CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º A presente normativa tem o intuito de definir a metodologia para a gestão de riscos no âmbito do Instituto Federal da Paraíba (IFPB), abrangendo, de forma estruturada e sistematizada, os aspectos detalhados inerentes a cada uma de suas etapas no processo de gestão de riscos.

§1º Este documento é indissociável à Política de Gestão de Riscos do IFPB, devendo com ela estar de acordo.

§ 2º O fluxo das etapas da metodologia, bem como os fluxos detalhados de cada uma de suas etapas, estarão disponíveis no sítio institucional para consulta.

Art. 2º A presente metodologia tem como principais referências os seguintes documentos:
I - Política de Gestão de Riscos do IFPB;

II - Instrução Normativa MP/CGU nº 01/2016;

III - Decreto nº 9.203/2017; e

VI - Gestão de Riscos: Avaliação da Maturidade, do TCU/2018.

Art. 3º O Apetite a Riscos do IFPB será considerado inicialmente como “moderado”, logo, serão assumidos riscos de forma controlada e mensurada, observados os limites previamente estabelecidos, de modo a assegurar o equilíbrio entre a segurança na condução das atividades e a promoção da inovação, visando ao alcance dos objetivos estratégicos.

CAPÍTULO II

DAS DEFINIÇÕES

Art. 4º As principais definições, necessárias para o entendimento do processo de gerenciamento de riscos, são:

I - Processo: é o conjunto de ações e atividades inter-relacionadas, que são executadas para alcançar um produto, resultado ou serviço predefinido;

II - Macroprocesso: é um agrupamento de processos necessários para gerar um determinado resultado, vinculado à missão e à visão da instituição. No IFPB, os macroprocessos se encontram na cadeia de valor.

III - Risco: é a possibilidade de ocorrência de um evento que tenha impacto no alcance dos objetivos;

IV - Evento de risco: é um fato ou acontecimento que impacta negativamente o alcance do resultado esperado de um processo;

V - Causas do evento risco: são as condições que podem dar origem a um evento de risco;
VI - Consequências do evento de risco: são os resultados da ocorrência de um evento de risco sobre os objetivos do processo ou da instituição.

VII - Gerenciamento de risco: É o processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações que possam afetar a instituição, destinado a fornecer segurança razoável no alcance dos seus objetivos;

VIII - Apetite a risco: é o nível de risco que uma organização está disposta a aceitar para atingir seus objetivos;

IX - Risco inerente: é o risco a que uma organização está exposta sem considerar quaisquer medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto;

X - Risco residual: é o risco a que uma organização está exposta após a implementação de medidas de controle para o tratamento do risco, incluindo controles corretivos; e

XI - Planos de Controle: são planos de ação gerados para mitigar ou reduzir os riscos de cada processo organizacional, contendo seus riscos, prazos e medidas de tratamento.

CAPÍTULO III

DOS AGENTES RESPONSÁVEIS E DA ESTRUTURA DE GOVERNANÇA DA GESTÃO DE RISCOS

Art. 5º Os agentes responsáveis são:

I - Gestor de Risco:

a) todo servidor responsável por um setor institucional, independente de ter ou não função gratificada;

b) são responsáveis pelo monitoramento e controle das atividades diretamente relacionadas ao seu setor e a alocação de recursos e servidores com o fim de favorecer a gestão de riscos da unidade.

II -Núcleo de Integridade e Governança:

a) é o núcleo vinculado ao Gabinete da Reitoria, responsável pela organização administrativa e planejamento no que se refere ao desenvolvimento das ações de integridade e governança; e

b) tem a função de auxiliar e assessorar as entidades envolvidas nas diversas etapas da gestão de riscos.

III - Comitê de Governança, Riscos e Controle:

a) O Comitê de Governança, Integridade, Riscos e Controles Internos da Gestão – CGIRC é a instância colegiada de caráter consultivo e estratégico destinada a assessorar a Alta Administração na implementação, monitoramento e aprimoramento das práticas de

governança institucional, integridade pública, gestão de riscos e controles internos da gestão no âmbito do IFPB.

