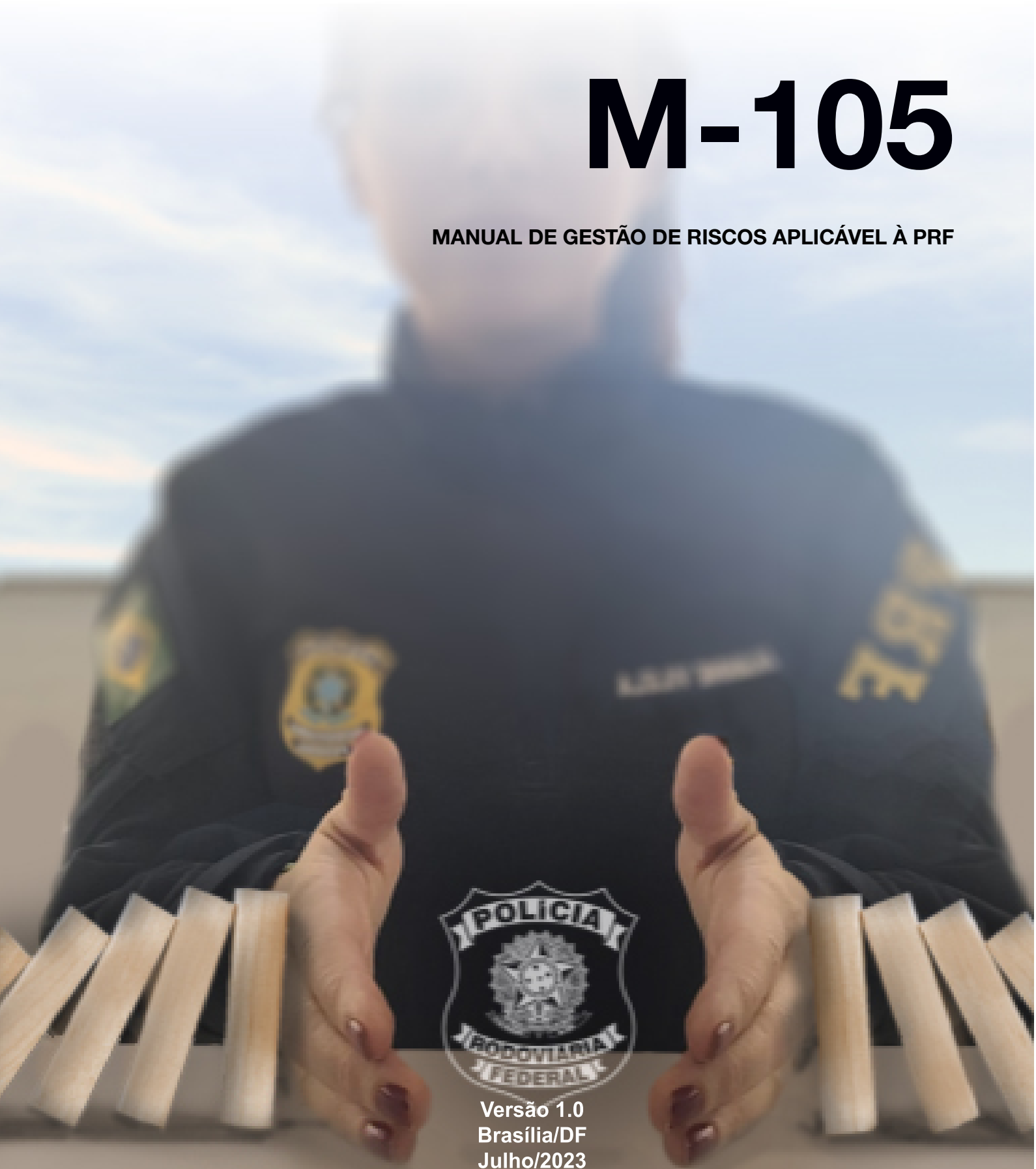
PRF

M-105

MANUAL DE GESTÃO DE RISCOS APLICÁVEL À PRF



Versão 1.0
Brasília/DF
Julho/2023

MINISTRO DA JUSTIÇA E SEGURANÇA PÚBLICA

Flávio Dino de Castro e Costa

POLÍCIA RODOVIÁRIA FEDERAL - PRF

SPO s/nº, Quadra 3, Lote 5 - Setor Policial Sul - Complexo Sede da PRF

CEP 70610-200 - Brasília/DF

DIRETOR-GERAL

Antônio Fernando Souza Oliveira

CORREGEDOR-GERAL - CGCI

Vinicius Behrmann Bento

COORDENADORA DE CONTROLE INTERNO - CI

Ellen Rodrigues D'andrea

CHEFE DO SETOR DE INTEGRIDADE E GESTÃO DE RISCOS

Julianne da Nóbrega Vilela

FICHA TÉCNICA

ORGANIZAÇÃO:

Coordenação de Controle Interno - CI

Setor de Integridade e Gestão de Riscos - SIGR

RESPONSÁVEIS:

Ellen Rodrigues D'andrea

Julianne da Nóbrega Vilela

PRF

SUMÁRIO

NOTA DO DIRETOR-GERAL

É com profunda satisfação que apresentamos a primeira edição do Manual de Gestão de Riscos da PRF, fomentando a incorporação das práticas de gestão de riscos em nossa cultura organizacional e estabelecendo um compromisso com a melhoria contínua dos nossos serviços à sociedade.

Compreendemos que a complexidade do ambiente em que operamos traz consigo desafios inerentes e que a adoção de práticas robustas de gestão de riscos é uma estratégia fundamental para enfrentá-los. É evidente que nos encontramos em uma era de rápidas transformações e evoluções constantes, sendo necessário adaptar e reformular continuamente nossos métodos de trabalho, buscando com afinco a excelência no serviço público mediante a adoção de práticas atualizadas e inovadoras.

A gestão de riscos, nesse cenário, assume um papel de destaque, sendo considerada uma ferramenta indispensável para enfrentarmos os desafios deste ambiente volátil. Acreditamos que, por meio da gestão de riscos eficaz, somos capazes de tomar decisões mais acertadas, bem como atuar de maneira mais eficiente e transparente, favorecendo assim o cumprimento de nossos objetivos estratégicos.

Mesmo assim, estamos cientes de que a jornada rumo à efetivação de uma cultura sólida de gestão de riscos é contínua, e que o aprimoramento das nossas práticas requer um comprometimento sincero por parte de todos nós. Apesar de não se tratar de tema inédito da PRF, reconhece-se que a matéria de gestão de riscos ainda está em fase de maturação e compreensão dentro do órgão, mas que já existe o reconhecimento da importância de estarmos receptivos a melhorias necessárias para atingir os objetivos associados à missão institucional da PRF.

Por meio deste Manual, portanto, a Polícia Rodoviária Federal demonstra seu compromisso não apenas com a gestão eficaz dos riscos inerentes ao nosso trabalho, mas também com a transparência, responsabilidade e melhor entrega de nossos serviços. Este Manual representa nosso desejo de buscar sempre a excelência, de evoluir constantemente e de enfrentar com coragem e preparo os desafios que se apresentam. Ele reflete o espírito da PRF de adaptar-se às mudanças, de aprender com as experiências e de continuar a servir com dedicação e profissionalismo à sociedade brasileira.

Antônio Fernando Souza Oliveira

Diretor-Geral

APRESENTAÇÃO

A gestão de riscos é uma área cada vez mais relevante na administração pública, pois possibilita ferramentas hábeis a garantir eficácia e eficiência na gestão de recursos e políticas públicas, podendo evitar o desperdício de recursos públicos e comprometimento inadequado de força de trabalho, fatores que são riscos inerentes aos processos e atividades governamentais e que podem ser evitados, ou mitigados, com o fortalecimento da cultura de gestão de riscos, variável decisiva para o sucesso ou o insucesso da missão institucional de um órgão.

Sabemos que PRF, enquanto órgão de segurança pública, trabalha cotidianamente com atividades que envolvem os mais variados riscos, nas mais diversas matérias, motivo fundamental para dedicarmos atenção à compreensão da gestão de riscos como ferramenta de trabalho de forma prática e que melhor garanta a consecução dos serviços de segurança pública com cidadania entregues à sociedade.

Corroborando com o empenho contínuo que a PRF tem apresentado ao longo dos anos para modernizar seus processos, normas, tecnologias e padrões para atender os anseios sociais e aperfeiçoar a qualidade de seus serviços, de modo a manter sua posição de instituição de Estado íntegra e eficaz, o presente manual se apresenta como uma ferramenta ao gestor para o estabelecimento da governança da PRF calcada nos pilares da integridade e *compliance*, unificando e esclarecendo procedimentos para consolidação da cultura da gestão de risco nos processos de interesse da instituição.

Destaca-se, inclusive, que se pretende por meio deste manual dar cumprimento à Instrução Normativa Conjunta nº 01, em 10 de maio de 2016, pelo Ministério do Planejamento, Orçamento e Gestão e a Controladoria-Geral da União, a qual estabeleceu a obrigação de implementar a integridade e a gestão de riscos em todas as políticas públicas executadas por entidades e órgãos do Poder Executivo Federal.

Neste cenário, resta indubitável que a inovação e melhoria de serviços almejada pela PRF, quando associada a uma gestão de riscos eficiente, permitirá não apenas a adaptação célere às mudanças no cenário de segurança pública, como também uma resposta mais rápida e eficaz aos desafios emergentes, em uma postura proativa e não mais apenas reagindo intempestivamente aos problemas sociais que permeiam o cenário nacional. Desta forma, ao aprimorar seus processos internos de trabalho, esta instituição reafirma seu compromisso contínuo de entregar serviços públicos com excelência e integridade, seguindo exitosa na missão constitucional de garantir a segurança pública com cidadania nas estradas.

CAPÍTULO I - DAS DISPOSIÇÕES INICIAIS

1. Inicialmente, é necessário destacar que a PRF possui um papel claro diante da sociedade e, assim, um contrato implícito de prestação de determinados serviços, com qualidade, celeridade e eficiência.

2. Esses serviços e a forma de sua execução, inclusive, estão consolidados no Plano Estratégico da PRF, conforme Portaria DG/PRF nº 245, de 30 de junho de 2023, que contempla ações para os anos de 2023 a 2028, a qual apresenta os objetivos estratégicos do órgão, as entregas institucionais esperadas, em quais valores elas se baseiam e qual a visão que justificou suas escolhas.

3. Isso significa dizer que, uma vez escolhidos os objetivos do órgão, todas as ações por ele praticadas devem dizer respeito a pelo menos um desses objetivos, de forma que se torna imprescindível criar ferramentas que protejam todas as decisões e procedimentos envolvendo o alcance desses objetivos.

4. Essa ferramenta de proteção é chamada de gestão de riscos, caracterizada como o processo de identificação, avaliação e resposta aos riscos que uma organização enfrenta em suas atividades diárias, os quais são eventos ou situações que podem ter um efeito adverso sobre os objetivos da organização, como perdas financeiras, interrupções nos negócios e danos à reputação.

