativos de Informação do Serpro.

4. ETAPAS DO GRSI

4.1. Risco de Projeto – Finalidade e Uso

O Risco de Projeto no método GRSI tem por finalidade agregar os riscos de um mesmo escopo.

> **IMPORTANTE**: Caso após a análise, seja identificada que as alterações ocorridas no sistema ou recurso não motivem a inclusão de novos riscos, essa decisão deverá ser documentada no campo Descrição do Projeto, bem como a justificativa.

4.1.1. Estabelecimento do Escopo e Contexto

Escopo é o conjunto de informações pertinentes a um GRSI, é o objetivo que se pretende atingir, como por exemplo, um Serviço, Recurso ou Processo.

Nesta etapa são abordadas a definição do escopo e seus limites, critérios básicos necessários para a gestão de riscos de segurança da informação.

Na ferramenta de gerenciamento de riscos, deve ser registrado o escopo no Risco de Projeto com uma breve descrição, se possível, seguido do código de serviço, a fim de associar a ele, todos os riscos e atores envolvidos, tais como: os facilitadores responsáveis por conduzirem o GRSI, e os participantes do GRSI – Unidade de Relacionamento com o Cliente, Desenvolvimento, Áreas operacionais da produção, dentre outras áreas envolvidas, caracterizando as partes interessadas.

4.2. Processo de Avaliação de Risco

4.2.1. Identificação dos Riscos

Os participantes da reunião de GRSI identificam os riscos associados ao processo, serviço ou recurso, de acordo com os aspectos de segurança da Informação (integridade, confidencialidade, disponibilidade e autenticidade), assim como a privacidade mediante a utilização das técnicas:

- *Brainstorming* para identificação dos riscos associados a Segurança através de exposição de ideias; ou,
- Arquitetura de Referência, para identificação dos riscos associados, comparando-a com a Arquitetura do Escopo, e se dedicam a verificação de riscos complementares apenas.

Observações:

- Identificação de riscos de alterações de Sistema ou Aplicação que já está em produção ou Recursos computacionais - os artefatos que servem de insumos para a identificação dos riscos são:
  - RTA (Reunião Técnica de Arquitetura) da solução já existente;
  - DASI (Documento de Arquitetura Simplificada de Infraestrutura);
  - Topologia ou Arquitetura com as alterações.
- Identificação de riscos de Sistema ou Aplicação que vai entrar em produção - os artefatos que servem de insumos para a identificação dos riscos são:
  - RTA (Reunião Técnica de Arquitetura) que tem como insumos a Arquitetura de Software Preliminar, os Documentos da Solução e o PIMP (Plano de Implantações de Ações) preliminar;

- DASI (Documento de Arquitetura Simplificada de Infraestrutura);
- AMISP - Análise Multidisciplinar de Segurança e Privacidade (caso realizada).

- Todos os riscos devem ser registrados, mesmo os que já possuam controles de tratamento de riscos em vigor.
- Considerações sobre o *Brainstorming:*
  - Para auxiliar na identificação dos riscos, utilizar questões do tipo "que evento ou acidente poderia afetar a indisponibilidade ou causar dano ao ativo?";
  - É fundamental que os facilitadores permaneçam neutros durante a atividade;
  - Não julgar as ideias (não existem ideias ruins);
  - Cada situação deve ser discutida e entendida por todos os participantes;
  - Todos devem contribuir;
  - Manter o encontro dentro do horário acordado (não dispersar em discussões paralelas ou filosóficas).
- Considerações sobre a Arquitetura de Referência (arquitetura com os riscos pré-definidos):
  - A arquitetura de referência será comparada com a do escopo em análise;
  - Os riscos em comum foram previamente definidos;
  - Caso haja mais algum risco a ser identificado, será alvo de avaliação complementar junto aos participantes;
  - Todos os participantes devem contribuir.

IMPORTANTE: A identificação dos riscos deve incluir os ativos envolvidos no escopo. O nível de detalhe utilizado na identificação dos riscos influenciará o aprofundamento em cada iteração na avaliação de riscos.

O levantamento dos ativos é importante, pois a partir deles é que são consideradas as vulnerabilidades, em função das ameaças. As categorias de ativos podem opcionalmente ser associados a cada risco identificado.

Associação a Categoria de Ativos – A fim de correlacionar os riscos com os ativos por eles atingidos, podem ser relacionadas as categorias de ativos para cada ameaça levantada. Isto permite evidenciar quais tipos de ativos estão associados a cada ameaça.

