METODOLOGIA DE GESTÃO DE RISCO E CONTROLES INTERNOS

SERPRO

DECISÃO DIRETIVA

RI-001/2023

Data Início: 11/01/2023

Data Fim:

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

TÍTULO

METODOLOGIA DE GESTÃO DE RISCOS E CONTROLES INTERNOS

TEMA

RI – Riscos Empresariais

PALAVRAS-CHAVE

metodologia, riscos, controles internos, gestão de riscos

PROCESSO

12.01 - Gerenciar Riscos Empresariais e Controles Internos

1.0 FINALIDADE

Atualizar a Metodologia de Gestão de Riscos e Controles Internos, conforme Anexo 1 – Metodologia de Gestão de Riscos e Controles Internos, visando a padronização do processo de identificação, tratamento e monitoramento de riscos sobre processos corporativos, projetos estratégicos e planejamento estratégico da empresa. Adequação da Metodologia para inclusão de levantamento e avaliação de riscos positivos, riscos do negócio, avaliação de controles, revisão das tipologias e inclusão do anexo 1C com o tratamento de riscos de tecnologia da informação (GRSI).

2.0 ÂMBITO DE APLICAÇÃO

Todos os órgãos da empresa.

3.0 DETERMINAÇÕES

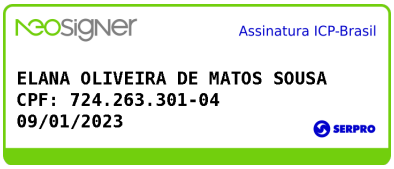
3.1 A Metodologia de Gestão de Riscos e Controles Internos deve ser utilizada por todas as Unidades Organizacionais, cabendo-as fazer a gestão dos riscos e controles internos sob sua responsabilidade.

3.2 As avaliações dos riscos e dos controles internos 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 DISPOSIÇÕES FINAIS

4.1 Este documento substituirá a Decisão de Diretoria RI-158/2021, de 29 de dezembro de 2021.



Diretora Jurídica e de Governança e Gestão – em exercício

ÓRGÃO/REDATOR: DIJUG/SUPCR/CRGRC/CRGER/gac

METODOLOGIA DE GESTÃO DE RISCOS E CONTROLES INTERNOS

Sumário

1.0 INTRODUÇÃO

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[1], 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;

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;

c) agregar valor à organização por meio do tratamento adequado dos riscos e dos impactos decorrentes de sua materialização;

d) atuar de forma integrada com o planejamento estratégico, processos e projetos corporativos;

e) Alinhar o apetite a riscos com a estratégia empresarial;

f) dar transparência de que os riscos empresariais são conhecidos e gerenciados; e

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 dos dados.

A Metodologia de Gestão de Riscos e Controles Internos do Serpro padroniza a implementação, manutenção e monitoramento do processo de gestão de riscos e controles internos. A Metodologia deve ser aplicada para identificação dos riscos da Empresa, visando o estabelecimento de matrizes de riscos, de controles internos para seu tratamento e de indicadores de evolução. A Metodologia abrange o

1 Esta versão da Metodologia abordará o tratamento de riscos positivos e negativos, apenas para os Riscos Estratégicos. Riscos Operacionais e Riscos de Projetos Estratégicos manterão a abordagem apenas sobre riscos negativos.

levantamento e tratamento dos **riscos empresariais**[2], 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 de Negócio**, que afetam os componentes estratégicos da empresa e os riscos dos **projetos estratégicos**.

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

2.0 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 internos 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 internos 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 a 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.

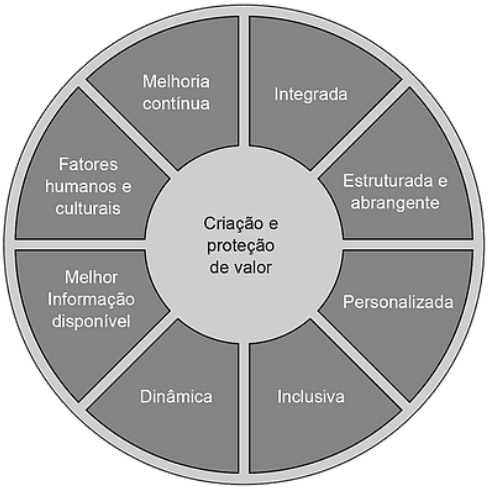
A gestão de riscos e os controles internos são mecanismos de governança corporativa e partes integrantes das atividades organizacionais. Seu propósito é a

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

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 Internos



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

2.1 Integrada

A gestão de riscos é parte integrante de todas as atividades organizacionais.

2.2 Estruturada e abrangente

A execução da gestão de riscos é realizada de forma sistemática, estruturada e oportuna, alinhada ao interesse público.

2.3 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.

2.4 Inclusiva

Todos os empregados e gestores são responsáveis pela gestão de riscos e controles internos em suas atividades e processos de trabalho.

2.5 Dinâmica

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

2.6 Melhor informação disponível

A gestão de riscos e controles internos 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.

2.7 Fatores humanos e culturais

Fatores humanos e culturais influenciam significativamente a gestão de riscos.

2.8 Melhoria contínua

O aprendizado e a internalização da cultura de gestão de riscos e controles internos 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 internos deve ser apoiada e monitorada pelos administradores da empresa.

3.0 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 internos por toda a organização.

Figura 2 - Linhas da Gestão de Riscos e Controles Internos

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

A estrutura de gestão de riscos e controles internos 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 internos, para que disponham de informações consistentes, relevantes e tempestivas, para que sejam utilizadas como ferramenta auxiliar na tomada de decisão, além de se tornar uma 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.

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 internos 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[3]: atuar na promoção da integridade no Serpro por meio da estruturação, execução e monitoramento do Programa de Integridade, de modo

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

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.

No que se refere à Gestão de Riscos e Controles Internos, a área de Gestão de Riscos e Controles Internos, no Serpro, atua como consultora da 1ª linha e submete 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 Internos.

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 processo é o principal insumo para identificação dos riscos operacionais, porém não é a única fonte, visto que o único impeditivo para a unidade organizacional se isentar de identificar e gerenciar riscos é a ausência de 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 pela área de Projetos. A área de Riscos e Controles da empresa realiza o monitoramento dos riscos e controles internos dos projetos estratégicos priorizados pela Diretoria Executiva por meio do Plano Anual de Riscos e Controles Internos. Estes riscos são tratados na

seção 8 deste documento. Ressalta-se que independente de constarem no Plano Anual de Riscos e Controles Internos, todos os projetos estratégicos devem ter seus riscos conhecidos e gerenciados por meio da aplicação do 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 de 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.

4.0 RESPONSABILIDADES

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

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

Todos os **empregados e gestores**, atores da 1ª linha, são responsáveis pela gestão de riscos e controles internos 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 internos, 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 internos. 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 internos, por supervisionar as atividades desenvolvidas nas áreas de gestão de riscos e controles internos e monitorar a qualidade e a integridade dos mecanismos de gestão de riscos e controles internos;

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 internos;

e) o **Diretor-Presidente (DP)** deve manter, sob sua supervisão direta, o gerenciamento de riscos de controles internos 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 Internos 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 internos e quanto a supervisão dos aspectos de segurança da informação, gestão de continuidade de negócios, privacidade, proteção e governança de dados:

> g1) cabe ao Comitê a criação, atualização e proteção da Política Corporativa de Gestão de Riscos e Controles Internos. Também é de responsabilidade do Comitê Estratégico dirimir temas transversais que permeiam Diretorias distintas;

h) os **Comitês Táticos de Gestão de Riscos e Controles Internos das Diretorias (COGRC)** são responsáveis por apoiar a institucionalização da gestão de riscos e controles internos das unidades organizacionais, pelo

monitoramento dos planos de tratamento de riscos e controles internos, 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 Internos** é responsável por gerenciar a Política de Gestão de Riscos e Controles Internos, por elaborar o Plano Anual de Gestão de Riscos e Controles Internos, 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 Internos, por avaliar os Controles Internos e por elaborar relatórios periódicos consolidados de gerenciamento de riscos e controles internos aos órgãos colegiados.