IV – Unidade de Auditoria Interna Governamental:

a) é o órgão vinculado ao Conselho Superior - CONSUPER, responsável pela avaliação e consultoria no que se refere ao desenvolvimento das ações de integridade e governança.

CAPÍTULO IV

DA CLASSIFICAÇÃO DA NATUREZA DOS RISCOS

Art. 6º Os riscos podem ser classificados da seguinte maneira:

I - Risco operacional: quando o evento de risco pode gerar falhas, deficiências ou inadequações de processos internos, pessoas, infraestrutura e sistemas;

II - Risco legal: quando o evento de risco pode gerar irregularidades em atividades já normatizadas;

III - Risco financeiro/orçamentário: quando o evento de risco pode gerar prejuízo ou comprometimento à execução financeira/orçamentária ou à obtenção de recursos;

IV - Risco de imagem/reputação: quando o evento de risco pode gerar prejuízo ou comprometimento à confiança da sociedade na capacidade da instituição cumprir a sua missão;

V - Risco social: quando o evento de risco pode provocar prejuízo direto à geração de valor por parte da instituição, afetando a sociedade e a missão institucional; e

VI - Risco à integridade: quando o evento de risco pode gerar corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta que possam comprometer os valores e padrões preconizados pela Instituição e a realização de seus objetivos.

Parágrafo único. Para fins do disposto no inciso VI, consideram-se categorias de riscos à integridade, dentre outras:

I – abuso de posição ou de poder em favor de interesses privados;

II – nepotismo;

III – conflito de interesses;

IV – pressão interna ou externa, de natureza ilegal ou antiética, com vistas a influenciar agente público a atuar de forma parcial ou em desconformidade com sua autonomia técnica;

V – solicitação ou recebimento de vantagem indevida;

VI – utilização de recursos públicos em favor de interesses privados;

VII – conduta profissional inadequada;

VIII – uso indevido de autoridade, inclusive contra o exercício profissional;

IX – uso indevido de autoridade contra a honra ou o patrimônio;

X – uso indevido, manipulação ou supressão de dados e informações;

XI – desvio de pessoal e/ou de recursos materiais; e

XII – interferências externas, políticas ou institucionais que possam comprometer a imparcialidade, a legalidade e a consecução dos objetivos institucionais.

CAPÍTULO V

DO GERENCIAMENTO DE RISCOS

Art. 7º O processo de gerenciamento de riscos se dará em cinco etapas sequenciais:

I - a primeira etapa consiste na seleção e caracterização do processo organizacional a ser gerenciado;

II - a segunda etapa consiste na identificação e caracterização dos riscos dos processos selecionados;

III - a terceira etapa consiste na avaliação dos riscos;

IV - a quarta etapa consiste na definição de resposta aos riscos; e

V - a quinta etapa consiste na comunicação e monitoramento dos riscos e controles.

§1º O planejamento e execução das etapas de I a IV são de responsabilidade de cada gestor de riscos.

§2º A comunicação e o monitoramento, com a devida divisão de atribuições, é responsabilidade do Gestor de Risco, Comitê de Governança, Riscos e Controles, NIG e UAIG.

Seção I

DA SELEÇÃO E CARACTERIZAÇÃO DOS PROCESSOS ORGANIZACIONAIS

Art. 8º A seleção dos processos organizacionais será realizada pelos gestores de risco a partir de uma análise que considere a sua relevância e o contexto institucional.

§ 1º É facultado ao gestor utilizar o modelo de priorização de processos disponível no site institucional.

§ 2º Para fins do disposto no caput, deverão ser considerados, sempre que disponíveis:

I – recomendações, determinações ou achados oriundos de órgãos de controle interno e externo;

II – resultados de auditorias internas e externas;

III – histórico de ocorrências, falhas ou irregularidades;

IV – grau de impacto potencial no alcance dos objetivos estratégicos; e

V – exposição a riscos à integridade e à conformidade normativa.