TABELA DE ATIVOS			
ATIVOS – PSS	**DESCRIÇÃO**	**CATEGORIA**	**EXEMPLOS**
INFORMAÇÃO	Alimenta as atividades produtivas ou processos de negócio. Também é produzida como resultado das atividades produtivas ou processos de negócio	Informação	▪ Informações armazenadas ▪ Dados armazenados / em trânsito ▪ Documentação de sistema ▪ Manual de usuário ▪ Material de treinamento ▪ Procedimentos operacionais e de suporte • Planos de continuidade e de recuperação ▪ Contratos e acordos ▪ Diretrizes ▪ Documentação da empresa ▪ Trilhas de auditoria ▪ Processo
TECNOLOGIA	Automatiza e suporta as atividades produtivas ou processos de negócios	Software	▪ Aplicativos ▪ Sistemas ▪ Software básico ▪ Ferramentas de desenvolvimento ▪ Utilitários
		Hardware	▪ Equipamentos computacionais (servidores, estações de trabalho, equipamentos de segurança, ...) ▪ Equipamentos de comunicação (roteadores, *switches*, ...) ▪ Mídias removíveis ▪ Meios de armazenamento ▪ Recurso
INSTALAÇÕES	Ambiente físico onde as atividades produtivas ou processos de negócio são executados	Ambientes	▪ Ambientes de escritório ▪ Centro de dados ▪ Salas de equipamentos ▪ Salas de monitoração ▪ Salas do sistema de energia elétrica ▪ Salas do sistema de climatização
		Equipamentos	▪ Fontes de energia ▪ Unidades de condicionamento de ar ▪ Móveis e acomodações
PESSOAS	Operam e monitoram as atividades produtivas ou processos de negócios	Pessoas	▪ Empregados ▪ Estagiários ▪ Fornecedores ▪ Visitantes ▪ Clientes ▪ Terceiros

A permanência de riscos na situação “em edição” deve durar apenas o tempo necessário para esclarecimento de dúvidas, caso existam ou até que todas as reuniões de riscos ocorram, após devem seguir o rito, sendo colocados como disponíveis para aprovação.

4.2.2. Análise de risco

A Análise dos Riscos deve contemplar:

- Descrição das Causas e Consequências, e das Ameaças e Vulnerabilidades: O impacto sobre o negócio para a organização, que pode ser causado por incidentes (possíveis ou reais) relacionados à segurança da informação, seja avaliado levando-se em conta as consequências de uma violação da segurança da informação, como por exemplo: a perda da confidencialidade, da integridade ou da disponibilidade dos ativos, cujo impacto pode ser determinado através de Análise de Impacto de Negócio (BIA). As consequências operacionais de cenários de incidentes podem ser identificadas em (não limitadas a):
  - Investigação e tempo de reparo
  - Tempo (de trabalho) perdido
  - Oportunidade perdida
  - Saúde e segurança
  - Custo financeiro das competências específicas necessárias para reparar o prejuízo
  - Imagem, reputação e valor de mercado
- Identificação das Vulnerabilidades: As vulnerabilidades são definidas como uma fragilidade de um ativo ou grupo de ativos, e que podem ser exploradas pelas ameaças. Caso isso ocorra, o resultado será um impacto negativo.
  Em função do escopo, ambiente, recursos e processos, devem ter identificadas as vulnerabilidades presentes no escopo, utilizando a relação de vulnerabilidades (ABNT NBR ISO/IEC 27005) previamente incluídas na ferramenta de gerenciamento de riscos, considerando as que mais se adéquem.
  As vulnerabilidades se caracterizam, dentre outras, por expressões: Ausência, Carência, Deficiência, Desproteção, Descontrole, Falta, Inadequação, Instabilidade, Insuficiência.
- Levantamento das Ameaças: Utilizar relação de ameaças (ABNT NBR ISO/IEC 27005) previamente incluídas na ferramenta de gerenciamento de riscos, e considerar quais dessas se adéquam ao escopo do trabalho, sendo que outras ameaças podem surgir durante o trabalho (*brainstorming*, entrevista ou reunião). Para cada ameaça e de sua relação com as vulnerabilidades (constituindo um evento) é que devem ser avaliados os níveis de impacto do risco.

- Avaliação da probabilidade dos incidentes: É feita através dos cenários de incidentes onde são avaliados a probabilidade de ocorrência e os impactos gerados em cada cenário.
- Determinação do Nível de Risco: É feito automaticamente pela ferramenta de gerenciamento de riscos, sendo o resultado da Probabilidade X Impacto.

IMPACTO	VALOR	DESCRIÇÃO
Muito Baixo	1	A materialização do risco pode afetar de forma insignificante os recursos, processos e/ou sistemas
Baixo	2	A materialização do risco pode afetar os recursos, processos e/ou sistemas, mas a implementação de controles é simples
Médio	3	A materialização do risco causa pequeno impacto nos recursos, processos e/ou sistemas envolvidos, mas a implementação de controles é viável.
Alto	4	A materialização do risco causa impacto significativo em vários recursos, processos e/ou sistemas envolvidos e a implementação de controles é complexa.
Muito Alto	5	A materialização do risco causa impactos significativos para os recursos, processos e/ou sistemas. A implementação de controles acarreta impactos ao negócio

Tipologia do Risco

Tem por objetivo a classificação dos riscos de acordo com o segmento que os apresenta, facilitando as análises dos Riscos de Segurança da Informação.