5. Dessa forma, a implementação da gestão de riscos na Polícia Rodoviária Federal é de suma importância para garantir uma melhor execução dos seus objetivos e das entregas planejadas para a sociedade. Uma vez que essa ferramenta permite identificar, avaliar e controlar os riscos presentes nas atividades desempenhadas pelo órgão, ademais, é capaz de garantir maior segurança e eficiência dos seus processos, contribuindo para a tomada de decisões mais acertadas e minimizando a possibilidade de eventos adversos.

6. Portanto, em um contexto de planejamento estratégico alinhado às práticas de governança pública, e partindo do pressuposto de que a alta gestão assume a responsabilidade por estabelecer, manter, monitorar e aperfeiçoar os controles internos do órgão, como demanda a Instrução Normativa Conjunta CGU 01/2016, torna-se fundamental o monitoramento das incertezas e de seus efeitos.

7. Entende-se que uma cultura de risco positiva, que dispensa formalismo excessivo e que foca na aplicação prática de mecanismos de controle, é absolutamente essencial para a gestão eficaz dos riscos.

8. Assim, o passo inicial para atingir um nível de governança apropriado e, consequentemente, incitar uma cultura organizacional de planejamento e tratamento a incertezas é a instauração de um modelo próprio de gestão de riscos na PRF. Esse modelo, integrado ao processo decisório e à formação da estratégia, deve possibilitar que os gestores e demais servidores realizem uma análise estruturada da probabilidade de riscos associados a uma determinada atividade organizacional, seja ela qual for, visando reduzir a gravidade dos impactos na atividade ou na habilidade de gestão.

9. Ao implementar a gestão de riscos, a PRF estará adotando uma abordagem proativa para lidar com possíveis ameaças, em vez de simplesmente reagir a elas quando ocorrerem. Isso significa uma capacidade de antecipar problemas, implementar medidas preventivas e preparar-se adequadamente para lidar com eventos adversos, minimizando o impacto que esses eventos podem causar em suas operações.

10. Além disso, a gestão de riscos também pode contribuir para o avanço contínuo dos procedimentos da PRF, pois permite a identificação de oportunidades de melhorias e a implementação de ações corretivas para evitar que contratempos ocorram novamente. Dessa forma, a PRF pode aumentar a eficiência e eficácia de suas atividades, garantindo a proteção da vida e patrimônio dos cidadãos, como ela se propõe a fazer.

11. Compete ainda informar que a gestão de riscos está diretamente relacionada com a consecução da cadeia de valor da PRF, conforme estabelecido no Plano estratégico da instituição para os anos de 2023 a 2028. Por exemplo, com base na análise de riscos, a PRF pode estabelecer medidas de segurança e fiscalização que minimizem a ocorrência de incidentes e protejam a vida e patrimônio dos cidadãos; pode direcionar seus

esforços de fiscalização para áreas mais críticas, monitorar o desempenho de seus agentes e implementar mecanismos de controle interno para garantir a transparência e integridade de suas atividades; e pode implementar ações de combate ao crime que sejam mais efetivas, minimizando os riscos de confrontos e garantindo a segurança de seus agentes e da população em geral.

12. Portanto, como foi visto até aqui, é possível que a gestão de riscos seja inserida tanto no planejamento dos processos estratégicos da PRF, entendidos como macroprocessos que englobam todos os serviços relativos a um dos objetivos estratégicos do órgão, como no dos processos finalísticos, responsáveis efetivamente pelas entregas à sociedade, a exemplo das operações policiais, ou que possibilitam o andamento de procedimentos corriqueiros da atividade meio, podendo-se mencionar as contratações, aquisições, pagamento de pessoal, entre outros.

13. Inclusive, é salutar apontar que enquanto a maioria dos modelos internacionais e nacionais de gestão de riscos que servem como base para a formalização da metodologia aqui apresentada, como a Instrução Normativa Conjunta CGU n.º 01/2016, o Orange Book, o COSO (II e ERM) e a ISO 31000, dão ênfase principalmente ao aspecto dos riscos estratégicos, a finalidade deste manual é desmistificar o instrumento e auxiliar qualquer servidor a de fato gerir os riscos de seus processos, qualquer que seja a categoria dos riscos observada.

14. Menciona-se que este manual se trata de um projeto piloto de metodologia aplicada aos processos e procedimentos da PRF, o qual busca apresentar os fundamentos da gestão de riscos na PRF, a sua estrutura e a metodologia propriamente dita, com detalhes das etapas do processo de gerenciamento de riscos de forma simplificada e didática.

15. O processo de implantação deve ser inicialmente simples, para que a continuidade e os efeitos sejam percebidos e para que a maturidade possa ampliar e fortalecer, cada vez mais, a organização. Neste sentido, este Manual da PRF contempla esta motivação inicial, criando uma estrutura de controle interno e oferecendo os meios necessários à implementação das mudanças. Busca-se, desse modo, concitar uma mudança nos processos, que seja capaz de se transformar em uma mudança de cultura organizacional, de modo a proporcionar aos gestores uma tomada de decisão baseada em evidências, o que tende a ensejar resultados mais precisos e eficazes.

16. Será dada, portanto, prioridade para uma abordagem prática da gestão de riscos, dispensando a descrição exaustiva de princípios, históricos, modelos e frameworks renomados, para objetivar a demonstração de como o gestor do processo pode, com uma visão mais ampla de seu próprio processo, guiar a efetiva gestão dos riscos verificados. Por isso mesmo também é que se escolhe desenvolver uma metodologia similar à utilizada por órgãos de referência, como o próprio Ministério da Justiça e Segurança Pública e a Controladoria Geral da União, facilitando o intercâmbio de informações quando necessário.

CAPÍTULO II - DAS DEFINIÇÕES

17. **Apetite a risco:** nível de risco que a PRF está disposta a assumir para atingir seus objetivos estratégicos e seus objetivos específicos. Apenas se ressalva que o termo é uma adaptação dos modelos usados em empresas privadas, que medem os riscos conforme a possibilidade de atingir lucro. No caso dos órgãos públicos, ele deve ser entendido como um nível de alerta para se aplicar o tratamento ao risco diferente do aceite.

18. **Análise de risco:** fase do processo de gestão de riscos em que se realiza a análise quantitativa e qualitativa dos riscos que podem impactar o alcance dos objetivos da PRF, de forma a se determinar a resposta apropriada ao risco.

19. **Avaliação de risco:** fase do processo de gestão de riscos em que é feita a comparação do nível do risco com o limite de tolerância a riscos da instituição, a fim de determinar se o risco é aceitável. Também pode denominar o conjunto de procedimentos que envolve as fases de identificação, análise e avaliação de riscos propriamente dita, conforme tratado pela ISO 31000. No presente manual, essa fase será realizada conjuntamente com a fase de análise de risco, sem prejuízo à estrutura do processo.

20. **Categorias de riscos:** classificação dos tipos de riscos definidos pela PRF que possam afetar o alcance de seus objetivos, de acordo com os fatores nele envolvidos.

21. **Causa:** motivo que pode promover a ocorrência do risco.

22. **Consequência:** resultado da ocorrência do risco que foi identificado, afetando diretamente o alcance do objetivo, de forma negativa. Consequências positivas também são possíveis, mas essas não agem sobre riscos, e sim sobre oportunidades.

23. **Controle:** qualquer medida aplicada no âmbito da PRF para gerenciar os riscos e aumentar a probabilidade de que os objetivos e as metas estabelecidos sejam alcançados.

24. **Controles preventivos:** controles que atuam sobre as possíveis causas do risco, com o objetivo de prevenir a sua ocorrência.

25. **Controles de atenuação e recuperação:** controles executados após a ocorrência do risco com o intuito de diminuir o impacto de suas consequências.

26. **Controles detectivos:** controles que atuam na detecção da materialização de um risco ou de sua iminência.

27. **Entendimento do contexto:** trata-se da primeira fase do processo de gestão de riscos, em que se busca a compreensão completa do processo a ser gerido. Ela se inicia com o estabelecimento dos objetivos e passa pelo levantamento das circunstâncias internas e externas que neles influenciam, podendo incluir dados históricos, análises teóricas, opiniões de pessoas informadas e de especialistas, e as necessidades das partes interessadas.

28. **Governança pública:** conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade.

29. **Governança:** combinação de processos e estruturas implantadas pela alta administração da organização para informar, dirigir, administrar, avaliar e monitorar atividades organizacionais, com o intuito de alcançar os objetivos e prestar contas dessas atividades para a sociedade.

30. **Identificação de riscos:** fase do processo de gestão de riscos em que se faz a busca, o reconhecimento e a descrição de riscos, por meio da demonstração de sua causa e de sua consequência.

31. **Incerteza:** incapacidade de saber com precisão a real probabilidade ou impacto de eventos futuros.

32. **Impacto:** efeito resultante da ocorrência do evento de risco.

33. **Mapeamento de processo:** procedimento de exposição documental do fluxo processual, que pode ser realizado na fase de entendimento do contexto, com a finalidade de possibilitar a identificação de gargalos e eventos com potencial para gerar riscos.

34. **Matriz de riscos:** instrumento de representação dos possíveis resultados da combinação das escalas de probabilidade e impacto.

35. **Medida de controle interno (ou medida de tratamento):** políticas e procedimentos adotados para tratar riscos, de modo a assegurar que os objetivos dos processos e da própria instituição sejam alcançados dentro dos padrões estabelecidos.

36. **Monitoramento:** processo de observação sistemática, verificação e registro regular de uma atividade, para que as informações geradas constituam um elemento de tomada de decisão por parte do responsável pelo processo.

37. **Nível de risco:** magnitude de um risco, expressa em termos da multiplicação de seu impacto e pela sua probabilidade.

38. **Processo de gestão de riscos:** aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de identificação, análise, avaliação, tratamento e monitoramento de riscos, bem como de comunicação com partes interessadas em assuntos relacionados a risco.

39. **Proprietário do risco:** pessoa ou conjunto de pessoas que, por lidarem diretamente com o processo que está sendo gerido, são capazes tecnicamente de identificar riscos, suas probabilidades e impactos sobre a atividade e quais as melhores medidas de tratamento aplicáveis.

40. **Probabilidade:** medida de possibilidade de ocorrência de um evento.

41. **Resposta ao risco:** qualquer ação adotada para lidar com risco, podendo consistir em: a) aceitar o risco por uma escolha consciente; b) transferir ou compartilhar o risco a outra parte; c) evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem ao risco; ou d) mitigar ou reduzir o risco diminuindo sua probabilidade de ocorrência ou minimizando suas consequências por meio de medidas de controle.

42. **Risco:** possibilidade de ocorrer um evento que venha a ter impacto no cumprimento dos objetivos, sendo medido em termos de impacto e de probabilidade.

43. **Riscos à conformidade:** eventos que comprometem as atividades de uma organização devido ao não cumprimento de leis, regulamentos, códigos de conduta ou padrões de práticas estabelecidos.

44. **Riscos à integridade:** eventos que configurem ações ou omissões que possam favorecer a ocorrência de fraudes ou atos de corrupção.

45. **Riscos adversos:** surgimento de novos riscos decorrentes da aplicação de uma medida de controle interno. Geralmente ocorrem quando se aplica a resposta de evitar a atividade geradora do risco, uma vez que a cessação de uma atividade pode exigir a criação de outra, cujo risco pode não ter sido gerido ainda.