Esta metodologia define também papéis que terão responsabilidades específicas na implementação das ações de gestão de riscos e controles internos:

a) Gestor de Riscos e Controles Internos;

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

c) Responsável pelos Controles Internos;

d) Agente Corporativo de Riscos e Controles Internos;

e) Aprovador de Riscos;

f) Partes Interessadas; e

g) Especialista da tipologia.

O **Gestor de Riscos e Controles Internos** 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 Internos**:

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 internos 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 internos 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 internos;

g) acompanhar a implementação dos controles internos propostos;

h) avaliar a efetividade dos controles internos; 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 Internos (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 Internos;

b) atuar como disseminadores do processo de gestão de riscos e controles internos e como facilitadores da aplicação desta metodologia e auxiliar os responsáveis pelos processos;

c) apoiar os Gestores de Riscos e Controles Internos de suas unidades;

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

e) atuar como facilitador em monitoramento dos riscos e seus controles internos, 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 Internos; e

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

Os Agentes de Riscos e Controles Internos das unidades organizacionais (primeira linha - Agentes GRCI) serão capacitados pelos Agentes Corporativos de Riscos e Controles Internos (segunda linha) em conhecimentos de gestão de riscos e controles internos, visando apoiar as atividades do processo em suas unidades. As Unidades Organizacionais devem indicar pelo menos dois Agentes de Riscos e Controles Internos (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 internos. 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 Internos** são empregados da área de Gestão de Riscos e Controles Internos responsáveis pela supervisão da implementação das atividades de gestão de riscos e avaliação dos controles internos nas unidades do Serpro. A área de Gestão de Riscos e Controles Internos deve manter pelo menos um agente corporativo de riscos indicado para atender a cada Diretoria.

São responsabilidades dos **Agentes Corporativos de Riscos e Controles Internos**:

a) prover treinamento da Metodologia de Gestão de Riscos e Controles Internos;

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

c) promover a análise crítica sobre os riscos e controles internos mapeados pelas Unidades Organizacionais;

d) supervisionar o monitoramento da evolução dos níveis de riscos e controles internos e a avaliação da presença, do funcionamento e da eficácia das medidas de 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 internos**. 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 aqueles que têm a responsabilidade sobre a aprovação dos riscos mapeados pelos Gestores e Agentes de Riscos das unidades (Agentes GRCI). Pode ser o Diretor da Unidade Organizacional, Superintendente(s) ou gerente(s) de grupo II indicado(s).

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** é o responsável, na 2ª linha, por auxiliar na definição do apetite a risco da tipologia, na declaração de níveis de impacto e análise sobre os riscos tipificados na tipologia.

5.0 PLANO DE GESTÃO DE RISCOS E CONTROLES INTERNOS

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

A área de Gestão de Riscos e Controles Internos 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 Internos busca em suas ações o fortalecimento da cultura de gestão de riscos e de controles internos 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 internos será conduzido, executado e monitorado.

6.0 APETITE A RISCOS

6.1 Definição do 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. De modo geral, quanto mais a organização tem a perder, menos ela pretende arriscar, isto é, quanto maior a criticidade associada ao risco, maior a tendência de o Apetite a Riscos ser mais baixo. 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 possíveis riscos. O excesso de controles torna o processo oneroso (tempo e custos), diminuindo o poder de competitividade da organização ou mesmo sua capacidade de inovação.

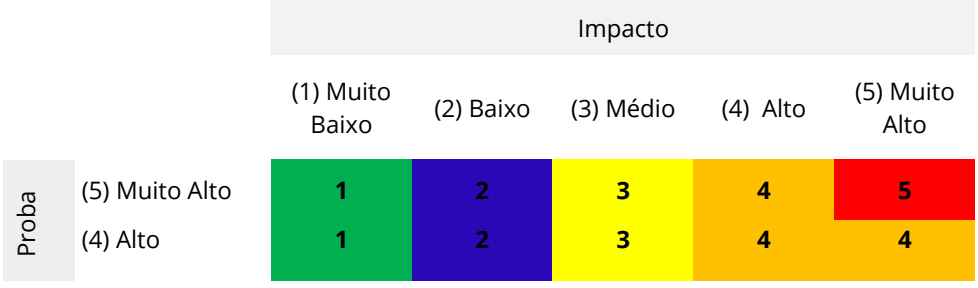
Os níveis de Apetite a Riscos estão relacionados às tipologias de riscos, apresentadas na seção 7.2.1, e determina valores considerados razoáveis a assumir na execução de sua estratégia de negócio, para cada uma dessas tipologias, considerando os critérios de riscos Negativos e Positivos.

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 a criticidade do risco, para cada tipologia de risco.

No Serpro, o Apetite para Riscos Negativos é definido por meio de 5 níveis, destacados no interior das células da matriz abaixo:

Figura 3 - Níveis de apetite para riscos negativos



(3) Médio	1	2	2	3	3
(2) Baixo	1	1	2	2	2
(1) Muito Baixo	1	1	1	1	1

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, relativas a cada tipologia de risco.

Assim como nos riscos negativos, a matriz de apetite para riscos positivos possui 5 níveis. Pode ser observado que tais níveis de apetite comportam-se de forma inversa à matriz de apetite para riscos negativos, conforme visualizado no interior das células da matriz abaixo.

Figura 4 - Níveis de apetite para riscos positivos

	Impacto				
	(1) Muito Baixo	(2) Baixo	(3) Médio	(4) Alto	(5) Muito Alto
(5) Muito Alto	5	4	3	2	1
(4) Alto	5	4	3	2	2
(3) Médio	5	4	4	3	3
(2) Baixo	5	5	4	4	4
(1) Muito Baixo	5	5	5	5	5

A área de Gestão de Riscos e Controles Internos 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. A revisão do apetite deve ser dinâmica, permitindo aos dirigentes configurar o esforço de gestão de riscos empregado nos processos, planejamento estratégico e projetos.

7.0 METODOLOGIA PARA GESTÃO DE RISCOS OPERACIONAIS

A Metodologia de Gestão de Riscos Operacionais e Controles Internos 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 visualizar, de forma estruturada, o apetite aos riscos e diretrizes gerais para o gerenciamento de riscos e controles internos.

Em conformidade com a ISO 31000:2018, o Processo de Gestão de Riscos e Controles Internos 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;

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 5 - Processo de Gestão de Riscos Operacionais

Fonte: NBR ISO 31000 - fev.2018 (adaptado)

A aplicação da metodologia de gestão de riscos operacionais e controles internos 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 Internos 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 Internos.

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, Riscos Estratégicos e Riscos de 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 de 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 também deve ser orientado pelos objetivos da organização e da própria Unidade Organizacional, pelos processos e seus objetivos, além do Apetite a Riscos definido para cada tipologia de risco.

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 Internos 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 internos 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 6 - Relação entre Causa, Evento e Consequência do Risco

Um risco pode ter mais de uma causa ou consequência e após a sua descrição, será possível categorizá-lo quanto à tipologia e aos controles internos.

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 classificação das tipologias auxilia a organização a entender quais os principais fatores de riscos que a podem afetar. No Serpro, as tipologias orientam ainda o nível de Apetite a Riscos, conforme descrito na seção 6.