IMPORTANTE: Tomando por base que a Segurança da Informação trata riscos produtivos de nível operacional, foi acordado com a Área de Gestão de Riscos e Controles e adotada como fixa, na ferramenta de gerenciamento de riscos, a tipologia Gestão de Risco de Segurança – GRSI, exclusivamente para este segmento, diferindo dos riscos corporativos.

4.2.3. Avaliação do Risco

Os critérios abaixo são básicos e devem ser considerados na tomada de decisões. Devem ser consistentes com o contexto ou escopo definido, externo e interno, relativo à gestão de riscos de segurança da informação e levam em conta os objetivos da organização, o ponto de vista das partes interessadas, requisitos contratuais, legais e regulatórios. É neste momento que devem ser identificados os controles existentes.

Na Avaliação de um Risco de Segurança da Informação devem ser considerados:

- O valor estratégico do processo que trata as informações de negócio;
- A criticidade dos ativos de informação envolvidos;
- Requisitos legais e regulatórios, bem como as obrigações contratuais;

- Importância, do ponto de vista operacional e dos negócios, da disponibilidade, da confidencialidade e da integridade;
- Expectativas e percepções das partes interessadas e consequências negativas para o valor de mercado (em especial, no que se refere aos fatores intangíveis desse valor), a imagem e a reputação;
- Além disso, critérios para avaliação de riscos podem ser usados para especificar as prioridades para o tratamento do risco.

Quanto ao Impacto, deve ser avaliado em função do montante dos danos ou custos à organização, causados por um evento relacionado com a segurança da informação, considerando os seguintes aspectos:

- Nível de classificação do ativo de informação afetado;
- Ocorrências de violação da segurança da informação (por exemplo, perda da disponibilidade, da confidencialidade e/ou da integridade);
- Operações comprometidas (internas ou de terceiros);
- Perda de oportunidades de negócio e de valor financeiro;
- Interrupção de planos e o não cumprimento de prazos;
- Dano à reputação;
- Violações de requisitos legais, regulatórios ou contratuais.

Quanto a Aceitação do Risco, os critérios dependem frequentemente das políticas, metas e objetivos da organização, critérios de negócios, aspectos legais e regulatórios, operações, tecnologia, finanças e fatores humanos e humanitários:

- Podem incluir mais de um limite, representando um nível desejável de risco, porém precauções podem ser tomadas pela alta liderança para aceitar riscos acima desse nível desde que sob circunstâncias definidas.
- Diferentes critérios para a aceitação do risco podem ser aplicados a diferentes classes de risco, por exemplo, riscos que podem resultar em não conformidade com regulamentações ou leis podem não ser aceitos, enquanto riscos de alto impacto podem ser aceitos se isto for especificado como um requisito contratual.
- Podem incluir requisitos para um tratamento adicional futuro, por exemplo, um risco pode ser aceito se for aprovado e houver o compromisso de que ações para reduzi-lo a um nível aceitável serão tomadas dentro de um determinado período.
- Podem ser diferenciados de acordo com o tempo de existência previsto do risco, por exemplo, o risco pode estar associado a uma atividade temporária ou de curto prazo.

Ao final da avaliação de Riscos é realizado o primeiro ponto de decisão do processo, no qual é verificado se a avaliação foi satisfatória ou não:

- Se não for satisfatória, é necessário rever a definição do contexto para nova verificação;
- Se for satisfatória, identificar para o risco uma das opções: Tratar ou Aceitar o Risco.

A identificação de uma das opções de tratamento a serem dadas ao risco tem como base, a própria avaliação do risco, no custo esperado de implementação da opção escolhida e/ou nos benefícios previstos a serem alcançados.

4.2.4. Priorização para o Tratamento dos Riscos

É a ordenação dos riscos feita de acordo com os critérios de avaliação de riscos estabelecidos na definição do contexto ou escopo, sendo considerados os valores dos níveis de riscos atuais.

IMPORTANTE··Durante·o·processo·de·gestão·de·riscos·de·segurança·da·informação,·é·importante·que·os·riscos·e·a·forma·com·que·são·tratados·sejam·comunicados·ao·pessoal·das·áreas·operacionais·e·gestores·apropriados.·Mesmo·antes·do·tratamento·do·risco,·informações·sobre·riscos·identificados·podem·ser·úteis·para·o·gerenciamento·de·incidentes·e·pode·ajudar·a·reduzir·possíveis·prejuízos.¶

A·conscientização·dos·gestores·e·pessoal·envolvido,·no·que·diz·respeito·aos·riscos,·à·natureza·dos·controles·aplicados·para·mitigá-los·e·às·áreas·definidas·como·de·interesse·pela·organização,·auxilia·a·lidar·com·os·incidentes·e·eventos·não·previstos·da·maneira·mais·efetiva.¤

4.3. Tratamento de Riscos de Segurança da Informação

O tratamento de riscos indica as ações a serem tomadas pelo responsável para mitigar os riscos.