Seção II

IDENTIFICAÇÃO E CARACTERIZAÇÃO DOS RISCOS

Art. 10 Nessa etapa, devem ser fornecidas as seguintes informações a respeito de cada processo:

I - os eventos de risco associados ao processo;

II - as causas desses eventos de risco;

III - as prováveis consequências; e

IV - a classificação da natureza dos riscos envolvidos em cada evento.

Art. 9º O processo deverá ser caracterizado através do fornecimento de informações básicas, sendo elas:

I - o nome do processo organizacional;

II - o macroprocesso a ele correspondente;

III - os objetivos do processo;

IV - nome do gestor do processo;

V - nome do responsável pela análise; e

VI - o período considerado para a realização da análise de riscos do processo.

Parágrafo único. Além dessas informações obrigatórias, outras informações podem ser solicitadas, de modo complementar, como a realização da análise ambiental do processo (matriz SWOT), brainstorming, entrevistas, visitas técnicas, pesquisas, diagrama de causa e efeito, bow-tie etc, conforme o manual disponível no site institucional.

Seção III

AVALIAÇÃO DOS RISCOS

Art. 11 Nesta etapa são determinadas a probabilidade de ocorrência das causas do evento de riscos, o impacto de suas consequências na instituição, o risco inerente e o risco residual. Para tanto, necessita-se das seguintes subetapas:

I - determinação da probabilidade;

II - determinação do impacto;

III - mensuração do risco inerente;

IV - verificação dos controles já existentes;

V - determinação da probabilidade incluindo os controles;

VI - determinação do impacto incluindo os controles; e

VII - mensuração do risco residual.

Art. 12 A probabilidade de ocorrência das causas dos eventos de risco segue os seguintes critérios:

I - caso seja improvável a sua ocorrência, a probabilidade é considerada “muito baixa” e tem resultado igual a 1;

II - caso o evento possa ocorrer, mas as circunstâncias pouco indicam essa possibilidade, a probabilidade é considerada “baixa” e tem resultado igual a 2;

III - caso seja possível que o evento ocorra, uma vez que as circunstâncias indicam moderadamente essa possibilidade, a probabilidade é considerada “média” e tem resultado igual a 5;

IV - caso seja provável que o evento ocorra, uma vez que as circunstâncias indicam fortemente essa possibilidade, a probabilidade é considerada “alta” e tem resultado igual a 8; e

V - caso seja praticamente certo que o evento ocorra, já que as circunstâncias indicam claramente essa possibilidade, a probabilidade é considerada “muito alta” e tem resultado igual a 10.

Parágrafo único Para aumentar o nível de precisão e confiabilidade de mensuração da probabilidade é muito importante que seja levado em consideração o histórico de ocorrência da causa avaliada.

Art. 13 Caso o evento de risco ocorra, a avaliação do impacto de suas consequências se dará sob seis eixos, definidos abaixo:

I - esforço de gestão;

II - regulação;

III - reputação;

IV - serviços à sociedade;

V - intervenção hierárquica; e

VI - orçamentário.

§1º Os pesos e a forma de mensuração de cada eixo estão definidos no referido manual.

§2º O nível do impacto possui escala de 1 (impacto muito baixo) a 10 (impacto muito alto).

Art. 14 O Risco Inerente é o resultado da multiplicação da probabilidade pelo impacto, desconsiderando os controles já existentes.

Art. 15 O Risco Residual é encontrado após a definição do Risco Inerente, devendo ser reavaliados a probabilidade e o impacto do evento de risco, agora considerando a influência dos controles já existentes.

§1º Os controles já existentes se referem a ações realizadas anteriormente à ocorrência do evento de risco, mitigando os seus efeitos negativos.

§2º Para cada controle existente deverão ser informados sua descrição, se o procedimento de controle está formalizado e é adequado (suficiente) bem como se está sendo executado, conforme o manual supracitado.

§3º A ausência de controles também deve ser informada.