Uma boa forma de se associar esta tipologia é sempre avaliar as causas do risco, para saber a que se relacionam (financeiro, legal, operacional, privacidade e proteção de dados, etc.), de forma a identificar a tipologia mais adequada. O Serpro dispõe das tipologias de riscos abaixo:

a) À Integridade: 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. O Anexo 1A - Orientação Técnica para a tipologia de Riscos à Integridade, traz orientações e informações complementares sobre a identificação e gestão dos riscos à integridade.

b) Equilíbrio Comercial e/ou Financeiro: eventos que prejudicam a relação receita versus custo do produto ou serviço, afetando capacidade de comercializar o produto ou serviço, incapacidade de reter os contratos de receita e clientes e dificuldade para captar novos clientes ou contratos.

c) Eventos Externos: eventos externos que podem comprometer as atividades do Serpro, geralmente, extrapolam a governança como: aspectos sociais, culturais, políticos, jurídicos, regulatórios, financeiros, tecnológicos, saúde pública, econômicos e ambientais em âmbito internacional, nacional, regional ou local.

d) Financeiro: eventos que podem comprometer a capacidade do Serpro de dispor dos recursos orçamentários e financeiros necessários à realização de suas atividades, ou que possam comprometer a própria execução orçamentária ou financeira.

e) Gestão de Risco de 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.

f) Imagem/Reputação: estão ligados a problemas e danos relacionados à imagem e a marca da empresa.

g) Legal/Não Conformidade: incluem riscos legais e regulatórios – geralmente estão associados às normas legais e decisões dos órgãos de controle e de fiscalização, em especial do Ministério da Transparência e Controladoria-Geral da União - CGU e do Tribunal de Contas da União – TCU, nesta tipificação incluem também os eventos derivados de alterações legislativas ou normativas que possam comprometer as atividades da organização ou ainda aqueles decorrentes de contestações judiciais às suas ações.

h) Pessoas: eventos que podem comprometer as atividades do órgão, departamento ou divisão relativo a pessoas, seja por uma falha humana ou desconhecimento sobre o assunto.

i) Privacidade e Proteção de Dados: Envolvem os riscos associados às regulamentações de privacidade, ao aumento da perda de dados ou ao crescimento excepcional dos dados pessoais[4].

j) Processos: eventos que podem comprometer as atividades do órgão, departamento ou divisão, normalmente associados à inadequação dos processos internos.

k) Segurança da Informação: São os riscos que impactam a confidencialidade, disponibilidade, autenticidade ou integridade da informação. Estão associados com o potencial de ameaças que possam explorar falhas e vulnerabilidades que podem expor dados e informações da empresa a ameaças. Nessa análise são avaliadas configurações de redes, problemas em aplicativos, softwares que podem causar falhas futuras.

l) Tecnologia: eventos que podem comprometer as atividades do órgão, departamento ou divisão, normalmente associados a falhas ou deficiências na infraestrutura e sistemas.

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 internos

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 de mapeamento dos riscos. 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).

4 Os impactos aos riscos com tipologia de Privacidade e Proteção de Dados devem ser avaliados conforme a Tabela 5 – Item 7.3.3 desta metodologia.

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 ("onde 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 ocorra a necessidade, ou não seja possível a possibilidade, de tratamento ao 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 Internos.

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 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:

a) eventos completamente inesperados que geram ganhos para a organização sem que haja um planejamento prévio (ganho por acaso);

b) não se deve confundir a excelência da gestão de riscos negativos com a gestão de riscos positivos;

c) uma gestão de riscos positivos ineficiente pode parecer uma gestão de riscos negativos; e

d) 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 de Negócio.

7.3 Avaliação dos riscos e 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 ao nível de risco Projetado buscando, sempre que possível, atingir o Nível de Apetite associado ao risco. Controles internos incluem, mas não estão limitados a processo, norma, política, dispositivo, prática, ou outras condições e/ou ações que mantêm ou modificam riscos.

Os controles internos podem ser:

a) Preventivos: atuam 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; e

b) Contingenciais: são controles previamente definidos para serem executados quando ocorrer a materialização do risco, com o intuito de diminuir o impacto de suas consequências para os riscos negativos ou ampliá-lo para os riscos positivos. Exemplos de controles de atenuação e recuperação: plano de contingência, tomada de contas especiais e procedimento apuratório.

Além disso, quanto à implementação podem ser:

a) Existentes: implementados na gestão de riscos atual;

b) A melhorar: controles existentes, mas que precisam de melhorias, a serem considerados no nível de risco projetado; e

c) Propostos: são os novos controles que devem ser implementados para reduzir o nível de risco, para atingir o nível de risco projetado.

A descrição dos controles existentes consiste no detalhamento dos controles internos 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 avaliação 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 afetará 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 abaixo demonstra um diagrama de comparação entre risco positivo e negativo, consolidando todos os elementos até aqui apresentados.

Figura 7 - 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 1 - Correspondência dos elementos da Gestão de Riscos Estratégicos Positivos

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 Cálculo 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 no cálculo do nível do 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 2, considerando-se o período de um ano.

Tabela 2 - 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 internos 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 internos 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 ~~ocorrer~~ se efetiva, pois as circunstâncias indicam moderadamente essa possibilidade, uma vez que políticas e procedimentos para controles internos 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 internos 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 internos 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 principais 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 3 a 5, utilizando a tipologia majoritariamente relacionada à consequência do risco. As tabelas são válidas tanto para riscos positivos (no caso de riscos estratégicos e Riscos de Negócio), quanto para riscos negativos, exceto quando houver ressalvas explícitas.

Tabela 3 - Impacto do Risco - descrição e valores

Impacto	Tipologia / Descrição do impacto nos objetivos (Consequência)			
	À Integridade	**Eventos Externos**	**Equilíbrio Comercial e/ou Financeiro**	**Financeiro**
Muito Baixo (MB=1)	Impacta minimamente o alcance dos objetivos do processo ou das atividades.	Impacta minimamente o alcance dos objetivos do processo ou das atividades.	Impacto comercial mínimo: o risco resulta em um insignificante impacto comercial/ financeiro, sem possibilidade de afetar o negócio e/ou produtos.	Pode gerar impacto financeiro insignificante: < 1% sobre o faturamento do Serpro.
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.	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.	Impacto comercial pequeno: o risco resulta em um pequeno impacto comercial/ financeiro, com possibilidade de afetar minimamente o negócio e/ou produtos.	Pode gerar impacto financeiro pequeno: ≥1% < 3% sobre o faturamento do Serpro.
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.	Impacta significativamente o alcance dos objetivos do processo ou das atividades, porém sem impactos pecuniários significativos.	Impacto comercial moderado: o risco resulta em um moderado impacto comercial/ financeiro, com possibilidade de afetar significativamente o negócio e/ou produtos.	Pode gerar impacto financeiro moderado: ≥ 3% < 10% sobre o faturamento do Serpro.
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.	Impacto alto no alcance dos objetivos do processo ou das atividades, com consequências econômico/ financeiras.	Impacto comercial alto: o risco resulta em um alto impacto comercial /financeiro, com possibilidade de afetar significativamente o negócio e/ou produtos.	Pode gerar impacto financeiro grande: ≥ 10% < 25% sobre o faturamento do Serpro.

Impacto	Tipologia / Descrição do impacto nos objetivos (Consequência)			
	À Integridade	**Eventos Externos**	**Equilíbrio Comercial e/ou Financeiro**	**Financeiro**
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.	Impacto muito alto no alcance dos objetivos do processo ou das atividades. Também pode acarretar consequências nos processos/ sistemas, comercial/ financeiro, ou na continuidade das operações do Serpro.	Impacto comercial muito alto: o risco resulta em um grave impacto comercial ou financeiro, com possibilidade de afetar decisivamente o negócio e/ou produtos.[5]	Pode gerar impacto financeiro que modifica significativamente a continuidade das operações do Serpro: ≥ 25% sobre o faturamento.

Tabela 4 - Impacto do Risco - descrição e valores

Impacto	Tipologia / Descrição do impacto nos objetivos (Consequência)			
	Gestão de Risco de Segurança - GRSI	**Imagem / Reputação**	**Legal/Não Conformidade**	**Pessoas**
Muito Baixo (MB=1)	A materialização do risco pode afetar de forma insignificante os recursos, processos e/ou sistemas envolvidos.	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.	Os efeitos da materialização do risco são meramente formais e podem ser absorvidos pelas atividades do processo, com pouco ou nenhum impacto no alcance de objetivos ou cumprimento de atividades operacionais, e sem repercussões significativas na atuação da gestão do risco.	Impacto circunscrito a um profissional ou percentual reduzido de pessoas/equipes (até 20%) atuantes no processo/área.