Nesta fase é definida a Estratégia de resposta ao risco a ser adotada, ou seja, a ação mais conveniente para os controles de Segurança da Informação, que podem ser: Aceitar ou Tratar.

O tratamento dos riscos deve ser controlado pelo gestor do escopo e pelos responsáveis pelos controles, de forma a garantir que o que foi planejado está sendo realizado até o seu encerramento, quando todas as ações forem implementadas ou de alguma forma encerradas. Os desvios devem ser tratados gerencialmente.

O tratamento dos riscos do método GRSI deve estar em conformidade com a Norma de Classificação dos Ativos de Informação do Serpro.

4.3.1. Definição dos controles e de respostas ao risco

Quando ocorre a decisão de opção pelo Tratamento de Riscos devem ser indicados novos controles, que nessa fase são chamados de Controles Propostos (Risco Projetado) ou melhoria dos existentes, e é onde é apontado o Nível de Risco Projetado

Implementação dos controles de respostas aos riscos e Responsável pelo Controle

Para a implementação dos controles de resposta aos riscos, deve ser definido o principal responsável pela implementação da iniciativa, denominado Responsável pelo Controle. Este Responsável também deve monitorar e avaliar a eficácia dos controles no nível de risco atual (NRA), a conclusividade das ações para implementação dos controles e reportar a evolução das iniciativas ao gestor do serviço ou processo referente ao escopo ou a qualquer outra forma de controle ou auditoria.

O gestor de risco deve acompanhar e analisar, durante um período necessário para esta análise, se o controle está efetivamente atuando na mitigação do risco. Caso positivo, o Nível de Risco Atual pode ser reduzido e considerado na próxima revisão.

Estratégia de Resposta ao Risco a ser adotada

Para os riscos de Segurança da Informação – GRSI existem as opções ACEITAR, TRATAR e CANCELAR.

RESPOSTA AO RISCO	DESCRIÇÃO
Tratar	Um risco normalmente é mitigado quando está acima do Apetite a Riscos definido, ou seja, seu Nível de Risco é classificado como “alto” ou “muito alto”. Geralmente há necessidade da implementação de um plano de ação para que possam diminuir as ameaças e as vulnerabilidades e as causas ou as consequências dos riscos.
Aceitar	Um risco geralmente é aceito quando o nível está nas faixas de Apetite a Riscos, não exige ação ou nenhum novo controle precisa ser implementado.
Cancelar	Quando para o risco for necessário o seu cancelamento (o risco deixou de existir ou não é mais válido devido a alterações no contexto interno ou externo).

O Gestor de Riscos deve identificar qual estratégia seguir (tratar, aceitar ou cancelar) em relação aos riscos mapeados e avaliados. A escolha da estratégia depende do Nível do Apetite a Riscos e dos recursos necessários para a implementação do controle.

Como referência, deve ser observada a Declaração de Apetite a Riscos do Serpro (RAS), quanto ao Apetite de Riscos e Criticidade, para os processos:

- 03.02 – Gerenciar Soluções de Segurança;
- 12.05 – Gerenciar Continuidade de Negócios; e
- 12.09 – Gerenciar Segurança da Informação

4.3.2. Validação dos resultados no Tratamento de Risco

Nesta etapa, os resultados da análise, avaliação, priorização e resposta aos riscos devem ser avaliadas e aprovadas pelo empregado designado (nível de departamento) da Superintendência de Segurança da Informação.

Ao final do tratamento de riscos é verificado se o tratamento foi satisfatório ou não:

- Se não for satisfatório, é necessário rever a definição do contexto para nova verificação;
- Se for satisfatório, seguir o rito ou optar pela aceitação do risco.

Aceitação do Risco

Os critérios para a aceitação do risco estão descritos no item 4.2.2., e em resumo podem ser:

- Nível desejável de risco versus precauções empresariais
- Tratar o risco versus o custo envolvido
- Riscos que podem resultar em não conformidade com regulamentações ou leis versus nível de impacto
- Risco aprovado versus requisitos de tratamento adicional futuro.
- Os critérios para a aceitação do risco podem ser diferenciados de acordo com o tempo de existência previsto do risco versus prazo de uma atividade temporária, considerando os itens: critérios de negócios, aspectos legais e regulatórios, operações, tecnologia, finanças e fatores humanos e humanitários.

A aceitação do risco deve assegurar que os riscos residuais sejam explicitamente aceitos pelos gestores. Isso é especialmente importante em uma situação em que a implementação de controles é omitida ou adiada, devido aos custos.

Em caso de aceitação do risco, o Nível de Risco Projetado (NRP) deve ser o mesmo do Nível de Risco Atual (NRA) (mesma probabilidade e mesmo impacto).