46. **Risco inerente:** eventos a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de ocorrer o evento ou seu impacto. É o risco em sua acepção bruta.

47. **Risco residual:** eventos a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco. Trata-se do resultado da equação Risco Inerente diminuído da Medida de Controle.

48. **Riscos de imagem ou reputação do órgão:** eventos que possam comprometer a confiança da sociedade ou de parceiros, de clientes ou de fornecedores, em relação à capacidade da PRF em cumprir sua missão institucional.

49. **Riscos financeiros ou orçamentários:** eventos que possam comprometer a capacidade da PRF de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária.

50. **Riscos legais:** eventos derivados de alterações legislativas ou normativas que possam comprometer as atividades da PRF ou, ainda, eventos que possam gerar percalços na seara judicial.

51. **Riscos operacionais:** eventos que possam comprometer as atividades da PRF, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas. Não ocorrem apenas na atividade operacional da PRF, compreendida como sua atividade, mas em todas as operacionalizações, em quaisquer áreas de conhecimento, que são necessárias em um processo de trabalho.

52. **Tolerância ao risco:** nível de variação do alcance de um objetivo que a PRF está disposta a tolerar. Equivale a uma taxa de tolerância de variação em relação ao desempenho ou ao resultado esperado.

53. **Tratamento dos riscos:** processo de estipular uma resposta aos riscos, de modo a mitigar, prevenir ou eliminá-los.

CAPÍTULO III - DA COMPETÊNCIA PARA REALIZAR GESTÃO DE RISCOS

54. A já mencionada Instrução Normativa CGU n.º 1/2016, que estabelece normas sobre a gestão de riscos no âmbito do Poder Executivo Federal, determina, em seu art. 16, parágrafo único, que "os gestores são os responsáveis pela avaliação dos riscos no âmbito das unidades, processos e atividades que lhes são afetos. A alta administração deve avaliar os riscos no âmbito da organização, desenvolvendo uma visão de riscos de forma consolidada."

55. Como se verifica da norma apresentada, há dois tipos de responsabilidades diferentes quando se trata da realização do processo de gestão de riscos, o qual depende do âmbito em que ela é realizada. Isso porque os procedimentos gerenciáveis dentro de uma organização são geralmente divididos entre processos estratégicos e processos operacionais, como já se mencionou em outra oportunidade neste manual.

56. Em termos simples, o gerenciamento de riscos operacionais deve garantir a continuidade das operações da organização, enquanto o gerenciamento de riscos estratégicos deve garantir a adaptação da organização ao ambiente externo e a realização de seus objetivos estratégicos.

57. Assim, no caso de gestão operacional (de todas as atividades corriqueiras da PRF), são os gestores das áreas ao qual o processo corresponde, juntamente com sua equipe, que possuem familiaridade suficiente para apontar quais são os riscos daquelas atividades e qual a melhor forma de lidar com eles. Em outras palavras, são eles que estão em uma posição privilegiada para observar e antecipar possíveis ameaças e tomar as medidas necessárias para tratar desses riscos.

58. A gestão de riscos, portanto, é uma ferramenta essencial do gestor para organizar e planejar os seus processos, sobre os quais detém o conhecimento técnico mais específico e adequado às situações que eles permeiam. A ingerência de qualquer outra área nesse gerenciamento processual afastaria indevidamente do gestor a possibilidade de aplicar sobre seus próprios processos as medidas de controle que ele, como especialista, entende adequadas, possibilitando que as medidas propostas por partes alheias ao tema sejam dissociadas da realidade.

59. Acrescenta-se, ademais, que tanto o COSO ERM quanto a ISO 31000, documentos internacionais que baseiam a política de gestão de riscos adotada pelo MJSP, também reconhecem que a gestão de riscos deve ser feita pelos envolvidos no processo que se pretende avaliar, uma vez que somente quem convive e observa os riscos da atividade é capaz de apontar também suas causas, probabilidades, impactos e consequências. Os órgãos de controle interno, por outro lado, são encarregados do monitoramento e avaliação das medidas de controle instituídas e na comunicação dos resultados para a alta direção e demais responsáveis.

60. A necessidade do presente manual está justamente sobre o fato de que os donos dos riscos precisam realizar seus próprios gerenciamentos. Caberia ao órgão de controle interno da PRF apenas o monitoramento e a avaliação da eficácia das medidas de controle implementadas pelos gestores das áreas ao final da gestão de riscos, conforme teor do art. 11 da IN 01/2016.

61. Por outro lado, tratando-se de processos a nível estratégico, determina a norma que a responsabilidade de realizar a gestão de riscos é da alta gestão, uma vez que os gestores máximos do órgão é que estão em posição de avaliar os riscos em nível organizacional. Esta responsabilidade implica desenvolver uma visão consolidada dos riscos, considerando todos os aspectos da PRF.

62. A alta administração também deve garantir que um ambiente adequado de gerenciamento de riscos esteja em vigor e seja mantido, que os riscos sejam devidamente identificados e avaliados, e que as respostas apropriadas aos riscos sejam implementadas. Isso também inclui a comunicação e a consulta com todas as partes interessadas relevantes, tanto internas quanto externas.

63. Em resumo ao exposto até aqui, apenas os responsáveis pelos respectivos processos é que possuem a competência técnica para gerenciar seus riscos. A PRF, contudo, conta com uma Coordenação de Controle Interno e um Setor de Integridade e Gestão de Riscos, os quais possuem a função de auxiliar e guiar os gestores durante a montagem de seus processos de gestão e, ademais, de monitorar o cumprimento das medidas de tratamento fixadas.

CAPÍTULO IV - DAS FASES DA GESTÃO DE RISCOS

64. Como já foi exposto, o presente manual pretende apresentar uma metodologia de gestão de riscos que tenha semelhança com a metodologia utilizada pela Controladoria Geral da União, mas que, em termos práticos, seja mais simplificada e objetiva.

65. Destaca-se que a escolha por adotar a CGU como parâmetro para a formação da metodologia própria da PRF decorre, inicialmente, do fato de que a principal regra de referência para gestão de riscos no serviço público federal é a Instrução Normativa Conjunta MP/CGU nº 01/2016, que dispõe sobre a sistematização de práticas relacionadas à governança, à gestão de riscos e aos controles internos no âmbito de órgãos e entidades do Poder Executivo Federal, editada justamente por aquele órgão e pelo Ministério do Planejamento, Orçamento e Gestão. Por isso mesmo se observa um nível mais elevado de maturidade na matéria de Gestão de Riscos na CGU, sendo salutar buscar a reprodução de modelos de boas práticas.

66. Acrescenta-se a isso que o próprio Ministério da Justiça e Segurança Pública, por meio do Sistema Agir, exige de seus órgãos subordinados essa mesma metodologia quando se trata da gestão de riscos estratégicos, de forma que é recomendável a sua adoção também por parte da PRF, para unificar procedimentos internamente e adequá-los ao órgão superior.

67. Esclarecido esse ponto, demonstra-se que a metodologia da CGU consta da Portaria nº 915/2017, denominada de Política de Gestão de Riscos (PGR), que estrutura os processos da gestão de riscos, com o alinhamento aos planejamentos estratégico, tático e operacional, considerando também as características específicas e a cultura organizacional.

68. O art. 6º da PGR/CGU, nesse sentido, aponta como sendo necessárias, no mínimo, as seguintes fases:

> I – entendimento do contexto: etapa em que são identificados os objetivos relacionados ao processo organizacional e definidos os contextos externo e interno a serem levados em consideração ao gerenciar riscos;
> II – identificação de riscos: etapa em que são identificados possíveis riscos para objetivos associados aos processos organizacionais;
> III – análise de riscos: etapa em que são identificadas as possíveis causas e consequências do risco;
> IV – avaliação de riscos: etapa em que são estimados os níveis dos riscos identificados;
> V – priorização de riscos: etapa em que são definidos quais riscos terão suas respostas priorizadas, levando em consideração os níveis calculados na etapa anterior;
> VI – definição de respostas aos riscos: etapa em que são definidas as respostas aos riscos, de forma a adequar seus níveis ao apetite estabelecido para os processos organizacionais, além da escolha das medidas de controle associadas a essas respostas; e
> VII – comunicação e monitoramento: etapa que ocorre durante todo o processo de gerenciamento de riscos e é responsável pela integração de todas as instâncias envolvidas, bem como pelo monitoramento contínuo da própria Gestão de Riscos, com vistas a sua melhoria.

69. Todavia, como se mencionou anteriormente, a intenção deste manual é adotar uma metodologia que seja mais acessível e prática para o uso cotidiano na Polícia Rodoviária Federal. Compreende-se que a eficácia da gestão de riscos não necessariamente reside na complexidade do método, mas na sua aplicabilidade no contexto operacional do órgão.

70. As normas e métodos da CGU, assim como as de referência internacional, como a ISO 31000 e a metodologia COSO ERM, por exemplo, proporcionam um robusto quadro de trabalho que abrange diversos aspectos da gestão de riscos, sendo que as peculiaridades e necessidades específicas da PRF tornaram necessária a realização de alguns ajustes procedimentais.

71. Portanto, buscou-se elaborar uma metodologia que agrupasse certas fases do processo de gestão de riscos que guardam semelhança entre si (a exemplo das fases dos incisos III a V do art. 6º da PGR/CGU), a fim de tornar sua utilização mais simplificada, ágil e integrada à rotina de trabalho dos nossos profissionais, reduzindo a sua complexidade sem comprometer a sua abrangência e profundidade. Isso porque a eficiência e

eficácia da gestão de riscos não residem unicamente na complexidade da metodologia, mas na sua adaptabilidade e aplicação direta no ambiente operacional em que a PRF está inserida.

72. Isso exposto, tem-se que a metodologia de Gestão de Riscos da PRF contemplará, no mínimo, as fases demonstradas a seguir:

- Compreensão do Contexto;
- Identificação de Riscos;
- Cálculo do nível de Risco;
- Resposta aos Riscos;
- Monitoramento.

73. Como se pode verificar, o processo de gestão de riscos é contínuo e ininterrupto, de forma que possa ser aperfeiçoado conforme novas situações vão surgindo durante a execução da atividade gerenciada.

74. Assim, uma vez que se compreendeu como será repartida a presente metodologia, parte-se para a melhor explanação de cada uma das etapas.

CAPÍTULO V - DA COMPREENSÃO DO CONTEXTO

75. A definição do contexto envolve a compreensão da situação em que o órgão está inserido, especialmente quanto aos seus objetivos, sua estrutura, seus processos e seu ambiente interno e externo, com o fim de obter uma visão abrangente dos fatores que podem influenciar na sua capacidade de atingir os seus objetivos estratégicos e operacionais e demais resultados esperados. Esse estudo sobre os contextos visa conhecer como o processo é influenciado e até mesmo como influencia o ambiente em que está.

76. Não se trata de uma mera listagem de fatores, mas de um verdadeiro esforço para se enxergar o processo, tarefa ou atividade de forma mais madura. Quanto mais esforço se realiza para compreender o contexto do processo, maior é a precisão nas decisões tomadas nele.