5

Impacto	Tipologia / Descrição do impacto nos objetivos (Consequência)			
	Gestão de Risco de Segurança - GRSI	**Imagem / Reputação**	**Legal/Não Conformidade**	**Pessoas**
Baixo (B=2)	A materialização do risco pode afetar os recursos, processos e/ou sistemas envolvidos, mas a implementação de controles é simples.	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.	Os efeitos da materialização do risco ainda podem ser absorvidos pelas atividades do processo, com baixo impacto no alcance de objetivos ou cumprimento de atividades operacionais, e requerem ações de caráter orientativo pela gestão do risco.	Impacto percentual reduzido de pessoas/equipes (de 20% a 40%) atuantes no processo/área.
Médio (M=3)	A materialização do risco causa pequeno impacto nos recursos, processos e/ou sistemas envolvidos, mas a implementação de controles é viável.	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	Os efeitos da materialização do risco são significativos, porém ainda podem ser tratados em condições normais de operação do processo. 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.	Moderado impacto no capital humano, atingindo percentual moderado de pessoas/equipes (de 40% a 60%) atuantes no processo/área.
Alto (A=4)	A materialização do risco causa impacto significativo em vários recursos, processos e/ou sistemas e a implementação de controles é complexa.	Impacto com potencial de repercutir de forma substancial na imagem ou reputação do Serpro, em âmbito nacional. Os prejuízos/ benefícios exigem ação estratégica para mitigar/ampliar os efeitos sobre a imagem e reputação do Serpro.	Os efeitos da materialização do risco são muito significativos. Acarretam impactos no alcance de objetivos da Unidade e/ou do processo. 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.	Impacto significativo no capital humano, atingindo grande percentual de pessoas/equipes (de 60% a 80%) atuantes no processo/área.

Impacto	Tipologia / Descrição do impacto nos objetivos (Consequência)			
	Gestão de Risco de Segurança - GRSI	**Imagem / Reputação**	**Legal/Não Conformidade**	**Pessoas**
Muito Alto (MA=5)	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.	Impacto que apresenta altíssimo potencial de repercutir na imagem e reputação do Serpro, cuja alteração é difícil ou improvável a curto ou médio prazo.	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.	Impacto significativo no capital humano, atingindo percentual crítico de pessoas/equipes (de 80% a 100%) atuantes no processo/área e/ou profissionais de mercado com potencial perspectiva de ingresso no quadro do Serpro.

Tabela 5 - Impacto do Risco - descrição e valores

Impacto	Tipologia / Descrição do impacto nos objetivos (Consequência)
	Privacidade e Proteção de Dados
Muito Baixo (MB=1)	Sob a ótica da organização, não envolve tratamento crítico de dados pessoais [6] e há possibilidade de impacto insignificante para a organização (financeira, imagem/reputação, segurança da informação, outras). Sob a ótica do titular de dado pessoal [7], os titulares de dados pessoais não serão afetados.
Baixo (B=2)	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.

6 (*) 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.

7 (**) 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 (Consequência)
	Privacidade e Proteção de Dados
Médio (M=3)	Sob a ótica da organização, não envolve tratamento crítico 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)	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)	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 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 - Impacto do Risco - descrição e valores

Impacto	Tipologia / Descrição do impacto nos objetivos (Consequência)		
	Processos	**Segurança da Informação**	**Tecnologia**
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.	1. Impacto no Nível de Serviço Contratado - não afeta ou é mínimo 2. Serviços afetados - nenhum, insignificante, mínimo 3. Sistemas de Missão Crítica envolvidos - não afeta 4. Solução aplicada - definitiva 5. Amplitude do Dano/Ganho – nenhuma.
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.	1. Impacto no Nível de Serviço Contratado - mínimo 2. Serviços afetados - mínimo ou pequeno 3. Sistemas de Missão Crítica envolvidos - não afeta 4. Solução aplicada - definitiva 5. Amplitude do Dano/Ganho – baixo.
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.	1. Impacto no Nível de Serviço Contratado - pequeno a moderado 2. Serviços afetados - mínimo, pequeno ou moderado 3. Sistemas de Missão Crítica envolvidos - não afeta 4. Solução aplicada - definitiva 5. Amplitude do Dano/Ganho – moderada.

Impacto	Tipologia / Descrição do impacto nos objetivos (Consequência)		
	Processos	**Segurança da Informação**	**Tecnologia**
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.	1. Impacto no Nível de Serviço Contratado - moderado a significativo 2. Serviços afetados - moderado a significativo 3. Sistemas de Missão Crítica envolvidos - no máximo 1 SMC 4. Solução aplicada - definitiva ou de contorno, em caso de impacto negativo 5. Amplitude do Dano/Ganho – significativa.
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.	1. Impacto no Nível de Serviço Contratado - significativo a alto 2. Serviços afetados - significativo a alto 3. Sistemas de Missão Crítica envolvidos - mais de 1 SMC 4. Solução aplicada - definitiva ou de contorno, em caso de impacto negativo. 5. Amplitude do Dano/Ganho – grande.

O Nível de Risco (NR) é gerado pelo produto resultante entre a probabilidade e o impacto. O NR pode ser calculado para três cenários distintos:

a) Nível de Risco Inerente (NRi) é calculado para os riscos em sua forma intrínseca, ou seja, sem a atuação de controles. O Nível de Risco Inerente (NRi) é gerado pelo produto resultante entre a probabilidade inerente e o impacto inerente (NRi = Pi x Ii). O nível de risco inerente deve ser avaliado nesta fase;

b) Nível de Risco Atual (NRa) é calculado para os riscos considerando-se os controles já implementados. O Nível de Risco Atual (NRa) é gerado pelo produto resultante entre a probabilidade atual e impacto atual (NRa = Pa x Ia). O NRa deve ser calculado durante esta fase do processo de gestão de riscos e controles internos; e

c) Nível de Risco Projetado (NRp) é calculado a partir da projeção ou expectativa de probabilidade e impacto, após a implementação dos controles propostos ou a melhoria dos existentes. O Nível de Risco Projetado (NRp) é gerado pelo produto resultante entre a probabilidade projetada e o impacto projetado (NRp = Pp x Ip). Em caso de aceitação do risco, o NRp deverá ser o mesmo do NRa (mesma Probabilidade e mesmo Impacto). 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.

A cada risco deve ser adotada uma estratégia de resposta. Após o cálculo do nível de risco atual, identifica-se e avalia-se a efetividade de políticas, procedimentos, técnicas e ferramentas, ou seja, os controles internos, que têm por objetivo manter ou diminuir 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 a seguir:

Tabela 7 - 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 normalmente é reduzido quando ele está acima do Apetite a Riscos definido. O tratamento é realizado por meio dos controles internos, 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 nível de risco 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, ou seja, um risco aceito não deve ser cancelado e prevalece o monitoramento sobre o mesmo.

Tabela 8 - Opções de estratégia de resposta aos riscos positivos

Estratégia	Descrição
Evitar	Decisão de não se envolver com a oportunidade, geralmente nas condições em que o risco positivo está muito abaixo 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 risco está acima 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 nível de risco 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.

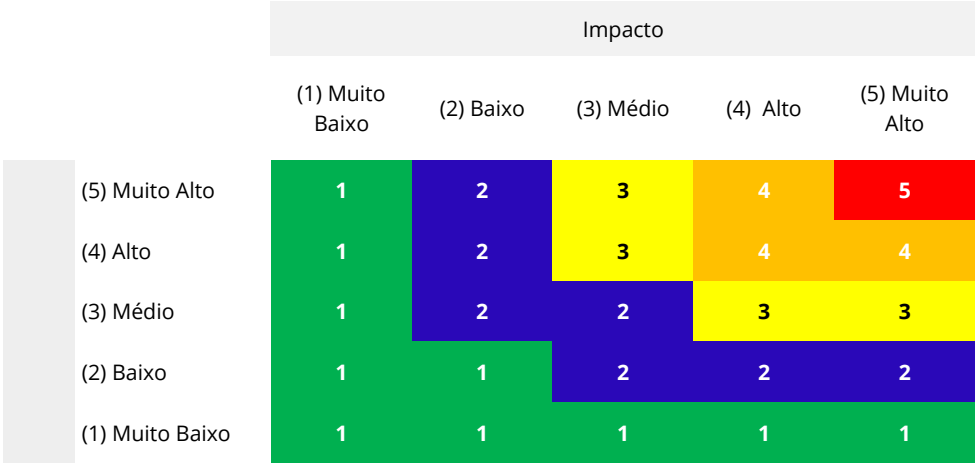
Fonte: Gestão de Riscos – Avaliação da Maturidade (TCU, 2018) - Adaptada

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 à tipologia do 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 Negativos é definido por meio de 5 níveis, relacionados às Tipologias de Riscos adotadas na empresa, grafados no interior das células da matriz abaixo:

Figura 8 - Níveis de apetite para riscos negativos



A tabela 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 da matriz de riscos, nível 3.