4.4. Comunicação e Consulta

Comunicar os riscos e os resultados para as partes interessadas

A comunicação do risco é uma atividade que objetiva alcançar um consenso sobre como os riscos devem ser gerenciados, fazendo uso para tal da troca e/ou partilha das informações sobre o risco entre os tomadores de decisão e as outras partes interessadas. A comunicação é bidirecional.

As finalidades da comunicação do risco são:

- Fornecer a garantia do resultado da gestão de riscos GRSI para a organização;
- Coletar informações sobre os riscos;

- Evitar ou reduzir tanto a ocorrência quanto as consequências das violações da segurança da informação que aconteçam devido à falta de entendimento mútuo entre os tomadores de decisão e as partes interessadas;
- Dar suporte ao processo decisório em relação à segurança da informação;
- Obter novo conhecimento sobre a segurança da informação;
- Coordenar com outras partes e planejar respostas para reduzir as consequências de um incidente;
- Dar aos tomadores de decisão e às partes interessadas um senso de responsabilidade sobre os riscos GRSI;
- Melhorar a conscientização;
- Compartilhar trimestralmente com a alta direção os resultados do processo de avaliação e tratamento de riscos por meio do *Relatório de identificação, análise, avaliação e tratamento dos riscos de segurança da informação;*
- Compartilhar anualmente ou sempre que houver alteração em algum dos fatores de risco ou em algum contexto interno ou externo, com a alta direção o *Plano de Gestão de Riscos de Segurança da Informação*.

Entende-se como contextos interno e externo o conjunto de eventos que possam influenciar a capacidade da organização de atingir seus objetivos estratégicos.

A SUPSI – Superintendência de Segurança da Informação é a área responsável pela elaboração e aprovação do *Plano de Gestão de Riscos de Segurança da Informação* e do *Relatório de identificação, análise, avaliação e tratamento dos riscos de segurança da informação*.

O processo de implementação do Plano de Gestão de Riscos de Segurança da Informação deve considerar, dentre outros aspectos, as recomendações de mudanças em relação aos critérios de aceitação de riscos, a abrangência da atuação do plano.

Detalhamento do *Relatório de identificação, análise, avaliação e tratamento dos riscos de segurança da informação*

O Relatório deve conter as seguintes informações

- Identificação:
  - Os riscos associados a cada ativo de informação, considerando as ameaças envolvidas, as vulnerabilidades existentes e as ações de segurança das informações já implementadas;
  - O grau de severidade dos riscos identificados, considerando os valores ou os níveis de probabilidade de ocorrência do risco e as consequências da ocorrência do risco (perda da integridade, disponibilidade, confiabilidade ou autenticidade nos ativos envolvidos);

- Os eventos de segurança da informação ocorridos, com a descrição das ações de segurança, e de eventuais consequências do evento para o órgão ou a entidade;
- As alterações nos fatores de risco; e
- As mudanças em relação a critérios de avaliação e análise.

- Tratamento:
  - A definição e a priorização das ações de segurança e as atividades de tratamento de riscos que deverão ser realizadas;
  - Os responsáveis pela execução e pelo acompanhamento das ações de segurança e atividades de tratamento de riscos;
  - Os prazos de execução das ações de segurança e das atividades de tratamento de riscos; e
  - As opções de tratamentos de riscos priorizados.
  - Para cada possibilidade de tratamento detectada em função do risco identificado, devem ser observados:
    - A eficácia das ações de segurança da informação;
    - As restrições técnicas;
    - As restrições físicas estruturais;
    - As restrições operacionais;
    - As restrições organizacionais;
    - Os requisitos legais; e
    - Relação custo-benefício.

Detalhamento do Plano de Gestão de Riscos de Segurança da Informação

O Plano de Gestão de Riscos de Segurança da Informação deve conter as seguintes informações:

- A abrangência da aplicação da gestão de riscos, delimitando seu âmbito de atuação (escopo) e os ativos de informação que serão objeto de tratamento;
- A metodologia a ser utilizada que deverá contemplar, no mínimo, critérios de avaliação e de aceitação de riscos;
- Os tipos de riscos;
- O nível de severidade dos riscos;
- Um modelo de Relatório de identificação, análise, avaliação e tratamento dos riscos de segurança da informação com as orientações necessárias para sua elaboração.

4.5. Registro, Relato e Contingência

Os resultados da avaliação e tratamento dos riscos de Segurança da Informação são registrados na ferramenta de gerenciamento de riscos e, se necessário, transcritos em relatórios específicos, conforme solicitação.

Os planos de Contingência/Continuidade de Negócios são os controles contingenciais planejados para recuperação de cenários previstos, quando o incidente respectivo não foi solucionado. A ferramenta de gerenciamento de riscos é o repositório dessas informações e artefatos.