77. Aproveita-se aqui para dizer que, como esta metodologia não pretende se limitar aos processos estratégicos da PRF, mas também ser utilizada em qualquer atividade de interesse, a fase de compreensão do contexto pode levar em conta informações bem específicas da atividade que se pretende gerir, avaliando-se fatores culturais, temporais e políticos que não necessariamente se apliquem a toda a PRF, mas que sejam realidade para a atividade em análise. A intenção é justamente colocar luz sobre cada procedimento tratado.

78. Outro ponto a se considerar é que a gestão de riscos precisa ser específica para o processo analisado, não bastando uma gestão genérica para ser utilizada em processos diversos. A ferramenta não pode ser meramente formal, mas precisa ter real utilidade.

79. O entendimento do processo organizacional envolve a obtenção de informações sobre o seu funcionamento, incluindo o fluxo atual do processo, se houver, e a identificação dos objetivos que devem ser alcançados.

1. DEFINIÇÃO DE OBJETIVOS

80. Sem a fixação de objetivos, o processo de gestão de riscos não pode ocorrer de forma eficaz e realista. Isso porque, enquanto não se sabe ou não se define a finalidade da realização de uma tarefa, não há motivos para melhorar os procedimentos que a envolvem.

81. Como se sabe, a função primária da gestão de riscos é justamente impedir que os objetivos de uma organização sejam frustrados, investigando-se quais os fatores que podem concorrer para tanto. Dessa forma, a definição clara de objetivos é um passo essencial no processo de gestão de riscos, servindo como o fundamento sobre o qual todas as outras etapas são construídas.

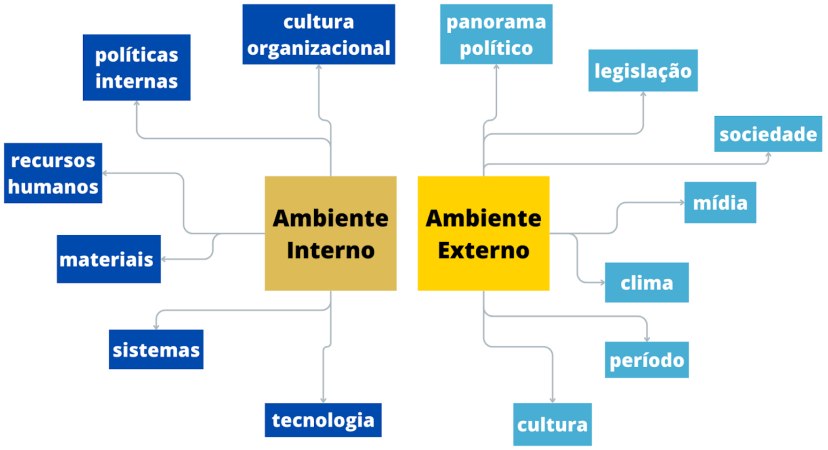
82. Nesse ponto, portanto, o Gestor de risco e sua equipe de apoio devem definir os objetivos do processo sob sua responsabilidade que pretendem gerenciar, de forma que esses sejam precisos, mensuráveis, alcançáveis, relevantes e temporais. Acrescenta-se, apenas, que no caso de processos com várias fases, a exemplo de uma licitação, é possível realizar a gestão de cada uma dessas fases, definindo-se os objetivos de acordo com elas.

2. AMBIENTE INTERNO E EXTERNO

83. O ambiente interno, como o nome já pode sugerir, diz respeito aos elementos de dentro da instituição que podem influenciar a maneira pela qual aquela gerenciará os seus riscos, positiva e negativamente. Essa análise inclui, entre outros elementos, a cultura organizacional, as políticas internas, as práticas, atividades, recursos humanos, materiais, tecnológicos, competências, os processos de tomada de decisão e os sistemas de informação.

84. O ambiente externo, por sua vez, trata de situações que estão fora do controle do órgão, mas que exercem influência positiva ou negativa em suas atividades, a exemplo do panorama socioeconômico e político, da legislação, a visão da sociedade e da mídia sobre a instituição, a relação com os órgãos de controle interno e

externo da União, entre outras coisas. Quando se pensa na atividade fim da PRF, ademais, também é preciso considerar condições climáticas da época em que aquela irá acontecer, a cultura local, feriados, modo de comportamento da população no período e outras especificidades.



85. O importante é que a gestão de riscos não seja genérica e desassociada da realidade, mas que verdadeiramente possibilite projeções acertadas que precisam ser geridas, garantindo que todos os fatores relevantes sejam levados em consideração.

86. Na presente fase é importante que se façam perguntas como “O que pode dar errado?”, “Onde somos vulneráveis?”, “Como nossas operações poderiam ser interrompidas?”, “Quais as tecnologias disponíveis e emergentes que podem influenciar nossas atividades?”, “Onde investimos mais recursos?”, “Quais atividades são mais regulamentadas?”, “Quem são os responsáveis?”, “Quais os interesses políticos e econômicos envolvidos na operação?”, “Onde devemos atuar com maior ênfase?”, “Como poderemos agir em caso de manifestações populares?”.

87. A ferramenta mais conhecida para organizar as informações de ambiente interno e externo é um diagrama intitulado de análise F.O.F.A., acrônimo para Forças, Oportunidades, Fraquezas e Ameaças, também conhecido como matriz SWOT. Trata-se de uma ferramenta que auxilia na identificação visual das situações importantes que incidem nos processos e podem incentivar a participação da equipe no oferecimento de ideias, de acordo com o ponto de vista de cada setor envolvido.

88. Destaca-se, todavia, que o preenchimento do diagrama em si não é fase obrigatória do processo de gestão de riscos, mas mera ferramenta de apoio para visualização de ideias, de forma que só deve ser utilizada se realmente se provar agregadora nesse procedimento, já que existem diversas outras formas de tratar esse ponto.

89. Necessário apenas se ressalvar que o sistema de gestão de riscos estratégicos utilizado pelo Ministério da Justiça e Segurança Pública, o sistema Agir, exige dos responsáveis pelos processos, quando da realização dos seus registros, que a fase de compreensão do contexto seja feita por meio dessa matriz, razão pela qual é necessário conhecê-la.

90. Como se mencionou, contudo, é possível se utilizar de outras formas de levantamento das informações, inclusive a própria oferta livre de ideias do grupo de trabalho. Dito de outra forma, o gestor pode se cercar de todos os atores daquele determinado processo para que todos eles lancem ideias de fatores internos e externos que podem influenciar na consecução da atividade.

91. No caso de uma Operação Policial, portanto, poderiam ser levantadas informações como as seguintes, sem necessariamente se utilizar de uma matriz como a F.O.F.A., desde que seja possível criar uma visualização abrangente da situação:

- Objetivos da operação
- Local da operação e período
- Legislação aplicável
- Recursos humanos disponíveis
- Sistemas
- Cenário político, financeiro, legal, tecnológico, econômico
- Problemas do passado em situações semelhantes
- Fluxo processual

92. Para auxílio da documentação dessa fase, pode ser utilizada a tabela disponível no Anexo I deste material.

93. Menciona-se, por fim, que apesar de a matriz F.O.F.A. levantar pontos positivos e negativos, geralmente se trabalha na gestão de riscos sobre os pontos negativos, buscando-se ajustar às situações que impedem ou dificultam a consecução dos objetivos. Em um nível mais maduro e consolidado, a gestão de riscos também pode ser utilizada para incrementar os pontos positivos dos processos. Todavia, para fins de inicialização da cultura de gestão de riscos na PRF, é necessário que primeiro se consolide o instrumento para tratar os riscos negativos.

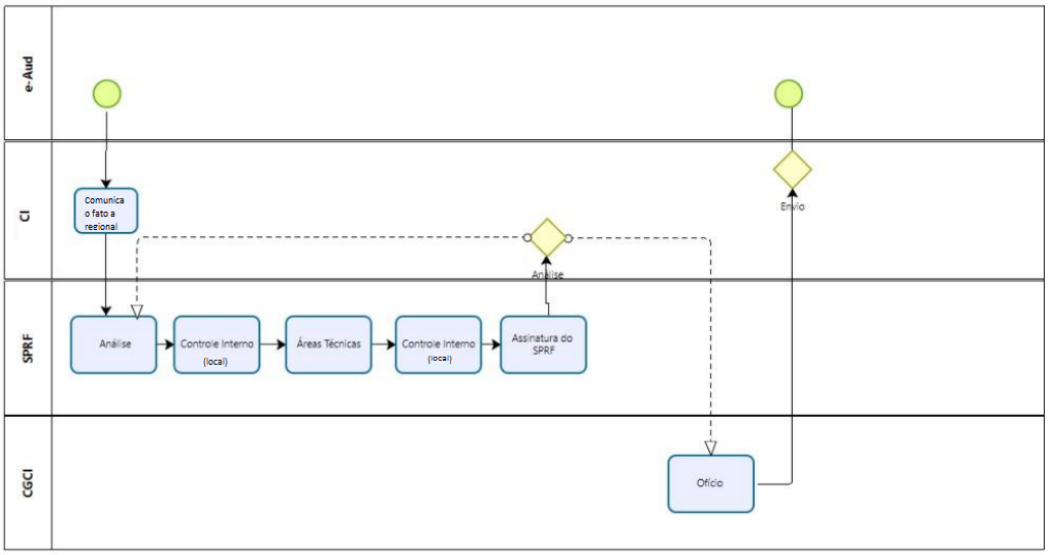
3. MAPEAMENTO DE PROCESSOS

94. O mapeamento do processo é uma ferramenta importante para entender onde e como realizar a gestão de riscos na PRF. Ele envolve a representação gráfica das etapas, atividades e fluxos de informação de um processo dentro da organização, proporcionando uma visualização clara e objetiva dos pontos críticos, redundâncias, gargalos e pontos de ineficiência em que os riscos podem ocorrer, permitindo-se a concentração de recursos e esforços onde já se visualizou ser necessário.

95. Importante ressaltar que o mapeamento tanto pode ser um método utilizado com a finalidade de se escolher processos para gerenciar, como também após as escolhas dos processos entendidos como relevantes, situação em que se encaixa nessa fase da gestão de riscos.

96. Apesar de ser altamente recomendado mapear o processo para se aplicar a metodologia de gestão de riscos de forma mais clara e fácil, também não se pretende transformar essa ferramenta em obrigatória, para que a burocratização do procedimento não iniba a sua utilização.

97. Sendo da opção do dono do risco a realização do mapeamento, por outro lado, tem-se que a notação internacional BPMN é a mais sugerida para tanto. Traz-se como exemplo o fluxo processual que a Coordenação de Controle Interno possui para o recebimento e resposta a uma auditoria da CGU enviada pelo sistema e-aud.



98. Ressalta-se que existem três possíveis abordagens para o mapa do processo:

- Mapa de como o processo está sendo feito atualmente - processo real, ideal para identificar gargalos;
- Mapa de como a norma interna demanda que ele seja feito - processo legal, utilizado para comparar com o que é feito de fato;
- Mapa de como seria o modo ideal para ele acontecer - processo ideal, quando se acredita que a norma está desatualizada, por exemplo.

99. A utilização de uma ou outra abordagem (ou até de mais de uma) é uma escolha do gestor e depende do grau de maturidade e correção do processo.