Tabela 9 - Referencial de diretrizes para apetite de riscos negativos

Apetite a Risco Negativo	Nível	Diretriz
Muito abaixo do Apetite	Muito Baixo (1)	Zona de conforto. Riscos devem ser monitorados para acompanhar sua evolução, mas 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.
Abaixo do Apetite	Baixo (2)	Nível de risco abaixo do apetite a risco. Condições favoráveis para convivência com o risco, com grande chance de sucesso .
Apetite	Médio (3)	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 (Diretoria responsável pelo risco) para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.
Acima do Apetite	Alto (4)	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	Muito Alto (5)	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 no Serpro o apetite a risco é definido de acordo com as tipologias, para o correto uso das diretrizes, deve-se tomar como base a tipologia associada ao risco. Por exemplo, se a tipologia do risco é relacionada ao Apetite negativo de nível 2 (NR=Baixo), teríamos as diretrizes orientadoras conforme a seguir:

Tabela 10 - Exemplo de diretrizes para apetite de riscos negativos

Apetite a Risco Negativo	NRa	Diretriz
Abaixo do Apetite	Muito Baixo (1)	Nível de risco abaixo do apetite a risco. Condições favoráveis para convivência com o risco, com grande chance de sucesso .
Apetite	Baixo (2)	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 (Diretoria responsável pelo risco) para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.
Acima do Apetite	Médio (3)	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) ou Muito Alto (5)	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 com nível 2 se torna o referencial para que os gestores avaliem as necessidades de tratamento ou aceitação do risco, assim:

a) Se o NRa = Muito Baixo o risco terá as condições favoráveis para aceite;

b) Se o NRa = Baixo, portanto, no mesmo nível do apetite, há uma certa tranquilidade para decidir ou não pela sua minimização;

c) Caso o NRa = Médio, o risco deve ser tratado com atenção; e

d) 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, Riscos Estratégicos e Riscos de 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 ser observado que tais níveis de apetite comportam-se de forma inversa à matriz de apetite para riscos negativos, conforme visualizado no interior das células da matriz abaixo.

Figura 9 - Níveis de apetite para riscos positivos

	Impacto				
	(1) Muito Baixo	(2) Baixo	(3) Médio	(4) Alto	(5) Muito Alto
(5) Muito Alto	5	4	3	2	1
(4) Alto	5	4	3	2	2
(3) Médio	5	4	4	3	3
(2) Baixo	5	5	4	4	4
(1) Muito Baixo	5	5	5	5	5

A tabela 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 da matriz, nível 3.

Tabela 11 - Referencial de diretrizes para apetite de riscos positivos

Apetite a Risco Positivo	Nível	Diretriz
Muito acima do Apetite	Muito Alto (1)	Condições extremamente favoráveis
Acima do Apetite	Alto (2)	Condições favoráveis, grande chance de sucesso
Apetite	Médio (3)	Condições favoráveis, com alguns riscos para gerenciar, mitigar e prevenir. Gestores decidem se a iniciativa deve ser operacionalizada.
Abaixo do Apetite	Baixo (4)	Condições favoráveis, porém, com chances concretas de insucesso se não tiver métricas claras para gerir os riscos do contexto. DIREX aprova as iniciativas.
Muito abaixo do Apetite	Muito Baixo (5)	Condições desfavoráveis, grandes chances de insucesso. Riscos severos em casos de materialização.

Entretanto, como no Serpro o apetite a risco é definido de acordo com as tipologias, para o correto uso das diretrizes, deve-se tomar como base a tipologia associada ao risco. Por exemplo, se a tipologia do risco é relacionada ao Apetite positivo de nível 2, teríamos as diretrizes orientadoras conforme a tabela seguinte:

Tabela 12 - Exemplo de diretrizes para apetite de riscos positivos

Apetite a Risco Positivo	NRa	Diretriz
Acima do Apetite	Muito Alto (1)	Condições favoráveis, com grande chance de sucesso
Apetite	Alto (2)	Condições favoráveis, com alguns riscos para gerenciar, mitigar e prevenir. Gestores decidem se a iniciativa deve ser operacionalizada.
Abaixo do Apetite	Médio (3)	Condições favoráveis, porém, com chances concretas de insucesso se não tiver métricas claras para gerir os riscos do contexto. DIREX aprova as iniciativas.
Muito abaixo do Apetite	Baixo (4) ou Muito Baixo (5)	Condições desfavoráveis, com grandes chances de insucesso. Riscos severos em casos de materialização. Não investir

Conforme o exemplo, o apetite com nível 2 se torna a régua para que os gestores possam realizar suas iniciativas para alavancar vantagens competitivas, assim:

a) Caso o risco tenha o NRa = Muito Alto, existirão “Condições favoráveis, com grande chance de sucesso” para aproveitamento das oportunidades apresentadas pelo risco positivo;

b) Se o NRa = Alto, existem “Condições favoráveis, com alguns riscos para gerenciar, mitigar e prevenir. Gestores decidem se a iniciativa deve ser operacionalizada.”;

c) No caso de o risco apresentar NRa = Médio, o aproveitamento da oportunidade deve ser realizado com cuidado, parâmetros muito claros de aproveitamento e haverá a necessidade de aprovação da iniciativa pela DIREX; e

d) Se o risco apresentar NRa = Baixo ou Muito Baixo, não deve ser depreendido esforço sobre a oportunidade uma vez que há “Condições desfavoráveis, com grandes chances de insucesso.”

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

Uma boa prática para apoiar o processo de avaliação de riscos é estabelecer critérios para priorização e tratamento associados à criticidade dos riscos (níveis de riscos), 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 de Negócio, Riscos de Projetos e Riscos Críticos Operacionais. Para os riscos vinculados a cada uma dessas dimensões, nesta etapa, devem ser considerados os valores dos níveis de riscos 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 13 - 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 indica que nenhuma medida especial é necessária além do monitoramento do risco e controles associados.
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

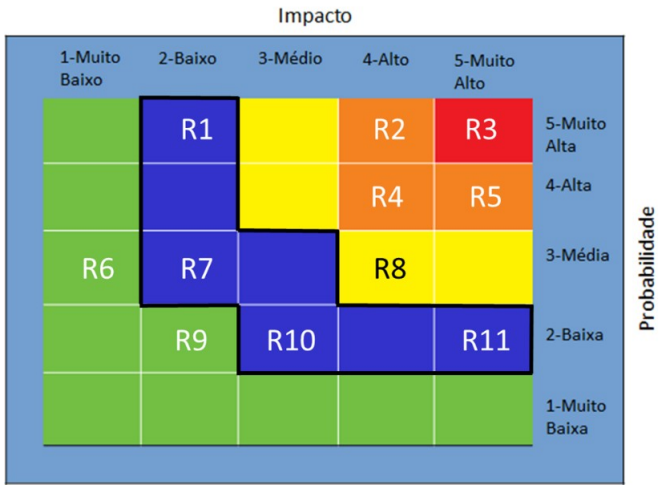
critérios de priorização de riscos positivos. A tabela abaixo representa os critérios referenciais para priorização e tratamento de riscos positivos no Serpro.