Art. 16 Para a definição dos níveis de risco inerente e residual devem ser utilizados os critérios e a matriz de probabilidade x impacto definidos a seguir:

I - “risco baixo”, caso o seu resultado seja menor ou igual a 9,99;

II - “risco médio”, caso o seu resultado seja maior que 9,99 e menor ou igual a 39,99;

III - “risco alto”, caso o seu resultado seja maior que 39,99 e menor que 79,99; e

IV - “risco extremo”, caso o seu resultado seja maior ou igual a 80,00.

Parágrafo único A matriz de probabilidade x impacto encontra-se no referido manual.

Seção IV

RESPOSTA AOS RISCOS

Art. 17 Nesta etapa são definidos os riscos que serão priorizados e as respectivas medidas de controle a serem adotadas para modificar o nível do Risco Residual.

Art. 18 A priorização dos riscos varia de acordo com o Risco Residual identificado e o Apetite a Riscos do instituto, conforme os critérios a seguir:

I - risco baixo, o nível de risco está dentro do apetite a risco da instituição:

a) geralmente não necessita ação especial nem requer atividade de monitoramento específica, e a adoção de medidas de mitigação pode gerar um custo mais elevado que a ocorrência do evento que prejudica o processo.

II - risco médio, o nível de risco está dentro do apetite a risco da instituição:

a) geralmente não necessita de ação especial, porém requer atividades de monitoramento específicas e atenção da unidade na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.

III - risco alto, o nível de risco está acima do apetite a risco:

a) qualquer risco neste nível deve ser comunicado ao gestor da unidade e deve ser tomada medida específica para sua redução.

IV - risco extremo, o nível de risco está muito acima do apetite a risco:

a) qualquer risco neste nível deve ser comunicado ao gestor da unidade e deve ser tomada medida imediata para sua redução.

Art. 19 Considerando o estágio inicial de implantação da gestão de riscos no IFPB, devem ser priorizados o tratamento dos riscos que estão acima do limite de apetite a risco da instituição, portanto os riscos mensurados como altos ou extemos.

§1º A adoção de medidas de controle para riscos que estão dentro do apetite a risco da instituição (risco baixo ou moderado) deve ser devidamente justificada pelo gestor de risco.

§2º Nos riscos altos ou extremos, caso a resposta a riscos tenha sido "aceitar" o gestor deve justificar porque não adotará medida de controle para diminuir o nível de risco em questão.

Art. 20 As medidas de controle adotadas podem ser as seguintes:

I - reduzir ou mitigar: um risco normalmente é reduzido ou mitigado quando é classificado como "alto" ou "crítico", e a implementação de controles, neste caso, apresenta um custo/benefício adequado, devendo ser adotadas medidas de tratamento capazes de diminuir os níveis de probabilidade e/ou impacto do risco a um nível dentro, ou o mais próximo possível, das faixas aceitáveis de apetite a risco do IFPB;

II - compartilhar ou transferir: um risco é compartilhado ou possui sua responsabilidade transferida quando é classificado como "alto" ou "crítico", mas a implementação de controles pelo IFPB não possui uma relação custo/benefício favorável. Nesse caso transfere-se parte, ou toda a responsabilidade das medidas de controle para terceiros;

III - evitar: um risco normalmente é evitado quando é classificado como "alto" ou "crítico" e a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades dispostas a compartilhar o risco com a instituição. O risco pode ser evitado através da remoção integral de todas as causas de sua ocorrência, o que na prática significa não executar o processo organizacional objeto do risco; e

IV - aceitar: um risco normalmente é aceito quando seu nível está nas faixas de apetite a risco da instituição ou quando não é possível ou viável tratá-lo de outra forma. Quando se aceita um risco, significa que a instituição concorda em enfrentar os impactos do risco caso ele ocorra. Um plano de contingência pode ser desenvolvido para essa eventualidade.

Art. 21 O Plano de Controle de Riscos consiste em um plano de ações para a implementação de medidas e iniciativas de controle aos riscos que tiveram como resposta a redução ou mitigação.

§1º Riscos que serão evitados, compartilhados, transferidos ou aceitos não devem fazer parte do Plano de Controle de Riscos.