CAPÍTULO VI - DA IDENTIFICAÇÃO DE RISCOS

100. A fase de identificação dos eventos de riscos é aquela por meio da qual se busca encontrar, reconhecer e registrar os riscos do processo em análise, a partir do que foi assimilado na fase anterior. Uma vez listadas todas as ameaças e fraquezas presentes no caso, por exemplo, é possível pensar em como essas podem impactar no alcance do resultado/objetivo.

101. Destaca-se que o risco não é um mero problema existente ou uma crítica ao processo organizacional (problemas devem ser resolvidos pela adequação do processo), mas a possibilidade de ocorrência de um evento que tenha impacto no atingimento dos objetivos do órgão naquele determinado processo. Há incerteza sobre sua ocorrência, ou seja, existe probabilidade, mesmo que pequena, de que ocorra, e somente se ele ocorrer é que pode haver impactos negativos nos objetivos. Por isso que se recomenda que o risco seja escrito com verbos no infinitivo, para enfatizar que se trata de um evento possível e futuro.

102. A intenção da gestão de riscos é eliminar o fator surpresa das eventuais ocorrências do processo.

103. Assim, é ideal que a equipe técnica construa lista abrangente de eventos de riscos relacionados a cada um dos objetivos do processo, por meio da resposta a perguntas como: “Quais eventos podem EVITAR, ATRASAR ou PREJUDICAR o atingimento de um ou mais objetivos do processo organizacional?”. De outra forma, também devem ser considerados os fatores de sucesso para determinada atividade e quais eventos podem agir negativamente nesses fatores.

104. No processo de identificação de riscos, deve-se buscar a participação de pessoas que conheçam bem o objeto de gestão de riscos, utilizando técnicas/ferramentas que permitam a coleta do maior número de riscos, tais como brainstorming, entrevistas, visitas técnicas, pesquisas etc.

105. Havendo dificuldade em realizar tal procedimento, ademais, é possível recorrer-se à seguinte listagem de tipos de risco, para se ter uma visão mais amplas de quais fatores agem sobre o processo:

106. Novamente se esclarece que a mencionada listagem serve apenas para guiar os atores da gestão de riscos durante o procedimento, não pretendendo limitar a sua atuação e nem gerar burocracias desnecessárias.

107. O que realmente importa nesse ponto é que todos os eventos de risco levantados tenham relação direta com algum dos objetivos do processo organizacional. Mesmo acontecendo de se levantar um evento de grande relevância, que com certeza pode trazer consequências a outros procedimentos, este não deve ser considerado na gestão de riscos atual. Isso acontece porque a escolha de determinado processo para o gerenciamento tem relação com sua importância dentro do órgão, de forma que o acréscimo de riscos de outros processos desviaria os esforços que ao primeiro deveriam ser dedicados.

108. Ademais, aponta-se que cada risco identificado deve acompanhar a demonstração de suas causas e consequências. Para um mesmo risco podem ser identificadas mais de uma causa e mais de uma consequência, assim como uma causa pode gerar mais de um risco.

109. Por fim, é importante apontar que a própria atividade de identificação de riscos não pode inviabilizar todo o processo avaliado. Por mais que seja ideal a reunião do maior número possível de riscos nesse ponto, a verificação de que esses beiram ao infinito pode dar ao gestor a possibilidade de prosseguir, inicialmente, apenas com aqueles que foram considerados mais emergentes.

110. Como será verificado ao fim deste manual, a etapa denominada de Monitoramento também possibilitará aos responsáveis que avaliem se ainda existem riscos que não foram considerados no procedimento inicial, podendo acrescentá-los ao plano de final de tratamento de riscos após feitas as fases da gestão também com esses.

1. DAS CAUSAS DOS RISCOS

111. Após a identificação dos riscos, cumpre documentá-los de acordo com os critérios de causa, eventos de risco, consequência e controles já existentes, sendo que não raro há confusão entre os três primeiros termos. Todavia, fazer essa distinção é essencial para, nas próximas etapas, entender se determinados controles podem ser aplicados diretamente à causa do risco, de forma preventiva, ou apenas à consequência deste, de forma reparatória.

112. A atenção aos pontos que serão demonstrados é importante para não se classificar um risco como causa ou vice-versa, o que pode acabar acontecendo durante um compartilhamento de ideias (brainstorming) da equipe de trabalho durante a presente fase do procedimento.

113. Inicialmente, é necessário apontar que as causas são os motivos ou gatilhos que podem promover a ocorrência do risco, ou as condições que dão possibilidade para o risco se materializar, as quais muitas vezes têm relação com as ameaças e fraquezas do processo que foram levantados na primeira fase da gestão de riscos.

114. Elas também podem ser identificadas a partir da análise das potenciais fontes de risco (pessoas, processos, sistemas, estrutura organizacional, infraestrutura física, tecnologia, etc) somada a uma vulnerabilidade (número insuficiente, falta de investimento, não regulamentação, obsolescência, falta de segurança, etc).

115. Em resumo, uma causa de risco pode ser qualquer situação, fato, circunstância ou conjunto de condições que aumentam a probabilidade de ocorrência de um risco. Diferente dos eventos de risco, que são incertos e futuros, as causas geralmente são situações que já se podem verificar, já existem, já exercem influência no meio. O evento de risco, por outro lado, é a projeção hipotética que pode decorrer daquela causa.

116. Por exemplo, a falta de capacitação adequada de um servidor (algo já verificável na prática) pode ser a causa do risco de haver erro humano em um procedimento (pode ou não acontecer). Se isso ocorrer, poderá ter como consequência a incidência de falhas no processo ou na qualidade do serviço.

117. Uma vez que a causa é algo sem o qual o risco não se materializa, investir em controles que atuam sobre as causas pode ser uma excelente estratégia para gerir riscos, o que se verá em momento oportuno.

2. DAS CONSEQUÊNCIAS DOS RISCOS

118. Entendido que a causa é algo anterior ao risco, é possível deduzir que a consequência é o resultado da ocorrência de um risco, afetando o objetivo do processo. Portanto, as consequências mais abrangentes de um risco são justamente a impossibilidade de se realizar o objetivo, o atraso na sua execução ou prejuízo à sua completude.

119. É o momento em que um determinado risco se materializa, ou seja, quando ele passa de uma simples possibilidade para uma realidade. Nesse ponto, já que o risco é uma incerteza futura, também deve se ter em mente que as consequências podem ser complexas e variadas, de acordo com os cenários prospectados.

120. Isso significa dizer que não é prudente considerar-se apenas as consequências imediatas e diretas, que ocorrem imediatamente após a incidência do risco, mas também aquelas de longo prazo.

121. Por exemplo, um incidente de segurança cibernética nos sistemas da PRF pode resultar em uma paralisação imediata e momentânea das operações. A longo prazo, todavia, essa violação de dados pode levar a perdas na confiança da sociedade, exposição de metodologias e técnicas sigilosas e danos à reputação, afetando as operações tanto quanto (ou mais que) a consequência imediata.

122. Por fim, as consequências dos riscos devem ser continuamente monitoradas e revisadas, já que mudanças internas ou externas podem alterar a natureza e o impacto dos riscos, o que será melhor explicado em breve. Este processo contínuo de avaliação e revisão ajuda a garantir que a organização esteja sempre preparada para enfrentar os riscos de maneira eficaz.

3. DOS CONTROLES PRÉVIOS

123. É possível que, mesmo antes de se organizar e formalizar propriamente a gestão de riscos sobre um processo de trabalho, já tenha sido notada a possibilidade de ocorrência de uma consequência negativa em algum ponto daquela matéria, razão pela qual pode ter sido criada uma medida de controle que se incorporou ao fluxo processual.

124. Isso decorre do fato de que a gestão de riscos é um procedimento tão natural que é muitas vezes inconsciente. A existência desses controles é salutar e serve para demonstrar que quando o processo natural de gerenciar riscos passa a ser organizado e pensado, muito maior se torna a possibilidade de seu êxito.

125. Esses controles prévios podem ser encarados de duas maneiras dentro da gestão de riscos. A primeira é considerá-los como redutores do nível de risco que será calculado na próxima fase, quando se passa a utilizar a seguinte equação: risco inerente - medida de controle = risco residual. A segunda é desconsiderá-lo inicialmente para que, ao final do procedimento de gerenciamento de riscos possa ser verificada se aquela medida é a mais adequada ao caso, se há outras mais salutares ou se outras medidas podem a ela ser acrescidas.

CAPÍTULO VII - DO CÁLCULO DO NÍVEL DE RISCO (ANÁLISE E AVALIAÇÃO DO RISCO)

126. Como o título deste capítulo já rememora, a presente metodologia sugere que esta fase da gestão de riscos seja a condensação das fases de análise e avaliação de riscos trazidas por outras metodologias conhecidas, sempre como forma de simplificação do processo.

127. Portanto, aqui será feito o cálculo da probabilidade de cada um dos riscos se materializar e do impacto gerado pela ocorrência do evento de risco, multiplicando-se o valor de um pelo outro, assim como será feita a priorização dos riscos conforme o resultado da mencionada equação, do mais alto ao mais baixo (do que exige a maior prioridade de tratamento ao que exige a menor).

128. Quando se fala de probabilidade, deve-se levar em conta a chance de um risco se materializar, conforme a experiência e o julgamento especializado dos donos do risco, ou seja, daqueles que efetivamente trabalham com a matéria. Será atribuído peso de 1 a 5 para a probabilidade de cada risco, conforme os parâmetros apresentados na tabela a seguir:

Probabilidade dos riscos					
Aspectos	Evento pode ocorrer apenas em circunstâncias excepcionais	Evento pode ocorrer em algum momento	Evento deve ocorrer em algum momento	Evento provavelmente ocorra na maioria das circunstâncias	Evento esperado para a maioria das circunstâncias
Frequência	Até 10%	Entre 10% e 30%	Entre 30% e 50%	Entre 50% e 90%	Mais de 90%
Peso	1 - Muito baixa	2 - Baixa	3 - Média	4 - Alta	5 – Muito alta

129. Por sua vez, o impacto se refere à extensão do dano que a materialização do risco pode causar ao objetivo da instituição tratado no processo específico. Essa extensão pode ser pensada a partir de termos financeiros, reputacionais, operacionais, entre outros, e também deve receber um peso de 1 a 5.

Impacto dos riscos					
Aspectos	Evento cujo impacto pode ser absorvido por meio de atividades normais	Evento cujas consequências podem ser absorvidas, mas carecem de esforço para minimizar o impacto	Evento significativo, mas que pode ser gerenciado em circunstâncias normais	Evento crítico, mas que com a devida gestão pode ser suportado	Evento com potencial para levar o negócio a colapso
Peso	1 - Insignificante	2 - Pequeno	3 - Moderado	4 - Grande	5 – Catastrófico

130. A combinação da probabilidade e do impacto ajuda a calcular o nível de risco, que é fundamental para priorizar os riscos e determinar ações de tratamento adequadas. O resultado deste cálculo será organizado em uma matriz de riscos, que é um facilitador visual da situação de todo o procedimento feito até aqui.