4.6. Monitoramento e Análise Crítica dos fatores de riscos GRSI (impactos, ameaças, vulnerabilidades, probabilidade de ocorrência)

Como os riscos não são estáticos, as ameaças, as vulnerabilidades, a probabilidade ou as consequências podem mudar. Portanto, o monitoramento constante é necessário para que se detectem essas mudanças.

O monitoramento e as análises críticas dos riscos GRSI são executados pela Superintendência de Segurança da Informação, contando com o apoio das áreas operacionais envolvidas.

O resultado da atividade de monitoramento de riscos pode fornecer os dados de entrada para as atividades de análise crítica. É recomendável a análise de todos os riscos regularmente e quando grandes mudanças ocorrerem.

Essa atividade de Monitoramento e Análise Crítica deve considerar no mínimo:

- Eficácia dos controles;
- Abordagem do processo de avaliação de riscos;
- Valor e categorias dos ativos;
- Critérios de impacto;
- Critérios para a avaliação de riscos;
- Critérios para a aceitação do risco;
- Custo total de propriedade; e
- Recursos necessários;

4.7. Indicadores GRSI

Todos os indicadores de riscos GRSI são obtidos através da ferramenta de solução de gerenciamento de riscos, tais como:

- Totais de riscos de projeto – é o fator agregador dos riscos GRSI por escopo;

- Riscos GRSI - Total de riscos ativos, aprovados, cancelados, em atraso, aguardando aprovação, rejeitados na aprovação, estratégia adotada para tratamento do risco, matriz de nível de risco atual, total de riscos por status;
- Controles GRSI - Total de controles, controles implementados, não implementados, em atraso, não implementados por Unidade de Gestão, previsão de implementação de controles por trimestre, controles por status, status de controles por Superintendência, quantidade de dias faltante para a implementação de um controle.

5. FUNÇÕES E ATRIBUIÇÕES NO GRSI

A estrutura de gestão de riscos e controles internos do Serpro, baseada nas melhores práticas e referenciais teóricos, estabelece o compartilhamento de responsabilidades para o adequado funcionamento da gestão de riscos e controles internos na empresa, e, portanto, adotado também no método GRSI.

Cada risco mapeado e avaliado deve estar associado a um responsável, definido como Gestor de Riscos.

Para o efetivo sucesso do trabalho, devem participar do GRSI as pessoas (especialistas ou não) envolvidas com o escopo definido (processo, serviço, sistema, recurso, aplicação e área de negócio).

Não existe um número ideal de participantes.

Ex: no caso de sistemas, devem participar da atividade o responsável pelo processo, analistas, programadores, usuários, administradores de banco de dados, o responsável pelo serviço, sistema ou processo, o gestor do produto, o gestor de negócio e representantes das áreas operacionais (Rede, *Firewall*, IPS, Filtro de conteúdo).

Funções e Atribuições no GRSI

FUNÇÃO NO GRSI	ATRIBUIÇÕES	FUNÇÃO NA FERRAMENTA (*)	USUÁRIO TÍPICO
Coordenador do GRSI	▪ Elaborar a arquitetura do escopo; ▪ Selecionar os participantes; ▪ Distribuir previamente, o material a ser utilizado na reunião; ▪ Apresentar o escopo escolhido para o grupo, e ▪ Controlar a execução das ações resultantes do levantamento dos riscos	▪ Consulta e edita os riscos sob sua gestão ▪ Visualiza os riscos, enquanto parte interessada	▪ Gestor do Serviço, Sistema, Recurso, Processo
Facilitador do GRSI ou Patrocinador- é utilizado esse campo	▪ Convocar as pessoas sugeridas; ▪ Apresentar o método a ser utilizado; ▪ Dirimir dúvidas quanto aos conceitos de Segurança, se houver; ▪ Preparar o material a ser utilizado nas reuniões; ▪ Agendar datas das reuniões junto ao responsável pelo escopo e participantes; ▪ Conforme a opção de Levantamento de riscos adotada: ▪ Registrar os resultados do brainstorming; ou ▪ Registrar os resultados da análise de risco mediante a arquitetura de referência	▪ Consulta e edita os riscos sob sua gestão ▪ Visualiza os riscos, enquanto parte interessada	▪ Empregado da Unidade Organizacional que conduz os trabalhos e media as reuniões ▪ GRSI – Empregado indicado da SUPSI/SIGSC ou DIDES
Participante do GRSI	▪ Conhecer o material enviado previamente; ▪ Participar do *brainstorming*, responder ao questionário de risco ou analisar a arquitetura de referência, e ▪ Identificar riscos e soluções associadas ao escopo do trabalho.	▪ Consulta os riscos sob sua gestão ▪ Visualiza os riscos, enquanto parte interessada	▪ Empregado indicado da Unidade Organizacional ▪ GRSI – Empregado indicado pelo Gestor do Escopo
Gestor de Risco (GRSI)	▪ Identificar e registrar os riscos; ▪ Assegurar que o risco seja gerenciado; ▪ Monitorar o risco frequentemente de forma a garantir que as respostas adotadas (controles) resultem na manutenção do risco em níveis adequados; ▪ Garantir que as informações adequadas sobre o risco estejam disponíveis para os envolvidos; ▪ Realizar revisão frequente dos riscos identificados; e ▪ Envolver os gestores de Riscos de outras unidades, sempre que houver essa necessidade, para o tratamento de um risco sob sua responsabilidade.	▪ Consulta e edita os riscos sob sua gestão ▪ Visualiza os riscos, enquanto Gestor de Riscos	▪ Proprietário e responsável pelo risco e deve estar formalmente identificado em cada risco ▪ GRSI – Empregado responsável pelo risco de SI do escopo