§2º Cada Gestor de Riscos deverá elaborar o plano de controle para os riscos sob sua responsabilidade, ou seja, os riscos do setor a qual é responsável.

§3º O Plano de Controle de Riscos será avaliado, no momento oportuno, pelo Comitê de Governança, Riscos e Controles, com o intuito de validar e propor melhorias ao seu conteúdo.

§4º Os Planos de Controle de Riscos devem ser enviados à NIG, 30 dias antes da conclusão da atualização do Plano de Desenvolvimento Institucional (PDI), para que possam ser anexados ao documento de forma adequada.

Art. 22 O Plano de Controle de Riscos deve conter, pelo menos, as seguintes informações:
I - controle proposto;

II - o tipo de controle, se será preventivo ou corretivo;

III - o objetivo do controle, se é adotar um novo controle ou melhorar um já existente;

IV - o setor responsável;

V - data prevista para início da implementação; e

VI - data prevista para o término da implementação.

Parágrafo único. Além dessas informações obrigatórias, outras informações podem ser solicitadas, de modo complementar.

Seção V

MONITORAMENTO E COMUNICAÇÃO

Art. 23 O monitoramento e a comunicação são atividades que se interrelacionam, fornecendo subsídios para possíveis atualizações na avaliação de riscos, no plano de controle e no processo de gestão de riscos.

Art. 24 O monitoramento poderá ocorrer nos seguintes âmbitos:

I - no funcionamento do processo de gestão de riscos institucionais;

II - na implementação das ações mitigadoras previstas no Plano de Controle de Riscos e seus resultados; e

III - no acompanhamento da evolução dos níveis dos riscos que ficaram fora do Plano de Controle de Riscos.

Art. 25 O Comitê de Governança, Riscos, Controles e Integridade é responsável por:

I - monitorar a evolução dos principais riscos institucionais;

II - monitorar a elaboração e execução dos planos de controle de risco; e

III - monitorar o cumprimento de suas recomendações e orientações.

Art. 26 Compete ao Gestor de Riscos monitorar a evolução dos riscos dos processos de sua responsabilidade.

§1º Anualmente os gestores de risco devem elaborar o Relatório de Monitoramento de Riscos (RMR), conforme Anexo disponibilizado no site institucional, que conterá as seguintes informações:

I - ocorrência de evento de risco não identificado anteriormente;

II - alteração nos níveis de riscos dos processos, em relação ao relatório anterior;

III - estágio de execução dos planos de controle, bem como seus resultados; e

IV - técnica de identificação de riscos utilizada (sugestões de técnicas presentes no referido manual).

§2º O RMR deverá ser enviado ao NIG um mês antes da reunião ordinária anual do Comitê de Governança, Riscos e Controles.

Art. 27 O Comitê de Governança, Riscos e Controles, o NIG e os gestores de riscos deverão manter fluxo regular e constante de informações entre si, visando o êxito na execução da gestão de riscos no IFPB.

Art. 28 Todos os gestores de riscos devem informar aos servidores do seu setor sobre os riscos envolvidos na execução dos processos e das medidas de controle adotadas.

Art. 29 Deverão ser disponibilizadas, no site institucional, informações relevantes sobre a gestão de riscos do IFPB para ciência e acompanhamento dos servidores e da comunidade externa.

Parágrafo único. Cabe ao NIG o gerenciamento das informações presentes no site.

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS

Art. 30. A gestão de riscos será apoiada por sistema informatizado ou ferramenta tecnológica institucional destinada ao registro, acompanhamento e monitoramento dos riscos, controles e planos de tratamento.

Art. 31 O NIG apoiará os setores no desenvolvimento das etapas da gestão de riscos apresentadas nesta metodologia.

Art. 32 Em sintonia com a Política de Gestão de Riscos do IFPB, a presente normativa deve ser aprovada pelo Comitê de Governança, Integridade, Riscos e Controles.

Art. 33 Este documento deve ser revisado periodicamente pelo NIG, e atualizado quando necessário.