131. Antes de apresentar a matriz, todavia, é importante ressalvar que ela não pode ser considerada como um resultado estático, mas apenas uma apresentação momentânea dos processos de trabalho gerenciados, uma vez que tanto os riscos em si quanto os impactos e probabilidades devem ser constantemente revisados, para refletir as mudanças no ambiente operacional e estratégico da PRF. A precisão e utilidade da análise de riscos dependem do conhecimento e compreensão contínuos da organização sobre seus riscos.

132. Pois bem, com base no resultado da multiplicação entre os pesos de impacto e probabilidade é possível saber o lugar do risco dentro da matriz exposta a seguir, que determina se o risco é pequeno, moderado, alto ou crítico.

133. Para que não reste dúvida, aponta-se que apenas constam na tabela os possíveis resultados entre as multiplicações entre os números 1 a 5, razão pela qual não há continuidade perfeita na numeração dos níveis. O que importa é que um nível sempre terá intervalo com valores superiores ao nível abaixo dele.

1. DA PRIORIZAÇÃO DE RISCOS

134. Assim esclarecido e tendo em mãos o resultado das multiplicações dos riscos do procedimento que está sendo gerido, é possível organizá-los, do mais alto ao mais baixo, como forma de priorizar a atuação naqueles que apresentam maiores níveis.

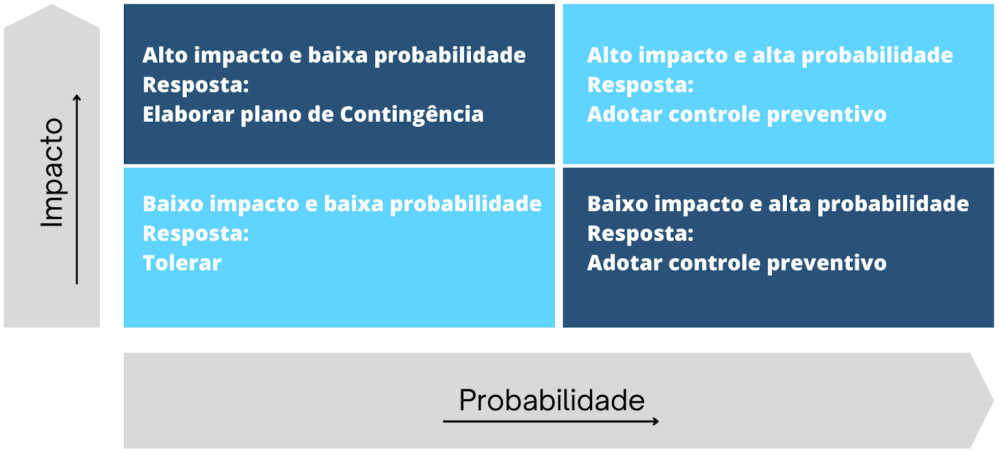
135. Essa organização pode ser feita em uma tabela resumo como a exemplificada a seguir e novamente reproduzida no Anexo V deste manual para auxiliar em procedimentos futuros.

Objetivo(s):				
Riscos (nominal)	**Probabilidade (P)**	**Impacto (I)**	**Cálculo de risco (PxI)**	**Nível do risco**
Risco hipotético 1	5	5	25	Crítico
Risco hipotético 2	5	3	15	Crítico
Risco hipotético 3	3	5	15	Crítico
Risco hipotético 4	2	5	10	Alto
Risco hipotético 5	1	4	4	Moderado
Risco hipotético 6	1	3	3	Pequeno

136. Em relação à priorização dos riscos, que deve ser feita por meio da organização do maior para o menor, é necessário se tecer uma importante observação. No caso de dois ou mais riscos do mesmo nível, como foi demonstrado no exemplo acima, o gestor deve priorizar o de maior impacto, mesmo que tenham valores iguais, já que o impacto é a dimensão mais preocupante.

137. Dentro desse mesmo raciocínio, é inclusive possibilitado ao gestor e sua equipe que eleve um risco cujo cálculo resultou em menor valor (dentro do mesmo nível) se o impacto se demonstrar mais proeminente que o de outro, considerando que apenas os donos do risco possuem a expertise necessária para compreender seus próprios riscos.

138. Mesmo assim, é relevante apontar que a percepção de diferentes valores para probabilidade e impacto também pode ser decisiva na escolha dos tratamentos que serão dedicados a cada risco, uma vez que um risco com impacto considerável, mas com poucas chances de acontecer, pode ser melhor tratado por meio de um controle reparatório, a exemplo de um plano de contingência. Enquanto isso, sendo alta a probabilidade de ocorrência do risco, melhor seria uma atuação prévia voltada para diminuí-la.



139. Outros aspectos dessa situação serão melhor tratados no capítulo seguinte, especialmente no que se refere à aplicação de controles prévios ou posteriores.

2. DA DEFINIÇÃO DO APETITE A RISCOS DA PRF

140. Como já se pôde verificar no Capítulo II deste manual, que diz respeito às definições utilizadas para a metodologia de gestão de riscos da PRF, entende-se que o apetite a riscos é um conceito originário do setor privado, principalmente em organizações financeiras, referindo-se ao montante máximo de risco que uma entidade está disposta a aceitar ou reter em busca de seus objetivos estratégicos e operacionais, que estão geralmente associados à busca de retornos financeiros.

141. No entanto, ao adaptarmos esse conceito para o contexto de um órgão público, como a Polícia Rodoviária Federal, é importante considerar as nuances e especificidades deste ambiente. A PRF, enquanto entidade de segurança pública, não visa ao lucro, mas à promoção do bem-estar coletivo, garantindo a segurança nas rodovias federais, a livre circulação e o combate ao crime.

142. Assim, na PRF, o apetite ao risco pode ser entendido como o grau máximo de risco que, na fase de tratamento aos riscos, pode ser simplesmente aceito (em vez de se adotar algum tratamento propriamente dito). Em um sentido prático, o apetite ao risco da PRF funciona como uma linha limítrofe a partir da qual se deve considerar um tratamento para o risco diferente do aceite.

143. É importante que se defina o apetite a riscos de forma prévia e sendo o mais baixo possível dentro dos recursos disponíveis, já que a PRF possui a incumbência de garantir a efetivação de direitos constitucionais aos cidadãos da forma que melhor estiver ao seu alcance.

144. Assim, sugere-se que o apetite a riscos da PRF apenas possibilite aplicar a aceitação quando se tratar de riscos baixos. Para os demais riscos deve ser no mínimo adotada alguma mitigação.

145. Todavia, reconhece-se que existem algumas atividades na PRF que envolvem um número tão significativo de riscos que os recursos disponíveis seriam incapazes de cobrir medidas de tratamento para grande parte deles, mesmo que acima do nível baixo. De forma semelhante, em processos com número de riscos que beiram o infinito é possível que sequer tenha sido feita a identificação da maioria deles nas fases anteriores, o que naturalmente envolveria a aceitação tácita de riscos que não são baixos.

146. Nesses casos, obviamente, a gestão de riscos deve ser feita dentro dos limites do possível, com aqueles riscos inicialmente identificados e apenas dentro da capacidade financeira da PRF de elaborar medidas de tratamento para eles.

147. Entende-se que a própria natureza da PRF exige que algumas atividades de extremo risco sejam realizadas para o seu bom funcionamento, de forma que o processo de gestão de riscos não deve ser um instrumento que, na medida em que evidencia os altos níveis de eventos danosos, simplesmente inviabilize essas atividades de ocorrerem.

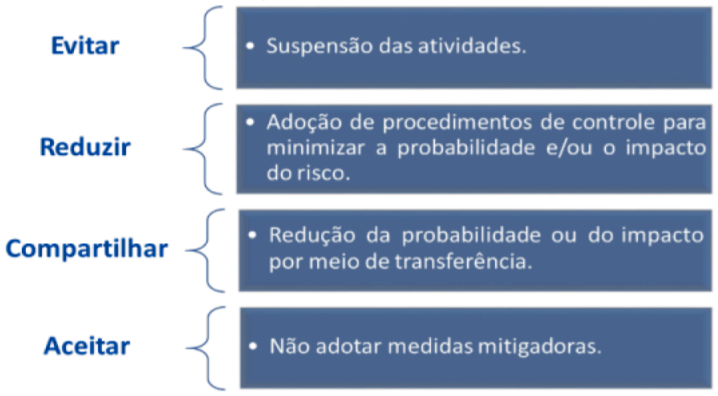
148. Pelo contrário: a gestão precisa servir justamente para auxiliar os servidores que atuam naquele processo a conhecerem com o que estão lidando e não se surpreenderem com certas ocorrências, caso essas de fato se realizem. Ainda que não sejam previstas a totalidade de ocorrências, a previsão de parte delas já pode ser de grande valia para o processo, sendo que o aumento progressivo da maturidade da gestão de riscos na PRF fará com que, com o tempo, novos riscos sejam levados em consideração para os processos que já estão sob análise.

149. O que se pretende dizer neste tópico é que quanto mais aproximado de uma situação ideal, mais baixos serão os riscos a serem aceitos. Por outro lado, uma situação distante da ideal deve se adequar aos recursos disponíveis, sendo justamente essa a razão de ser da tabela de priorização de riscos.

CAPÍTULO VIII – DA RESPOSTA AO RISCO

150. Chegou-se aqui à penúltima fase da gestão de riscos, que de certa forma se caracteriza como a razão de ser de todas as demais fases. Nesse momento deverá ser estabelecido um plano de atuação contra os potenciais riscos encontrados.

151. É possível resumir as modalidades de resposta ou tratamento a riscos nas categorias de evitar, reduzir (ou mitigar), compartilhar (ou transferir) e aceitar. Afora aquela de aceitar, da qual já se falou algumas vezes durante esse manual, as demais servem para todos os níveis de risco e dependem do mérito do responsável pelo risco.



152. A figura aqui representada já é capaz de explicar minimamente o que significa cada uma das modalidades, mas tais exposições serão melhor aprofundadas.

153. A medida de evitar é o mesmo que interromper ou não iniciar a atividade sujeita ao risco. Sugere-se a adoção desta resposta quando a relação custo-benefício da implementação de controles superam os próprios impactos estimados pela eventual ocorrência do risco.

154. Quando se fala em reduzir ou mitigar, tem-se a adoção de medidas que atuem tanto nas causas quanto nas consequências do risco, ou mesmo nas duas, buscando-se reduzir a probabilidade do risco ou seu impacto sobre os objetivos do órgão. Os custos das medidas não podem ser superiores ao impacto estimado da ocorrência do risco.

155. Compartilhar ou Transferir significa compartilhar o risco ou parte dele por meio de terceirização, da contratação de seguros ou da designação de pessoal ou unidade com melhores recursos para gerir o risco. Esta resposta pode ser tomada quando o custo-benefício para adoção de medidas não é adequado ao proprietário do risco e o risco não pode ser evitado.

156. Importante que, no caso de uma unidade da PRF transferir a outras unidades a responsabilidade de tratar aquele determinado risco, estas devem estar cientes e devem ter aceitado a transferência, sendo inútil qualquer designação de responsabilidade não devidamente acertada. Situações como essas já foram responsáveis por atrasos e descumprimentos frente ao Ministério da Justiça e Segurança Pública e a outros órgãos de controle.