FUNÇÃO NO GRSI	ATRIBUIÇÕES	FUNÇÃO NA FERRAMENTA (*)	USUÁRIO TÍPICO
Agente de Risco/ Corresponsável (GRSI)	▪ Apoiar os Gestores de Riscos de suas Unidades; ▪ Realizar e registrar mensalmente o monitoramento dos riscos e o acompanhamento dos controles associados aos riscos; ▪ Atuar como canal de comunicação para que os empregados da unidade citem riscos percebíveis em suas atividades	▪ Consulta e edita os riscos sob sua gestão ▪ Visualiza os riscos, enquanto Agente de risco	▪ Empregado indicado da Unidade Organizacional ▪ GRSI – Empregado responsável pelo risco de SI do escopo
Responsável pelos Controle e Corresponsável (GRSI)	▪ Implementar e manter os controles que visam a redução da probabilidade ou impacto do risco, durante o processo de gestão dos riscos.	▪ Consulta e edita os controles sob sua gestão ▪ Visualiza os riscos, enquanto Responsável pelos Controles e Corresponsável	▪ Designados para implementar e manter os controles que visam a redução da probabilidade ou impacto do risco
Agentes Corporativos de Riscos (GRSI)	▪ Responsável pela supervisão da implementação das atividades de gestão dos riscos de segurança da informação nas unidades do Serpro; ▪ Oferecer capacitação continuada em Gestão de Riscos de Segurança da Informação para os empregados do Serpro; ▪ Medir o desempenho da Gestão de Riscos em Segurança da Informação objetivando a sua melhoria contínua; ▪ Promover a Análise sobre os riscos mapeados nos GRSI elaborados; ▪ Monitorar a evolução os níveis de riscos e a eficácia das medidas de controles implementadas, e ▪ Dar suporte a identificação, análise e avaliação dos riscos, se necessário	▪ Consulta e edita os riscos sob sua gestão ▪ Visualiza os riscos, enquanto agente corporativo do risco	▪ Empregados indicados da Unidade Organizacional ▪ GRSI – Empregado indicado da SUPSI/SIGSC

FUNÇÃO NO GRSI	ATRIBUIÇÕES	FUNÇÃO NA FERRAMENTA (*)	USUÁRIO TÍPICO
Aprovador do Risco (GRSI)	▪ Aprovar os riscos mapeados pelos Gestores e participantes das Unidades no GRSI	▪ Aprovadores de Riscos são aqueles que têm autoridade final sobre a aprovação dos riscos mapeados pelos Gestores e participantes do GRSI das Unidades	▪ Diretor ou Empregados indicados da Unidade Organizacional ▪ GRSI – Empregado indicado da SUPSI/SIGSC

(*) Ferramenta de solução de gerenciamento de riscos adotada pela empresa

6. CONSIDERAÇÕES GERAIS

- Acidentes, erros e omissões geralmente são responsáveis por maiores perdas do que atos deliberados;
- Nenhum controle de segurança é 100% efetivo;
- Não é possível eliminar todos os riscos;
- Os riscos não eliminados devem ter essa condição documentada;
- Para a realização do método GRSI devem ser conhecidas pelos participantes a sistemática e o escopo do trabalho;
- O responsável ou gestor deve decidir quando um custo para prevenir um risco (controle) é maior que o custo das consequências do risco (impacto da perda ou dano);
- O método GRSI é executado visando a obtenção das contribuições de todos que detenham conhecimento sobre o escopo a ser analisado. Isto pode ser feito numa reunião de trabalho ou em entrevistas individuais, que devem ser previamente agendadas, em qualquer dos casos;
- A participação dos convidados no grupo é de fundamental importância para o resultado do trabalho;
- Quando for executada a sistemática para um determinado escopo, devem participar as pessoas mais experientes no assunto em questão, de forma que o primeiro resultado seja o mais completo possível. A experiência sobre escopos semelhantes e outras avaliações já realizadas podem auxiliar no trabalho;