Tabela 14 - 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 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 do cálculo dos níveis de risco atuais é possível a construção da Matriz de Riscos. Sugere-se que a priorização para tratamento dos riscos se dê por tipologias de mesmo apetite e, observando-se a matriz, uma maior prioridade aos riscos que mais se distanciarem acima do apetite estabelecido.

Figura 10 - Exemplo de priorização de riscos negativos na Matriz de Riscos



A matriz apresenta um exemplo de situação na qual os riscos negativos (R1, R2, Rn) estão relacionados a tipologias cuja faixa de apetite a risco se encontram no nível 2 - Baixo (faixa 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 de Negócio**.

7.5 Definição dos controles de respostas aos riscos

Pressupõe-se que os controles internos 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 da faixa 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 internos 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 do 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 a faixa 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; e

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 da faixa 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 calculado 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 Nível de Risco atual Alto ou Muito Alto 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 da criticidade dos riscos, 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 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 internos, 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 internos, conforme descrito na seção 7.9, que trata de monitoramento desta metodologia.

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 (Responsável, Aprovador, Consultado, Informado), da tabela a seguir.

Tabela 15 - Matriz RACI com principais atores e papéis na Gestão de Riscos e controles Internos

Atividade	Gestor de Riscos	Agente de Riscos (Agentes GRCI) / Correspon sável	Agente Corporativ o de Riscos	Aprovador	Parte Interessad a	Responsáv el pelo controle	Especialist a 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				
Enviar Risco para Aprovação	R	C	I	I	I		
Aprovar Risco	CI	CI	I	A	I		
Recusar Risco	C	C	I	R	I		

Atividade	Gestor de Riscos	Agente de Riscos (Agentes GRCI) / Correspon sável	Agente Corporativ o de Riscos	Aprovador	Parte Interessad a	Responsáv el pelo controle	Especialist a da Tipologia
Cancelar Risco	R	C	I	I	I	I	
Registrar materialização de Risco	R	C	I	I	I		
Concluir Ocorrência de Materialização do Risco	R	C	I	I	I		
Alterar Data Final Prevista de Implementação do Controle	C	C	I			R	
Implementar Controle	I	I	I			R	
Avaliar Controle	I		R			C	
Cancelar Controle	C	C	I			R	

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[8]:

a) Em Edição: é a situação em que o risco e informações associadas estão sendo editadas na solução de gerenciamento de riscos;

b) Disponível para Análise Crítica: é a situação em que o risco aguarda a avaliação pelo Agente Corporativo de Riscos;

c) Disponível para Análise pelo Especialista da Tipologia: é a situação em que o risco aguarda a avaliação do Especialista da Tipologia;

d) Análise Crítica Concluída: é a situação em que se encontra um risco, quando todas as informações sobre o risco são validadas pelo Agente Corporativo de Riscos;

e) Disponível para Aprovação: é a situação na qual o risco aguarda a aprovação pelo Aprovador de Riscos, normalmente o Superintendente da unidade;

f) Recusado: é a situação na qual o aprovador do risco considera que as informações registradas não são pertinentes à unidade ou não reconhece o registro como risco;

g) Aprovado: é a situação em que as informações registradas são consideradas válidas pelo Aprovador de Riscos;

h) Cancelado: esta situação é indicada quando: houve registro incorreto do risco, o risco deixou de existir; o risco 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 risco (o risco não é válido), ele deve ser cancelado[9]. Neste caso deve ser registrada a justificativa para o cancelamento;

i) Materializado: quando se observa a materialização do risco durante a atividade de monitoramento. Após o adequado tratamento ao risco, por meio da utilização dos controles de contingência, deve ser avaliado o motivo da materialização (causa), impacto causado (consequência), além da verificação da necessidade de criação de novos controles ou melhoria dos controles existentes bem como a revisão dos níveis de probabilidade e impacto sobre o risco; e

j) Materializado com Ocorrência Concluída: quando a ocorrência de um risco materializado foi resolvida por meio de tratamento por controle(s) contingencial(ais).

8 O fluxo detalhado está descrito na ferramenta de diagramação de processos.

9 Riscos nunca são apagados fisicamente da solução de gerenciamento de riscos

Importante observar que os riscos cancelados poderão ser reativados, voltando à situação de edição e retornando o ciclo de aprovação.

O processo de gestão de riscos e controles internos 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 internos em toda a organização;

b) fornecer informações para a tomada de decisão;

c) melhorar as atividades de gestão de riscos e controles internos;

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 internos 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 de riscos 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 Internos elabora o relatório de monitoramento semestral consolidado que é reportado aos órgãos colegiado, DIREX e CA.

7.8.3 Contingência

Os planos de contingência10 compõem o conjunto de controles planejados para a recuperação ou atenuação do impacto, quando da materialização de um risco. A Figura 11 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 11 - 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 crítica da 2ª linha.

7.9.1 Análise crítica

A etapa de **análise crítica dos riscos** é realizada tanto pelo Agente Corporativo de Riscos 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.

Caso o Agente Corporativo de Riscos 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 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 sobre os riscos da tipologia de seu conhecimento constatando se o risco se encontra vinculado à tipologia correta.

O especialista deve avaliar se os controles definidos de fato modificam o nível de risco.

Além disso, caso os controles não possibilitem a redução do NRp para a faixa de apetite a riscos, o risco deve conter uma justificativa. Caso a justificativa seja acatada, o risco deve ser aceito. Em caso contrário, o risco deve ser devolvido para a 1ª linha com as ressalvas registradas.

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 riscos atual, visando alcançar o nível 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 a faixa de apetite a riscos, 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; e

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 internos.

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 da faixa de apetite a riscos 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 avaliação da eficácia do(s) controle(s) implementado(s); e

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 risco atingir o nível de risco projetado (NRp), ou seja, seu nível de risco atual (NRa) 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 VICA - Volatilidade, Incerteza, Complexidade e 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 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;

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

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 nível de risco atual.

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.

8.0 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 Internos para os Projetos Estratégicos deve atender a todas as definições para Processos Operacionais, com exceção das peculiaridades dos projetos, descritas a seguir:

Figura 12 - 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.

Como cada projeto é único, os benefícios, as oportunidades e os retornos obtidos também são singulares, portanto, cada projeto deverá ter seu próprio apetite aos riscos. Deve partir do gestor do projeto sugestão do Apetite a Riscos que o projeto está disposto a assumir na busca do alcance de seus objetivos. Este apetite deverá ser aprovado pelo Diretor ou Superintendente patrocinadores do projeto.

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 Internos, disponibilizando um Agente Corporativo de Riscos 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 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 controles sobre o projeto, 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 Nível de Risco atual Alto ou Muito Alto 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.

9.0 METODOLOGIA PARA GESTÃO DE RISCOS ESTRATÉGICOS E RISCOS DE NEGÓCIO DO SERPRO

Entende-se como Riscos Estratégicos (RE) aqueles eventos que afetam os componentes estratégicos (Visão, Missão ou Valores) ou os objetivos estratégicos da empresa. Riscos de Negócio do Serpro (RNS) também são riscos estratégicos para a empresa uma vez que afetam a missão, a visão ou o valor da empresa, ou seja, seus componentes estratégicos. Riscos Estratégicos e Riscos de 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:

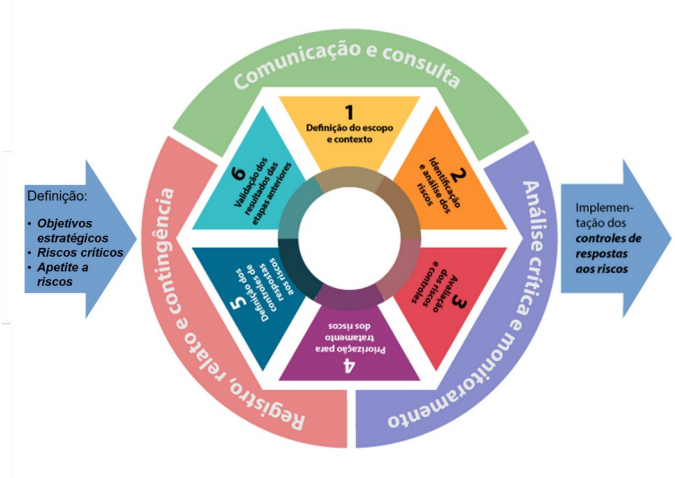
a) conhecimento profundo do negócio da empresa, incluindo o mercado em que atua, ambiente legal, social, político e cultural; e

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 13, 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 13 - Processo de Gestão de Riscos Estratégicos



Fonte: NBR ISO 31000 - fev.2018 (adaptado)

O trabalho de gestão sobre os Riscos Estratégicos e Riscos de 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. Da mesma forma, a Declaração de Apetite a Riscos (RAS), é necessária para iniciar-se o ciclo de gestão dos riscos estratégicos.