157. Por fim, aceitar ou tolerar o risco diz respeito a não adotar nenhuma medida em relação ao risco. Como foi apontado na fase anterior acerca da priorização e do apetite a riscos, a princípio só podem ser aceitos os riscos dentro da faixa do apetite. Na excepcionalidade de se aplicar a aceitação a um risco de nível superior, esta deve ser devidamente justificada pelo dono do risco e a justificativa necessita de autorização da chefia imediata.

158. Para deixar de se aplicar o aceite a um risco dentro do apetite, por outro lado, não é necessária autorização da chefia superior, devendo apenas ficar comprovado que os recursos necessários já foram empregados no tratamento dos demais riscos com prioridade superior e ainda é possível agir sobre aquele risco de menor escala.

159. Com esses apontamentos, os donos do risco devem começar a identificar possíveis medidas de resposta ao risco.

160. Essa identificação deve ser da mais abrangente possível, considerando todas as hipóteses aplicáveis, para que só depois seja feita uma comparação entre a eficácia de cada uma delas, considerando a quantidade e o nível dos riscos por elas mitigados, bem como o grau de redução do nível do risco gerado.

161. Todavia, é necessário se ressaltar que os controles também devem ser propostos sob a ótica de custo/benefício, para que seja possível otimizá-los. Como já mencionado anteriormente, é possível que exista uma quantidade tão elevada de riscos em um procedimento que os recursos disponíveis não são suficientes para a cobertura de medidas para a maioria deles.

162. Isso porque, no setor público, há circunstâncias em que a solução ideal enfrenta obstáculos que impedem sua implementação imediata ou até mesmo a médio prazo. Esses desafios podem incluir a complexidade inerente da solução, custos proibitivos ou um elevado grau de intervenção necessária. Em tais cenários, é prudente propor, como complemento, alternativas viáveis de baixo custo que possam agir diretamente sobre os eventos de riscos, funcionando como controles compensatórios.

163. Um controle compensatório funciona como uma espécie de balanço ou correção temporária dentro da estrutura de controles de uma organização. Sua finalidade é evitar que os eventos de risco ocorram ou, caso ocorram, atenuar sua gravidade.

164. Por exemplo, sendo verificado que o controle ideal é a informatização de um processo, mas essa demanda um período prolongado para ser concretizada, podem ser adotadas medidas manuais temporárias que servem como uma ponte até que a solução definitiva seja implementada.

165. Essa abordagem flexível pode permitir que a PRF continue a funcionar de maneira eficaz, mesmo em face de desafios significativos, garantindo que os riscos sejam gerenciados de forma proativa e econômica.

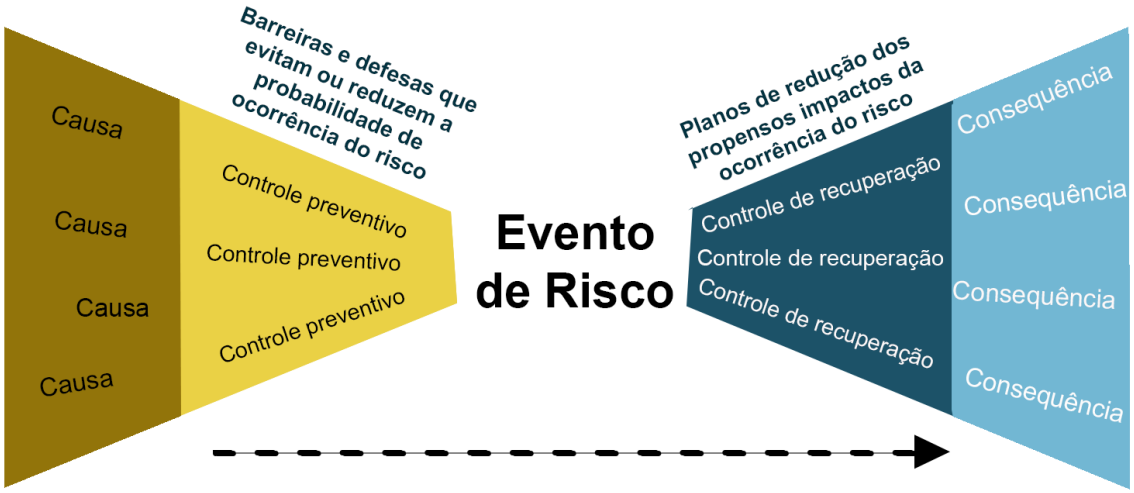
166. Sobre a forma de adoção do momento do controle, ademais, algumas importantes considerações devem ser feitas nesse ponto.

167. É possível que algumas medidas de controle visem agir sobre as causas dos riscos, evitando ou reduzindo a probabilidade de sua ocorrência. Rememora-se que as causas são fatores que dão possibilidade à ocorrência do risco, o que significa dizer que o tratamento dessas causas é geralmente a forma mais eficaz de se eliminar ou mitigar um risco.

168. Assim, uma vez que as causas podem estar ligadas ao contexto em que se insere o processo ou à combinação dos fatores fonte+vulnerabilidade, algumas medidas sobre as causas podem envolver, por exemplo, a realocação de pessoas, a realização de ações de capacitação, o desenvolvimento ou aperfeiçoamento de soluções de TI, a adequação da estrutura organizacional, entre outros.

169. Ocorre que nem todas as vezes será possível agir antes da ocorrência de um risco, seja por impossibilidade lógica, seja por estratégia de trabalho, como no caso mencionado anteriormente de que se tem um risco com baixíssima probabilidade de acontecer, apesar de que sua ocorrência poderia significar um alto impacto nos objetivos do órgão. Nesses casos, muito mais útil e econômico seria prever planos posteriores de lidar com as propensas consequências (que também já foram devida e extensamente projetadas na fase anterior).

170. A visualização da possibilidade de aplicação desses controles prévios ou a posteriori será feita pelo chamado método Bow Tie, ou Laço de Gravata:



171. Para se delimitar quais controles poderão ser utilizados dentro das possibilidades já descritas até aqui, é possível fazer um compartilhamento de ideias entre a equipe por meio da resposta das seguintes perguntas:

- Que medidas poderiam ser adotadas para reduzir a probabilidade de ocorrência do risco?
- Que medidas poderiam ser adotadas para reduzir o impacto do risco no objetivo/resultado?
- É possível adotar medidas para transferir o risco?

172. Ressalta-se que não há qualquer impedimento teórico para a combinação de medidas, mas não se pode esquecer que elas precisam ser escolhidas de acordo com a capacidade técnica e financeira do órgão, de acordo com a priorização dos riscos.

173. Para facilitar essa fase, é possível utilizar a tabela trazida a seguir, com situações meramente hipotéticas para fins didáticos, que será repetida no Anexo tal ao final deste manual.

Causa	É possível amenizar/evitar a causa?	Evento de Risco	É possível amenizar/evitar a consequência?	Consequência
Pessoal sem capacitação	Realização de convênio com fundação de ensino para capacitação Levantamento de cursos disponíveis em plataformas de governo	Erros em procedimentos	-	Paralisação de atividades
Sistemas obsoletos	Estudar contratação de novas tecnologias Aumentar frequência de backup	Perda de dados salvos em sistemas	Plano de recuperação de desastres	Paralisação de atividades Retrabalho Potencial perda de confiança da sociedade

174. Aqui é importante expor os controles que por acaso já existiam no procedimento (conforme exposto no item 3 do capítulo VI deste manual), inclusive para verificar se realmente são as melhores escolhas entre as possíveis.

175. Além disso, a escolha de qual ação de controle será aplicada dentre as possíveis deve levar em consideração eventuais riscos adversos, que são justamente aqueles que surgem como consequência da aplicação de uma medida de controle interno. Assim, é essencial que as medidas propostas sejam pensadas com profundidade.

176. Por fim, escolhidos os controles, deve ser criado um plano de ação para a implementação das medidas de tratamento, que deve conter, pelo menos:

- Medida(s) de tratamento contemplada(s) e o risco relacionado que deseja tratar;
- Objetivos/benefícios esperados por medida de tratamento;
- Responsável pela implementação;
- Breve descrição sobre a implementação;
- Custo estimado para implementação;
- Data prevista para início da implementação;
- Data prevista para o término da implementação.

177. Quanto à definição de quem será o responsável por efetivar o controle são necessários alguns esclarecimentos.

178. Inicialmente, entende-se que essa responsabilidade deveria ser dada a uma área ou a um cargo, uma vez que a indicação nominal de servidores pode gerar o risco de se criar a pessoalização de um processo que tem natureza coletiva e comunitária.

179. Inclusive, nesse sentido, para que a gestão de riscos proporcionasse uma melhor continuidade do processo de trabalho mesmo em situação de mudanças de gestão, suavizando as circunstâncias que geralmente envolvem tais transições.

180. Com a responsabilidade formalmente atribuída a uma área específica (em vez de a um gestor ou servidor), assegurar-se-ia que a prática de gestão de riscos persistisse de maneira constante e eficaz, independentemente das mudanças de pessoal na liderança de uma Diretoria, Coordenação, Setor, entre outros. Desta forma, a continuidade das operações e a eficácia na gestão de riscos seriam mantidas, independentemente das flutuações na composição da equipe.

181. Todavia, a já mencionada Instrução Normativa Conjunta MP/CGU nº 01/2016, em seu art. 20, *caput* e parágrafo primeiro, determina que cada risco mapeado e avaliado deve estar associado a um agente responsável formalmente identificado, o qual deve ser o gestor com alçada suficiente para orientar e acompanhar as ações de mapeamento, avaliação e mitigação do risco.

182. Isso acontece especialmente diante da ausência de cultura de gestão de riscos nos órgãos, de forma que apenas uma definição clara quanto ao agente de quem será cobrado o bom funcionamento dos planos de controle garantiria o real andamento da atividade.

183. Essa situação também diz respeito ao dever tácito do gestor de coordenar sua equipe na boa execução de uma tarefa, de forma que mesmo em se tratando de uma falta de todo um setor, o gestor será responsável em nome de todos os servidores sob sua chefia.

184. Infelizmente, enquanto não se estabelece uma cultura sólida que permita a prática de monitoramento do plano de controle de riscos como algo natural às atividades dos setores, ainda permanecerá a prática de identificação pessoal do responsável.

185. Esclarecidos esses pontos, volta a se destacar que sendo o caso de as iniciativas definidas no Plano de Ação envolverem mais de uma unidade, a equipe responsável pelo processo de gerenciamento de riscos deve encaminhar a proposta de Plano para que essas unidades validem as iniciativas de que irão participar.

186. Por fim, em se tratando de gestão de riscos estratégicos, os planos aprovados necessariamente devem ser remetidos à Coordenação de Controle Interno e seu Setor de Integridade e Gestão de Riscos para atuação no monitoramento dos controles, uma vez que essas medidas também são acompanhadas pela Assessoria Especial de Controle Interno do Ministério da Justiça e Segurança Pública, a qual possui a mencionada Coordenação como intermediária do contato entre os órgãos.

187. Da mesma forma, recomenda-se que os planos de controle da gestão de macroprocessos dentro da PRF também sejam remetidos para acompanhamento, como forma de aperfeiçoar cada vez mais os procedimentos.