- Se revisão, devem ser consideradas as avaliações e tratamento anteriores, em especial as considerações sobre as decisões adotadas (histórico), de forma a tornar o trabalho reproduzível e comparável, mesmo se tratando de equipes diferentes;
- De acordo com a norma de Classificação de Ativos de Informação do Serpro, os relatórios gerados pela ferramenta de gerenciamento de riscos e referentes ao método GRSI são classificados como sigilosos;
- Ferramenta de gerenciamento de riscos adotada pela empresa para o registro do método GRSI:
  - *Dashboards* – são gerados diversos, a partir das informações incluídas na ferramenta;
  - Resultados do trabalho de análise ficam arquivados no banco de dados da própria ferramenta;
  - O acesso é feito através do endereço: https://grc.serpro/Default.aspx
  - Risco e Controle – a forma de preencher o risco e o controle do método GRSI estão documentadas no Demonstra:
    RISCO:https://demonstra.serpro/DEMOS/inclusao_de_resgist/demo/html/demo_1.html?d=31052021102557
    CONTROLE:https://demonstra.serpro/DEMOS/teste_/demo/html/?d=04042022090420

Anexo 1D

CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS NA GESTÃO DE RISCOS

1. INTRODUÇÃO

Este anexo complementa a Metodologia de Gestão de Riscos e Controles ao integrar conceitos e práticas de continuidade de negócios, assegurando que a organização esteja preparada para responder de forma estruturada à materialização de riscos críticos. Ele reflete as diretrizes estabelecidas na Resolução CGPAR nº 48, de 6 de setembro de 2023, Art. 23, inciso IX, que enfatiza a necessidade de articulação entre gestão de riscos e continuidade de negócios.

2. OBJETIVO

O objetivo deste anexo é detalhar como os planos de continuidade de negócios (PCNs) são acionados no contexto da gestão de riscos organizacionais, abrangendo tanto riscos estratégicos e de negócio, quanto operacionais e de projetos, independentemente de estarem vinculados à área de TI ou a processos críticos.

3. DIRETRIZES

1. **Definição e Vinculação**:
    - Os Planos de Continuidade de Negócios devem estar alinhados aos riscos classificados como críticos na matriz de riscos organizacionais.
    - Os planos devem ser abrangentes, cobrindo riscos que impactem áreas operacionais (relatórios a Serviços de Missão Crítica - SMC e a Infraestruturas Críticas Internas - ICI) e estratégicas.
2. **Processos e Responsabilidades**:
    - A Área de Gestão de Riscos e Controles é responsável por assegurar que os riscos críticos identifiquem claramente os cenários que exigem ativação de PCNs para processos corporativos.
    - A Área de Gestão da Segurança da Informação e da Continuidade de Negócio é responsável por assegurar que os riscos operacionais identifiquem claramente os cenários que exigem ativação de PCNs e coordenar a elaboração e revisão dos PCNs relativos a Serviços de Missão Crítica (SMC) e de Infraestrutura Crítica Interna (ICI) de TIC.
    - Cada unidade organizacional deve indicar agentes de continuidade, responsáveis por coordenar as ações de resposta em sua área de atuação.
3. **Coordenação e Integração**:
    - O Comitê Estratégico de Governança, Riscos, Controles e Segurança da Informação (COGRS) será responsável por supervisionar a integração dos PCNs de processos à metodologia de gestão de riscos.

- Para os PCNs relativos a Sistemas de Missão Crítica (SMC) e de Infraestrutura Crítica Interna (ICI) de TIC, a integração é feita através da Gestão de Incidentes e registrada nos riscos para ciência e acompanhamento do COGRS.
- A integração deve incluir reuniões regulares com representantes das áreas de TI, unidades de negócio, gestão de riscos e controles, e continuidade de negócios.

4. APLICAÇÃO PRÁTICA - EXEMPLOS DE CENÁRIOS

1. **Risco Estratégico**: No caso de uma greve que comprometa processos críticos, o plano de continuidade deve prever ações de negociação e medidas temporárias para manter a entrega de serviços essenciais.
2. **Risco Operacional Crítico**: Para uma falha em sistemas críticos de TI, o PCN deve incluir alternativas técnicas e manuais para continuidade dos serviços afetados.

5. REFERÊNCIAS A DOCUMENTOS EXISTENTES

- Programa de Continuidade de Negócios vigente;
- Política Corporativa de Continuidade de Negócios vigente;
- Processo institucionalizado baseado nas melhores práticas de mercado, relacionados à elaboração, revisão e ativação de PCNs.

6. MONITORAMENTO E ATUALIZAÇÃO

Este anexo será revisado anualmente, garantindo sua adaptação a mudanças no ambiente interno e externo da organização.

7. CONCLUSÃO

A inclusão dos conceitos de continuidade de negócios na gestão de riscos reforça a capacidade organizacional de enfrentar adversidades e assegurar a resiliência de suas operações. Este anexo fornece a base para uma integração mais efetiva e estratégica entre as áreas responsáveis pelo tratamento dos riscos e a preservação da continuidade operacional.