Um ponto específico a ser considerado para o levantamento dos riscos estratégicos é a identificação de Riscos de 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 de Negócio, uma vez que, independentemente dos objetivos estratégicos traçados, sempre impactarão 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 Internos 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:

9.1.1 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;

9.1.2 Estabelecer *roadmap* para identificação de RE do próximo ano:

a) O plano de ação para formalização dos riscos estratégicos negativos e positivos é estabelecido nessa atividade.

b) 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;

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

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.

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

9.2.1.1 **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.

Não há um limite para o número de riscos identificados após contribuição dos superintendentes, porém é recomendável, que não seja um número elevado que dificulte a fase de seleção pelos Diretores. Recomenda-se que neste momento sejam levantados até '10' riscos estratégicos ('5' Negativos e '5' Positivos) para cada Diretoria.

9.2.1.2 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;

9.2.1.3 Submeter à revisão dos RE, pelo COGRS: os RE consolidados são submetidos à apreciação pelo COGRS;

9.2.1.4 Submeter RE para apreciação da DIREX / Indicar Diretor responsável: Os RE são apresentados à DIREX para revisão, validação e indicação de responsáveis pelos riscos;

9.2.1.5 Submeter RE para apreciação do COAUD: Os RE são apresentados ao COAUD para revisão e validação;

9.2.1.6 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 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.

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, os controles existentes que não tenham pelo menos um registro de avaliação, 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 indicado um corresponsável. Ele será o responsável por definir a estratégia de resposta.

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.

9.9 Análise crítica e monitoramento

9.9.1 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).

9.9.2 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 avaliação, devem ser avaliados.

Sempre que um controle passe para o estado “implementado”, o Agente Corporativo de Riscos e Controles Internos deve fazer e registrar a avaliação do controle, atestando, com coleta e registro de evidências:

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; e

c) a efetividade, pelo cálculo do nível de risco atual, confrontado com o nível de risco inerente.

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

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 de Negócio deverão ser realizadas conforme descrito na seção 7.10 deste documento, tanto para riscos negativos quanto para riscos positivos.

10.0 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.

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 08/12/2022)

Brasiliano INTERISK - Inteligência em Riscos
www.brasiliano.com.br/software-interisk-apetite-riscos
(último acesso em 08/12/2022)

Gestão de Riscos – Diretrizes para Implementação da ISO 31000:2018
Coleção Risk Tecnologia
São Paulo, 2018.

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.

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

11 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 08/12/2022)

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 08/12/2022)

Elo Group - Handbook para Gestão de Riscos Positivos
©Outubro 2007. ELO Group - www.elogroup.com.br

Gestão de Riscos Positivos
André Macieira, Daniel Karrer, Leandro Jesus e Rafel Clemente
Editora Sicurezza, 1ª edição, 2011

11.0 FICHA TÉCNICA

Gileno Gurjão Barreto
Diretor Presidente - DP

Andre Luiz Sucupira Antonio
Diretor Jurídico e de Governança e Gestão

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

João Vicente Belle Pimentel de Castro
Gerente do Departamento de Controles Internos e Riscos - DIJUG/SUPCR/CRGRC

Equipe técnica:
Alexandre Vieira Coutinho - DIJUG/SUPCR/CRGRC/CRGER
Claudia de Moraes Amaral Marques - DIJUG/SUPCR/CRGRC/CRRCI
Claudia Ferreira Giambastiani da Silva - DIJUG/SUPCR/CRGRC/CRRCI
Daniella Freitas Garcia Dupin - DIJUG/SUPCR/CRGRC/CRGER
Fernando Cezar Xabregas – DIJUG/SUPCR/CRGRC/CRRCI
Gustavo Assis Chaves - DIJUG/SUPCR/CRGRC/CRGER
Nilson Costa da Silva - DIJUG/SUPCR/CRGRC/CRRCI
Patricia Borges de Sousa Wasowski - DIJUG/SUPCR/CRGRC/CRGER

1.0 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, 2022)."

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.

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

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

de Riscos e Controles Internos e, de forma complementar, o disposto nesta Orientação Técnica.

2.0 COMO IDENTIFICAR UM RISCO À INTEGRIDADE

De forma geral, o risco à integridade se materializa quando um agente público[13] 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.

Para os **riscos à integridade** não há tolerância. Uma vez identificados e 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. Em certos casos os controles definidos não são suficientes para se atingir o Nível de Apetite a Risco desejado, podendo ser adotada a Estratégia “ACEITAR”, com a devida justificativa, que deve ser acatada pelo Especialista 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 integridade2:

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.

b1) **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

b2) **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.

d1) **Formas de pressão interna ilegal ou antiética**: influência sobre empregados subordinados para violar sua conduta devida; e ações de retaliação contra possíveis denunciantes; e

d2) **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 Fiscal, de modo a permitir o devido acompanhamento das ações de mitigações estabelecidas pelos colegiados.

3.0 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.

4.0 CONCLUSÃO

A identificação dos riscos à integridade permite aos gestores 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 impacto na empresa.

Conhecidos pela sigla KRI (proveniente do inglês *Key Risk Indicators*), os Indicadores Chave de Riscos referem-se às métricas usadas por uma empresa para que monitorem o grau de exposição a um risco.

Quando tratamos de indicadores chave de desempenho (KPI) falamos de métricas que ajudam uma organização a avaliar o progresso em direção às metas declaradas. Já os indicadores chave de risco (KRI) atuam como métricas de rastreamento, pois ajudam a entender como está o perfil de risco da empresa e qual o impacto de um risco para modificar o objetivo organizacional.

Tanto KRIs quanto KPIs trabalham com os objetivos da organização. Por isso, cada KRI deve ser capaz de ser medido e refletir com precisão o impacto que teria nos KPIs da organização.

De modo geral, KRIs podem ser qualquer métrica utilizada para identificar uma exposição ao risco ao longo do tempo. Na hora de defini-los, é importante entender que para cada risco mapeado pode existir um ou mais indicadores chave.

A figura a seguir ilustra didaticamente o conceito do KRI.

Figura 1 - Indicadores Chave de Risco (KRI)

***Fonte**: ENAP - Escola Nacional de Administração Pública*

Vale ressaltar que a fim de definir os principais indicadores chave de riscos é fundamental que as metas da organização sejam compreendidas. Muitas estratégias de gestão de riscos falham porque não existe um alinhamento com as metas organizacionais.

Note ainda que existe uma relação entre risco e desempenho, e para ilustrar, imagine que uma empresa decida criar um KPI para monitorar o crescimento de sua participação no mercado. Como o objetivo dessa empresa é o de expandir a participação, o que pode evitar que isso aconteça?

Rapidamente podemos imaginar o surgimento de novos concorrentes ou perda de clientes. 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.

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

a) Relevância: os KRIs 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.

1.0 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 Internos.

2.0 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 internos. O Método GRSI deve ser aplicado na entrada em produção de novos serviços e nas situações de alteração de arquitetura dos serviços.

3.0 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 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 SG005 - Classificação dos Ativos de Informação do Serpro.