188. Planos referentes a outros processos podem permanecer dentro do âmbito das unidades, estando a Coordenação de Controle Interno e o Setor de Integridade e Gestão de Riscos a disposição para dirimir dúvidas e prestar auxílios.

CAPÍTULO IX – DO MONITORAMENTO

189. Dessa forma, o monitoramento deve ser contínuo (antes, durante e depois da implementação do tratamento de riscos), e tem por finalidade detectar mudanças, obter mais informações, analisar tendências, identificar novos riscos, assegurar a eficiência dos controles, identificar possíveis desvios e necessidade de implementar novas ações corretivas, visando ao alcance dos objetivos de cada processo.

190. Na PRF, esse monitoramento é primeira e principalmente feito pelos próprios donos dos riscos, que deverão se atentar para mudanças no ambiente político, de regulamentações, de tecnologia e outras condições que podem afetar os riscos identificados e a eficácia dos controles implantados. O monitoramento regular permite ajustes rápidos e apropriados à medida que os riscos mudam, mantendo-se sempre a ideia de eliminar fatores surpresa.

191. De forma geral, portanto, deve ser verificado se as premissas sobre os riscos permanecem válidas, se houve alguma mudança no contexto ou no processo no qual o risco está associado, no seu nível de risco ou, ainda, se existem novos riscos.

192. Como já se mencionou no capítulo anterior, ademais, o monitoramento deve ser realizado não apenas em nível operacional, mas também estratégico, a depender do tipo de processo em que a gestão de riscos foi realizada. Assim, a alta administração deve se envolver no processo de monitoramento dos riscos para garantir uma visão consolidada e estratégica dos riscos que afetam a organização como um todo.

193. Quanto ao monitoramento das ações de tratamento de riscos, deve ser verificado o funcionamento, o desempenho e os resultados das medidas mitigadoras de forma contínua ou periódica. Assim, tem-se que o monitoramento é parte integrante do processo de gestão e de tomada de decisão e a sua obrigatoriedade e periodicidade deve ser estabelecida como parte das rotinas organizacionais.

194. O monitoramento das ações, desta forma, deve analisar se as ações propostas no Plano de Tratamento de Riscos estão sendo executadas conforme planejado e se estão sendo efetivas, se devem ser ajustadas ou mesmo substituídas.

195. Nesta etapa, é essencial documentar todas as ações de monitoramento e revisões realizadas, bem como as conclusões e decisões tomadas. Isso contribui para a transparência e responsabilização, permitindo uma visão clara do status dos riscos e dos controles estabelecidos. Com base nos resultados do monitoramento, é possível identificar pontos que precisam ser ajustados e melhorados para fins de atualização e melhoria contínua do processo de gestão de riscos.

196. Por fim, aponta-se que a Coordenação de Controle Interno e o Setor de Integridade e Gestão de Riscos tem atribuição de monitorar, junto aos donos dos riscos, o cumprimento dos planos de tratamento definidos na PRF, realizando periodicamente a análise da continuidade das medidas.

197. O monitoramento de alguns processos, inclusive, como já foi citado anteriormente, precisam ser reportados à Assessoria Especial de Controle Interno do Ministério da Justiça e Segurança Pública, razão pela qual se faz necessário que a área técnica responsável apresente informações atualizadas e contínuas àquela Coordenação.

CAPÍTULO X – DAS DISPOSIÇÕES FINAIS

198. O presente manual se presta a fortalecer a cultura de gestão de riscos na PRF, tendo em vista a relevância da ferramenta para a melhoria de processos internos e de entregas de resultados à sociedade.

199. Nesse sentido, a Coordenação de Controle Interno e o Setor de Integridade e Gestão de Riscos têm conduzido uma série de oficinas, centradas na capacitação dos gestores do órgão, buscando disseminar o conteúdo e a metodologia aqui expostos, desmistificando a ideia de complexidade exacerbada ligada à gestão de riscos.

200. Essas oficinas foram desenhadas para abordar os conceitos fundamentais da gestão de riscos, bem como as ferramentas e técnicas de identificação, análise, avaliação e tratamento de riscos. Elas oferecem uma oportunidade valiosa para os gestores entenderem a relevância da gestão de riscos e como ela pode ajudar a alcançar os objetivos da PRF, além de prepará-los para a implementação eficaz do processo de gestão de riscos em suas respectivas áreas de responsabilidade.

201. Para além do compromisso em fortalecer a cultura de gestão de riscos na Sede Nacional, a Coordenação de Controle Interno também está levando as oficinas para as unidades regionais da PRF, como forma de facilitar a aplicação da ferramenta nas operações diárias do órgão e de acordo com as especificidades de cada Estado da Federação.

202. Este movimento é parte integral do planejamento anual e periódico da área, com o intuito de garantir que todos os membros da PRF, independentemente de sua localização, estejam equipados com o conhecimento e as habilidades necessárias para gerenciar efetivamente os riscos.

203. Ao enfatizar a gestão de riscos como uma responsabilidade compartilhada por todos na PRF, a Coordenação de Controle Interno e o Setor de Integridade e Gestão de Riscos estão empenhados em fortalecer a excelência institucional e garantir a entrega contínua de serviços de alta qualidade à sociedade.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT NBR ISO 31000:2019. Gestão de riscos — Princípios e diretrizes. Rio de Janeiro: ABNT.

BRASIL. Constituição da República Federativa do Brasil de 1988.

BRASIL. Controladoria-Geral da União. (2016). Instrução Normativa Conjunta CGU/MP No 01, de 10 de maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. Diário Oficial da União, Brasília, DF, 11 maio de 2016.

BRASIL. Decreto nº 10.180, de 22 de janeiro de 2020. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Brasília, DF, 2020.

BRASIL. Portaria CGU nº 1.089, de 25 de abril de 2018. Institui o Programa de Fortalecimento da Gestão de Riscos e do Controle Interno do Poder Executivo Federal. Brasília, DF, 2018.

BRASIL. Controladoria-Geral da União. (2017). Modelo de Gestão de Riscos para o Poder Executivo Federal. Brasília, DF: CGU.

BRASIL. Controladoria-Geral da União. (2017). Guia de Integração de Gestão de Riscos, Controles Internos e Governança. Brasília, DF: CGU.

BRASIL. Ministério da Economia. (2019). Manual de Gestão de Riscos e Controles Internos da Gestão. Brasília, DF: ME.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). Enterprise Risk Management – Integrating with Strategy and Performance. New Jersey: COSO.

CARDOSO, R. R. Sistema de gestão de riscos – Requisitos com orientações para uso (ISO 31000:2018). Rio de Janeiro: Quality Way, 2019.

CHAPMAN, C.; WARD, S. (2011). Gestão de Riscos em Projetos. Rio de Janeiro: Elsevier.

COSO. (2017). Enterprise Risk Management – Integrating with Strategy and Performance. USA: COSO.

FERREIRA, Gabriela Figueiredo. A governança de riscos nas organizações públicas e privadas. Revista de Administração Pública, Rio de Janeiro, v. 52, n. 3, maio/jun. 2018.

HUBBARD, D.W. A medida do risco: métodos quantitativos aplicados à avaliação de riscos de negócio. Porto Alegre: Bookman, 2009.

HOPKIN, P. (2018). Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management. London: Kogan Page.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (2018). ISO 31000 - Risk management. Geneva: ISO.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (2018). ISO 31010 - Risk management - Risk assessment techniques. Geneva: ISO.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (2021). ISO 31022 - Legal risk management – Guidelines. Geneva: ISO.

INSTITUTE OF RISK MANAGEMENT. (2012). Risk Management Standard. London: IRM.

MANAGEMENT OF RISK: GUIDANCE FOR PRACTITIONERS (ORANGE BOOK). (2010). 3rd Edition. London: The Stationery Office.

PROJECT MANAGEMENT INSTITUTE. (2017). A Guide to the Project Management Body of Knowledge (PMBOK Guide) – Sixth Edition. Pennsylvania: PMI.

PAULO, J. S. (2010). Gerenciamento de Riscos Corporativos: estruturação de um modelo para a prática sob a ótica da governança corporativa. São Paulo: Atlas.

RENN, O.; WALKER, K. D. (2008). Global Risk Governance: Concept and Practice Using the IRGC Framework. Dordrecht: Springer.

TAYLOR, J. (2010). Enterprise Risk Management: A Common Framework for the Entire Organization. Burlington: Elsevier.

ANEXO I - Template auxiliar para compreensão do contexto

Meu processo/atividade/projeto/contrato/operação tem os seguintes objetivos:	
Objetivos Gerais:	Objetivos Específicos:
Como o meu processo/atividade/projeto/contrato/operação é influenciada por...	
Cultura organizacional	Panorama político
Políticas Internas	Panorama Socioeconômico
Recursos humanos	Legislação
Materiais disponíveis	Visão da sociedade e da mídia
Sistemas	Cultura
Tecnologia	Feriados, movimentações locais, etc
(...)	(...)

ANEXO II - Template auxiliar para levantamento de riscos

Com base nos levantamentos de contexto, consigo visualizar os seguintes riscos:

ANEXO III - Template auxiliar para definir causas e consequências dos riscos

Devido a <CAUSA>	poderá ocorrer <EVENTO DE RISCO>	o que poderá levar a <CONSEQUÊNCIA>	impactando no <OBJETIVO>

ANEXO IV - Templates auxiliares para pontuar causas e consequências

Probabilidade dos riscos					
Aspectos	Evento pode ocorrer apenas em circunstâncias excepcionais	Evento pode ocorrer em algum momento	Evento deve ocorrer em algum momento	Evento provavelmente ocorra na maioria das circunstâncias	Evento esperado para a maioria das circunstâncias
Frequência	Até 10%	Entre 10% e 30%	Entre 30% e 50%	Entre 50% e 90%	Mais de 90%
Peso	1 - Muito baixa	2 - Baixa	3 - Média	4 - Alta	5 – Muito alta

Impacto dos riscos					
Aspectos	Evento cujo impacto pode ser absorvido por meio de atividades normais	Evento cujas consequências podem ser absorvidas, mas carecem de esforço para minimizar o impacto	Evento significativo, mas que pode ser gerenciado em circunstâncias normais	Evento crítico, mas que com a devida gestão pode ser suportado	Evento com potencial para levar o negócio a colapso
Peso	1 - Insignificante	2 - Pequeno	3 - Moderado	4 - Grande	5 – Catastrófico

ANEXO V - Template auxiliar para cálculo do nível de risco

Objetivo (s):				
Riscos (nominal)	**Probabilidade (P)**	**Impacto (I)**	**Cálculo de risco (PxI)**	**Nível do risco**

ANEXO VI - Template auxiliar para identificação de possíveis controles

Causa	É possível amenizar/evitar a causa?	Evento de Risco	É possível amenizar/evitar a consequência?	Consequência

ANEXO VII - Template auxiliar para formalização de Plano de Controle

Risco	Medida(s) de tratamento escolhidas	Como será feita a implementação da medida	Benefícios esperados pela medida	Responsável pela implementação	Custo estimado para implementação	Data prevista para início da implementação	Data prevista para o término da implementação