4.0 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:

a) *Brainstorming* para identificação dos riscos associados a Segurança através de exposição de ideias; ou

b) 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:

c) 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:

c1) RTA (Reunião Técnica de Arquitetura) da solução já existente, e

c2) Topologia ou Arquitetura com as alterações;

d) Identificação de riscos de Sistema ou Aplicação que vai entrar em produção - os artefatos que servem de insumos para a identificação dos riscos são:

d1) 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,

d2) DASI (Documento de Arquitetura Simplificada de Infraestrutura), e

d3) AMISP - Análise Multidisciplinar de Segurança e Privacidade (caso realizada);

e) Todos os riscos devem ser registrados, mesmo os que já possuam controles de tratamento de riscos em vigor;

f) Considerações sobre o *Brainstorming*:

f1) Para auxiliar na identificação dos riscos, utilizar questões do tipo “que evento ou acidente poderia afetar a indisponibilidade ou causar dano ao ativo?”,

f2) É fundamental que os facilitadores permaneçam neutros durante a atividade,

f3) Não julgar as ideias (não existem ideias ruins),

f4) Cada situação deve ser discutida e entendida por todos os participantes,

f5) Todos devem contribuir, e

f6) Manter o encontro dentro do horário acordado (não dispersar em discussões paralelas ou filosóficas);

g) Considerações sobre a Arquitetura de Referência (arquitetura com os riscos pré-definidos):

g1) A arquitetura de referência será comparada com a do escopo em análise,

g2) Os riscos em comum foram previamente definidos,

g3) Caso haja mais algum risco a ser identificado, será alvo de avaliação complementar junto aos participantes, e

g4) 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 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:

a) Descrição das Causas e Consequências, e das Ameaças e Vulnerabilidades; e

b) 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):

b1) Investigação e tempo de reparo,

b2) Tempo (de trabalho) perdido,

b3) Oportunidade perdida,

b4) Saúde e segurança,

b5) Custo financeiro das competências específicas necessárias para reparar o prejuízo, e

b6) Imagem, reputação e valor de mercado.

4.2.2.1 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.

4.2.2.2 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.

4.2.2.3 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.

4.2.2.4 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

4.2.2.5 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 Internos 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:

a) O valor estratégico do processo que trata as informações de negócio;

b) A criticidade dos ativos de informação envolvidos;

c) Requisitos legais e regulatórios, bem como as obrigações contratuais;

d) Importância, do ponto de vista operacional e dos negócios, da disponibilidade, da confidencialidade e da integridade; e

e) 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:

a) Nível de classificação do ativo de informação afetado;

b) Ocorrências de violação da segurança da informação (por exemplo, perda da disponibilidade, da confidencialidade e/ou da integridade);

c) Operações comprometidas (internas ou de terceiros);

d) Perda de oportunidades de negócio e de valor financeiro;

e) Interrupção de planos e o não cumprimento de prazos;

f) Dano à reputação; e

g) 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:

a) 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;

b) 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;

c) 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; e

d) 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:

a) Se não for satisfatória, é necessário rever a definição do contexto para nova verificação; ou

b) 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 SG005 – 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 efetividade 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 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:

a) 03.02 – Gerenciar Soluções de Segurança;

b) 12.05 – Gerenciar Continuidade de Negócios; e

c) 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:

a) Se não for satisfatório, é necessário rever a definição do contexto para nova verificação; ou

b) Se for satisfatório, seguir o rito ou optar pela aceitação do risco.

4.3.2.1 Aceitação do Risco

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

a) Nível desejável de risco versus precauções empresariais;

b) Tratar o risco versus o custo envolvido;

c) Riscos que podem resultar em não conformidade com regulamentações ou leis versus nível de impacto; e

d) 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 Final (NRf) deve ser o mesmo do Nível de Risco Atual (NRa) (mesma Probabilidade e mesmo Impacto).

4.4 Comunicação e Consulta

Comunicar os risos 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:

a) Fornecer a garantia do resultado da gestão de riscos GRSI para a organização;

b) Coletar informações sobre os riscos;

c) 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;

d) Dar suporte ao processo decisório em relação a segurança da informação;

e) Obter novo conhecimento sobre a segurança da informação;

f) Coordenar com outras partes e planejar respostas para reduzir as consequências de um incidente;

g) Dar aos tomadores de decisão e às partes interessadas um senso de responsabilidade sobre os riscos GRSI;

Melhorar a conscientização;

h) 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; e*

i) 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.

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

O Relatório deve conter as seguintes informações

a) Identificação:

a1) Os riscos associados a cada ativo de informação, considerando as ameaças envolvidas, as vulnerabilidades existentes e as ações de segurança das informações já implementadas,

a2) 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),

a3) 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,

a4) As alterações nos fatores de risco, e

a5) As mudanças em relação a critérios de avaliação e análise;

1) d5b) Tratamento:

b1) A definição e a priorização das ações de segurança e as atividades de tratamento de riscos que deverão ser realizadas,

b2) Os responsáveis pela execução e pelo acompanhamento das ações de segurança e atividades de tratamento de riscos,

b3) Os prazos de execução das ações de segurança e das atividades de tratamento de riscos, e

b4) As opções de tratamentos de riscos priorizados;

Para cada possibilidade de tratamento detectada em função do risco identificado, devem ser observados:

a) A eficácia das ações de segurança da informação;

b) As restrições técnicas;

c) As restrições físicas estruturais;

d) As restrições operacionais;

e) As restrições organizacionais;

f) Os requisitos legais; e

g) Relação custo-benefício.

4.4.2 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) A abrangência da aplicação da gestão de riscos, delimitando seu âmbito de atuação (escopo) e os ativos de informação que serão objeto de tratamento;

b) A metodologia a ser utilizada que deverá contemplar, no mínimo, critérios de avaliação e de aceitação de riscos;

c) Os tipos de riscos;

d) O nível de severidade dos riscos; e

e) 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:

a) Efetividade dos controles;

b) Abordagem do processo de avaliação de riscos;

c) Valor e categorias dos ativos;

d) Critérios de impacto;

e) Critérios para a avaliação de riscos;

f) Critérios para a aceitação do risco;

g) Custo total de propriedade; e

h) 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:

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

b) 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; e

c) 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.

5.0 FUNÇÕES E ATRIBUIÇÕES NO GRSI

A estrutura de gestão de riscos e controles internos do Serpro, baseada nas melhores práticas e referenciais teóricos, estabelecem 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).

5.1 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;	. Consulta e edita os riscos sob sua gestão	Gestor do Serviço, Sistema, Recurso, Processo

	. Apresentar o escopo escolhido para o grupo, e . Controlar a execução das ações resultantes do levantamento dos riscos	. Visualiza os riscos, enquanto parte interessada	
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	. 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

	unidades, sempre que houver essa necessidade, para o tratamento de um risco sob sua responsabilidade.		
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 efetividade das medidas de controles implementadas, e	. 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
	. Dar suporte a identificação, análise e		

	avaliação dos riscos, se necessário		
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

6.0 CONSIDERAÇÕES GERAIS

6.1 Acidentes, erros e omissões geralmente são responsáveis por maiores perdas do que atos deliberados.

6.2 Nenhum controle de segurança é 100% efetivo.

6.3 Não é possível eliminar todos os riscos.

6.4 Os riscos não eliminados devem ter essa condição documentada.

6.5 Para a realização do método GRSI devem ser conhecidas pelos participantes a sistemática e o escopo do trabalho;

6.6 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);

6.7 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;

6.8 A participação dos convidados no grupo é de fundamental importância para o resultado do trabalho;

6.9 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;

6.10 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;

6.11 De acordo com a norma SG005 – 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;

6.12 Ferramenta de gerenciamento de riscos adotada pela empresa para o registro do método GRSI:

a) *Dashboards* – são gerados diversos, a partir das informações incluídas na ferramenta;

b) Resultados do trabalho de análise ficam arquivados no banco de dados da própria ferramenta;

c) O acesso é feito através do endereço: https://grc.serpro/Default.aspx; e

d) Risco e Controle – a forma de preencher o risco e o controle do método GRSI estão documentadas no Demonstra:

d1) RISCO

https://demonstra.serpro/DEMOS/inclusao_de_resgist/demo/html/demo_1.html?d=31052021102557

d2) CONTROLE

https://demonstra.serpro/DEMOS/teste_/demo/html/?d=04042022090420


SERPRO